Integriertes Management von Security-Frameworks

Habilitationsschrift

an der
Fakultät für Mathematik, Informatik und Statistik
der Ludwig-Maximilians-Universität München

von

Wolfgang Hommel

Januar 2012

Integriertes Management von Security-Frameworks

Habilitationsschrift im Fach Informatik

an der
Fakultät für Mathematik, Informatik und Statistik
der Ludwig-Maximilians-Universität München

vorgelegt von

Wolfgang Hommel

Tag der Einreichung: 14. Januar 2012

Fachmentorat:

Prof. Dr. Heinz-Gerd Hegering	Ludwig-Maximilians-Universität München
Prof. Dr. Dieter Kranzlmüller	Ludwig-Maximilians-Universität München
Prof. Dr. Martin Wirsing	Ludwig-Maximilians-Universität München
Prof. Dr. Burkhard Stiller	Universität Zürich, ETH Zürich

Freude an der Arbeit lässt das Werk trefflich geraten. — Aristoteles

Die vorliegende Habilitationsschrift setzt sich unter anderem mit der Herausforderung auseinander, die Sicherheitseigenschaften komplexer IT-Systeme quantitativ zu analysieren. In Ermangelung standardisierter Basisgrößen und Einheitendefinitionen muss beim aktuellen Stand der Technik oft auf indirekte und nur eingeschränkt ausdrucksstarke Indikatoren zurückgegriffen werden. Analog dazu lassen auch die thematische Breite und der Umfang der Darstellung der erarbeiteten Ergebnisse nur indirekte Rückschlüsse darauf zu, welche Leidenschaft der Vorbereitung und Erstellung dieses Werks zugrunde liegt.

Trotz dieser Schwierigkeiten bei der exakten Quantifizierung ist offensichtlich, dass die hier dargelegten wissenschaftlichen Arbeiten nicht möglich gewesen wären, wenn sie nicht in ein Umfeld eingebettet worden wären, das ihre freie Entfaltung begünstigt und vorangetrieben hat. Denjenigen, die dieses Umfeld für mich am Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften und an der Ludwig-Maximilians-Universität München geschaffen und maßgeblich zu ihm beigetragen haben, möchte ich an dieser Stelle danken.

Mein außerordentlicher Dank gilt Prof. Dr. Heinz-Gerd Hegering, der mich und meine Arbeit nicht nur jahrelang begleitet und gefördert, sondern auch weit über methodische und inhaltliche Aspekte hinausgehend geprägt hat. Ohne seine herausragende wissenschaftliche Betreuung, die mir von ihm übertragenen Aufgaben und Verantwortungen sowie die gelassenen Freiheiten würde es diese Arbeit nicht geben.

Sehr großer Dank gebührt meinen Fachmentoren Prof. Dr. Dieter Kranzlmüller und Prof. Dr. Martin Wirsing von der Ludwig-Maximilians-Universität München sowie Prof. Dr. Burkhard Stiller als externem Gutachter. Sie alle wurden vor meiner Tendenz gewarnt, mich im Schriftlichen nicht immer kurz zu fassen, haben sich davon aber nicht abschrecken lassen, sondern im Gegenteil erheblich zum Gelingen dieser Arbeit beigetragen.

Sehr herzlich danke ich Prof. Dr. Arndt Bode, Dr. Victor Apostolescu und PD Dr. Helmut Reiser, die mich am Leibniz-Rechenzentrum immer sehr unterstützt und meine persönliche Weiterentwicklung gefördert haben. Viele Kolleginnen und Kollegen am Leibniz-Rechenzentrum, insbesondere im Security-Team und in der Gruppe Netzplanung, waren mir stets kompetente Diskussionspartner. Dafür bin ich ihnen und auch allen ehemaligen und aktiven Mitgliedern meiner wissenschaftlichen Heimat, des Munich Network Management Teams, sehr dankbar.

Mein innigster Dank gilt meiner Familie, die mir mit Rückhalt und Geduld zur Seite stand und mich nie vergessen ließ, dass das Leben bei Weitem nicht nur aus Arbeit besteht.

München, im Frühjahr 2012

Kurzfassung

Security-Frameworks sind baukastenähnliche, zunächst abstrakte Konzepte, die aufeinander abgestimmte technische und organisatorische Maßnahmen zur Prävention, Detektion und Bearbeitung von Informationssicherheitsvorfällen bündeln. Anders als bei der Zusammenstellung eigener Sicherheitskonzepte aus einer Vielzahl punktueller Einzelmaßnahmen wird bei der Anwendung von Security-Frameworks das Ziel verfolgt, mit einem relativ geringen Aufwand auf bewährte Lösungsansätze zur Absicherung von komplexen IT-Diensten und IT-Architekturen zurückgreifen zu können. Die praktische Umsetzung eines Security-Frameworks erfordert seine szenarienspezifische Adaption und Implementierung, durch die insbesondere eine nahtlose Integration in die vorhandene Infrastruktur sichergestellt und die Basis für den nachhaltigen, effizienten Betrieb geschaffen werden müssen.

Die vorliegende Arbeit behandelt das integrierte Management von Security-Frameworks. Im Kern ihrer Betrachtungen liegen folglich nicht individuelle Frameworkkonzepte, sondern Managementmethoden, -prozesse und -werkzeuge für den parallelen Einsatz mehrerer Frameworkinstanzen in komplexen organisationsweiten und -übergreifenden Szenarien. Ihre Schwerpunkte werden zum einen durch die derzeit sehr technische Ausprägung vieler Security-Frameworks und zum anderen durch die fehlende Betrachtung ihres Lebenszyklus über die szenarienspezifische Anpassung hinaus motiviert. Beide Aspekte wirken sich bislang inhibitorisch auf den praktischen Einsatz aus, da zur Umsetzung von Security-Frameworks immer noch ein erheblicher szenarienspezifischer konzeptioneller Aufwand erbracht werden muss.

Nach der Diskussion der relevanten Grundlagen des Sicherheitsmanagements und der Einordnung von Security-Frameworks in Informationssicherheitsmanagementsysteme werden auf Basis ausgewählter konkreter Szenarien mehr als 50 Anforderungen an Security-Frameworks aus der Perspektive ihres Managements abgeleitet und begründet gewichtet. Die anschließende Anwendung dieses Anforderungskatalogs auf mehr als 75 aktuelle Security-Frameworks zeigt typische Stärken sowie Schwächen auf und motiviert neben konkreten Verbesserungsvorschlägen für Frameworkkonzepte die nachfolgend erarbeiteten, für Security-Frameworks spezifischen Managementmethoden.

Als Bezugsbasis für alle eigenen Konzepte dient eine detaillierte Analyse des gesamten Lebenszyklus von Security-Frameworks, der zur grundlegenden Spezifikation von Managementaufgaben, Verantwortlichkeiten und Schnittstellen zu anderen Managementprozessen herangezogen wird. Darauf aufbauend werden an den Einsatz von Security-Frameworks angepasste Methoden und Prozesse u. a. für das Risikomanagement und ausgewählte Disziplinen des operativen Sicherheitsmanagements spezifiziert, eine Sicherheitsmanagementarchitektur für Security-Frameworks konzipiert, die prozessualen Schnittstellen am Beispiel von ISO/IEC 27001 und ITIL v3 umfassend ausgearbeitet und der Einsatz von IT-Sicherheitskennzahlen zur Beurteilung von Security-Frameworks demonstriert.

Die praktische Anwendung dieser innovativen Methoden erfordert dedizierte Managementwerkzeuge, die im Anschluss im Detail konzipiert und in Form von Prototypen bzw. Simulationen umgesetzt, exemplifiziert und bewertet werden. Ein umfassendes Anwendungsbeispiel demonstriert die praktische, parallele Anwendung mehrerer Security-Frameworks und der spezifizierten Konzepte und Werkzeuge. Abschließend werden alle erreichten Ergebnisse kritisch beurteilt und ein Ausblick auf mögliche Weiterentwicklungen und offene Forschungsfragestellungen in verwandten Bereichen gegeben.

Abstract

Security frameworks at first are modular, abstract concepts that combine technical as well as organizational measures for the prevention, detection, and handling of information security incidents in a coordinated manner. Unlike the creation of scenario-specific security concepts from scratch, for which one has to choose from a plethora of individual measures, using security frameworks pursues the goal of reducing the required time and effort by applying proven solutions for securing complex IT services and IT architectures. The practical realization of a security framework requires its scenario-specific customization and implementation, which especially need to ensure its seamless integration into the existing infrastructure and provides the basis for sustained, efficient operations.

This thesis highlights the integrated management of security frameworks. Therefore, it does not focus on individual security framework concepts, but on innovative management methods, processes, and tools for operating multiple security framework instances in complex enterprise-wide and inter-organizational scenarios. Its core contributions are motivated by the very technically oriented characteristics of current security frameworks on the one hand and by the lack of a holistic view on their life cycle that reaches beyond the customization phase on the other hand. These two aspects still inhibit the wide-spread practical application of security frameworks because still significant scenario-specific conceptual efforts have to be made in order to operate and manage the framework instances.

After the discussion of the relevant fundamentals of security management and the classification of security frameworks into information security management systems, more than 50 management-specific requirements for security frameworks are derived from practical scenarios and get reasonably weighted. The application of the resulting criteria catalogue to more than 75 current security frameworks points out their typical strengths and weaknesses; besides improvement proposals for the analyzed security frameworks, it also motivates the security-framework-specific management methods that are developed afterwards.

For each of the proposed concepts, a detailed analysis of the complete security framework life cycle serves as a reference base. It is also used to specify the basic management tasks, responsibilities, and interfaces to related management processes. Based on this life cycle specification, security-framework-specific management methods and processes, e. g., for risk management and for selected security operations tasks are specified, a security management architecture for security frameworks is designed, process-related interfaces based on ISO/IEC 27001 and ITIL v3 are elaborated, and the application of security metrics to quantitatively assess security frameworks is demonstrated.

The practical application of the proposed innovative methods requires several dedicated management tools, which are devised in detail, implemented as prototypes or as simulations, exemplified, and evaluated. An extensive usage example demonstrates the practical application of multiple security frameworks in parallel based on the specified concepts and tools. Finally, all achieved results are critically assessed and an outlook to further research as well as open issues in related disciplines is given.

Inhaltsverzeichnis

Kapitel 1.

Einleitung

Inhalt dieses Kapitels

Trotz einer anhaltenden Fokussierung auf funktionale Innovationen werden die Sicherheitseigenschaften zunehmend als essentielle Bestandteile von IT-Systemen erkannt, die nicht mehr vernachlässigt werden dürfen. Einen nicht unwesentlichen Beitrag zu dieser Bewusstseinsbildung leistet das gesteigerte Eigeninteresse der IT-Nutzer und -Verantwortlichen: Zum einen werden Privatanwender unter anderem durch die Berichterstattung in den Medien beispielsweise hinsichtlich der Risiken beim Online-Banking sensibilisiert. Zum anderen traten in vielen Wirtschaftsnationen gesetzliche Auflagen in Kraft, durch die nunmehr auch die Unternehmensleitung persönlich haftbar für Schäden gemacht werden kann, die durch IT-Sicherheitsprobleme entstehen. An der Berücksichtigung dieser Compliance-Regelungen führt insbesondere für multinationale und global agierende Organisationen sowie ganze Wirtschaftszweige wie das Gesundheitswesen und die Finanzbranche kein Weg vorbei. Dadurch steigt der Bedarf, neue IT-Komponenten und -Services nicht nur schnell, kosteneffizient und funktional zielorientiert zu entwickeln und einzusetzen, sondern auch ein adäquates IT-Sicherheitsniveau von Grund auf zu berücksichtigen und zu halten, und dieses beispielsweise bei internen Revisionen und Audits nachweisen zu können.

Allerdings sind bereits eine vollständige Definition des Begriffs „IT-Sicherheit“ und eine darauf aufbauende Quantifizierung von Sicherheits- bzw. Schutzniveaus aufgrund der Dynamik und Vielzahl zu berücksichtigender Komponenten, Technologien und Szenarien – und somit der inhärenten Komplexität der Materie – keine triviale Aufgabe. Dies äußert sich einerseits in zum Teil sehr unterschiedlichen Definitionsversuchen in der Literatur und ist andererseits daraus ersichtlich, dass auch Industriestandards wie die ISO/IEC 27000-Reihe und De-facto-Standardwerke wie die IT-Grundschutz-Kataloge des BSI auf zum Teil umfangreiche Aufzählungen angestrebter Ziele anstatt auf eine präzise, formale Charakterisierung und darauf abgestimmte Metriken zurückgreifen (vgl. [ISO27k, BSIGSK]).

Unter Ausklammerung dedizierter IT-Security-Produkte ist die Sicherheit eines IT-Systems weder ein Selbstzweck noch einer von mehreren funktionalen Bereichen; vielmehr handelt es

sich um eine **Querschnittsfunktion** (engl. *cross-cutting concern*), die Konzepte, Implementierungen und deren Betrieb umfassen und vollständig durchdringen muss. Die IT-Sicherheit steht und fällt damit, dass im IT-System und seinem unmittelbaren Umfeld keine Bereiche ungeschützt bleiben und der am schwächsten geschützte Bereich Angriffe ausreichend lange abwehren kann (vgl. [BS00]). Bei der Entwicklung von IT-Systemen und komplexen IT-Service-Infrastrukturen ist in der Praxis jedoch immer noch häufig zu beobachten, dass Sicherheitsmechanismen entweder gänzlich unberücksichtigt bleiben oder erst nachträglich – und dabei häufig unvollständig und somit vergeblich – integriert werden [BDL06]. Dabei entstehen nicht nur durch von Angreifern ausgenutzte Sicherheitslücken potentiell große Schäden, sondern es fällt auch erheblicher administrativer Aufwand, z. B. zum fast schon kontinuierlich notwendigen Einspielen von Software-Security-Patches, an, wodurch wiederum die Kosten für den Betrieb einer *sicheren* IT-Infrastruktur deutlich erhöht werden.

Das Paradigma „**security by design**“ zielt deshalb darauf ab, Sicherheitseigenschaften bereits bei der Konzeption sowohl einzelner IT-Komponenten als auch deren Synthese zu komplexen IT-Architekturen und IT-Service-Infrastrukturen und somit ab initio zu berücksichtigen. Wenngleich ein empirischer Nachweis aufgrund mangelnder Vergleichbarkeit nur selten gelingt, kann im Allgemeinen davon ausgegangen werden, dass sich der in der Konzeptionsphase notwendige Zusatzaufwand im laufenden Betrieb rasch amortisiert und zu einer Reduktion der Gesamtkosten führt.

Aufgrund der bereits angedeuteten Komplexität der IT-Sicherheit als Ganzes ist offensichtlich, dass nicht beispielsweise jeder Softwarearchitekt, Softwareentwickler, Systemadministrator und IT-Service-Verantwortliche ein IT-Sicherheitsexperte sein kann, der sein dazu notwendiges und breit gestreutes Wissen immer auf dem aktuellen Stand hält. Vielmehr müssen die verschiedenen Interessentengruppen gezielt mit der **Vermittlung von Methoden** und **Werkzeugen** unterstützt werden, um ein durchgängiges, hohes IT-Sicherheitsniveau zu ermöglichen.

Eine zentrale Rolle nehmen dabei dedizierte, so genannte **Security-Frameworks** ein: Wie durch die Bezeichnung als Rahmenwerk bereits impliziert wird, steckt ein Security-Framework zunächst ein Gebiet ab, auf das es angewendet werden soll, und gibt intrinsische IT-Sicherheitsthemenbereiche vor, die bei der konkreten, szenarienspezifischen Umsetzung entweder verpflichtend berücksichtigt werden müssen oder optional zur Verbesserung des Sicherheitsniveaus eingesetzt werden können. Für jeden Themenbereich werden **IT-Sicherheitsmaßnahmen** oder -mechanismen vorgestellt und zur Auswahl angeboten, die sich zum Erreichen des jeweiligen Schutzziels prinzipiell eignen. Aufgrund der typischerweise großen Lösungsvielfalt werden der Zielgruppe des Security-Frameworks **Methoden zur Bewertung und Selektion** der einzelnen Maßnahmen an die Hand gegeben, um das Framework für das jeweilige Szenario zu adaptieren. Ein Security-Framework ist somit im Allgemeinen kein fertiges Off-the-shelf-Produkt, das ohne Zusatzaufwand in eine IT-Architektur integriert werden kann, sondern es ist für das jeweilige Szenario maßgeschneidert zu instanziieren.

Wie an mehreren Stellen in dieser Arbeit nachgewiesen wird, mangelt es jedoch auch dem Begriff „Security-Framework“ noch an einer standardisierten und in der Praxis anerkannten Definition. Aus diesem Grund wird bereits an dieser Stelle darauf hingewiesen, dass sich einerseits die nachfolgend betrachteten Eigenschaften fast ausschließlich auf die (Informations-)Sicherheit beziehen, die englisch als *(information) security* bezeichnet wird, wohingegen auf weitere Aspekte der umfassenden Funktionssicherheit (engl. *safety*) nur an ausgewähl-

ten Stellen eingegangen wird, an denen entsprechende thematische Querverbindungen existieren. Andererseits beschränken sich die Betrachtungen auf Software- und damit eng verknüpfte Hardwarekomponenten, wohingegen Eigenschaften der physischen und physikalischen IT-Sicherheit, beispielsweise im Hinblick auf Einbruchs- und Brandschutz oder die Materialbelastbarkeit von Security-Tokens wie Chipkarten, nicht näher behandelt werden. Die Begriffe Framework und Rahmenwerk werden synonym und, sofern im Einzelfall nicht anders angegeben, auf die Sicherheit bezogen verwendet.

Die vorliegende Arbeit behandelt das **integrierte Management von Security-Frameworks**. Dieses schlägt, wie im nächsten Abschnitt motiviert wird, die Brücke zwischen den sehr vielen einzelnen und häufig techniklastigen Security-Frameworks und dem Management umfangreicher, komplexer und häufig heterogener IT-Infrastrukturen. Die betont integrale Betrachtung zielt dabei sowohl auf die **Beherrschbarkeit** der parallel eingesetzten zahlreichen Security-Frameworks als auch auf adäquate **Schnittstellen zu IT-Service- und anderen Managementprozessen** ab (vgl. [HAN99]). Die gewonnenen Ergebnisse sind dadurch gleichermaßen für Autoren von Security-Frameworks, Softwarearchitekten, Leiter von IT-Infrastrukturprojekten, IT-Serviceadministratoren und IT-Sicherheitsverantwortliche relevant.

1.1. Motivation und Zielsetzung

Security-Frameworks wurden bereits für zahlreiche Bereiche spezifiziert und in der Praxis erfolgreich eingesetzt. Sie unterscheiden sich beispielsweise hinsichtlich ihrer Zielgruppe und des Umfangs ihres Anwendungsgebiets, wie der folgende, bewusst nur grobe Überblick über aktuell verfügbare Security-Frameworks zeigt:

- *Security-Frameworks für das Software Engineering* fungieren als Leitfäden und Werkzeugkonzepte für Softwareentwickler. Diverse Frameworks in diesem Bereich decken z. B. das UML-basierte Softwaredesign, die Konzeption grundlegender Sicherheitsmechanismen wie Authentifizierung und Autorisierung über zahlreiche so genannte **Security Patterns** und Programmierparadigmen wie die aspektorientierte Programmierung (AOP) ab. Für Laufzeitumgebungen wie Microsoft .NET und Programmiersprachen wie Java sowie deren komplexe Bestandteile, z. B. das Java Reflection API, existieren dedizierte Security-Frameworks, deren Anwendung zum Teil durch so genannte **Security Platforms** erleichtert wird; diese stellen im Wesentlichen Funktionsbibliotheken mit parametrisierbaren Sicherheitsmechanismen bereit und reduzieren somit den Implementierungsaufwand.
- *Security-Frameworks für Dienste* existieren unter anderem für netzbasierte Dienste wie IP-Konnektivität, WLAN, E-Mail und Voice-over-IP und finden sich verstärkt im Web-Umfeld (Web-Applikationen, Web Services, E-Commerce, etc.). Da für viele Dienste wie verteilte Speicherlösungen, Datenbanken und Learning Management Systeme eigene Security-Frameworks geschaffen wurden, sind einerseits die **Vielfalt der Security-Frameworks**, andererseits aber auch ihre voneinander meist **isolierte Entstehung** in dieser Kategorie am deutlichsten sichtbar.
- *Security-Frameworks für Architekturen* decken mehrere IT-Komponenten und deren Zusammenspiel ab; sie existieren beispielsweise für Betriebssysteme, Embedded Systems,

service-orientierte Architekturen (SOA), unternehmensweite IT-Infrastrukturen und organisationsübergreifende Architekturen wie Grids und Föderationen.

Daneben existieren viele weitere Security-Frameworks, beispielsweise für ausgewählte Teilbereiche der IT-Sicherheit wie die Zugriffssteuerung und für herstellerspezifische Produktportfolios, so dass eine Kategorisierung auf Basis unterschiedlichster Kriterien vorgenommen werden kann, auf die in Kapitel 4 näher eingegangen wird.

Die vorliegende Arbeit wird primär dadurch motiviert, dass jedes Security-Framework für sein Anwendungsgebiet spezifisch ist und somit – beispielsweise im Hinblick auf das breite Servicespektrum vieler IT-Dienstleister – nur ein **punktuelles Lösungskonzept** darstellen kann, das in ein **Gesamtsicherheitskonzept** integriert werden muss. Damit verbunden sind die folgenden Herausforderungen, deren konkrete Ausprägungen in den Kapiteln 3 und 4 aufgezeigt werden:

- Unter anderem durch die unscharfe Verwendung des Begriffs „Security-Framework“ bedingt fehlen einheitliche **Differenzierungs- und Bewertungskriterien**. Die prinzipielle Beurteilung der Eignung eines Frameworks für sein Anwendungsgebiet, beispielsweise unter dem Aspekt der **Vollständigkeit** der behandelten Aspekte und angebotenen Mechanismen, wird dadurch ebenso erschwert wie die Entscheidung zwischen mehreren Frameworks für dasselbe Anwendungsgebiet.
- Im Hinblick auf den **parallelen Einsatz** mehrerer Frameworks, z. B. für verschiedene IT-Services innerhalb einer Organisation, kann bislang weder auf Untersuchungen zur Kombinierbarkeit und Interoperabilität zurückgegriffen werden noch existiert eine Methodik zur gezielten Auswahl bei thematisch partiell überlappenden Frameworks unter der Zielsetzung eines flächendeckenden, aber möglichst redundanzfreien Einsatzes.
- Durch die bislang unzureichende Berücksichtigung der Zusammenhänge zwischen den bereits existierenden Frameworks fehlt die Basis für eine Methodik zur zielorientierten und effizienten **Entwicklung von Security-Frameworks** für neue Anwendungsgebiete bzw. zur Verbesserung existierender Frameworks. Dies äußert sich einerseits darin, dass ein signifikanter Teil der existierenden Frameworks seit ihrer Initialveröffentlichung nicht überarbeitet wurde, und andererseits darin, dass bestehende Frameworks beim Design neuer Frameworks meist nicht angemessen berücksichtigt und folglich Lösungskonzepte unnötig partiell neu erarbeitet werden.
- Die existierenden Frameworks befassen sich nahezu ausschließlich mit nur einer oder sehr wenigen Phasen im **Lebenszyklus** des gesamten IT-Systems, beispielsweise mit der Implementierung im Rahmen der Softwareentwicklung oder der initialen Inbetriebnahme in einer Organisation. Eine vollständige Betrachtung, die beim Design eines Systems beginnt, seine Integration in vorhandene und häufig heterogene Infrastrukturen berücksichtigt und den produktiven Einsatz inklusive Change Management und Außerbetriebnahme bzw. Ablösung nicht vernachlässigt, fehlt bislang in der notwendigen Breite.
- Unter anderem durch die historische Entwicklung bedingt sind viele der existierenden Frameworks sehr techniklastig, so dass Sicherheitsprobleme zwar behoben werden, die Lösungen jedoch nur unzureichend in das gesamtheitliche Security Management eingebunden werden können. Dies betrifft beispielsweise **frameworkübergreifende und**

nachweislich konsistente Policies, aber auch **Kennzahlen**, die beispielsweise in Risikomanagement und Kosten-/Leistungsrechnung verwendet werden können und grundlegend für die Auswertung durch Governance- und Compliance-Management sind.

Unter Berücksichtigung dieser Herausforderungen werden deshalb die folgenden Ziele und Aufgaben verfolgt:

- *Entwicklung einer adaptierbaren Methodik für die szenariengetriebene Analyse, Bewertung und Gegenüberstellung von Security-Frameworks:* Auf Basis ausgewählter repräsentativer Szenarien werden zunächst Anforderungen und Randbedingungen an ein breites Spektrum von Security-Frameworks und ihr Zusammenspiel spezifiziert. Die daraus abgeleiteten Bewertungs- und Differenzierungskriterien werden auf Basis aktueller Literatur und verwandter Arbeiten ergänzt, verfeinert und auf die existierenden Security-Frameworks angewandt. Somit wird der aktuelle Stand der Technik hinsichtlich der typischen **Framework-Kernbestandteile**, der Vollständigkeit von Security-Frameworks und ihrer internen und externen **Abhängigkeiten** dargelegt und gegenüber dem Soll-Zustand positioniert. Aus den Ergebnissen wird eine flexible Herangehensweise zur **Beurteilung von Security-Frameworks in konkreten Szenarien** abgeleitet.
- *Entwicklung eines modularen Leitfadens für die Entwicklung von Security-Frameworks aus der Sicht ihres Managements:* Die bei der Analyse existierender Security-Frameworks gewonnen Erkenntnisse werden so aufbereitet, dass bei der Weiterentwicklung von Security-Frameworks oder der Entwicklung von Security-Frameworks für neue Bereiche zielorientierter vorgegangen werden kann. Aus der Perspektive des Framework-Managements spielen dabei einerseits der Umfang sowie die Vollständigkeit und andererseits die Wiederverwendbarkeit bzw. **Übertragbarkeit existierender Konzepte** und instanzenübergreifend gemeinsame Nutzung der Kernkomponenten zentrale Rollen.
- *Spezifikation des vollständigen Security-Framework-Lebenszyklus:* Durch die sich im Laufe der Zeit ändernden Anforderungen und im Betrieb gewonnene Erfahrungen ergibt sich in der Praxis der Bedarf, Security-Frameworks iterativ weiterzuentwickeln; diesem Bedarf kommt bislang jedoch fast kein Security-Framework nach. Über eine in dieser Breite neue, durchgängige Erläuterung der Phasen, die ein Security-Framework von seinem Design über seine Einführung in einem konkreten Szenario bis hin zur Außerbetriebnahme durchläuft, werden die Grundlagen für eine **durchgängige Integration in Entwicklung, Deployment und Betrieb** geschaffen, die sowohl bei der Gestaltung der Frameworks als auch bei ihrer Anwendung berücksichtigt werden müssen.
- *Spezifikation von Security-Framework-Managementprozessen und ausgewählten Aspekten ihrer Werkzeugunterstützung:* Hierzu werden neben Anpassungen des Security Management selbst zum einen **Schnittstellen zu essentiellen IT-Service-Management-Prozessen** (ITSM) wie dem Configuration und dem Change Management spezifiziert, die zu einer service- und frameworkübergreifend konsistenten Umsetzung von Security-Policies beitragen müssen. Zum anderen wird eine gemeinsame Basis für das integrierte Management der eingesetzten Security-Frameworks geschaffen, indem notwendige **Managementinformationen und -operationen** analysiert werden. Diese Managementebene bildet dabei auch die Schnittstelle zu weiteren Managementprozessen, indem sie unter anderem beispielsweise Key Performance Indikatoren (KPIs) bereitstellt, die in die Beurteilung des Gesamtsicherheitsniveaus einfließen.

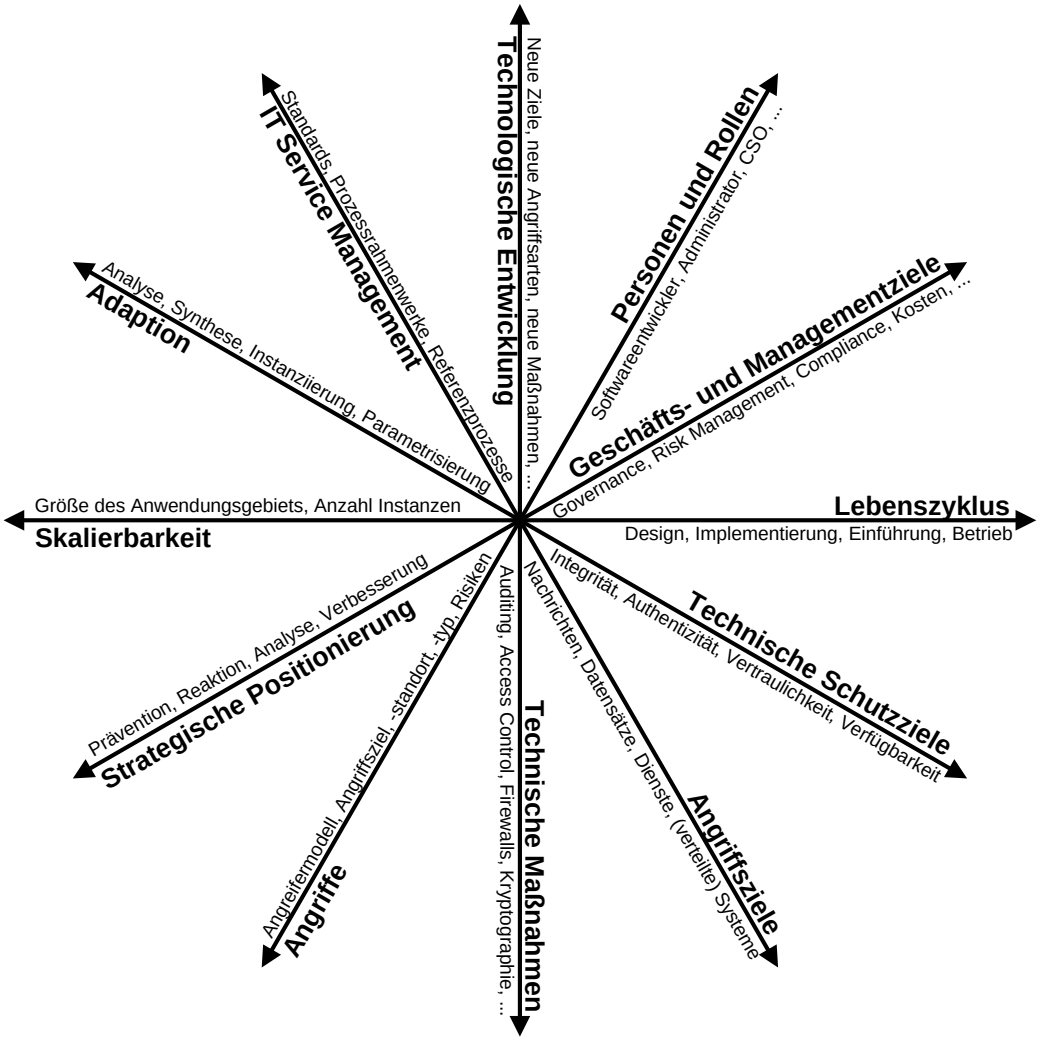


Abbildung 1.1.: Ausgewählte Dimensionen des Managements von Security-Frameworks

Der nächste Abschnitt gibt einen Überblick über die wissenschaftlichen Fragestellungen, die im Rahmen dieser Arbeit untersucht werden, und skizziert die eigenen Beiträge, um die genannten Ziele zu erreichen.

1.2. Fragestellungen und wissenschaftliche Beiträge

Zur Einordnung in das Forschungsumfeld und zur Verdeutlichung der Komplexität des Managements von Security-Frameworks zeigt Abbildung 1.1 einige ausgewählte Dimensionen des Problemraums:

- *Lebenszyklus:* Nach Eckert können Sicherheitsprobleme in IT-Systemen prinzipiell in den drei Phasen Design, Implementierung und Administration entstehen [Ecke09]. Dieses weit verbreitete Phasenmodell wird in dieser Arbeit zu einem feiner granulierten

vollständigen Lebenszyklus erweitert, der auf Security-Frameworks spezialisiert ist und dabei stärker zwischen der Implementierung im Sinne des Software Engineerings bzw. der Produktentwicklung und der Anschaffung sowie initialen Einführung (Deployment) in einem Szenario differenziert. Aus der Phase des laufenden Betriebs heraus wird darüber hinaus die zyklische Verbesserung durch einen optionalen erneuten Übergang in die Designphase unterstützt.

- *Technische Schutzziele:* Die große Zahl existierender Security-Frameworks wird selbstverständlich durch den jeweils anwendungsgebietsspezifischen Schutzbedarf motiviert. Als gemeinsamer Nenner der im Allgemeinen angestrebten Basisschutzziele können jedoch die Integrität, die Authentizität, die Vertraulichkeit und die Verfügbarkeit aufgefasst werden. Im Hinblick auf die Bewertung von Security-Frameworks liefert diese Dimension **Vollständigkeitskriterien** und unterstützt die **Analyse von Schwerpunkten**.
- *Angriffsziele:* Jeglicher Angriff zielt darauf ab, dass mindestens eines der vorgenannten technischen Schutzziele nicht mehr vollständig erreicht werden kann. Prinzipiell kann jeder Bestandteil eines IT-Systems angegriffen werden; eine grobe Kategorisierung umfasst ausgetauschte Nachrichten, gespeicherte Datensätze, Software zum Erbringen von Diensten, einzelne Rechnersysteme und verteilte Systeme als Ganzes. Eine umfassendere Betrachtung von Angriffszielen muss darüber hinaus auch Personen, z. B. unter dem Aspekt des Social Engineerings, und Geschäfts- sowie Managementprozesse berücksichtigen.
- *Technische Maßnahmen:* Zur Erlangung der technischen Schutzziele steht eine Fülle technischer Maßnahmen bzw. Sicherheitsmechanismen zur Verfügung, deren vollständige Diskussion den Rahmen dieser Arbeit sprengen würde. Beispielsweise kann die Vertraulichkeit von Nachrichten z. B. über deren Verschlüsselung erreicht werden, wofür wiederum Dutzende kryptographischer Verfahren mit verschiedensten Parametrisierungen eingesetzt werden können. Eine **Systematik zur Kategorisierung** der für Security-Frameworks essentiellen und häufig eingesetzten Sicherheitsmechanismen wird in Kapitel 2 vorgestellt.
- *Angriffe:* Bei der Analyse von existierenden Security-Frameworks zeigt sich überraschend häufig, dass Sicherheitsmechanismen proklamiert werden, ohne explizit die Angriffe zu diskutieren, vor denen sie schützen sollen. Eine Beurteilung von Vollständigkeit und Verhältnismäßigkeit setzt jedoch voraus, dass **Angreifermodelle** definiert werden, die beispielsweise über das Angriffsziel, den Standort des Angreifers (z. B. intern bzw. extern) und die berücksichtigten Angriffstypen (z. B. aktiv oder passiv) Aufschluss geben. Als Schnittstelle zum **Risikomanagement** müssen beispielsweise die angenommenen Angriffswahrscheinlichkeiten, -häufigkeiten, -dauern und -auswirkungen bekannt gemacht werden.
- *Strategische Positionierung:* Sicherheitsmechanismen können verschiedenen Phasen eines Angriffs zugeordnet werden. Häufig liegt der Schwerpunkt bei präventiven Maßnahmen, die sicherstellen sollen, dass Angriffe scheitern. Da die Annahme eines absolut sicheren Systems in der Praxis nicht aufrecht erhalten werden kann, sind auch reaktive Maßnahmen erforderlich, die beispielsweise eine weitere **Eskalation** eines Sicherheitsvorfalls durch die **Isolation** einer betroffenen Komponente verhindern sollen. Die Erkennung von Angriffen durch Monitoring (Intrusion Detection) kann mit Präven-

tivmaßnahmen kombiniert werden (Intrusion Prevention), wohingegen die Aufklärung erfolgreicher Angriffe häufig Mechanismen der **IT-Forensik** benötigt. Ein umfassendes Security-Framework sollte entsprechende Mechanismen oder Schnittstellen zu externen Werkzeugen vorsehen.

- *Skalierbarkeit:* Die Skalierbarkeit von Security-Frameworks betrifft sowohl die Größe ihres Anwendungsgebiets als auch die Anzahl ihrer Instanzen. So spielen beispielsweise bei einem Security-Framework für organisationsübergreifende Verbünde sowohl die Anzahl der an einem Verbund beteiligten Organisationen als auch die Anzahl an Verbünden, an denen eine ausgewählte Organisation gleichzeitig beteiligt ist, eine Rolle. Aufgrund derzeit typischer physischer und geographischer Ausbreitungen wird eine Kategorisierung in eingebettete Systeme, einzelne Rechensysteme, verteilte Systeme, unternehmensweite Infrastrukturen und organisationsübergreifende Dienste als Ausgangsbasis verwendet.
- *Adaption:* Da Security-Frameworks in der Regel losgelöst von einem einzelnen Anwendungsszenario spezifiziert werden, müssen Methoden zur gezielten Anpassung an konkrete Anwendungsumgebungen festgelegt werden. Diese umfassen unter anderem die systematische Analyse des Szenarios, die Abbildung zwischen Konzepten und Komponenten im Framework und der bereits vorhandenen Infrastruktur unter Lösung eventueller Zielkonflikte, die Synthese der relevanten Bestandteile des Frameworks und ihre Instanziierung unter Berücksichtigung möglicher Besonderheiten, durch die sich Abweichungen vom Gesamtkonzept des Frameworks ergeben können. Das Resultat kann beispielsweise in einem Post-Implementation-Review (PIR) dem ursprünglichen Frameworkkonzept und der Ausgangssituation gegenübergestellt werden.
- *IT Service Management:* Die Erbringung von IT-Diensten und der Betrieb von IT-Infrastrukturen, in denen jeweils Security-Frameworks zum Einsatz kommen können, ist in ITSM-Prozesse eingebettet. Standardisierte und weit verbreitete ITSM-Prozessrahmenwerke wie ITIL v3 sehen **Referenzprozesse für das Security Management** vor, das selbst wiederum Querschnittsaufgaben wahrnimmt und somit Schnittstellen zu den anderen ITSM-Prozessen wie dem Configuration und Change Management enthält. Das Zusammenspiel dieser Prozesse mit zu Security-Frameworks gebündelten Sicherheitsmaßnahmen und die Konsequenzen aus dem parallelen Einsatz mehrerer Security-Frameworks sind größtenteils noch nicht untersucht worden.
- *Technologische Entwicklung:* Die zu schützenden Angriffsziele, die zur Verfügung stehenden Schutzmechanismen und die Angriffe entwickeln sich ebenso weiter wie die angewandten Sicherheits- und Managementkonzepte. Neben der überwiegend evolutionären Weiterentwicklung, die sich beispielsweise durch häufig neu entdeckte Sicherheitslücken in Software und entsprechende Gegenmaßnahmen ausdrückt, müssen auch Technologiesprünge berücksichtigt werden, z. B. im Hinblick auf die Auswirkungen auf die Wirksamkeit herkömmlicher Verschlüsselungsverfahren beim Erreichen der Marktreife von Quantenrechnern. Für Security-Frameworks ist dabei eine Strategie zu wählen, die sich sowohl am aktuellen **Stand der Technik** orientiert als auch die **Anwendbarkeit unter ökonomischen Gesichtspunkten** sicherstellt.
- *Personen und Rollen:* Das Management von Security-Frameworks ist für mehrere Personenkreise mit unterschiedlichen Interessenschwerpunkten relevant. So sind einerseits die Perspektiven der unmittelbar Beteiligten, z. B. des Framework-Designers, Softwareentwicklers, Systemadministrators und Sicherheitsverantwortlichen zu berücksichtigen.

Andererseits müssen auch Externe, z. B. Auditoren oder Angreifer, und deren berechtigte oder auch konfliktäre Ziele berücksichtigt werden.

- *Geschäfts- und Managementziele:* Aus der Perspektive der Unternehmensführung sind die Bereitstellung und der Betrieb von IT-Infrastrukturen Hilfsmittel bei der Umsetzung der Geschäftsprozesse oder – bei IT-Dienstleistern – Bestandteile des Produktportfolios. Da eine Erhöhung der Sicherheitsniveaus in der Regel keine unmittelbare Erhöhung des Ertrags zur Folge hat, werden häufig möglichst kostengünstige Sicherheitslösungen angestrebt. Im Rahmen der als **Governance** bezeichneten top-down Steuerung der Vorgänge im Unternehmen wird erwartet, dass strategische Sicherheitsentscheidungen flächendeckend konsistent umgesetzt werden und zu überprüfbaren Ergebnissen führen. Diese internen Vorgaben werden häufig auch zu großen Teilen von außen, beispielsweise durch Gesetze und Verordnungen, beeinflusst. Für Security-Frameworks ist somit zu untersuchen, wie sie die Umsetzung von Unternehmensrichtlinien unterstützen und zum **Compliance Management** beitragen können.

Unter Berücksichtigung dieser Problemdimensionen werden die folgenden offenen und in dieser Breite bislang noch nicht betrachteten Fragestellungen untersucht:

- Welche für ihren parallelen Einsatz und ihr integriertes Management relevanten *Eigenschaften* und *Schnittstellen* müssen Security-Frameworks im Allgemeinen aufweisen und welche gegenseitigen *Abhängigkeiten* sind dabei zu berücksichtigen?
- Wie kann bei der *Zusammenstellung*, *Strukturierung* und *Priorisierung* von Kriterien, anhand derer die Eignung eines Security-Frameworks für seine Anwendung und Integration in bereits vorhandene Infrastrukturen beurteilt werden soll, methodisch und effizient vorgegangen werden? Mit welchen Eigenschaften kann ein Security-Framework dabei die einzelnen Aktivitäten im Rahmen der *Anforderungsanalyse* und des *Maßschneiderns* in konkreten Szenarien unterstützen?
- Welche *Integrations-* und *Betriebsaspekte* müssen bereits bei Design, Anpassung und Instanziierung von Security-Frameworks generell berücksichtigt werden? Wie sind analog dazu IT-Infrastrukturen allgemein auf den parallelen Einsatz und das Management von Security-Frameworks vorzubereiten?
- Welche *Schnittstellen* sind in den Entwicklungs-, Einführungs- und Betriebsprozessen erforderlich, um die Sicherheits- und Managementeigenschaften von Security-Frameworks kontinuierlich verbessern zu können?
- Wie können welche Kerneigenschaften existierender Security-Frameworks und die bei ihrer Anwendung gemachten Erfahrungen genutzt werden, um das *Design von Security-Frameworks* auch unter Managementaspekten für neue Anwendungsgebiete zu unterstützen?
- Worauf muss bei Einführungsprojekten geachtet werden, um das Paradigma „secure by design“ nicht auf das Security-Framework selbst zu begrenzen, sondern eine *nahtlose Einbettung in bereits vorhandene IT-Infrastrukturen* zu ermöglichen?
- Welche Auswirkungen hat die parallele Anwendung verschiedener Security-Frameworks auf *IT-Service-Management-Prozesse* wie das Security Management, das Service Level Management, das Incident Management, das Configuration Management und das Change Management? Welche Konsequenzen ergeben sich aus der Verzahnung des fortlaufenden Betriebs mit den Lebenszyklusphasen von Security-Frameworks?

- Wie kann im Rahmen des Security Management sichergestellt werden, dass eine *integrierte Sicht* geschaffen wird, d. h. dass z. B. Security-Policies frameworkübergreifend konsistent umgesetzt werden? Wie kann eine frameworkübergreifend einheitliche Schnittstelle zur Steuerung und Kontrolle der dafür relevanten *Sicherheitsparameter* und *Sicherheitsmetadaten* realisiert werden? Welche Anforderungen an das *Informations-* und das *Funktionsmodell* der Managementarchitekturen ergeben sich daraus? Welche zusätzlichen *Schnittstellenkomponenten* und *Werkzeuge* sind dafür erforderlich?
- Welche *Kennzahlen* und *Bewertungskriterien* können im Betrieb frameworkübergreifend eingesetzt werden, um weitere Managementprozesse und deren Werkzeuge z. B. durch *Key Performance Indicators* (KPIs) bei der Beurteilung der Rentabilität einzelner Sicherheitsmaßnahmen und somit bei der initialen wie auch der iterativen szenarien- und risikenspezifischen Anpassung von Security-Frameworks zu unterstützen? Wie kann der Einfluss eines Security-Frameworks auf das *Gesamtsicherheitsniveau* analysiert und quantifiziert werden?

Im nächsten Abschnitt wird die zur Analyse und Lösung dieser Problemstellungen gewählte Herangehensweise erläutert.

1.3. Überblick über das Vorgehensmodell

Wie in Abbildung 1.2 dargestellt ist, werden in *Kapitel 2* zunächst ausgewählte Begriffe und Konzepte eingeführt, um einerseits eine einheitliche terminologische Basis für die nachfolgenden Betrachtungen der teilweise sehr unterschiedlichen Security-Frameworks und andererseits einen Rahmen für das Verständnis des gesamten Themenkomplexes zu schaffen.

Darauf aufbauend werden in *Kapitel 3* mehrere Szenarien vorgestellt, die den Bedarf an der parallelen Anwendung verschiedener Security-Frameworks und deren integriertem Management verdeutlichen; aus ihnen werden systematisch Anforderungen an Security-Frameworks abgeleitet und kategorisiert. Ergänzende Anforderungen und Randbedingungen werden aus der Analyse verwandter Arbeiten gewonnen und zusammen mit den abgeleiteten und abstrahierend dargestellten Anforderungen schließlich zu einem erweiterbaren und parametrisierbaren **Anforderungskatalog** zusammengestellt, der zur Bewertung existierender Security-Frameworks unter Fokussierung ihrer Managementeigenschaften herangezogen werden kann.

In *Kapitel 4* werden aus einem breiten Spektrum ausgewählte existierende Security-Frameworks aus Forschung und Praxis vorgestellt, anhand des Kriterienkatalogs analysiert und einander gegenübergestellt. Auf Basis dieses Überblicks über den aktuellen Stand der Technik können die in Kapitel 2 erarbeiteten Definitionen verfeinert und Aussagen über allgemeine Stärken und Schwächen derzeitiger Security-Frameworks im Hinblick auf ihr integriertes Management getroffen werden. Daraus werden insbesondere Aspekte abgeleitet, die bei der weiteren Entwicklung gezielt gefördert werden müssen.

Kapitel 5 spezifiziert die einzelnen Phasen im **Lebenszyklus** eines Security-Frameworks und die jeweils zu berücksichtigenden Soll-Schnittstellen sowohl zwischen den Phasen als auch zu den anderen Prozessen im Rahmen des Software Engineerings, von Einführungs- und Integrationsprojekten und des operativen Betriebs und Managements. Auf Basis dieses Lebenszyklus und der in Kapitel 4 ermittelten Eigenschaften aktueller Security-Frameworks wird in diesem Kapitel ferner eine Vorgehensweise für die Berücksichtigung von Managementeigenschaften bei

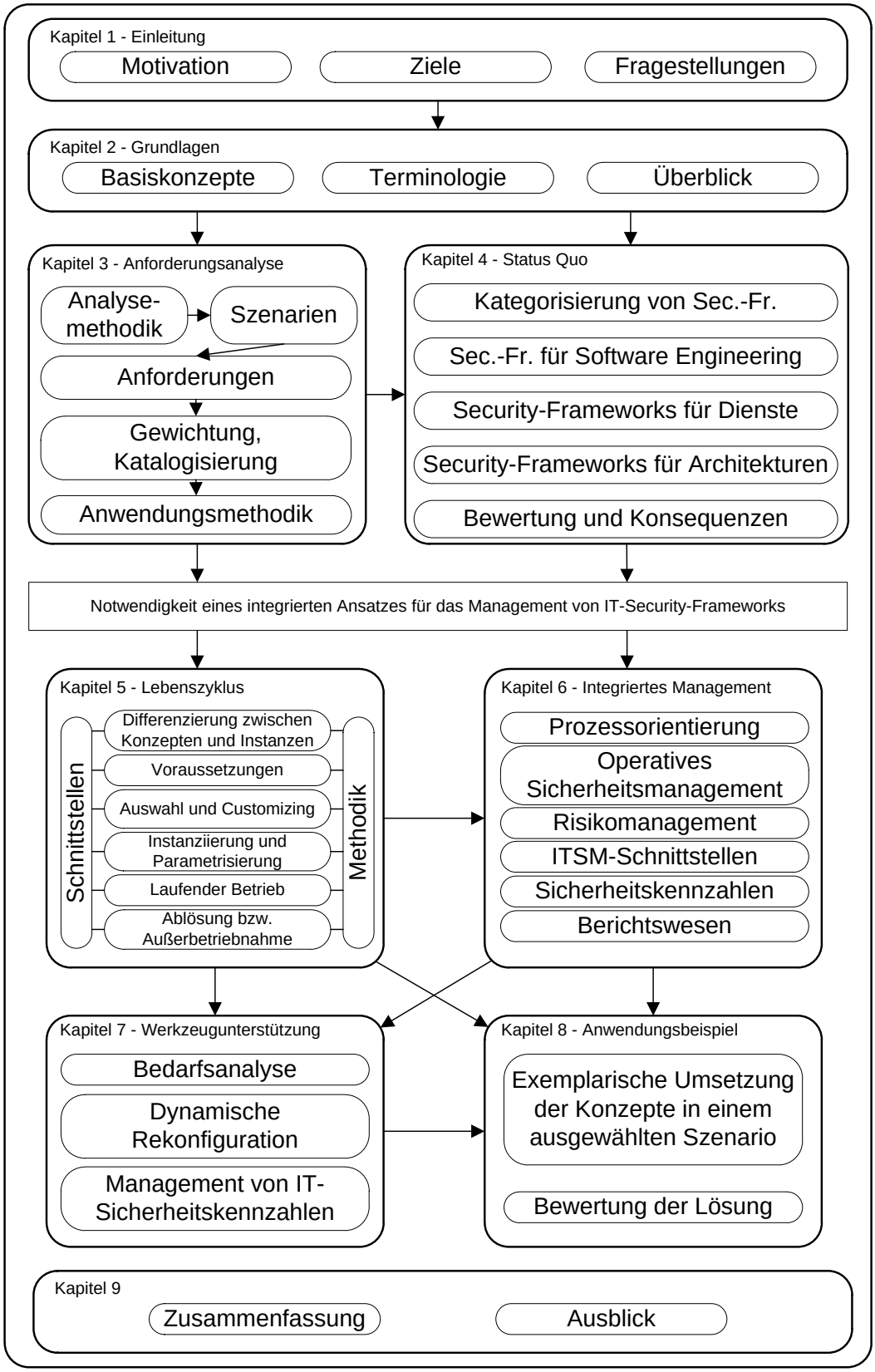


Abbildung 1.2.: Vorgehensmodell der vorliegenden Arbeit

der **Entwicklung neuer Security-Frameworks** spezifiziert, die den Anforderungskatalog berücksichtigen und möglichst weitgehend auf bereits bekannte Lösungskonzepte zurückgreifen.

In *Kapitel 6* wird das **integrierte Management** anhand seiner Prozesse und Schnittstellen sowohl zu den verwalteten Security-Frameworks als auch zu den anderen Managementprozessen analysiert. Hierzu gehören neben dem prozessorientierten Management der Informationssicherheit an sich das operative Sicherheitsmanagement, das Risikomanagement, die ITSM-Prozesse und der Umgang mit informationssicherheitsspezifischen Kennzahlen und deren Verwertung im Rahmen des Berichtswesens, das beispielsweise wichtige Grundlagen für die Beurteilung getätigter und die Planung weiterer Investitionen in Sicherheitsmaßnahmen liefert.

Aus der Untersuchung der vorhandenen Security-Frameworks und der Definition gewünschter Managementeigenschaften ergeben sich Diskrepanzen, die nur durch eine gezielte Erweiterung der Frameworks und einer Verbesserung ihrer gegenseitigen Schnittstellen behoben werden können. Zu diesem Zweck sind **ergänzende Konzepte** und **neue Werkzeuge** erforderlich. In *Kapitel 7* werden nach einer Bedarfsanalyse exemplarisch zwei Managementwerkzeuge konzipiert, die der dynamischen Steuerung der Angriffserkennungssensorik in Security-Frameworks bzw. der Erfassung und Aufbereitung von IT-Sicherheitskennzahlen dienen; neben der Evaluation von Anwendungsbeispielen und der Analyse von Simulationsergebnissen werden Möglichkeiten zur zukünftigen Weiterentwicklung vorgestellt.

In *Kapitel 8* werden die erarbeiteten Konzepte exemplarisch auf eines der in Kapitel 3 vorgestellten Szenarien angewandt und das Ergebnis sowie die noch verbleibenden offenen Punkte kritisch beurteilt. Abschließend werden die Ergebnisse der Arbeit in *Kapitel 9* zusammengefasst und weitere verwandte Forschungsfragestellungen vorgestellt.

Kapitel 2.

Basiskonzepte für Security-Frameworks

Inhalt dieses Kapitels

Dieses Kapitel vermittelt zunächst ausgewählte grundlegende Begriffe und Konzepte der IT-Sicherheit, die im Kontext des Managements von Security-Frameworks relevant sind. Es führt in die in dieser Arbeit verwendete Terminologie ein und schafft damit die Basis für die präzise Formulierung der Sachverhalte in den folgenden Kapiteln. Darauf aufbauend führt es zu einer exakten Definition von Security-Frameworks und zeigt schließlich, wie der hier erarbeitete Security-Framework-Begriff in die durch Information Security Management Systeme realisierten Sicherheitsarchitekturen eingeordnet werden kann.

Security-Frameworks weisen die inhärente Eigenschaft auf, dass diverse Aspekte der IT-Sicherheit in ihnen zu einem komplexen Gesamtkonstrukt zusammenfließen. Unter Berücksichtigung der Auswirkungen auf die Gestaltung und die Beurteilung von Security-Frameworks werden in Abschnitt 2.1 deshalb die grundlegenden **Ziele der IT-Sicherheit**

kurz rekapituliert; darauf aufbauend wird umrissen, wie ihnen die **Ziele des IT-Sicherheitsmanagements** zugeordnet werden können.

In Abschnitt 2.2 werden anschließend ausgewählte **Begriffe, Methoden und Prozesse** wie Bedrohungsanalysen und Risikomanagement skizziert. Die vorgestellten Definitionen orientieren sich an internationalen Standards und anerkannter wissenschaftlicher Literatur, betten die behandelten Aspekte jedoch zusätzlich in den Kontext von Security-Frameworks ein.

Viele der behandelten Themen können der noch relativ jungen, aber methodisch bereits gereiften Disziplin **Security Engineering** zugeordnet werden. Da diese beispielsweise auch für die in Kapitel 5 diskutierte Verzahnung der Entwicklungs- und Managementlebenszyklen relevant ist, wird sie in Abschnitt 2.3 für einen knappen Überblick über weitere relevante technische Aspekte der IT-Sicherheit herangezogen.

Zur Konkretisierung und Veranschaulichung werden anschließend in Abschnitt 2.4 ausgewählte **Angriffe** und technische **Sicherheitsmaßnahmen** vorgestellt, die in den in Kapitel 4 diskutierten aktuellen Security-Frameworks besonders häufig berücksichtigt bzw. eingesetzt werden. Dieser Überblick wird in Kapitel 4 deshalb auch im Rahmen der Spezifikation der Charakteristika von Security-Frameworks mit dem Ziel einer Kategorisierung herangezogen.

Auf Basis der somit in diesem Kapitel aufbereiteten Terminologie wird in Abschnitt 2.5 eine **Definition des Begriffs „Security-Framework“** erarbeitet und diskutiert. Sie ist zum einen, wie in Kapitel 1 bereits umrissen wurde, für die Präzisierung des Wirkungsbereichs der vorliegenden Arbeit zwingend erforderlich, da der Begriff bislang weder in Literatur noch Praxis einheitlich verwendet wird. Zum anderen dient sie als grundlegendes Selektions- und Bewertungskriterium für die in Kapitel 4 exemplarisch vorgestellten Security-Frameworks.

Die somit festgelegten Charakteristika von Security-Frameworks ermöglichen im Anschluss ihre Einordnung in Sicherheitsarchitekturen. Abschnitt 2.6 diskutiert deren grundlegende Eigenschaften und verdeutlicht die Schnittstellen zu anderen Managementsystemen und -prozessen, die in Kapitel 6 vertiefend behandelt werden.

Eine knappe Zusammenfassung der Ergebnisse in Abschnitt 2.7 schließt das Kapitel ab, dessen Struktur zusammenfassend in Abbildung 2.1 dargestellt ist.

2.1. Ziele der IT-Sicherheit und ihres Managements

Ein offensichtlich notwendiger Schritt bei der Beurteilung der Eignung eines Security-Frameworks ist die Analyse, ob die mit seinem Einsatz verbundenen Ziele erreicht werden können. Obwohl diese im Allgemeinen szenarien- und frameworkspezifisch sind, existiert eine Reihe grundlegender Ziele, die fest mit dem Begriff IT-Sicherheit verbunden sind und deshalb in einem Security-Framework nicht ohne guten Grund vernachlässigt werden dürfen.

Die systematische Strukturierung dieser Ziele ist aufgrund der historischen Entwicklung der verwendeten Begriffe mit zwei Herausforderungen verbunden. Einerseits werden die beiden Begriffe *Informationssicherheit* und *IT-Sicherheit* häufig vereinfachend oder unbewusst synonym verwendet; die resultierende Ungenauigkeit wird oftmals durch die Vermischung von deutschem und englischem Fachvokabular noch verstärkt. Andererseits können den Basiszielen der IT-Sicherheit ihrerseits Teilziele untergeordnet werden, die in manchen Veröffentlichungen jedoch selbst als Basisziele aufgeführt bzw. in den Vordergrund gerückt werden.

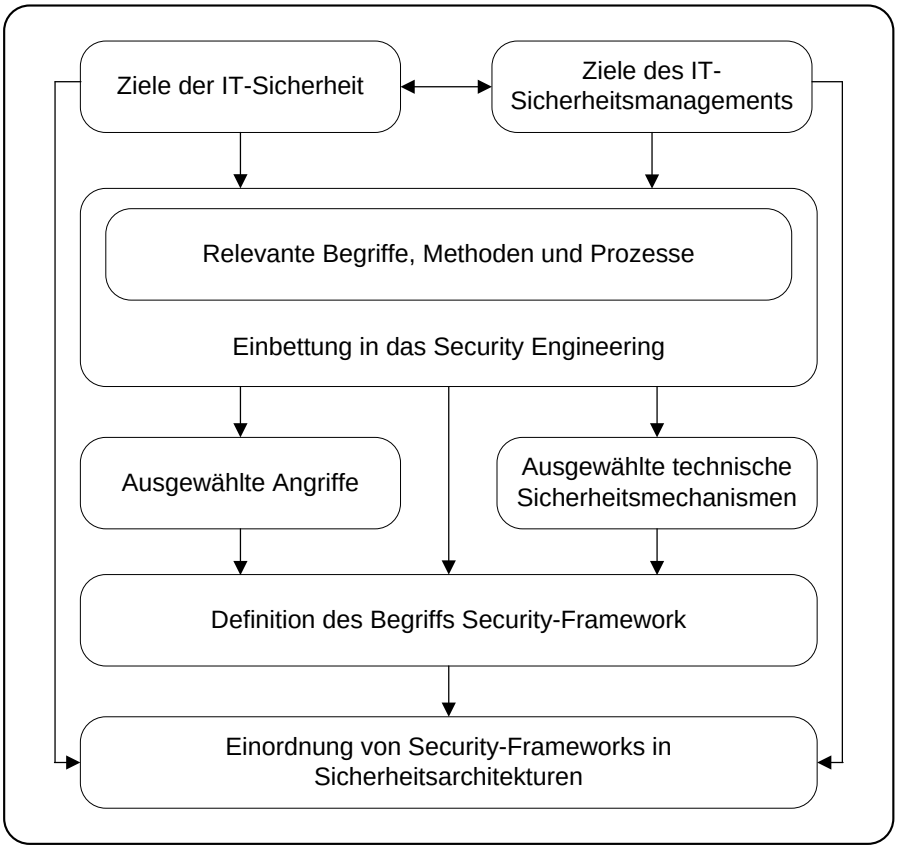


Abbildung 2.1.: Vorgehensmodell in diesem Kapitel

Die in der vorliegenden Arbeit verwendete Terminologie orientiert sich deshalb an den kontinuierlichen Bemühungen von Pohl zur Taxonomie und Modellbildung in der Informationssicherheit im deutschsprachigen Raum [Poh04].

Wie in Abbildung 2.2 dargestellt ist, muss zunächst zwischen den englischen Begriffen *Safety* und *Security* unterschieden werden, die nach Eckert mit *Funktionssicherheit* und *Informationssicherheit* übersetzt werden (vgl. [Ecke09, S. 4f.]). In Anlehnung an RFC 2828 [RC2828] und Eckert charakterisiert Pohl vereinfachend

- **Safety** als „Schutz der Rechnerumgebung vor inkorrektem Verhalten des Rechners (Output)“, und
- **Security** als „Schutz des Rechners vor inkorrektem Verhalten der Rechnerumgebung (Input)“ (vgl. [Poh04b, S. 2]).

Offensichtlich ergeben sich dabei Wechselwirkungen zwischen beiden Bereichen, die auch erhalten bleiben, wenn der von Pohl verwendete Begriff des *Rechners* zu einem offenen **IT-System** nach Eckert verallgemeinert wird, d. h. einem „offene[n], dynamische[n] technische[n] System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen„ ([Ecke09, S. 2]). Eckert merkt hierzu an, dass die Grenzen zwischen Security- und Safety-Fragestellungen fließend sind und Überlappungen existieren (vgl. [Ecke09, S. 6]).

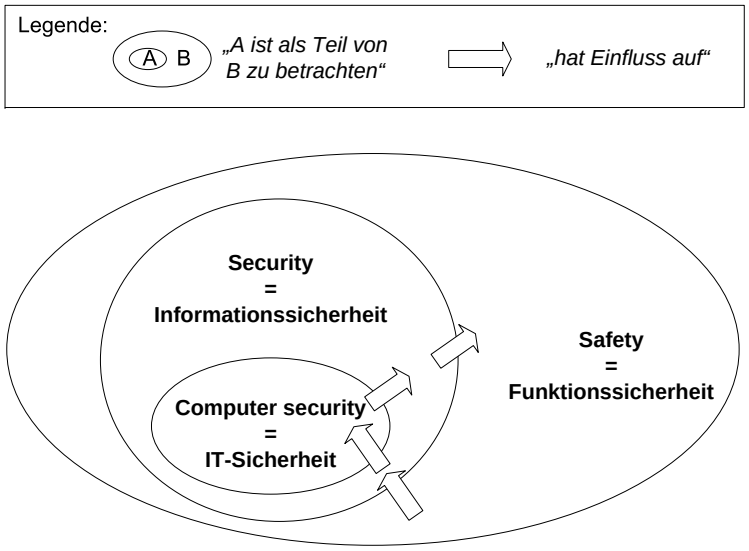


Abbildung 2.2.: Beziehung zwischen Safety, Security und Computer Security nach [Poh04]

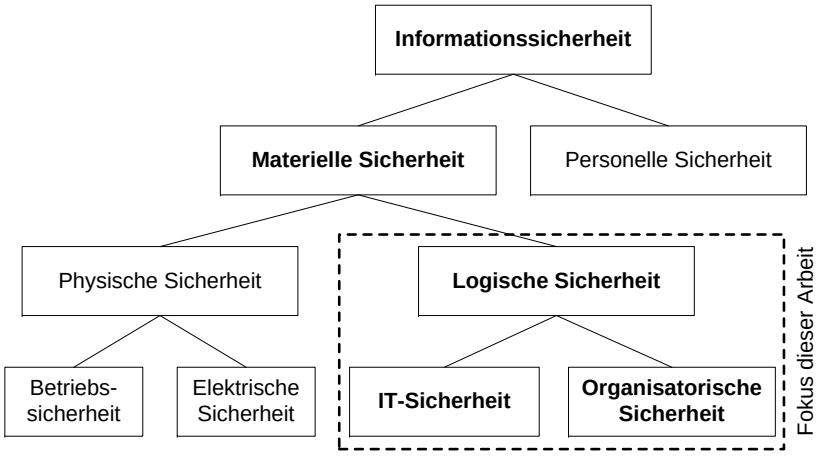


Abbildung 2.3.: Inhalte der Informationssicherheit nach [Poh04]

Abbildung 2.3 zeigt verfeinernd einen Überblick über die Inhalte der Informationssicherheit nach Pohl (vgl. [Poh04b, S. 3]). Die *IT-Sicherheit* ist demnach Bestandteil der *logischen Sicherheit*, die wiederum dem Aspekt der *materiellen Sicherheit* zuzuordnen ist. Dem deutschen Begriff *IT-Sicherheit* entspricht dabei Pohl zufolge am besten der englische Begriff *computer security* (vgl. [Poh04, S. 679]).

Die vorliegende Arbeit behandelt den in Abbildung 2.3 hervorgehobenen Bereich der logischen Sicherheit. Die IT-Sicherheit als derjenige der beiden Bestandteile der logischen Sicherheit, dem Security-Frameworks in der Regel schwerpunktmäßig zugeordnet werden können, ist stark technisch geprägt; ihre Ziele werden im nachfolgenden Abschnitt vorgestellt. Dazu

komplementär ist die *organisatorische Sicherheit*, deren Ziele aus der Perspektive des IT-Sicherheitsmanagements in Abschnitt 2.1.2 diskutiert werden. Berücksichtigt man, dass die Informationssicherheit sehr häufig unter technischen Gesichtspunkten diskutiert wird, so ist verständlich, dass IT-Sicherheit oft als pars pro toto für Informationssicherheit verwendet wird. Dennoch muss bewusst sein, dass der Begriff Security-Framework prinzipiell nicht nur auf die IT-Sicherheit, sondern die Informationssicherheit als Ganzes bezogen zu verwenden ist.

2.1.1. Ziele der IT-Sicherheit

Die Notwendigkeit zur Diskussion der Schutzziele der IT-Sicherheit ergibt sich daraus, dass die IT-Sicherheit selbst sehr häufig über ebendiese Ziele definiert wird. Beispielsweise definiert ISO/IEC 27001:2005 den Begriff *information security* wie folgt: „Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved“ [I27001, S. 2]. Diese Definition weist wie viele andere die charakteristische Eigenschaft auf, dass eine kleine Menge an Kernzielen postuliert wird, die durch eine Aufzählung optionaler weiterer Ziele ergänzt wird. Allerdings unterscheiden sich sowohl die Kernziele als auch die weiteren Ziele in verschiedenen Teilen und je nach Autor; die folgenden Ausführungen orientieren sich an den Definitionen in der ISO 27000-Normenreihe [ISO27k], den BSI Grundschutzkatalogen [BSIGSK] sowie den Erläuterungen von Anderson [Ande08], Eckert [Ecke09] und Whitman/Mattord [WhMa09].

2.1.1.1. Grundlegende Ziele der IT-Sicherheit

Die in der oben zitierten ISO-Definition genannten Sicherheitseigenschaften *confidentiality*, *integrity* und *availability* gehören zweifellos zu den grundlegenden Schutzzielen. Sie werden in der englischsprachigen Literatur häufig in Form des Akronyms *CIA* referenziert und können wie folgt charakterisiert werden:

Definition 1 (Vertraulichkeit)

Vertraulichkeit (engl. confidentiality) ist gewährleistet, wenn geschützte Daten nur von Berechtigten abgerufen werden können.

Auf organisatorischer Ebene erfordert dies die klare Festlegung entsprechend autorisierter Personen, Systeme und Prozesse, die in diesem Kontext als **Subjekte** bezeichnet werden. Auf technischer Seite müssen einerseits Kontrollen der Autorisierung durchgeführt werden; andererseits ist geeignet sicherzustellen, dass autorisierte Subjekte die Daten nicht an unautorisierte Subjekte weitergeben. Ein *Bruch der Vertraulichkeit* liegt somit vor, wenn geschützte Daten von unautorisierten Subjekten eingesehen werden können (vgl. Abbildung 2.4 links).

Definition 2 (Integrität)

Integrität (engl. integrity) ist gewährleistet, wenn geschützte Daten nicht unautorisiert und unbemerkt modifiziert werden können.

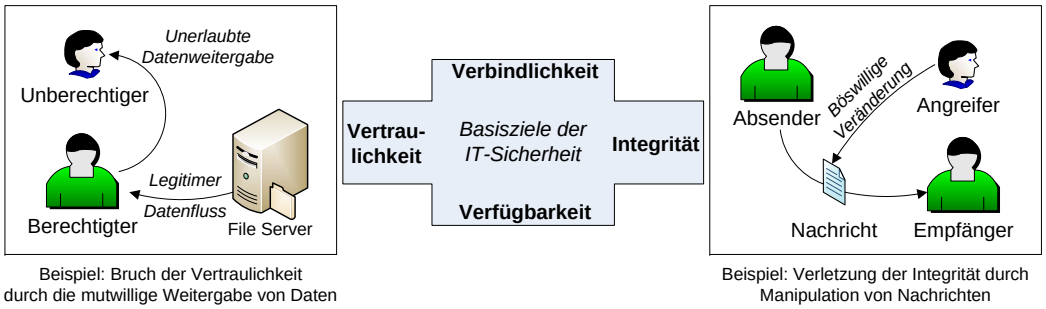


Abbildung 2.4.: Basisziele der IT-Sicherheit und exemplarische Verletzungen

Diese Definition über Ausschluss unerwünschter Datenmanipulationen in Anlehnung an Eckert betont, dass einerseits Subjekte und ihre Berechtigungen zum Anlegen, Verändern und Löschen von Daten definiert und entsprechende technische Kontrollmaßnahmen vorgesehen werden müssen. Andererseits wird gefordert, dass Modifikationen, sofern sie nicht autorisiert wurden, erkannt werden können (vgl. [Ecke09, S. 7f.]). Dadurch kann zumindest eine Weiterverarbeitung verfälschter Daten, die z. B. auch durch defekte Datenträger verursacht sein kann, verhindert werden. Im Deutschen wird der Begriff Validität im Umfeld der IT-Sicherheit synonym zu Integrität verwendet [Poh04b, S. 4]. Die Integrität der Daten muss nicht nur bei ihrer persistenten Speicherung, sondern auch im Transit geschützt werden (vgl. Abbildung 2.4 rechts).

Definition 3 (Verfügbarkeit)

Verfügbarkeit (engl. availability) ist gewährleistet, wenn autorisierte Subjekte störungsfrei ihre Berechtigungen wahrnehmen können.

Diese Definition umfasst nicht nur Daten, sondern allgemein **Objekte**, zu denen beispielsweise auch Dienste und IT-Infrastrukturen gehören können. Die Verfügbarkeit ist ein Dienstgütemerkmal, dessen Sicherheitsrelevanz sich aus den Schäden ergibt, die durch den temporär oder permanent eingeschränkten Zugriff auf benötigte Objekte entstehen.

Die genannten Ziele thematisieren vorrangig den Erhalt statischer Sicherheitseigenschaften von Objekten. Um den Aspekt der dynamischen Veränderung von Daten durch autorisierte oder unerwünschte Verarbeitungsprozesse zu berücksichtigen, wird auch die Verbindlichkeit als grundlegendes Ziel angesehen:

Definition 4 (Verbindlichkeit)

Verbindlichkeit (engl. non-repudiation) ist gewährleistet, wenn ein Subjekt weder die Informationsgewinnung noch die Manipulation von Objekten im Nachhinein unwiderlegbar abstreiten kann.

Diese vier Basisziele fungieren darüber hinaus als Kategorien, denen die im nächsten Abschnitt beschriebenen weiteren Sachziele der IT-Sicherheit untergeordnet werden können. Dabei wird

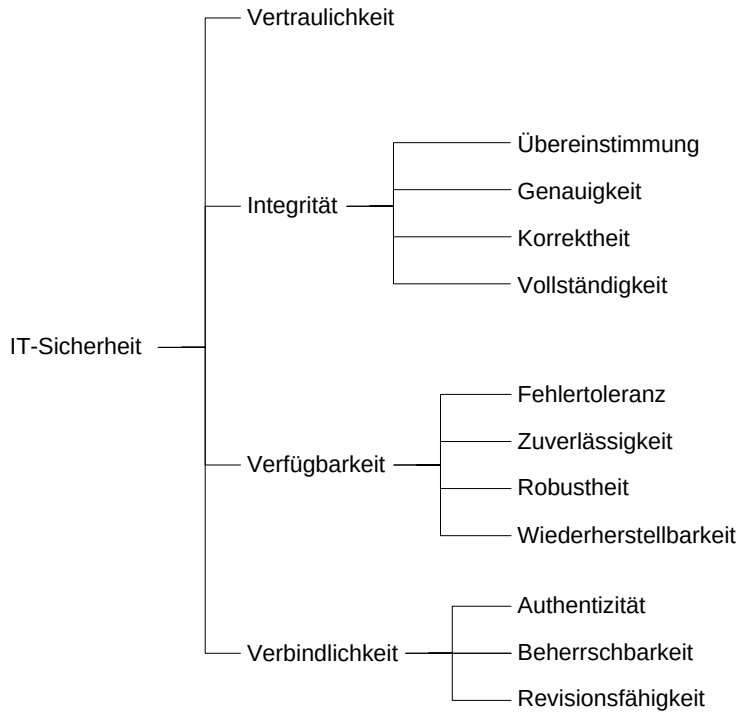


Abbildung 2.5.: Sachziele der IT-Sicherheit und ihre Komponenten nach Pohl [Poh04b, S. 6]

jedoch keine vollständige, disjunkte Zerlegung in Teilziele angestrebt, sondern lediglich eine knappe Vorstellung der über die Basisziele hinausgehenden, in der Literatur am häufigsten adressierten Ziele. Ihre systematische Einordnung unterstützt die Beurteilung der von Security-Frameworks abgedeckten Bereiche.

2.1.1.2. Weitere Ziele der IT-Sicherheit

Alle Definitionen der Basisziele der IT-Sicherheit beinhalten einen Bezug auf Subjekte, denen beispielsweise Berechtigungen zugeordnet werden können. Eine Prüfung dieser Autorisierung setzt eine verlässliche Identifizierung und Authentifizierung des Subjekts voraus. Analog dazu muss auch die Echtheit von Objekten überprüft werden können:

Definition 5 (Authentizität)

Authentizität (engl. authenticity) ist die Echtheit eines Subjekts bzw. Objekts, die anhand eindeutiger Identifikationsmerkmale überprüft werden kann.

Die zuverlässige Sicherstellung der Authentizität ist somit insbesondere eine zwingende Voraussetzung für die Gewährleistung der Verbindlichkeit; dieser ist auch der Schutz gegen mangelnde Überprüfbarkeit als Teilziel zuzuordnen:

Definition 6 (Revisionsfähigkeit)

Revisionsfähigkeit (engl. auditability) ermöglicht das lückenlose Nachvollziehen aller relevanten Verarbeitungsvorgänge während und nach ihrer Durchführung.

Zielkonflikte verdeutlichen, dass die Auswahl und Priorisierung der Ziele szenarienspezifisch erfolgen muss. Beispielsweise kann die Revisionsfähigkeit im Widerspruch zum Datenschutz stehen, wenn in einem Unternehmen verhindert werden soll, dass Mitarbeiter durch eine detaillierte Protokollierung ihrer Arbeitsschritte potentiell überwacht werden können.

Während der Datenschutz lange als primär organisatorische Aufgabe angesehen wurde, rücken technische Maßnahmen zu seiner Umsetzung zunehmend in das Kernaufgabengebiet der IT-Sicherheit:

Definition 7 (Datenschutz)

Datenschutz im engeren Sinn (engl. privacy) ermöglicht die volle Kontrolle einer natürlichen Person über die Weitergabe und Verarbeitung ihrer personenbezogenen Daten.

Der Datenschutz kann somit dem Ziel der Vertraulichkeit zugeordnet werden. Eine Schlüsselrolle nehmen dabei Auswahl und Umfang der Daten ein, die als personenbezogen gelten. Folgende datenschutzrelevante Teilziele haben sich in der aktuellen Forschung – meist mit Bezug auf Telekommunikations- und Internet-Anwendungen – herauskristallisiert (vgl. [Poh04b, S. 6]):

- Anonymität (engl. *anonymity*) als Schutz gegen die Identifizierung von Subjekten.
- Pseudonymität (engl. *pseudonymity*) als Schutz gegen die namentliche Identifizierung einer natürlichen Person.
- Unbeobachtbarkeit (engl. *untraceability*) als Schutz vor Protokollierung.

Offensichtlich schließen sich beispielsweise Anonymität und Verbindlichkeit ebenso gegenseitig aus wie Revisionsfähigkeit und Unbeobachtbarkeit.

Diesen Überblick abschließend ist zu erwähnen, dass die Erkenntnis, trotz verstärkter Bemühungen in der Praxis keine absolut sicheren Systeme implementieren zu können, dazu geführt hat, die Teilziele der Verfügbarkeit nicht nur unter Dienstgüte-, sondern verstärkt auch unter Sicherheitsaspekten zu betrachten. Insbesondere soll in verteilten Systemen die **Ausbreitung** eines Sicherheitsproblems von einer betroffenen Komponente auf die anderen vermieden bzw. eingedämmt werden (engl. non-propagation).

2.1.2. Ziele des IT-Sicherheitsmanagements

Das IT-Sicherheitsmanagement umfasst die gesamtheitliche Planung, Steuerung und Kontrolle der IT-Sicherheit in einem festzulegenden Bereich. Dieser Wirkungsbereich entspricht in der Praxis meist einer größeren Organisationseinheit oder einem ganzen Unternehmen; Teile des IT-Sicherheitsmanagements werden jedoch immer stärker auch für organisationsübergreifende Verbünde relevant.

Analog zur IT-Sicherheit wird auch das IT-Sicherheitsmanagement häufig über seine Ziele definiert. Die nachfolgenden Ausführungen orientieren sich an Standards und international anerkannten Best Practice Dokumentationen, insbesondere an der ISO 27000-Reihe [ISO27k], dem NIST Information Security Handbook [N80010], dem Standard of Good Practice for Information Security des Information Security Forums [ISFSGP], den BSI Grundschutzkatalogen [BSIGSK] sowie ITIL Version 3 [ITILv3] und CobiT 4.1 [CobiT4].

Grundlegend für das Verständnis der Ziele des IT-Sicherheitsmanagements ist seine Auffassung als Querschnittsprozess im Rahmen des gesamten IT-Managements; die häufig anzutreffende Bezeichnung der Konfiguration der Sicherheitseigenschaften von Systemen durch Administratoren als Sicherheitsmanagement würde zu kurz greifen. Als Prozess unterliegt IT-Sicherheitsmanagement dem von Deming geprägten PDCA-Lebenszyklus mit den Phasen Plan (Planung), Do (Implementierung), Check (Kontrolle) und Act (Anpassung), der auf eine kontinuierliche Verbesserung abzielt (vgl. [Demi86]).

In den folgenden beiden Abschnitten werden die Ziele des IT-Sicherheitsmanagements skizziert und eine Methode zur Zuordnung zu den Zielen der IT-Sicherheit kurz vorgestellt.

2.1.2.1. Zielkategorisierung am Beispiel ISO/IEC 27001:2005

Für die Spezifikation der Ziele und Aufgaben des IT-Sicherheitsmanagements ist, wiederum vergleichbar mit der Festlegung der Basisziele der IT-Sicherheit, charakteristisch, dass je nach Autor bzw. Standardisierungsgremium leicht unterschiedliche Kategorien zur Zerlegung des Problemraums definiert werden. Der Standard ISO/IEC 17799:2005, der auch das Security Management nach ITIL maßgeblich beeinflusst hat, wird seit Juli 2007 als ISO/IEC 27002:2005 geführt und dient als Leitfaden für das Informationssicherheitsmanagement. Dieser Leitfaden vertieft die in ISO/IEC 27001:2005 genannten normativen Anforderungen an Informationssicherheitsmanagementsysteme. Diese basieren auf der Idee, den PDCA-Zyklus auch auf das IT-Sicherheitsmanagement anzuwenden, und verfolgen einen *risikogetriebenen* Ansatz. Ferner werden zur Gruppierung von organisatorischen und technischen IT-Sicherheitsmaßnahmen elf Kategorien definiert. Somit lassen sich wie in Abbildung 2.6 dargestellt angelehnt an ISO/IEC 27001:2005 die folgenden zwölf Aufgabenbereiche identifizieren:

1. **Risk management**: Das Risikomanagement dient der Identifikation und Bewertung von Risiken sowie der Auswahl geeigneter Maßnahmen zum Umgang mit ihnen; hierauf wird in Abschnitt 2.2.3.1 näher eingegangen.
2. **Security policy**: Die Definition einer (Informations-)Sicherheitsleitlinie verfolgt das Ziel, die angestrebten Sicherheitseigenschaften systemübergreifend, d. h. für alle Objekte und Subjekte im Wirkungsbereich des IT-Sicherheitsmanagements, in einem top-down Verfahren verbindlich vorzugeben. Die Sicherheitsrichtlinie enthält darüber hinaus typischerweise Angaben zu Verantwortlichkeiten, Schulungen sowie Sensibilisierungsmaßnahmen, Maßnahmen zur Überprüfung ihrer Einhaltung und Sanktionen beim Verstoß.
3. **Organization of information security**: Die interne und externe Weitergabe und Verarbeitung sicherheitsrelevanter Daten muss genau geregelt werden. Die Organisation der Informationssicherheit verfolgt deshalb einerseits das Ziel, den internen Umgang mit diesen Daten zu koordinieren; hierzu gehören das klare Engagement der Führungsebene

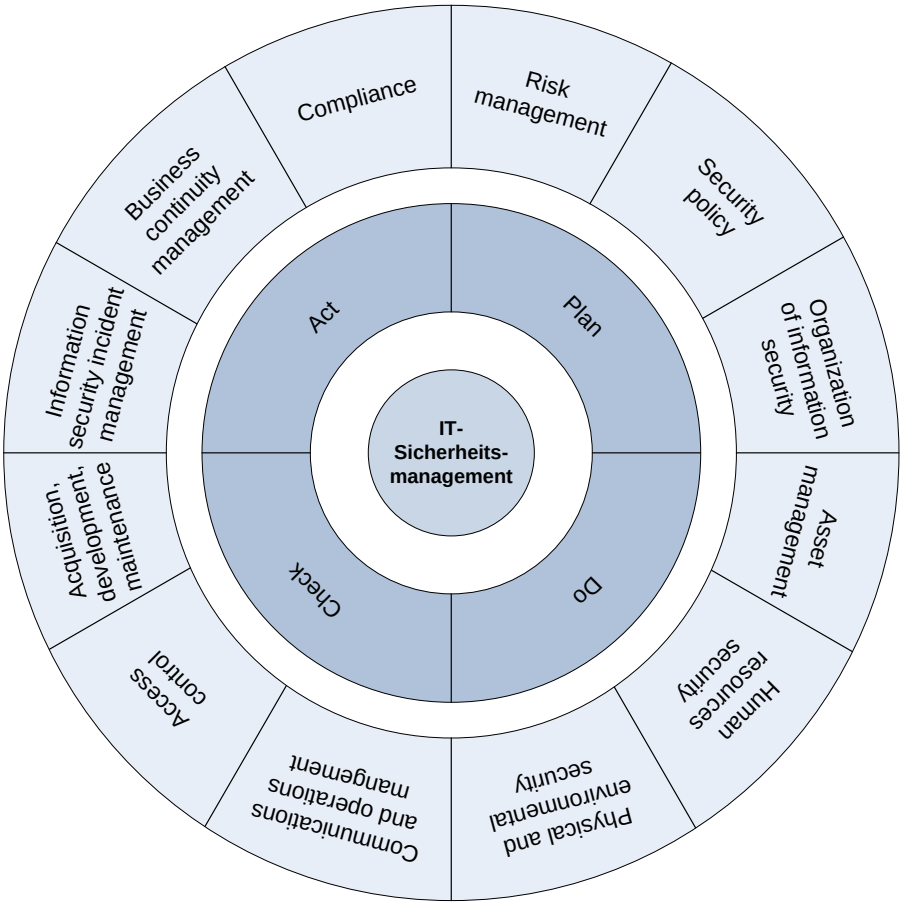


Abbildung 2.6.: IT-Sicherheitsmanagement als Prozess mit seinen Aufgabenbereichen in Anlehnung an ISO/IEC 27001:2005

und die Regelung von Zuständigkeiten genauso wie Vertraulichkeitsvereinbarungen und die Festlegung von Genehmigungsverfahren. Andererseits wird der Umgang mit Dritten festgelegt, beispielsweise Kunden, externen Mitarbeitern und Behörden.

4. **Asset management**: Das Management organisationseigener Werte verfolgt nach ISO 27002 unter anderem das Ziel, deren zulässigen Gebrauch festzulegen; als essentielles Teilziel gehört hierzu die Klassifikation von Informationen, die als Parameter in die unten genannten Autorisierungsprozesse einfließt. Auf den Begriff *Asset* wird in Abschnitt 2.2.2 näher eingegangen.

5. **Human resources security**: Der Bereich Personalsicherheit umfasst die Spezifikation von organisatorischen Maßnahmen, die bereits vor der Anstellung potentieller Mitarbeiter ergriffen werden, von Sicherheitsregelungen während der gesamten Anstellung und von Verfahren bei einer Änderung oder der Beendigung der Anstellung. Im Zusammenspiel mit der definierten Sicherheitsrichtlinie sind hier insbesondere auch die Schulung und Sensibilisierung von Mitarbeitern angesiedelt.

6. **Physical and environmental security**: Der Bereich der physischen und umgebungs-

bezogenen Sicherheit verfolgt primär zwei Ziele: Einerseits sollen Sicherheitsbereiche definiert werden, für die unter anderem entsprechende Zutrittskontrollen einzurichten sind. Andererseits sind Maßnahmen zur Sicherheit von Betriebsmitteln, z. B. von Datenträgern, zu spezifizieren, die beispielsweise auch deren sichere Entsorgung umfassen.

7. **Communications and operations management**: Das Gebiet des Kommunikations- und Betriebsmanagements stellt eine breite Schnittstelle sowohl zu ausgewählten Prozessen des IT Service Management als auch zu technischen Maßnahmen dar. Es verfolgt ein breites Spektrum an Zielsetzungen:

   - Alle Betriebsprozesse sind zu dokumentieren, wobei die Verfahren und Verantwortlichkeiten genau zu spezifizieren sind. Für jegliche Änderungen muss ein Change Management vorgesehen sein; dieses kann durch die Trennung von Entwicklungs-, Test- und Produktivumgebungen unterstützt werden.
   - Die Dienstleistungserbringung durch Dritte muss überwacht und überprüft werden.
   - Die Systemplanung muss durch Kapazitätsmanagement unterstützt werden; neue Systeme müssen einen präzise definierten Abnahmeprozess durchlaufen, bevor sie produktiv eingesetzt werden.
   - Die Verfügbarkeit der Daten ist durch Maßnahmen zur Datensicherung (Backup) sicherzustellen.
   - Die Netzsicherheit muss durch Maßnahmen für Netzkomponenten und Netzdienste gewährleistet werden.
   - Speicher- und Aufzeichnungsmedien, insbesondere auch mobile Wechselmedien, müssen unter Sicherheitsaspekten verwaltet werden.
   - Für den Austausch von Informationen, beispielsweise über den Transport physischer Medien oder in Form elektronischer Nachrichten, müssen Leitlinien erstellt werden.
   - Unternehmenskritische Anwendungen, insbesondere E-Commerce-Anwendungen und Online-Transaktionen, müssen geeignet geschützt werden.
   - Die Systemnutzung ist zu überwachen; dabei angelegte Auditprotokolle sind geeignet zu schützen. Die Qualität der protokollierten Daten ist beispielsweise durch eine systemübergreifende Zeitsynchronisation zu erhöhen.

8. **Access control**: Analog zur Zutrittskontrolle auf physischer Ebene zielt die Zugangskontrolle auf die Überprüfung der Autorisierung bei der angestrebten Nutzung von IT-Diensten ab. Sie umfasst Reglementierungen zur Benutzererfassung und -verwaltung, Richtlinien für Authentifizierungsvorgänge wie Passwort-Policies sowie Konzepte zur Zugriffskontrolle auf Rechner bzw. Betriebssysteme, Anwendungen und Netze. Dabei ist insbesondere auch auf Anforderungen durch mobile Geräte und z. B. Telearbeitsplätze Rücksicht zu nehmen.

9. **Information systems acquisition, development, and maintenance**: Der Bereich der Beschaffung, Entwicklung und Wartung von informationsverarbeitenden Systemen beinhaltet unter anderem die Spezifikation von Sicherheitsanforderungen an neue Systeme, von Maßnahmen zur Entwicklung sicherer Software, z. B. die Überprüfung der von Benutzern eingegebenen Daten, und kryptographische Maßnahmen.

10. **Information security incident management**: Der Umgang mit sicherheitsrelevanten Vorfällen muss genau geregelt werden, um beispielsweise unnötige Verzögerungen bei der Bearbeitung oder die Zerstörung von Beweisen zu verhindern. Somit muss einerseits eine Schnittstelle zum Incident Management Prozess des IT Service Management geschaffen werden, über die sicherheitsrelevante Ereignisse gemeldet werden können; andererseits sind Richtlinien für die Vorbereitung und ggf. die eigene Durchführung IT-forensischer Maßnahmen erforderlich.
11. **Business continuity management**: Diese Kategorie verfolgt das Ziel, Sicherheitsaspekte nachhaltig in die Sicherstellung des Geschäftsbetriebs zu integrieren. Zu ihren Teilzielen gehören die Bereitstellung der zur Planung benötigten Informationen und die Mitwirkung an Konzeption, Testen, Instandhaltung und Neubewertung entsprechender Pläne.
12. **Compliance**: Unter Compliance wird allgemein die Einhaltung von Vorgaben verstanden. Im Bereich des IT-Sicherheitsmanagements sind sowohl externe als auch interne Vorgaben zu berücksichtigen. Eine Zielsetzung ist somit die Identifikation und Berücksichtigung relevanter externer Vorgaben, beispielsweise bezüglich des Datenschutzes und der Rechte an geistigem Eigentum. Ein weiteres Teilziel ist die Prüfung der Einhaltung technischer Vorgaben, beispielsweise auch der definierten Sicherheitsleitlinie. Schließlich sind Maßnahmen für die Audits von Informationssystemen zu definieren und durchzuführen, wobei auch die eingesetzten Revisionswerkzeuge geschützt werden müssen.

Die Aufgabenbereiche sind im Standard in rund 40 so genannte Maßnahmenziele untergliedert, die wiederum durch mehr als 130 Sicherheitsmaßnahmen unterstützt werden. Security-Frameworks können sowohl Lösungen für diese Bereiche beitragen als auch weitere Systeme in die IT-Infrastruktur einbringen, die entsprechend dieser Zielvorgaben verwaltet werden müssen.

2.1.2.2. Zuordnung zu den Zielen der IT-Sicherheit

Ein direkter Zusammenhang zwischen den Zielen des IT-Sicherheitsmanagements und den Basiszielen der IT-Sicherheit ist offensichtlich nur an wenigen Stellen explizit gegeben, beispielsweise bei der Konzeption von Datensicherungen zur Gewährleistung der Verfügbarkeit von Daten.

Die Zuordnung von Zielen des IT-Sicherheitsmanagements zu den im von ihm abgedeckten Bereich relevanten IT-Sicherheitszielen muss deshalb näher analysiert werden. Dabei zeigt sich, dass beispielsweise die Aufgabe, eine Sicherheitsleitlinie zu konzipieren, noch keinen unmittelbaren Einfluss auf die Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit haben kann.

Zur Veranschaulichung der Zusammenhänge erweitert CobiT deshalb die im englischen Sprachraum gebräuchliche Menge der Basisziele der IT-Sicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – um die Ziele Effektivität (engl. *effectiveness*), Effizienz (engl. *efficiency*), Compliance und Zuverlässigkeit (engl. *reliability*); in ihrer Gesamtheit werden diese Ziele von CobiT als *business requirements* bezeichnet (vgl. [CobiT4, S. 25ff.]).

Auf dieser Basis wird konsequent für jeden der von CobiT definierten Prozesse angegeben, ob sich dieser primär oder sekundär auf die einzelnen Ziele auswirkt. So wirkt sich beispielswei-

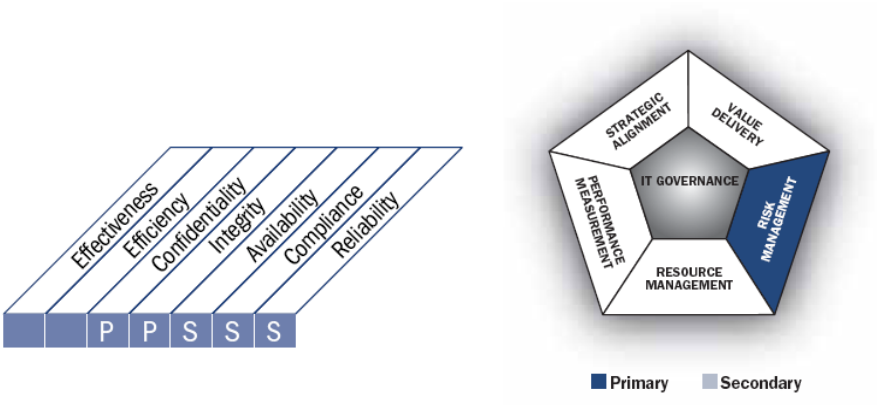


Abbildung 2.7.: Beispiel für die Zielzuordnung nach CobiT 4.1 (Quelle: [CobiT4, S. 117])

se die regelmäßige Sicherheitsüberprüfung der Infrastruktur, die als Maßnahme zum Prozess *DS5: Ensure Systems Security* gehört, wie in Abbildung 2.7 dargestellt primär auf die Vertraulichkeit sowie die Integrität der Daten und sekundär auf die Verfügbarkeit, Compliance und Zuverlässigkeit aus [CobiT4, S. 117].

Diese Zuordnungsmethodik kann als Funktion aufgefasst werden, die Prozesse und Maßnahmen des IT-Sicherheitsmanagements auf Teilmengen der definierten *business requirements* abbildet. Im Hinblick auf Security-Frameworks und ihr Management liegt nahe, dass ähnliche, aber umfassendere Ansätze benötigt werden, um zu beurteilen, ob die in einem Szenario relevanten Ziele der IT-Sicherheit bzw. des IT-Sicherheitsmanagements erfüllt werden. Die Festlegung, wie die Ziele konkret aufeinander abgebildet werden, basiert auf einer zwangsläufig subjektiven Einschätzung der im jeweiligen Bereich eingesetzten Maßnahmen sowie Methoden und ihrer Zusammenhänge, die in der Dokumentation des Security-Frameworks festzuhalten ist. Einen gemeinsamen Nenner hierfür können die Erläuterungen im folgenden Abschnitt bilden.

2.2. Relevante Begriffe, Methoden und ihre Zusammenhänge

In diesem Abschnitt werden ausgewählte weitere Begriffe knapp erläutert und Methoden aus dem Umfeld der IT-Sicherheit und ihres Managements vorgestellt, um einerseits die in dieser Arbeit verwendete Terminologie explizit darzulegen und andererseits bereits auf besonders relevante Bereiche hinzuweisen.

Die für die Vorstellung der Begriffe und Methoden gewählte Reihenfolge ermöglicht, dass die Definitionen aufeinander aufbauen können, reflektiert jedoch keine Prioritäten. Alle vorgestellten Ansätze sind lediglich Beispiele; eine vollständige Analyse aller Lösungen für die geschilderten Aufgabenbereiche ist nicht Gegenstand dieser Arbeit.

2.2.1. Rollen im Umfeld von Security-Frameworks

Betrachtet man den Lebenszyklus eines Security-Frameworks von seiner Konzeption über die szenarienspezifische Anpassung und Implementierung bis hin zum dauerhaften Betrieb und Management, so wird schnell offensichtlich, dass verschiedenste Personen damit in Kontakt kommen. Jede dieser Personen hat abhängig von ihrer eigenen Aufgabenstellung unterschiedliche Interessen am und Anforderungen an das Security-Framework.

Die Kategorien, in die sich die involvierten Personen anhand dieser Kriterien einteilen lassen, werden als Rollen bezeichnet. Eine natürliche Person kann dabei mehr als eine Rolle einnehmen, sofern die entsprechenden Rollen nicht explizit als sich gegenseitig ausschließend gekennzeichnet sind. Dieses Verständnis von Rollen ist somit stark organisatorisch geprägt und deckt sich mit der Identifikation und Formalisierung von *business roles*, wie sie im Enterprise Role Engineering durchgeführt wird. Eine Zuordnung von technischen Berechtigungen zu diesen Rollen, die für die rollenbasierte Zugangskontrolle (engl. *role-based access control*, RBAC) benötigt werden würde, wird an dieser Stelle bewusst nicht durchgeführt.

Im Zusammenhang mit Security-Frameworks werden primär die folgenden Rollen in den geschilderten Ausprägungen betrachtet (alphabetische Reihenfolge):

- **Administrator**: Ein Administrator führt den operativen Betrieb von Teilen eines Systems durch. Typischerweise findet eine starke Spezialisierung statt, so dass beispielsweise beim Betrieb eines Webservers die Administration des Betriebssystems, des Dienstes, der Serverhardware und der Netzinfrastruktur von verschiedenen Personen übernommen wird. Zu den vielfältigen Aufgaben eines Administrators gehört auch die praktische Umsetzung der Sicherheitsrichtlinien in seinem Bereich.
- **Angreifer**: Der Angreifer versucht, das Erreichen der für Ressourcen definierten Schutzziele temporär oder dauerhaft zu verhindern. Die Kenntnis bzw. Charakterisierung möglicher Angreifer ist eine zwingende Voraussetzung für die Planung adäquater Sicherheitsmechanismen. Hierauf wird in Abschnitt 2.4 näher eingegangen.
- **Anwender**: Als Anwender bzw. Benutzer werden alle Personen bezeichnet, die ein legitimes Interesse an der Verwendung geschützter Ressourcen haben. Sie stellen unter anderem eine der Zielgruppen für Sicherheitsschulungen dar und entscheiden letztendlich darüber, ob die eingesetzten Sicherheitsmaßnahmen im Hinblick auf die möglichst einfache Nutzung der Ressourcen handhabbar sind.
- **Architekt**: Der Architekt ist für die Planung eines Gesamtkonstrukts aus Einzelkomponenten unter funktionalen, technischen, gestalterischen und wirtschaftlichen Aspekten verantwortlich. Im Kontext von Security-Frameworks wird zwischen einem **Softwarearchitekt**, der die modulare Zusammenstellung komplexer Softwareprodukte fachlich leitet, und einem **Systemarchitekt** unterschieden; dieser ist für die Synthese komplexer IT-Systeme, die aus mehreren Software- und Hardwarekomponenten bestehen können, verantwortlich.
- **Auditor**: Ein Auditor führt ein Untersuchungsverfahren durch, das die Erfüllung von Anforderungen bzw. Richtlinien auf Basis des aktuellen Ist-Zustands bewerten soll und somit allgemein dem Qualitätsmanagement zuzuordnen ist. Entsprechend muss auch der prinzipielle Soll-Zustand definiert und dokumentiert sein. Unabhängig davon, ob es sich um einen unternehmensinternen oder externen Auditor handelt, ist sicherzustellen, dass

er keine andere Rolle wahrnimmt, die in einem Interessenkonflikt zu einem möglichst objektiven Untersuchungsergebnis mündet.

- **CEO** (chief executive officer, Geschäftsführer bzw. Vorstandsvorsitzender): Die persönliche Haftbarkeit auf Basis der Compliance-Regelungen motiviert ein ebenso persönliches Interesse der Führungsebene an der Vermeidung sicherheitsrelevanter Vorfälle; zur Führungsebene gehören alle hier vorgestellten Rollen, deren Name ein mit dem Buchstaben C beginnendes Akronym ist (engl. *C-level management*). Der CEO spielt darüber hinaus beim Treffen unternehmensweit relevanter Entscheidungen eine zentrale Rolle, so dass er insbesondere für das Security Reporting als wichtige Zielgruppe fungiert.
- **CFO** (chief financial officer, Finanzvorstand): Der CFO bzw. der von ihm geleitete Finanzbereich ist einerseits für die Budgetierung u. a. des Sicherheitsbereichs zuständig; andererseits ist dort typischerweise das Risikomanagement – auch für die Belange der IT – angesiedelt.
- **CIO** (chief information officer, Leiter für Informationstechnologie): Der CIO übernimmt die Gesamtverantwortung für die Planung der IT-Infrastruktur, die Technologieauswahl und den Betrieb der IT-Dienste.
- **CSO** bzw. **CISO** (chief (information) security officer, Sicherheitsverantwortlicher): Der CSO ist direkt verantwortlich für die Planung, Durchführung und Einhaltung aller sicherheitsrelevanten Themen. In größeren Unternehmen, insbesondere wenn diese nicht in der IT-Branche angesiedelt sind, werden die Rollen CSO und CISO häufig von verschiedenen Personen wahrgenommen, um zwischen der physischen Sicherheit und der IT-Sicherheit zu differenzieren; der CISO ist in diesem Fall meist dem CIO unterstellt.
- **Designer**: Während der Architekt die Zusammenstellung mehrerer Komponenten zu einem größeren Ganzen übernimmt, hat der Designer die Aufgabe, eine dieser Komponenten im Detail zu planen. Dabei ist im Kontext von Security Frameworks zwischen Hardware-, Software- und Systemdesignern zu unterscheiden.
- **Entwickler** (engl. *developer*): Der Entwickler übernimmt die Implementierung von Komponenten oder Systemen, die von Designern bzw. Architekten vorgegeben wurden. Dabei kann es sich sowohl um die Programmierung, z. B. unter Orientierung an einem Security-Framework für Softwareentwickler, handeln als auch um die szenarienspezifische Instanziierung entsprechend angepasster Security-Frameworks für IT-Dienste oder IT-Architekturen.
- **Projektleiter** (von Einführungsprojekten): Im Kontext dieser Arbeit werden insbesondere solche Projekte betrachtet, die sich mit der Auswahl und Einführung von Security-Frameworks in bestehenden IT-Infrastrukturen befassen. Der Projektleiter ist für die Planung und Durchführung aller damit verbundenen Tätigkeiten fachlich verantwortlich.
- **Prozesseigner** (engl. *business process owner*): Der Prozesseigner ist der Verantwortliche für einen dokumentierten Geschäftsprozess; er hat Entscheidungskompetenzen und übernimmt die Verteilung der Ressourcen.
- **Technologieexperte**: Der Technologieexperte befasst sich mit der aktuell und potentiell zukünftig eingesetzten Technologie und steht den anderen Rollen in seiner Funktion als Wissensträger beratend zur Verfügung. Das von ihm abgedeckte fachliche Spektrum

ist somit breiter als bei den anderen Rollen; an ihn wenden sich die Hintergrundinformationen, die einige Security-Frameworks liefern und die nicht unmittelbar in die operative Praxis umgesetzt werden können.

- **Security Engineer** (IT-Sicherheitsingenieur): Als Security Engineer werden Personen bezeichnet, die die in Abschnitt 2.3 vorgestellten Methoden des Security Engineering beherrschen und praktisch anwenden. Sie übernehmen somit insbesondere die operativen Tätigkeiten in den Bereichen, für die hier entsprechende leitende Rollen definiert sind. Beispielsweise kann ein Security Engineer die Aufgabe übernehmen, ein System auf bekannte Sicherheitslücken zu überprüfen (engl. *penetration tester*).

Auf weitere Rollen, die von einigen Security-Frameworks spezifiziert werden bzw. die von einigen der in dieser Arbeit verwendeten Verfahren vorausgesetzt werden, wird an der jeweiligen Stelle eingegangen.

2.2.2. Verwundbarkeiten, Angriffe und Maßnahmen

In diesem Abschnitt werden weitere Begriffe eingeführt, deren Unterschiede und Zusammenhänge für die präzise Beschreibung der nachfolgend vorgestellten Verfahren relevant sind.

In der Praxis existieren so viele verschiedene Objekte, dass diese aufgrund der damit verbundenen Kosten nicht alle gleich gut geschützt werden können. Folglich muss eine Selektion vorgenommen werden, welche Objekte geschützt werden sollen, auf deren Basis anschließend weitere Planungsschritte, z. B. eine Priorisierung, durchgeführt werden können. In erster Näherung kommen alle Objekte in Frage, die mit einem quantifizierbaren Gegenwert verbunden sind; ISO 27001 definiert den Begriff *Asset* als „anything that has value to the organization“ [I27001, S. 2]. Darauf aufbauend wird er in dieser Arbeit wie folgt verwendet:

Definition 8 (Asset)

Assets sind materielle oder immaterielle Güter, bei denen das Verfehlen mindestens eines der Basisziele der IT-Sicherheit zu Schaden führen kann.

Beispielsweise handelt es sich beim Backup einer Kundendatenbank auf DVD um ein Asset, dessen Wert offensichtlich über die Materialkosten für den Datenträger deutlich hinausgeht; allerdings ist die exakte Quantifizierung des monetären Gegenwerts häufig sehr schwierig und eine der Herausforderungen für das *Asset Management*.

Für die weiteren Ausführungen in diesem Abschnitt wird ohne Beschränkung der Allgemeinheit angenommen, dass die betrachteten IT-Systeme die Basisziele der IT-Sicherheit nicht absichtlich oder fahrlässig verfehlen, wie dies beispielsweise bei Trojanischen Pferden oder Honeypots der Fall ist (siehe Abschnitt 2.4). Durch unbemerkte Fehler an einer beliebigen Stelle im Lebenszyklus des IT-Systems, der grob in die Phasen Design, Implementierung und Betrieb unterteilt werden kann, können sich jedoch Schwachstellen und Verwundbarkeiten einschleichen (vgl. [Ecke09]):

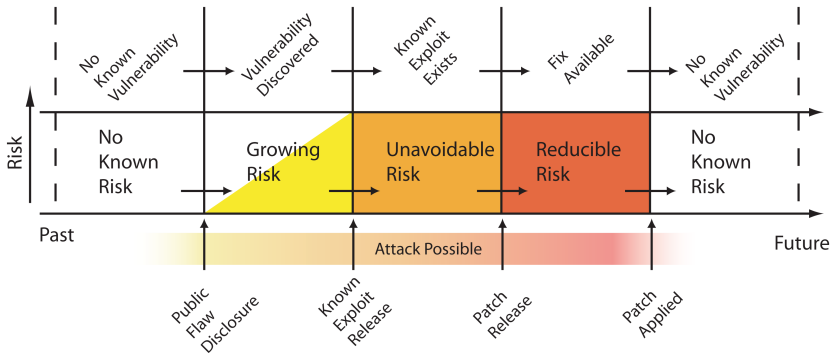


Abbildung 2.8.: Vulnerability Lifecycle bei öffentlicher Diskussion von Verwundbarkeiten nach Hewlett-Packard (Quelle: [HPVULC, S. 14])

Definition 9 (Schwachstellen und Verwundbarkeiten)

Eine Schwachstelle (engl. weakness*) ist ein punktueller Fehler eines Systems, der noch nicht beseitigt wurde. Eine Verwundbarkeit (engl.* vulnerability*) ist eine Schwachstelle, die zur Verletzung mindestens eines der angestrebten Basisziele der IT-Sicherheit führen kann.*

Für Verwundbarkeiten kann ein Lebenszyklus definiert werden, der je nach Detailgrad auch differenziert, ob und welchen Personengruppen eine Verwundbarkeit bereits bekannt ist; Abbildung 2.8 zeigt eine vereinfachte Variante, die von einer öffentlichen Diskussion der Verwundbarkeit ausgeht, und den Zusammenhang mit dem jeweiligen Risiko. Damit verbundene Verfahren sind unter anderem im Rahmen des Risikomanagements relevant (siehe Abschnitt 2.2.3). Jede Schwachstelle kann genau einem System zugeordnet werden, wobei mehrere Systeme dieselbe oder miteinander verwandte Schwachstellen aufweisen können. Da die im Kontext der IT-Sicherheit betrachteten Schwachstellen als potentielle Verwundbarkeiten aufgefasst werden können bzw. jeder Verwundbarkeit eine Schwachstelle zugrunde liegt, werden beide Begriffe häufig synonym verwendet.

Das Vorhandensein mindestens einer Verwundbarkeit ist ein latenter Zustand, der mit einer **Bedrohung** (engl. *threat*) verbunden ist: Die Ausnutzung einer Verwundbarkeit würde zum Verfehlen der Basisziele der IT-Sicherheit führen. Eine **Bedrohungsanalyse** (threat assessment) hat somit die Aufgabe, die bekannten und potentiellen Schwachstellen zu identifizieren und die Ausnutzung von Verwundbarkeiten einzuschätzen. Ein *Angriff* kann als konkrete Instanz einer Bedrohung betrachtet werden:

Definition 10 (Angriff)

Ein Angriff (engl. attack) ist im engeren Sinn die versuchte Ausnutzung einer bekannten oder vermuteten Verwundbarkeit. Im weiteren Sinn werden auch alle Maßnahmen zur gezielten Vorbereitung dieses Versuchs zum Angriff gezählt.

Angriffe lassen sich nach verschiedensten Gesichtspunkten kategorisieren, wobei besonders

häufig zwischen aktiven und passiven Angriffen unterschieden wird; in Abschnitt 2.4 wird darauf näher eingegangen.

Im Idealfall würde der Erfolg von Angriffen dadurch verhindert werden, dass a priori alle Schwachstellen beseitigt werden. Da sich dies in der Praxis als de facto unmöglich herausgestellt hat, müssen Maßnahmen ergriffen werden, die den Umgang mit Angriffen regeln. Auf technischer Ebene werden Sicherheitsmechanismen zur Verhinderung, Erkennung und weiteren Behandlung von Angriffen eingesetzt:

Definition 11 (Sicherheitsmechanismus)

Ein Sicherheitsmechanismus ist eine technische Sicherheitsmaßnahme, die der Prävention oder Detektion von Angriffen dient oder zur Reaktion auf Angriffe eingesetzt wird.

Sicherheitsmechanismen sind üblicherweise feste Bestandteile von IT-Systemen. Sie können jedoch auch als externe Komponenten beispielsweise dazu eingesetzt werden, die Ausnutzung bekannter, aber noch nicht behobener Verwundbarkeiten zu unterbinden, indem entsprechende unerwünschte Zugriffe auf das geschützte System blockiert werden. Dabei ist jedoch zu beachten, dass auch Sicherheitsmechanismen selbst wiederum Schwachstellen aufweisen können.

Im Rahmen eines potentiellen Angriffs liefern die Sicherheitsmechanismen Daten, die wie folgt klassifiziert werden können:

Definition 12 (Sicherheitsereignisse, -alarme und -vorfälle)

*Ein **Sicherheitsereignis** (engl. security event) ist eine von einem Sicherheitsmechanismus bereitgestellte Information über eine Zustandsänderung des Systems, die potentiell sicherheitsrelevant ist.*
*Ein **Sicherheitsalarm** (engl. security alert) wird ausgelöst, wenn das Ergebnis der Korrelation und Auswertung von Sicherheitsereignissen auf Basis einer Sicherheitsrichtlinie den Anlass dazu gibt, automatische Gegenmaßnahmen zu ergreifen oder einen Administrator auf die aktuelle Sicherheitslage hinzuweisen.*
*Ein **Sicherheitsvorfall** (engl. security incident) wird durch eine nicht leere Menge von Sicherheitsereignissen ausgelöst, deren Signifikanz automatisch oder manuell bestätigt wurde; er darf nicht ignoriert werden, sondern muss im Rahmen eines definierten Security Incident Management Prozesses bearbeitet werden.*

Die Zusammenhänge zwischen den in diesem Abschnitt vorgestellten Begriffen sind zusammenfassend in Abbildung 2.9 dargestellt.

2.2.3. Wichtige Managementprozesse im Umfeld des IT-Sicherheitsmanagements

Die beispielsweise in ITIL verwendete Bezeichnung des IT-Sicherheitsmanagements als Querschnittsprozess verdeutlicht die Vielzahl an Schnittstellen zu diversen anderen Managementprozessen, von denen in diesem Abschnitt einige ausgewählte skizziert werden. Zunächst wird

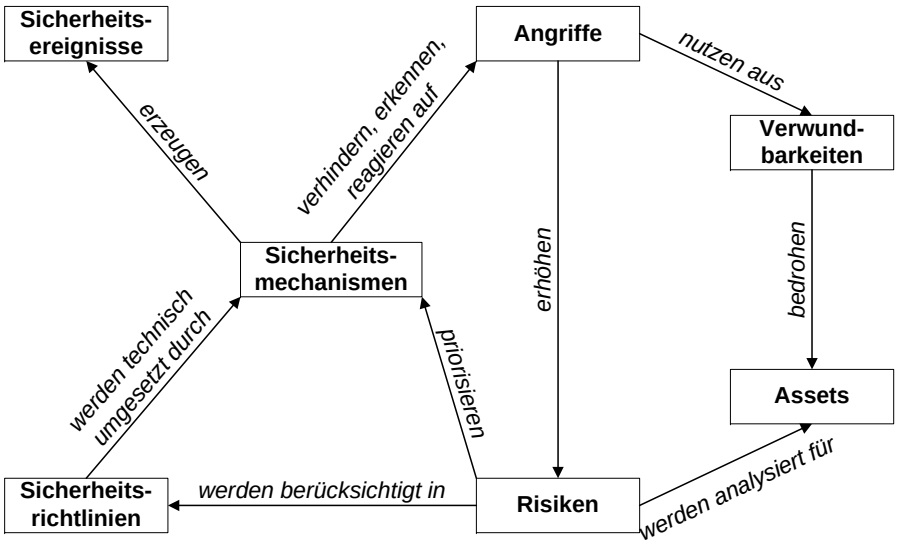


Abbildung 2.9.: Zusammenhänge zwischen den in Abschnitt 2.2.2 vorgestellten Begriffen

auf das Risikomanagement eingegangen, das klassisch dem Finanzwesen zuzuordnen ist. Daran anschließend werden Methoden zur Bewertung der Sicherheit von IT-Systemen vorgestellt. Schließlich wird umrissen, welchen Einfluss das IT-Sicherheitsmanagement auf die IT Service Management Prozesse nach ITIL v3 hat.

2.2.3.1. Risikomanagement

Unter einem Risiko R ist grundlegend die Wahrscheinlichkeit P des Eintretens eines negativen Ereignisses e multipliziert mit seinem finanziellen Ausmaß, dem Schaden S, zu verstehen: $R_e = P_e \cdot S_e$. Ein negatives Ereignis kann beispielsweise ein erfolgreicher Angriff sein; führt dieser zu einem temporären Ausfall eines Dienstes, so ist der Schaden, der sich aus der Nichtverfügbarkeit ergibt, als Bestandteil des finanziellen Ausmaßes zu berücksichtigen.

Die gewünschte Risikoquantifizierung scheitert praktisch häufig an der objektiven und präzisen Beurteilung sowohl der Eintrittswahrscheinlichkeit als auch des Schadens: Am Beispiel des Ereignisses „Kundendatenbank wird ausgespäht“ wird klar, dass Auswirkungen, die sich z. B. durch den Verlust von Ansehen auf Bestands- und Neukunden ergeben, im Allgemeinen nicht a priori berechnet, sondern nur geschätzt werden können. Analog dazu wäre die exakte Bestimmung der Eintrittswahrscheinlichkeit mit einem hohen Analyseaufwand verbunden, der meist nicht gerechtfertigt ist. Insbesondere können sich sowohl die Eintrittswahrscheinlichkeit, die u. a. von der Effektivität der Schutzmaßnahmen und der praktischen Häufigkeit von Angriffen abhängt, als auch der Schaden im Laufe der Zeit ändern, so dass das Risiko regelmäßig neu bestimmt werden muss.

Das Risikomanagement muss deshalb durch Methoden unterstützt werden, die trotz unscharfer und häufig subjektiver Eingabeparameter eine Ableitung und Priorisierung von Aktivitäten zum Umgang mit Risiken ermöglichen:

Definition 13 (Risikomanagement)

Das Risikomanagement (engl. risk management) ist ein Prozess zur gesamtheitlichen Identifikation, Analyse und Bewertung von Risiken sowie zur Festlegung und Steuerung von Maßnahmen, durch die Risiken eliminiert bzw. auf ein akzeptables Niveau reduziert werden können.

In [WhMa09, S. 117ff.] werden die Prozessbestandteile *risk identification*, *risk assessment* und *risk control* differenziert und wie folgt charakterisiert:

- **Risk identification** beginnt mit einer Kategorisierung der betrachteten Systeme und ihrer Komponenten, die entsprechend inventarisiert und anhand ihres Wertes priorisiert werden müssen. Zu jeder Komponente werden Verwundbarkeiten und Bedrohungen dokumentiert.
- **Risk assessment** bestimmt den potentiellen Schaden und die Eintrittswahrscheinlichkeit unerwünschter Ereignisse und berechnet daraus Risiken, die ebenfalls dokumentiert werden.
- **Risk control** umfasst die strategische Konzeption und Umsetzung von Maßnahmen zur Vermeidung, Delegation, Reduktion und Toleranz der ermittelten Risiken.

Insbesondere im Bereich des *risk assessment* und der darauf aufbauenden Priorisierung von technischen Schutzmaßnahmen existieren verschiedene Ansätze zum Umgang mit inhärent unscharfen Schätzungen; hierauf wird in Kapitel 6 eingegangen. Aufgrund der Dynamik bezüglich der betrachteten Systeme, Verwundbarkeiten und Bedrohungen müssen die Risiken kontinuierlich neu identifiziert und bewertet werden. Die resultierenden Strategien zum Umgang mit den Risiken sind typischerweise längerfristig ausgelegt, können jedoch auch die Spezifikation akuter Notfallmaßnahmen durch das IT-Sicherheitsmanagement anstoßen.

2.2.3.2. Bewertung der Sicherheit von IT-Systemen

Eine grundlegende Aufgabe bei der Anschaffung neuer bzw. Analyse vorhandener IT-Systeme ist die Bewertung ihrer Sicherheitseigenschaften. Die Standardisierung von Beurteilungskriterien trägt maßgeblich zur Vergleichbarkeit von Systemen bei. Durch die darauf basierende Zertifizierung von Systemen durch neutrale Dritte kann zudem der szenarienspezifische Evaluationsaufwand reduziert werden.

Eine zentrale Rolle nimmt der Kriterienkatalog *Common Criteria for Information Technology Security Evaluation* (kurz: CC) ein, der in Version 2.3 als ISO-Standard 15408 anerkannt wurde; in Deutschland vergibt das Bundesamt für Sicherheit in der Informationstechnik als akkreditierte Prüfstelle auf CC basierende Zertifizierungen.

Die Entstehungsgeschichte, der Inhalt und die Grenzen der CC werden in [Ecke09, S. 211ff.] umfassend analysiert. Aus diesem Grund werden an dieser Stelle nur die wichtigsten und im Rahmen dieser Arbeit relevanten Aspekte der CC rekapituliert.

Generell wird in den CC zwischen den von einem zu evaluierenden System vorgesehenen **Sicherheitsfunktionalitäten** und deren jeweiliger **Vertrauenswürdigkeit** bzw. Qualität unterschieden. Unter der Qualität werden dabei sowohl die theoretische Wirksamkeit der

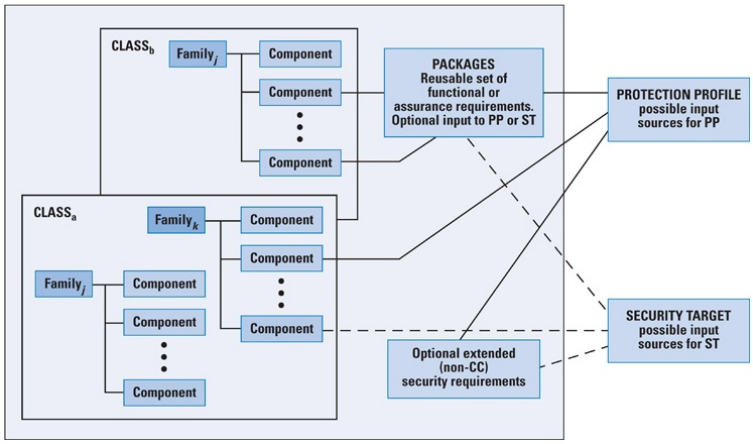


Abbildung 2.10.: Strukturierung von Anforderungen nach Common Criteria, Quelle: [Stal07]

ausgewählten Sicherheitsmechanismen als auch die Korrektheit ihrer Implementierung verstanden. Die CC sehen sieben Stufen der Vertrauenswürdigkeit (Evaluation Assurance Level, EAL1 – EAL7) vor, zu denen Prüfaufwand und -tiefe proportional sind: Die niedrigste Stufe EAL1 entspricht einem rein funktionalen Test, wohingegen die höchste Stufe EAL7 den formal verifizierten Entwurf und Test voraussetzt.

Die Sicherheitsfunktionalitäten werden in die Klassen FAU (Sicherheitsprotokollierung), FCO (Kommunikation), FCS (kryptographische Unterstützung), FDP (Schutz der Benutzerdaten), FIA (Identifikation und Authentifizierung), FMT (Sicherheitsmanagement), FPR (Privacy), FPT (Schutz der Sicherheitsfunktionen), FRU (Betriebsmittelnutzung), FTA (Schnittstelle) und FTP (vertrauenswürdiger Pfad/Kanal) unterteilt. Diese Klassen sind wiederum in so genannte Familien aufgeteilt, die als Komponenten bezeichnete Sicherheitsanforderungen spezifizieren. Bei der Zertifizierung eines Systems kann somit in Form einer **Sicherheitsvorgabe** (Security Target, ST) einheitlich angegeben werden, welche Sicherheitsanforderungen berücksichtigt werden.

Implementierungsunabhängige Mengen von Sicherheitsanforderungen können wie in Abbildung 2.10 dargestellt in so genannte **Schutzprofile** (Protection Profiles, PP) einfließen, die auch weitere zur Beurteilung von zu evaluierenden Systemen relevante Angaben, z. B. über mögliche Betriebsumgebungen, enthalten und somit als Anforderungsanalyse bzw. Lastenheft angesehen werden können.

Obwohl die CC die differenzierte Zertifizierung konkreter Produkte zum Ziel haben, sind ihre Methoden auch für die Beurteilung der Sicherheitseigenschaften von Security-Frameworks durchaus interessant.

2.2.3.3. Bezug zwischen dem Security Management und den weiteren ITSM-Prozessen

Unter IT Service Management (ITSM) wird allgemein das Management von IT-Infrastrukturen unter starker Dienstleistungs- und Kundenorientierung verstanden. Best Practices Werke wie die IT Infrastructure Library (ITIL) oder das Microsoft Operations Frame-

work (MOF) haben weite Verbreitung gefunden und basieren auf der Methodik, abstrakte Referenzprozesse für die einzelnen ITSM-Teildisziplinen zu spezifizieren.

Ohne Beschränkung der Allgemeinheit wird am Beispiel der aktuellen Version ITIL v3 [ITILv3] skizziert, welche Rolle das IT-Sicherheitsmanagement im Hinblick auf die weiteren ITSM-Prozesse einnimmt. ITIL v3 orientiert sich mit seinem fünf Büchern am grundlegenden Dienstlebenszyklus: Strategie (Service Strategy), Entwurf (Service Design), Produktivführung (Service Transition), Betrieb (Service Operation) und Verbesserung (Continual Service Improvement). Der Prozess **Information Security Management** ist im Bereich Service Design angesiedelt; er wird durch den in ITIL v3 im Bereich Service Operation neu eingeführten Prozess **Access Management** ergänzt.

Das IT-Sicherheitsmanagement wird von ITIL selbst als Querschnittsprozess gesehen, der Schnittstellen zu fast allen anderen ITSM-Prozessen hat. Die Schwerpunkte liegen jedoch auf den Beziehungen zu den folgenden Prozessen:

- Die Beziehungen zum **Service Level Management** (Bereich Service Design) nehmen eine hervorgehobene Rolle ein, da Sicherheitsanforderungen zu den Bestandteilen von Service Level Agreements mit Kunden (SLAs), internen Operational Level Agreements (OLAs) und Underpinning Contracts (UCs) mit Zulieferern gehören. Damit verbunden ist die Notwendigkeit zur Definition und kontinuierlichen Überwachung von Kennzahlen (**Key Performance Indicators**, KPIs), die auch zur Beurteilung der Effektivität und Effizienz des IT-Sicherheitsmanagementprozesses selbst herangezogen werden; dies ist den Prozessen **Measurement** und **Service Reporting** im Bereich Continual Service Improvement zuzuordnen.
- Die in Abschnitt 2.2.2 diskutierte Behandlung von Sicherheitsvorfällen erfolgt im Rahmen des **Incident Management** (Bereich Service Operation). Mit dem Übergang von ITIL v2 auf ITIL v3 wurde zudem der Prozess **Event Management** (ebenfalls im Bereich Service Operation) eingeführt, der auf eine stärker automatisiert ablaufende Überwachung abzielt und somit auch die Verantwortung für die Auswertung von Sicherheitsereignissen übernimmt.
- Die Berücksichtigung von Sicherheitsaspekten spielt auch bei jeglichen Änderungen an der IT-Infrastruktur, die vom **Change Management** (Bereich Service Transition) zu genehmigen sind, eine essentielle Rolle. Beispielsweise müssen sowohl Sicherheitsexperten im so genannten Change Advisory Board vertreten sein als auch Sicherheitsregeln für den Umgang mit kurzfristigen Emergency Changes definiert werden, bei deren Genehmigung häufig die Zeit für eine vollständige Analyse aller Sicherheitsaspekte fehlt.

Die Schnittstellen zu den weiteren ITIL-Prozessen lassen sich wie folgt zusammenfassen:

- Im Bereich Service Strategy beinhaltet das Financial Management das Risikomanagement und muss somit ebenfalls IT-Sicherheitsrisiken berücksichtigen. Ferner umfasst das Service Portfolio Management auch Sicherheitsdienste, die als separate Dienstleistung oder im Zusammenspiel mit anderen Diensten angeboten werden.
- Im Bereich Service Design haben sowohl das IT Service Continuity Management als auch das Availability Management einen direkten Bezug zur Verfügbarkeit als IT-Sicherheitsbasisziel, so dass hier auch beispielsweise Maßnahmen zur Wiederherstellung der IT-Infrastruktur nach IT-sicherheitsbezogenen Angriffen zu beachten sind. IT-Sicherheit muss unter dem Aspekt der möglichst uneingeschränkten Dienstverfügbarkeit

auch während laufender Angriffe zudem im Capacity Management berücksichtigt werden.

- Zum Bereich Service Transition gehören neben dem bereits diskutierten Change Management auch die Prozesse Service Asset and Configuration Management, Release and Deployment Management, Evaluation sowie Service Validation and Testing. Neben den funktionalen Aspekten des jeweils betrachteten Dienstes sind hierbei selbstverständlich auch seine Sicherheitseigenschaften zu berücksichtigen.
- Sofern Sicherheitsvorfälle nicht im Incident Management geklärt werden können, da sie beispielsweise auf neu entdeckte Verwundbarkeiten zurückzuführen sind, übernimmt das Problem Management im Bereich Service Operation die Bearbeitung.

Diese Schnittstellen und ihre Auswirkungen auf die internen Abläufe der Prozesse werden – spezifisch für das Management von Security-Frameworks – in Kapitel 6 vertieft.

2.3. Relevante Aspekte und Methoden des Security Engineering

Die von Ross Anderson grundlegend geprägte Disziplin Security Engineering konzentriert sich auf die Prozesse, Methoden und Werkzeuge, die für das Design, die Implementierung, die Anpassung und das Testen komplexer Systeme notwendig sind, um deren Zuverlässigkeit auch bei böswilligem oder fehlerhaftem Umgang sowie unter anderen widrigen Umständen sicherzustellen [Ande08, S. 3]. Security Engineering ist interdisziplinär, da neben softwaretechnischen Methoden beispielsweise auch juristische Aspekte, wirtschaftliche Betrachtungen sowie Maßnahmen zum physischen Schutz und zur Verbesserung der Benutzbarkeit unter psychologischen Aspekten einfließen.

Nachfolgend werden zunächst die vom Security Engineering abgedeckten Teildisziplinen skizziert, da diese auch für die Konzeption und Umsetzung von Security-Frameworks relevant sind, und anschließend die Auswirkungen auf das Software Engineering und das Design komplexer Softwaresysteme diskutiert.

2.3.1. Überblick über die Teildisziplinen des Security Engineering

Beim Design der Sicherheitseigenschaften umfangreicher Systeme berücksichtigt das Security Engineering konsequent, dass selbst bei einer fehlerfreien Implementierung eines lückenlosen Konzepts der Faktor Mensch als häufig schwächstes Glied in der Kette der Schutzmaßnahmen verbleibt. Diesem inhärenten Problem wird durch die Kombination zweier Prozesse entgegen gewirkt:

1. Systeme und insbesondere ihre sicherheitsrelevanten Bestandteile werden unter Berücksichtigung aktueller Erkenntnisse der allgemeinen Psychologie sowie der Sozialpsychologie konzipiert. Wenn beim Design bewusst nach intuitiverer Bedienbarkeit und einer Steigerung der Benutzerfreundlichkeit (engl. *usability*) gestrebt wird, können als Seiteneffekt auch potentielle Schwachstellen leichter identifiziert werden: Beispielsweise haben viele Benutzer Schwierigkeiten, sich komplexe Passwörter zu merken, so dass je nach angestrebtem Schutzniveau andere Authentifizierungsverfahren in Erwägung gezogen werden müssen.

2. Die Anwender der Systeme müssen sensibilisiert und geschult werden. Dies deckt sich mit den in Abschnitt 2.1.2 diskutierten Zielen des IT-Sicherheitsmanagements; vom Security Engineering werden insbesondere systemspezifische Materialien beigetragen, wohingegen die Vermittlung allgemeiner Sicherheitsgrundlagen und deren Komposition auf Basis didaktischer Methoden nicht zu seinem Schwerpunkt gehören.

Das Security Engineering geht im Allgemeinen davon aus, dass die betrachteten Systeme beliebig verteilt sind. Entsprechend gehören Verfahren zum sicheren Umgang mit nebenläufigen Systemprozessen, z. B. zur Vermeidung von Race Conditions oder Deadlocks, ebenso zum Grundrepertoire wie die Fehlertoleranz bezüglich des Ausfalls oder der Kompromittierung einzelner Komponenten.

Zur Kommunikation zwischen den Komponenten des Systems werden Protokolle entworfen, die gegenüber Angriffen wie dem Abhören oder Manipulieren von Datenpaketen immun sein müssen. Ebenso gehören die Anwendung von Authentifizierungs- und Autorisierungsverfahren sowie die Abschottung der Systemanwender gegeneinander, beispielsweise durch Virtualisierung oder Sandboxing, zum Aufgabengebiet des Security Engineering. In vielen Fällen unterstützen kryptographische Maßnahmen, mit denen der Security Engineer vertraut sein muss, die eingeschlagenen Lösungswege.

Neben mehrschichtigen und multilateralen Sicherheitsmodellen, die softwareseitig realisiert werden können, wie beispielsweise das Bell-LaPadula- und das Chinese-Wall-Modell, werden auch hardwarebasierte Schutzmaßnahmen vielfältig eingesetzt. Hierzu gehören unter anderem mechatronische Zutrittskontrollsysteme, manipulations- und fälschungssichere Hardware, Maßnahmen zur Reduktion elektromagnetischer Emissionen und biometrische Authentifizierungssysteme.

Einen wesentlichen Beitrag zum Charakter als Ingenieursdisziplin leistet die Orientierung an ökonomischen Aspekten: Methoden zur Einschätzung des Wertes der eingesetzten Systeme sowie der verarbeiteten Informationen und zur Gegenüberstellung mit dem Aufwand für geeignete Schutzmaßnahmen spielen ebenso eine Rolle wie der Schutz der eigenen Entwicklungen durch digitales Rechtemanagement; dieses wird beispielsweise im Bereich Kopierschutz oder zur nutzungsbasierten Abrechnung eingesetzt.

Schließlich gehören zum Security Engineering auch Methoden zum Management von Software Engineering Projekten unter besonderer Berücksichtigung von Sicherheitseigenschaften und alle Maßnahmen rund um die Evaluation und Zertifizierung der resultierenden Systeme, beispielsweise auf Basis der in Abschnitt 2.2.3.2 diskutierten Common Criteria. Da sich diese Aspekte einerseits auf das Design von Security-Frameworks auswirken und andererseits Gegenstand zahlreicher Forschungsarbeiten in den letzten Jahren waren, geht der nächste Abschnitt näher auf sie ein.

2.3.2. Auswirkungen auf das Software Engineering

In keinem anderen Bereich innerhalb oder außerhalb der IT werden so viele neue Sicherheitslücken entdeckt, offen diskutiert und so häufig von Angreifern ausgenutzt wie bei Software. Die Verbesserung der Sicherheitseigenschaften von Software ist deshalb nicht nur ein gemeinsames wissenschaftliches Schwerpunktthema von Security Engineering und Software Engineering, sondern hat auch für nahezu alle namhaften industriellen Softwarehersteller hohe

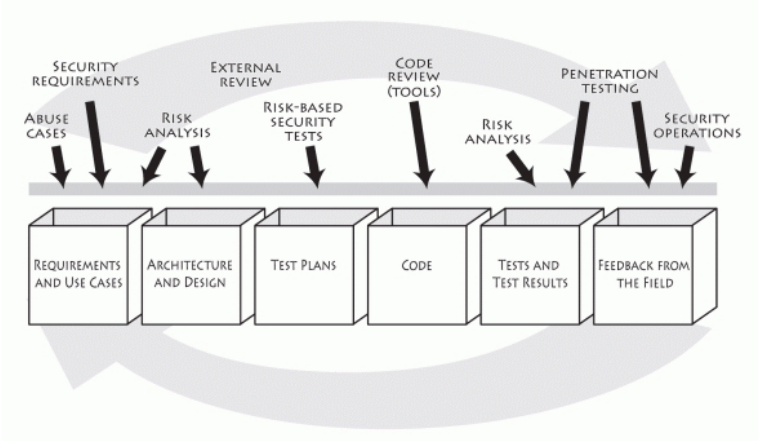


Abbildung 2.11.: Integration von Security Engineering Methoden in der Softwareentwicklung, Quelle: [SeTo08]

Priorität. Die dabei verfolgten Ziele fasst der Security Development Lifecycle von Microsoft wie folgt zusammen [Mic10]:

1. **Secure by design**: Beim Design von Softwaresystemen müssen Sicherheitseigenschaften von Anfang an explizit berücksichtigt werden; insbesondere muss das erst nachträgliche Aufpfropfen von Sicherheitsmechanismen vermieden werden.
2. **Secure by default**: Das Softwaresystem muss in seinem Auslieferungszustand eine vom Hersteller als sicher eingeschätzte Konfiguration aufweisen; dadurch sollen Risiken vermieden werden, die entstehen, wenn sich Administratoren nicht umgehend nach der Inbetriebnahme um die Systemkonfiguration unter Sicherheitsaspekten kümmern. Dieses Paradigma stellt eine radikale Abkehr von der früheren Praxis dar, möglichst sämtliche Zusatzfunktionen der Software bereits im Auslieferungszustand zu aktivieren, um den szenarienspezifischen Konfigurationsaufwand möglichst zu minimieren.
3. **Secure in deployment**: Das Softwaresystem darf während seiner Inbetriebnahme keine Angriffsfläche bieten. Dies zielt beispielsweise auf Betriebssysteme ab, die auf mit dem Internet verbundenen Rechnern installiert und bereits potentiell kompromittiert werden, noch bevor die aktuellen Security-Patches installiert werden können.

Offensichtlich muss sich die Berücksichtigung von Sicherheitsaspekten folglich konsequent durch alle Phasen der Softwareentwicklung ziehen (vgl. [DS00]). Legt man vereinfachend einen Lebenszyklus mit den Phasen Anforderungsanalyse, Design, Implementierung, Verifikation, Release und Support zugrunde, so werden wie in Abbildung 2.11 dargestellt alle Aktivitäten durch Methoden des Security Engineering unterstützt; insbesondere die ersten beiden Phasen wurden unter Sicherheitsaspekten wissenschaftlich fundiert aufbereitet:

- Im Rahmen der Anforderungsanalyse werden Sicherheitsanforderungen und potentielle Sicherheitsprobleme explizit festgehalten. Hierfür wurden mehrere Ansätze entwickelt, die insbesondere auf eine Erweiterung von UML Use-Case-Diagrammen und deren textueller Beschreibung abzielen.

Einen hohen Bekanntheitsgrad hat das von Jürjens geprägte UMLsec [Jurj02] erzielt, das für mehrere UML-Diagrammtypen sicherheitsspezifische Annotationen vorsieht. Dieser Ansatz beschreibt zudem einen Entwicklungsprozess, der auf die Vermittlung der Sicherheitsanforderungen an Entwickler und die Dokumentation der sicherheitsspezifischen Designentscheidungen eingeht.

Einen noch expliziteren Ansatz wählen Sindre und Opdahl in [SO05]: Use Cases werden zu so genannten *Misuse Cases* erweitert, um einerseits potentielle Angreifer und Schwachstellen aufzuzeigen; andererseits ist auch die explizite Modellierung von Gegenmaßnahmen vorgesehen, um deren Vollständigkeit und Korrektheit leichter beurteilen zu können.

- Das bekannte Konzept der Design Patterns, die als Musterlösungen für bei der Softwareentwicklung häufige Designprobleme fungieren, wurde um Security Patterns erweitert. Nach zahlreichen Einzelbeiträgen aus Wissenschaft und Praxis wird inzwischen an einer systematischen Katalogisierung gearbeitet.

  Eine Vorreiterrolle nehmen hierbei die Open Group Security Design Patterns [OGSDP] ein. Sie unterscheiden grundlegend zwischen den *Available System Patterns*, die den ununterbrochenen Dauerbetrieb des entworfenen Systems unterstützen sollen, und den *Protected System Patterns*, die die Vertraulichkeit gewährleisten und gegen unberechtigte Nutzung und Modifikationen schützen sollen. Neben den Mustern selbst wird auch ihre Anwendung von der Open Group beschrieben; im Unterschied zum oben erläuterten Paradigma *secure by design* wird hierbei jedoch vorrangig die in der Praxis noch häufig anzutreffende Situation behandelt, dass Sicherheitsmaßnahmen in bereits vorhandenen Programmcode nachträglich integriert werden müssen.

Diesen Fortschritten gegenüber ist festzuhalten, dass beim Testen der entwickelten Software die Sicherheitsaspekte häufig noch vernachlässigt werden, da internes Expertenwissen fehlt und der Zeit- und Kostenaufwand für externe Sicherheitstests häufig unökonomisch erscheint (vgl. [BBH+03]). Die verbleibenden Schwachstellen werden somit weiterhin überwiegend erst gefunden, wenn das System bereits in Betrieb ist.

Eine offizielle Bekanntmachung der Schwachstellen bzw. Verwundbarkeiten erfolgt in der Regel durch den Hersteller des betroffenen Systems, sobald eine Lösung in Form eines Work-Arounds oder Security-Patches verfügbar ist. Darüber hinaus werden Sicherheitslücken in weit verbreiteten Softwaresystemen, die von unabhängigen Sicherheitsexperten entdeckt wurden, häufig bereits vorab in Internet-Foren wie Bugtraq [BUGTRQ] diskutiert. Obwohl es üblich geworden ist, den Hersteller rechtzeitig vor der öffentlichen Diskussion auf die Sicherheitsprobleme aufmerksam zu machen, muss im Allgemeinen angenommen werden, dass qualifizierten Angreifern viele Verwundbarkeiten schon lange bekannt sind, bevor sie ins öffentliche Bewusstsein rücken. Auf Basis der öffentlichen Diskussion können typische Schwachstellen identifiziert und zur Prävention an Entwickler kommuniziert werden; das Open Web Application Security Project veröffentlicht beispielsweise regelmäßig Listen der häufigsten Angriffe auf web-basierte Anwendungen und dokumentiert deren Funktionsweise sowie empfohlene Gegenmaßnahmen [OWASP].

2.4. Überblick über Angriffe und Sicherheitsmechanismen

Zu den im nachfolgenden Abschnitt 2.5 definierten Aufgaben von Security-Frameworks gehört der Schutz vor ausgewählten Angriffen mittels ausgewählter Sicherheitsmechanismen. Für eine Einordnung und Beurteilung der von Security-Frameworks abgedeckten Bereiche wären Taxonomien für Angriffe und Sicherheitsmechanismen ein effektives Hilfsmittel. Aufgrund des sehr breiten Anwendungsbereichs der IT-Sicherheit und der kontinuierlichen Weiterentwicklung von Angriffen und Gegenmaßnahmen existieren Taxonomien bislang aber nur für einige, in Relation zum Gesamtspektrum kleine Bereiche wie beispielsweise die internet-basierten Angriffe [ASM06].

In den Abschnitten 2.4.1 und 2.4.2 werden deshalb die von den in Kapitel 4 vorgestellten Security-Frameworks am häufigsten betrachteten Angriffe und Sicherheitsmechanismen kurz vorgestellt. Beide Aufstellungen erheben bei Weitem keinen Anspruch auf Vollständigkeit. Zudem können nicht alle der vorgestellten Elemente den verwendeten Kategorien disjunkt zugeordnet werden; diese bilden somit keine Taxonomie.

Der Auswahl von Angriffen und dagegen schützenden Sicherheitsmaßnahmen ist konzeptionell ein **Angreifermodell** zugrunde zu legen, das Aufschluss über die Position und Fähigkeiten des Angreifers sowie seine Motivation für einen Angriff gibt. Bei der Tätertypisierung ist beispielsweise zu berücksichtigen, ob es sich um einen Innentäter oder einen externen Angreifer handelt, da sich sowohl das Wissen über das angegriffene System als auch die bereits initial vorhandenen Berechtigungen signifikant unterscheiden können (vgl. Abbildung 2.12).

Auch die technischen Fähigkeiten und Hilfsmittel des Angreifers, zu denen die Qualität der Schutzmaßnahmen mindestens proportional sein muss, unterscheiden sich grundlegend, beispielsweise zwischen experimentierfreudigen Teenagern und erfahrenen Industriespionen. Die Spezifikation der technischen Fähigkeiten des Angreifers erfolgt meist in Anlehnung an die betrachteten IT-Sicherheitsziele: Geht man davon aus, dass ein Angreifer die ausgetauschten Nachrichten abhören kann, so ist durch diesen passiven Angriff primär deren Vertraulichkeit gefährdet. Hat der Angreifer jedoch die Möglichkeit, die Kommunikation nicht nur abzuhören, sondern im Rahmen eines aktiven Angriffs auch zu modifizieren, so sind zusätzlich auch die Integrität und – je nach angenommener Manipulation – die Verfügbarkeit in Gefahr.

Schließlich ist auch die Motivation bzw. Zielsetzung des Täters zu betrachten, da hiervon beispielsweise auch abhängen kann, wie schnell dieser bei mangelndem Erfolg aufgibt; häufig werden die vier Motive Spieltrieb, Geltungsbedürfnis, Geldgier und Vandalismus unterschieden (vgl. [Poh04b, S. 10]).

2.4.1. Von Security-Frameworks häufig berücksichtigte Angriffe

Trotz ihrer Vielfalt und Individualität sind zu schützende Systeme überwiegend ähnlichen Angriffen und Angriffsmethoden ausgesetzt. Zu den von den aktuellen Security-Frameworks am häufigsten berücksichtigten Angriffen gehören:

- **Physische Angriffe** auf geschützte Objekte: Hierzu gehören neben nicht unmittelbar IT-bezogenen Angriffen wie Einbruch, Diebstahl oder Zerstörung insbesondere die Manipulation von Hardware (engl. *tampering*) und das Ausspähen von Informationen durch

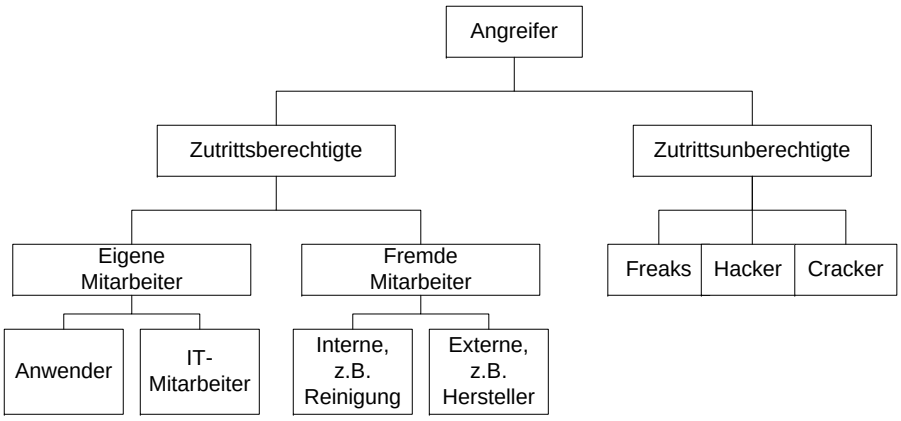


Abbildung 2.12.: Tätertypisierung in der IT-Sicherheit nach Pohl (vgl. [Poh04b, S. 10])

die Analyse elektromagnetischer Emissionen; hierbei tritt häufig die Besonderheit auf, dass der legitime Eigentümer als Angreifer fungiert.

- **Social Engineering**: Hierunter wird im Umfeld der IT-Sicherheit eine Manipulation von Personen verstanden, die das Ziel verfolgt, vertrauliche Informationen zu erhalten oder Aktionen auszuführen, die der Angreifer nicht selbst ausführen könnte.

  Viele Angriffe nutzen weit verbreitete menschliche Eigenschaften wie Hilfsbereitschaft und Neugier aus. So werden beispielsweise einem Angreifer, der am Telefon glaubwürdig behauptet, im Auftrag des eigenen Vorgesetzten zu handeln, oft interne Informationen anvertraut (vgl. [MS03]). Untersuchungen zeigen auch, dass scheinbar versehentlich liegen gelassene oder öffentlich verschenkte Datenträger, die Schadsoftware enthalten, häufig unbedacht genutzt werden (vgl. [Sta06]).

  Problematisch bei dieser Art von Angriffen ist insbesondere, dass sie oftmals weder von den Opfern noch von den Sicherheitsbeauftragten rechtzeitig erkannt werden und somit bei der Einschätzung der aktuellen Sicherheitslage nur unzureichend berücksichtigt werden können.

- **Softwarebasierte Angriffe**: Die softwarebasierten Angriffe auf andere Software bzw. Daten werden mit großem Abstand am häufigsten von den betrachteten Security-Frameworks behandelt. Sie können wie folgt differenziert werden:

  - **Implementierungsfehler**: Wie aus dem Namen bereits hervorgeht, handelt es sich um Sicherheitslücken, die sich bei der Programmierung der Software, also nicht beim Design oder im Betrieb, einschleichen. Besonders weit verbreitet sind folgende Fehlertypen:

    * Buffer overflow: Für die Aufnahme einer Benutzereingabe wird vom Programm weniger Speicherplatz vorgesehen als tatsächlich benötigt wird. Dadurch kommt es bei zu umfangreichen Eingaben zum namensgebenden Pufferüberlauf, der dazu führt, dass der mit anderen Daten oder Programmcode belegte Speicher überschrieben wird. Ein Angreifer kann mittels einer gezielt vorbereiteten, zu langen Eingabe eigenen Programmcode einschleusen, der im weiteren Programmverlauf ausgeführt wird.

  - Code injection: Wenn Benutzereingaben ungeprüft weiterverarbeitet werden, um sie in Datenbankabfragen oder den Aufruf von Systemprogrammen zu integrieren, kann ein Angreifer beispielsweise eigene SQL- oder Systembefehle absetzen.
  - TOCTTOU (time of check to time of use): Hierbei handelt es sich um eine Race Condition, bei der eine Bedingung, z. B. eine Berechtigung, nur geprüft wird, bevor mit einer Aktion begonnen wird. Bis zum Abschluss der Aktion kann sich die Bedingung aber bereits geändert haben, so dass die Aktion unautorisiert durchgeführt wird. Das Problem kann aufgrund der Nebenläufigkeit auch an Einzelrechnern und in langdauernden verteilten Transaktionen auftreten.

  In allen Fällen muss der Angreifer die Verwundbarkeiten kennen; sie können z. B. durch Analyse des Quelltextes, Reverse Engineering oder empirische Versuche gefunden werden.

- **Schadsoftware**: In diese Kategorie fallen
  - Viren; diese modifizieren primär Dateien auf einem befallenen Rechner und werden bei deren Nutzung aktiviert, um sich weiter verbreiten zu können.
  - Würmer, die sich über ein Netz unter Ausnutzung bekannter Sicherheitslücken selbst verbreiten können, ohne sich hierzu zwingend in ein Wirtsprogramm einnisten zu müssen.
  - Trojanische Pferde, die Schadfunktionen in einer ansonsten nützlichen und vom Benutzer gewünschten Software verstecken. Eine Sonderform stellt so genannte Spyware dar, die keinen direkten Schaden am befallenen System verursacht, sondern Daten an den Angreifer übermittelt, z. B. mitprotokollierte Passwörter oder Informationen über das Nutzungsverhalten.
  - Rootkits, die von einem Angreifer dazu verwendet werden, einen erfolgreichen Einbruch zu vertuschen und jederzeit wieder unbemerkt Vollzugriff auf das System zu erhalten, indem Systemprogramme bis hin zum Betriebssystemkern gegen kompromittierte Varianten ausgetauscht werden.

  Alle Angriffe dieser Art haben die Gemeinsamkeit, dass die Ausführung des Schadcodes initial angestoßen werden muss. Bei Viren und Trojanischen Pferden basiert dies überwiegend auf Social Engineering, wohingegen Würmer Implementierungsfehler in Software ausnutzen. Rootkits können installiert werden, sobald ein Angreifer die Kontrolle über ein System hat; die Installation kann manuell erfolgen oder Teil eines automatisierten Prozesses sein.

- **Brute Force**: Im engeren Sinn werden unter Brute Force Angriffe auf kryptographische Schutzmechanismen verstanden, durch die beispielsweise ein zur Dekodierung benötigter Schlüssel bzw. ein Passwort durch das systematische Ausprobieren aller möglichen Werte ermittelt werden soll. Im weiteren Sinn werden darunter alle Angriffe verstanden, die sich durch ihre Quantität, aber nicht durch ihre Qualität auszeichnen. So basiert beispielsweise auch ein Distributed Denial of Service (DDoS) Angriff, bei dem ein aus mehreren zehntausend Rechnern bestehendes Botnet gezielt einen einzelnen Server überlastet, letztendlich ebenfalls auf „roher Gewalt“.

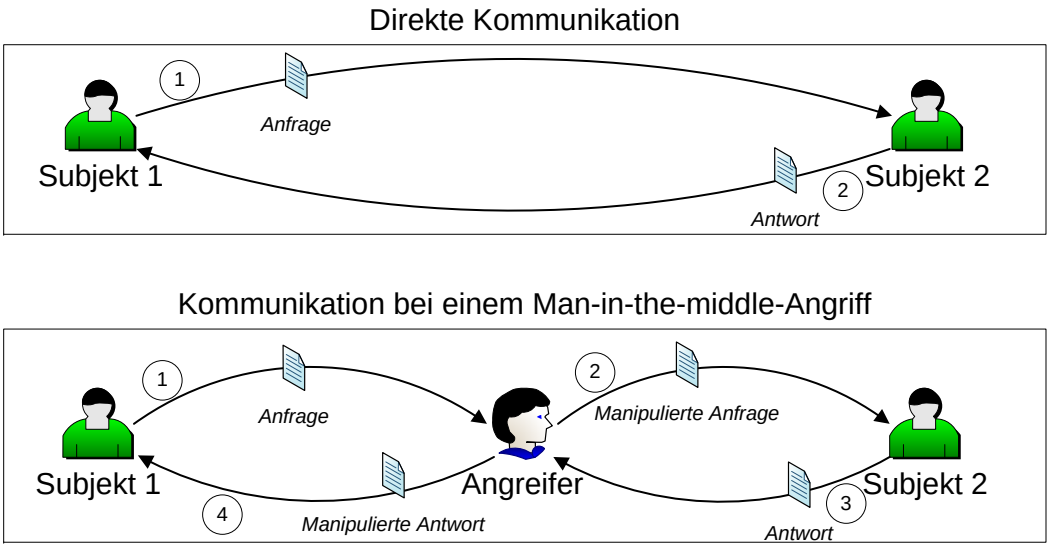


Abbildung 2.13.: Datenfluss bei einem Man-in-the-middle-Angriff

– **Eingriffe in den Nachrichtenaustausch**: Neben dem rein passiven Abhören (engl. *sniffing*) der ausgetauschten Daten zum Zweck der Informationsgewinnung gehören hierzu:

  * Replay: Durch das Wiedereinspielen von Nachrichten verfolgt der Angreifer das Ziel, nicht idempotente Aktionen mehrfach auszuführen. Sofern Nachrichtenduplikate nicht erkannt werden, funktioniert dieser Angriff auch bei verschlüsselten Nachrichten, die der Angreifer nicht modifizieren kann.

  * Spoofing: Der Angreifer versucht, sich als ein anderes Subjekt auszugeben. Der Begriff ist in Bezug auf die Fälschung von IP-Adressen, E-Mail-Absenderadressen und Webseiten weit verbreitet. Der Missbrauch der Kenntnis personenbezogener Daten von Dritten wird hingegen als Identitätsdiebstahl (engl. *identity theft*) bezeichnet.

  * Man-in-the-middle: Hierbei handelt es sich prinzipiell um ein Angreifermodell, bei dem Sender und Empfänger nicht mehr direkt miteinander kommunizieren; vielmehr fungiert der Angreifer wie in Abbildung 2.13 dargestellt unbemerkt als Empfänger für den eigentlichen Sender und als Sender für den eigentlichen Empfänger. Unter einem Man-in-the-middle-Angriff wird allgemein die Ausnutzung dieser Angreiferposition verstanden, um Nachrichteninhalte beliebig modifizieren zu können. Seine Relevanz ergibt sich daraus, dass die Punkt-zu-Punkt-Verschlüsselung der Nachrichten keinen Schutz bietet, wenn die Authentizität des Kommunikationspartners nicht ausreichend überprüft wurde.

  Diese Angriffe sind zwar nur praktikabel, wenn sich der Angreifer an einer geeigneten Position im Netz befindet. Dies kann aber je nach Szenario, beispielsweise durch die Kompromittierung eines in der Netztopologie nahe gelegenen Rechners oder einer Netzkomponente, eine nur triviale Hürde sein.

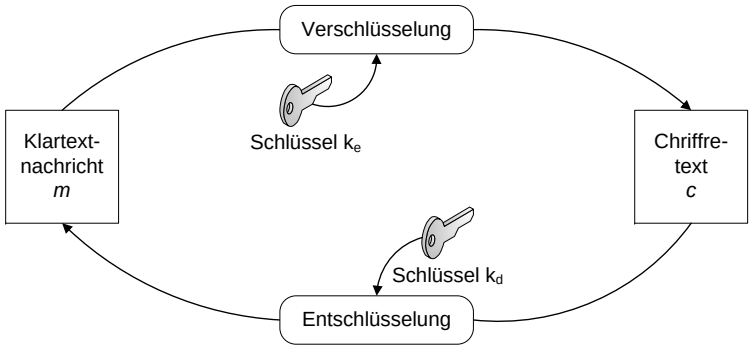


Abbildung 2.14.: Grundlegender Ablauf von Ver- und Entschlüsselung

Beispiel – Kombination von Angriffsarten:

Häufig werden mehrere Angriffsarten miteinander kombiniert. So gilt ein so genannter **Phishing**-Angriff primär als *Social Engineering*: Ein Benutzer soll durch eine offiziell anmutende E-Mail, die beispielsweise scheinbar von seiner Bank stammt, dazu verleitet werden, sein Online-Banking-Passwort auf einer in der E-Mail verlinkten Webseite einzugeben. Diese gehört in Wirklichkeit jedoch dem Angreifer und sieht nur äußerlich wie die richtige Webseite der Bank aus. Sowohl die E-Mail als auch die Webseite sind folglich Beispiele für *Spoofing*. Hinzukommen kann, dass die für die Netzkommunikation zuständigen Betriebssystemkomponenten durch *Schadsoftware* manipuliert wurden, so dass auch ein Aufruf der richtigen Online-Banking-Webseite zu einer Verbindung mit dem Webserver des Angreifers führen kann (sog. **Pharming**-Angriff).

Im Allgemeinen sind Sicherheitsmechanismen überwiegend als Lösungen für physische und softwarebasierte Angriffe ausgelegt. Gegen Social Engineering und Fehler in Prozessabläufen sind organisatorische Maßnahmen erforderlich, da rein technische Sicherheitsmaßnahmen keinen ausreichenden Schutz bieten können.

2.4.2. Von Security-Frameworks häufig verwendete Sicherheitsmechanismen

Die im Folgenden beschriebenen, von Security-Frameworks häufig verwendeten Sicherheitsmechanismen sind primär den im vorherigen Abschnitt beschriebenen softwarebasierten Angriffen zuzuordnen. Auf eine Vorstellung der möglichen Maßnahmen gegen physische Angriffe und Social Engineering wird an dieser Stelle verzichtet, da die in Kapitel 4 betrachteten Security-Frameworks in ihrer Gesamtheit die Notwendigkeit solcher Maßnahmen zwar betonen, aber fast ausschließlich eigene Lösungen für softwarebasierte Angriffe vorschlagen. Eine Konkretisierung weiterer Maßnahmen erfolgt in Kapitel 6.

Die Sicherheitsmechanismen können folgenden Kategorien zugeordnet werden:

- **Kryptographische Maßnahmen**: Ohne die Anwendung kryptographischer Verfahren, die direkt auf die Erhaltung der Vertraulichkeit und Integrität von Daten abzielen, sind viele Sicherheitslösungen heute nicht mehr denkbar:

– Durch Verschlüsselung wird angestrebt, dass Informationen nur von autorisierten Subjekten, denen der zur Entschlüsselung notwendige Schlüssel explizit mitgeteilt wurde, eingesehen werden können.

  Dabei wird eine Menge von Klartextnachrichten M (engl. *messages*) betrachtet, die von einem Verschlüsselungsverfahren E (engl. *encryption*) mittels Parametrisierung durch eine Schlüsselmenge K_E (engl. *keys*) auf eine Menge von Chiffretexten C (engl. *ciphertexts*) abgebildet wird: $E : M \times K_E \longrightarrow C$. Ein Entschlüsselungsverfahren D (engl. *decryption*) nimmt mittels Parametrisierung durch einen passenden Schlüssel aus der Menge K_D die Abbildung des Chiffretextes auf die ursprüngliche Klartextnachricht vor: $D : C \times K_D \longrightarrow M$; dieser Ablauf ist in Abbildung 2.14 zusammengefasst. Sofern zur Ver- und Entschlüsselung derselbe Schlüssel verwendet wird, wird das Verfahren als symmetrisch, ansonsten als asymmetrisch bezeichnet. Da in der Regel nur der zur Entschlüsselung benötigte Schlüssel geheim gehalten werden muss, entscheidet diese Eigenschaft grundlegend über den szenarienspezifischen Aufwand zur Schlüsselverwaltung (engl. *key management*).

  Soll jegliche Kommunikation zwischen zwei von insgesamt n Subjekten so verschlüsselt werden, dass sie von keinem anderen Subjekt entschlüsselt werden kann, sind bei symmetrischen Verfahren $\frac{n \cdot (n-1)}{2} = O(n^2)$ verschiedene Schlüssel notwendig; bei asymmetrischen Verfahren ist hingegen nur je ein Schlüssel zum Ver- bzw. Entschlüsseln pro Subjekt erforderlich, wodurch sich der Verwaltungsaufwand auf $O(n)$ reduziert. Bei symmetrischen Verfahren wird der Schlüssel häufig als *shared secret* bezeichnet, da er nur genau Absender und Empfänger bekannt sein soll. Bei asymmetrischen Verfahren wird häufig die Bezeichnung *Public Key* für den zur Verschlüsselung notwendigen Schlüssel verwendet, da dieser nicht geheimgehalten werden muss; ihm steht der zur Entschlüsselung notwendige *Private Key* gegenüber, der vom Empfänger geheimzuhalten ist.

  Der praktischen Anwendung von Verschlüsselungsverfahren werden durch den anfallenden Berechnungsaufwand Grenzen gesetzt; insbesondere eignen sich die in der Praxis derzeit weit verbreiteten asymmetrischen Verfahren nur für relativ kurze Klartexte, wohingegen umfangreiche Nutzdaten aus Performanzgründen symmetrisch verschlüsselt werden. Zur Kommunikation werden deshalb häufig hybride Verschlüsselungsverfahren eingesetzt: Ein zur effizienten symmetrischen Ver- und Entschlüsselung der Nutzdaten benötigter Schlüssel wird vorab mit höherem Berechnungsaufwand asymmetrisch verschlüsselt ausgetauscht.

  Durch Programmierbibliotheken, die Lese- und Schreibzugriffe auf Netzverbindungen durch transparent ver- bzw. entschlüsselnde Varianten der entsprechenden Systemaufrufe ersetzen, kann eine manipulationsevidente, verschlüsselte Kommunikation mit relativ wenig Aufwand implementiert werden.

– Mittels kryptographischer Prüfsummen, die von Hashfunktionen erzeugt werden, kann die Integrität der Daten überwacht werden.

  Eine Hashfunktion H bildet Eingaben beliebiger Länge aus dem Alphabet M auf Ausgaben fester Länge k aus dem Alphabet D ab: $H : M^* \longrightarrow D^k$. H hat dabei die Eigenschaften,

  * eine Einweg-Funktion zu sein, so dass sich die Eingabe nicht aus der Ausgabe

berechnen lässt,

- für eine gegebene Eingabe effizient berechenbar zu sein, und
- es andererseits praktisch unmöglich zu machen, zu einer gegebenen Ausgabe eine Eingabe zu konstruieren, die dieselbe Ausgabe liefert.

  Für eine *starke* Hashfunktion wird darüber hinaus gefordert, dass es praktisch unmöglich ist, zwei verschiedene (sinnvolle) Eingaben zu finden, deren Hashwerte übereinstimmen (Kollisionsresistenz).

Jede Änderung an den Daten, die als Eingabe für die Hashfunktion dienen, würde zu einer Änderung der Prüfsumme führen. Eine Verletzung der Datenintegrität kann folglich erkannt werden, indem die aktuelle Prüfsumme der Daten mit einer früher ermittelten Prüfsumme verglichen wird: Falls die beiden Prüfsummen nicht übereinstimmen, wurden die Daten zwischenzeitlich verändert. Im praktischen Einsatz muss allerdings offensichtlich sichergestellt werden, dass ein Angreifer nicht sowohl die Nutzdaten als auch die gespeicherte Prüfsumme manipulieren kann.

Häufig werden die Anwendung von Hash-Verfahren und die Verschlüsselung miteinander kombiniert: **Elektronische Signaturen** werden erstellt, indem der Absender eine Prüfsumme des zu signierenden Dokuments berechnet und mit seinem Private Key verschlüsselt; die Signatur kann anschließend, wie in Abbildung 2.15 dargestellt ist, vom Empfänger überprüft werden, indem dieser die vom Absender berechnete Prüfsumme mit dessen Public Key entschlüsselt und mit der selbst errechneten Prüfsumme vergleicht. Dieses Verfahren wird auch im Rahmen von **Public-Key-Infrastrukturen** (PKIs) eingesetzt: Eine vertrauenswürdige Instanz, die als Certificate Authority (CA) bezeichnet wird, signiert den Public Key eines Subjektes; Informationen über das Subjekt, dessen Public Key und die Signatur bilden zusammen ein so genanntes Zertifikat. Dadurch wird der praktische Aufwand zur Schlüsselverwaltung weiter reduziert, da sich andere darauf verlassen können, dass ihnen der richtige – und nicht beispielsweise ein von einem Angreifer untergeschobener – Schlüssel vorliegt, sofern sie der CA vertrauen und deren richtigen Public Key zur Verifikation des Zertifikats vorliegen haben.

Es muss jedoch Sorgfalt bei der Auswahl der konkret genutzten Verschlüsselungsverfahren (insbesondere Algorithmus, Schlüssellänge, Schlüsselqualität) angewandt und auf die jeweilige Nutzergruppe Rücksicht genommen werden; beispielsweise haben viele Anwender nur wenig Erfahrung im Umgang mit PKIs und Zertifikaten.

Einen wesentlichen Beitrag zur Sicherheit der kryptographischen Verfahren stellen die Verfügbarkeit qualitativ hochwertiger Zufallszahlen und die sichere Speicherung von Schlüsseln dar. Beide Funktionen werden zunehmend durch zusätzliche Hardware, die auf den Hauptplatinen von Rechnern verbaut bzw. in CPUs integriert wird, übernommen, um einige der inhärenten Defizite rein softwarebasierter Lösungen zu vermeiden.

Beispiel – VPNs:

Eine typische Anwendung für die Verschlüsselung mit Überprüfung der Integrität der übertragenen Daten sind virtuelle private Netze (VPNs), mittels derer Netze miteinander über nicht vertrauenswürdige dritte Netze, z. B. das Internet, sicher gekoppelt werden können.

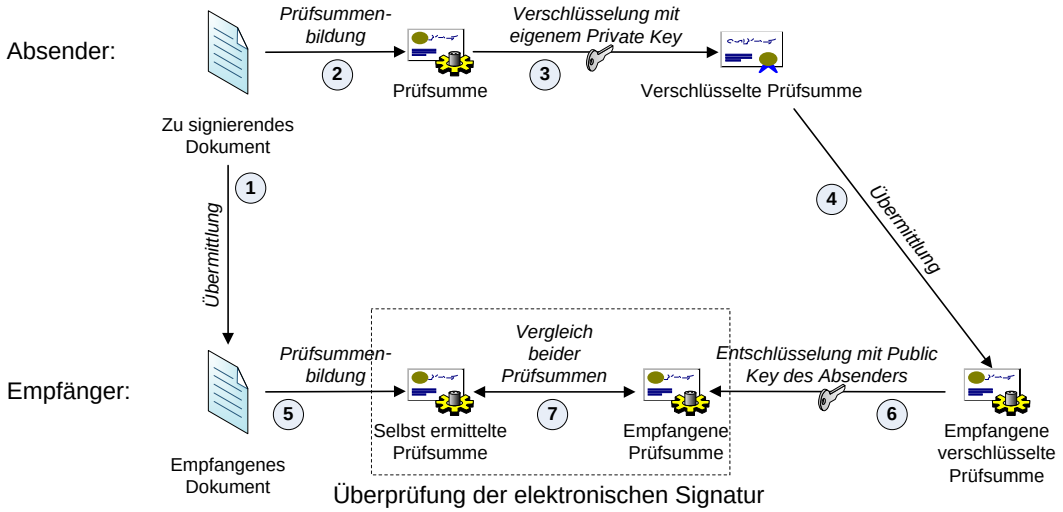


Abbildung 2.15.: Ablauf des Erstellens und Prüfens einer elektronischen Signatur

- **Access Control**: Durch Zugangskontrolle auf Netz- und Anwendungsebene wird sichergestellt, dass kritische Aktionen nur von autorisierten Personen vorgenommen werden können. Separate Sicherheitsmechanismen existieren für die beiden Phasen der Zugangskontrolle:

  1. **Authentifizierung**: Zunächst muss die Authentizität des zu überprüfenden Subjekts sichergestellt werden. Die Authentifizierung erfolgt typischerweise über Wissen (z. B. Passwort), Besitz (z. B. Smartcard) oder Biometrie (z. B. Venenmuster der Hand) und kann optional an vertrauenswürdige Dritte (engl. *trusted third party*, TTP) delegiert werden.

     Auf die Delegation wird häufig in Kombination mit ticketbasierten Mechanismen wie Kerberos [RC4120] oder WS-Federation [KE03] zurückgegriffen, auch um **Single Sign-On** zu unterstützen: Hierbei wird es als ausreichend betrachtet, wenn sich das Subjekt innerhalb einer definierten Zeitspanne einmalig gegenüber einer TTP authentifiziert, ohne dass die Authentifizierung für jeden in dieser Zeitspanne genutzten Dienst wiederholt werden muss.

  2. **Autorisierung**: Die Autorisierung entspricht der Überprüfung, ob ein authentifiziertes Subjekt zur Durchführung einer Aktion berechtigt ist. In einfachen Anwendungsfällen kann bei den Objekten in Form von Access Control Lists hinterlegt werden, welche Subjekte zu welchen Aktionen berechtigt sind. Alternativ führt jedes Subjekt eine Liste seiner Berechtigungen mit sich; diese muss von einer TTP ausgestellt worden und gegen Manipulationen durch das Subjekt geschützt sein.

     Um auch große Mengen von Subjekten, Berechtigungen und Objekten effizient verwalten zu können, hat sich in der Praxis die **rollenbasierte Zugangskontrolle** (RBAC) durchgesetzt (vgl. [SFK00]). Mengen von Berechtigungen werden dabei zu so genannten (technischen) Rollen gebündelt, die dann wiederum Subjekten oder Gruppen von Subjekten zugeordnet werden. Die Anzahl der zu pflegenden Zuordnungen kann dadurch wie in Abbildung 2.16 dargestellt drastisch gesenkt

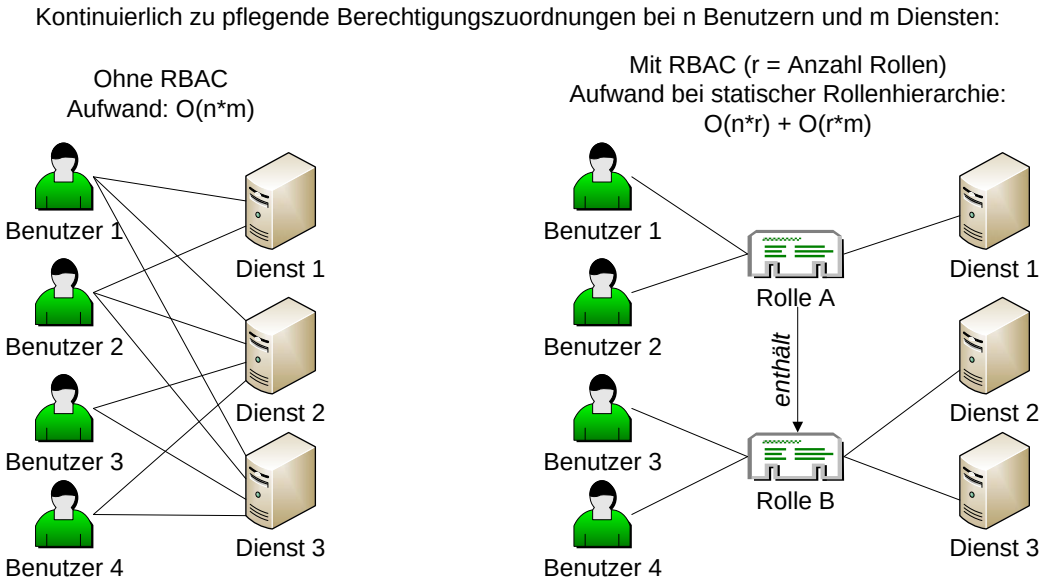


Abbildung 2.16.: Reduktion des Aufwands zur Verwaltung von Autorisierungen durch RBAC

werden, insbesondere indem die Anzahl der Rollen klein gegenüber der Anzahl der Subjekte gehalten wird; durch Rollenhierarchien kann zudem die Anzahl der zu pflegenden Zuordnungen zwischen Rollen und Berechtigungen reduziert werden. Im Rahmen der **attributbasierten Zugangskontrolle** (attribute based access control, ABAC) werden zunehmend neben explizit definierten Rollen auch weitere Eigenschaften des Subjekts, beispielsweise seine organisatorische Zugehörigkeit, für Autorisierungsentscheidungen herangezogen. Hierdurch kann der Aufwand zur expliziten Erfassung autorisierungsrelevanter Kriterien in der Praxis weiter reduziert werden, da viele Datenfelder nicht ausschließlich sicherheitsrelevant sind, sondern z. B. bereits im Personalverwaltungssystem einer Organisation erfasst werden.

Um die Autorisierungen systemübergreifend einheitlich zu regeln und den Implementierungsaufwand für jedes System zu reduzieren, werden häufig **policybasierte Verfahren** eingesetzt. Jedes System, das Benutzeraktionen durchführen soll, fungiert dabei wie in Abbildung 2.17 dargestellt als Policy Enforcement Point (PEP); dieser delegiert die Entscheidung über die Autorisierung an einen Policy Decision Point (PDP). Auf Basis von als Policies bezeichneten, maschineninterpretierbaren Regelwerken, die in einer als Policy Repository (PR) bezeichneten Datenbasis hinterlegt sind, entscheidet der PDP darüber, ob der Benutzer zur gewünschten Aktion autorisiert ist oder abgewiesen werden muss. Zur Formulierung von Policies existiert eine Vielzahl von zum Teil Turing-vollständigen Sprachen, über die auch Umgebungsbedingungen wie die aktuelle Uhrzeit und Messwerte von Sensoren in die Autorisierungsentscheidung einbezogen werden können. Analog dazu können in Abhängigkeit von der Zugriffsentscheidung Aktionen wie das Erzeugen von Sicherheitsereignissen (vgl. Abschnitt 2.2.2) angestoßen werden.

Auf Netzebene werden nach wie vor bevorzugt **Firewalls** zur Zugangskontrolle eingesetzt, um zu erreichen, dass durch eine Vorauswahl von Zugriffsversuchen möglichst nur

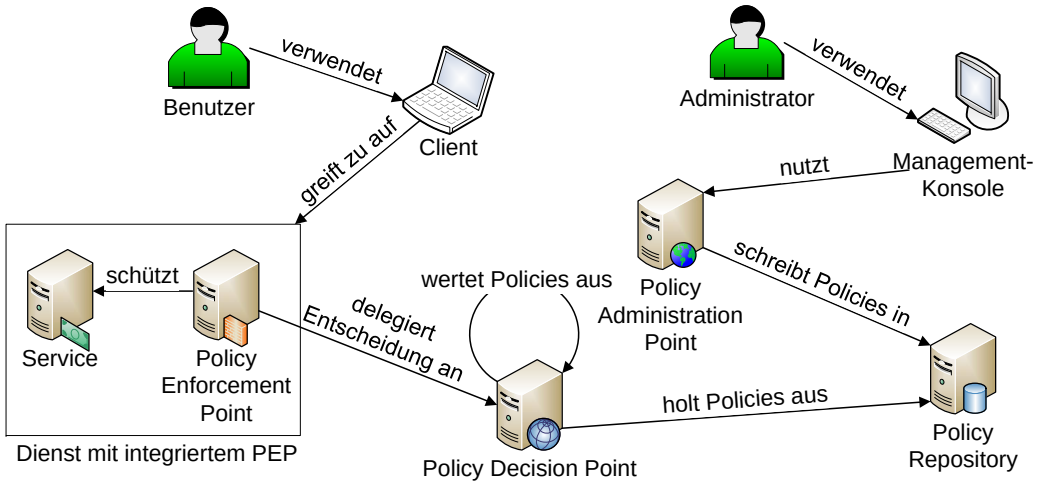


Abbildung 2.17.: Policy-basierte Zugriffskontrolle mit zentralem Repository und Decision Point

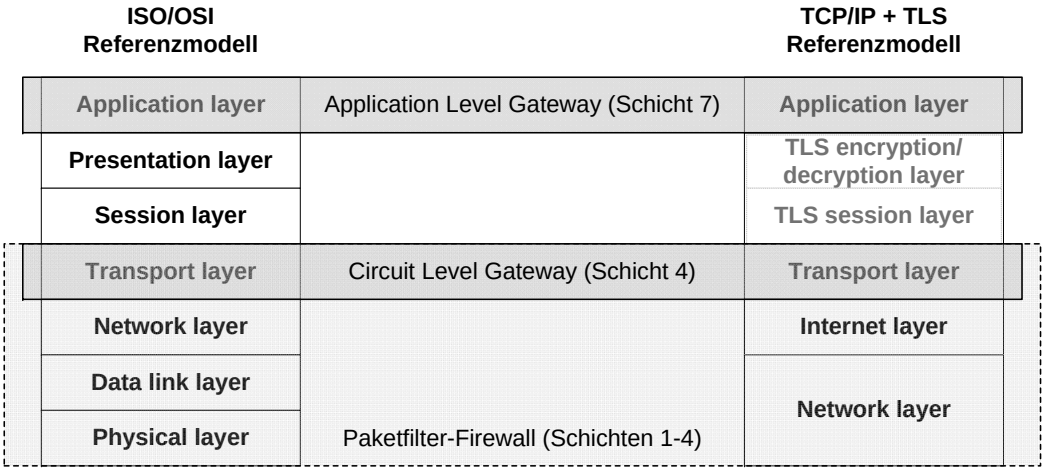


Abbildung 2.18.: Einordnung der drei klassischen Firewallarten in die Schichtenmodelle

genau die hierzu autorisierten Personen die netzbasierten Dienste verwenden können. Dabei sind reine Paketfilter-Firewalls, die einzelne Pakete auf Basis von Headerinformationen wie Absende- und Zieladresse verwerfen, von Firewalls zu unterscheiden, die weitere Informationen wie die Benutzeridentität heranziehen oder eine Inhaltsanalyse und -modifikation (engl. *content filtering*) vornehmen können. Diese werden in Abhängigkeit von der Schicht des ISO/OSI-Referenzmodells, auf der sie arbeiten, wie in Abbildung 2.18 dargestellt als Circuit Level Gateways (Schicht 4) bzw. Application Level Gateway (Schicht 7) bezeichnet. Mit der stark zunehmenden Nutzung von Web Services, die zur Nachrichtenübertragung HTTP bzw. HTTPS und damit nur wenige verschiedene TCP/IP-Ports nutzen, verlieren reine Paketfilter-Firewalls strategisch an Bedeutung: Sie können die verschiedenen Dienste ohne Inhaltsanalyse nicht unterscheiden, werden für ein grundlegendes Schutzniveau allerdings noch weiterhin benötigt.

- **Protokollierung**: Die Protokollierung ist per se kein präventiver oder detektierender Sicherheitsmechanismus, sondern dient dem in Abschnitt 2.1.1.2 definierten Ziel der Revisionsfähigkeit. Die Protokollierung sollte systemübergreifend einheitlich sein, muss gegen nachträgliche Modifikationen geschützt werden und bildet häufig die Basis für die Erzeugung von Sicherheitsereignissen (vgl. Abschnitt 2.2.2).
- **Isolation**: Isolationsmaßnahmen verfolgen das Ziel, Benutzer, Komponenten und Systeme so stark voneinander abzuschotten, dass sie sich gegenseitig nicht negativ beeinflussen können. Dadurch sollen einige Angriffe ganz verhindert oder zumindest die Auswirkungen erfolgreicher Angriffe vermindert werden. Die Schaffung so genannter Sandkästen (engl. *sandbox*) als Ausführungsumgebung für nicht vertrauenswürdigen Code war lange Zeit die Aufgabe von Betriebssystemen. Mit der zunehmenden Hardwareunterstützung für Rechnervirtualisierung wird verstärkt auf dedizierte virtuelle Maschinen als Isolationsmechanismus gesetzt.
- **Intrusion detection**: Die Erkennung von Angriffen erfolgt zwar primär durch von den potentiellen Angriffszielen hierfür vorgesehene Mechanismen, wird jedoch häufig durch **Intrusion Detection Systeme** (IDS) unterstützt. Ein so genanntes *hostbasiertes* IDS kann bei unerwünschten Änderungen an Daten und Systemen einen Alarm auslösen, wohingegen ein *netzbasiertes* IDS potentielle Angriffe durch Beobachten der gesamten Kommunikation im Netz erkennen kann; hierzu muss das netzbasierte IDS wie in Abbildung 2.19 dargestellt mit einer geeigneten Netzkomponente verbunden werden, um den gesamten Netzverkehr in seinem Aufgabenbereich abgreifen zu können. Zur Analyse werden entweder als Signaturen bezeichnete Muster bekannter Angriffe als Referenz herangezogen oder Heuristiken angewandt, die nach einer Trainingsphase abnormes Nutzungs- bzw. Kommunikationsverhalten identifizieren sollen.

  Das Erkennen eines Angriffs kann mit der automatisierten Durchführung von Gegenmaßnahmen, beispielsweise der Rekonfiguration eines Firewalls zum Aussperren des identifizierten Angreifers, verknüpft werden. Obwohl es sich dabei um eine reaktive und nicht um eine präventive Maßnahme handelt, hat sich marketingbedingt der Begriff **Intrusion Prevention System** (IPS) durchgesetzt. Um zu verhindern, dass erst reagiert wird, nachdem bereits mindestens ein Angriff stattgefunden hat, werden IPS zunehmend mit Application Level Gateways kombiniert, d. h. die Nachricht wird an das Zielsystem erst zugestellt, nachdem sie auf potentiell schädliche Inhalte untersucht wurde.

  Als Frühwarnsysteme und für über den reinen Schutz hinausgehende Analysen können so genannte **Honeypots** eingesetzt werden. Dabei handelt es sich um Systeme, die bewusst Angriffe auf sich ziehen sollen, beispielsweise indem Software mit bekannten Schwachstellen darauf installiert wird oder indem die dort gespeicherten Daten durch Verweise auf anderen Systemen besonders interessant gemacht werden. Angriffsversuche und das weitere Vorgehen der Angreifer nach erfolgreichen Einbrüchen werden aufgezeichnet und genau analysiert, um daraus Rückschlüsse auf den Angreifer, neue Angriffsarten und vom Angreifer möglicherweise entdeckte Verwundbarkeiten anderer Systeme zu ziehen. Beim Betrieb von Honeypots ist einerseits darauf zu achten, dass die Angreifer möglichst lange nicht erkennen, dass es sich um ein präpariertes System handelt. Andererseits sollte vermieden werden, dass der Honeypot als Ausgangsbasis für Angriffe auf andere, insbesondere externe Systeme verwendet wird.
- **Proaktive Sicherheitstests**: Über ein regelmäßiges bis hin zum kontinuierlichen Über-

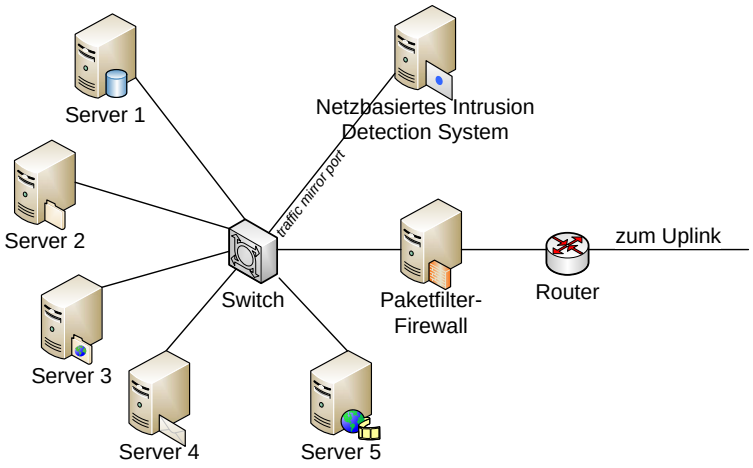


Abbildung 2.19.: Positionierung eines netzbasierten Intrusion Detection Systems

prüfen kann analysiert werden, ob die Ist-Sicherheitskonfiguration noch mit der Soll-Konfiguration übereinstimmt und ob in der lokalen Umgebung den Testwerkzeugen bekannte Sicherheitslücken vorliegen.

Als Hilfsmittel können beispielsweise Portscanner, dedizierte Vulnerability Scanner und Passwortcracker eingesetzt werden. Dabei ist jedoch zu beachten, dass die Verfügbarkeit und der Einsatz solcher Werkzeuge je nach Einsatzort gesetzlich eingeschränkt sein können. In Deutschland regelt beispielsweise der im Sommer 2007 eingeführte §202c StGB, dass die Vorbereitung einer Straftat durch Herstellung, Beschaffung, Verkauf, Überlassung, Verbreitung oder Zugänglichmachen von geeigneten Computerprogrammen mit Geld- oder Freiheitsstrafe belegt wird. Da von der Bereitstellung entsprechender Werkzeuge nicht nur sicherheitsbewusste Administratoren, sondern auch böswilligen Angreifer profitieren können, kann diese als illegal angesehen werden.

Bei der Durchführung entsprechender Tests muss ferner verhindert werden, dass diese fälschlicherweise als tatsächliche Angriffe interpretiert werden, z. B. indem die Systeme, von denen die Tests ausgehen, in eine Ausnahmeliste aufgenommen werden. Im Umkehrschluss stellen genau diese Systeme jedoch besonders attraktive Angriffsziele dar, die entsprechend geschützt werden müssen.

Um Konsequenzen aus dem Ausfall oder der Unwirksamkeit einzelner Sicherheitsmechanismen vorzubeugen, sollten diese in der Regel nicht für sich alleine, sondern in Kombination mit anderen eingesetzt werden. Da die Implementierung und der Betrieb der Sicherheitsmechanismen mit Kosten verbunden sind, muss abgewogen werden, welcher Aufwand in den individuellen Schutz der potentiellen Angriffsziele investiert werden sollte.

2.5. Begriffsdefinition Security-Framework

Die in den obenstehenden Abschnitten eingeführten Begriffe und Konzepte bilden die Basis für die nun vorgestellte Definition des Begriffs Security-Framework, die im Rahmen dieser

Arbeit entwickelt wurde. Sie ist für die Spezifikation der Managementaspekte von Security-Frameworks in den weiteren Kapiteln essentiell, insbesondere da die in Kapitel 4 vorgestellten Security-Frameworks – mit sehr wenigen, aber unvollständigen Ausnahmen – den Framework-Begriff weder selbst definieren noch auf eine andere Definition Bezug nehmen.

Definition 14 (Security-Framework)

*Als **Security-Framework** werden ein Konzept sowie seine methodisch unterstützte, szenariengetrieben adaptierte organisatorische und technische Umsetzung im Rahmen eines kontinuierlichen Verbesserungsprozesses bezeichnet; das Konzept*

- *bezieht sich dabei auf Mengen von zu schützenden Assets, ausgewählten Zielen der IT-Sicherheit und des IT-Sicherheitsmanagements, betrachteten Schwachstellen und berücksichtigten Angriffen, und*
- *spezifiziert die zum Erreichen der Ziele und zum Betrieb essentiellen sowie optionalen organisatorischen wie auch technischen Maßnahmen und Sicherheitsmechanismen.*

Aufgrund des in der Praxis dualen Begriffsgebrauchs werden als Security-Framework somit sowohl das meist allgemeingültige Konzept als auch seine szenarienspezifische Instanz bezeichnet. Dies ist unter Zugrundelegung eines Lebenszyklus kein Widerspruch, erzwingt jedoch die Angabe der betrachteten Phase in diesem Zyklus zur Präzisierung.

Konzeptionell ist ein Security-Framework nach dieser Definition eine Abstraktionsschicht, in der als schützenswert eingestufte Assets und ausgewählte Sicherheitsmaßnahmen zusammen betrachtet werden. Die Vollständigkeit und Korrektheit der Lösung kann zudem nur geprüft werden, wenn bekannt ist, welche Schwachstellen und potentielle Angriffe unter welchen technischen und organisatorischen Zielsetzungen berücksichtigt wurden. Informell kann ein Security-Framework somit als bausteinbasierte Musterlösung angesehen werden, die ihren Anwendern für einem Problemraum, der durch die betrachteten Assets und deren Schwachstellen abgesteckt wird, die Konzeption eigener Sicherheitslösungen abnehmen bzw. den dazu notwendigen Aufwand deutlich reduzieren kann. Folglich wird dadurch insbesondere die für die praktische Umsetzung hochgradig relevante Skalierbarkeit gegenüber einer Einzelbetrachtung aller Assets, Schwachstellen, Angriffe und Schutzmaßnahmen verbessert.

Prinzipiell könnte ein Security-Framework durchaus für genau ein Szenario entworfen werden; es würde sich dann jedoch nicht von herkömmlichen szenarienspezifischen Sicherheitskonzepten unterscheiden. In dieser Arbeit werden deshalb primär solche Security-Frameworks betrachtet, die von ihrem Abstraktionsgrad und Anspruch her allgemeiner konzipiert sind und auf in vorgegebenen Grenzen beliebige Szenarien, die vergleichbare Assets beinhalten, übertragen werden sollen. Offensichtlich sollte das Konzept diese Form der Anpassung vorsehen und unterstützen.

Die konkrete Umsetzung eines Security-Frameworks ist klar von den vorgesehenen bzw. szenarienspezifisch ausgewählten Sicherheitsmaßnahmen abhängig; allgemeingültig kann also nicht festgelegt werden, ob es sich z. B. um eine softwarebasierte Lösung oder die Einführung eines neuen Prozesses handelt. Durch die per Definition erzwungene Einbettung in einen kontinuierlichen Verbesserungsprozess wird jedoch sichergestellt, dass Maßnahmen nicht nur einmalig implementiert bzw. als statisch angesehen werden, sondern dass sowohl das Konzept als auch

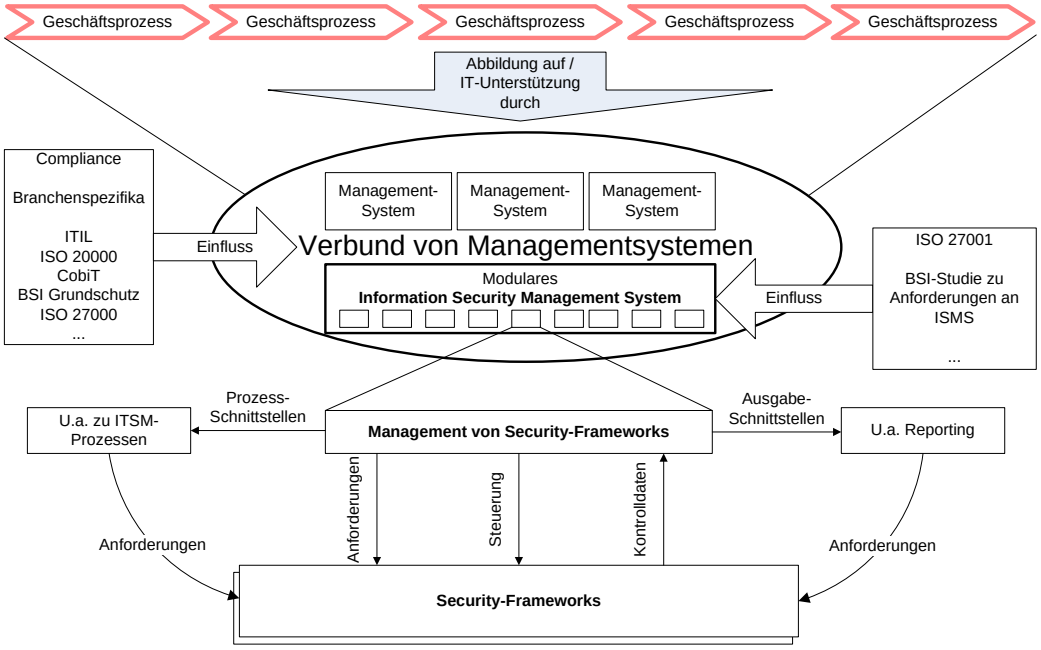


Abbildung 2.20.: Management von Security-Frameworks als Teil des Information Security Management Systems

seine szenarienspezifische Umsetzung regelmäßig analysiert und überarbeitet werden. Dies dient dazu, neu entdeckte Verwundbarkeiten, neuartige Angriffe und verbesserte Sicherheitsmechanismen genauso wie sich verändernde Zielsetzungen dynamisch zu berücksichtigen.

2.6. Einordnung von Security-Frameworks in Information Security Management Systeme

Ihrer Definition entsprechend und durch die in Kapitel 4 vorgestellten Beispiele bestätigt können Security-Frameworks einerseits als relativ techniklastig eingestuft werden, da sie sich beispielsweise mit einzelnen Angriffen und Sicherheitsmechanismen auseinandersetzen. Andererseits fassen sie mehrere zueinander gehörende Aspekte aus ihrem jeweiligen Anwendungsgebiet zusammen und bilden damit eine Abstraktionsschicht, durch die die Einzelaspekte zu einem bestimmten Grad verschattet werden können. In diesem Abschnitt wird zunächst das Konzept der Sicherheitsarchitekturen skizziert, die durch so genannte **Information Security Management Systeme** (ISMS) umgesetzt werden, um anschließend Security-Frameworks darin einordnen zu können.

Wie in Abbildung 2.20 dargestellt ist, besteht die top-down orientierte Grundannahme darin, dass ausgewählte oder alle Geschäftsprozesse geeignet IT-unterstützt werden müssen. Hierzu wird ein Verbund verschiedener Managementsysteme eingesetzt, da es im Allgemeinen kein einzelnes, monolithisches Managementsystem gibt, das alle Prozesse ausreichend abdeckt. Die Möglichkeiten zur Auswahl und Zusammenstellung der Managementsysteme sind so vielfältig

wie die Organisationen selbst und unterliegen u. a. branchen- und landesspezifischen gesetzlichen Auflagen, so dass hier nicht näher darauf eingegangen wird. Die Unterstützung des IT-Sicherheitsmanagements, dessen Ziele in Abschnitt 2.1.2 beschrieben wurden, erfolgt dabei durch das ISMS als eines der beteiligten Managementsysteme. Dieses ist nicht als reines Softwaresystem zu verstehen; vielmehr umfasst der Begriff sämtliche Aktivitäten und Ressourcen rund um das prozessorientierte IT-Sicherheitsmanagement und die dazu benötigte IT-Unterstützung.

Da ein ISMS so komplex zu realisieren ist, wie die damit verfolgten Ziele zu erreichen sind, wurden die Anforderungen, die an ein ISMS zu stellen sind, durch ISO 27001 standardisiert und in Deutschland vom BSI analysiert (siehe [I27001] und [BSISMS]). Die BSI-Studie dokumentiert die 25 Kernelemente eines ISMS, zu denen auch die Aspekte *Steuerung und Kontrolle* sowie *Informationsfluss* gehören (vgl. [BSISMS, S. 15–18]). Für die Durchführung der Kontrolle ist es erforderlich, dass die vom Managementsystem abgedeckten Prozesse und Systeme überwacht und quantitativ wie auch qualitativ beurteilt werden können. Die dazu erforderlichen Informationen sind ebenso wie die anzuwendenden Kontrollverfahren und Prüfkriterien zu ermitteln und zu dokumentieren. Ausgewählte Kontrollwerte und die Ergebnisse ihrer Auswertung sind zudem für den Informationsfluss relevant, der einerseits dafür sorgen soll, dass alle Mitarbeiter mit den für sie notwendigen Daten versorgt werden, andererseits aber auch die Aggregation und Aufbereitung in Form von **Berichten an das Management** (engl. *reporting*) umfasst. Offensichtlich müssen auch Security-Frameworks diesen Regelungen unterliegen und entsprechende Daten bereitstellen, die vom eingesetzten Managementwerkzeug aufbereitet und über Schnittstellen propagiert werden können.

Die technischen Kontrollprozesse sehen einen Datenfluss vor, bei dem ausgewählte Daten der kontrollierten Systeme ausgelesen und aufbereitet werden; an den Systemen ergeben sich dadurch keine Veränderungen, die nicht mit der Gewinnung der Kontrolldaten in Verbindung stehen. Im Unterschied dazu soll es durch Steuermechanismen ermöglicht werden, auch von außen – meist von zentralen Managementwerkzeugen aus – Einfluss auf die Systeme zu nehmen, um beispielsweise ihre Konfiguration hinsichtlich ausgewählter Sicherheitsparameter modifizieren zu können. Beim Einsatz von Security-Frameworks müssen diese also auch entsprechende Steuerschnittstellen aufweisen und können somit als so genanntes Managed Object (MO) angesehen werden (vgl. [HAN99, S. 115]). Folglich benötigt das Security-Framework Mechanismen, um die Änderungen in seinen Einzelkomponenten umsetzen zu können.

Zu einer gesamtheitlichen Sicherheitsarchitektur, zu dessen Kern das ISMS gehört, werden im technischen Sinn alle Komponenten gezählt, die systemübergreifend und wiederverwendbar dazu beitragen, die organisationsweiten Sicherheitsstandards, -richtlinien und -entscheidungen operativ umzusetzen (vgl. [Pet07]). Ohne den Einsatz von Security-Frameworks ist dabei eine Vielzahl von Einzelsystemen zu betrachten, die zu komplexen und aufgrund ihres Umfangs nur schwer zu beherrschenden Sicherheitsarchitekturen führt. Durch die von Security-Frameworks gebotene Abstraktion ergeben sich, wie in Abbildung 2.21 dargestellt ist, potentiell deutliche Vereinfachungen. Sie ist jedoch mit der Schwierigkeit verbunden, dass wiederverwendbare Komponenten nicht mehr unmittelbar ersichtlich sind. Bei der Kombination mit anderen Security-Frameworks und Systemen muss dieser Aspekt besonders berücksichtigt werden.

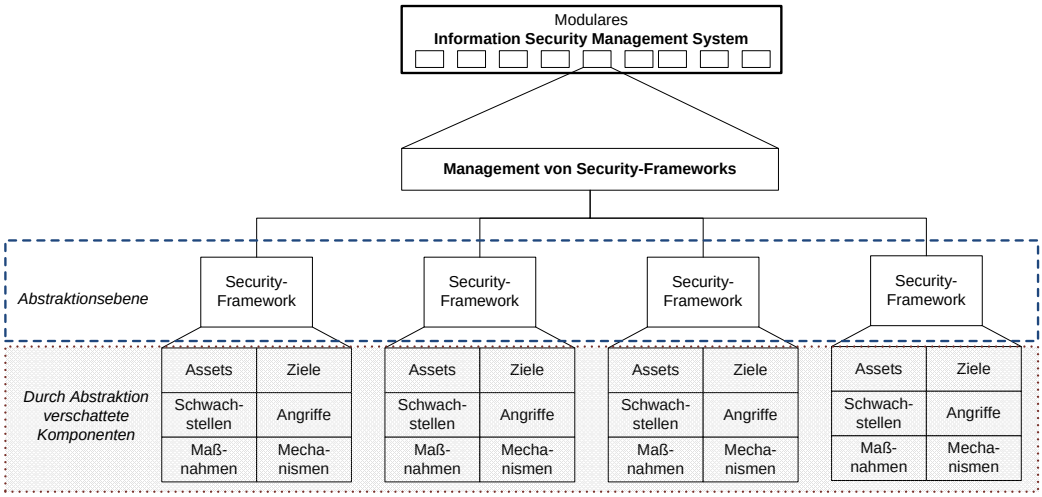


Abbildung 2.21.: Security-Frameworks als Abstraktionsebene aus Managementsicht

2.7. Zusammenfassung

In diesem Kapitel wurden anfangs die Ziele der IT-Sicherheit und des IT-Sicherheitsmanagements, zu deren Erreichen Security-Frameworks offensichtlich beitragen sollen, zusammengestellt. Nach einer Vorstellung relevanter Personengruppen und Rollen wurde gezeigt, wie Schwachstellen, Verwundbarkeiten, Angriffe und Sicherheitsmechanismen zusammenhängen und in Managementprozessen wie dem Risikomanagement zu berücksichtigen sind. Darauf aufbauend wurde eine Einordnung in die Prozesse und Methoden des IT Service Management und des Security Engineering vorgenommen, wobei auch die Auswirkungen auf das Software Engineering, insbesondere unter dem Blickwinkel des Security Requirements Engineering, untersucht wurden.

Zur Konkretisierung wurden danach die von aktuellen Security-Frameworks am häufigsten abgedeckten Angriffe und eingesetzten Sicherheitsmechanismen ermittelt, kategorisiert und knapp vorgestellt. Durch die Zusammenführung der vorgestellten Begriffe konnte anschließend der Begriff Security-Framework präziser und umfassender als in der bisherigen Literatur definiert und diskutiert werden. Schließlich wurde die Eingliederung von Security-Frameworks in das Konzept der Sicherheitsarchitekturen vorgenommen.

Insgesamt wurden mit diesem Kapitel die Grundlagen dafür geschaffen, die Verwendung von Security-Frameworks in konkreten Szenarien präzise zu diskutieren, ihre Komponenten und Eigenschaften hinsichtlich der Sicherheitszielsetzungen zu analysieren und sie im Hinblick sowohl auf die Architektur als auch die Managementprozesse in ihr Umfeld einzubetten.

Kapitel 3.

Managementanforderungen an Security-Frameworks

Inhalt dieses Kapitels

Die Beurteilung von Security-Frameworks und ihrer Managementeigenschaften setzt die genaue Kenntnis der zu erreichenden **Ziele** und der zu erfüllenden **Anforderungen** voraus. Da die relevanten Ziele und Anforderungen vom jeweiligen Einsatzszenario abhängen, steht die in diesem Kapitel erarbeitete Anforderungsanalyse vor der Herausforderung, dass in nahezu jedem Szenario, in dem Informationstechnologie eingesetzt wird, auch die IT-Sicherheit berücksichtigt werden muss und somit prinzipiell Security-Frameworks zum Einsatz kommen könnten. Die daraus resultierende thematische Breite macht eine für alle möglichen Szenarien nachweislich vollständige Anforderungsanalyse offensichtlich praktisch unmöglich.

Für dieses Kapitel wurde deshalb die Vorgehensweise gewählt, zunächst die Anforderungen für mehrere **ausgewählte Szenarien** strukturiert abzuleiten. Eine besondere Rolle spielen somit die Auswahl und die Modellierung der betrachteten, für den Einsatz von Security-Frameworks möglichst repräsentativen Szenarien. In Abschnitt 3.1 wird deshalb zunächst vorgestellt, wie potentielle Szenarien grundlegend charakterisiert werden können, wie die jeweiligen Szenarienbeschreibungen und -analysen strukturiert sind und in welche **Kategorien** die Anforderungen an Security-Frameworks grundlegend eingeteilt werden können.

Im Anschluss daran werden die ausgewählten Szenarien in den Abschnitten 3.2 bis 3.5 diskutiert. Neben der Ableitung von Anforderungen an Security-Frameworks werden dabei zwei weitere Ziele verfolgt: Zum einen wird konkret veranschaulicht, welchen **technischen und organisatorischen Mehrwert** der Einsatz von Security-Frameworks im jeweiligen Szenario mit sich bringt. Zum anderen wird verdeutlicht, dass im Hinblick auf einen praktischen Einsatz auch diverse Anforderungen an die Szenarien selbst und die dort eingesetzten Managementprozesse existieren und adäquat berücksichtigt werden müssen. Dieser grundlegende Aspekt der partiellen wechselseitigen Beeinflussung wird in den Kapiteln 5 und 6 wieder aufgegriffen.

Die aus den Szenarien abgeleiteten Anforderungen werden in Abschnitt 3.6 ergänzt, indem weitere relevante Aspekte vorgestellt und entsprechende **Vorgaben aus Standardspezifikationen** strukturiert zusammengetragen werden. Die damit bereits erzielte Breite der nach wie vor keinen Anspruch auf Vollständigkeit für alle möglichen Szenarien erhebenden Anforderungsliste motiviert neben der Katalogisierung auch eine grundlegende **Gewichtung der Anforderungen**, die in Abschnitt 3.7 präsentiert und begründet wird.

In Abschnitt 3.8 wird daraufhin vorgestellt, wie der resultierende **Anforderungskatalog** zur Beurteilung und Auswahl von Security-Frameworks für eigene Szenarien angepasst werden kann. Zu den wesentlichen Prozessschritten gehören dabei die szenarienspezifische Vervollständigung der Anforderungsmenge und die optionale Repriorisierung ihrer Bestandteile.

Die zum Einsatz kommenden Anforderungskategorien und deren Inhalte werden schließlich in Abschnitt 3.9 zu einer **Checkliste** zusammengestellt, die sich an die Autoren von Security-Frameworks wendet und die nunmehr bekannten Anforderungen aus einer anderen Perspek-

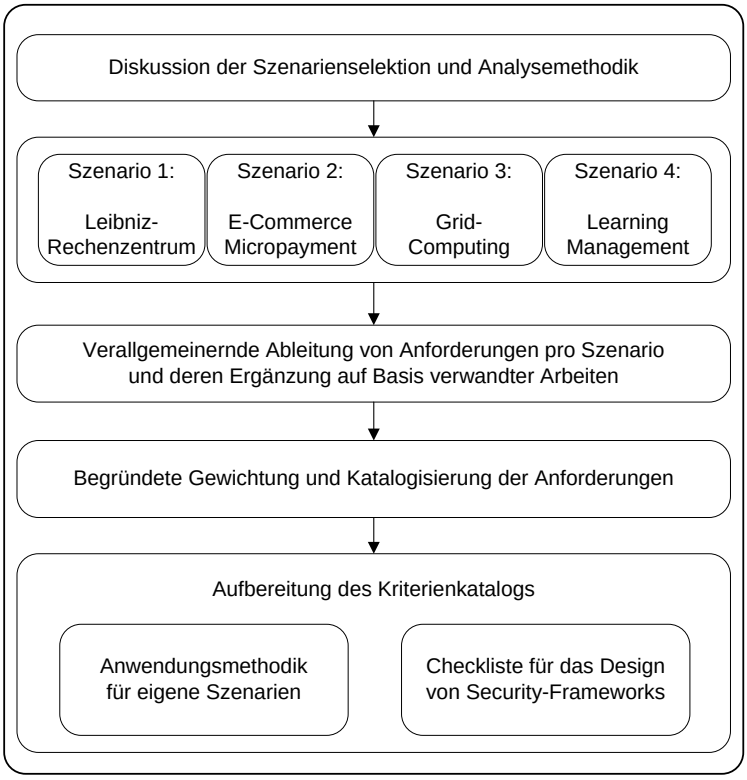


Abbildung 3.1.: Vorgehensmodell in diesem Kapitel

tive betrachtet. Sie bietet einen kompakten Überblick über die inhaltlichen wie auch darstellungsspezifischen Aspekte, die beim Design neuer bzw. bei der Überarbeitung existierender Security-Frameworks zu berücksichtigen sind.

Das Kapitel, dessen Struktur in Abbildung 3.1 dargestellt ist, endet mit einer Zusammenfassung in Abschnitt 3.10.

3.1. Vorgehensweise bei der Szenarienselektion und Anforderungsermittlung

Da die ausgewählten Szenarien die Basis für die Spezifikation eines umfangreichen Anforderungskatalogs und einer Vorgehensweise in beliebigen anderen Szenarien bilden, werden ihre Auswahl und das Vorgehen bei ihrer Analyse im Folgenden näher erläutert. Zunächst wird vorgestellt, wie Szenarien, in denen Security-Frameworks eingesetzt werden, grob charakterisiert werden können. Jedes der ab Abschnitt 3.2 beschriebenen Szenarien wird entsprechend dieser Charakterisierung eingeordnet; über alle Szenarien summiert werden im Rahmen der Anforderungsanalyse viele Ausprägungen angesprochen, wobei durch die überschaubare Anzahl betrachteter Szenarien jedoch bei Weitem nicht alle beliebigen Kombinationen dieser Szenarienmerkmale abgedeckt werden können.

Im Anschluss daran wird in Abschnitt 3.1.2 die Methodik skizziert, nach der jede Szenarienanalyse aufgebaut ist. Sie wird nicht nur einheitlich für die in diesem Kapitel vorgestellten Szenarien angewandt, sondern kann auch als systematische Basis für die Analyse eigener bzw. weiterer Szenarien eingesetzt werden, wie es der konkrete praktische Einsatz des erarbeiteten Kriterienkatalogs erfordert. In Abschnitt 3.1.3 werden schließlich die im Rahmen dieser Arbeit definierten Kategorien von Anforderungen vorgestellt. Ihre Vorwegnahme ermöglicht die kompakte und strukturierte Darstellung der Anforderungen pro Szenario, für die auf die alternative Darstellung des Zwischenschritts – der Ableitung von Kategorien aus allen gesammelten Anforderungen – verzichtet wurde.

3.1.1. Rudimentäre Charakterisierung von Szenarien

Um das Ziel zu erreichen, eine in ihrer Breite möglichst repräsentative Szenarienauswahl zu treffen, muss bekannt sein, in welchen Punkten sich die in Frage kommenden Szenarien ähneln bzw. charakteristisch unterscheiden. Analog zum Überblick über Angriffe und Sicherheitsmechanismen in Abschnitt 2.4 stellt sich dabei jedoch wiederum das Problem, dass bislang kein vollständiger Ansatz zur Definition einer Taxonomie für IT-Szenarien – ggf. mit Einschränkung bzw. Spezialisierung auf IT-Sicherheit, deren Management oder entsprechende Frameworks – existiert.

Für die Charakterisierung der Szenarien wurde deshalb der pragmatische Ansatz gewählt, einerseits die von den in Kapitel 4 vorgestellten Security-Frameworks adressierten Einsatzszenarien miteinander zu vergleichen und andererseits die Umgebungen, auf die sich die in Abschnitt 2.1.2 diskutierten Standards und Best Practices zum Sicherheitsmanagement beziehen, zu berücksichtigen.

Die Charakterisierung der Szenarien akkumuliert somit Eigenschaften, die zumindest von einigen gegenwärtig bereits existierenden Security-Frameworks bzw. der aktuellen Sicherheitsmanagementpraxis berücksichtigt werden. Während dieser Umstand für die Einordnung ebendieser Security-Frameworks in Kapitel 4 durchaus hilfreich ist, ergibt sich die konzeptionelle Einschränkung, dass entsprechend dieser Kriterien zusammengestellte Szenarien potentiell nicht alle Anforderungen und Schwerpunkte ableiten lassen, die sich bei der Szenarienwahl auf Basis einer alternativen **Charakterisierungsmethodik** ergeben würden. Diesem Defizit wird dadurch Rechnung getragen, dass die szenarienspezifische Ergänzung des Anforderungskatalogs gefordert und der in jedem Einzelfall damit verbundene Aufwand bewusst in Kauf genommen werden. Neben der davon unabhängig erforderlichen, szenarienspezifischen Überprüfung und gegebenenfalls partiellen Neugewichtung der Anforderungen trägt dieses Vorgehen zur vollständigen Anforderungsanalyse im jeweiligen Einsatzbereich bei.

Für die in dieser Arbeit betrachteten Szenarien werden die folgenden **Unterscheidungsmerkmale** herangezogen:

- *Anzahl zu berücksichtigender Organisationen:* Die Anzahl der an einem Szenario beteiligten Organisationen ist ein offensichtlich grundlegendes Differenzierungsmerkmal, das die Gesamtkomplexität stark beeinflusst. In dieser Arbeit werden drei Ausprägungen unterschieden:
  - 0 – am Szenario ist keine Organisation beteiligt, sondern z. B. eine einzelne Privatperson.

  - 1 – jede am Szenario beteiligte Organisation ist im Hinblick auf Security-Frameworks unabhängig und isoliert voneinander zu betrachten.
  - *n* – am Szenario sind mehrere, miteinander kooperierende Organisationen beteiligt, auf welche die Komponenten von Security-Frameworks verteilt werden können oder müssen.

- *Organisation der Sicherheitsverantwortung:* In komplexen Szenarien, in denen beispielsweise zahlreiche Dienste betrieben oder mehrere Security-Frameworks eingesetzt werden, kann die Verantwortung für die IT-Sicherheit organisatorisch wie folgt angesiedelt werden:
  - *dezentral* – die Sicherheitsverantwortung ist gleichberechtigt dezentral organisiert, d. h. statt einer Hierarchie liegt eine Heterarchie vor.
  - *hierarchisch* – die Verantwortung für die IT-Sicherheit unterliegt einer Verteilung gemäß einer der Gesamtorganisationsstruktur ähnlichen Hierarchie.
  - *zentral* – die gesamte Verantwortung wird zentral getragen, wodurch beispielsweise auch Informationen zur Sicherheitslage vorrangig zentral aggregiert werden.
- *Anzahl eingesetzter Security-Frameworks:* Die Anzahl eingesetzter Security-Frameworks wirkt sich unmittelbar auf die Managementkomplexität des Szenarios aus. Der nachfolgend genannte Schwellenwert wurde unter der Maßgabe gewählt, die Szenarien einfach und übersichtlich halten zu können:
  - 1 – im Szenario wird genau ein Security-Framework eingesetzt.
  - *2 bis 3* – im Szenario kommen zwei oder drei Security-Frameworks zum Einsatz.
  - *mehr als 3* – im Szenario müssen mehr als drei Security-Frameworks parallel berücksichtigt werden.
- *Verarbeitung personenbezogener Daten:* Ausschließlich anonym nutzbare Dienste und Infrastrukturen weisen in der Regel ein anderes Anforderungsprofil, z. B. bezüglich Vertraulichkeit und Datenschutz, auf als solche, in denen Benutzerdaten beispielsweise zur Personalisierung oder Rechnungsstellung herangezogen werden. Unterschieden wird folglich:
  - *keine* – das Szenario kommt vollständig ohne personenbezogene Daten aus.
  - *Kontaktdaten* – im Szenario werden personenbezogene Daten verarbeitet, deren Umfang und Sensibilität das heute bei Kunden-Anbieter-Beziehungen übliche Maß nicht überschreitet.
  - *Profildaten* – im Szenario werden zusätzlich zu den Kontaktdaten weitere, besonders schützenswerte personenbezogene Daten erfasst und verarbeitet; Beispiele sind Kranken- oder Personalakten.
- *Ausprägung von Kontrollen und externen Vorgaben:* Szenarien unterscheiden sich im Hinblick auf die Überprüfung der Sicherheitslage bezüglich externer Vorgaben – beispielsweise des Datenschutzgesetzes – wie folgt:
  - *keine* – die Einhaltung entsprechender Vorgaben wird nicht kontrolliert.

  - *intern* – es finden interne Revisionen statt, bei denen die Einhaltung externer Vorgaben überprüft wird.
  - *extern* – von externen Dritten durchgeführte Audits beurteilen, ob externe Vorgaben ausreichend umgesetzt werden. In vielen Fällen kommt hinzu, dass das Szenario branchenspezifische, extern durchgeführte Audits erfordert, z. B. für in USA börsennotierte Unternehmen oder solche, die im Banken- oder Gesundheitswesen tätig sind.

- *Szenariendynamik:* Die Häufigkeit und der Umfang von Änderungen am betrachteten Szenario entscheiden darüber mit, wie flexibel Sicherheitslösungen und ihr Management gestaltet werden müssen und mit welchem Aufwand nachhaltige Lösungen umgesetzt werden können. Vereinfachend werden folgende Ausprägungen unterschieden:
  - *statisch* – die im Szenario relevanten technischen Komponenten und ihre Umgebung bleiben im Betrachtungszeitraum unverändert.
  - *evolutionär* – die für das Szenario relevanten technischen Komponenten und seine Umgebung entwickeln sich regulär weiter.
  - *dynamisch* – sowohl die im Szenario relevanten technischen Komponenten als auch ihre Umgebung ändern sich im Betrachtungszeitraum stark bzw. häufig.
- *Benutzerkreis:* Die Szenarienkomplexität wird nicht nur von der Anzahl involvierter Organisationen und technischen Komponenten beeinflusst, sondern hängt auch vom Kreis der Anwender ab:
  - *geschlossen, klein* – das Szenario betrachtet eine kleine Menge von Benutzern.
  - *geschlossen, groß* – im Szenario wird eine große, aber klar definierte Menge von Benutzern berücksichtigt.
  - *offen* – der Benutzerkreis wird nicht a priori begrenzt und kann somit beliebig groß werden.
- *Angreifermodelle:* Die sicherheitsspezifische Größe und Komplexität des Szenarios ist abhängig von der Anzahl und den Ausprägungen der zu berücksichtigenden Angreifermodelle. Dabei werden folgende Fälle unterschieden:
  - *wenige* – im Szenario müssen nur wenige, klar definierte Angreifermodelle berücksichtigt werden.
  - *viele, bekannte* – im Szenario müssen viele Angreifermodelle berücksichtigt werden, die aufgrund von Vorarbeiten in vergleichbaren Szenarien jedoch als allgemein bekannt vorausgesetzt werden können, beispielsweise bei E-Commerce-Webanwendungen.
  - *viele, spezifische* – es muss eine Vielzahl von Angreifermodellen berücksichtigt werden, von denen mindestens ein Teil szenarienspezifisch ist oder dafür spezifisch ausgearbeitet werden muss.
- *Infrastruktur und Prozessorientierung:* Die Ausgangslage im Szenario unterscheidet sich, je nachdem wie weit das Sicherheitsmanagement bereits formalisiert wurde. Die Beurteilung könnte beispielsweise anhand des Capability Maturity Models (CMM, [Hump87]) erfolgen, wird für die nachfolgenden Ausführungen jedoch stark vereinfacht zu:

Charakteristikum	**Ausprägung**		
Anzahl Organisationen	0	1	n
Sicherheitsverantwortung	dezentral	hierarchisch	zentral
Anzahl Security-Frameworks	1	2-3	mehr als 3
Personenbezogene Daten	keine	Kontaktdaten	Profildaten
Kontrollen / ext. Vorgaben	keine	intern	extern
Dynamik	statisch	evolutionär	dynamisch
Benutzerkreis	klein, geschl.	groß, geschl.	offen
Angreifermodelle	wenige	viele, bekannte	viele, spezifische
Infrastruktur/Prozesse	Neuaufbau	ohne Prozesse	Prozessorientiert
Interne Abhängigkeiten	vernachlässigbar	gegeben	stark

Abbildung 3.2.: Schablone für die Szenariencharakterisierung

  - *Neuaufbau* – die Infrastruktur und die Sicherheitsmanagementprozesse werden erst zusammen mit dem Security-Framework eingeführt.
  - *ohne Prozesse* – die für das Szenario relevante IT-Infrastruktur ist bereits vorhanden, es wurden jedoch noch keine expliziten Sicherheitsmanagementprozesse definiert.
  - *Prozessorientierung* – die Einführung eines Security-Frameworks erfolgt für eine bereits vorhandene Infrastruktur und erfordert die Integration in ein instanziiertes Prozessrahmenwerk sowie gegebenenfalls dessen Anpassung.

- *Interne Abhängigkeiten:* Die Kohäsion der im Szenario betrachteten technischen Dienste ist ein ausschlaggebender Aspekt für die Integration von Security-Frameworks. Entsprechend wird unterschieden:
  - *vernachlässigbar* – die betrachteten Dienste können unabhängig voneinander betrachtet werden.
  - *gegeben* – zwischen den betrachteten Diensten sind zu berücksichtigende Abhängigkeiten vorhanden.
  - *stark* – die Verzahnung zwischen den betrachteten Diensten ist eng und darf nicht eingeschränkt werden.

Es ist zu berücksichtigen, dass die genannten Charakteristika nicht notwendigerweise unabhängig voneinander sind; beispielsweise sind die Größe des Benutzerkreises und die Anzahl relevanter Angreifermodelle in vielen Szenarien zueinander proportional.

Abbildung 3.2 zeigt eine mögliche **Visualisierung** dieser Ausprägungen in Form einer Schablone mit einem Charakterisierungsmerkmal pro Zeile und seiner diskreten Wertemenge als Spalten.

Neben einer breiten Abdeckung dieser Charakteristika wurde bei der Auswahl der Szenarien besonders darauf geachtet, mit dem Paralleleinsatz verschiedener Security-Frameworks in einem Szenario einerseits und deren gegenseitigem Zusammenspiel im Rahmen des Security-Framework-Lebenszyklus andererseits zwei erfolgsentscheidende Managementherausforderungen darzustellen. Szenarien, in denen lediglich ein einziges Security-Framework eingesetzt wird, dienen deshalb vorrangig der Verdeutlichung der Integrationsaspekte und der Skizzierung der Vorteile, die der Einsatz von Security-Frameworks mit sich bringt.

3.1.2. Struktur der Szenarienbeschreibungen und -analysen

Die ausgewählten Szenarien weisen zwar bewusst klare Unterschiede auf, um aus ihnen eine möglichst breite Basis an Anforderungen ableiten zu können; sie werden aber nach derselben, im folgenden beschriebenen Methodik aufbereitet und analysiert. Diese Vorgehensweise kann – gegebenenfalls an umgebungsspezifische Randbedingungen geeignet angepasst – auf eigene Szenarien angewandt werden, um den in diesem Kapitel erstellten Kriterienkatalog zu vervollständigen.

Zu Beginn der Beschreibung jedes Szenarios wird die jeweilige **Ist-Situation** präsentiert. Die Darstellung erfolgt dabei möglichst ohne Wertung und konzentriert sich auf – notwendigerweise subjektiv – **ausgewählte Kernaspekte**, um den Umfang zu begrenzen. In der Regel liegt der Ist-Zeitpunkt in einer Phase des Szenarios, in der Security-Frameworks noch nicht oder zumindest nicht flächendeckend im Einsatz sind.

Auf die neutrale Darstellung der Ist-Situation folgt eine **Defizitanalyse**, die Schwachstellen und im praktischen Ablauf störende Eigenschaften (engl. *pain points*) aufzeigt, ohne jedoch bereits konkrete Lösungsansätze dafür zu diskutieren.

Im Anschluss daran wird der für das Szenario durch den Einsatz von Security-Frameworks zu erwartende Mehrwert untersucht; somit werden für ausgewählte Bereiche **Soll-Zustände** vorgegeben, ohne die für die szenarienspezifischen Einsatzgebiete aktuell verfügbaren Security-Frameworks konkret zu berücksichtigen. Insgesamt liegt der Fokus dabei auf einer Diskussion der mit der Einführung von Security-Frameworks verbundenen Änderungen an den Servicearchitekturen und den Managementprozessen. Aufgrund der Komplexität der Szenarien und der vielfältigen Möglichkeiten, die sich durch den Einsatz von Security-Frameworks ergeben, beschränkt sich auch die Darstellung dieses Mehrwerts und der Veränderungen auf die wesentlichen Kernaspekte.

Aus den Unterschieden, die sich zwischen dem Soll- und dem Ist-Zustand ergeben, werden anschließend Anforderungen an Security-Frameworks und ihre Managementeigenschaften abgeleitet. Der Beschreibungsumfang sowie die Auswahl und Granularität der abgeleiteten Anforderungen und ihre vom konkreten Szenario abstrahierte Darstellung zielen darauf ab, in den folgenden Kapiteln mit möglichst allgemeingültigen und somit auf möglichst viele andere Szenarien übertragbaren Anforderungen arbeiten zu können.

Die Darstellung der Anforderungen erfolgt *szenarienübergreifend inkrementell*, um sie möglichst kompakt zu halten. Folglich werden bereits ermittelte Anforderungen in den nachfolgenden Szenarien nicht erneut detailliert diskutiert, sofern sich nicht neue Aspekte ergeben, die sich grundlegend auf den Inhalt oder die Relevanz der jeweiligen Anforderung auswirken.

Nach der Beschreibung der Szenarien werden schließlich die ermittelten Anforderungen abstrahiert und ihre gegenseitigen Abhängigkeiten analysiert. Nach einer begründeten Gewichtung jeder Anforderung kann die resultierende Anforderungsmenge somit geeignet aufbereitet werden, beispielsweise in Form des Anforderungskatalogs oder der Checkliste für Frameworkautoren. Diese Vorgehensweise ist in Abbildung 3.3 zusammengefasst.

3.1.3. Kategorisierung von Anforderungen an Security-Frameworks

Die Notwendigkeit der in diesem Kapitel vorgestellten Anforderungsanalyse ergibt sich unter anderem durch den in Kapitel 4 diskutierten Hauptkritikpunkt, dass die den einzelnen

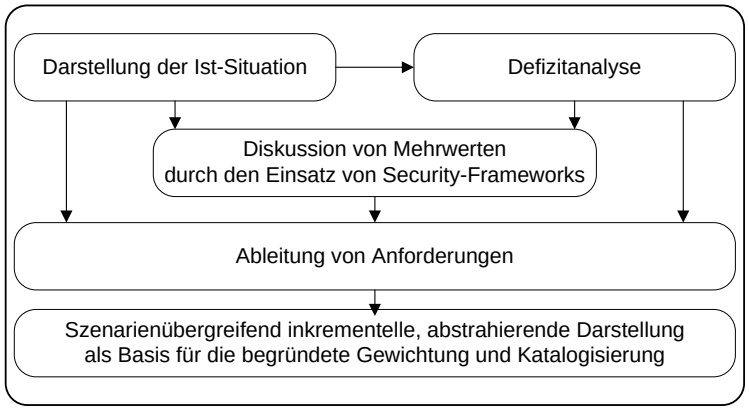


Abbildung 3.3.: Vorgehensweise bei der Analyse eines Szenarios

Security-Frameworks zugrundeliegenden Anforderungsanalysen – oder die Darstellung der entsprechenden Ergebnisse – in vielen Fällen unvollständig in Bezug auf den gesamten Lebenszyklus des Security-Frameworks und die Managementaspekte während seines praktischen Einsatzes sind. Als Folge davon können die Anforderungen an Security-Frameworks nicht als gemeinsamer Nenner oder Vereinigungsmenge aus der Literatur extrahiert bzw. daraus aggregiert werden.

Das von ihrer Anzahl unabhängige, breite Spektrum der in dieser Arbeit ermittelten Anforderungen motiviert die Definition von Kategorien, denen die Anforderungen zugeordnet werden können, um ihre Handhabbarkeit zu verbessern. In Anlehnung an die Definition des Begriffs Security-Framework in Abschnitt 2.5 werden in dieser Arbeit die folgenden Anforderungskategorien verwendet:

- *Funktionale Anforderungen:* Diese Kategorie deckt alle technischen und sicherheitsspezifischen Anforderungen ab, die durch den Einsatz eines Security-Frameworks erreicht werden sollen. Ihr sind insbesondere alle Anforderungen zuzuordnen, die im Bezug zu den in Abschnitt 2.1.1 diskutierten Zielen der IT-Sicherheit bzw. den in Abschnitt 2.4 skizzierten Angriffen und Sicherheitsmechanismen stehen. Dieser Anforderungskategorie ist das Kürzel [**SF-FUNK**] zugeordnet. Die in diese Kategorie fallenden Anforderungen werden in diesem Kapitel jedoch nur allgemein, d. h. nicht konkret und detailliert für die einzelnen Szenarien, betrachtet.
- *Integrations- und Betriebsanforderungen:* Anforderungen mit Bezug auf die szenariengetriebene Adaption von Security-Frameworks, die sowohl in einem initialen Customizing-Prozess zur Integration des Security-Frameworks in die bereits vorhandene Infrastruktur als auch im Rahmen des kontinuierlichen Verbesserungsprozesses erfolgen kann, werden dieser Kategorie mit dem Kürzel [**SF-INT**] zugeordnet.
- *Anforderungen an die Managementschnittstellen:* Sämtliche Anforderungen, die sich auf die Schnittstellen zur Steuerung und Kontrolle des Frameworks aus Managementprozessen und -architekturen beziehen und die aus Sicht der Führungsebene der jeweiligen Organisation relevant sind, gehören zu dieser Kategorie mit dem Kürzel [**SF-MGMT**].
- *Anforderungen an die Dokumentation:* Der Inhalt und die Form der Dokumentation

eines Security-Framework-Konzepts sind offensichtlich ausschlaggebend dafür, wie effizient es für beliebige Szenarien evaluiert und adaptiert werden kann. Entsprechende Anforderungen werden in dieser Kategorie mit dem Kürzel **[SF-DOKU]** zusammengetragen. Es ist anzumerken, dass die Dokumentation von szenarienspezifischen Security-Framework-Instanzen im Allgemeinen keinen Rückschluss auf diejenige des Konzepts zulässt; umgekehrt kann die Konzeptdokumentation jedoch eine Ausgangsbasis für die Instanzendokumentation darstellen.

Bereits an dieser Stelle sei darauf hingewiesen, dass viele existierende Security-Frameworks fast ausschließlich die Kategorie [SF-FUNK] berücksichtigen und für ihr jeweils konkretes Anwendungsgebiet geeignete Subkategorien einführen. Auf eine detaillierte Untergliederung wird in dieser Arbeit jedoch bewusst verzichtet, da die Feinheiten der technischen Eigenschaften der betrachteten Security-Frameworks zugunsten des gesamtheitlichen, framework-übergreifenden Managements in den Hintergrund treten.

3.2. Szenario 1: Ausgewählte Dienste des Leibniz-Rechenzentrums

Das Leibniz-Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften ist das gemeinsame Rechenzentrum der Münchner Hochschulen und eines der modernsten Zentren für technisch-wissenschaftliches Höchstleistungsrechnen in Europa. Aus dieser Rollenkombination und den IT-Bedürfnissen seiner mehr als 100.000 Benutzer resultiert ein Dienstspektrum auf dem aktuellen Stand der Technik, dessen Breite in dieser Szenarienanalyse nicht annähernd vollständig abgedeckt werden könnte. Entsprechend werden im Folgenden lediglich einige ausgewählte LRZ-Dienste näher betrachtet. Dabei darf jedoch nicht übersehen werden, dass gerade die Dienstvielfalt den Einsatz von Security-Frameworks besonders motiviert und die Anforderungen an deren Zusammenspiel veranschaulicht; auf diesen wichtigen Aspekt, auf dem die Auswahl und die relativ ausführliche Darstellung dieses Szenarios basieren, wird entsprechend vertiefend eingegangen.

3.2.1. Darstellung der Ist-Situation im LRZ-Szenario

In diesem Abschnitt wird die aktuelle Situation im Szenario geschildert. Nach einer Einordnung auf Basis der Charakteristika des Szenarios werden die betrachteten Dienste und die im Szenario bereits eingesetzten IT-Sicherheitsmaßnahmen dargestellt.

3.2.1.1. Szenariencharakteristika

Gemäß Abschnitt 3.1.1 kann dieses Szenario wie folgt charakterisiert werden: Es werden die Sicherheitsanforderungen genau *einer* Einrichtung – nämlich des LRZ – diskutiert; dies trifft auf die hier exemplarisch vorgestellten LRZ-Dienste zu, würde für das LRZ insgesamt jedoch zu kurz greifen. Eine mit anderen Organisationen gemeinsame Umsetzung von Security-Frameworks wird deshalb am Beispiel von Grid Computing Projekten (Szenario 3) in Abschnitt 3.4 analysiert.

Die Sicherheitsverantwortung ist am LRZ *hierarchisch* verteilt, weil jeder Dienstverantwortliche auch für die IT-Sicherheit in seinem Bereich zuständig ist und Sicherheitsvorfälle ent-

Charakteristikum	Ausprägung		
Anzahl Organisationen	0	1	n
Sicherheitsverantwortung	dezentral	hierarchisch	zentral
Anzahl Security-Frameworks	1	2-3	mehr als 3
Personenbezogene Daten	keine	Kontaktdaten	Profildaten
Kontrollen / ext. Vorgaben	keine	intern	extern
Dynamik	statisch	evolutionär	dynamisch
Benutzerkreis	klein, geschl.	groß, geschl.	offen
Angreifermodelle	wenige	viele, bekannte	viele, spezifische
Infrastruktur/Prozesse	Neuaufbau	ohne Prozesse	Prozessorientiert
Interne Abhängigkeiten	vernachlässigbar	gegeben	stark

Abbildung 3.4.: Charakterisierung von Szenario 1

sprechend der LRZ-Organisationsstruktur gegebenenfalls bis zur Leitungsebene eskaliert werden. Da aufgrund der Verschiedenartigkeit der Dienste bislang kein gesamtheitliches Security-Framework existiert, wird der Einsatz von *mehr als 3* Security-Frameworks erforderlich. Von seinen Benutzern liegen dem LRZ zumindest rudimentäre *Kontaktinformationen* vor, sodass im Szenario eine Berücksichtigung von Datenschutzaspekten zwingend erforderlich ist. Aufgrund seiner expliziten Service- und Prozessorientierung, die unter anderem in eine Zertifizierung nach ISO/IEC 20000 mündet, führt das LRZ *interne Kontrollen* durch.

Die Dynamik im beschriebenen Szenario ist als *evolutionär* anzusehen, da nicht nur der Nutzerkreis – wie im Hochschulumfeld typisch – einer sehr hohen Fluktuation unterliegt, sondern auch die Dienste und die zu ihrer Erbringung erforderlichen Komponenten stets dem aktuellen Bedarf angepasst werden. Der Nutzerkreis des LRZ ist prinzipiell *geschlossen, aber groß*; davon unabhängig können Dienste, die von den Kunden auf Basis von LRZ-Diensten realisiert werden, selbst wiederum auch offene Nutzerkreise haben. Entsprechend sind die LRZ-Dienste und -Systeme einer Vielzahl möglicher Angriffe ausgesetzt, wobei zwar *viele, aber bekannte Angreifermodelle* berücksichtigt werden müssen.

Bezüglich der Sicherheitsmanagementprozesse ist mit der Orientierung an ISO/IEC 20000 bereits ein entsprechendes Rahmenwerk zur *Prozessorientierung* gegeben, in das die Security-Frameworks eingebettet werden müssen. Die hier betrachteten Dienste haben interne, *nicht besonders starke Abhängigkeiten*. Diese Charakterisierung ist in Abbildung 3.4 zusammengefasst.

3.2.1.2. Im LRZ-Szenario betrachtete Dienste

Im Folgenden werden fünf Dienste diskutiert, die einerseits einen repräsentativen Querschnitt der Angebote der verschiedenen LRZ-Abteilungen darstellen und für die andererseits Security-Frameworks vorliegen. Es handelt sich dabei um:

1. *Webhosting*: Das LRZ bietet das Hosting von Webservern an, bei dem sich die Kunden weder um die Servermaschinen noch um die Konfiguration des Dienstes kümmern müssen, sondern sich auf die Inhalte ihrer Webpräsenzen konzentrieren können. Aktuell nutzen über 400 Einrichtungen – überwiegend in der Granularität von Lehrstühlen und Fakultäten – im Münchner Wissenschaftsnetz (MWN) dieses Angebot. Neben dem Einspielen statischer Webseiten ist es möglich, dynamische Inhalte mittels eigener

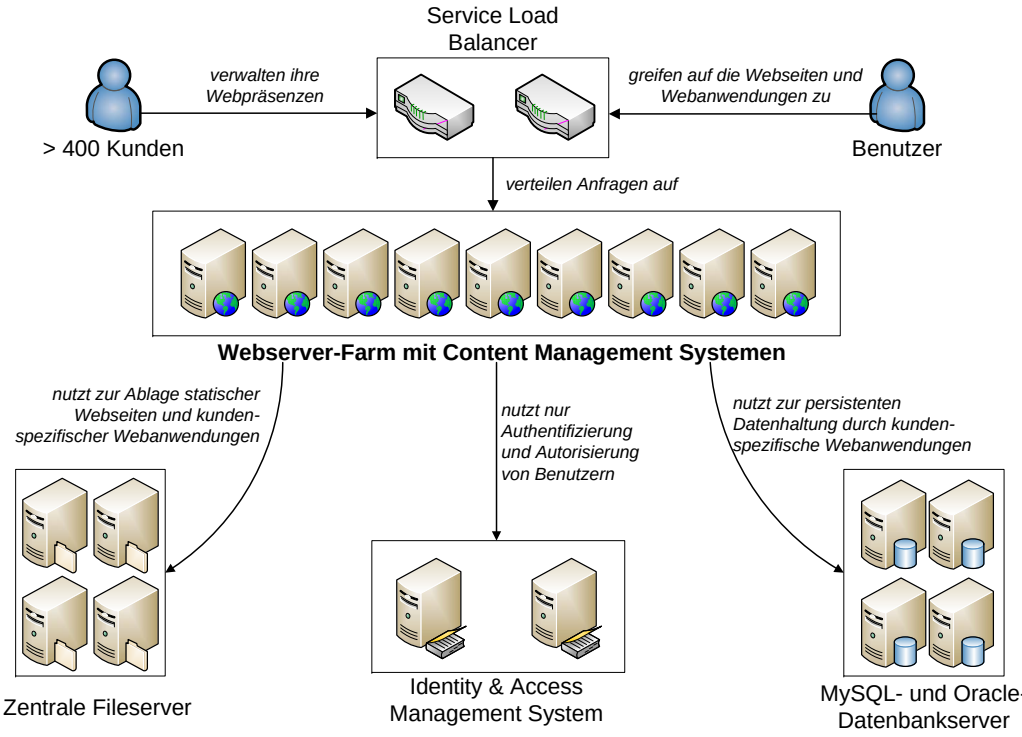


Abbildung 3.5.: Szenario 1: Webhosting am Leibniz-Rechenzentrum

Webanwendungen in Form von CGI- und PHP-Skripten in Kombination mit einem relationalen Datenbankmanagementsystem zur Datenhaltung zu erzeugen. Dabei stehen sowohl MySQL- als auch Oracle-Datenbanksysteme zur Auswahl, auf die optional auch mit einem von mehreren vorkonfigurierten Content Management Systemen (CMS) zugegriffen werden kann. Das in Abbildung 3.5 dargestellte Angebot ist mandantenfähig in dem Sinn, dass die von Kunden realisierten Webanwendungen ihre Benutzer unabhängig voneinander in Eigenregie verwalten können, wobei neben dem Aufbau eines eigenen Benutzerdatenbestands optional auch die Möglichkeit zur Nutzung der unten beschriebenen, bereits vorhandenen Identity Management Infrastruktur besteht. Bei allen involvierten Komponenten wird dabei auf Hochverfügbarkeit und Lastverteilung geachtet.

2. *E-Mail / Groupware*: Der elektronische Nachrichten- und Dokumentenaustausch hat sich im Hochschulumfeld längst zu einem der wichtigsten Kommunikationsprozesse entwickelt. Mit der Zunahme lehrstuhl- und fakultätsübergreifender Projekte spielen auch Groupwaredienste, z. B. elektronische Kalender zur gemeinsamen Terminplanung, eine immer wichtigere Rolle im Hochschulumfeld. Dabei müssen insbesondere Delegationskonzepte unterstützt werden, damit beispielsweise Terminplanungen durch Sekretariate und die grundlegende Konfiguration von E-Mail-Accounts durch dezentrale Administratoren erfolgen können. In diesem Umfeld bietet das LRZ eine E-Mail-Grundversorgung mit kundenspezifischen Internetdomänen an, die beispielsweise für alle Angehörigen (d. h. Mitarbeiter, Studenten und ausgewählte Gäste) der Ludwig-Maximilians-Universität (LMU, `@[campus.]lmu.de`) München und der Technischen

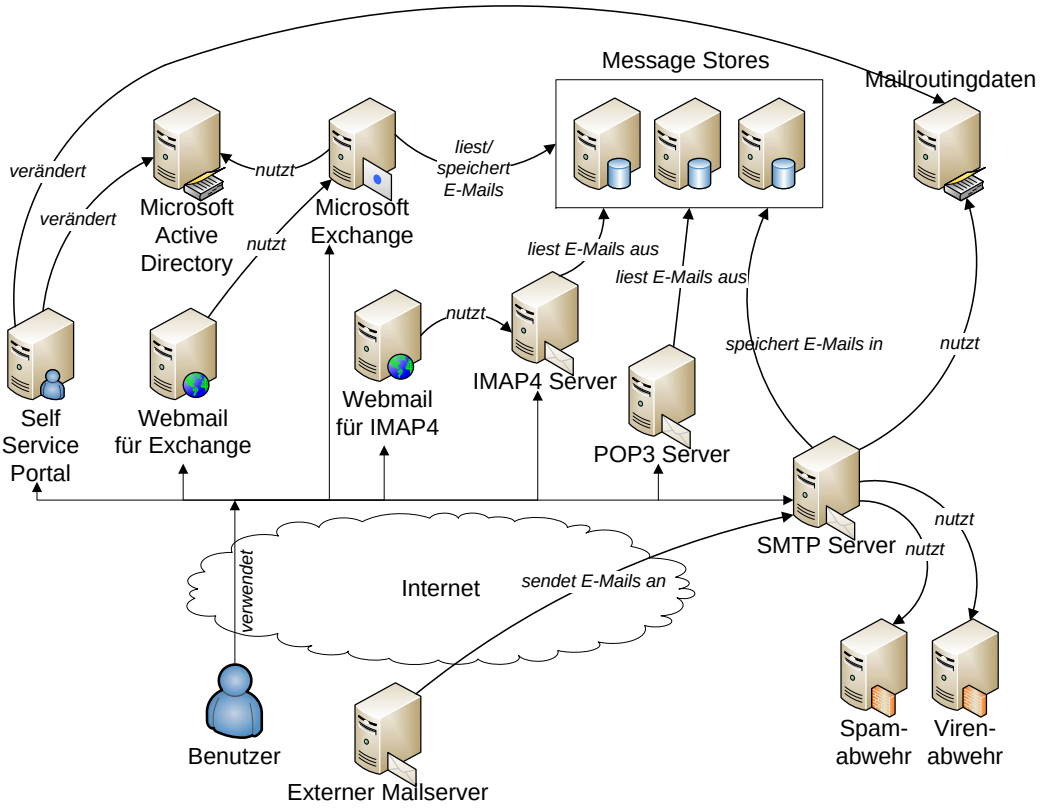


Abbildung 3.6.: Szenario 1: E-Mail- und Groupwaredienste am Leibniz-Rechenzentrum

Universität München (TUM, `@[my]tum.de`) genutzt wird. Zur Kommunikation mit E-Mail-Clients kommen die TCP/IP-basierten Protokolle POP3, IMAP4 und (E)SMTP zum Einsatz, die wie in Abbildung 3.6 dargestellt von entsprechenden Serverdiensten bereitgestellt werden. Als Groupwarelösung kommt Microsoft Exchange zum Einsatz; die Nutzung erfolgt über dedizierte Clientsoftware oder ein Webfrontend. Für die Anwender nicht direkt sichtbar muss ein enormer Arbeitsaufwand in die Abwehr E-Mail-spezifischer Gefahren investiert werden; beispielsweise kommen umfangreiche Spam-Zustellversuche praktisch Denial-of-Service-Angriffen gleich und virenverseuchte E-Mails haben nach wie vor ein hohes Potential zur Kompromittierung von Endsystemen. Durch die notwendige Kombination verschiedener Abwehrmechanismen ergibt sich eine durchaus heterogene Landschaft diverser Systeme, deren stabiles Zusammenspiel zum Teil über von Mitarbeitern programmierte Schnittstellenkomponenten sichergestellt wird. Die Konfiguration der E-Mail-spezifischen Eigenschaften von Benutzerkennungen, beispielsweise von E-Mail-Adressen und -Aliasen, Abwesenheitsnotizen und Weiterleitungen bzw. Mailverteilern erfolgt über das webbasierte LRZ Self Service Portal.

3. *WLAN- und VPN-Zugang*: Da die Nutzung privater mobiler Geräte (z. B. Notebooks, Netbooks und Smartphones) insbesondere durch Studenten auf dem Campus stark zugenommen hat und eine Vielzahl der Hochschulangehörigen die zentralen IT-Dienste auch vom eigenen Heimarbeitsplatz aus bzw. während Dienstreisen nutzen möchte, kommt dem flächendeckenden WLAN-Zugang auch dem Campus in Kombination mit dem Ein-

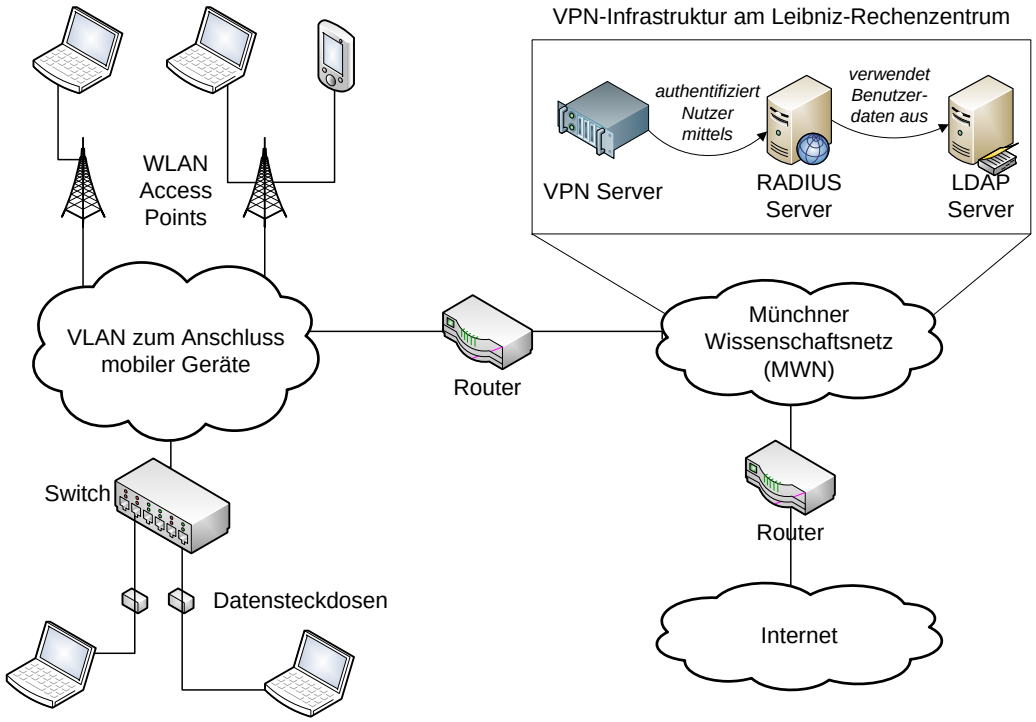


Abbildung 3.7.: Szenario 1: WLAN- und VPN-Zugang über das Leibniz-Rechenzentrum

satz von virtuellen privaten Netzen eine strategisch wichtige Bedeutung zu. Das LRZ betreibt deshalb inzwischen in den über 400 Gebäuden, über die sich die mehr als 60 Standorte der Münchner Hochschulen erstrecken, mehr als 1.000 WLAN Access Points und stellt VPN-Einwahlkapazitäten bereit, die für die parallele, performante Nutzung durch rund ein Fünftel aller potentielle Anwender ausreichen würde. Für beide hier zusammen betrachteten und in Abbildung 3.7 dargestellten Dienste wird bewusst in Kauf genommen, dass dezentral, eventuell unzureichend administrierte und somit potentiell kompromittierte Systeme angeschlossen werden, die ohne explizite Sicherheitsmaßnahmen ein deutliches Risiko für die anderen Systeme darstellen würden. Angesichts der Nutzerzahlen und beteiligten technischen Komponenten ist die Skalierbarkeit eine offensichtliche Anforderung sowohl hinsichtlich der von der Infrastruktur bereitgestellten Funktionalität als auch ihrer Sicherheitskonzepte.

4. *Elektronische Medien*: Zur Unterstützung effizienter Literaturrecherchen im Rahmen des wissenschaftlichen Arbeitens setzen Hochschulbibliotheken und akademische Verlage massiv auf elektronische Medien. Beispielsweise können inzwischen die meisten Konferenzbeiträge und Journalartikel in Form elektronischer Dokumente bezogen werden, wodurch der Aufwand für herkömmliche logistische Prozesse wie die Fernausleihe drastisch gesenkt werden kann. Im Unterschied zu den aktuellen *Open Access* Bewegungen sind viele Verlagsangebote nach wie vor an kostenpflichtige Lizenzangebote gebunden, sodass ein freies Zirkulieren der elektronischen Medien unerwünscht ist. Die primitive Beschränkung der Dienstnutzung auf Rechner, die in der Bibliothek bzw. auf dem Campus stationiert sind, hat sich inzwischen beispielsweise im Hinblick auf Telearbeit als zu

starr und bezüglich des Intellectual Property und Digital Rights Managements als relativ ineffizient herausgestellt. In enger Zusammenarbeit mit den Hochschulbibliotheken bietet das LRZ deshalb wie in Abbildung 3.8 dargestellt zwei alternative Zugangsverfahren an, die auch von außerhalb des Campusnetzes genutzt werden können, aber den Nutzerkreis auf autorisierte Personen einschränken:

- Zum einen steht über den LRZ DocWeb-Gateway ein proxybasierter Ansatz zur Verfügung. Dabei wendet sich der Benutzer per Browser an den Gateway, der wiederum die Kommunikation mit den verlagsseitigen Servern übernimmt. Aus Perspektive der Verlage erfolgt die Nutzung also durch einen Rechner auf dem Campus; aus Benutzersicht ist die Verwendung des Proxy nahezu transparent, da die Dienstnutzung nach dem erforderlichen Gateway-Login genauso abläuft wie vom Campus aus. Die Verantwortung dafür, nur autorisierten Benutzern Zugriff zu gewähren, wird bei diesem Verfahren offensichtlich an den Gateway-Betreiber delegiert.
- Zum anderen bietet eine zunehmende Zahl von Verlagen und Datenbankdiensten die Möglichkeit zur Nutzung über die Authentifizierungs- und Autorisierungsinfrastruktur des Deutschen Forschungsnetzes (DFN-AAI) an. Diese beruht auf der durch Federated Identity Management (FIM) geschaffenen technischen Möglichkeit, dass Dienstleister den Loginvorgang zur als Identity Provider bezeichneten Heimateinrichtung des jeweiligen Benutzers auslagern und von dieser auch Informationen zum Autorisierungsstatus des Benutzers abrufen können. Die archaische und inhärent nur beschränkt wirksame IP-adressbasierte Autorisierung kann somit durch personalisierte Webanwendungen ersetzt werden, ohne dass der Dienstleister dazu einen eigenen umfassenden Benutzerdatenbestand aufbauen müsste. Im Unterschied zum zuvor genannten Gateway-Ansatz muss der jeweilige Dienstleister diesen Mechanismus jedoch explizit unterstützen.

Beide Zugangsvarianten sind zur Authentifizierung der Benutzer und zur Überprüfung des jeweiligen Berechtigungsstatus an das unten beschriebene Identity Management System angebunden. Ferner arbeiten beide Verfahren webbasiert, setzen clientseitig also nur einen Browser voraus, werden allerdings organisatorisch und technisch unabhängig von dem oben skizzierten LRZ-Webhosting-Angebot betrieben.

5. *High Performance Computing (HPC)*: Mit seinem Höchstleistungsrechner, den Linux-Clustern und den Visualisierungsplattformen stellt das LRZ Rechenkapazitäten auf unterschiedlichen Leistungsebenen zur Verfügung. Je nach Plattform variieren dabei die typischen Anwenderkreise und Zugangsmodalitäten. Rechenkapazität muss dabei wie in Abbildung 3.9 dargestellt grundsätzlich unter Angabe der wissenschaftlichen Ziele beantragt werden. Über die Genehmigung entscheidet beispielsweise im Fall des Bundeshöchstleistungsrechners ein Gutachtergremium; die einem Projekt von ihm zugewiesenen Kapazitäten werden von LRZ-Administratoren ins lokale Identity Management System eingetragen und über Automatismen auf die HPC-Systeme übernommen.

   Aus der Perspektive der IT-Sicherheit stechen drei zusammenhängende Merkmale von HPC-Infrastrukturen hervor: Clustersysteme und Hochleistungsrechner bestehen aus einer Vielzahl von Einzelknoten, sodass Sicherheitsprobleme häufig auf vielen oder allen Knoten gleichzeitig auftreten. Die damit verbundenen Risiken werden dadurch verstärkt, dass Anwender beliebigen eigenen Code – auch solchen, der eventuelle Verwundbarkeiten

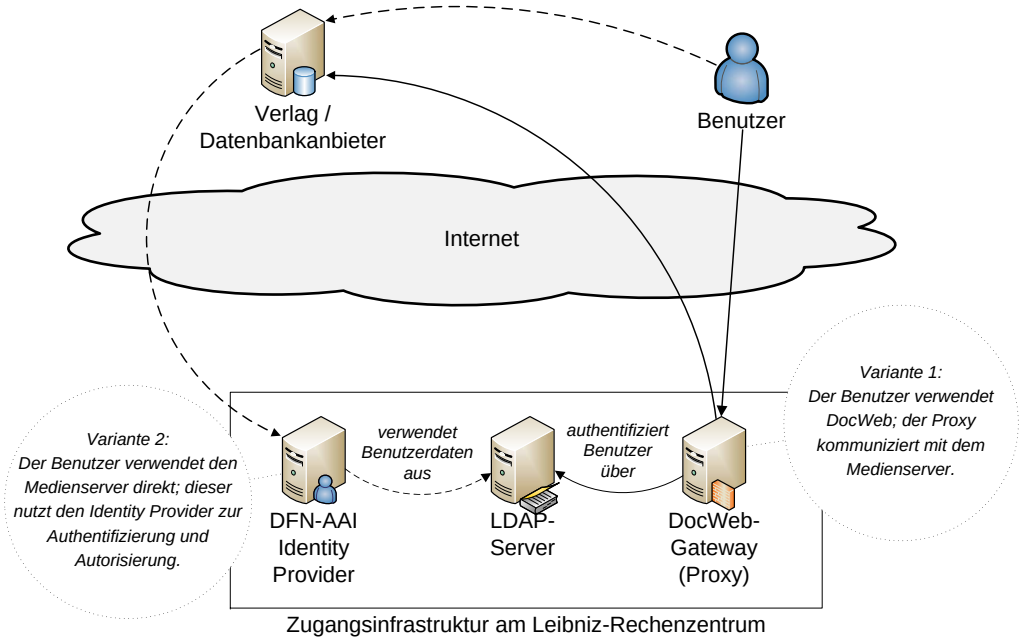


Abbildung 3.8.: Szenario 1: Zugang zu elektronischen Medien über das Leibniz-Rechenzentrum

ausbeutet – auf den Maschinen ausführen können. Schließlich können Sicherheitslücken oftmals nicht sofort nach ihrem Bekanntwerden geschlossen werden, da die betroffenen Systemprogramme und -bibliotheken auch von regulären Programmen und wissenschaftlichen Anwendungen verwendet werden, deren Kompatibilität und Verfügbarkeit nicht gefährdet werden darf.

Offensichtlich liegen diesen Diensten andere zugrunde, über die beispielsweise die notwendige hochverfügbare Netzinfrastruktur bereitgestellt wird. Eine vollständige Beschreibung würde den Rahmen sprengen und keine signifikanten zusätzlichen Anforderungen beisteuern. Diese bewusste Vereinfachung ist jedoch allgemein nicht auf die vollständige Analyse eigener Szenarien zu übertragen (vgl. Abschnitt 3.8).

3.2.1.3. Im LRZ-Szenario bisher eingesetzte Sicherheitsmaßnahmen

Das LRZ setzt bereits eine Fülle von technischen und organisatorischen Sicherheitsmaßnahmen um, von denen nachfolgend einige ohne Anspruch auf Vollständigkeit vorgestellt werden, um die Ansatzpunkte für den Einsatz von Security-Frameworks aufzuzeigen.

Auf **technischer Seite** kommen dabei zunächst auf Netzseite Segmentierungskonzepte zum Einsatz, über die verschiedene Sicherheitszonen gebildet werden. Auf Basis von Paketfilter-Firewalls, die Bestandteil der im MWN betreuten Netzkomponenten sind, werden beispielsweise öffentliche Server, interne Server, Mitarbeiterrechner, Studenten-Rechnerpools, Test- sowie Laborumgebungen und WLAN-nutzende Endgeräte in verschiedene, voneinander zunächst abgeschottete Bereiche eingeteilt. Verbindungen zwischen diesen Zonen, die beispiels-

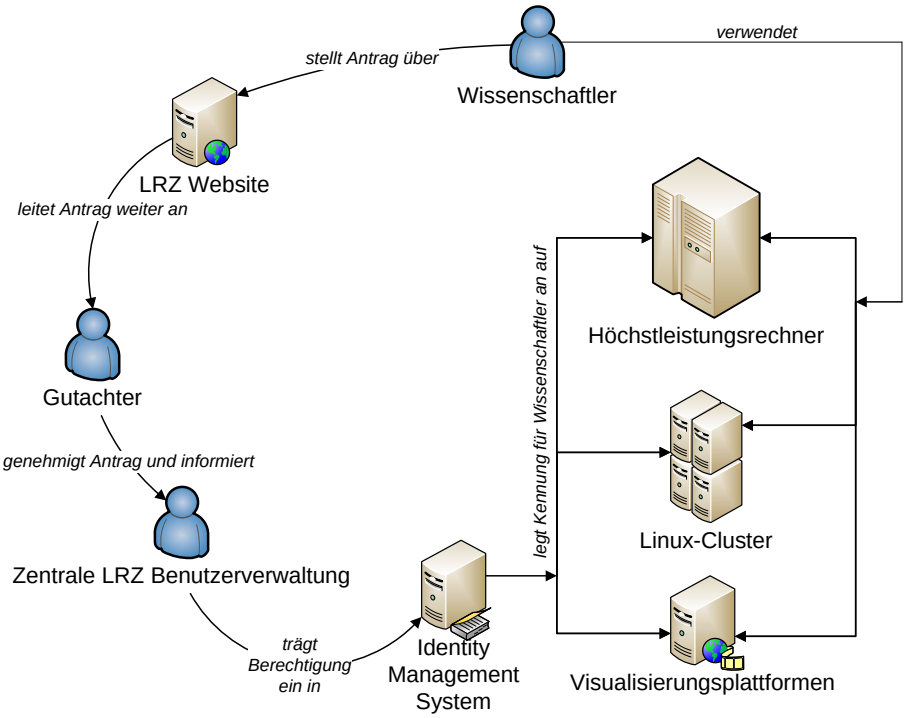


Abbildung 3.9.: Szenario 1: High Performance Computing am Leibniz-Rechenzentrum

weise für die reguläre Dienstnutzung erforderlich sind, werden anschließend bei Vorliegen einer hinreichenden Begründung der Notwendigkeit jeweils explizit ermöglicht.

Die Isolation von Einzelsystemen oder ganzen Netzbereichen fungiert dabei auch als fachlicher Eskalationsmechanismus. Beispielsweise wird der Netzverkehr per VPN eingewählter, potentiell z. B. vireninfizierter Endgeräte mit Verfahren, die beispielsweise auch bei Intrusion Detection Systemen eingesetzt werden, automatisch auf Auffälligkeiten untersucht; beim Überschreiten von Grenzwerten wird das Gerät in einem Quarantänenetz isoliert, bis das zugrunde liegende Problem beseitigt wurde oder zumindest die beobachteten Symptome einige Zeit lang nicht mehr auftreten. Systeme, deren legitimes Verhalten als auffällig eingestuft wird, können in eine Ausnahmeliste aufgenommen werden (Whitelist-Ansatz).

Alle Dienste und Servermaschinen werden darüber hinaus von einem Monitoringsystem erfasst und überwacht. Bei Auffälligkeiten, z. B. bei sich auf einmal änderndem Verhalten bezüglich der CPU- oder Speichernutzung, können Administratoren automatisch per E-Mail benachrichtigt werden. Die Integrität der eingesetzten Systeme und verarbeiteten Daten wird unter anderem durch Antivirus-Software geprüft, die beispielsweise auch alle eingehenden E-Mails auf Viren überprüft und allen regionalen LRZ-Benutzern als kostenloser Download für ihre dienstlichen und privaten Rechner angeboten wird.

Die Verwaltung von Benutzern und deren Zugangsberechtigungen zu den angebotenen Diensten wird wie in Abbildung 3.10 dargestellt über ein zentrales Identity Management System realisiert. Um die große Anzahl von Benutzern effizient handhaben zu können, werden die Daten möglichst weitgehend automatisch aus den zentralen Beständen der angeschlossenen Hochschulen, die z. B. aus Studenten- und Mitarbeiterverwaltungssystemen gespeist werden,

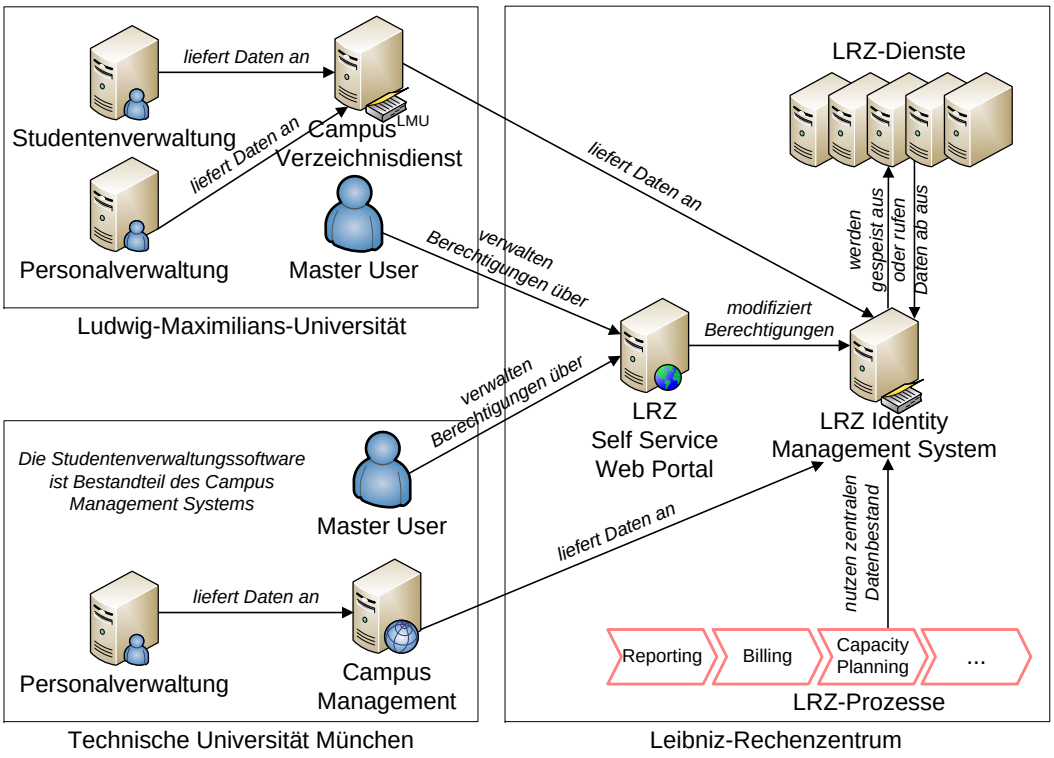


Abbildung 3.10.: Szenario 1: Identity Management am Leibniz-Rechenzentrum

übernommen. Die Erfassung von Benutzern, für die diese Möglichkeiten nicht zur Verfügung stehen, und die Vergabe der über die Grundversorgung hinausgehenden Berechtigungen erfolgt – sofern keine Antragsprüfung erforderlich ist bzw. diese für ein Projekt bereits positiv beschieden wurde – primär durch dezentrale Administratoren, die als Master User bezeichnet werden und für die Sicherstellung der benötigten Datenqualität verantwortlich sind. Die betrachteten Dienste können den somit vorhandenen zentralen Benutzerdatenbestand direkt verwenden bzw. werden aus diesem mit den für sie relevanten Daten versorgt. Der somit vorhandene zentrale Überblick über alle Benutzer und deren Berechtigungen dient auch als Basis für die Erzeugung von Statistiken und Kapazitätsplanungen sowie die Rechnungserstellung.

Darüber hinaus werden zahlreiche dienstspezifische Sicherheitsmechanismen eingesetzt; beispielsweise werden im E-Mail-Bereich diverse Spam-Abwehrmaßnahmen wie Greylisting oder DNS-Blacklisting eingesetzt und die HPC-Knoten regelmäßig auf von Angreifern installierte Rootkits untersucht.

Auch auf **organisatorischer Ebene** werden Sicherheitsaspekte umfassend berücksichtigt; die Basis dafür bilden die ITSM-Referenzprozesse nach ITIL und ISO/IEC 20000. Diesbezüglich wird zunächst der physische Zugang zu den Rechnern und Netzkomponenten eingeschränkt. Durch die umfassenden Fernwartungsmöglichkeiten, die den jeweiligen Dienstadministratoren auf ihren Maschinen zur Verfügung stehen, kann der Zutritt zu den Serverräumen auf den kleinen Kreis derjenigen Personen beschränkt werden, die zur Wartung der Hardware bzw. der In- und Außerbetriebnahme von Komponenten und der damit verbundenen Verkabelungsarbeiten unbedingt vor Ort sein müssen. Unter den vereinfachenden Annahmen, dass

die eingesetzte Hardware weder vor ihrer Anlieferung noch von der kleinen mit ihr in Kontakt kommenden Personenmenge manipuliert wird und dass die physische Zugangskontrolle nicht unbemerkt umgangen werden kann, rücken damit software- und social-engineering-basierte Angriffe in den Vordergrund.

Um erfolgreiche Social-Engineering-Angriffe, bei denen beispielsweise die Hilfsbereitschaft privilegierter Anwender ausgenutzt wird, einzudämmen und das allgemeine Sicherheitsbewusstsein zu schärfen, werden regelmäßig Sicherheitskurse und -schulungen für verschiedene Zielgruppen – beispielsweise Benutzer oder Master User – angeboten. Die vom LRZ vorgegebenen Sicherheitsrichtlinien (Policies) sind zudem Bestandteil der Nutzungsrichtlinien, die von jedem Benutzer bei der Ausgabe seines Benutzerkennzeichens schriftlich anerkannt werden müssen.

LRZ-intern und im Zusammenspiel mit den Kunden sind die Zuständigkeiten und Verantwortlichkeiten für die verschiedenen Bereiche genau festgelegt; die Eskalation von Sicherheitsvorfällen erfolgt hierarchisch – gegebenenfalls bis zur Hausleitung, die bei Bedarf auch die Kommunikation mit externen Dritten, z. B. der Staatsanwaltschaft, übernimmt. Darüber hinaus sind die Aspekte Datenschutz und Datensicherheit sowohl beim Aufbau neuer Dienste und Systeme als auch im Betrieb fest verankert. Beispielsweise gehört die Datensicherung per Backup zum Standardumfang neu installierter Serversysteme und nachts sowie an den Wochenenden werden die Systeme von Operateuren betreut, die bei größeren Problemen und Sicherheitsvorfällen umgehend die entsprechenden Dienstadministratoren benachrichtigen können.

3.2.2. Herausforderungen und Ansatzpunkte zur Optimierung

Wie für fast jede komplexe Infrastruktur, die über mehrere Jahre hinweg gereift ist und unter verschiedenen Gesichtspunkten überarbeitet wurde, lassen sich auch für die oben dargestellte Ist-Situation im LRZ-Szenario mehrere sicherheitsspezifische Punkte erkennen, die noch Potential zur Verbesserung aufweisen. Sie werden in diesem Abschnitt knapp skizziert, um nachfolgend zu zeigen, welchen Beitrag Security-Frameworks leisten können.

Ein im Hinblick auf die Vollständigkeit der getroffenen Sicherheitsmaßnahmen wichtiger Aspekt ist, dass die Konzeption und Realisierung dienstspezifischer Sicherheitsmechanismen bislang ausschließlich den jeweiligen Dienstadministratoren überlassen bleiben. Während für die Netzsicherheit beispielsweise über die zentral verwalteten Firewalls und für die Serversicherheit über zentral koordinierte Updatemechanismen und Backupkonzepte ein über die Anwendungsbereiche hinweg einheitlich hohes Sicherheitsniveau erzielt wird, können keine vergleichbaren Aussagen über dienstspezifische Maßnahmen getroffen werden. In einigen Bereichen würden sich Defizite zwar schnell und einfach erkennbar zeigen, beispielsweise durch Benutzerbeschwerden, wenn im E-Mail-Bereich die Spam-Abwehrmaßnahmen unzureichend wären. In anderen Bereichen bleibt jedoch – zumindest von außerhalb des Dienstbetriebs, z. B. unter dem Schlagwort IT-Governance von der Leitungsebene aus betrachtet – unklar, ob tatsächlich keine Verwundbarkeiten existieren oder ob diese bisher nur nicht ausreichend auffällig ausgenutzt worden sind.

Die somit seitens der Dienstadministratoren erforderliche Einarbeitung in allgemeine und spezifische Sicherheitskonzepte folgt dabei bisher keinem explizit definierten didaktischen Konzept. Als Folge davon muss sich ein Administrator selbständig und tiefgehend mit den

verschiedenen Assets, Verwundbarkeiten, Angriffen und Sicherheitsmechanismen auseinandersetzen. Es bleibt ihm dabei selbst überlassen, thematische Schwerpunkte zu erkennen und Prioritäten zu setzen. Das Vorgehen für den Fall, dass für das Detailverständnis der Sicherheitsaspekte zu wenig Zeit bleibt oder nicht ausreichend geeignetes Lehrmaterial vorliegt, ist nicht explizit definiert. Auf dieser Ebene verbleibende Wissenslücken werden im Allgemeinen nicht entdeckt, da die Umsetzung der LRZ-Policies, z. B. in Form von Dienstkonfigurationsparametern, nur dann im Detail kontrolliert wird, wenn bei der Nutzung des Dienstes ein offensichtliches Fehlverhalten feststellbar ist.

Als Konsequenz daraus ergibt sich, dass viele Dienste zwar grundlegend nach anerkannten Architekturkonzepten aufgebaut worden sind, im Hinblick auf das Sicherheitsmanagement jedoch in eine Menge von Einzelkomponenten zerfallen, für die – abgesehen von der Kenntnis ihrer gegenseitigen Abhängigkeiten – kein gemeinsames Sicherheitskonzept vorliegt. Die dienstspezifische Umsetzung durch die jeweiligen Administratoren führt dazu, dass sich viele Personen unabhängig voneinander ähnliches Sicherheitswissen aneignen und bei der anschließenden Umsetzung eine Reihe von Sicherheitsmechanismen mehrfach redundant implementiert wird. Im Szenario trifft dies beispielsweise auf die drei Dienste Webhosting, E-Mail und elektronische Medien zu, in denen jeweils unabhängig voneinander Webanwendungen betrieben und gegen Angriffe und unautorisierte Nutzung abgesichert werden.

Schließlich ist dem Szenario zu attestieren, dass zwar eine Vielzahl von Präventions- und Detektionsmechanismen zum Einsatz kommt und die Reaktionsprozesse spezifiziert wurden, dass darüber hinaus jedoch keine proaktiven Sicherheitsmaßnahmen wie regelmäßige Penetration Tests durchgeführt werden. Schwierigkeiten stellen dabei wiederum die Zusammenstellung und Priorisierung der konkreten Ansatzpunkte dar, damit nicht nur Einzelkomponenten isoliert voneinander getestet, sondern auch Sicherheitslücken erkannt werden können, die sich erst aus Fehlern im Zusammenspiel mehrerer Komponenten ergeben.

3.2.3. Durch Security-Frameworks zu erwartender Mehrwert

Mit Ausnahme des Zugangs zu elektronischen Medien, der diesbezüglich z. B. verallgemeinert als Webanwendung betrachtet werden kann, existiert für jeden der oben skizzierten Dienste mindestens ein Security-Framework, dessen Einsatz im Szenario in Erwägung gezogen werden sollte. Nachfolgend wird geschildert, wie sich der Dienstbetrieb und das Sicherheitsmanagement von der bisherigen Situation unterscheiden, wenn eine frameworkbasierte Vorgehensweise gewählt wird, ohne dass bereits auf die Schritte zu einer konkreten Wahl zwischen den verfügbaren Alternativen eingegangen wird.

Aus Perspektive der Dienstadministratoren bieten Security-Frameworks den Vorteil, dass sie unter Berücksichtigung der üblicherweise am Dienst beteiligten Komponenten (Assets), der damit verbundenen Angriffspunkte und typischen Angriffe spezifiziert wurden und dafür eine anpassbare Auswahl geeigneter Sicherheitsmechanismen anbieten. Die Einarbeitung in die für den Dienst relevanten Sicherheitsthemen kann somit wesentlich gebündelter und gezielter erfolgen. Idealerweise würden begründete Designentscheidungen im Frameworkkonzept nicht nur das Verständnis der zugrundeliegenden Sicherheitsproblematiken, sondern auch die Beurteilung der vorgeschlagenen bzw. zur Auswahl gestellten Lösungsansätze ermöglichen. Der über die Frameworkanpassung hinausgehende konzeptionelle Aufwand für die Administratoren kann somit darauf reduziert werden, z. B. aufgrund ihrer Neuheit eventuell noch nicht

abgedeckte oder szenarienspezifische Sicherheitsaspekte zu ergänzen, deren Priorisierung – wiederum im Idealfall – analog zur im Frameworkkonzept bereits dargelegten Risikoanalyse durchgeführt werden kann. Die notwendige Anpassung und Instanziierung des Security-Frameworks erfolgt dabei von diesem methodisch geführt, sodass das beim Frameworkdesign eingebrachte Wissen zu einer weiteren Reduktion des szenarienspezifischen Aufwands beiträgt.

Die vom jeweiligen Security-Framework vorgegebene Strukturierung trägt auch zu einer Verbesserung der Übersichtlichkeit der dienstspezifischen Sicherheitseigenschaften bei. Dieser Vorteil ist für die dienstübergreifende, zentrale Unterstützung des operativen Sicherheitsmanagements, die im Szenario in das Monitoring der LRZ-Systeme integriert ist, ausschlaggebend: Sicherheitsspezifische Zusammenhänge und Abhängigkeiten zwischen den beteiligten Komponenten werden auf Basis des Frameworkkonzepts explizit erkennbar; die notwendige Dokumentation kann im Rahmen der Instanziierung direkt aus dem Frameworkkonzept abgeleitet, muss also nicht mehr wie bisher üblich durch eine Bottom-up-Vorgehensweise zusammengetragen werden.

Im Hinblick auf das dienstübergreifende Sicherheitsmanagement und die hierarchische Organisation der Sicherheitsverantwortung ergeben sich durch die Orientierung an Security-Frameworks mehrere Vorteile: Zunächst bildet der Einsatz anerkannter Security-Frameworks eine stärkere argumentative Basis als lokal erarbeitete Dienstkonzepte, die nur am Rande auf Sicherheitsaspekte eingehen. Wenn beispielsweise Zertifizierungsaudits durchgeführt werden oder dennoch eingetretene Sicherheitsvorfälle gerechtfertigt werden müssen, kann gezielter nachgewiesen werden, dass alle üblichen und mit angemessenem Aufwand vertretbaren Maßnahmen im jeweiligen Bereich umgesetzt worden sind. Die durch Security-Frameworks induzierte Gruppierung von Komponenten bildet darüber hinaus die Basis für die Strukturierung von Sicherheitsberichten; akute Sicherheitsvorfälle können somit gezielter nicht nur einzelnen Komponenten, sondern auch Diensten bzw. Dienstgruppen zugeordnet werden, wodurch ein mögliches Übergreifen auf benachbarte oder ähnliche Bereiche einfacher antizipiert werden kann. Durch ihre Anpassbarkeit ist zudem sichergestellt, dass Security-Frameworks für mehrere ähnliche Dienste – im Szenario die für verschiedene Dienste benötigten Webanwendungen – verwendet werden können, ohne dass die resultierenden Sicherheitsmechanismen redundant implementiert und betrieben werden müssen. Schließlich werden Planungs- und Änderungsprozesse dadurch systematisch unterstützt, dass beim Wegfall, Austausch oder Ausbau ausgewählter Komponenten, beispielsweise im E-Mail-Bereich der Umstieg auf ein anderes IMAP-Server-Produkt, die sicherheitsspezifischen Auswirkungen und die für ausgetauschte Komponenten durchzuführenden Sicherheitsmaßnahmen bekannt sind.

3.2.4. Ableitung und Diskussion von Anforderungen aus dem LRZ-Szenario

In diesem Abschnitt wird eine Grundmenge von Anforderungen an Security-Frameworks und ihre Managementeigenschaften aus dem LRZ-Szenario begründet abgeleitet. Die meisten der hier vorgestellten Anforderungen gelten auch für die nachfolgend diskutierten Szenarien; umgekehrt werden einige der auch für das LRZ-Szenario zutreffenden Anforderungen erst im Kontext der anderen Szenarien vorgestellt, weil sie dort noch deutlicher hervortreten. Da die Dienste im Szenario bereits in Betrieb sind und eine größere Zahl von Security-Frameworks eingeführt werden soll, liegt nahe, dass die nahtlose Integration von Security-Frameworks in bereits vorhandene Infrastrukturen und ihre Interoperabilität zu den Anforderungsschwerpunkten gehören.

Eine mit der Einführung von Security-Frameworks in bestehende Umgebungen offensichtlich verbundene Randbedingung ist, dass hinsichtlich der damit erreichbaren Sicherheitsfunktionalität keine Rückschritte gegenüber dem bisherigen Zustand in Kauf genommen werden müssen. Unter Bezugnahme auf die Definition von Security-Frameworks in Abschnitt 2.5 und die oben genannten Einzelaspekte, mit denen sich Dienstadministratoren bisher direkt auseinandersetzen mussten, ergeben sich daraus die folgenden vier grundlegenden **funktionalen Anforderungen**:

- Die von einem Security-Framework geschützten Assets müssen definiert sein und sich mit den im konkreten Szenario vorhandenen Komponenten hinreichend decken [**SF-FUNK-Assets**].
- Die mit den zu schützenden Assets verbundenen Schwachstellen müssen vom Security-Framework analysiert worden sein und sich mit den im konkreten Szenario bereits bekannten hinreichend decken oder diese erweitern [**SF-FUNK-Schwachstellen**].
- Die vom Security-Framework berücksichtigten Angriffe müssen definiert sein und sich mit den im konkreten Szenario erwarteten Angriffen hinreichend decken [**SF-FUNK-Angriffe**].
- Für die berücksichtigten Angriffe müssen vom Security-Framework Sicherheitsmaßnahmen vorgesehen sein, deren Wirksamkeit nachgewiesen wird. Dabei kann einerseits eine Maßnahme gegen mehrere Angriffe schützen; andererseits kann es sinnvoll sein, zum Schutz gegen kritische Angriffe mehrere, bewusst redundante Maßnahmen einzusetzen [**SF-FUNK-Maßnahmen**].

Im Bezug auf die **Integration** der Komponenten in die bereits vorhandene Infrastruktur und den darauffolgenden Betrieb sind folgende Aspekte zu berücksichtigen:

- Da die in einem komplexen Szenario wie dem LRZ zu berücksichtigenden Schutzziele immer von dem einem Security-Framework zugrunde liegenden abstrakten Modell abweichen können, sind aus der Integrationsperspektive entsprechende Erweiterungsschnittstellen für die oben genannten funktionalen Aspekte erforderlich [**SF-INT-Erweiterung**].
- Wiederum in der Begriffsdefinition verankert und im Beispiel offensichtlich ist die Anforderung, dass Security-Frameworks einen methodisch unterstützten Anpassungsprozess vorsehen müssen, durch den die Adaption an die lokalen Gegebenheiten geführt wird [**SF-INT-Customizing**].
- Auf konzeptioneller Ebene setzt der angesprochene Anpassungsprozess eine geeignete, explizite Modularität des gesamten Security-Frameworks voraus [**SF-INT-Modularität**]. Ein grundlegendes Customizing kann beispielsweise in der Auswahl der relevanten Module bestehen.
- Die bereits im Kontext des Paradigmas *secure by design* in Kapitel 2 diskutierte Eigenschaft, dass Sicherheitsmaßnahmen einem System oder einem Szenario nicht nachhaltig nachträglich aufgepfropft werden können, steht nicht im Widerspruch zu der Notwendigkeit, Security-Frameworks in bereits vorhandene Infrastrukturen und für bereits vorhandene Dienste einführen zu können; dabei sollen die bisherigen Sicherheitskonzepte entsprechend abgelöst oder erweitert werden. Für den Einsatz in solchen Szenarien sollte das Security-Framework geeignete Migrationsschritte vorsehen, die mit entsprechenden

Ergänzungen auch beim Neuaufbau im Rahmen der initialen Einführung eines Dienstes verwendet werden können [**SF-INT-Einführung**].

- Ein weiterer, mit den vom Security-Framework vorgesehenen Maßnahmen eng zusammenhängender Integrationsaspekt ist die Wiederverwendung der im Szenario bereits vorhandenen Komponenten und Konzepte; so sollte beispielsweise für die von einem Security-Framework vorgesehene Speicherung von Policies eher auf ein bereits vorhandenes relationales Datenbankmanagementsystem zurückgegriffen werden können als dass ein zusätzliches eingeführt werden muss [**SF-INT-Wiederverwendbarkeit**].
- Die vom Security-Framework verwendete technische Basis muss zu der im Szenario bereits vorhandenen Infrastruktur passen. Beispielsweise wäre ein Security-Framework, das zum Austausch von sicherheitsrelevanten Nachrichten einen Enterprise Service Bus voraussetzt, im LRZ-Szenario nur mit einem sehr hohen Aufwand einsetzbar, da eine flächendeckende Umstellung auf web-service-basierte Kommunikation bisher nicht erforderlich war. Somit ist die Kompatibilität der vorgesehenen Komponenten eine zu berücksichtigende Anforderung [**SF-INT-Kompatibilität**].
- Für den praktischen Einsatz ist zudem essentiell, ob die Skalierbarkeit der Lösung beim Frameworkdesign adäquat berücksichtigt wurde [**SF-INT-Skalierbarkeit**]; beispielsweise könnte ein Security-Framework für WLAN Access Points hervorragende Sicherheitseigenschaften aufweisen, aber zu komplex sein, um wie im LRZ-Szenario für mehr als 1.000 räumlich stark verteilte Exemplare eingesetzt werden zu können.

Auch bezüglich der Managementoperationen und -prozesse treten im Szenario diverse Anforderungen hervor:

- Mit Blick auf den breiten Kundenkreis ergibt sich im LRZ-Szenario zunächst die Anforderung, dass die Mandantenfähigkeit der Dienste nicht beeinträchtigt werden darf. Ein angepasstes, instanziiertes und operativ eingesetztes Security-Framework muss in der Umgebung dieses Szenarios folglich für verschiedene Kunden separat parametrisiert werden können [**SF-MGMT-Mandantenfähigkeit**].
- Komplementär zu dieser grundlegenden Mandantenfähigkeit muss im LRZ-Szenario auch die pro Kunde mögliche delegierte Administration, beispielsweise durch Lehrstuhlbeauftragte an einer der Münchner Hochschulen, beibehalten werden [**SF-MGMT-Delegation**]; die Einführung eines Security-Frameworks darf somit keinen Paradigmenwechsel, beispielsweise von dezentraler hin zu zentraler Administration, erforderlich machen, wenn dieser nicht bereits unabhängig vom Einsatz des Security-Frameworks in Planung ist.
- Für den operativen Betrieb stellen die für das Security-Framework gesamtheitlich definierten Managementoperationen den zentralen Ansatzpunkt dar, der darüber entscheidet, in welchen Bereichen das Security-Framework als Ganzes verwaltet werden kann und in welchen anderen Bereichen zwar zusammenhängende, aber nach wie vor einzelne zu verwaltende Komponenten vorliegen [**SF-MGMT-Operationen**]. Dieser Aspekt kommt offensichtlich nur dann zum Tragen, wenn das Security-Framework über ein Architekturkonzept hinausgehend mindestens eine dedizierte Managementkomponente vorsieht, durch die darunter liegende Managementoperationen aus der Sicht eines zentralen, integrierten Managementwerkzeugs verschattet werden.

- Bezüglich der Prävention und Detektion der vom Security-Framework betrachteten Angriffe ist eine entsprechende Spezifikation von Sicherheitsereignissen, -alarmen und -vorfällen notwendig, die von der vorhandenen oder zusätzlich vorgesehenen Managementinfrastruktur verarbeitet werden müssen [**SF-MGMT-Events**].
- Für das Zusammenspiel mit anderen Prozessen wie dem Incident Management und der Kapazitätsplanung müssen geeignete Schnittstellen zu ITSM-Prozessen definiert worden sein [**SF-MGMT-ITSM-Schnittstellen**].

Das Szenario zeigt auch bereits mehrere grundlegende Anforderungen an die Dokumentation von Security-Frameworks:

- Zur Beurteilung eines Security-Frameworks ist seine strategische Ausrichtung im Hinblick auf die Beiträge zur Prävention, Detektion und Reaktion auf Angriffe relevant; entsprechende Schwerpunkte und bewusste Auslassungen sollten explizit dokumentiert sein [**SF-DOKU-Ausrichtung**].
- Die Auswahl potentiell einzusetzender Security-Frameworks muss unter anderem die Vollständigkeit der betrachteten Angriffe und die Wirksamkeit der vorgeschlagenen Sicherheitsmaßnahmen berücksichtigen. Beides setzt voraus, dass die dem Security-Framework zugrunde gelegten Angreifermodelle explizit dokumentiert worden sind [**SF-DOKU-Angreifermodelle**].
- Sofern ein Security-Framework – wie es praktisch häufig der Fall ist – bestimmte Bereiche von der Betrachtung ausklammert, sollten die resultierenden Anforderungen an die bereits vorhandene Infrastruktur explizit genannt werden. Bietet ein Security-Framework für den Betrieb von Mail-Servern beispielsweise keine eigenen Konzepte für den Schutz der Maschinen, auf denen die Mail-Dienste betrieben werden, so sollten die Anforderungen daran – beispielsweise, dass automatisch Betriebssystemupdates durchgeführt werden sollen – postuliert werden. Diese und ähnliche Aspekte werden unter der Anforderung, dass die für den Einsatz des Security-Frameworks notwendigen Voraussetzungen dokumentiert sind, subsummiert [**SF-DOKU-Voraussetzungen**].
- Aus der Dokumentation des Frameworkkonzepts sollte deutlich hervorgehen, an welche Zielgruppe es sich wendet, z. B. ob es sich um eine vollständige Betrachtung für Dienstadministratoren handelt oder ob additive Sicherheitsaspekte diskutiert werden, die von einer auf IT-Sicherheit spezialisierten Gruppe umgesetzt werden müssen [**SF-DOKU-Zielgruppe**].

Die aus diesem ersten Szenario ermittelten Anforderungen geben bereits grob einen Rahmen vor, der zur Analyse von Security-Frameworks herangezogen werden kann. Sie werden in den folgenden Abschnitten unter anderem durch Berücksichtigung der Charakteristika und Besonderheiten der anderen Szenarien ergänzt.

3.3. Szenario 2: Micropayment für webbasierte E-Commerce-Anwendungen

Umständliche Anmeldeverfahren und hohe Gebühren für die Abwicklung von Kredit- und Debitkartentransaktionen haben das Bezahlen geringer Geldbeträge (im Bereich von Cents

bis zu wenigen Euros) für webbasierte Anwendungen lange Zeit ausgebremst. Mittlerweile hat sich jedoch die Erkenntnis durchgesetzt, dass auch die moderate Beteiligung an einer entsprechend großen Anzahl von kleineren Transaktionen, beispielsweise beim Online-Erwerb von Zeitungs- und Zeitschriftenartikeln, attraktive Gewinnmargen abwerfen kann. So genannte Micropayment-Provider wickeln die Bezahlung für den E-Commerce-Anbieter im Hintergrund kostengünstig ab; zudem garantieren sie dem Käufer einen sicheren Bezahlvorgang und buchen die angefallenen Beträge beispielsweise am Monatsende per Lastschriftverfahren vom Konto des Kunden ab.

Das hier vorgestellte Szenario ist von den bekannten Architekturen realer Micropayment-Provider inspiriert, jedoch in mehreren Bereichen vereinfacht und insgesamt als fiktiv zu betrachten. Es soll verstärkt die Besonderheiten aufzeigen, die sich im Bereich der IT-Sicherheit im Hinblick auf gesetzliche Rahmenbedingungen (Compliance) und Transparenz durch Revisionen (Audits) ergeben.

3.3.1. Darstellung der Ist-Situation im Micropayment-Szenario

Im Folgenden wird das Szenario wiederum anhand der bekannten Kriterien eingeordnet; daran anschließend werden die Architektur des Micropayment-Dienstes und die im Szenario eingesetzten Sicherheitsmaßnahmen vorgestellt.

3.3.1.1. Szenariencharakteristika

Neben dem Micropayment-Provider selbst müssen in diesem Szenario auch die E-Commerce-Anbieter, die ihren Kunden das entsprechende Bezahlverfahren anbieten möchten, und die Beziehungen zu anderen Organisationen – beispielsweise den Banken der Kunden, von denen die fälligen Beträge eingezogen werden sollen – und somit insgesamt *n Organisationen* berücksichtigt werden. Die Sicherheitsverantwortung liegt dabei *zentral* beim Micropayment-Provider, dessen zentrale Sicherheitsmanagementgruppe direkt dem CISO unterstellt ist.

Da für den Webauftritt, über den sich auch neue Kunden registrieren können, und die Transaktionsabwicklung unterschiedliche Security-Frameworks betrachtet werden sollen, fällt das Szenario in die Kategorie mit *2–3 Security-Frameworks*. Zur Abwicklung der Bezahlvorgänge werden offensichtlich personenbezogene Informationen verarbeitet, die aufgrund der enthaltenen Finanzdaten als besonders sensibel anzusehen sind und in die Kategorie *Profildaten* fallen. Der Micropayment-Provider unterliegt Überwachungs- sowie Meldepflichten, muss alle Transaktionen protokollieren und wird im Rahmen von Revisionen durch *externe Gutachter* regelmäßig überprüft, um beispielsweise Geldwäscheversuche aufzudecken.

Das Szenarios entwickelt sich insgesamt *evolutionär*, da sowohl die angeschlossenen E-Commerce-Anbieter als auch die Privatkunden einer nicht vernachlässigbaren Fluktuation unterliegen und auch die Infrastrukturbestandteile regelmäßig erweitert und aktualisiert werden; der Benutzerkreis selbst ist dabei *offen*, da der Dienst von jeder Person genutzt werden kann, die ein Bankkonto hat.

Da im Szenario mit internetbasierten Finanzdienstleistungen für E-Commerce genau ein Geschäftsbereich analysiert wird, sind zum einen *viele, bekannte* Angreifermodelle zu berücksichtigen und zum anderen die relevanten *Sicherheitsmanagementprozesse* genau definiert.

Charakteristikum	Ausprägung		
Anzahl Organisationen	0	1	n
Sicherheitsverantwortung	dezentral	hierarchisch	zentral
Anzahl Security-Frameworks	1	2-3	mehr als 3
Personenbezogene Daten	keine	Kontaktdaten	Profildaten
Kontrollen / ext. Vorgaben	keine	intern	extern
Dynamik	statisch	evolutionär	dynamisch
Benutzerkreis	klein, geschl.	groß, geschl.	offen
Angreifermodelle	wenige	viele, bekannte	viele, spezifische
Infrastruktur/Prozesse	Neuaufbau	ohne Prozesse	Prozessorientiert
Interne Abhängigkeiten	vernachlässigbar	gegeben	stark

Abbildung 3.11.: Charakterisierung von Szenario 2

Die hier betrachteten technischen Dienste sind *stark* voneinander abhängig; Abbildung 3.11 fasst diese Charakterisierung zusammen.

3.3.1.2. Architektur und Workflows des Micropayment-Dienstes

Abbildung 3.12 zeigt vereinfachend die Architektur des Micropayment-Dienstes, die nachfolgend am Beispiel der Abwicklung einer Transaktion erläutert wird. In die Webanwendung eines E-Commerce-Anbieters, die vom Käufer genutzt wird und eine lokale Benutzerdatenbank verwendet, wurde eine Schnittstelle zum Micropayment-Provider integriert; diese wird in Form eines Application Programming Interfaces (API) angeboten, das lediglich mit den Vertragsdaten des E-Commerce-Anbieters parametrisiert werden muss. Sobald sich der Käufer dazu entscheidet, die Bezahlung über den Micropayment-Provider abzuwickeln, kommt eine proprietäre Abwandlung des Micro Payment Transfer Protocol (MPTP, [MPTP]) zum Einsatz. Der Benutzer wird dabei auf die Webseite des Micropayment-Providers umgeleitet; die Angaben über Geldbetrag, Verwendungszweck und Empfänger werden in Form verschlüsselter Parameter an das Micropayment-System übermittelt.

Die weitere Abwicklung des Zahlungsvorgangs ist davon abhängig, ob sich der Kunde bereits früher beim Micropayment-Provider angemeldet hat oder ihn zum ersten Mal verwendet:

- Bestandskunden können sich mit ihrer im System hinterlegten E-Mail-Adresse und einer PIN, die bei der Erstanmeldung zugeteilt wurde, authentifizieren.
- Neukunden müssen einen Registrierungsprozess durchlaufen, bei dem Kontakt- und Kontodaten abgefragt werden. Zur Vermeidung von Kosten durch nicht gedeckte Konten wird dabei im Hintergrund eine Auskunft über die Einschätzung der Kreditwürdigkeit der Person bei einer Scoring-Agentur eingeholt; zudem kann die Existenz des angegebenen Kontos bei einigen Banken, mit denen das Micropayment-Unternehmen einen entsprechenden Vertrag hat, sofort online verifiziert werden.

  Für den Fall, dass die Kontodaten nicht sofort überprüft werden können oder die Kreditauskunft nicht positiv ist, wird der maximale Umsatz für den Neukunden auf einen niedrigen Pauschalbetrag begrenzt, bis die erste Abbuchung vom Bankkonto erfolgreich durchgeführt wurde.

  Nach der Registrierung wird der Bezahlvorgang wie bei Bestandskunden fortgesetzt.

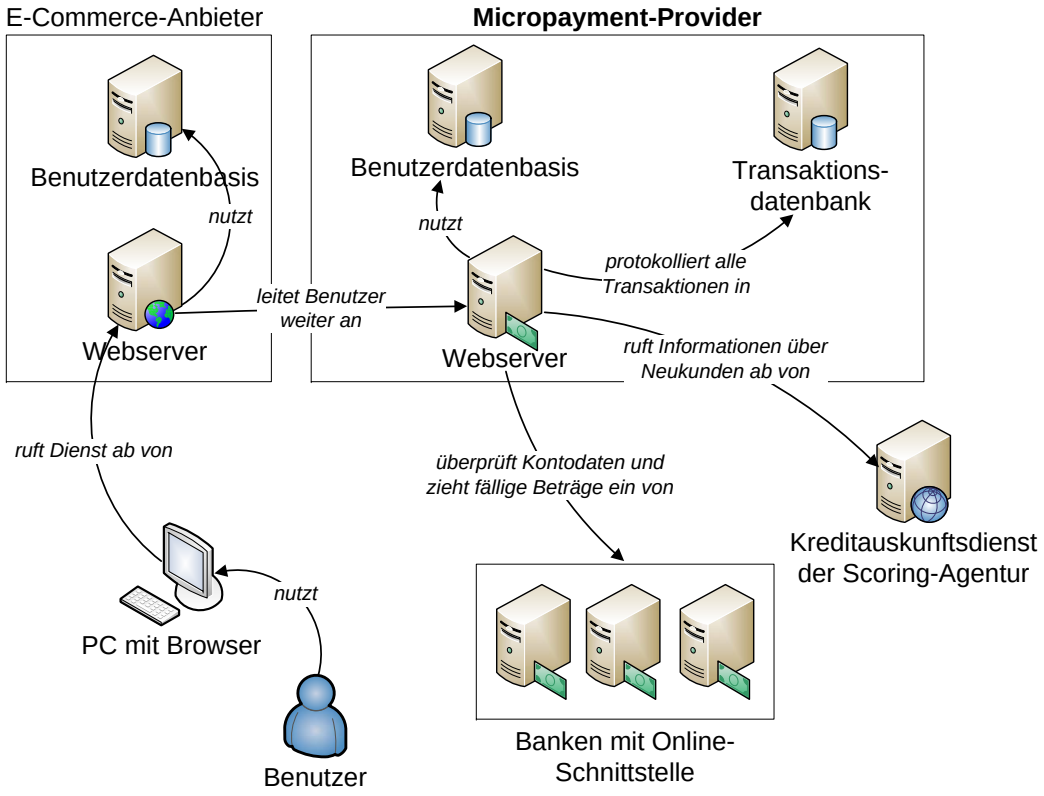


Abbildung 3.12.: Überblick über das Micropayment-Provider-Szenario

Nachdem der Benutzer erfolgreich authentifiziert wurde, werden ihm die Transaktionsdetails angezeigt; aufgrund der geringen Beträge und der Möglichkeit, die Lastschrift-Abbuchung bei Missbrauchsfällen nachträglich stornieren zu können, erfolgt die Freigabe der Transaktion ohne weitere (Einmal-)Passwörter per Knopfdruck. Die für den Benutzer damit abgeschlossene Bezahlung wird an den E-Commerce-Anbieter zurückgemeldet, der seinem Kunden Zugriff auf die bezahlte Ware gewährt. Eine Bestätigung über die Bezahlung wird vom Micropayment-Provider zusätzlich an den Benutzer und den E-Commerce-Anbieter per E-Mail verschickt.

Am Ende des Monats werden die so akkumulierten Transaktionen tatsächlich abgewickelt, indem die von den Kunden fälligen Beträge abgebucht und um die Gebühren, die der Micropayment-Provider für sich behält, verringert an die E-Commerce-Anbieter überwiesen. Am Jahresanfang erhalten alle Kunden und angeschlossenen E-Commerce-Anbieter zudem ein elektronisch signiertes Dokument per E-Mail zugesandt, in dem nochmals alle Transaktionen des vergangenen Kalenderjahres zusammengefasst sind.

3.3.1.3. Im Micropayment-Szenario bisher eingesetzte Sicherheitsmaßnahmen

Wie in der Finanzbranche üblich setzt der Micropayment-Provider auf **technischer Ebene** verstärkt auf Kontrollen der Datenflüsse und sichert sich insbesondere auch gegen Insider-Angriffe weitgehend ab. Dazu werden als Grundlage sämtliche Kommunikationsbeziehungen zwischen den an der Infrastruktur beteiligten Rechnergruppen über Firewalls abgewickelt,

wobei eine mehrstufige Vorgehensweise nach dem bekannten Architekturmuster so genannter demilitarisierter Zonen gewählt wurde. Die über das Internet erreichbaren Frontends werden zudem von einem Intrusion Prevention System überwacht, das am zentralen Internet-Gateway die IP-Adressen solcher Clients automatisch sperrt, die wiederholt syntaktisch falsche Datenpakete senden oder innerhalb einer Minute mehr als fünf Logins mit falschem Passwort versuchen.

Sämtliche Transaktionen werden in einer Datenbank gespeichert, die so konfiguriert ist, dass sie keine Modifikation und kein Löschen der angelegten Einträge zulässt. Die Transaktionen der letzten 30 Tage werden zudem kontinuierlich von einem Algorithmus zur Erkennung von Ausreißern analysiert, bei dem die Frequenz und das Volumen der jüngsten Transaktionen jedes Kunden mit seinem sonst üblichen Kaufverhalten verglichen werden. Entdeckte Auffälligkeiten, die beispielsweise ein Indiz für einen gestohlenen oder geknackten Account sein können, werden an die Sicherheitsgruppe gemeldet.

Die Übertragung und Ablage der Benutzer- und Transaktionsdaten erfolgt ausschließlich in verschlüsselter Form. Technische Kommunikationspartner wie die Webserver der angeschlossenen E-Commerce-Provider und Banken werden auf Basis von Serverzertifikaten ausgewählter Certificate Authorities authentifiziert.

Die Aktivitäten der Systemadministratoren werden durch ein revisionsfähiges Privileged Account Management (PAM) System überwacht, das administrativen Zugang zu den Systemen nur nach Anmeldung mit der persönlichen Kennung des Benutzers erlaubt und sämtliche Aktionen in der Granularität einzelner Tastenanschläge jeweils mit Zeitstempel in einem manipulationsevidenten Protokoll aufzeichnet. Ausgewählte Änderungen sind zudem nur nach dem Vier-Augen-Prinzip möglich, d. h. sie werden erst wirksam, nachdem sie von einem zweiten Administrator bestätigt wurden.

Auf **organisatorischer Ebene** sind die folgenden Sicherheitsmaßnahmen für das Szenario charakteristisch: Die Qualitätssicherung im Unternehmen und das Sicherheitsmanagement des angebotenen Micropayment-Dienstes sind nach ISO 9000 und ISO/IEC 20000 zertifiziert; dies dient einerseits als Voraussetzung für die Nutzung der Online-Schnittstelle zu den Banken und wird andererseits im Marketing gegenüber E-Commerce-Anbietern und Benutzern eingesetzt.

Zur Ausfallsicherheit wird die gesamte Infrastruktur identisch in einem Backup-Rechenzentrum betrieben, zu dem auch die Datenbestände inkrementell gespiegelt werden. Die Sicherheitsmanagementgruppe nimmt zudem werktäglich stichprobenbasierte Analysen der Transaktions- und PAM-Protokolle vor. Diese dienen auch als Vorbereitung für die jährlich stattfindende Revision, bei der eine Gruppe externer Prüfer neben den Bilanzen ebenfalls Stichproben der Transaktionen begutachtet. Seit im Rahmen einer solchen Revisionsprüfung das Fehlen proaktiver Sicherheitsüberprüfungen bemängelt wurde, wird vierteljährlich ein IT-Sicherheitsberatungsunternehmen mit der Durchführung von Penetration Tests beauftragt.

3.3.2. Herausforderungen und Ansatzpunkte zur Optimierung

Der Micropayment-Provider ist mit seiner sich bereits auf hohem Niveau befindenden IT-Sicherheitslage nicht unzufrieden, steht jedoch wie andere internetbasierte Unternehmen unter dem Druck sich ständig wandelnder Anforderungen, die zügig umgesetzt werden müssen, als Konsequenz jedoch beispielsweise eine Neuauflage der Zertifizierungen erforderlich machen;

dies ist bei den bisherigen, eigenentwickelten Konzepten meist mit einem hohen Aufwand verbunden.

Zum einen sinkt mit der zunehmenden Anzahl konkurrierender Micropayment-Provider die Bereitschaft angeschlossener E-Commerce-Anbieter, jeweils proprietäre Transaktionsprotokolle zu unterstützen, sodass der Bedarf zum Umstieg auf eine standardisierte Lösung wächst. Zum anderen wachsen auch das Sicherheitsbewusstsein und Schutzbedürfnis der Anwender, beispielsweise im Hinblick auf die Möglichkeit, ab einem bestimmten Geldbetrag stärkere Authentifizierungsverfahren als die PIN-Eingabe verwenden zu können.

Entsprechende Änderungen haben umfangreiche Auswirkungen, da sie Kernbestandteile der Infrastruktur betreffen und damit bei jedem Eingriff eine Neubewertung der Sicherheitssituation erforderlich machen. Da neben den Kosten für die Implementierung und Zertifizierung auch der konzeptionelle Aufwand meist sehr hoch ist, kann die stärkere Orientierung an geeigneten Security-Frameworks helfen, moderne Sicherheitskonzepte effizienter umzusetzen.

Eine besondere Rolle spielen im Szenario zudem das Fehlermanagement und der Benutzersupport. Ihre Effizienz ist kritisch, da die manuelle Bearbeitung einer Kundenanfrage – selbst wenn sie nur wenige Minuten in Anspruch nimmt – wesentlich höhere Kosten verursacht als durch die jeweilige Transaktion umgesetzt bzw. eingenommen wird. Deshalb muss auch die Benutzerfreundlichkeit kontinuierlich verbessert werden, um das Aufkommen von Anfragen möglichst zu vermeiden.

3.3.3. Durch Security-Frameworks zu erwartender Mehrwert

Die Webschnittstelle, über die Kundenanmeldungen und Bezahlvorgänge abgewickelt werden, und das Finanztransaktionsbackend sind zwar stark voneinander abhängig, aber lediglich durch eine exakt definierte Schnittstelle miteinander verbunden, sodass beide Bereiche prinzipiell unabhängig voneinander weiterentwickelt werden können. Somit kann die kontinuierliche Ausarbeitung und änderungsbedingte Neuerstellung eines eigenen Gesamtsicherheitskonzepts durch den Einsatz getrennter Security-Frameworks für die beiden Bereiche gezielt unterstützt werden.

Grundlegend wird angenommen, dass ein Security-Framework für den gesamten Bereich des Webauftritts keine einmalige, statische Lösung darstellt, sondern unter Berücksichtigung aktueller Entwicklungen, z. B. der Entdeckung neuer Verwundbarkeiten und Angriffsvarianten, kontinuierlich weiterentwickelt wird. Damit wird der konzeptionelle Aufwand reduziert, den die lokalen Sicherheitsbeauftragten betreiben müssen, um sich jederzeit im Bezug auf aktuelle Sicherheitsentwicklungen vollständig auf dem Laufenden zu halten; beispielsweise wird der Bewertungsprozess, der entscheidet, ob neue Angriffe für die eigene Infrastruktur relevant sind, dadurch gezielt unterstützt und basiert nicht mehr rein auf der subjektiven Einschätzung durch den vor Ort Zuständigen.

In einem für das Szenario geeigneten Web-Security-Framework stehen beispielsweise bereits verschiedene Varianten der Benutzerauthentifizierung zur Verfügung, sodass bei der angestrebten Umstellung auf stärkere oder kontextsensitiv zusätzliche Authentisierungsschritte solche existierenden Konzepte genutzt werden können, deren Auswirkungen auf die übrigen Komponenten bereits vorab bekannt sind. Durch die Orientierung an diesen Vorgaben können die notwendigen Umstellungen darüber hinaus minimalinvasiv erfolgen.

Beim Einsatz im Backend ergibt sich der Vorteil, dass auf Micropayment-Transaktionen spezialisierte Security-Frameworks die in diesem Umfeld relevanten Standards und Best Practices berücksichtigen. Dadurch kann nicht nur der Aufwand für die Implementierung und Wartung proprietärer Verfahren gesenkt werden, sondern es bietet sich auch wiederum der Vorteil, die Auswahl und die Wirksamkeit der eingesetzten Maßnahmen beispielsweise im Rahmen von Revisionen strukturiert begründen zu können. Im Hinblick auf die sich abzeichnende Bildung von Standards und die durch die beteiligten Banken vorangetriebene Vereinheitlichung könnte sich daraus mittelfristig ein allgemeines Micropayment Security Framework entwickeln, das beispielsweise bezüglich der Inbetriebnahme von Aktualisierungen nach entsprechender Anpassung durch die beteiligten Micropayment-Provider branchenweit koordiniert ausgerollt wird.

3.3.4. Ableitung und Diskussion von Anforderungen aus dem Micropayment-Szenario

Aus dem Micropayment-Szenario ergibt sich eine Reihe weiterer Anforderungen, die nachfolgend entsprechend der Einteilung in die vier Anforderungskategorien diskutiert werden. Auf **funktionaler Ebene** zeichnet sich zunächst die folgende Anforderung ab:

- Es ist notwendig, dass neben dem eigentlichen Autorisierungsmanagement, das durch eine Zugriffskontrolle umgesetzt wird, auch die revisionssichere Protokollierung aller relevanten Vorgänge zwingend berücksichtigt werden muss [**SF-FUNK-Auditing**], die entsprechend in allen vom Security-Framework vorgesehenen Komponenten geeignet integriert sein muss.

An die **Integration** und den Betrieb von Security-Frameworks wird die folgende neue Anforderung gestellt:

- Es ist erforderlich, dass die vorhandenen Hochverfügbarkeitskonzepte unterstützt werden [**SF-INT-Hochverfügbarkeit**]; im Szenario entspricht dies dem Aufbau einer gespiegelten Infrastruktur im Standby-Betrieb, deren Konfigurations- und Nutzdatenbestand mit der Primärinfrastruktur synchronisiert werden muss.

Im Bereich der **Managementanforderungen** sind die folgenden Aspekte zu berücksichtigen:

- Das Szenario zeigt deutlich, dass Security-Frameworks die szenarientypischen Administrationskonzepte – hier das Privileged Account Management und das Vier-Augen-Prinzip – unterstützen müssen [**SF-MGMT-Administrationskonzepte**]. Andernfalls könnten branchenspezifische Anforderungen nicht umgesetzt oder massive Erweiterungen der vom Framework vorgesehenen Administrationsprozesse notwendig werden.
- Im Hinblick auf Compliance-Anforderungen ist die bereits in Abschnitt 2.1.1.2 diskutierte Abwägung zwischen einander möglicherweise widersprechenden Zielen, beispielsweise Datenschutz und präzise Nachvollziehbarkeit der Handlungen von Administratoren und Benutzern, durchzuführen. Das Security-Framework sollte diese Aspekte explizit berücksichtigen, eine klare Position beziehen und ggf. für mehrere Realisierungsvarianten die entsprechenden Aufgaben der Managementprozesse vorgeben [**SF-MGMT-Compliance**]. Diese Anforderung wird durch in der jeweiligen Branche spezifische Compliance-Auflagen weiter verstärkt.

- Die durch das Security-Framework eingeführten Komponenten dürfen sich nicht negativ auf die Performanz und Hochverfügbarkeit der Infrastruktur auswirken [**SF-MGMT-Performanz**].
- Im Hinblick auf die Inbetriebnahme und die kontinuierliche proaktive Überwachung der Infrastruktur sollten Ansatzpunkte für die Funktionsüberprüfung und beispielsweise auch Penetration Tests und entsprechende Vorgehensweisen beschrieben sein [**SF-MGMT-Tests**].
- Die mit der Anpassung, der Anschaffung und dem Betrieb verbundenen Aufwendungen und die Wirtschaftlichkeit der Lösung müssen aus dem Frameworkkonzept ersichtlich oder ableitbar sein und sich mit den szenarienspezifischen Randbedingungen decken [**SF-MGMT-Kosten**].

Die Dokumentation des Security-Frameworks ist für seinen Einsatz in kommerziellen Szenarien unerlässlich; dabei sind insbesondere die folgenden beiden Anforderungen zu berücksichtigen:

- In der Dokumentation sind zunächst die Geschäfts- und Managementziele sowie die IT-Sicherheits- und Sicherheitsmanagementziele festzuhalten, die vom Security-Framework angestrebt werden [**SF-DOKU-Ziele**].
- Ein zusätzlicher Mehrwert ergibt sich, wenn konkrete Beiträge zu den im Szenario angestrebten Zertifizierungen geliefert werden; die dafür notwendigen Schritte müssen beim Design berücksichtigt und explizit festgehalten worden sein [**SF-DOKU-Zertifizierung**].

Eine Reihe weiterer Anforderungen, die insbesondere in organisationsübergreifenden Szenarien relevant sind, werden im Rahmen des nachfolgenden Szenarios erläutert.

3.4. Szenario 3: Grid Computing am Beispiel DEISA

Aktuelle Grid-Projekte ermöglichen Wissenschaftlern die Nutzung von auf mehrere Standorte verteilten, lose gekoppelten und heterogenen Rechen- und Speicherkapazitäten. Die technische Weiterentwicklung in diesem Bereich zielt unter anderem darauf ab, die räumliche Verteilung und Heterogenität der Ressourcen gegenüber den Benutzern noch stärker zu verschatten, um damit der Vision von der flächendeckend verfügbaren, einfach nutzbaren und passend zum jeweiligen Bedarf dimensionierter Rechnerleistung immer näher zu kommen.

Das Grid-Projekt DEISA (Distributed European Infrastructure for Supercomputing Applications, `http://www.deisa.eu/`) ist wie in Abbildung 3.13 dargestellt ein Zusammenschluss mehrerer europäischer wissenschaftlicher Höchstleistungsrechenzentren, der das Ziel verfolgt, im Rahmen eines EU-geförderten Forschungsprojekts eine effiziente und nachhaltige europäische Grid-Infrastruktur für wissenschaftliche Anwendungen aufzubauen.

Dieses Szenario zeigt zum einen die Herausforderungen für den Einsatz von Security-Frameworks, die sich bei einer losen Kopplung der beteiligten Organisationen ergeben, und geht zum anderen auf die Schwierigkeiten bei der Integration in heterogene Infrastrukturen, deren Komponenten auch außerhalb des Grid-Projekts genutzt werden, ein.

Abbildung 3.13.: Szenario 3: An DEISA beteiligte Rechenzentren (Quelle: http://www.deisa.eu/)

3.4.1. Darstellung der Ist-Situation im Grid-Szenario

Nach der Charakterisierung des Szenarios werden die Varianten zur Nutzung der DEISA-Infrastruktur skizziert und die aktuell eingesetzten technischen und organisatorischen Sicherheitsmaßnahmen diskutiert.

3.4.1.1. Szenariencharakteristika

Wie in Abbildung 3.14 dargestellt werden im Szenario *n Organisationen* betrachtet. Im Umfeld des Grid Computing ist dabei zwischen realen Organisationen und so genannten virtuellen Organisationen zu unterscheiden, zu denen sich reale Organisationen zum Zweck der gemeinsamen, koordinierten Problemlösung unter weitgehender Beibehaltung ihrer technischen, organisatorischen und juristischen Selbständigkeit zusammenschließen. Da es im DEISA-Projekt keine ausgezeichnete Organisation gibt, die technische Vorgaben für alle Beteiligten erlässt, werden im Folgenden die jeweiligen realen Organisationen mit ihren internen Strukturen betrachtet.

Trotz gemeinsamer Konzepte verbleibt die Sicherheitsverantwortung in DEISA *dezentral* bei jeder beteiligten Einrichtung, die als DEISA-Site bezeichnet wird. In der Regel ist dort die jeweilige lokale DEISA-Projektgruppe für die Sicherheitsaspekte verantwortlich, wobei Sicherheitsvorfälle fachlich projektweit und hierarchisch typischerweise entsprechend der lokalen Organisationsstruktur eskaliert werden. Ein Beispiel dafür ist das in Szenario 1 beschriebene LRZ, das ebenfalls an DEISA beteiligt ist.

In diesem Szenario wird der Einsatz *eines Security-Frameworks* für Grid-Infrastrukturen untersucht; im Allgemeinen ist jedoch davon auszugehen, dass an Grid-Projekten beteiligte Organisationen noch weitere Dienste anbieten, sodass eine nahtlose Integration in die lokale

Charakteristikum	Ausprägung		
Anzahl Organisationen	0	1	n
Sicherheitsverantwortung	dezentral	hierarchisch	zentral
Anzahl Security-Frameworks	1	2-3	mehr als 3
Personenbezogene Daten	keine	Kontaktdaten	Profildaten
Kontrollen / ext. Vorgaben	keine	intern	extern
Dynamik	statisch	evolutionär	dynamisch
Benutzerkreis	klein, geschl.	groß, geschl.	offen
Angreifermodelle	wenige	viele, bekannte	viele, spezifische
Infrastruktur/Prozesse	Neuaufbau	ohne Prozesse	Prozessorientiert
Interne Abhängigkeiten	vernachlässigbar	gegeben	stark

Abbildung 3.14.: Charakterisierung von Szenario 3

Infrastruktur erforderlich ist. DEISA setzt eine explizite Identifizierung und Autorisierung seiner Benutzer voraus; letztere wird beispielsweise unter anderem aus der Nationalität des Benutzers abgeleitet. Somit werden deutlich mehr als die grundlegenden Kontaktdaten benötigt, d. h. es werden *Profildaten* verarbeitet. Bisher finden *keine Kontrollen* der Sicherheitslage auf Basis externer Vorgaben statt, die über die bei jeder DEISA-Site bereits üblichen Verfahren hinausgehen würden.

Das Szenario ist unter anderem aufgrund seiner Organisation als Forschungsprojekt hochgradig *dynamisch* sowohl im Hinblick auf die Vielfalt der Nutzung als auch die innere technische Weiterentwicklung und hat einen derzeit *kleinen, geschlossenen* Benutzerkreis, der sich zu einem späteren Zeitpunkt mit zunehmender Reife der Infrastruktur deutlich vergrößern soll. Durch die Begrenzung der Teilnehmer und die unten diskutierte Isolation der Kommunikation sind aktuell nur vergleichsweise *wenige* Angreifermodelle zu betrachten.

Das DEISA-Projekt widmet sich dem *Neuaufbau* einer Infrastruktur, und obwohl Sicherheitsaspekte berücksichtigt und in einer dedizierten Projektgruppe analysiert werden, wurden soweit aufgrund der eher technischen Projektausrichtung keine umfassenden formalen Sicherheitsmanagementprozesse definiert. Die an DEISA beteiligten Organisationen und die von ihnen angebotenen Dienste sind prinzipiell nicht voneinander abhängig; auch bei der Bereitstellung inhärent zentraler DEISA-Infrastrukturdienste wird darauf geachtet, dass der Einfluss einzelner Organisationen nicht dominant werden kann und dass die anderen DEISA-Sites auch bei Ausfällen der Partnersysteme autark weiterarbeiten können. Die internen Abhängigkeiten sind somit *vernachlässigbar*.

3.4.1.2. Im Grid-Szenario betrachtete Dienste

Die DEISA-Infrastruktur bietet aus Benutzersicht vorrangig die in Abbildung 3.15 dargestellte Möglichkeit, die an den beteiligten Standorten verfügbaren Hochleistungsrechner nutzen zu können. Am LRZ wurden beispielsweise fünf Prozent der Rechenkapazität des Bundeshöchstleistungsrechners für die Verwendung in DEISA reserviert. Um Programme und Daten einfach und effizient zwischen diesen Rechenressourcen austauschen zu können, wird zudem ein hochperformantes globales Dateisystem bereitgestellt.

Zur Nutzung dieser Dienste existieren zwei in Abbildung 3.16 dargestellte, aus Benutzersicht grundlegend verschiedene, wenngleich aufeinander aufbauende Zugangsmethoden. In der klas-

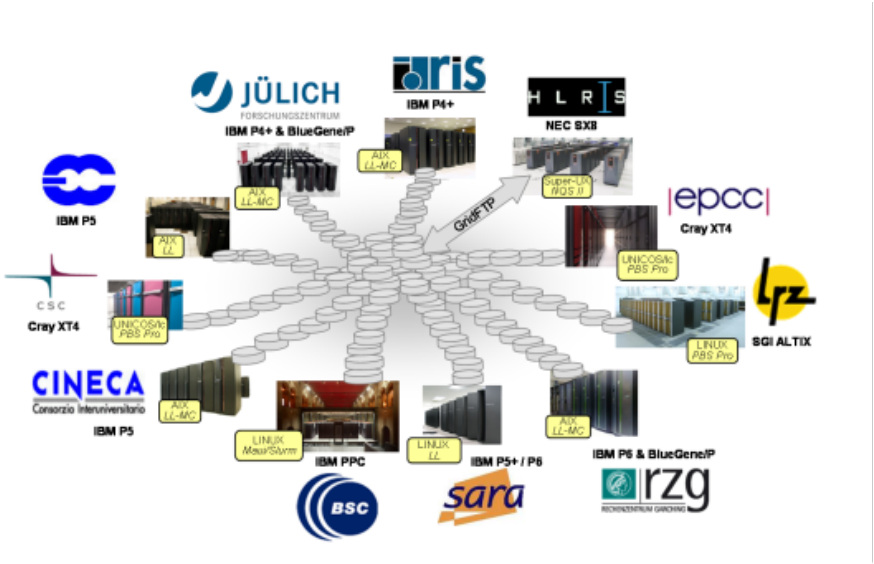


Abbildung 3.15.: Szenario 3: Hochleistungsrechner im DEISA-Verbund (Quelle: http://www.deisa.eu/)

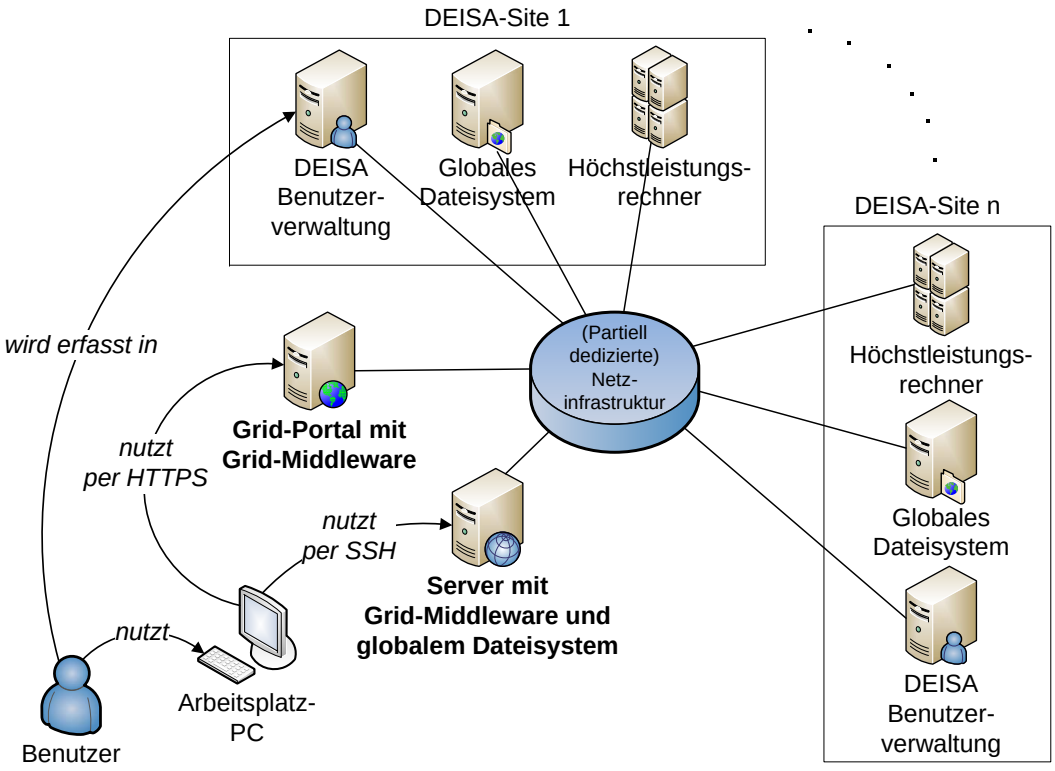


Abbildung 3.16.: Szenario 3: Dienstnutzung über Grid-Middleware oder Grid-Portal

sischen Variante arbeitet der Benutzer direkt mit der so genannten Grid-Middleware, die in Form von Kommandozeilenbefehlen bereitgestellt wird. Über Aufrufparameter und Job Description Textdateien, die einem vorgegebenen syntaktischen Aufbau folgen, legt der Benutzer fest, welcher Programmcode ausgeführt werden soll und wo die entsprechenden Ein- und Ausgabedateien hinterlegt sind bzw. abgespeichert werden sollen. Die Auswahl des Rechners, auf dem der Code ausgeführt wird, kann prinzipiell beeinflusst werden, soll mittelfristig jedoch durch einen in der Grid-Middleware realisierten Automatismus abgelöst werden, der geeignete Anbieter unter anderem unter ökonomischen Gesichtspunkten selektiert. Der Rechenauftrag des Benutzers wird somit einem Schedulingsystem übergeben, über das sich der Benutzer auch über den aktuellen Bearbeitungsstand informieren kann.

Da verschiedene Grid-Middleware-Implementierungen mit entsprechend unterschiedlichen Aufrufkonventionen existieren und die Arbeit mit relativ komplexen Kommandozeilenwerkzeugen eine nicht zu unterschätzende Hürde für viele an der Infrastrukturnutzung interessierte Wissenschaftler ist, werden grafische Benutzeroberflächen als attraktive Zugangsalternative angesehen. Sie existieren wiederum in zwei Ausprägungen: Zum einen in Form von Client-Software, die Benutzer auf ihren Arbeitsplatzrechnern installieren und die im Wesentlichen das Hantieren mit den Kommandozeilenwerkzeugen hinter einer ansprechenderen Oberfläche verschatten; diese Variante wird hier nicht näher betrachtet, da sie aus Sicht des Infrastrukturbetriebs und seiner Sicherheitseigenschaften keinen Unterschied bewirkt. Zum anderen werden so genannte Grid-Portale eingesetzt, die Benutzeraufträge über eine Webschnittstelle entgegennehmen, wiederum über die Middleware zur Ausführung bringen und die Ergebnisse in geeigneter Weise zurückliefern.

Die Nutzung beider Zugangsvarianten ist nur für authentifizierte und autorisierte Benutzer möglich. Zur Erfassung der Benutzer betreibt jede DEISA-Site einen dedizierten Verzeichnisdienst, in dem die Stammdaten der über sie zugelassenen Benutzer hinterlegt werden. Darauf aufbauend kann jede DEISA-Site die Verzeichnisdienste aller anderen DEISA-Sites auslesen und somit für die eigenen und externen Benutzer dedizierte Accounts auf den eigenen Maschinen anlegen; dieser Vorgang erfolgt üblicherweise automatisch einmal pro Tag. Bei der Accountvergabe werden auch lokale Policies berücksichtigt; beispielsweise werden derzeit Benutzer bestimmter Nationalitäten nicht auf allen Maschinen aller DEISA-Sites zugelassen.

Die Autorisierung und der Umfang, zu dem die Rechenressourcen in Anspruch genommen werden dürfen, werden darüber hinaus in Form von wissenschaftlichen Projekten festgelegt, die ein DEISA-internes Genehmigungsverfahren durchlaufen müssen. In dieser Granularität wird auch ein Accounting durchgeführt, das Rohdaten für Statistiken und Berichte liefert. Im Projekt wird darüber hinaus an einer grafischen Aufbereitung von Monitoringinformationen gearbeitet und die Anwender werden bei der Nutzung der Infrastruktur gezielt unterstützt.

3.4.1.3. Im Grid-Szenario bisher eingesetzte Sicherheitsmaßnahmen

Die im Rahmen des DEISA-Projekts realisierte Infrastruktur stützt sich bezüglich ihrer **technischen Sicherheitsmechanismen** überwiegend auf die von der eingesetzten Grid-Middleware bereitgestellten Sicherheitsdienste. Diese umfassen insbesondere die starke Authentifizierung von Benutzern und technischen Kommunikationsendpunkten über Zertifikate, die von den Certificate Authorities der jeweils nationalen Forschungsnetze ausgestellt werden. Darüber hinaus werden bei jeder beteiligten Site Autorisierungsrichtlinien und Mappingfi-

les gepflegt, die festlegen, welche lokalen und externen Benutzer die jeweiligen lokalen Ressourcen in Anspruch nehmen dürfen. Auf Basis der vorhandenen Public Key Infrastruktur wird auch eine verschlüsselte Übertragung aller Daten ermöglicht, die beispielsweise zur Verbesserung des Datendurchsatzes auf Benutzerwunsch jedoch auch deaktiviert werden kann. Grundlegende Protokollierungsfunktionen ermöglichen in Kombination mit Teilen der ausgereiften Accountingdienste das Erkennen und Zurückverfolgen potentieller Missbrauchsfälle. Der Fokus liegt bislang jedoch deutlich auf der Prävention, wohingegen die Detektion von Sicherheitsvorfällen überwiegend manuell oder durch externe Werkzeuge erfolgen muss.

Diese Sicherheitsdienste ergänzend wird die Rechnerkommunikation partiell über dedizierte Netzverbindungen abgewickelt und zusätzlich durch Paketfilter-Firewalls eingeschränkt, sodass klassische netzbasierte Angriffe über das Internet deutlich erschwert werden. Die notwendigen Firewall-Konfigurationsparameter werden dabei manuell über Mailinglisten abgestimmt und in die jeweiligen Netzkomponenten eingetragen. Die dedizierte, LDAP-basierte verteilte Benutzerverwaltung bildet die Grundlage für das zeitnahe Anlegen, Modifizieren, Sperren und Löschen von Benutzerkennungen und ermöglicht einen Überblick über den gesamten aktuellen Benutzerkreis und die vergebenen Berechtigungen.

Auf **organisatorischer Ebene** wird zunächst davon ausgegangen, dass die von jeder Site bereitgestellten Ressourcen nicht DEISA-dediziert sind, sondern auch den örtlichen Benutzerkreisen zur Verfügung gestellt werden und somit bereits in ein jeweils lokales Sicherheitsmanagement integriert sind. Aufgrund der Heterogenität, die sich aus den Standorten in ganz Europa und den zum Teil unterschiedlichen Ausrichtungen der beteiligten Rechenzentren ergibt, werden von den DEISA-Richtlinien bewusst lediglich die für das Zusammenspiel im Rahmen des Projektes relevanten Sicherheitsaspekte geregelt.

Hervorzuheben ist diesbezüglich ein Workflow für die Out-of-Band-Kommunikation von Sicherheitsvorfällen, für die bei jeder DEISA-Site rund um die Uhr ein Ansprechpartner telefonisch erreichbar sein muss. Das für das Autorisierungsmanagement auf technischer Ebene erforderliche Trust Management wird implizit durch die DEISA-Mitgliedschaft gesteuert. Die Einteilung von Benutzern in Gruppen wird hingegen explizit über das Genehmigungsverfahren für Projekte angestoßen.

3.4.2. Herausforderungen und Ansatzpunkte zur Optimierung

Wie in vielen anderen Projekten ist auch an DEISA zu beobachten, dass u. a. aufgrund des Zeit- und Erwartungsdrucks die möglichst umfassende Funktionalität und einfache Benutzbarkeit Vorrang vor einer strikt und durchgängig auf IT-Sicherheit bedachten Lösung eingeräumt bekommen. Hinzu kommt die im Grid-Umfeld noch fehlende Standardisierung von Lösungen, die sich nicht nur in der Heterogenität beispielsweise der eingesetzten Middleware-Implementierungen abzeichnet, sondern auch dazu führt, dass einige Basisabläufe in vielen Projekten wieder von Grund auf neu konzipiert und umgesetzt werden.

In DEISA äußert sich diese Tendenz beispielsweise konkret in der verteilten Benutzerverwaltung: Mit ihr wurde nicht nur wie in [Homm07, S. 86f.] dargelegt eine architektonisch vergleichsweise komplexe und nur mit hohem Aufwand in die bei jeder DEISA-Site bereits vorhandene Identity Management Infrastruktur zu integrierende Lösung geschaffen, sondern es werden durch die versuchte Automatisierung auch neue Sicherheitsprobleme geschaffen, die organisatorisch und technisch nur unzureichend berücksichtigt werden konnten. So werden von

einer DEISA-Site neu eingetragene Kennungen automatisch innerhalb eines Tages auf allen DEISA-Ressourcen aller beteiligten Rechenzentren angelegt, sofern ausgewählte Benutzereigenschaften – beispielsweise die Nationalität – nicht dagegen sprechen. Bei diesem Prozess findet allerdings keine manuelle oder wirksame automatische Qualitäts- oder Plausibilitätsprüfung statt. Wird die DEISA-Benutzerverwaltung einer Site kompromittiert, können folglich vom Angreifer quasi über Nacht automatisch vollwertige Kennungen in allen beteiligten Rechenzentren angelegt werden, die unter anderem als Ausgangspunkt für weitere Angriffe dienen können. Darüber hinaus führen mangels geeigneter Administrationswerkzeuge auch Flüchtigkeitsfehler dazu, dass z. B. Benutzerverwaltungseinträge für neue Benutzer aus alten Einträgen kopiert, aber nur unvollständig angepasst werden; der neue Benutzer bekommt als Folge davon unbeabsichtigt Zugriff auf die Dateien des alten Benutzers, bis die Korrektur des Fehlers durchgeführt und an jede DEISA-Site propagiert wurde. Da der Aufbau dieser Benutzerverwaltungsinfrastruktur aber mit erheblichem Aufwand verbunden war und sich die beteiligten Administratoren zwischenzeitlich an die Notwendigkeit manueller Konsistenzprüfungen und Korrekturen gewöhnt haben, wird die erforderliche Designüberarbeitung nur spärlich vorangetrieben.

Im Unterschied zum Automatisierungsgrad, der mit der geschilderten Benutzerverwaltung erreicht wird, werden viele andere Workflows nach wie vor ausschließlich manuell durchgeführt, wodurch deutlich erkennbar wird, dass insgesamt noch keine einheitlichen Prozesskonzepte vorliegen. Beispielsweise werden neue Serverzertifikate und Firewallregeln explizit manuell und als Konsequenz daraus bei jeder Site um bis zu einige Tage zeitversetzt eingespielt, wodurch zum Teil die Serverkommunikation zwischen ganzen Standorten temporär zum Erliegen kommt. Dass die hier implizit vorhandenen elektronischen Signaturen gerade in diesem Bereich qualitätssichernde Automatismen zulassen würden, wurde von den zuständigen Projektgruppen noch nicht ausreichend berücksichtigt, unter anderem da sich die davon betroffenen Administratoren an die bisher notwendige Routinearbeit gewöhnt haben.

Die fehlende Durchgängigkeit der Sicherheitsrichtlinien erschwerend kommt hinzu, dass – möglicherweise auch bedingt durch einen Mangel an Schulungsangeboten – die Benutzer der Infrastruktur meist sehr pragmatisch agieren. Ein mangelndes Sicherheitsbewusstsein zeigt sich beispielsweise beim Umgang mit den zur Authentifizierung eingesetzten Benutzerzertifikaten. Die theoretische Stärke der zertifikatsbasierten Authentifizierung, die sich aus ihrer Resistenz gegen Brute-Force-Angriffe ergibt, wird in der Praxis häufig dadurch konterkariert, dass Benutzer die zu ihren Zertifikaten gehörenden Private Keys nicht durch Passwörter gegen fremden Zugriff schützen. Angreifer, z. B. auch böswillige Administratoren, die auf dem System oder über ein Backup Zugang zur entsprechenden Datei erlangen, können somit ohne weitere Hürden unter der Identität des Benutzers auf die anderen DEISA-Sites zugreifen.

Neben der nur eingeschränkten Interoperabilität mit anderen Grid-Projekten, die sich verstärkt auch aus den diversen DEISA-Eigenentwicklungen ergeben, sind zwei weitere essentielle Ansatzpunkte für Verbesserungen festzuhalten: Zum einen wird der Datenschutz bislang stark vernachlässigt, da z. B. jede DEISA-Site die vollständigen personenbezogenen Daten aller Benutzer jeder DEISA-Sites einsehen kann, selbst wenn diese keinerlei lokale Ressourcen nutzen (vgl. [Homm09]). Zum anderen fehlt mit Ausnahme der Kommunikation erkannter Sicherheitsvorfälle ein Security-Reporting, das einen Überblick über die Sicherheitsgesamtsituation der DEISA-Infrastruktur gibt, der trotz der dezentralen Verantwortlichkeiten notwendig wäre. Entsprechend werden auch Schwachstellenanalysen und proaktive Sicherheitsmaßnahmen höchstens bei jeder Site lokal, aber nicht infrastrukturweit angegangen.

Der Einsatz eines Security-Frameworks soll deshalb offensichtlich den Mehrwert bieten, dass anerkannte und durchgängige Sicherheitskonzepte auf Basis nahtlos in die lokalen Infrastrukturen zu integrierender, interoperabler Komponenten umgesetzt und die notwendigen Administrations- und Managementkonzepte verbindlich spezifiziert werden.

3.4.3. Durch Security-Frameworks zu erwartender Mehrwert

Aus der Diskussion zu verbessernder Sicherheitseigenschaften lässt sich zusammenfassend schließen, dass an der Vollständigkeit der Sicherheitskonzepte und ihrer nachhaltigen Umsetzung im DEISA-Projekt noch gearbeitet werden muss. Der Einsatz eines Security-Frameworks bietet sich entsprechend an, da mit ihm Verbesserungen hinsichtlich der Vollständigkeit der abgedeckten Sicherheitsaspekte und der Flexibilität bezüglich der projektweiten wie auch jeweils lokalen Instanziierung erwartet werden können.

Bei der Verwendung eines entsprechend dokumentierten Security-Frameworks ergibt sich der Vorteil, dass die an der Umsetzung und am Betrieb beteiligten Personen, auch wenn sie überwiegend selbst keine Sicherheitsexperten sind, einen möglichst umfassenden Überblick über die relevanten Sicherheitsaspekte bekommen und dieses Wissen auch gezielter an die Benutzer weitergeben können. Im Idealfall würden sich gegenüber der dargestellten Ist-Situation folgende ausgewählte Aspekte beim Einsatz eines Security-Frameworks ändern:

- Die Modularität und Anpassbarkeit ermöglichen das bewusst erst spätere Ergänzen zusätzlicher Sicherheitsmechanismen über bereits berücksichtigte Schnittstellen. Beispielsweise ist der Nutzerkreis in der aktuellen Projektphase noch vergleichsweise klein, sodass weder die Benutzer selbst noch deren Heimatorganisationen großen Anstoß an den fehlenden Datenschutzkonzepten nehmen; allen Beteiligten ist dabei jedoch klar, dass entsprechende Sicherheitsfunktionalitäten für den späteren, nachhaltigen Betrieb mit einer wesentlich größeren Nutzermenge zwingend erforderlich sind. Um zu vermeiden, dass dazu unter anderem das gesamte Benutzerverwaltungskonzept umgestellt werden muss, würde das Security-Framework beispielsweise die Möglichkeit bieten, entsprechende Schutzmechanismen zu einem beliebigen späteren Zeitpunkt in die Datenaustauschprozesse einzuschleifen, da es die entsprechenden funktionalen Anforderungen bereits berücksichtigt hat.
- Die resultierende Architektur und ihr Management sind einerseits erkennbar strukturiert und vergleichbar mit den Lösungen, die in anderen Grid-Projekten eingesetzt werden, und andererseits über Standardschnittstellen in die jeweils lokalen Sicherheitsmanagementprozesse integriert. Aus Betreibersicht ergibt sich daraus der Vorteil, dass keine besondere Behandlung der DEISA-Komponenten mehr erforderlich ist und entsprechende Managementtätigkeiten einfacher von den anderen, dafür thematisch zuständigen Arbeitsgruppen bei den einzelnen DEISA-Sites übernommen werden können. Die Orientierung an Frameworks und gemeinsamen Konzepten kann zudem helfen, die Abläufe sicherheitsrelevanter Aktivitäten aus Benutzersicht zu vereinheitlichen, sodass nicht mehr pro genutzter Grid-Infrastruktur verschiedene Vorgehensweisen notwendig sind; allerdings verbleiben bezüglich der Benutzbarkeit unabhängig von den Sicherheitsaspekten die Schwierigkeiten, die sich aus dem Einsatz verschiedener Middleware-Implementierungen ergeben.

- Es sind Reporting-Schnittstellen vorhanden, die sowohl DEISA-weit als auch bei jeder DEISA-Site intern genutzt werden können, um objektive, quantitative Informationen zur aktuellen Sicherheitslage zu erhalten. Insbesondere müssen die entsprechenden Konzepte nicht von Grund auf neu überlegt werden, sondern es kann auf für das Umfeld geeignete, bereits definierte Metriken zurückgegriffen werden, deren Semantik im Hinblick auf die korrekte Interpretation und Ableitung von notwendigen Korrekturmaßnahmen bekannt ist.

Das modulare Security-Framework kann darüber hinaus gerade bei der Aufnahme weiterer Sites in den DEISA-Verbund als Checkliste verwendet werden, in der verpflichtende und optionale Sicherheitsmaßnahmen gebündelt zusammengefasst sind; das Framework dient damit auch als Basis für die DEISA-Sicherheitsdokumentation, die in dieser Form bisher nicht existierte.

3.4.4. Ableitung und Diskussion von Anforderungen aus dem Grid-Szenario

Aus den Charakteristika des Szenarios, der geschilderten Ausgangssituation und der Analyse möglicher Ansatzpunkte zur Verbesserung ergeben sich unter Berücksichtigung des Soll-Zustands verallgemeinert folgende weitere **funktionale Anforderungen**:

- Die vom Security-Framework vorgesehenen Maßnahmen, Komponenten und Workflows müssen dem gegebenen Anspruch an eine möglichst weitgehende Automatisierung gerecht werden [**SF-FUNK-Automatisierung**]; offensichtlich wäre der Anreiz für die Einführung einer Lösung, die in einigen Bereichen einen deutlich höheren manuellen administrativen Aufwand erforderlich macht, gering.
- Trotz der engen organisationsübergreifenden Zusammenarbeit muss vom Security-Framework berücksichtigt werden, dass weder die Autarkie einzelner Organisationen gefährdet noch zu großzügig bei der gemeinsamen Nutzung von sicherheitsrelevanten, internen Daten vorgegangen werden darf [**SF-FUNK-Abschottung**]. Das Frameworkdesign und die von ihm vorgegebenen Komponenten müssen entsprechend darauf ausgelegt sein, dass die im Szenario betrachtete, gemeinsam betriebene Infrastruktur die ihre zugrunde liegende Organisationsstruktur adäquat berücksichtigt.

An **Integration und Betrieb** ergeben sich folgende zusätzliche Anforderungen:

- Einzelne, zunächst bewusst nicht verwendete Module des Frameworks sollen zu einem späteren Zeitpunkt in das szenarienspezifisch angepasste Framework aufgenommen werden können, ohne dass hierfür der gesamte Customizing-Prozess erneut vollständig durchlaufen werden muss [**SF-INT-Ausbauphasen**]. Dies setzt abschwächend voraus, dass sich die szenarienspezifischen Anforderungen zwischen den Ausbauphasen nicht grundlegend ändern.
- Dasselbe Framework muss an die heterogenen Infrastrukturen der jeweiligen Einsatzorte angepasst werden können [**SF-INT-Polyinstanziierbarkeit**]. Diesbezüglich muss auch definiert sein, wie stark sich die verschiedenen Einsatzorte voneinander unterscheiden dürfen.
- Das Security-Framework muss berücksichtigen, dass die betrachteten Assets möglicherweise auch von anderen Security-Frameworks geschützt werden, da die eingesetz-

ten Komponenten teilweise auch von anderen Diensten genutzt werden [**SF-INT-Parallelbetrieb**]. Die über DEISA nutzbaren Höchstleistungsrechner stehen beispielsweise überwiegend anderen Benutzern zur Verfügung, die nicht über die DEISA-Infrastruktur darauf zugreifen.

Bezüglich der **Managementabläufe** sind ebenfalls weitere Anforderungen zu berücksichtigen:

- Das Security-Framework muss über ein reines Architekturkonzept hinausgehen, indem es auch Schnittstellen zu den Managementprozessen und organisatorische Abläufe spezifiziert [**SF-MGMT-Prozesse**].
- Für die kontinuierliche Überwachung müssen vom Security-Framework geeignete Metriken definiert oder ausgewählt worden sein [**SF-MGMT-Metriken**]. Auf die Anforderungen an objektive, aussagekräftige und bevorzugt quantitative Metriken bzw. Kennzahlen wird in Kapitel 6 eingegangen.
- Ausgewählte Kennzahlen sollten als Key Performance Indicators ausgezeichnet sein, damit sie beispielsweise in die Spezifikation von Service Level Agreements einfließen können [**SF-MGMT-KPIs**].
- Der Umfang der für das Erzeugen von Berichten bereitgestellten Rohdaten muss für verschiedene Zielgruppen angepasst werden können [**SF-MGMT-Berichtsdetails**]; dabei ist beispielsweise zwischen organisationsinterner und -externer Weiterverarbeitung zu unterscheiden.
- Das Security-Framework soll vorgeben, ob und in welchem Umfang bei seinem Einsatz Schulungen für verschiedene Zielgruppen, z. B. Administratoren, Sicherheitsverantwortliche oder Benutzer, notwendig bzw. sinnvoll sind [**SF-MGMT-Schulungen**].
- Die länderübergreifende Zusammenarbeit ist im Hinblick auf die erforderliche Einhaltung der nationalen gesetzlichen Rahmenbedingungen im Rahmen der bereits beschriebenen Anforderung [SF-MGMT-Compliance] geeignet zu berücksichtigen.

Schließlich ist im Hinblick auf die **Dokumentation** festzuhalten:

- Zur Sicherstellung der Übertragbarkeit auf das eigene Szenario und zur Unterstützung der Überprüfung der dafür erforderlichen Vollständigkeit ist die beim Frameworkdesign angewandte Methodik zur Durchführung der Anforderungsanalyse zu dokumentieren [**SF-DOKU-Anforderungsanalyse**].
- Die zu seiner szenarienspezifischen Anpassung und Realisierung vom Security Framework spezifizierten Methodik soll die einfache Nutzung als Prüfliste ermöglichen, anhand derer der Status der Umsetzung intern und bei Bedarf auch extern überwacht werden kann [**SF-DOKU-Checkliste**].

Für das Szenario ist zudem zu bedenken, dass die meisten Organisationen parallel an mehreren Grid-Projekten beteiligt sind. Da analog zum derzeitigen parallelen Einsatz mehrerer Middleware-Implementierungen davon ausgegangen werden muss, dass in verschiedenen Grid-Projekten unterschiedliche Security-Frameworks zum Einsatz kommen, verstärken sich dadurch die bereits diskutierten Anforderungen an die Schnittstellen und die Interoperabilität zwischen den Frameworkkomponenten.

3.5. Szenario 4: Learning Management Systeme

Learning Management Systeme (LMS) bilden die Basis für eine durchgängige IT-Unterstützung von Lernumgebungen, die klassische Präsenzveranstaltungen ergänzen (engl. *blended learning*) oder sogar vollständig ersetzen können. Im Rahmen der beruflichen Weiterbildung und durch moderne Bildungsparadigmen wie das lebenslange Lernen (vgl. [Graf09]) motiviert werden LMS nicht nur an Schulen und Hochschulen, sondern auch in Unternehmen und von einschlägigen Dienstleistern eingesetzt.

Die Kernaufgaben von LMS liegen dabei einerseits bei der Bereitstellung von Lerninhalten und andererseits bei der Abwicklung von Prozessen im Rahmen des Kurslebenszyklus, also von der Anmeldung der Teilnehmer bis zum Abschluss des Kurses mit einer elektronisch unterstützten Prüfung. Moderne LMS zeichnen sich zum einen durch eine starke Personalisierung, durch die den Benutzern beispielsweise eine auf sie abgestimmte Kursauswahl angeboten wird, und zum anderen durch die Förderung der Kommunikation zwischen und unter Dozenten und Lernenden aus.

In allen genannten Einsatzgebieten ist zu beobachten, dass LMS-Projekte meist mit kleinen Installationen beginnen, die nur wenige Kurse für einen relativ kleinen Kreis potentieller Teilnehmer anbieten. Bei erfolgreichem Einsatz entwickeln sie sich jedoch zügig weiter und entwickeln sich zu organisationsweiten Lösungen, die einen entsprechend größeren Teilnehmerkreis haben. Durch den Einsatz von Lernmaterial, das kommerziell von Dritten bereitgestellt wird, und die zunehmende organisationsübergreifende LMS-Nutzung ergeben sich rasch neue Anforderungen im Bereich der IT-Sicherheit. Hinzu kommt, dass LMS-Benutzer relativ häufig bereit dazu sind, Schwachstellen im System zu ihren Gunsten auszunutzen, um beispielsweise zu verhindern, dass sich schlechte Prüfungsergebnisse negativ auf ihre weitere Laufbahn auswirken [Gra02].

Dieses Szenario demonstriert somit zum einen Herausforderungen, die sich aus dem starken Wachstum der Infrastruktur und ihrer Öffnung für weitere Nutzergruppen ergibt, und zum anderen die Besonderheit, dass reguläre wie auch privilegierte Benutzer zu den vorrangig zu berücksichtigenden Angreifern gehören.

3.5.1. Darstellung der Ist-Situation im LMS-Szenario

Wie bei den anderen Szenarien erfolgt zunächst die Einordnung anhand der Szenariencharakteristika; im Anschluss werden die für LMS relevanten technischen Dienste skizziert und die im LMS-Umfeld typischerweise eingesetzten Sicherheitsmaßnahmen erläutert.

3.5.1.1. Szenariencharakteristika

Im Szenario wird genau *eine Organisation* betrachtet; selbst bei der organisationsübergreifenden LMS-Nutzung sind die beteiligten Einrichtungen i. A. nur lose miteinander gekoppelt und können unabhängig voneinander analysiert werden. Die Sicherheitsverantwortung liegt dabei prinzipiell *zentral* beim LMS-Betreiber. Im Folgenden wird der Einsatz von *2–3 Security-Frameworks* diskutiert, die verschiedene LMS-Teilaspekte und -Subdienste abdecken.

Aufgrund der umfassenden Personalisierung und der Möglichkeit, elektronische Prüfungen abzulegen und deren Ergebnisse zu verwalten, werden von LMS sensible personenbezogene Daten

Charakteristikum	Ausprägung		
Anzahl Organisationen	0	1	n
Sicherheitsverantwortung	dezentral	hierarchisch	zentral
Anzahl Security-Frameworks	1	2-3	mehr als 3
Personenbezogene Daten	keine	Kontaktdaten	Profildaten
Kontrollen / ext. Vorgaben	keine	intern	extern
Dynamik	statisch	evolutionär	dynamisch
Benutzerkreis	klein, geschl.	groß, geschl.	offen
Angreifermodelle	wenige	viele, bekannte	viele, spezifische
Infrastruktur/Prozesse	Neuaufbau	ohne Prozesse	Prozessorientiert
Interne Abhängigkeiten	vernachlässigbar	gegeben	stark

Abbildung 3.17.: Charakterisierung von Szenario 4

in der Kategorie *Profildaten* verarbeitet. Aus diesem Grund unterliegen LMS-Installationen typischerweise *internen* Kontrollen, beispielsweise bezüglich der Einhaltung von Datenschutzauflagen, wohingegen von Externen durchgeführte Revisionen bisher unüblich sind. Allgemein ist von einem *großen, geschlossenen* Benutzerkreis auszugehen.

Die meisten LMS-Produkte arbeiten web-basiert und sind für ihre Anwender über das Internet zugänglich; entsprechend müssen zahlreiche, insbesondere auch die oben angedeuteten *spezifischen* Angreifermodelle berücksichtigt werden. Bei vielen aktuellen LMS-Installationen ist festzustellen, dass die Initiative zum LMS-Einsatz und ihre Initialkonfiguration von Personenkreisen ausging, die stark an den didaktischen und funktionalen Aspekten der LMS-Software interessiert sind, aber auf Sicherheitseigenschaften nur sekundär eingehen. Entsprechend finden sich zwar häufig die von LMS-Architekturen vorgesehenen technischen IT-Sicherheitsmaßnahmen, aber der Betrieb wird *ohne sicherheitsspezifische Prozesse* abgewickelt. Schließlich ist festzuhalten, dass die hier betrachteten Teildienste *stark voneinander abhängig* sind. Abbildung 3.17 fasst diese Charakterisierung zusammen.

3.5.1.2. Im LMS-Szenario betrachtete Dienste

Abbildung 3.18 zeigt den typischen Aufbau eines organisationsintern eingesetzten LMS, der dem klassischen 3-Tier-Konzept folgt:

- Als *Frontend* dient eine graphische Benutzeroberfläche, die entweder aus einer clientseitig installierten Software („fat client“) oder einem Webserver besteht, der die Lerninhalte an den benutzerseitigen Browser („thin client“) ausliefert, wobei in der Praxis deutlich überwiegend der zweite Ansatz zum Einsatz kommt. Dieses Frontend ist die zentrale Schnittstelle zur Nutzung der gesamten LMS-Funktionalität sowohl für Dozenten als auch Lernende; häufig ist es darüber hinaus auch das primäre Konfigurations- und Verwaltungswerkzeug für LMS-Administratoren.

  Die angebotene Funktionalität unterscheidet sich je nach Benutzergruppe. Beispielsweise können den Lerninteressierten die für sie relevante Kurse angezeigt und die Anmeldung dazu angeboten werden. Bei der Teilnahme an einem Kurs werden der Zugang zu den entsprechenden Lernmaterialien und das Ablegen eigener Inhalte, z. B. der Ergebnisse von Übungsaufgaben, ermöglicht. Ferner stehen Kommunikationswerkzeuge wie digitale

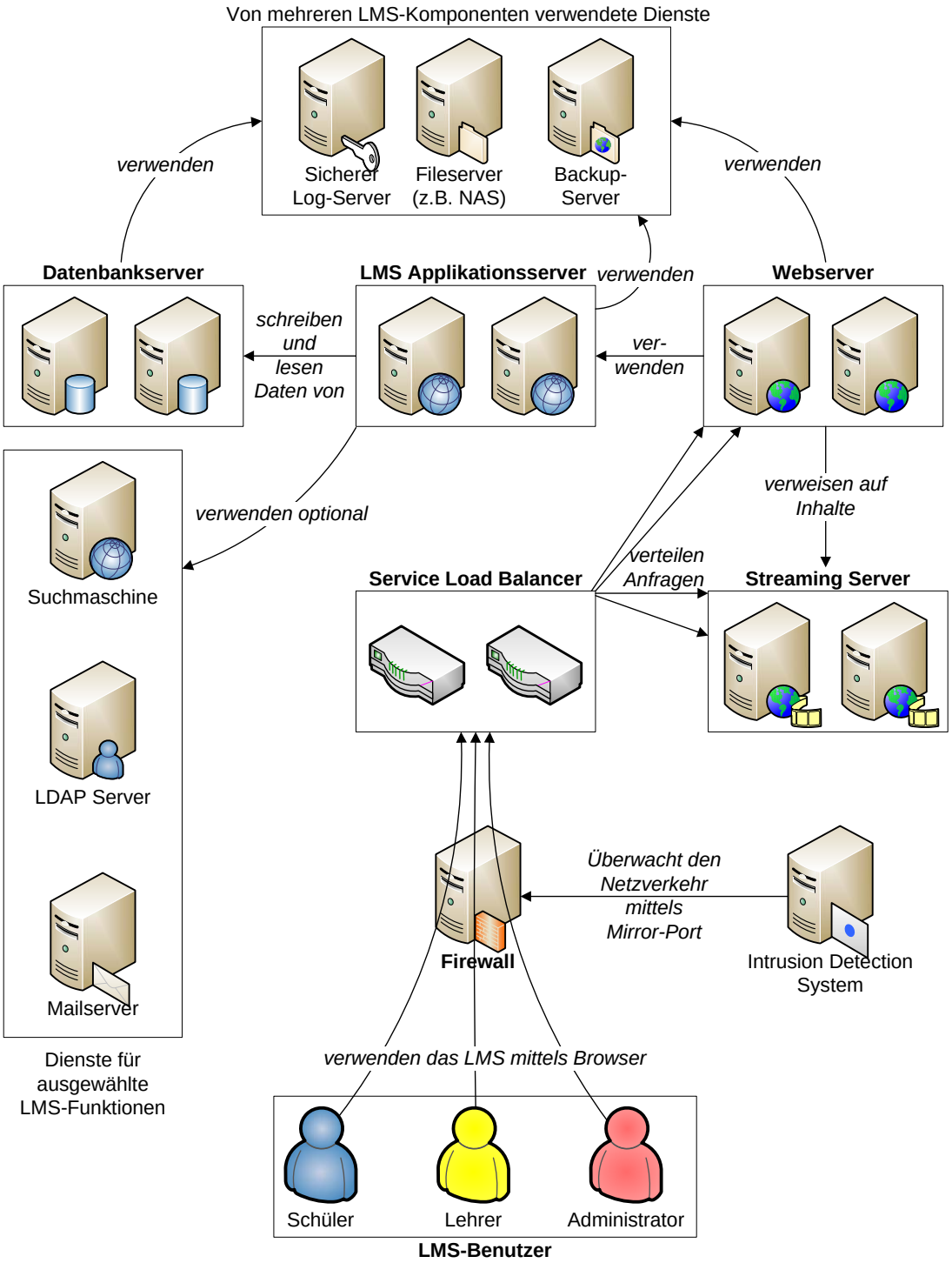


Abbildung 3.18.: Szenario 4: Grundlegende Architektur von LMS-Infrastrukturen

Diskussionsforen zum Austausch mit anderen Lernenden und Funktionen zum Ablegen von Prüfungen („E-Tests“) zur Verfügung.

Für Dozenten und Tutoren werden ergänzend Funktionen zum Einbringen neuer Lernmaterialien sowie zur Zusammenstellung, Vorbereitung und Durchführung von Kursen und Prüfungen angeboten. LMS-Administratoren können schließlich Verwaltungsfunktionen wie das Zuweisen von Rollen und Berechtigungen an Benutzer und die LMS-Konfiguration, beispielsweise im Hinblick auf den genutzten Funktionsumfang und das Design, verwenden.

- Die *Programmlogik* wird bei den meisten LMS-Produkten auf der Basis von Applikationsservern oder Servlet-Containern bereitgestellt, zum Teil sind auch noch herkömmliche CGI-Skripte im Einsatz; aus Sicherheitsperspektive müssen in diesem Komponentenverbund alle auf Anwendungsebene (ISO/OSI-Schicht 7) greifenden Sicherheitsmechanismen implementiert werden, beispielsweise also die Benutzer- und Berechtigungsverwaltung.
- In der *Persistenzschicht* werden sämtliche LMS-bezogenen Daten gespeichert; typischerweise kommen relationale Datenbankmanagementsysteme zum Einsatz, wobei grob zwischen drei Datenkategorien unterschieden werden kann:

  1. Lernmaterial: Da die Konzeption und Umsetzung von Online-Kursen ein nach wie vor aufwendiger Vorgang ist, legen nahezu alle LMS-Autoren Wert auf den Schutz ihres geistigen Eigentums; insbesondere beim Einsatz von kommerziellem Lernmaterial, das von Dritten lizenziert wurde, müssen entsprechende Maßnahmen vorgesehen werden, um ein freies Zirkulieren der Daten zu verhindern. Ähnliche Auflagen gelten beispielsweise im medizinischen Bereich: Aufgrund der Verordnungen zum Patientenschutz dürfen an Universitäten in der Regel Fallbeispiele mit Patientenfotos nur fachlich einschlägigen Personen, aber nicht anderen Interessierten zur Verfügung gestellt werden.
  2. Benutzerdaten: Neben den vollständigen Benutzerkontaktdaten liegen umfassende Informationen über die Vorgeschichte und den Lernverlauf vor; an Hochschulen wird beispielsweise auf Basis der Haupt- und Nebenfächer des gewählten Studiengangs entschieden, welche Online-Kurse wann und unter welchen Voraussetzungen belegt werden können. Ähnlich zu E-Commerce-Webseiten stellt die Benutzerdatenbasis eines LMS somit ein lukratives Angriffsziel dar. Tutoren, Dozenten, Lernmaterialautoren und LMS-Administratoren haben darüber hinaus zusätzliche Berechtigungen. Bei der Vergabe von Berechtigungen an einzelne Benutzer müssen einander gegenseitig ausschließende Rollen berücksichtigt werden; beispielsweise sollte ein Dozent nicht an einem von ihm selbst erstellten E-Test teilnehmen und dafür Punkte oder Zertifikate bekommen können.
  3. Metadaten: Vereinfachend werden alle Daten, die nicht einer der beiden anderen Kategorien zugeordnet werden können, als Metadaten bezeichnet; sie umfassen beispielsweise die LMS-Konfiguration, die auch das äußere Erscheinungsbild festlegt und entsprechend gegen unerwünschte Änderungen geschützt werden muss.

Größere LMS-Installationen machen von diversen weiteren Diensten Gebrauch, die zumindest zum Teil in der jeweiligen Infrastruktur der Organisation bereits vorhanden sein können:

- *Streaming-Server* verteilen Multimedia-Lernmaterial so an die Clients, dass es bereits während des Transfers wiedergegeben werden kann; zudem kann der Benutzer Teilinhalte überspringen, die ihn nicht interessieren und die folglich zur Einsparung von Server- und Netzressourcen nicht an den Client übertragen werden.
- Mittels *E-Mail-Server* können die LMS-Benutzer über Ereignisse wie die Verfügbarkeit neuer Lernmaterialien oder die Möglichkeit zur Prüfungsanmeldung informiert werden.
- Spezielle *Suchmaschinen* können das Durchforsten umfassender Kursunterlagen gezielt unterstützen; beispielsweise sind in Fachbereichen wie Medizin oder Architektur umfangreiche Bilddatenbanken verfügbar, die anhand von Schlagworten, die in die Bild-Metadaten integriert sind oder mittels Bilderkennungsalgorithmen auffindbar sein sollen.
- Zur Authentifizierung der Benutzer und für den Import von Benutzerdatensätzen können von vielen LMS-Produkten die organisationsinternen *Identity & Access Management Systeme* verwendet werden, auf die beispielsweise mit dem Protokoll LDAP zugegriffen wird.

Zur Ausfallsicherheit und zur Lastverteilung werden in der Regel *Service Load Balancer* eingesetzt; da somit mehrere Maschinen dieselbe Aufgabe übernehmen (z. B. Webserver-Farm), müssen die von ihnen benötigten Nutzdaten beispielsweise über zentrale Dateiserver bereitgestellt werden. Analog dazu werden protokollierte Informationen meist zentral aggregiert, um die Auswertung zu vereinfachen.

Da ein LMS somit ein komplexes verteiltes System ist, dessen Aufbau und Betrieb für kleinere Organisationen häufig zu aufwendig ist, gewinnt das zentrale Hosting von LMS-Infrastrukturen zunehmend an Bedeutung. Auch diverse Drittanbieter kommerzieller Lernmaterialien bevorzugen es mittlerweile, die Daten zentral zum Abruf bereitzustellen, um ein unkontrolliertes Zirkulieren besser verhindern zu können. Komplementär dazu existieren vor allem im Hochschulumfeld Bestrebungen, selbst produziertes Lernmaterial auch Studenten anderer Hochschulen zugänglich zu machen, allerdings ohne es dabei komplett aus der Hand zu geben, indem beispielsweise Kopien an andere Dozenten verteilt werden.

In jedem dieser drei neuen Anwendungsbereiche ergibt sich eine Öffnung des lokal betriebenen LMS für externe Nutzer. Neben der Verbreiterung der potentiellen Angriffsfläche stellt sich dabei im Hinblick auf die Benutzer- und Berechtigungsverwaltung die Frage, wie die Benutzerdatensätze externer Anwender effizient ins LMS eingespeist werden können. Technisch wird hierzu verstärkt auf Federated Identity Management (FIM), beispielsweise auf Basis des Standards SAML [CKPH05], gesetzt. Dabei wird jeder Benutzer wie in Szenario 1 erläutert einer als Identity Provider bezeichneten Heimateinrichtung zugeordnet, die sowohl die Authentifizierung des Benutzers für das LMS des Dienstleisters übernimmt als auch die benötigten Benutzerdaten zum Abruf zur Verfügung stellt. Für die LMS-Infrastruktur ergibt sich daraus die Konsequenz, dass Bestandteile wie die Anmeldemaske für Benutzer durch gänzlich andere Verfahren ersetzt bzw. dass verschiedene Zugangsalternativen angeboten werden müssen. Offensichtlich ergeben sich dabei noch zahlreiche weitere, zu berücksichtigende Aspekte, beispielsweise im Bezug auf Datenschutz, die hier nicht näher diskutiert werden; einen grundlegenden Überblick gibt [Homm07, S. 91ff.].

Die Diskussion bereits eingesetzter Sicherheitsmaßnahmen im nächsten Abschnitt setzt die Kenntnis ausgewählter, LMS-spezifischer Angreifermodelle und Angriffe voraus, die nachfol-

gend skizziert werden:

- Benutzer können versuchen, die vorhandenen Zugriffskontrollmechanismen zu umgehen; in [Gra02] wird beispielsweise dargelegt, warum die Bereitschaft von Lernenden, bewusst LMS-Schwachstellen zu ihren eigenen Gunsten auszunutzen, wesentlich höher als bei vielen anderen IT-Diensten ist.

  Tutoren und Dozenten haben zusätzlich Möglichkeiten zur Einsichtnahme in den Lernmaterial- und Benutzerdatenbestand; es muss verhindert werden, dass diese Privilegien über die betreuten Kurse hinausgehen oder zweckentfremdend eingesetzt werden.

- LMS-Administratoren erhalten über dasselbe Frontend Zugang zur administrativen Funktionalität wie Benutzer und werden deshalb in den meisten Produkten ebenfalls nur mit einer simplen Passwortüberprüfung authentifiziert. Neben kompromittierten Administratorkennungen stellt auch der bewusste Missbrauch der administrativen Berechtigungen, z. B. um einzelne Benutzer auszuspähen, ein Risiko dar, da es sich um Personendaten handelt, die sonst nur im eingeschränkten Kreis der Personalverwaltung oder der Prüfungsverwaltung von Hochschulen verarbeitet werden.

Abgeleitet aus der Risikoanalyse in [vS05] sind insbesondere die folgenden LMS-spezifischen Angriffe festzuhalten:

- *Unautorisierter Zugriff auf Lernmaterial*: Ein Aushebeln des Zugriffsschutzes kann dazu führen, dass der Angreifer lesenden Zugriff auf Lernmaterial erhält, den er nicht oder noch nicht haben sollte. Ist sogar schreibender Zugriff möglich, sind beispielsweise subtile Änderungen am Lernmaterial, deren völliges Entstellen in Analogie zum „Defacement“ von Webseiten oder das Vernichten der Daten möglich.

- *Unautorisierter Zugriff auf Inhalte, die von anderen Benutzern eingespielt wurden*: Hierunter fällt das Kopieren, Manipulieren oder Löschen beispielsweise von Lösungen zu Übungsaufgaben, die ein anderer Benutzer zur Beurteilung durch Tutoren bzw. Dozenten eingereicht hat.

- *Unautorisierter Zugriff auf Prüfungsunterlagen und -ergebnisse*: Viele LMS unterstützen die Durchführung von Online-Prüfungen, an denen jedoch häufig nur von dedizierten Rechnerpools aus teilgenommen werden kann, um die Identitäten der Geprüften leichter verifizieren und die Umgebung z. B. im Hinblick auf erlaubte Hilfsmittel besser kontrollieren zu können. Offensichtlich darf der Prüfungsinhalt nicht vor Beginn der Prüfung zugänglich sein; analog dazu müssen Prüfungsergebnisse gegen nachträgliche Manipulation geschützt und der Personenkreis, der individuelle Prüfungsergebnisse einsehen darf, eingeschränkt werden.

- *Unautorisierter Zugriff auf Benutzerdaten*: Ein für die Benutzerakzeptanz sehr wichtiger Faktor ist, dass sorgfältig mit personenbezogenen Daten umgegangen wird. Nach [EvSS06] leiden Glaubwürdigkeit und Ruf einer Organisation nachhaltig unter Datenschutzvorfällen, zumal auch ein Beheben der zugrundeliegenden Verwundbarkeit das Ausspähen der Daten nicht ungeschehen machen kann.

Schließlich ist zu berücksichtigen, dass auch LMS-spezifische Varianten von Denial-of-Service-Angriffen gegen die gesamte Infrastruktur oder ausgewählte Komponenten existieren; beispielsweise könnte ein Angreifer erreichen wollen, den Termin für eine Online-Prüfung aufzu-

schieben, indem das LMS zum Prüfungszeitpunkt überlastet wird, sodass die Prüfungsteilnehmer nicht damit arbeiten können.

3.5.1.3. Im LMS-Szenario bisher eingesetzte Sicherheitsmaßnahmen

In diesem Abschnitt werden die Sicherheitsmaßnahmen skizziert, die sich in einer exemplarischen LMS-Infrastruktur finden. Auf **technischer Ebene** werden zunächst grundlegend die Kommunikationspfade über Firewalls kanalisiert und eingeschränkt sowie die automatische Softwareaktualisierung für Betriebssysteme aktiviert. Auf den Webserver kann von den Clients nur verschlüsselt über HTTPS zugegriffen werden und alle Protokolleinträge werden an einen zentralen Logserver übermittelt, der nur das Hinzufügen neuer Einträge, aber kein Bearbeiten oder Löschen alter Einträge erlaubt. Alle Dienste werden zudem auf dedizierten (virtuellen) Maschinen erbracht und sind somit voneinander isoliert. Zur Erkennung akuter Angriffe wird ein beim Betreiber bereits vorhandenes Intrusion Detection System mitgenutzt.

Für die Zugriffskontrolle wird RBAC verwendet, wobei zwischen den Rollen Lernender, Tutor, Dozent, Autor und Administrator unterschieden wird. Die Rollen werden mit Ausnahme der global gültigen Administratorrolle mit den einzelnen Kursen parametrisiert, sodass der Dozent eines Kurses gleichzeitig Lernender in einem anderen Kurs sein kann, ohne diesen ebenfalls als Dozent verwalten zu können. Zudem kann pro Kurs nur eine Rolle übernommen werden, sodass sich gegenseitig ausschließende Rollen nicht explizit modelliert werden müssen.

E-Mails, die personalisierte Benachrichtigungen wie die Zulassung zu einem Kurs enthalten, werden elektronisch signiert, um sie einerseits für den Empfänger als offizielle Mitteilung erkennbar zu machen und sie andererseits gegen Manipulation zu schützen; damit wird verhindert, dass sich Lernende mit gefälschten E-Mails z. B. an die Dozenten wenden, nachdem sie eine automatische Absage zur Teilnahme an einem Kurs durch Bearbeiten des Textes in eine Zusage verwandelt haben.

Auf **organisatorischer Ebene** sind im Beispiel lediglich rudimentäre Maßnahmen getroffen worden, da funktionale Aspekte und didaktische Konzepte im Vordergrund stehen und die LMS-Infrastruktur bislang von größeren Sicherheitsvorfällen verschont geblieben ist. Beispielsweise sind redundante Serverkapazitäten vorhanden, die sowohl Lastspitzen als auch primitive Denial-of-Service-Angriffe abfangen können; die Daten aller Teildienste werden durch ein gemeinsames Backupkonzept gegen Verlust durch Defekte gesichert. Für Lernende, Tutoren und Dozenten wurden Benutzungsrichtlinien festgelegt, denen Lernende vor der ersten Nutzung des Dienstes elektronisch und Tutoren sowie Dozenten schriftlich zustimmen müssen.

Prozesse, die über die Prävention von sicherheitsrelevanten Vorfällen hinausgehen, beispielsweise wann, von wem und in welchem Umfang betroffene Benutzer bei einem Vorfall informiert werden, und welche Recovery-Workflows durchzuführen sind, wurden hingegen noch nicht spezifiziert.

3.5.2. Herausforderungen und Ansatzpunkte zur Optimierung

Wie in vielen anderen Bereichen ist auch bei vielen LMS-Infrastrukturen zu beobachten, dass sich die Betreiber nicht primär und nicht im Detail mit den Sicherheitsaspekten beschäftigen können. Im Hinblick auf die organisationsweite Gesamtsicherheitslage werden die LMS

häufig nur am Rande berücksichtigt, da beispielsweise öffentliche Webserver und Geschäftsanwendungen höher priorisiert werden als Lernumgebungen. Dabei wird leicht übersehen, dass erfolgreiche Angriffe auf die LMS-Infrastruktur, bei denen Daten ausgespäht oder manipuliert werden, weitreichende Konsequenzen haben können.

Vielen aktuellen LMS-Infrastrukturen liegt kein modular aufgebautes Sicherheitskonzept zugrunde, das auf Weiterentwicklungen in den einzelnen Bereichen Intellectual Property Management, Identity & Access Management und web-basierte Serviceinfrastruktur möglichst unabhängig voneinander reagieren kann. Änderung führen somit häufig zu tiefen Eingriffen in die Systemarchitektur, die durch die Notwendigkeit, die Kompatibilität mit früheren Verfahren zumindest übergangsweise noch beizubehalten, noch komplexer werden.

Hauptmanko ist jedoch die sehr technikzentrierte Betrachtung der IT-Sicherheit, die zudem über die Prävention und Detektion von Angriffen nicht hinausgeht. So fehlen im geschilderten Beispiel einerseits proaktive Maßnahmen, durch die potentielle Verwundbarkeiten entdeckt werden könnten, bevor Angriffe durchgeführt werden. Andererseits sind die Reaktionen auf erfolgreiche Angriffe bzw. massive Angriffsversuche nicht definiert; bei akuten Angriffen kann es deshalb leicht zu unkoordinierten und falschen Reaktionen kommen.

Schließlich werden zwar üblicherweise LMS-Nutzungsstatistiken angefertigt, ein sicherheitsbezogenes Berichtswesen existiert hingegen im LMS-Umfeld bisher nur selten. Damit können Fragen nach dem Sicherheitsniveau der LMS-Infrastruktur nicht quantitativ beantwortet werden, sodass Entscheidungen über die Priorisierung weiterer Sicherheitsmaßnahmen anhand anderer Kriterien getroffen werden müssen.

3.5.3. Durch Security-Frameworks zu erwartender Mehrwert

Bisher existieren keine umfassenden, LMS-spezifischen Security-Frameworks. Um zu zeigen, dass dennoch kurzfristig Vorteile aus dem Einsatz von Security-Frameworks gezogen werden können, wird nachfolgend davon ausgegangen, dass in den drei Bereichen Lizenzmanagement, Benutzer- und Berechtigungsverwaltung sowie web-basierte Benutzeroberfläche jeweils darauf spezialisierte Security-Frameworks eingesetzt werden, die an den konkreten Bedarf eines LMS-Szenarios, insbesondere also auch die spezifischen Angriffsarten, angepasst werden.

Aus Betreibersicht ergibt sich erneut der Vorteil, nicht für alle an der LMS-Infrastruktur beteiligten Komponenten von Grund auf neue Sicherheitskonzepte aufstellen zu müssen; vielmehr werden die technischen Maßnahmen, die für ein brauchbares Sicherheitsniveau erforderlich sind, vorgegeben. Durch die Aufteilung der Infrastruktur in verschiedene Bereiche, die von dedizierten Security-Frameworks abgedeckt und über Schnittstellen miteinander verbunden sind, ergibt sich die gewünschte Möglichkeit, jeweils nur genau die zum jeweiligen Framework gehörenden Komponenten weiterzuentwickeln, ohne tief in die gesamte Infrastruktur eingreifen zu müssen. Für dabei getroffene Designentscheidungen liegen im Idealfall auch für das Szenario gültige Begründungen vor, ansonsten können bei Bedarf Anpassungen vorgenommen werden.

Gerade in einem sich weiterentwickelnden Szenario ergibt sich aus der damit schritthaltenden Verbesserung der Security-Frameworks der Vorteil, dass ein Bewusstsein dafür geschaffen wird, dass das Deployment von Sicherheitsmechanismen keine einmalige Maßnahme ist, sondern nachhaltigen Betriebs- und Anpassungsaufwand erfordert.

Produktive LMS-Infrastrukturen, in denen reale Kurs- und Personendaten verarbeitet werden, sind offensichtlich keine geeignete Testumgebung für Experimente mit neuen Sicherheitskonzepten; Security-Frameworks tragen diesbezüglich durch die Berücksichtigung der mit ihrem Einsatz gemachten praktischen Erfahrungen in neuen Versionen zur Stabilität im operativen Betrieb bei. Insbesondere kann bei Security-Frameworks, die aus den industriellen und privatwirtschaftlichen Bereichen stammen – wie im Szenario beispielsweise für Lizenzmanagement weit verbreitet – bei Bedarf auch auf professionelle Unterstützung zurückgegriffen werden, wenn Probleme nicht intern gelöst werden können.

3.5.4. Ableitung und Diskussion von Anforderungen aus dem LMS-Szenario

Die anderen Szenarien ergänzend ist die folgende **funktionale** Anforderung festzuhalten:

- Das Security-Framework muss beispielsweise bezüglich Schwellenwerten für die Erzeugung von Sicherheitsalarmen die sich ändernden Benutzerzahlen und sich im Laufe der Zeit wandelndes Nutzungsverhalten berücksichtigen [**SF-FUNK-Adaptivität**].

Im Bereich der **Integrations- und Betriebsanforderungen** ergibt sich aus dem Szenario die folgende Ergänzungen:

- Im Rahmen des Anpassungsprozesses müssen das zur jeweiligen Ausbaustufe des Frameworkeinsatzes im Szenario gehörende Umfeld mit den daraus resultierenden Angreifermodellen berücksichtigt werden [**SF-INT-Umfeld**].

Auch hinsichtlich der **Managementschnittstellen und -prozesse** ergeben sich zusätzliche Anforderungen:

- Eingesetzte Security-Frameworks müssen aktiv weiterentwickelt werden, um die sich verändernden Anforderungen und technischen wie auch organisatorischen Möglichkeiten zu berücksichtigen [**SF-MGMT-Verbesserung**].
- Mit dem einzusetzenden Security-Framework sollte es bereits Erfahrungen in anderen konkreten Szenarien geben, da sich das vorliegende Szenario aufgrund des produktiven Einsatzes nicht für den Pilotbetrieb oder die praktische Evaluation von Security-Frameworks eignet, sondern bewährte Konzepte mit einem entsprechenden Reifegrad erfordert [**SF-MGMT-Praxis**].
- Für den praktischen Einsatz wirkt es sich positiv aus, wenn das Security-Framework nicht nur als kontinuierlich weiterentwickeltes Konzept bereitgestellt wird, sondern auch entsprechender Support dafür geleistet wird [**SF-MGMT-Support**].

Schließlich sind im Hinblick auf die **Dokumentation** von Security-Frameworks die folgenden Anforderungen zu stellen:

- Aus der Dokumentation des Security-Frameworks sollten sein Prozesscharakter klar hervorgehen und seine Anwender zu einer kontinuierlichen verbessernden Auseinandersetzung mit der Thematik angeregt werden [**SF-DOKU-Kontinuum**]. Insbesondere darf nicht der Eindruck erweckt werden, dass ein einmaliges Anpassen und Ausrollen einer auf dem Framework basierenden Architektur eine wartungsfreie Dauerlösung darstellt.

Charakteristikum	Ausprägung		
Anzahl Organisationen	0	1	n
Sicherheitsverantwortung	dezentral	hierarchisch	zentral
Anzahl Security-Frameworks	1	2-3	mehr als 3
Personenbezogene Daten	keine	Kontaktdaten	Profildaten
Kontrollen / ext. Vorgaben	keine	intern	extern
Dynamik	statisch	evolutionär	dynamisch
Benutzerkreis	klein, geschl.	groß, geschl.	offen
Angreifermodelle	wenige	viele, bekannte	viele, spezifische
Infrastruktur/Prozesse	Neuaufbau	ohne Prozesse	Prozessorientiert
Interne Abhängigkeiten	vernachlässigbar	gegeben	stark

Abbildung 3.19.: Zusammenfassung der behandelten Szenariencharakteristika

- Die Vollständigkeit der vom Security-Framework geschaffenen Lösung und die bekannten nicht abgedeckten Aspekte sollten explizit dokumentiert sein, um das gegebenenfalls notwendige Heranziehen weiterer Sicherheitsmaßnahmen gezielt zu unterstützen [**SF-DOKU-Vollständigkeit**].
- Die beim Frameworkdesign getroffenen Entscheidungen sollten durch geeignete Dokumentation nachvollziehbar sein [**SF-DOKU-Designentscheidungen**].

Diese Anforderungen schließen die Analyse von Szenarien ab. Im folgenden Abschnitt werden weitere Anforderungen zusammengestellt, die aus den Standards im Umfeld des IT-Sicherheitsmanagements und aus verwandten Arbeiten abgeleitet werden können.

3.6. Ergänzung der Anforderungsaufstellung

Abbildung 3.19 zeigt erneut die Schablone für Szenariencharakteristika, wobei alle Ausprägungen, die – wenngleich aufgrund der Anzahl möglicher Kombinationen nicht in allen Variationen – in den vier analysierten Szenarien angesprochen wurden, grau hinterlegt sind. In der Szenarienzusammenstellung bewusst ausgelassen wurden die drei folgenden Aspekte:

1. Szenarien, an denen *keine Organisation*, sondern lediglich Einzelpersonen beteiligt sind, wurden nicht berücksichtigt, da in diesen die für diese Arbeit im Vordergrund stehenden Integrations- und Managementaspekte üblicherweise weniger stark ausgeprägt sind.
2. Szenarien, in denen *keine personenbezogenen Daten* verarbeitet werden, stellen in der Regel eine Vereinfachung gegenüber den hier analysierten Szenarien dar, sodass die resultierenden Anforderungen dort entsprechend geringer gewichtet werden können. Eine Ausnahme sind Szenarien, in denen die anonyme Nutzung einen wichtigen Mehrwert darstellt; in diesem Fall sind die entsprechenden Anforderungen durch höhere Gewichtung zu betonen.
3. *Statische Szenarien* sind im Allgemeinen als Vereinfachung von dynamischen Szenarien aufzufassen und wurden deshalb nicht exemplifiziert. Eine Ausnahme stellen jedoch Szenarien dar, deren geringe Dynamik nicht inhärent, sondern eine Folge ist, beispielsweise aufgrund eines hohen Verteilungsgrads und mit jeder Änderung verbundenen hohen

Kosten. In diese Kategorie fallen beispielsweise Security-Frameworks, die sich mit sicherer IT-Unterstützung des Gesundheitswesens auf landesweiter Ebene auseinandersetzen (E-Health). Dabei ergeben sich einige weitere Anforderungen:

- Die bisherige und die neue, security-framework-basierter Architektur müssen während einer längeren Übergangsphase parallel betrieben werden können; dabei handelt es sich um eine Sonderform der bereits diskutierten Anforderung [SF-INT-Parallelbetrieb].
- Das Framework muss darauf ausgelegt sein, dass an der resultierenden Architektur und bei den sie nutzenden Entitäten keine Änderungen schneller erforderlich sein dürfen als es logistisch möglich ist [**SF-MGMT-Releasezyklus**]; beispielsweise wäre auch ein Rollback nach einem fehlgeschlagenen Deployment nur mit unvertretbar hohem Aufwand verbunden.

In Anlehnung an die Vorgaben an IT-Sicherheitsmanagementprozesse, wie sie in Abschnitt 2.1.2 diskutiert wurden, sind ferner die folgenden Anforderungen zu berücksichtigen, die prinzipiell szenarienübergreifend gelten:

- Die Berührungspunkte zwischen den Sicherheitsrichtlinien (auf Organisationsebene) und dem Security-Framework müssen spezifiziert sein. Zum einen müssen also Schnittstellen zur Umsetzung der für den jeweils betrachteten Dienst relevanten Policies vorhanden sein, zum anderen sollten vom Frameworkkonzept Anregungen geliefert werden, welche neuen Aspekte in den Policies berücksichtigt werden sollten [**SF-MGMT-Policies**].
- Vom Frameworkkonzept sollten Vorschläge bezüglich der Verantwortlichkeiten und Zuständigkeiten für die einzelnen Frameworkkomponenten sowie die definierten Managementprozesse, beispielsweise auf Basis eines allgemein bekannten Rollenmodells (vgl. Abschnitt 2.2.1) gemacht werden [**SF-MGMT-Zuständigkeiten**].
- Aussagen zu im Frameworkkonzept diskutierten Sicherheitseigenschaften und Metriken, die u. a. als Grundlage für das Security-Reporting dienen, sollten möglichst quantitativ und nicht nur qualitativ sein [**SF-MGMT-Quantifizierung**].
- Um beurteilen zu können, ob ein Security-Framework erfolgreich an ein Szenario angepasst und anschließend in Betrieb genommen wurde, sind Kriterien, anhand derer das Erreichen der angestrebten Ziele gemessen und beurteilt werden kann, zu definieren [**SF-DOKU-Beurteilung**]. Damit muss insbesondere verhindert werden, dass ein Security-Framework zwar als grobe Anregung dient, sich die Umsetzung jedoch zu weit von den ursprünglichen Konzepten entfernt.

Wie in Kapitel 4 gezeigt wird, decken viele aktuelle Security-Frameworks nicht alle Lebenszyklusphasen ab, sondern fokussieren sich überwiegend auf das Architekturdesign, wohingegen Anpassungs- und Einführungsprozesse weniger und Aspekte des operativen Betriebs bis hin zur Außerbetriebnahme nur am Rande betrachtet werden. Um diese Einschränkungen, die einen entsprechend höheren konzeptionellen Aufwand in konkreten Szenarien mit sich bringen, effizient handhaben zu können, wird an die Dokumentation die Anforderung gestellt, dass die vom Konzept abgedeckten Lebenszyklusphasen benannt werden [**SF-DOKU-Lifecyclephasen**].

Abschließend wird der insbesondere im Security Engineering betonte Aspekt, dass bei allen technischen Sicherheitslösungen auch der Faktor Mensch berücksichtigt werden muss, unter

dem Schlagwort Benutzerfreundlichkeit als Anforderung festgehalten [**SF-INT-Usability**]. Sie erstreckt sich sowohl über die Handhabung des Frameworkkonzepts selbst, beispielsweise bezüglich der spezifizierten Vorgehensweise bei der Frameworkanpassung, als auch über die Nutzung framework-spezifischer Komponenten durch Benutzer und Administratoren. Die diesbezügliche Beurteilung eines Security-Frameworks ist jedoch zwangsweise hochgradig szenarienspezifisch und subjektiv.

3.7. Gewichtung und Katalogisierung der Anforderungen

Bereits die Anzahl der insgesamt ermittelten Anforderungen legt nahe, dass diese nicht alle gänzlich unabhängig voneinander sind; andererseits wurde auf eine Untergliederung in Teilaspekte bewusst verzichtet, sodass keine strenge Anforderungshierarchie vorliegt. Abbildung 3.20 zeigt deshalb zusammenfassend die Kürzel aller diskutierten Anforderungen und ergänzt diese um ihre gegenseitigen **kategorieübergreifenden Abhängigkeiten**. Diese Einflussnahmen werden nachfolgend insoweit berücksichtigt, als dass das vollständige Erfüllen eines Kriteriums deutlich erschwert wird, wenn verwandte Anforderungen nicht oder nur unvollständig erfüllt sind.

In diesem Abschnitt werden die ermittelten Anforderungen gewichtet und katalogisiert. Dazu wird nachfolgend diskutiert, welche **Bewertungsverfahren** und welche **Gewichte** zum Einsatz kommen, nach welcher Methodik die Gewichtung pro Kriterium festgelegt wird und wie bei der Definition des jeweiligen **Erfüllungsgrads** vorgegangen wird. In Abschnitt 3.7.2 wird anschließend die Gewichtung aller nach ihrer Kategorie sortierten Kriterien vorgestellt. Abschließend werden die Resultate in Abschnitt 3.7.3 zu einem Kriterienkatalog zusammengestellt.

3.7.1. Bewertungsverfahren, Gewichte und Erfüllungsgrade

Für die Beurteilung und den Vergleich von Security-Frameworks wird in dieser Arbeit die klassische **Nutzwertanalyse** (NWA) von Zangemeister [Zang76] verwendet. Sie hat in der Industrie insbesondere im deutschsprachigen Raum eine große Verbreitung gefunden und ermöglicht die objektive Bewertung komplexer Problemstellungen (vgl. [Eng07]). Die für die NWA notwendige Anordnung und Gewichtung der Kriterien kann auf diverse von der NWA abgeleitete bzw. mit ihr verwandte Bewertungsverfahren übertragen werden, sodass der hier resultierende Kriterienkatalog gut als Ausgangsbasis für eigene Szenarien und darin übliche Beurteilungsverfahren und Evaluationsprozesse verwendet werden kann.

Zur Durchführung der NWA werden die Bewertungskriterien zunächst als Baum angeordnet; die vier Kategorien [SF-FUNK], [SF-INT], [SF-MGMT] und [SF-DOKU] bieten sich hierbei offensichtlich als Wurzelknoten der entsprechenden Teilbäume an. Die einzelnen Kriterien bilden darauf aufbauend die Blattknoten des Baums.

Die NWA sieht vor, dass jeder Knoten so gewichtet wird, dass die Summe der Gewichte aller Knoten mit demselben übergeordneten Knoten den Wert 1 ergibt. Dabei wird für jedes Kriterium zwischen seinem *Ebenengewicht* und seinem aus seiner Position im Baum und dem Ebenengewicht ableitbaren *globalen Gewicht* unterschieden: Über das Ebenengewicht wird festgelegt, wie wichtig das Kriterium im Vergleich zu seinen Geschwisterkriterien ist. Das

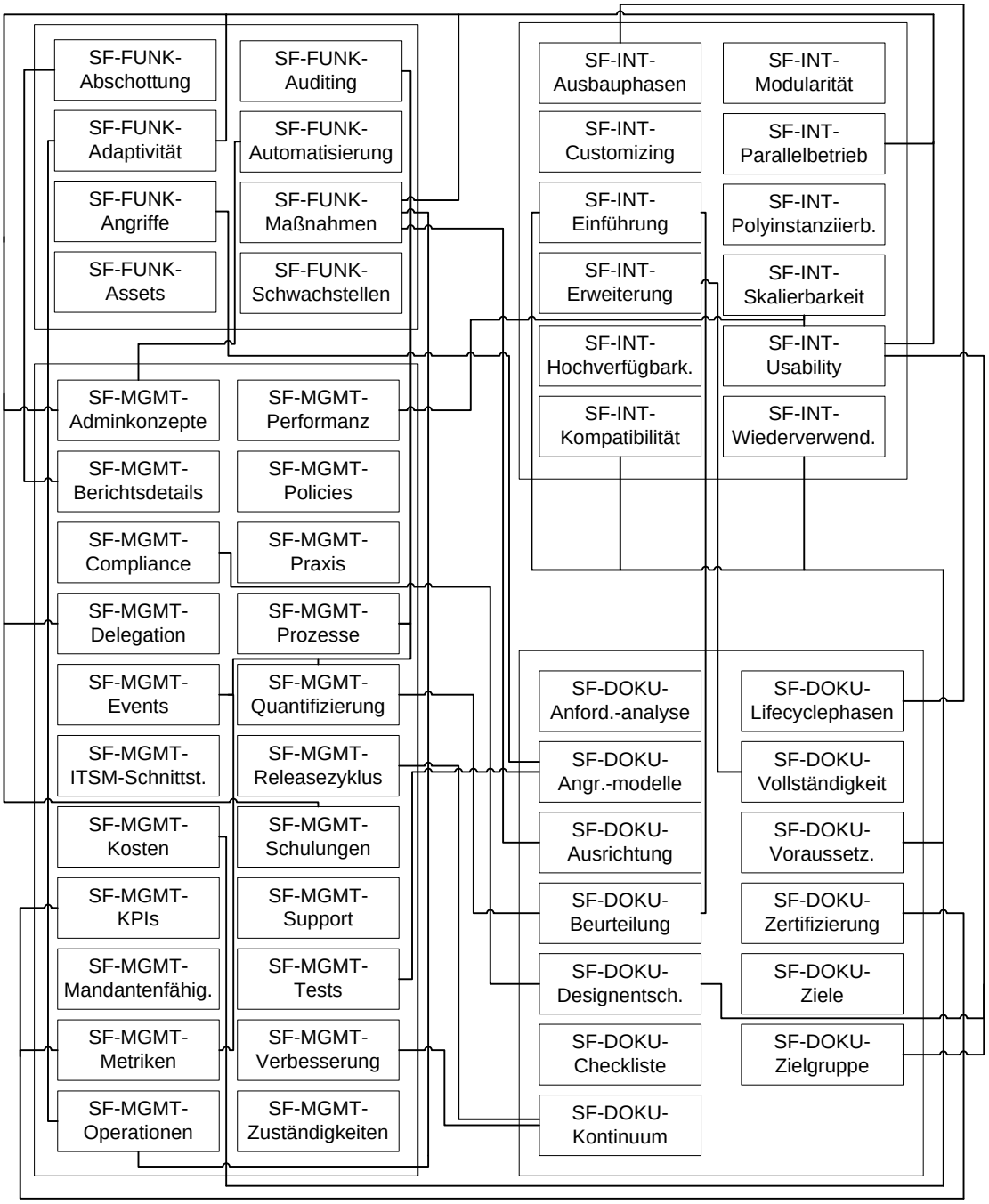


Abbildung 3.20.: Überblick über alle Anforderungen und kategorieübergreifende Abhängigkeiten

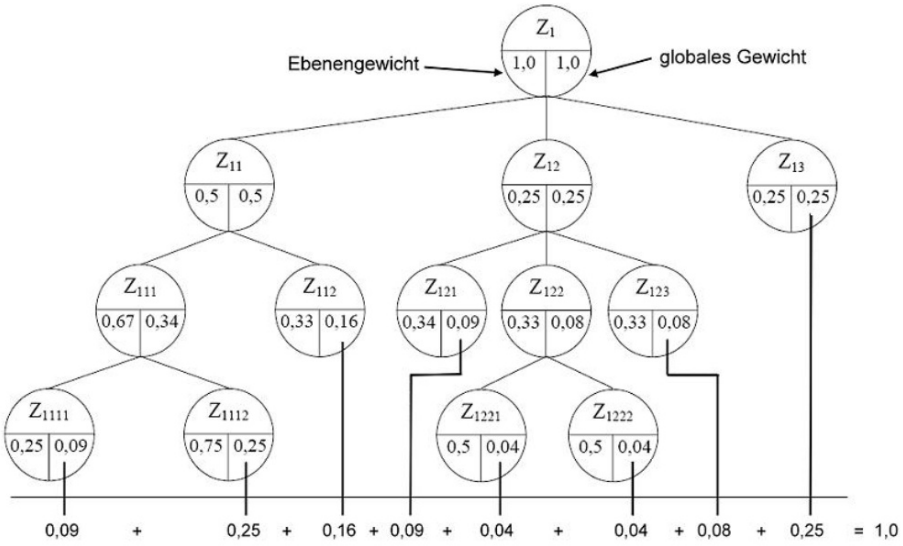


Abbildung 3.21.: Ebenengewichte und globale Gewichte bei der NWA (Quelle: [Bewe01])

globale Gewicht ist das Produkt aller Ebenengewichte entlang des Pfades vom betrachteten Knoten bis zur Wurzel. Abbildung 3.21 zeigt ein einfaches Beispiel, aus dem das Zusammenspiel zwischen Ebenengewichten und globalem Gewicht hervorgeht; die Beispielrechnung zeigt, dass die Summe der globalen Gewichte aller Blattknoten immer den Wert 1 ergibt.

Die Anwendung des mit Gewichten versehenen Baums erfordert, dass der Erfüllungsgrad aller Blattkriterien bewertet wird. Dazu wird jedem Blattkriterium eine Punktezahl zugewiesen, wobei für alle Kriterien dieselbe Punktewertemenge, d. h. eine Bewertung anhand derselben Punkteskala, verwendet werden muss, um Verfälschungen zu vermeiden. Über das Aufsummieren der gewichteten Punktzahlen von den Blättern bis zur Wurzel ergibt sich bei dieser eine gesamtheitliche Punktbewertung des analysierten Security-Frameworks, die den Punktbewertungen anderer untersuchter Security-Frameworks gegenübergestellt werden kann, um eine Rangfolge von Lösungsalternativen zu erhalten.

In dieser Arbeit werden zunächst die folgenden drei qualitativen Gewichtsfaktoren an Kriterien auf Basis der jeweils angegebenen Entscheidungsgrundlage vergeben:

1. **Faktor 1 – wünschenswert**: Sofern die Anforderung nicht erfüllt wird, kann es bei einigen Szenarien zu Einschränkungen kommen, die jedoch entweder toleriert werden können oder zu einem geringfügig höheren Realisierungsaufwand für vorhandene, alternative Lösungswege führen.
2. **Faktor 2 – wichtig**: Das Nichterfüllen einer wichtigen Anforderung beeinträchtigt die allgemeine Eignung des Security-Frameworks spürbar, ist jedoch auf den von ihr abgedeckten Teilbereich beschränkt.
3. **Faktor 4 – essentiell**: Das Nichterfüllen einer essentiellen Anforderung hat breitere Auswirkungen auf die Eignung des Security-Frameworks, da grundlegende Konzepte für den Einsatz und das Management von Security-Frameworks nicht mehr umgesetzt werden können.

Auf Basis der Vorgabe, dass die Ebenengewichte aller Geschwisterkriterien in Summe den Wert 1 ergeben müssen, erfolgt die Abbildung des qualitativen Gewichtsfaktors $F_{i_k} \in [1, 2, 4]$ für die i-te von n_k Anforderungen in der Kategorie $k \in$ [*SF-FUNK, SF-INT, SF-MGMT, SF-DOKU*] auf ihr quantitatives Ebenengewicht E_{i_k} im Anschluss wie folgt:

$$E_{i_k} = \frac{F_{i_k}}{\sum_{j=1}^{n_k} F_{j_k}}$$

Das globale Gewicht G_{i_k} der i-ten Anforderung ergibt sich durch die Aufteilung in die vier Kategorien k entsprechend aus der Multiplikation des Ebenengewichts der Anforderung mit dem Ebenengewicht seiner Kategorie:

$$G_{i_k} = E_{i_k} \cdot E_k$$

Für die szenarienunabhängige Analyse der Security-Frameworks werden dabei alle Anforderungskategorien als gleich wichtig erachtet, d. h. $E_k = 1/|k| = 0,25$ und somit $G_{i_k} = E_{i_k}/4$.

Der Grad, zu dem ein untersuchtes Security-Framework eine Anforderung erfüllt, wird anhand der folgenden diskreten Wertemenge beurteilt:

1. **0 Punkte** – die Anforderung wird nicht erfüllt bzw. vom untersuchten Security-Framework nicht berücksichtigt.
2. **1 Punkt** – die Anforderung wird nur unzureichend partiell erfüllt.
3. **2 Punkte** – die Anforderung wird zwar nur teilweise erfüllt, die behandelten Aspekte können jedoch zielführend eingesetzt werden.
4. **3 Punkte** – die Anforderung wird vollständig erfüllt.

Der Schwellenwert, ab dem eine *teilweise erfüllte* Anforderung als *ausreichend erfüllt* eingestuft werden kann, ist dabei prinzipiell szenarienspezifisch festzulegen. Für die szenarienunabhängigen Analysen in dieser Arbeit wird eine Anforderung als unzureichend partiell erfüllt eingestuft, wenn sie im Konzept des Security-Frameworks zwar in erkennbarer Form behandelt, aber kein Lösungsansatz erörtert wird. Insbesondere wird also der Fall, dass eine Anforderung erkannt, aber explizit und nachvollziehbar begründet von der Betrachtung ausgeschlossen wurde, mit einem statt mit null Punkten bewertet; als nicht ausreichend wird es dabei jedoch angesehen, wenn der jeweilige Aspekt lediglich als zukünftiger Arbeitspunkt angekündigt wird. In Abschnitt 3.8 wird gezeigt, wie diese Vorgehensweise bei Bedarf an eigene Szenarien angepasst werden kann.

Die Summe über alle mit ihrem globalen Gewicht G_{i_k} multiplizierten Punktbewertungen P_{i_k} liefert eine Bewertungskennzahl B für das Security-Framework SF im Wertebereich [0; 3]:

$$B_{SF} = \sum_{k} \sum_{i=1}^{n_k} G_{i_k} \cdot P_{i_k}$$

Offensichtlich ist die Reduktion auf eine einzige Zahl mit einem großen Informationsverlust verbunden, sodass die resultierenden Bewertungskennzahlen zwar zur Bildung einer Rangordnung zwischen Security-Frameworks herangezogen werden können. Da sich jedoch insbesondere Werte im mittleren Bereich auf vielfältige Weise ergeben können, darf das quantitative Ergebnis für sich alleine genommen nicht überbewertet werden.

3.7.2. Begründete Gewichtung der Anforderungen

In diesem Abschnitt wird die Gewichtung der ermittelten Anforderungen vorgestellt. Dazu werden die Anforderungen unter Beibehaltung der Einteilung in die vier Kategorien [SF-FUNK], [SF-INT], [SF-MGMT] und [SF-DOKU] in alphabetischer Reihenfolge zunächst jeweils knapp und von den Szenarien losgelöst zusammengefasst. Jeweils im Anschluss wird die Gewichtung kurz erläutert; sie orientiert sich an den im vorherigen Abschnitt definierten Kriterien zur Wahl der Gewichtsfaktoren.

3.7.2.1. Gewichtung der Anforderungen in Kategorie [SF-FUNK]

Die technischen und IT-sicherheitsspezifischen funktionalen Anforderungen werden wie folgt gewichtet:

- **[SF-FUNK-Abschottung]** – Faktor 2 – wichtig (vgl. Seite 93)

  Zusammenfassung: Das Security-Framework muss technische Komponenten derart einsetzen und Datenflüsse so gestalten, dass die beteiligten Organisationen weder ihre Autarkie verlieren noch interne Daten nach außen geben müssen.

  Begründung der Gewichtung: Die Anforderung betrifft die grundlegende Abstimmung des Zusammenspiels der Beteiligten beim organisationsübergreifenden Einsatz von Security-Frameworks. Die nicht ausreichende gegenseitige Abschottung der beteiligten Organisationen stellt eine deutlich spürbare Einschränkung dar, die jedoch auf die entsprechenden Teilbereiche beschränkt ist.

- **[SF-FUNK-Adaptivität]** – Faktor 1 – wünschenswert (vgl. Seite 103)

  Zusammenfassung: Das Security-Framework muss berücksichtigen, dass Parameter wie beispielsweise Schwellenwerte für die Erzeugung von Sicherheitsalarmen im laufenden Betrieb dynamisch an die Umgebung angepasst werden müssen.

  Begründung der Gewichtung: Sofern das Security-Framework keine entsprechenden Anpassungen zur Laufzeit vorsieht, können diese dennoch mit entsprechend höherem Aufwand manuell für die einzelnen betroffenen Komponenten durchgeführt werden.

- **[SF-FUNK-Angriffe]** – Faktor 2 – wichtig (vgl. Seite 76)

  Zusammenfassung: Angriffe, vor denen das Security-Framework schützen soll, müssen konkret benannt sein und sich mit den im Einsatzgebiet erwarteten Angriffen decken.

  Begründung der Gewichtung: Eine unzureichende Berücksichtigung der erwarteten Angriffe erfordert einerseits umfangreiche konzeptionelle Ergänzungen oder den Paralleleinsatz zusätzlicher Schutzkonzepte; andererseits hängt die Beurteilung der funktionalen Vollständigkeit (vgl. [SF-FUNK-Maßnahmen]) stark von den berücksichtigten Angriffen ab.

- **[SF-FUNK-Assets]** – Faktor 4 – essentiell (vgl. Seite 76)

  Zusammenfassung: Die vom Security-Framework berücksichtigten Assets müssen sich mit den im Einsatzgebiet vorhandenen Assets decken.

  Begründung der Gewichtung: Für die grundlegende Entscheidung, ob ein Security-Framework zu einem konkreten Einsatzgebiet passt und dort erfolgreich wirken kann, ist die Abdeckung der vorhandenen Assets eines der zentralen Kriterien.

- **[SF-FUNK-Auditing]** – Faktor 4 – essentiell (vgl. Seite 84)

  Zusammenfassung: Sicherheitsrelevante Vorgänge müssen den entsprechenden Vorgaben gemäß – und damit im Hinblick auf Datenschutz ggf. auch bewusst eingeschränkt – von den Komponenten des Security-Frameworks revisionsfähig protokolliert werden.

  Begründung der Gewichtung: Die Protokollierung sicherheitsrelevanter Ereignisse in dafür geeigneten Granularitätsstufen ist essentiell für darauf aufbauende technische Schnittstellen, beispielsweise zur Erzeugung von Sicherheitsalarmen. Über diese ist sie nahtlos mit zahlreichen Managementprozessen verbunden, denen bei Nichterfüllen dieser Anforderung eine der technischen Grundlagen entzogen wird.

- **[SF-FUNK-Automatisierung]** – Faktor 2 – wichtig (vgl. Seite 93)

  Zusammenfassung: Die mit dem Security-Framework eingeführten Workflows, Maßnahmen und Komponenten sollen einen möglichst hohen Automatisierungsgrad aufweisen.

  Begründung der Gewichtung: Die weitgehende Automatisierung ist ein wichtiger Mehrwert im operativen Betrieb, entscheidet jedoch im Allgemeinen nicht allein über die grundlegende Eignung eines Security-Frameworks für einen konkreten Einsatzbereich und wirkt sich nicht unmittelbar auf andere Anforderungsbereiche aus.

- **[SF-FUNK-Maßnahmen]** – Faktor 4 – essentiell (vgl. Seite 76)

  Zusammenfassung: Das Security-Framework muss Sicherheitsmaßnahmen vorsehen, die zur nachweislich wirksamen Umsetzung des angestrebten Schutzniveaus beitragen.

  Begründung der Gewichtung: Diese Anforderung umfasst sämtliche sicherheitsspezifischen technischen und funktionalen qualitativen Ansprüche, die klassisch an die aus dem Einsatz eines Security-Frameworks resultierende Architektur gestellt werden. Sie wird somit herangezogen, um zu bewerten, ob die vom Security-Framework vorgeschlagene Lösung das im Einsatzgebiet vorliegende Problem funktional adäquat löst. Dieses Kriterium ist offensichtlich entscheidend für die szenarienspezifische Anwendbarkeit des Security-Frameworks.

- **[SF-FUNK-Schwachstellen]** – Faktor 2 – wichtig (vgl. Seite 76)

  Zusammenfassung: Die vom Security-Framework berücksichtigten Schwachstellen müssen konkret benannt sein und sich mit den im Einsatzgebiet vorhandenen Schwachstellen decken.

  Begründung der Gewichtung: Eine unzureichende Berücksichtigung vorhandener Schwachstellen erfordert analog zu [SF-FUNK-Angriffe] einerseits zusätzliche Schutzkonzepte und beeinflusst andererseits die Vollständigkeit der im Rahmen von [SF-FUNK-Maßnahmen] zu beurteilenden Lösung negativ. Die Konsequenzen beschränken sich jedoch auf genau den Bereich der nicht berücksichtigten Schwachstellen.

In der Kategorie [SF-FUNK] liegen somit acht Anforderungen vor, von denen drei als essentiell eingestuft wurden; die Summe ihrer Gewichtsfaktoren beträgt 21.

3.7.2.2. Gewichtung der Anforderungen in Kategorie [SF-INT]

Die Integrations- und Betriebsanforderungen werden wie folgt gewichtet:

- **[SF-INT-Ausbauphasen]** – Faktor 2 – wichtig (vgl. Seite 93)

  Zusammenfassung: Die vollständige Einführung des Security-Frameworks muss in mehreren Stufen erfolgen können, ohne dass der vollständige Customizing-Prozess in jeder Iteration erneut vollständig durchlaufen werden muss.

  Begründung der Gewichtung: Beim Vorliegen komplexer Szenarien oder umfangreicher Security-Frameworks kann eine Umstellung der vorhandenen Infrastruktur in der Praxis häufig nicht in einem großen Schritt erfolgen. Die mangelnde Unterstützung für ein phasenbasiertes Rollout würde somit einen erheblichen Mehraufwand verursachen, hätte jedoch keine gravierenden Auswirkungen auf den Einsatz und das Management der umgesetzten Teile.

- **[SF-INT-Customizing]** – Faktor 4 – essentiell (vgl. Seite 76)

  Zusammenfassung: Das Security-Framework muss einen methodisch unterstützten Anpassungsprozess beinhalten.

  Begründung der Gewichtung: Durch diese Anforderung werden Security-Frameworks von Musterlösungen für Beispielszenarien bzw. szenarienspezifischen Sicherheitskonzepten differenziert. Es handelt sich um eine essentielle, unmittelbar der Definition des Begriffs Security-Framework entnommene Anforderung.

- **[SF-INT-Einführung]** – Faktor 2 – wichtig (vgl. Seite 77)

  Zusammenfassung: Den reinen Adaptionsprozess ergänzend muss das Security-Framework seine Einführung im Einsatzgebiet methodisch unterstützen. Dies umfasst sowohl Situationen, in denen das Security-Framework zusammen mit den Assets neu eingeführt wird, als auch Migrationsprojekte, bei denen ein bestehendes Sicherheitskonzept durch das Security-Framework ergänzt oder abgelöst wird.

  Begründung der Gewichtung: Sofern die Einführung des Security-Frameworks nicht methodisch unterstützt wird, erschwert sich die praktische Umsetzung entsprechender Einführungsprojekte erheblich, da wesentliche framework-spezifische Aspekte konzeptionell nachgetragen werden müssen. Die Anforderung ist jedoch nicht essentiell, da sie keinen direkten Einfluss auf den späteren Betrieb ausübt.

- **[SF-INT-Erweiterung]** – Faktor 2 – wichtig (vgl. Seite 76)

  Zusammenfassung: Das Security-Framework muss die Flexibilität aufweisen, über konzeptionelle und technische Schnittstellen für eigene – in der Regel szenarienspezifische – Erweiterungen zu verfügen.

  Begründung der Gewichtung: Die Erweiterbarkeit ist für alle Szenarien relevant, die wichtige, zu berücksichtigende Besonderheiten aufweisen, und in denen im Rahmen der Einführung oder des kontinuierlichen Verbesserungsprozesses eigene Sicherheitskonzepte einfließen sollen. Ihr Fehlen stellt dort eine deutliche, aber auf die betroffenen Teilbereiche begrenzte Einschränkung dar.

- **[SF-INT-Hochverfügbarkeit]** – Faktor 2 – wichtig (vgl. Seite 84)

  Zusammenfassung: Das Security-Framework muss adäquate Hochverfügbarkeitskonzepte für die von ihm vorgesehenen Komponenten und Abläufe vorsehen und darf vorhandene Hochverfügbarkeitsmechanismen nicht beeinträchtigen.

Begründung der Gewichtung: In Szenarien mit einem Bedarf an hochverfügbarer Infrastruktur macht sich das Fehlen entsprechender Konzepte gravierend bemerkbar, sodass ein signifikanter Aufwand in die Ergänzung und Umsetzung von Security-Frameworks fließen muss, ohne den das Security-Framework zu kurz greifen würde. Es sind jedoch keine anderen qualitativen Aspekte direkt davon betroffen.

- [**SF-INT-Kompatibilität**] – Faktor 2 – wichtig (vgl. Seite 77)

  Zusammenfassung: Die technische Basis der vom Security-Framework vorgesehenen Komponenten muss zur im konkreten Einsatzgebiet bereits vorhandenen Infrastruktur passen.

  Begründung der Gewichtung: Grundlegende technische Differenzen zwischen dem Security-Framework und der in einem Szenario bereits vorhandenen Infrastruktur können nicht ignoriert oder durch einfache Workarounds kompensiert werden. Der zur Umsetzung notwendige Zusatzaufwand stellt jedoch keine Beeinträchtigung im Hinblick auf den späteren Einsatz und das operative Management dar.

- [**SF-INT-Modularität**] – Faktor 2 – wichtig (vgl. Seite 76)

  Zusammenfassung: Das Security-Framework muss in einzelne Bereiche untergliedert sein, deren Aufgaben und Zusammenspiel definiert sind.

  Begründung der Gewichtung: Die hier geforderte Eigenschaft ist bei komplexen, größeren Security-Frameworks eine grundlegende Voraussetzung für die Flexibilität, auf der beispielsweise die Anpassungsmethodik aufsetzt. Ihr Fehlen beeinträchtigt die allgemeine Eignung des Security-Frameworks erheblich, gefährdet die Betriebs- und Managementkonzepte nach erfolgreicher Umsetzung jedoch nicht.

- [**SF-INT-Parallelbetrieb**] – Faktor 4 – essentiell (vgl. Seite 94)

  Zusammenfassung: Das Security-Framework muss berücksichtigen, dass Teile der von ihm abgedeckten Assets potentiell parallel von framework-externen Sicherheitsmaßnahmen geschützt werden, beispielsweise wenn einige Komponenten auch von anderen, vom Security-Framework nicht betrachteten Diensten genutzt werden.

  Begründung der Gewichtung: Die Anforderung ist grundlegend in Szenarien, in denen von Security-Frameworks betrachtete Komponenten nicht ausschließlich durch die vom Security-Framework abgedeckten Dienste genutzt werden. In diesem Fall würden Betriebs- und Managementkonzepte durch den Einsatz des Security-Frameworks massiv beeinträchtigt werden.

- [**SF-INT-Polyinstanziierbarkeit**] – Faktor 1 – wünschenswert (vgl. Seite 93)

  Zusammenfassung: Ein organisationsübergreifend einzusetzendes Security-Framework muss die an jedem Einsatzort potentiell divergierenden Anforderungen in einem auf die Mehrfachinstanziierung zugeschnittenen Customizing-Prozess unterstützen.

  Begründung der Gewichtung: Sofern die Polyinstanziierung nicht explizit berücksichtigt wird, verbleibt die alternative Lösungsvariante, die jeweils organisationsinternen Customizing-Prozesse losgelöst vom Security-Framework zwischen den beteiligten Organisationen zu koordinieren. Der damit verbundene Zusatzaufwand ist vertretbar und wirkt sich nicht limitierend auf den Einsatz des Security-Frameworks aus.

- [**SF-INT-Skalierbarkeit**] – Faktor 4 – essentiell (vgl. Seite 77)

Zusammenfassung: Das Design des Security-Frameworks muss eine für das Einsatzgebiet adäquate Skalierbarkeit aufweisen, damit die Umsetzbarkeit gewährleistet und Performanzprobleme im Betrieb vermieden werden.

Begründung der Gewichtung: Der praktische Einsatz eines Security-Frameworks hängt offensichtlich stark davon ab, ob die resultierende Lösung mit unverhältnismäßig hohem Betriebsaufwand oder Dienstqualitätsverschlechterungen verbunden ist. In allen Szenarien, in denen Dienstumfang und -qualität nicht gegenüber den Sicherheitseigenschaften deutlich in den Hintergrund treten, ist die ausreichende Skalierbarkeit deshalb eine für die Entscheidung über den Einsatz des Security-Frameworks essentielle Anforderung und hat umfassende Auswirkungen auf die Betriebs- und Managementprozesse.

- **[SF-INT-Usability]** – Faktor 2 – wichtig (vgl. Seite 106)

  Zusammenfassung: Die Handhabung des Security-Frameworks sowohl bezüglich des Umgangs mit dem Konzept und der von ihm gebotenen Methodik als auch im Hinblick auf den Betrieb und das Management der resultierenden Architektur muss eine dem Einsatzgebiet angemessene Benutzerfreundlichkeit aufweisen.

  Begründung der Gewichtung: Die Beurteilung der Benutzerfreundlichkeit ist ebenso wie die Definition von konkreten Usability-Kriterien szenarienspezifisch. Über den Gewichtsfaktor muss somit im Einzelfall entschieden werden (vgl. Abschnitt 3.8). Sie wird in dieser Arbeit allgemein als *wichtig* eingestuft, da sie die szenarienspezifische Eignung zwar spürbar beeinflusst, die übrigen vom Security-Framework vorgesehenen Funktionen und Managementeigenschaften jedoch nicht notwendigerweise beeinträchtigt.

- **[SF-INT-Wiederverwendbarkeit]** – Faktor 2 – wichtig (vgl. Seite 77)

  Zusammenfassung: Das Security-Framework muss vorsehen, dass in der Infrastruktur typischerweise bereits vorhandene Komponenten, beispielsweise relationale Datenbankmanagementsysteme zur Speicherung von Policies, genutzt werden können, um die Anzahl zusätzlich notwendiger Komponenten zu minimieren.

  Begründung der Gewichtung: Für den praktischen Einsatz ist es im Allgemeinen nicht akzeptabel, lediglich aufgrund mangelnder Flexibilität des Security-Frameworks eine Reihe neuer Komponenten einzuführen, die ähnliche Funktionalität aufweist wie die bereits vorhandenen Infrastrukturbestandteile. Entsprechend wird ein potentiell hoher Anpassungsaufwand am Frameworkkonzept und damit verbundenen Teilen der Implementierung erforderlich. Die Auswirkungen sind jedoch auf die jeweils betroffenen Komponenten beschränkt.

Die Kategorie [SF-INT] enthält somit 12 Anforderungen, davon drei essentielle; die Summe der Gewichtsfaktoren beträgt 29.

3.7.2.3. Gewichtung der Anforderungen in der Kategorie [SF-MGMT]

Die Anforderungen an die Schnittstellen für Managementoperationen und -prozesse werden wie folgt gewichtet:

- **[SF-MGMT-Administrationskonzepte]** – Faktor 2 – wichtig (vgl. Seite 84)

Zusammenfassung: Das Security-Framework muss in seinem Einsatzgebiet typische, sicherheitsrelevante Administrationskonzepte (z. B. Privileged Account Management oder Vier-Augen-Prinzip) unterstützen.

Begründung der Gewichtung: Die integrierte Unterstützung bereits eingesetzter Administrationsverfahren erleichtert nicht die Einführung des Security-Frameworks, sondern ist in vielen Bereichen eine zwingende Voraussetzung. Gegebenenfalls müssen entsprechende Verfahren mit relativ hohem Aufwand im Rahmen des Customizing-Prozesses ergänzt werden; alternativ kann auch eine Umstellung auf die vom Security-Framework vorgesehenen Administrationskonzepte erfolgen. Es ergeben sich keine direkten Einschränkungen für andere funktionale oder managementspezifische Teilbereiche.

- [**SF-MGMT-Berichtsdetails**] – Faktor 2 – wichtig (vgl. Seite 94)

  Zusammenfassung: Der Umfang von Security-Reports bzw. der für ihre Erstellung verwendeten Rohdaten muss zielgruppenspezifisch angepasst werden; in organisationsübergreifenden Bereichen muss insbesondere zwischen organisationsinterner und -externer Weiterverarbeitung unterschieden werden.

  Begründung der Gewichtung: Ohne Vorgaben oder Vorschläge zur Gestaltung von Sicherheitsberichten müssten entsprechende Konzepte im jeweiligen Einsatzgebiet separat erarbeitet werden. Dadurch wird die Eignung des Security-Frameworks begrenzt auf das Berichtswesen eingeschränkt.

- [**SF-MGMT-Compliance**] – Faktor 4 – essentiell (vgl. Seite 84)

  Zusammenfassung: Das Security-Framework muss die Compliance-Anforderungen im von ihm abgedeckten Bereich thematisieren und dabei auf mögliche Zielkonflikte (z. B. Nachvollziehbarkeit vs. Datenschutz) eingehen.

  Begründung der Gewichtung: Die Einhaltung externer, beispielsweise gesetzlicher Auflagen ist essentiell für die praktische Einsatzfähigkeit eines Security-Frameworks. Berücksichtigen die vorgeschlagenen Konzepte diese Randbedingungen nicht, ergeben sich massive Einschränkungen für den Betrieb und das Management.

- [**SF-MGMT-Delegation**] – Faktor 2 – wichtig (vgl. Seite 77)

  Zusammenfassung: Das Security-Framework muss vorsehen, dass Teile der administrativen Tätigkeiten nicht zentral ausgeführt werden, sondern beispielsweise an kundenseitige Administratoren delegiert werden.

  Begründung der Gewichtung: Die Delegation ausgewählter administrativer Berechtigungen ist für komplexe Szenarien eine grundlegende Voraussetzung für effizientes operatives Management. Sofern nur eine zentrale Verwaltung unterstützt wird, müssen Delegationsmechanismen mit hohem Aufwand aufgepfropft werden; diese Einschränkung ist jedoch auf den Teilbereich Administration begrenzt.

- [**SF-MGMT-Events**] – Faktor 1 – wünschenswert (vgl. Seite 78)

  Zusammenfassung: Das Security-Framework muss spezifizieren, welche Sicherheitsereignisse, -alarme und -vorfälle, die von den von ihm bereitgestellten Komponenten ausgelöst werden, von der Managementinfrastruktur weiterverarbeitet werden müssen.

  Begründung der Gewichtung: Die Festlegung zu überwachender Ereignisse bildet die Grundlage für die nahtlose Integration der Komponenten des Security-Frameworks in

das operative Sicherheitsmanagement. Die Definition entsprechender Trigger, Verarbeitungsprozesse und Eskalationsmechanismen muss alternativ im jeweiligen Einsatzgebiet erfolgen.

- **[SF-MGMT-ITSM-Schnittstellen]** – Faktor 4 – essentiell (vgl. Seite 78)

  Zusammenfassung: Das Zusammenspiel des Security-Frameworks mit den relevanten ITSM-Prozessen (z. B. Incident Management für Security Incidents) muss beispielsweise über die Spezifikation entsprechender Schnittstellen und Abläufe definiert sein.

  Begründung der Gewichtung: Diese Anforderung verstärkt die Differenzierung zwischen rein technisch orientierten Sicherheitskonzepten und Security-Frameworks, die ganzheitlich in die Managementprozesse integriert werden sollen. Die adäquate Berücksichtigung der Zusammenhänge zwischen den framework-internen Abläufen und den ITSM-Prozessen ist hierfür essentiell, da bei ihrem Fehlen grundlegende Managementkonzepte nicht mehr umgesetzt oder nur mit sehr hohem Aufwand ins Security-Framework integriert werden könnten.

- **[SF-MGMT-Kosten]** – Faktor 2 – wichtig (vgl. Seite 85)

  Zusammenfassung: Die mit dem Customizing, der Implementierung und dem Betrieb des Security-Frameworks anfallenden Kosten müssen zu einer Beurteilung der Wirtschaftlichkeit der Lösung aus dem Frameworkkonzept hervorgehen und sich mit den im Einsatzgebiet gegebenen Randbedingungen decken.

  Begründung der Gewichtung: Die mit der Einführung und dem Betrieb verbundenen Kosten sind aus offensichtlichen Gründen entscheidend für den Einsatz eines Security-Frameworks. Zur Unterstützung entsprechender Planungen ist es wichtig, dass die Kosten vorab realistisch eingeschätzt werden können; das Fehlen der dazu notwendigen Informationen beeinträchtigt jedoch keine der übrigen Betriebs- und Managementkonzepte.

- **[SF-MGMT-KPIs]** – Faktor 1 – wünschenswert (vgl. Seite 94)

  Zusammenfassung: Das Security-Framework muss sicherheitsspezifische Key Performance Indicators spezifizieren, die beispielsweise in SLAs einfließen können.

  Begründung der Gewichtung: Der Vorschlag von KPIs reduziert den im Einsatzgebiet notwendigen konzeptionellen Aufwand und ermöglicht organisationsübergreifend einheitliche Kennzahlen. Die Festlegung entsprechender Kriterien zur Beurteilung des Dienstes kann alternativ jedoch auch szenarienspezifisch, beispielsweise auf Basis der vom Security-Framework definierten Metriken (vgl. [SF-MGMT-Metriken]) erfolgen.

- **[SF-MGMT-Mandantenfähigkeit]** – Faktor 2 – wichtig (vgl. Seite 77)

  Zusammenfassung: Das Security-Framework muss beispielsweise in Hosting-Umgebungen pro Kunde separat parametrisiert werden können.

  Begründung der Gewichtung: Die Anforderung betrifft primär Einsatzgebiete, in denen ein Dienst in unterschiedlichen Ausprägungen für verschiedene Benutzergruppen angeboten wird. In entsprechenden Szenarien können Alternativlösungen beispielsweise darin bestehen, ausgewählte Komponenten des Security-Frameworks, die kundenspezifisch konfiguriert werden müssen, mit entsprechend deutlich höherem Aufwand mehrfach zu instanziieren.

- **[SF-MGMT-Metriken]** – Faktor 4 – essentiell (vgl. Seite 94)

  Zusammenfassung: Das Security-Framework muss Kennzahlen definieren, die zur kontinuierlichen Überwachung und als Basis für das Berichtswesen herangezogen werden können.

  Begründung der Gewichtung: Die aussagekräftige Beurteilung der laufenden Frameworkinstanz durch Kennzahlen ist essentiell für viele Managementprozesse und Grundlage für die Entscheidung, ob die mit dem Frameworkeinsatz verbundenen Ziele in der Praxis erreicht werden konnten. Eine ausbleibende Thematisierung von Kennzahlen schränkt das Management des Security-Frameworks entsprechend stark ein.

- **[SF-MGMT-Operationen]** – Faktor 4 – essentiell (vgl. Seite 77)

  Zusammenfassung: Die im Kontext des Security-Frameworks relevanten Security-Managementoperationen müssen spezifiziert sein, insbesondere wenn sie für das Zusammenspiel mehrerer Komponenten oder den Einsatz einer dedizierten Steuerungskomponente erforderlich sind.

  Begründung der Gewichtung: Die Festlegung von Managementoperationen bildet die Brücke zwischen der Zusammenstellung der am Security-Framework beteiligten Komponenten zu einer Gesamtarchitektur und deren Betrieb. Ihr Fehlen entzieht dem operativen Management somit eine grundlegende Voraussetzung.

- **[SF-MGMT-Performanz]** – Faktor 2 – wichtig (vgl. Seite 85)

  Zusammenfassung: Die Performanz der zu schützenden Infrastruktur darf vom instanziierten Security-Framework nicht zu stark negativ beeinflusst werden.

  Begründung der Gewichtung: Die durch den Einsatz des Security-Frameworks bedingte Einführung technischer und organisatorischer Sicherheitsmaßnahmen ist häufig mit zusätzlichem Ressourcenverbrauch auf vorhandenen Komponenten oder Erweiterungen bestehender Datenflüsse, z. B. zur Inhaltsanalyse der Meta- oder Nutzdaten, verbunden und führt dadurch i. A. zu schlechterer Performanz als beim Verzicht auf Sicherheitsmaßnahmen. Massive Performanzeinbußen reduzieren die Eignung des Security-Frameworks spürbar, wirken sich jedoch nicht auf andere Managementaspekte aus.

- **[SF-MGMT-Policies]** – Faktor 2 – wichtig (vgl. Seite 105)

  Zusammenfassung: Für das Security-Framework muss einerseits festgelegt sein, wie Managementrichtlinien auf die technische Konfiguration der vorgegebenen Komponenten abgebildet werden können; andererseits muss spezifiziert sein, welche neuen technischen Optionen des Security-Frameworks beispielsweise in einer Gesamtsicherheitsrichtlinie berücksichtigt werden müssen.

  Begründung der Gewichtung: Das Fehlen einer Schnittstelle zwischen dem Security-Framework und den vom Sicherheitsmanagement vorgesehenen Sicherheitsrichtlinien stellt eine Einschränkung dar, die durch szenarienspezifischen konzeptionellen Aufwand kompensiert werden muss, sich aber nicht unmittelbar auf andere Managementbereiche auswirkt.

- **[SF-MGMT-Praxis]** – Faktor 2 – wichtig (vgl. Seite 103)

  Zusammenfassung: Das Security-Framework muss praxiserprobt sein; bei seiner Weiterentwicklung müssen die im Praxisbetrieb gewonnenen Erfahrungen berücksichtigt worden sein.

Begründung der Gewichtung: Der Einsatz eines noch nicht praxiserprobten Security-Frameworks ist mit dem Risiko verbunden, dass möglicherweise einige grundlegende Betriebsaspekte bei der Konzeption übersehen wurden und sich erst im laufenden Betrieb bemerkbar machen. Die grundlegenden Managementkonzepte werden dadurch jedoch nicht gefährdet.

- **[SF-MGMT-Prozesse]** – Faktor 4 – essentiell (vgl. Seite 94)

  Zusammenfassung: Das Security-Framework muss die für sein Management notwendigen organisatorischen Abläufe spezifizieren.

  Begründung der Gewichtung: Die Definition der für das Security-Framework spezifischen Managementprozesse ist offensichtlich essentiell für seinen Betrieb. Das Fehlen entsprechender Festlegungen schränkt die Eignung des Security-Frameworks aus der Perspektive des operativen Managements massiv ein.

- **[SF-MGMT-Quantifizierung]** – Faktor 2 – wichtig (vgl. Seite 105)

  Zusammenfassung: Das Security-Framework muss Sicherheitseigenschaften sowohl auf konzeptioneller Ebene als auch im Betrieb quantitativ und nicht lediglich qualitativ bewerten.

  Begründung der Gewichtung: Die quantitative Erfassung von Sicherheitseigenschaften ist beispielsweise für die Priorisierung im Rahmen des Risikomanagements und für das Sicherheitsberichtswesen notwendig. Rein qualitative Aussagen zur Sicherheitslage stellen eine Einschränkung dar, die sich jedoch nicht unmittelbar auf die anderen Managementbereich auswirkt.

- **[SF-MGMT-Releasezyklus]** – Faktor 2 – wichtig (vgl. Seite 105)

  Zusammenfassung: Das Security-Framework muss Releasezyklen, Rollout- und Rollbackkonzepte vorsehen, die sich mit den terminlichen und logistischen Anforderungen des Einsatzgebietes decken.

  Begründung der Gewichtung: Ein auf die Randbedingungen im Szenario abstimmbares Vorgehen im Rahmen des kontinuierlichen Verbesserungsprozesses ist für den nachhaltigen Betrieb grundlegend. Die Einführungs- und Aktualisierungsplanungen für die vom Security-Framework abgedeckten Komponenten wirken sich jedoch nicht auf die übrigen Managementbereiche aus.

- **[SF-MGMT-Schulungen]** – Faktor 2 – wichtig (vgl. Seite 94)

  Zusammenfassung: Das Security-Framework muss den Schulungsbedarf und die Schulungsinhalte für die relevanten Zielgruppen – beispielsweise Administratoren und Benutzer – thematisieren.

  Begründung der Gewichtung: Sofern das Security-Framework nicht lediglich Komponenten und Abläufe vorsieht, die den von seinem Einsatz Betroffenen nicht bereits bekannt sind, stellt das Fehlen von Schulungskonzepten eine Einschränkung dar, die durch eigenen, meist nicht geringen Aufwand kompensiert werden muss. Der grundlegende Betrieb und das Management des Security-Frameworks werden dadurch jedoch nicht gefährdet.

- **[SF-MGMT-Support]** – Faktor 1 – wünschenswert (vgl. Seite 103)

  Zusammenfassung: Für das Security-Framework muss externe Unterstützung, beispielsweise durch den Hersteller oder durch Beratungsunternehmen, verfügbar sein.

Begründung der Gewichtung: Die Relevanz kommerzieller Unterstützung bei der Umsetzung und beim Betrieb des Security-Frameworks ist szenarienspezifisch. Ihr Fehlen schränkt die übrigen Eigenschaften des Security-Frameworks jedoch nicht ein; die Auswirkungen können beispielsweise durch die gezielte Unterstützung des Aufbaus eigenen Wissens reduziert werden.

- **[SF-MGMT-Tests]** – Faktor 1 – wünschenswert (vgl. Seite 85

  Zusammenfassung: Das Security-Framework muss Schnittstellen, Methoden und Ansatzpunkte für die initiale sowie die kontinuierliche Funktionsüberprüfung und proaktive Sicherheitsmaßnahmen vorgeben.

  Begründung der Gewichtung: Die Spezifikation entsprechender Tests rundet das Gesamtkonzept eines Security-Frameworks zwar ab; entsprechende Ansatzpunkte für die Funktionsüberprüfung und proaktive Sicherheitsmaßnahmen können alternativ aber auch vom operativen Management oder z. B. von mit Penetrationstests beauftragten Sicherheitsunternehmen festgelegt werden.

- **[SF-MGMT-Verbesserung]** – Faktor 4 – essentiell (vgl. Seite 103)

  Zusammenfassung: Das Security-Framework muss aktiv weiterentwickelt und dabei an die sich verändernden Anforderungen sowie neue technische und organisatorische Möglichkeiten angepasst werden.

  Begründung der Gewichtung: Die kontinuierliche Verbesserung des Security-Frameworks ist essentiell, da gerade im Bereich der IT-Sicherheit einmalige, statische Lösungen nur einen unzureichenden, temporären Schutz bieten.

- **[SF-MGMT-Zuständigkeiten]** – Faktor 1 – wünschenswert (vgl. Seite 105)

  Zusammenfassung: Die personellen Zuständigkeiten müssen vom Security-Framework beispielsweise durch die konkrete Benennung entsprechender Rollen spezifiziert werden.

  Begründung der Gewichtung: Die präzise Festlegung von Verantwortlichkeiten trägt dazu bei, die Abläufe im Einsatzgebiet auf die vom Security-Framework vorgesehenen auszurichten. Alternativ kann die Zuordnung der verschiedenen Bereiche zu den bereits vorhandenen Rollen und Personen jedoch mit geringem Aufwand auch szenarienspezifisch konzipiert werden.

Die Kategorie [SF-MGMT] beinhaltet somit 22 Anforderungen, davon werden sechs als essentiell eingestuft; die Summe der Gewichtsfaktoren ist 51.

3.7.2.4. Gewichtung der Anforderungen in der Kategorie [SF-DOKU]

Die Anforderungen an die Dokumentation von Security-Frameworks werden wie folgt gewichtet:

- **[SF-DOKU-Anforderungsanalyse]** – Faktor 2 – wichtig (vgl. Seite 94)

  Zusammenfassung: Aus der Dokumentation des Security-Frameworks muss hervorgehen, welche Methodik bei der Anforderungsanalyse angewandt wurde, um die Übertragbarkeit und Vollständigkeit beurteilen zu können.

Begründung der Gewichtung: Die Eignung des Security-Frameworks für ein konkretes Einsatzgebiet ist potentiell höher, wenn bei seinem Design mit dem Szenario vergleichbare Anforderungen berücksichtigt wurden. Ohne eine explizite Dokumentation leidet die Nachvollziehbarkeit, sodass eine entsprechende Gegenüberstellung des Security-Frameworks mit den lokalen Gegebenheiten mit entsprechendem konzeptionellen Aufwand durchgeführt werden muss; die Betriebs- und Managementeigenschaften des Security-Frameworks sind davon jedoch nicht betroffen.

- **[SF-DOKU-Angreifermodelle]** – Faktor 2 – wichtig (vgl. Seite 78)

  Zusammenfassung: Die dem Security-Framework zugrunde liegenden Angreifermodelle müssen dokumentiert sein.

  Begründung der Gewichtung: Die Auswahl der in der Kategorie [SF-FUNK] behandelten Angriffe und Sicherheitsmaßnahmen hängt maßgeblich davon, welche Angreifertypen berücksichtigt und welche Eigenschaften ihnen zugeschrieben wurden. Die Dokumentation der Angreifermodelle trägt deshalb wesentlich zur Transparenz und Nachvollziehbarkeit sowie zur Beurteilung der Übertragbarkeit auf ein konkretes Einsatzgebiet bei, hat darüber hinaus jedoch keinen Einfluss auf die Betriebs- und Managementeigenschaften.

- **[SF-DOKU-Ausrichtung]** – Faktor 2 – wichtig (vgl. Seite 78)

  Zusammenfassung: Die generelle Ausrichtung und die Schwerpunkte des Security-Frameworks im Bezug auf die Prävention und Detektion von bzw. die Reaktion auf Angriffe müssen dokumentiert sein.

  Begründung der Gewichtung: Die Ausrichtung eines Security-Frameworks kann zwar prinzipiell aus seinem Konzept abgeleitet werden. Die mangelnde Dokumentation deutet aber i. A. auf Unvollständigkeit hin; insbesondere werden bisher häufig lediglich präventive Maßnahmen diskutiert. Somit fällt gegebenenfalls szenarienspezifischer konzeptioneller Mehraufwand an, der sich jedoch nicht auf die übrigen Betriebs- und Managementaspekte auswirkt.

- **[SF-DOKU-Beurteilung]** – Faktor 1 – wünschenswert (vgl. Seite 105)

  Zusammenfassung: Die Dokumentation des Security-Frameworks muss Kriterien, anhand derer das Erreichen der mit seiner Instanziierung und Inbetriebnahme angestrebten Ziele beurteilt werden kann, definieren.

  Begründung der Gewichtung: Die explizite Spezifikation der Beurteilungskriterien vereinfacht die Durchführung von Post-Implementation-Reviews (PIRs) am Ende entsprechender Einführungsprojekte. Diese Kriterien müssen alternativ mit eigenem konzeptionellen Aufwand aus dem Frameworkkonzept abgeleitet werden.

- **[SF-DOKU-Checkliste]** – Faktor 1 – wünschenswert (vgl. Seite 94)

  Zusammenfassung: Die Dokumentation des Security-Frameworks muss als Checkliste für den Anpassungsprozess sowie die Implementierung und Einführung der Frameworkinstanz herangezogen werden können.

  Begründung der Gewichtung: Die methodische Unterstützung der Anpassung und Instanziierung des Security-Frameworks wird durch die Aufbereitung in Form einer Checkliste weiter verbessert. Alternativ kann eine Vorgehensweise zur Überprüfung der notwendigen Zwischenschritte aus dem Frameworkkonzept abgeleitet werden.

- [**SF-DOKU-Designentscheidungen**] – Faktor 2 – wichtig (vgl. Seite 104)

  Zusammenfassung: Die Dokumentation des Security-Frameworks muss die Hintergründe für getroffene Designentscheidungen explizit festhalten.

  Begründung der Gewichtung: Aufgrund der in der Regel gegebenen Vielzahl zueinander äquivalenter oder mit individuellen Vor- und Nachteilen verbundenen Lösungsvarianten ist die explizite Dokumentation von Designentscheidungen eine wichtige Voraussetzung für die fachliche Beurteilung des resultierenden Security-Frameworks. Falls sie fehlt, muss mit erheblichem Aufwand überprüft werden, ob im konkreten Einsatzgebiet dieselben Designentscheidungen getroffen worden wären, ohne dass dies jedoch Auswirkungen auf die späteren Betriebs- und Managementeigenschaften hat.

- [**SF-DOKU-Kontinuum**] – Faktor 1 – wünschenswert (vgl. Seite 94)

  Zusammenfassung: Aus der Dokumentation des Security-Frameworks muss sein prozessunterstützender Charakter im Hinblick auf die kontinuierliche Verbesserung deutlich hervorgehen.

  Begründung der Gewichtung: Die explizite Dokumentation der Notwendigkeit einer kontinuierlichen Weiterentwicklung sowohl des Security-Frameworks selbst als auch seiner Instanziierung im Einsatzgebiet trägt zur Bewusstseinsbildung bei und erleichtert die entsprechenden Planungen. Alternativ müssen die entsprechenden Ansatzpunkte und Ablaufschritte szenarienspezifisch konzipiert werden.

- [**SF-DOKU-Lifecyclephasen**] – Faktor 1 – wünschenswert (vgl. Seite 105)

  Zusammenfassung: Das Frameworkkonzept muss alle von ihm abgedeckten Lebenszyklusphasen – beispielsweise von der Anpassung und Instanziierung über den Einsatz bis zur Außerbetriebnahme – benennen.

  Begründung der Gewichtung: Die vom Security-Framework berücksichtigten Lebenszyklusphasen können alternativ auch aus seinem Konzept abgeleitet werden; die explizite Diskussion erleichtert jedoch die Beurteilung der Vollständigkeit des Frameworkkonzepts und die Definition entsprechend notwendiger Anknüpfungspunkte.

- [**SF-DOKU-Vollständigkeit**] – Faktor 2 – wichtig (vgl. Seite 104)

  Zusammenfassung: Die Dokumentation des Security-Frameworks muss die Vollständigkeit der von ihm geschaffenen Lösung beurteilen.

  Begründung der Gewichtung: Die Analyse der Vollständigkeit entspricht einer grundlegenden Selbsteinschätzung des Frameworkkonzepts und erleichtert damit die fachliche Beurteilung und die Spezifikation im Einsatzgebiet zusätzlich erforderlicher Sicherheitsmaßnahmen. Sie ist prinzipiell aus dem Frameworkkonzept ableitbar, aber mit hohem Aufwand verbunden, ohne jedoch Eigenschaften des Betriebs und des Managements einzuschränken.

- [**SF-DOKU-Voraussetzungen**] – Faktor 4 – essentiell (vgl. Seite 78)

  Zusammenfassung: Das Konzept eines Security-Frameworks muss explizit und präzise dokumentieren, welche Voraussetzungen an die bereits vorhandene Infrastruktur gestellt werden, um eine nahtlose Integration und einen reibungslosen Betrieb zu ermöglichen.

  Begründung der Gewichtung: Die Spezifikation der Voraussetzungen ist essentiell für die Entscheidung, ob und mit welchem Aufwand ein Security-Framework in einem konkreten

Szenario eingesetzt werden kann. Ihr Fehlen kann dazu führen, dass Ausschlusskriterien oder die Notwendigkeit weiterer lokaler Maßnahmen nicht rechtzeitig erkannt werden und im weiteren Verlauf zu massiven Einschränkungen beim Betrieb und Management führen.

- **[SF-DOKU-Zertifizierung]** – Faktor 1 – wünschenswert (vgl. Seite 85)

  Zusammenfassung: Die Dokumentation muss darauf eingehen, wie die mit dem Einsatz des Security-Frameworks erzielte Infrastruktur gezielt für dienst- bzw. branchenübliche Zertifizierungen positioniert werden kann.

  Begründung der Gewichtung: Die explizite Beschreibung der Schritte zur Erlangung von Zertifizierungen im Zusammenhang mit dem Frameworkeinsatz stellt zwar einen Mehrwert dar, der in vielen Branchen auch als wichtiges Differenzierungsmerkmal gegenüber alternativen Lösungen fungiert; entsprechende Konzepte können aber auf Basis des angepassten Security-Frameworks auch abgeleitet werden.

- **[SF-DOKU-Ziele]** – Faktor 4 – essentiell (vgl. Seite 85)

  Zusammenfassung: Die Dokumentation muss die mit dem Einsatz des Security-Frameworks verbundenen Ziele sowohl auf organisatorischer als auch auf technischer Ebene explizit spezifizieren.

  Begründung der Gewichtung: Das Übereinstimmen der dem Security-Framework zugrunde liegenden mit den im konkreten Einsatzgebiet vorliegenden Zielen ist ein essentielles Kriterium für die Einscheidung über den Einsatz des Security-Frameworks. Signifikant abweichende oder unbekannte Zielsetzungen bergen das Risiko von sich erst im Laufe der Anpassung oder im Betrieb abzeichnenden massiven Einschränkungen für Betrieb und Management.

- **[SF-DOKU-Zielgruppe]** – Faktor 1 – wünschenswert (vgl. Seite 78)

  Zusammenfassung: Die von der Dokumentation des Security-Frameworks adressierte Zielgruppe muss explizit benannt sein.

  Begründung der Gewichtung: Nur wenige der aktuellen Security-Frameworks sind für verschiedene Zielgruppen (beispielsweise Administratoren oder Sicherheitsverantwortliche) separat dokumentiert. Die Zielgruppen eines Konzepts können aus diesem zwar – ggf. erst nach vollständiger Lektüre – abgeleitet werden; die Handhabung des Konzepts wird durch die explizite Benennung jedoch deutlich vereinfacht.

Die Kategorie [SF-DOKU] umfasst folglich 13 Anforderungen, davon zwei essentielle; die Summe der Gewichtsfaktoren beträgt 24.

3.7.3. Resultierender Kriterienkatalog

Die nachfolgende Tabelle fasst alle Anforderungen mit ihren Gewichten zusammen; sie dient als Anforderungskatalog in den weiteren Kapiteln.

Funktionale Anforderungen [SF-FUNK]			
[SF-FUNK-Abschottung]	2	[SF-FUNK-Auditing]	4
[SF-FUNK-Adaptivität]	1	[SF-FUNK-Automatisierung]	2
[SF-FUNK-Angriffe]	2	[SF-FUNK-Maßnahmen]	4
[SF-FUNK-Assets]	4	[SF-FUNK-Schwachstellen]	2
Integrations- und Betriebsanforderungen [SF-INT]			
[SF-INT-Ausbauphasen]	2	[SF-INT-Modularität]	2
[SF-INT-Customizing]	4	[SF-INT-Parallelbetrieb]	4
[SF-INT-Einführung]	2	[SF-INT-Polyinstanziierbarkeit]	1
[SF-INT-Erweiterung]	2	[SF-INT-Skalierbarkeit]	4
[SF-INT-Hochverfügbarkeit]	2	[SF-INT-Usability]	2
[SF-INT-Kompatibilität]	2	[SF-INT-Wiederverwendbarkeit]	2
Management- und Prozessanforderungen [SF-MGMT]			
[SF-MGMT-Adminkonzepte]	2	[SF-MGMT-Performanz]	2
[SF-MGMT-Berichtsdetails]	2	[SF-MGMT-Policies]	2
[SF-MGMT-Compliance]	4	[SF-MGMT-Praxis]	2
[SF-MGMT-Delegation]	2	[SF-MGMT-Prozesse]	4
[SF-MGMT-Events]	1	[SF-MGMT-Quantifizierung]	2
[SF-MGMT-ITSM-Schnittst.]	4	[SF-MGMT-Releasezyklus]	2
[SF-MGMT-Kosten]	2	[SF-MGMT-Schulungen]	2
[SF-MGMT-KPIs]	1	[SF-MGMT-Support]	1
[SF-MGMT-Mandantenfähigk.]	2	[SF-MGMT-Tests]	1
[SF-MGMT-Metriken]	4	[SF-MGMT-Verbesserung]	4
[SF-MGMT-Operationen]	4	[SF-MGMT-Zuständigkeiten]	1
Dokumentationsanforderungen [SF-DOKU]			
[SF-DOKU-Anford.-analyse]	2	[SF-DOKU-Lifecyclephasen]	1
[SF-DOKU-Angreifermodelle]	2	[SF-DOKU-Vollständigkeit]	2
[SF-DOKU-Ausrichtung]	2	[SF-DOKU-Voraussetzungen]	4
[SF-DOKU-Beurteilung]	1	[SF-DOKU-Zertifizierung]	1
[SF-DOKU-Checkliste]	1	[SF-DOKU-Ziele]	4
[SF-DOKU-Designentscheid.]	2	[SF-DOKU-Zielgruppe]	1
[SF-DOKU-Kontinuum]	1		

Insgesamt werden somit 55 Anforderungen betrachtet, von denen 14 als essentiell, 28 als wichtig und 13 als wünschenswert eingestuft werden.

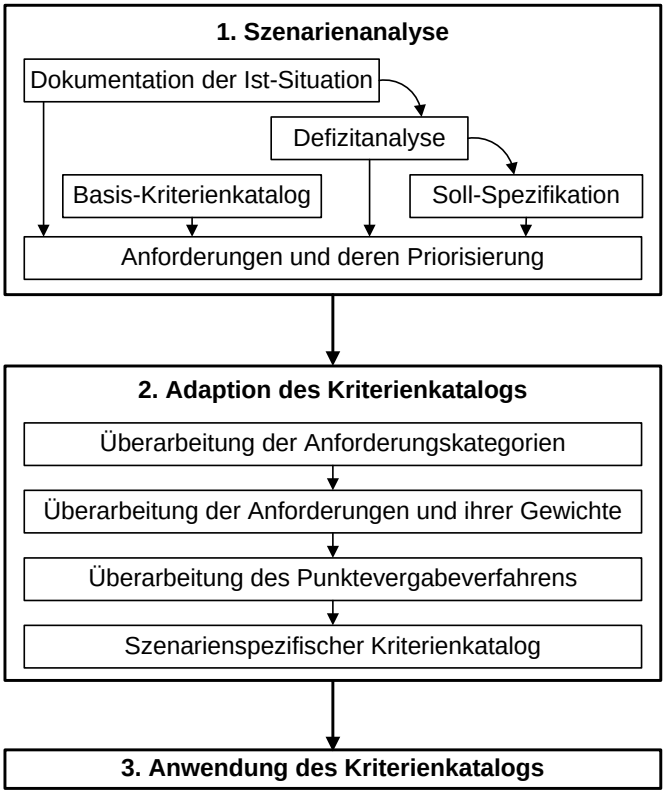


Abbildung 3.22.: Methodik zur szenarienspezifischen Anpassung des Kriterienkatalogs

3.8. Anpassung des Kriterienkatalogs an eigene Szenarien

Der in Abschnitt 3.7.3 vorgestellte Kriterienkatalog fasst die in dieser Arbeit ermittelten, von konkreten Szenarien losgelösten Anforderungen mit dem Ziel zusammen, genau ein Werkzeug zur Analyse vieler verschiedener Security-Frameworks aus den unterschiedlichsten Anwendungsbereichen verwenden zu können. Dieser Kriterienkatalog ist somit zwar auch eine interessante Ausgangsbasis für die Beurteilung von Security-Frameworks in einem konkreten Szenario, muss für diesen Zweck jedoch noch szenarienindividuell gezielt aufbereitet werden. In diesem Abschnitt werden die wichtigsten Schritte zur Integration konkreter Szenariencharakteristika in den Kriterienkatalog und zu dessen Anwendung beschrieben. Durch die Anwendung der hier vorgestellten Methodik und die Wiederverwendung der in dieser Arbeit definierten Kriterien lässt sich somit der szenarienspezifische Analyse- und Evaluationsaufwand minimieren.

Abbildung 3.22 zeigt die nachfolgend diskutierten Schritte innerhalb der drei Phasen *Szenarienanalyse*, *Adaption des Kriterienkatalogs* und *Anwendung des Kriterienkatalogs*.

Die *Szenarienanalyse* soll zunächst ergänzende Informationen über die im Szenario konkret vorliegenden Anforderungen und deren Priorisierung liefern. Dabei kann wie bei der Analyse der in dieser Arbeit vorgestellten Szenarien vorgegangen werden, indem zunächst die aktuelle Situation dokumentiert wird. Auf Basis einer Benennung der vorgefundenen Defizite

und der Skizzierung der angestrebten Soll-Situation können die konkreten Erwartungen an den Einsatz eines oder mehrerer Security-Frameworks im Szenario formuliert werden. Aus der Gegenüberstellung von Soll- und Ist-Situation können anschließend die konkreten Anforderungen abgeleitet und mit szenarienspezifischen Randbedingungen ergänzt werden. Die Ermittlung beider Arten von Anforderungen wird dadurch signifikant erleichtert, dass bereits viele Kriterien in diesem Kapitel diskutiert wurden und somit a priori bekannt sind.

Entscheidend für die Qualität des Ergebnisses dieser ersten Phase ist das zielorientierte Vorgehen bei der *Eingrenzung* der zu analysierenden Szenarienbestandteile. Zum einen muss die Auswahl auf den zu schützenden Infrastrukturteil, beispielsweise einen netzbasierten Dienst, fokussiert sein; zum anderen müssen die erforderlichen Schnittstellen, die sich einerseits z. B. aus *technischen Dienstabhängigkeiten* und andererseits durch die *Management- und Geschäftsprozesse* ergeben, in der notwendigen Breite berücksichtigt werden. Hierfür empfiehlt sich eine *iterative Vorgehensweise*, bei der der Blick zunächst nur auf den technischen Kern gerichtet und nachfolgend sukzessive auf die technische wie auch organisatorische Umgebung ausgeweitet wird, bis sich keine signifikanten Änderungen mehr ergeben.

Zur *Adaption des Kriterienkatalogs* kann anschließend wie folgt vorgegangen werden:

- Es ist zu entscheiden, ob **zusätzliche Anforderungskategorien** verwendet werden sollen bzw. ob bestehende Kategorien gänzlich entfallen können. Bei der Definition neuer Kategorien ist deren Einordnung in die Hierarchie festzulegen: Beispielsweise könnte der Bereich funktionaler Anforderungen in mehrere dienst- bzw. szenarienspezifische Unterkategorien gegliedert werden. Ebenso könnte eine stärkere Differenzierung zwischen Anforderungen des operativen Managements und Anforderungen aus Perspektive der Geschäftsführung gewünscht werden, sodass [SF-MGMT] entsprechend zweigeteilt wird.
- Bei Bedarf oder nach der **Einführung bzw. Entfernung von Anforderungskategorien** müssen die Ebenengewichte der Kategorien angepasst werden. Über diesen Mechanismus können auch szenarienspezifische Prioritäten umgesetzt werden, beispielsweise falls die funktionalen Anforderungen in ihrer Gesamtheit stärker betont werden sollen als die Dokumentationsanforderungen.
- Analog zur Überarbeitung der Kategorien müssen die in ihnen enthaltenen Anforderungen an das jeweilige Szenario angepasst werden. Hierzu können einerseits nicht relevante Anforderungen entfernt und **neue Anforderungen** eingebracht werden. Andererseits müssen die Anforderungen konkretisiert werden, beispielsweise indem die Schwellenwerte für akzeptable Investitions- und Betriebskosten festgelegt oder die Menge relevanter Angriffe spezifiziert wird.
- Ebenso können die **Gewichtsfaktoren** der einzelnen Anforderungen verändert werden. Dies betrifft insbesondere die erwähnten subjektiven bzw. szenarienspezifisch ausgeprägten Anforderungen, z. B. die Benutzerfreundlichkeit des Security-Frameworks, die möglicherweise in einem Szenario irrelevant ist und in einem anderen Szenario ein Ausschlusskriterium darstellt. Nach der Anpassung der Anforderungen und ihrer Gewichtsfaktoren müssen die Ebenengewichte – und implizit damit verbunden auch die globalen Gewichte der Anforderungen – wie in Abschnitt 3.7.1 beschrieben neu berechnet werden.
- Auch die **Bewertung des Erfüllungsgrads** der einzelnen Kriterien kann bei Bedarf angepasst werden. Beispielsweise kann festgelegt werden, dass ein zwar rudimentär be-

rücksichtigtes, aber nicht ausreichend erfülltes Kriterium mit null Punkten statt wie in dieser Arbeit mit einem Punkt bewertet wird. Für den Einsatz der NWA ist in diesem Zusammenhang lediglich relevant, dass dieselbe Punktewertemenge für alle Anforderungen verwendet wird und die relative Gewichtung der Anforderungen innerhalb einer Kategorie somit ausschließlich über deren Ebenengewicht gesteuert werden muss.

Nach Fertigstellung dieser Schritte liegt ein für das konkrete Einsatzgebiet angepasster Anforderungskatalog vor, der zur Beurteilung in Frage kommender Security-Frameworks angewendet werden kann. Die Anwendung des Kriterienkatalogs wird in Kapitel 4 exemplifiziert und deshalb hier nicht näher beschrieben.

Sofern die NWA-basierte Evaluation von in Frage kommenden Security-Frameworks keine eindeutigen Ergebnisse liefert, da beispielsweise zwei oder mehrere Security-Frameworks zu einander sehr ähnlichen Bewertungszahlen führen, sollte nicht versucht werden, durch Modifikationen am Kriterienkatalog klarere Aussagen zu erhalten. Vielmehr kann die NWA in diesem Fall durch andere Verfahren ergänzt werden, bei denen die Lösungsalternativen beispielsweise bezüglich der einzelnen Kriterien direkt miteinander verglichen statt unabhängig voneinander bewertet werden. Aufgrund der hohen Anzahl notwendiger Paarvergleiche eignen sich Verfahren wie der Analytic Hierarchy Process (AHP, [AHP]) jedoch nur, wenn die Menge zu evaluierender Kandidaten vorab bereits geeignet minimiert wurde.

3.9. Checkliste für die Entwicklung neuer Security-Frameworks

Der hier erarbeitete Kriterienkatalog kann nicht nur zur Analyse und zur Bewertung bzw. zum Vergleich von Security-Frameworks herangezogen werden, sondern vielmehr auch als **Leitfaden bei der Spezifikation** neuer oder der Überarbeitung bestehender Security-Frameworks dienen.

In diesem Abschnitt wird als Beispiel für eine solche Aufbereitung des Kriterienkatalogs gezeigt, wie primär durch gezielte Änderungen an der Reihenfolge, in der die Kriterien genannt werden, und Umformulierungen eine Checkliste für Frameworkautoren erstellt werden kann. Die nachfolgenden Ausführungen sind inhaltlich folglich redundant und dienen als Beispiel, wie die Ergebnisse der in dieser Arbeit durchgeführten Anforderungsanalyse kompakt dargestellt und zur weiteren Verwendung durch Frameworkautoren herangezogen werden können: Bei der Konzeption und der Dokumentation neuer Security-Frameworks können auf der hier vorgestellten Basis die für ihren späteren Betrieb und ihr Management relevanten Anforderungen somit von Anfang an strukturiert und mit dem Ziel der möglichst vollständigen Behandlung berücksichtigt werden, sodass sich die Frameworkautoren auf die Inhalte konzentrieren können.

In alle Aufzählungen der Checkliste fließen die Gewichte der einzelnen Anforderungen in die Formulierung der Punkte der Checkliste ein: „muss“ entspricht Faktor 4, „soll“ ist äquivalent zu Faktor 2 und „sollte“ reflektiert Faktor 1 (vgl. [RC2119]).

Zunächst ist bei der Checkliste generell zwischen fachlichen Schwerpunkten und der Art der Präsentation des gesamten Inhalts des Security-Frameworks zu unterscheiden. Inhaltlich werden von einem Security-Framework dabei **drei Schwerpunkte** erwartet:

1. Die technische Architektur (vgl. grob Kategorie [SF-FUNK]),

2. die Managementprozesse (vgl. grob Kategorie [SF-MGMT]) und
3. die Schnittstellen zu relevanten technischen Komponenten und anderen Prozessen aus der Umgebung des Security-Frameworks (vgl. grob Kategorie [SF-INT]) sowohl bei der Einführung als auch im Betrieb.

Bevor auf diese Schwerpunkte nachfolgend einzeln eingegangen wird, werden zunächst die **Randbedingungen** festgehalten, die für das gesamte Security-Framework inklusive dieser drei Themenbereiche zu berücksichtigen sind und somit auch die Struktur der Frameworkdokumentation betreffen (vgl. grob Kategorie [SF-DOKU]):

- In der Dokumentation des Security-Frameworks oder – bei Bedarf – jedem ihrer Bestandteile sollte explizit erwähnt sein, an welche Zielgruppe(n) sie sich wendet, beispielsweise an Entwickler, Administratoren oder den Sicherheitsverantwortlichen (vgl. [SF-DOKU-Zielgruppe]).
- Die mit dem Einsatz des Security-Frameworks verbundenen Ziele müssen explizit benannt sein, wobei zwischen technischen Zielen (IT-Sicherheit), operativen Managementzielen (IT-Sicherheitsmanagement) und Zielen auf Geschäftsebene (Business Management) zu unterscheiden ist (vgl. [SF-DOKU-Ziele]).
- In allen inhaltlichen Bereichen sind vom Frameworkkonzept folgende Aspekte zu berücksichtigen:
  - Zu allen vom Security-Framework vorgeschlagenen technischen und organisatorischen Sicherheitsmaßnahmen müssen die an die bereits vorhandene Infrastruktur gestellten Anforderungen erläutert werden (vgl. [SF-DOKU-Voraussetzungen]).
  - Die Zusammenstellung der technischen und organisatorischen Maßnahmen zum Security-Framework soll unter dem Aspekt der Vollständigkeit der damit erzielbaren Lösung diskutiert werden (vgl. [SF-DOKU-Vollständigkeit]).
  - Die beim Design des Frameworks berücksichtigten Anforderungen sollen dokumentiert werden (vgl. [SF-DOKU-Anforderungsanalyse]).
  - Alle getroffenen Designentscheidungen sollen unter Skizzierung der Alternativen und Entscheidungsargumente begründet werden (vgl. [SF-DOKU-Designentscheidungen]).
  - Bei allen organisatorischen und technischen Maßnahmen sollte der Lebenszyklus des Security-Frameworks (vom Design über die szenarienspezifische Instanziierung bis zur Außerbetriebnahme) berücksichtigt werden (vgl. [SF-DOKU-Lifecyclephasen]).
  - Die Dokumentation des Security-Frameworks sollte eine Checkliste enthalten, die während der Umsetzung abgearbeitet werden oder ggf. durch ihre lineare Struktur selbst als solche fungieren kann (vgl. [SF-DOKU-Checkliste]). Darüber hinaus sollten Merkmale spezifiziert werden, anhand derer der erfolgreiche Einsatz des Security-Frameworks festgemacht werden kann (vgl. [SF-DOKU-Beurteilung]).
  - Bei allen vom Security-Framework ausgewählten Komponenten und spezifizierten Abläufen soll auf Gangbarkeit der vorgeschlagenen Lösungen – insbesondere auch unter dem Aspekt der Benutzerfreundlichkeit – geachtet werden (vgl. [SF-INT-Usability]).

Bei der mit dem Security-Framework vorgestellten **technischen Architektur** sind folgende Aspekte zu beachten:

- Die vom Security-Framework abgedeckten Assets müssen konkret benannt werden (vgl. [SF-FUNK-Assets]).
- Die im Rahmen des Security-Frameworks berücksichtigten Schwachstellen bzw. Verwundbarkeiten und Angriffe sollen diskutiert werden. Dabei sollen auch die zugrunde gelegten Angreifermodelle beschrieben werden (vgl. [SF-FUNK-Schwachstellen], [SF-FUNK-Angriffe] und [SF-DOKU-Angreifermodelle]).
- Die vom Security-Framework selektierten technischen und organisatorischen Schutzmaßnahmen müssen dokumentiert werden (vgl. [SF-FUNK-Maßnahmen]). Dabei soll auch auf ihre Ausrichtung bezüglich des Verlaufs von Angriffen (Prävention, Detektion bzw. Reaktion) eingegangen werden (vgl. [SF-DOKU-Ausrichtung]). Zudem müssen die im Security-Framework zusammengestellten bzw. spezifizierten Komponenten über eine dem Umfeld angemessene Auditingfunktionalität aufweisen (vgl. [SF-FUNK-Auditing]).

Neben der stark technisch orientierten Architektur sind vom Security-Framework die folgenden **managementrelevanten Eigenschaften, Funktionen und Prozesse** zu berücksichtigen:

- Die zum Management des Frameworks bzw. des Zusammenspiels seiner Komponenten notwendigen organisatorischen Abläufe müssen spezifiziert sein (vgl. [SF-MGMT-Prozesse]). Darüber hinaus müssen die Schnittstellen zu den ITSM-Prozessen spezifiziert sein (vgl. [SF-MGMT-ITSM-Schnittstellen]); ebenso soll das Zusammenspiel mit den Unternehmenssicherheitsrichtlinien festgelegt werden (vgl. [SF-MGMT-Policies]).
- Für den Betrieb des Security-Frameworks müssen die für seine Komponenten und deren Zusammenspiel sowie ggf. deren zentrale Steuerung und Kontrolle relevanten Managementoperationen spezifiziert sein (vgl. [SF-MGMT-Operationen]). Die technischen Komponenten sollten dabei auf die dynamische Anpassung, z. B. abhängig von regelmäßigen Lastspitzen oder sich im Laufe der Zeit wandelnden Nutzungsverhaltens, ausgelegt sein (vgl. [SF-FUNK-Adaptivität]). Zudem sollten die von den Frameworkkomponenten erzeugten Events und deren Verarbeitung zu Sicherheitsalarmen festgelegt werden (vgl. [SF-MGMT-Events]).
- Im Rahmen der kontinuierlichen Überwachung des Betriebs und als Basis des Berichtswesens müssen Kennzahlen definiert werden (vgl. [SF-MFGMT-Metriken]). Diese sollen einerseits quantitativ und nicht lediglich qualitativ sein (vgl. [SF-MGMT-Quantifizierung]). Andererseits sollte bei der Auswahl von Kennzahlen darauf geachtet werden, dass einige von ihnen als KPIs in SLAs einfließen könnten (vgl. [SF-DOKU-KPIs]). Darüber hinaus sollten konkrete Beiträge und Schritte zur Erlangung von Zertifizierungen, bei denen auch diese Kennzahlen relevant sein können, dokumentiert sein (vgl. [SF-DOKU-Zertifizierung]).
- Auf Basis u. a. dieser Kennzahlen erstellten Berichte sollen für verschiedene, insbesondere sowohl interne wie auch externe Zielgruppen anpassbar sein; in diesem Zusammenhang soll auch die Architektur Zugriffsbeschränkungen vorsehen, die eine geeignete Abschottung ermöglichen (vgl. [SF-MGMT-Berichtsdetails] und [SF-FUNK-Abschottung]).

- Bei der Beschreibung der Architektur des Security-Frameworks, seines Anpassungsprozesses und seiner Managementabläufe muss das Thema Compliance behandelt werden (vgl. [SF-MGMT-Compliance]).
- Das Security-Framework darf keine einmalige, statische Lösung sein, sondern muss weiterentwickelt und dabei beispielsweise an neue Angriffe und verbesserte Schutzmaßnahmen angepasst werden; diesen kontinuierlichen Verbesserungsprozess und seine Relevanz für den praktischen Einsatz sollte auch die Dokumentation widerspiegeln (vgl. [SF-MGMT-Verbesserung] und [SF-DOKU-Kontinuum]). Er sollte operativ dadurch unterstützt werden, dass Analyseverfahren zur Beurteilung des aktuell erreichten Sicherheitsniveaus inklusive proaktiver Tests vorgegeben werden (vgl. [SF-MGMT-Tests]).
- Die mit der Einführung und dem Betrieb des Security-Frameworks verbundenen Kosten sollen diskutiert werden (vgl. [SF-MGMT-Kosten]). Dabei sollen insbesondere auch Schulungen für verschiedene Zielgruppen (z. B. Administratoren oder Anwender) berücksichtigt werden, deren Bedarf und Inhalte darzulegen sind (vgl. [SF-MGMT-Schulungen]). Ergänzend sollte verdeutlicht werden, in welchem Umfang Supportdienstleitungen beim Einsatz des Security-Frameworks in Anspruch genommen werden können (vgl. [SF-MGMT-Support]).
- Sofern sich das Security-Framework auf einen Dienst bezieht, der für ein zentrales Hosting für mehrere Kunden in Frage kommt, sollen die Aspekte Mandantenfähigkeit und delegierte Administration berücksichtigt werden (vgl. [SF-MGMT-Mandantenfähigkeit] und [SF-MGMT-Delegation]).
- Für das operative Management des Security-Frameworks soll auf für den Dienst übliche Administrationskonzepte gesetzt werden (vgl. [SF-MGMT-Administrationskonzepte]); dazu soll architekturseitig sichergestellt werden, dass der erforderliche Grad an Automatisierung erreicht wird (vgl. [SF-FUNK-Automatisierung]). Zudem sollten die Zuständigkeiten für die einzelnen Bereiche des Frameworkmanagements explizit festgelegt werden (vgl. [SF-MGMT-Zuständigkeiten]).
- Sofern das Security-Framework bereits praktisch eingesetzt wurde, sollen entsprechende Einsatzgebiete skizziert und die im Betrieb gewonnenen Erfahrungen dokumentiert in die Weiterentwicklung einfließen (vgl. [SF-MGMT-Praxis]).

Im Rahmen der Einführung des Security-Frameworks und seines nachhaltigen Betriebs sind ferner die folgenden Punkte abzudecken:

- Das Security-Framework muss einen Customizingprozess zur szenarienspezifischen Anpassung vorsehen (vgl. [SF-INT-Customizing]). Dazu soll es über eine reine Parametrisierung hinaus geeignet modular aufgebaut sein und Schnittstellen für eigene Erweiterungen bieten (vgl. [SF-INT-Modularität] und [SF-INT-Erweiterung]).
- Bei der Auswahl und Zusammenstellung der Frameworkkomponenten soll darauf geachtet werden, dass im Hinblick auf eine einfache Instanziierung und Integration in bereits vorhandene Infrastrukturen zum einen im jeweiligen Dienstumfeld typische Technologien eingesetzt werden und zum anderen bereits vorhandene Komponenten für das Security-Framework wiederverwendet werden können (vgl. [SF-INT-Kompatibilität] und [SF-INT-Wiederverwendbarkeit]). Zudem muss berücksichtigt werden, dass Teile der verwendeten Komponenten und zu schützenden Assets parallel auch von anderen Diens-

ten verwendet und von deren Sicherheitskonzepten abgedeckt werden können (vgl. [SF-INT-Parallelbetrieb]).

- Die Einführung des Security-Frameworks soll über den Anpassungsprozess hinaus methodisch unterstützt werden, beispielsweise indem Meilensteine von Einführungsprojekten skizziert werden (vgl. [SF-INT-Einführung]). Dabei soll die in mehrere Phasen unterteilte Einführung unterstützt werden (vgl. [SF-INT-Ausbauphasen]); bei organisationsübergreifend einzuführenden Security-Frameworks sollte darüber hinaus die pro Einsatzort individuell abgewandelte Instanziierung berücksichtigt werden (vgl. [SF-INT-Polyinstanziierbarkeit]). Ebenso soll die kontinuierliche Verbesserung durch eine Spezifikation der Verzahnung der Frameworkreleasezyklen mit dem Release und Change Management im Einsatzgebiet unterstützt werden (vgl. [SF-MGMT-Releasezyklus]).
- Das Security-Framework soll bezüglich der Zusammenstellung der Komponenten die üblichen und notwendigen Hochverfügbarkeitskonzepte unterstützen und eine für den Einsatz in komplexen Szenarien ausreichende Skalierbarkeit aufweisen (vgl. [SF-INT-Hochverfügbarkeit] und [SF-INT-Skalierbarkeit]). Insbesondere soll es sich diesbezüglich nahtlos in die vorhandenen Performance-Managementprozesse integrieren (vgl. [SF-MGMT-Performanz]).

Analog zu der oben vorgestellten Checkliste kann der Anforderungskatalog durch Auswahl, Vereinfachung und Reihenfolgeänderung auch für weitere unterstützende Maßnahmen eingesetzt werden, beispielsweise in Form von Dokumentenvorlagen für Security-Frameworks, die sich an jeweils verschiedene Zielgruppen wenden. Auf die Ausarbeitung weiterer Beispiele wird an dieser Stelle verzichtet, da sich daraus keine wesentlichen inhaltlichen Neuerungen ergeben.

3.10. Zusammenfassung

In diesem Kapitel wurden eingangs Anforderungen an Security-Frameworks und ihre Managementeigenschaften aus vier Szenarien ermittelt. Dabei wurde zunächst eine Charakterisierung von Szenarien, in denen der Einsatz von Security-Frameworks attraktiv ist, vorgenommen, um darauf aufbauend durch entsprechende Szenarienselektion ein möglichst breites Spektrum an Anforderungen zu erhalten. Die im Anschluss zur Szenarienanalyse eingesetzte, einheitliche Methodik ist auf die Anwendung in eigenen Szenarien übertragbar und liefert als Ergebnis Bewertungskriterien, die in vier Kategorien eingeteilt wurden: Funktionale Anforderungen, Anforderungen an Integration und Betrieb, Anforderungen an Managementprozesse bzw. Managementschnittstellen und Anforderungen an die Dokumentation von Security-Frameworks. Ergänzt um aus verwandten Arbeiten zusammengetragene Anforderungen wurden insgesamt 55 Anforderungen und ihre Hintergründe betrachtet.

Um die ermittelten Anforderungen effizient zur Analyse existierender Security-Frameworks einsetzen zu können, wurden sie anschließend begründet gewichtet. Zum Einsatz der Nutzwertanalyse als Bewertungsverfahren wurden neben den Gewichtungskriterien auch die Punktevergaberegeln spezifiziert, die den Erfüllungsgrad jeder Anforderung bemessen. Der resultierende Anforderungskatalog unterscheidet zwischen 14 essentiellen, 28 wichtigen und 13 wünschenswerten Anforderungen an Security-Frameworks, die sich auf die vier genannten Kategorien verteilen.

Auf Basis der bei der Erstellung des Kriterienkatalogs angewandten Methodik wurde eine Vorgehensweise zu seiner Anpassung an eigene, konkrete Szenarien vorgestellt, die insbesondere die gezielt unterstützte Ergänzung szenarienspezifischer Anforderungen und die optionale Repriorisierung der Bewertungskriterien vorsieht. Die Ergebnisse dieser Arbeit vereinfachen somit unmittelbar die Evaluation von Security-Frameworks in der Praxis. Als weiteres Beispiel dafür, wie der erarbeitete Kriterienkatalog gewinnbringend eingesetzt werden kann, wurde eine Checkliste für die Autoren von Security-Frameworks erstellt, die in kompakter Form alle Anforderungen zusammenfasst und somit dazu beiträgt, dass beim Design neuer oder der Überarbeitung bestehender Security-Frameworks von Anfang an alle Kriterien berücksichtigt werden können, um ein qualitativ hochwertiges Ergebnis zu erhalten.

Neben diesen konkreten Anwendungsmöglichkeiten in eigenen Szenarien dient der zusammengestellte Kriterienkatalog insbesondere als Basis für die Untersuchung aktueller Security-Frameworks im folgenden Kapitel; zudem ist die Erfüllung ausgewählter Anforderungen eine Grundvoraussetzung für die in Kapitel 6 diskutierten Managementprozesse.

Kapitel 4.

Aktueller Stand der Security-Framework-Technik

Inhalt dieses Kapitels

In diesem Kapitel werden ausgewählte Security-Frameworks vorgestellt und auf Basis des in Kapitel 3 erarbeiteten Kriterienkatalogs analysiert, um konkrete Ansatzpunkte für weitere Verbesserungen zu ermitteln und die Motivation für die Schwerpunkte dieser Arbeit aufzuzeigen.

Hierzu wird zunächst in Abschnitt 4.1 eine grobe **Kategorisierung der aktuellen Security-Frameworks** vorgenommen. Anschließend wird die **Recherchemethodik**, mit der die für die Analyse in Frage kommenden Security-Frameworks ermittelt wurden, vorgestellt. Ebenso wird diskutiert, anhand welcher Kriterien die in dieser Arbeit näher betrachteten Security-Frameworks ausgewählt wurden. Darauf aufbauend wird eine **knappe Übersicht** über die im weiteren Verlauf behandelten Security-Frameworks gegeben. Diesen Überblick abschließend wird erneut die Problematik aufgegriffen, dass der Begriff Security-Framework in Wissenschaft und Industrie bislang relativ unscharf verwendet wird und dass

Abbildung 4.1.: Vorgehensmodell in diesem Kapitel

das **Design von Security-Frameworks** mangels übergeordneter Richtlinien von den jeweiligen Autoren mit entsprechenden Auswirkungen auf die Ergebnisse teilweise sehr unterschiedlich angegangen wird.

In Abschnitt 4.3 werden anschließend zwei begründet ausgewählte, aktuelle Security-Frameworks im Detail untersucht. In diesem Rahmen wird zunächst die im vorherigen Kapitel vorgestellte **Anwendungsmethodik für den Kriterienkatalog exemplifiziert** und darauf basierend gezeigt, wie die **Ergebnisse** mit dem Ziel einer weiteren Verbesserung des jeweiligen Security-Frameworks zu **interpretieren** sind. Diese Vorgehensweise wurde im Rahmen der Literaturrecherche analog auf die **über 70 vorgestellten Security-Frameworks** angewandt; die Ergebnisse werden in Abschnitt 4.4 kompakt dargestellt, d. h. der Erfüllungsgrad der über 50 Einzelkriterien wird lediglich in Form der Bewertungspunkte und einer kurzen Zusammenfassung angegeben, folgt jedoch wie ausführlich in Abschnitt 4.3 gezeigt genau den in Abschnitt 3.7.1 gesetzten Maßstäben.

Auf Basis dieser umfangreichen Analyse zeichnen sich die **typischen Stärken** und die **tendenziellen Schwächen aktueller Security-Frameworks** deutlich ab. In Abschnitt 4.5 werden diese Resultate – differenziert nach den vier Kategorien SF-FUNK, SF-INT, SF-MGMT und SF-DOKU – zusammengetragen und bezüglich der **Konsequenzen für den praktischen Einsatz** und im Hinblick auf die **Schwerpunkte dieser Arbeit** diskutiert. Eine Zusammenfassung schließt das Kapitel, dessen Struktur in Abbildung 4.1 dargestellt ist, ab.

4.1. Aktuelle Security-Frameworks

Die Methodik, mehrere sicherheitsrelevante Aspekte in Form eines Rahmenwerks zusammenzufassen, hat sich nicht erst in den letzten Jahren herausgebildet, sondern wird praktiziert, seit in der Wissenschaft und der Industrie eine strukturierte Auseinandersetzung mit dem Thema IT-Sicherheit stattfindet. Dabei sind jedoch insbesondere solche Security-Frameworks, die vor vielen Jahren entstanden sind und seit der Veröffentlichung ihres Konzepts nicht aktualisiert wurden, aufgrund der Weiterentwicklung sowohl der zu schützenden Infrastruktur als auch der relevanten Schwachstellen, Angriffe und Gegenmaßnahmen aus heutiger Sicht in der Regel inhaltlich veraltet.

Für die Analyse des Stands der Technik im Rahmen dieser Arbeit ist deshalb zunächst zu klären, welche Security-Frameworks näher betrachtet werden sollen und wie bei der Analyse von Arbeiten aus diesem Umfeld vorzugehen ist. Zu diesem Zweck wird in Abschnitt 4.1.1 zunächst eine zwar nur grobe, für die Strukturierung der größeren Anzahl vorhandener Arbeiten aber sehr hilfreiche Kategorisierung von Security-Frameworks vorgenommen. Darauf aufbauend wird in Abschnitt 4.1.2 erläutert, welche Methodik bei der Recherche nach und Auswahl von Security-Frameworks angewandt wurde und als Überblick eine knappe Aufzählung der Ergebnismenge vorgestellt. In Abschnitt 4.2 wird anschließend ein Überblick darüber gegeben, welchen Designkonzepten die aktuellen Security-Frameworks typischerweise folgen; mangels dokumentierter Richtlinien oder Best Practices, an denen sich die Autoren von Security-Frameworks bislang hätten orientieren können, spiegelt dieser Überblick eine empirische Analyse der Struktur der ausgewählten Security-Frameworks wider und darf nicht als Soll-Spezifikation verstanden werden.

4.1.1. Arten und Schwerpunkte von Security-Frameworks

Wie bereits in Kapitel 2 bei der Beschreibung von Sicherheitsmaßnahmen und -mechanismen erörtert wurde, findet erst nach und nach eine top-down-strukturierte Kategorisierung der vielen verschiedenen Teilbereiche der Informationssicherheit statt. Trotz der größeren Anzahl an Arbeiten, die als Ergebnis ein Security-Framework liefern oder sich zumindest mit Teilaspekten davon beschäftigen, fehlt bislang insbesondere auch eine Taxonomie für Security-Frameworks.

Analog zur Charakterisierung von Szenarien und Security-Framework-Einsatzgebieten in Kapitel 3 wird deshalb nachfolgend eine rudimentäre Kategorisierung von Security-Frameworks vorgenommen. Sie erfolgt an dieser Stelle bewusst nur grob granuliert und mit dem primären Ziel, die nachfolgende Analyse strukturiert darstellen zu können. Diese Kategorisierung könnte zwar anhand der von den Security-Frameworks abgedeckten funktionalen Bereiche, insbesondere der berücksichtigten Assets und angewandten Sicherheitsmechanismen, feiner untergliedert werden. Für die im Vordergrund stehende Analyse der Managementeigenschaften ist dies jedoch insbesondere unter der Randbedingung des parallelen Einsatzes mehrerer verschiedener Security-Frameworks im selben Szenario nicht erforderlich, so dass später bei Bedarf auch eine feinere Differenzierung anhand anderer Merkmale vorgenommen werden kann.

Für die nachfolgende Vorstellung der gewählten Kategorien von Security-Frameworks wurde der folgende Aufbau gewählt: Zunächst erfolgt eine kurze Beschreibung der **Ziele** der jeweiligen Art von Security-Frameworks, die durch knappe **Beispiele** verdeutlicht wird. Auf dieser

Basis schließt sich eine **Gegenüberstellung mit der Definition des Begriffs Security-Framework** aus Abschnitt 2.5 an. Darauf aufbauend wird die Bedeutung der Frameworkkategorie für diese Arbeit beurteilt und skizziert, welche **Schwerpunkte** bei der Berücksichtigung und Erfüllung der in Kapitel 3 postulierten Anforderungen zu erwarten sind. Diese resultieren unter anderem daraus, dass sich Security-Frameworks zum Teil auf ausgewählte Lebenszyklusphasen wie die Entwicklung sicherer Software beschränken. Dadurch ergeben sich einerseits häufig implizite Annahmen der Frameworkautoren, beispielsweise über die Einsatzszenarien oder die Zielgruppe der Konzeptdokumentation. Diese Randbedingungen müssen bei einer wohlwollend kritischen Beurteilung von Security-Frameworks aus vielen verschiedenen Bereichen mit dem Ziel eines Vergleichs und der Ableitung von Verbesserungsmöglichkeiten adäquat berücksichtigt werden. Andererseits verschiebt sich die Erwartungshaltung an Security-Frameworks, die sich explizit auf ausgewählte inhaltliche Bereiche beschränken, dahingehend, dass deren feinere Untergliederung – beispielsweise der Software-Designphase in mehrere Abschnitte – berücksichtigt wird.

In den nächsten Abschnitten werden die drei für diese Arbeit gewählten Kategorien von Security-Frameworks – für das Software Engineering, für einzelne IT-Dienste bzw. für komplexe IT-Architekturen – unter diesen Aspekten erläutert.

4.1.1.1. Security-Frameworks für das Software Engineering

Die erste Kategorie von Security-Frameworks ist auf den Einsatz im Rahmen von Softwareentwicklungsprozessen ausgelegt und zielt darauf ab, das Design, die Implementierung und das Testen von Softwareprodukten aus IT-Sicherheitsperspektive nicht nur punktuell, sondern großflächig zu unterstützen. Beispielsweise werden von Security-Frameworks dieser Kategorie umfangreiche und komplexe Themenbereiche wie Access Control, die – wie in Abschnitt 2.4.2 diskutiert – verschiedene Komponenten zur Authentifizierung und Autorisierung umfassen, für konkrete Programmiersprachen wie Java oder C# behandelt.

Bezugnehmend auf die Definition des Begriffs Security-Framework (siehe Seite 50) ergeben sich abweichend von den weiteren Kategorien von Security-Frameworks einige **Besonderheiten**, die bei der Analyse bewusst sein müssen: So können die vom Security-Framework geschützten Assets grundsätzlich nicht a priori konkret benannt werden, da es sich hierbei um die vom Frameworkanwender zu realisierenden Softwareprodukte handelt; entsprechend muss eine möglichst universelle Eignung für beliebige Softwareprodukte im Vordergrund stehen. Analog dazu können keine konkreten Schwachstellen dieses Produkts berücksichtigt werden, sondern es wird vielmehr ein Beitrag zur Vermeidung potentieller Sicherheitslücken geleistet. Die szenariengetriebene Adaption ist bei Security-Frameworks für das Software Engineering im Wesentlichen mit deren konzeptioneller Integration in das Softwareprodukt gleichzusetzen. Schließlich entspricht die Instanziierung des Frameworks entweder seiner Implementierung als Bestandteil des Softwareprodukts oder z. B. der Nutzung der von den Frameworkautoren bereitgestellten Funktionsbibliotheken im Rahmen der Produktimplementierung.

Wie die in Abschnitt 4.4 diskutierte Analyse bestehender Security-Frameworks dieser Kategorie zeigt, werden die Zielgruppen nur selten explizit im Frameworkkonzept genannt. Bezugnehmend auf die in Abschnitt 2.2.1 definierten Rollen ist jedoch in den meisten Fällen offensichtlich, dass sich die Security-Frameworks für das Software Engineering typischerweise fast ausschließlich an Softwarearchitekten, -designer und -entwickler sowie zum Teil an

Technologieexperten wenden.

Durch die Einschränkung, dass ein Security-Framework für das Software Engineering keine unmittelbar vom operativen Management zu verwaltende Entität ist, sind Vertreter dieser Frameworkkategorie zwar insbesondere für die Verbesserung der IT-Sicherheitseigenschaften von Softwareprodukten sehr wichtig. Im weiteren Verlauf dieser Arbeit können sie aber nur indirekt betrachtet werden, da sie ohne die konkrete Einbettung in ein Softwareprodukt nicht als einzuführende, zu betreibende und zu verwaltende Entität existieren können. Somit müssten jedoch auch primär an dieses Produkt – und nicht direkt an das verwendete Security-Framework – die Anforderungen aus den beiden Kategorien SF-INT und SF-MGMT gestellt werden. Diese Einschränkungen werden bei der Analyse der in diese Kategorie fallenden Security-Frameworks deutlich und im Weiteren entsprechend berücksichtigt.

4.1.1.2. Security-Frameworks für einzelne IT-Dienste

Ein Security-Framework für einen (einzelnen) IT-Dienst zielt darauf ab, dass aus ihm szenarienspezifische Sicherheitslösungen für den entsprechenden Dienst an sich, aber auch für die ihm dedizierten **Komponenten** und **Subdienste** sowie – bis zu einem festzulegenden Grad – **externe Dienstabhängigkeiten** abgeleitet werden können. So würde sich beispielsweise ein Security-Framework für den Dienst „E-Mail-Server“ typischerweise nicht nur mit dem zentralen Message Transfer Agent (MTA) auseinandersetzen, sondern auch auf Komponenten für Spam- und Virenschutz sowie z. B. das für das eingesetzte Protokoll SMTP relevante Zusammenspiel mit DNS-Servern und deren in diesem Kontext relevante Sicherheitseigenschaften eingehen.

Für die direkte Gegenüberstellung mit dem auf Seite 50 definierten Security-Framework-Begriff bedeutet dies grundlegend, dass als Assets dieser Art von Security-Frameworks sowohl die Dienstkomponenten als auch die unmittelbar relevanten Subdienste aufzufassen sind, für die je nach Abstraktionsgrad des betrachteten Dienstes konkrete oder allgemeine Schwachstellen und Angriffe zu berücksichtigen sind: Im obigen Beispiel sind offensichtlich konkretere Aussagen zu erwarten, wenn sich das Security-Framework auf eine spezifische E-Mail-Server-Software und nicht die Thematik im Allgemeinen bezieht. Damit eng verbunden ist die Notwendigkeit, im Rahmen des Security-Frameworks Annahmen über die in den Anwendungsszenarien vorliegenden Dienstinstanzen zu treffen – beispielsweise, ob es sich um Installationen mit typischem bzw. voreingestelltem oder erweiterten Funktionsumfang handelt. Im Beispiel kann die Flexibilität des Security-Frameworks unter anderem daran beurteilt werden, ob es sowohl auf E-Mail-Server in kleinen und mittelständischen Unternehmen als auch für professionelles, mandantenfähiges E-Mail-Hosting durch spezialisierte IT-Dienstleister anwendbar ist.

Aufgrund der breiten Ausrichtung dieses Frameworktyps können im Unterschied zu den Security-Frameworks für das Software Engineering a priori keine generellen Annahmen z. B. über die Zielgruppen des Frameworkkonzepts gemacht werden. Security-Frameworks für IT-Dienste bilden somit einen der Schwerpunkte bei den weiteren Betrachtungen in dieser Arbeit.

4.1.1.3. Security-Frameworks für komplexe IT-Architekturen

Als dritte Kategorie von Security-Frameworks werden solche für IT-Architekturen analysiert. Sie zeichnen sich dadurch aus, dass sie nicht einen einzelnen Dienst, sondern mehrere, in geeignetem Zusammenhang zueinander stehende Dienste, die von den jeweiligen Anwendern auch unabhängig voneinander genutzt werden könnten, betrachten. In diese Kategorie fallen beispielsweise Security-Frameworks für das (internationale) Grid Computing, für nationale E-Health-Infrastrukturen und Enterprise Security Frameworks, wobei die geographische Verteilung der Dienste und Komponenten zwar keine zwingende Voraussetzung, aber eine in realen Szenarien häufig anzutreffende Eigenschaft ist.

Offensichtlich erhöht sich die Komplexität dieser Security-Frameworks mit der Anzahl beteiligter Dienste, da nicht nur deren spezifische Schwachstellen und Angriffe, sondern auch ihre Abhängigkeiten und ihr Zusammenspiel auf technischer wie auch organisatorischer Ebene berücksichtigt werden müssen. Aufgrund des damit verbundenen Konzeptions- und Dokumentationsaufwands liegt nahe, dass nur eine überschaubare Anzahl von Security-Frameworks aus dieser Kategorie sowohl in die Breite als auch die Tiefe geht; häufig werden lediglich ausgewählte Aspekte in der Tiefe behandelt. Dadurch ergibt sich wiederum die Herausforderung in der Praxis, verschiedene Ansätze geeignet miteinander oder mit lokal erarbeiteten Konzepten kombinieren zu müssen. Bei der Analyse und Beurteilung sind deshalb insbesondere der Aspekt der Vollständigkeit und die im Security-Framework bereits vorgesehenen Schnittstellen und Erweiterungsmöglichkeiten zu berücksichtigen.

Aufgrund der thematischen Breite läge es nahe, dass sich Security-Frameworks für IT-Architekturen, die in den weiteren Kapiteln dieser Arbeit ebenfalls als Schwerpunkt betrachtet werden, verstärkt mit den Integrations- und Managementeigenschaften befassen und im Gegenzug für die Sicherheitsfunktionalität auf bereits vorhandene Arbeiten zurückgreifen. Bei den untersuchten Arbeiten zeigt sich jedoch deutlich, dass die technischen Aspekte wie bei den anderen Kategorien überwiegen; der Fokus liegt dabei sowohl auf der Auswahl und Integration bestehender als auch auf der Entwicklung komplementärer, spezifischer Sicherheitsmechanismen.

4.1.2. Überblick über aktuelle Security-Frameworks

In diesem Abschnitt wird ein knapper Überblick über die in diesem Kapitel analysierten Security-Frameworks gegeben. Um Transparenz zu schaffen, werden im Folgenden zunächst die angewandte Recherchemethodik und die Selektionskriterien skizziert, die zur Auswahl der letztlich analysierten aus allen ermittelten Security-Frameworks dienten. Daran anschließend werden die ausgewählten Security-Frameworks tabellarisch dargestellt.

4.1.2.1. Recherchemethodik und Selektionskriterien

Die Ermittlung, Auswahl und Analyse der in diesem Kapitel betrachteten Arbeiten erfolgte auf Basis der Richtlinien für *Systematic Reviews*, einem ursprünglich in der medizinischen Forschung weit verbreiteten Verfahren, das von Kitchenham auf Anwendungen in der Informatik, insbesondere im Umfeld des Software Engineering, übertragen wurde [SYSREV]. Es zielt

darauf ab, möglichst alle für eine Forschungsfragestellung relevanten Arbeiten so zu ermitteln und auszuwerten, dass belastbare, vollständige und objektiv nachvollziehbare Ergebnisse erarbeitet werden.

Für die vorliegende Arbeit wurde eine umfassende Literaturrecherche durchgeführt. Komplementäre Ansätze, beispielsweise Befragungen von Security-Framework-Autoren oder an Unternehmen gerichtete Anfragen, wurden nur in wenigen Einzelfällen und somit nicht systematisch verfolgt, da kein signifikanter Beitrag zur weiteren Ergänzung der ermittelten Security-Frameworks zu erwarten war.

Die Literaturrecherche zielte darauf ab, alle in deutscher oder englischer Sprache verfassten Arbeiten, die sich *konzeptionell* mit Security-Frameworks im Sinne dieser Arbeit befassen, zu ermitteln. Als Konsequenz resultiert ein starker Fokus auf andere *wissenschaftliche* Arbeiten, da bei den überwiegend kommerziellen Software- bzw. Appliance-Produkten in der Regel keine Dokumente frei zugänglich waren, in denen die für diese Arbeit wichtigen Hintergrundinformationen und Konzepte erläutert werden. Auf die damit verbundenen Herausforderungen im praktischen Einsatz wird deshalb separat in den Kapiteln 5 und 6 eingegangen.

Zur Ermittlung in Frage kommender Arbeiten wurden – jeweils soweit technisch unterstützt – deren Titel, Zusammenfassung (engl. *abstract*) und Volltext durchsucht. Als Stichworte wurden neben *„security framework“* auch Synonyme (z. B. *„security architecture“*) und jeweils alle vier Kasus sowie Singular- und Pluralformen sowie die entsprechenden deutschen Begriffe verwendet. Es wurden folgende Recherchewerkzeuge und Vorgehensweisen eingesetzt:

- Die Online-Recherchewerkzeuge der Münchner Universitätsbibliotheken sowie der Verlage und Datenbankanbieter ACM, Elsevier, IEEE Xplore und Metapress / Springer wurden zur Ermittlung von Konferenzbeiträgen in Tagungsbänden, Journalartikeln und Büchern bzw. Buchkapiteln verwendet.
- Über Internet-Suchmaschinen wie Google Scholar wurden technische Berichte, Abschlussarbeiten, Dissertationen und Habilitationsschriften ermittelt.
- Die Literaturverweise und -verzeichnisse aller so ermittelten Arbeiten wurden mit folgenden Einschränkungen rekursiv ausgewertet: Eine Arbeit, auf die verwiesen wird, wurde nur dann als relevant eingestuft, wenn sie eines der relevanten Stichwörter im Titel trägt oder von der referenzierenden Arbeit als Security-Framework (oder Synonym davon) bezeichnet wird.
- Mittels Internet-Suchmaschinen und -Buchhandlungen wurden Webseiten, Produktbeschreibungen und Fachbücher, d. h. weitere, nicht-wissenschaftliche Literatur ermittelt.

Um die Menge der analysierten Arbeiten überschaubar zu halten, wurde die zustande gekommene Kandidatenmenge wie folgt mit dem Ziel, die am stärksten relevanten Arbeiten auszuwählen, eingeschränkt:

- Es wird nur Literatur betrachtet, die im oder nach dem Jahr 2000 veröffentlicht wurde. Dies zielt angesichts der kontinuierlichen Weiterentwicklung von zu schützenden Assets, Verwundbarkeiten, Angriffen und Sicherheitsmaßnahmen darauf ab, möglichst keine inhaltlich inzwischen völlig veralteten Arbeiten in die Gesamtbeurteilung mit einzubeziehen. Für den Fall, dass besonders gelungene Arbeiten als Basis oder Vorlage für weitere Security-Frameworks dienen, wurden begründete Ausnahmen zugelassen.

- An die analysierten Arbeiten wird die Anforderung gestellt, dass sie zumindest die grundlegenden Eigenschaften von Security-Frameworks im Sinne dieser Arbeit (vgl. Definition auf Seite 50) erfüllen; hierzu gehört:
  1. Die Anpassung des in der jeweiligen Arbeit vorgestellten Konzepts an eigene Szenarien muss zumindest theoretisch möglich sein. Durch dieses Kriterium sollen Arbeiten, die sich selbst als Security-Framework bezeichnen, im Kontext dieser Arbeit jedoch als Sicherheitskonzepte für jeweils nur ein festes Szenario gelten, ausgeschlossen werden.
  2. Die jeweilige Arbeit muss mindestens auf zu schützende Assets und einzusetzende Sicherheitsmaßnahmen eingehen. Dadurch sollen einerseits allgemeine, von konkreter Anwendung abstrahierte Sicherheitsempfehlungen und andererseits Sicherheitsanalysen ohne dazu passende Handlungsempfehlungen ausgeschlossen werden.
- In den Fällen, dass zu einem Security-Framework mehrere Publikationen vorliegen, wurde wie folgt verfahren:
  1. Sofern die einzelnen Veröffentlichungen inhaltlich aufeinander aufbauen, wurden sie als Ganzes betrachtet und als zusammenhängendes Frameworkkonzept ausgewertet.
  2. Bei zeitnaher Veröffentlichung derselben Arbeit in verschiedenen Varianten, beispielsweise in Form einer Dissertation und eines Journalartikels, wurde die bezüglich ihrer Darstellung ausführlichere Fassung analysiert.
  3. Bei zeitnaher Veröffentlichung derselben Arbeit in vergleichbarem Umfang, aber in verschiedenen Sprachen (deutsch; englisch), wurde die englische Fassung analysiert, da sie einen größeren Leser-/Anwenderkreis anspricht.
  4. Andernfalls wurde die jeweils neueste Publikation des Security-Frameworks bewertet, wobei sich die Vorarbeiten gegebenenfalls positiv auf die Anforderung SF-MGMT-Verbesserung auswirken.

Die auf diese Weise ermittelte Menge an Arbeiten erhebt somit zwar keinen Anspruch auf Vollständigkeit, hat sich jedoch – wie unten ersichtlich wird – als überaus ausreichend für die Ableitung konkreter Aussagen über den aktuellen Stand der Security-Framework-Technik erwiesen.

4.1.2.2. Verzeichnis analysierter Security-Frameworks

Nachfolgend wird eine nach den identifizierten Security-Framework-Kategorien sortierte, grobe Übersicht über die auf Basis des oben erläuterten Verfahrens ermittelten und in dieser Arbeit analysierten Literatur gegeben. Für jedes Security-Framework werden der Titel, die Autoren, das Veröffentlichungsjahr sowie die Seite, auf der die Analyse vorgestellt wird, angegeben.

Security-Frameworks für das Software Engineering:

Titel	Autor(en)	Referenz	Jahr	Seite
A generic framework for context-based distributed authorizations	Mostéfaoui; Brezillon	[MB03]	2003	168

Titel	Autor(en)	Referenz	Jahr	Seite
A Multi-Tier, Multi-Role Security Framework for E-Commerce Systems	Cachia; Micallef	[CM07]	2007	169
A Policy Language for Adaptive Web Services Security Framework	Che	[Che07]	2007	170
A Public Web Services Security Framework Based on Current and Future Usage Scenarios	Thelin; Murray	[TM02]	2002	171
A Security Framework for a Mobile Agent System	Bryce	[Bry00]	2000	172
An adaptable security framework for service-based systems	Yau; Yao; Chen; Zhu	[YYCZ05]	2005	173
An aspect-oriented security framework	Shah; Hill	[SH03]	2003	174
Guide to Microsoft .NET Framework Security	NSA	[NSA04]	2004	175
Java^{TM} security overview	Sun Microsystems	[Sun05]	2005	175
SAgent: A Security Framework for JADE	Gunupudi; Tate	[GT06]	2006	177
The Generalized Security Framework	Detry; Kleban; Moore	[DKM01]	2001	178
UDDI and WSDL extensions for Web services: a security framework	Adams; Boeyen	[AB02]	2002	179
Using aspects for security engineering of web service compositions	Charfi; Mezini	[CM05]	2005	180

Security-Frameworks für einzelne IT-Dienste:

Titel	Autor(en)	Referenz	Jahr	Seite
A dynamic, context-aware security infrastructure for distributed healthcare applications	Hu; Weaver	[HW04]	2004	181
A general framework for robust watermarking security	Barni; Bartolini; Furon	[BBF03]	2003	182
A new security framework for HIPAA-compliant health information systems	Tulu; Chatterjee	[TC03]	2003	183
A policy-based security framework for Web-enabled applications	Ventuneac; Coffey; Salomie	[VCS03]	2003	184
A security framework for an ERP system	Marnewick; Labuschagne	[ML05]	2005	185
A Security Framework for Collaborative Distributed System Control at the Device-Level	Xu; Korba; Wang; Hao; Shen; Lang	[XKW^{+}03]	2003	186

Titel	Autor(en)	Referenz	Jahr	Seite
A security framework for mobile-to-mobile payment network	Das; Saxena; Gulati	[DSG05]	2005	187
A software framework for autonomic security in pervasive environments	Saxena; Lacoste; Jarboui; Lucking; Steinke	[SLJ+07]	2007	188
A Unified Security Framework for Networked Applications	Abendroth; Jensen	[AJ03]	2003	188
An Integrated Security Framework for XML based Management	Cridlig; State; Festor	[CSF05]	2005	190
Energy efficient security framework for wireless local area networks	Kiratiwintakorn	[Kir05]	2005	159
iSecurity: A Security Framework for Interactive Workspaces	Song; Tobagus; Leong; Johanson; Fox	[STL+03]	2003	191
Linux Security Modules: General Security Support for the Linux Kernel	Wright; Cowan; Smalley; Morris; Kroah-Hartman	[WCS+02]	2002	192
Location-based security framework for use of handheld devices in medical information systems	Hansen; Oleshchuk	[HO06]	2006	193
Performance Analysis of Unified Enterprise Application Security Framework	Shaikh; Sharif; Ahmed	[SSA05]	2005	194
PITMA Security Framework – Policy, Implementation, Training, Maintenance and Auditing	PITMA	[PIT08]	2008	195
Scalable multicast security with dynamic recipient groups	Molva; Pannetrat	[MP00]	2000	196
SecureTorrent: A Security Framework for File Swarming	Wilson; Machanick	[WM06]	2006	197
Security for Internet banking: a framework	Hutchinson; Warren	[HW03]	2003	198
Security framework for DPWS Compliant Devices	Hernández; López; Prieto; Martínez; García; Da-Silva	[HLP+09]	2009	199
Security Framework for IP Telephony White Paper	Dadoun	[Dad02]	2002	200
Security Framework for Mobile Applications	Petersen	[Pet08]	2008	201
Security Framework in a Virtual Large-Scale Disk System	Uehara	[Ueh08]	2008	202
Sicherheitskonzepte in global verteilten Anwendungen	Rubarth	[Rub07]	2007	203
Study on Security Framework in E-Commerce	Tao; Xue	[TX07]	2007	204

Titel	Autor(en)	Referenz	Jahr	Seite
Towards an IPv6-based security framework for distributed storage resources	Bassi; Laganier	[BL03]	2003	205

Security-Frameworks für komplexe IT-Architekturen:

Titel	Autor(en)	Referenz	Jahr	Seite
A Context-Aware Security Architecture for Emerging Applications	Covington; Fogla; Zhan; Ahamad	[CFZA02]	2002	206
A Framework for an Institutional High Level Security Policy for the Processing of Medical Data and their Transmission through the Internet	Pangalos; Ilioudis	[PI01]	2001	207
A framework for security on NoC technologies	Gebotys; Gebotys	[GG03]	2003	208
A hierarchical framework model of mobile security	Sun; Howie; Koivisto; Sauvola	[SHKS01]	2001	209
A multi-agent security framework for e-health services	Sulaiman; Sharma; Ma; Tran	[SSMT07]	2007	210
A New Grid Security Framework with Dynamic Access Control	Xie; Gui; Li; Qian	[XGLQ04]	2004	211
A policy based approach to security for the semantic web	Kagal; Finin; Joshi	[KFJ03]	2003	212
A Policy-based Security Framework for Ad-hoc Networks	Keoh	[Keo05]	2005	213
A Security Framework for Card-Based Systems	Tsiounis	[Tsi02]	2002	214
A security framework for distributed brokering systems	Pallickara; Pierce; Fox; Yan; Huang	[PPF+03]	2003	215
A Security Framework for Personal Networks	Shin; Kobara; Imai	[SKI08]	2008	216
A security framework for service oriented architectures	Candolin	[Can07]	2007	217
A security framework for wireless sensor networks	Zia	[Zia08]	2008	218
A security framework with trust management for sensor networks	Yao; Kim; Lee; Kim; Jang	[YKL+05]	2005	219
An extended security framework for e-government	Al-Ahmad; Al-Kaabi	[AAAK08]	2008	220
An Identity-Based Security Framework For VANETs	Kamat; Baliga; Trappe	[KBT06]	2006	221
An Integrated Security Framework for Assisting in the Defense of Computer Networks	Onwubiko; Lenaghan; Hebbes	[OLH06]	2006	222

Titel	Autor(en)	Referenz	Jahr	Seite
A Study on Security Framework for Ambient Intelligence Environment	Ko; Ramos	[KR09]	2009	223
Attack analysis & bio-inspired security framework for IP multimedia subsystem	Awais; Farooq; Javed	[AFJ08]	2008	224
Building a Practical Framework for Enterprise-Wide Security Management	Allen	[All04]	2004	225
Context-Sensitive Security Framework for Pervasive Environments	Pigeot; Gripay; Scuturici; Pierson	[PGSP07]	2007	225
Distributed Intrusion Detection and Attack Containment for Organizational Cyber Security	Batsell; Rao; Shankar	[BRS06]	2006	227
Ein Framework für föderiertes Sicherheitsmanagement	Reiser	[Rei08]	2008	149
Grid Security Framework for Managing the Certificate	Thein; Naing	[TN06]	2006	228
Implementation of a Security Framework for Wireless Multi-hop Networks	Paris; Capone	[PC09]	2009	229
Interoperable Internet-Scale Security Framework for RFID Networks	Mao	[Mao09]	2009	230
Network Security Framework	Gupta; Ramamohanarao	[GR06]	2006	231
Phyllo: a peer-to-peer overlay security framework	Heinbockel; Kwon	[HK05]	2005	232
Secure SocialAware: A Security Framework for Mobile Social Networking Applications	Beach; Gartrell; Ray; Han	[BGRH09]	2009	233
Security Framework for Home Network: Authentication, Authorization, and Security Policy	Kim; Lee; Han; Kim; Kim	[KLH+07]	2007	234
Security framework for integrated networks	Alkassar; Stüble	[AS03]	2003	235
Security Frameworks for Virtual Organizations	Magiera; Pawlak	[MP05]	2005	236
Semantic policy-based security framework for business processes	Huang	[Hua05]	2005	236
Sicherheit in Mobilen Ad hoc Netzwerken	Kargl	[Kar03]	2003	238
Toward a Usage-Based Security Framework for Collaborative Computing Systems	Zhang; Nakae; Covington; Sandhu	[ZCS08]	2008	239
Towards a flexible security framework for peer-to-peer based grid computing	Detsch; Gaspary; Barcellos; Cavalheiro	[DGBC04]	2004	240

Titel	Autor(en)	Referenz	Jahr	Seite
Unified security framework	Wilson; Tharakan	[WT03]	2003	241

Nach dem folgenden Überblick über die den Security-Frameworks zugrunde liegenden Designkonzepte werden in Abschnitt 4.3 zwei Arbeiten im Detail analysiert und die Ergebnisse der Analysen der anderen Security-Frameworks in Abschnitt 4.4 vorgestellt.

4.2. Überblick über Designkonzepte für Security-Frameworks

Für viele Bereiche der IT-Sicherheit existieren inzwischen Vorgaben und Leitfäden, die festlegen, wie Konzepte strukturiert erarbeitet und dokumentiert werden sollen und worauf bei der praktischen Umsetzung zu achten ist. Beispielsweise sind für die Entwicklung neuer kryptographischer Prüfsummen und Verschlüsselungsverfahren diverse Designkriterien sowie kryptoanalytische Methoden und Angriffe auf verschiedene Klassen neu entworfener Algorithmen frei verfügbar (vgl. [ACRYPT]). Neben den Sicherheitsmechanismen selbst wurde beispielsweise auch das benutzerfreundliche Design von Sicherheits-Managementwerkzeugen im Detail untersucht (siehe z. B. [JBHB03]). Für das Design von Security-Frameworks sind hingegen keine vergleichbaren Arbeiten bekannt: Einerseits referenzieren die untersuchten Security-Frameworks keine allgemeinen Designrichtlinien; andererseits konnten im Rahmen der oben erläuterten Literaturrecherche nur einige wenige Arbeiten ermittelt werden, die sich mit ausgewählten Teilaspekten der Security-Framework-Konzeption befassen; auch diese decken jedoch nicht das Design von Security-Frameworks als Ganzes ab.

Obwohl security-framework-übergreifende Gestaltungskonzepte bislang fehlten oder zumindest nicht explizit dokumentiert und allgemein bekannt waren, zeigt die im Rahmen dieser Arbeit durchgeführte Analyse einer größeren Anzahl Security-Frameworks deutliche Parallelen in deren Dokumentationsstruktur. Diese empirisch ermittelte und verallgemeinerte Struktur von Security-Framework-Konzepten wird nachfolgend skizziert. Bei der Interpretation dieses Zwischenergebnisses muss jedoch berücksichtigt werden, dass es sich bei den untersuchten Arbeiten nahezu ausschließlich um wissenschaftliche Literatur handelt, für die eine vergleichbare Struktur allgemein üblich ist. Insbesondere konnten keine Besonderheiten identifiziert werden, die inhärent mit der Thematik verbunden oder besonders charakteristisch für Security-Frameworks sind. Die Kenntnis des üblicherweise vorzufindenden Aufbaus erweist sich jedoch auch als hilfreich bei der Analyse davon abweichender Arbeiten.

Die ermittelte typische Struktur ist in Abbildung 4.2 dargestellt und umfasst die folgenden Blöcke:

- Einleitend werden in der Regel die **Motivation** für die Zusammenstellung des Security-Frameworks erläutert und ein grober Überblick über **Ziele** und mögliche Anwendungsszenarien gegeben.
- In vielen Security-Frameworks werden entweder konkrete **Szenarien**, aus denen Anforderungen an die jeweilige Arbeit abgeleitet wurden, oder fiktive Szenarien und **Beispiele**, die zur Erläuterung der Konzepte dienen sollen, vorgestellt. Die Anzahl diskutierter Szenarien kann dabei als direkt proportional zum Gesamtumfang der jeweiligen Arbeit angesehen werden.

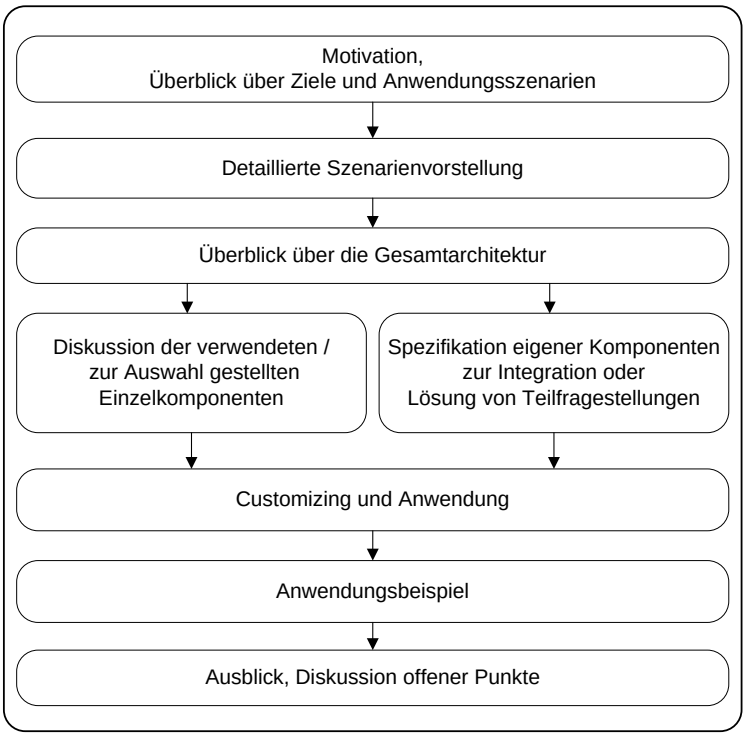


Abbildung 4.2.: Typische Struktur von Security-Framework-Konzepten

Dabei fällt auf, dass insbesondere solche Arbeiten, in denen konkrete Szenarien geschildert werden, häufiger die bei der Konzeption berücksichtigten Anforderungen dokumentieren als andere Arbeiten, die eigene Konzepte anhand kleiner, in sich geschlossener Beispiele erläutern.

- Eine deutliche Mehrheit der Security-Frameworks gibt anschließend einen **Überblick über die Gesamtarchitektur**, um darauffolgend alle oder zumindest die als besonders relevant eingestuften Einzelkomponenten zu erläutern (Top-down-Vorgehensweise). Die alternative Bottom-up-Vorgehensweise, bei der zunächst die **Einzelkomponenten** erläutert und anschließend zu einer Gesamtarchitektur zusammengestellt werden, findet sich überwiegend bei Security-Frameworks für (einzelne) IT-Dienste sowie bei denjenigen Arbeiten, die sich explizit auf ausgewählte Teilaspekte beschränken.
- Für jede Einzelkomponente wird meist mindestens eine **konkrete Lösung** (z. B. ein zu verwendender Sicherheitsmechanismus oder eine einzuführende organisatorische Maßnahme) vorgeschlagen oder es wird die **Auswahl aus mehreren Alternativen** thematisiert, wobei nicht immer klare Selektionskriterien vorgegeben werden, sondern teilweise nur ein neutraler Überblick über verschiedene Varianten gegeben wird.
- Ein signifikanter Teil der Security-Frameworks zeichnet sich dadurch aus, dass zusätzlich zur Zusammenstellung diverser bereits existierender Einzelkomponenten auch **eigene, neue Komponenten** eingeführt werden. Diese dienen entweder der Integration der anderen Komponenten im Sinne von Schnittstellenadaptern bzw. zur Koordination von Arbeitsabläufen und Datenflüssen oder lösen im Themenumfeld des jeweiligen Security-

Frameworks noch nicht bzw. nicht hinlänglich bearbeitete technisch-wissenschaftlichen Teilprobleme.

- Einige – leider bei Weitem nicht alle – Security-Frameworks gehen im Anschluss auf die Anpassung und den Einsatz des Security-Frameworks in eigenen Szenarien ein. Die **Beschreibung dieser Customizingphase** fällt in der Regel sehr knapp aus; in den meisten Fällen wird die notwendige Vorgehensweise nur skizziert, so dass sich der Leser die Details unter Zuhilfenahme des Security-Framework-Konzepts selbst erarbeiten muss. Insbesondere bei denjenigen Security-Frameworks, die bereits bei der Beschreibung der Einzelkomponenten auf mögliche Beurteilungs- und Selektionskriterien eingehen, fällt die Beschreibung der Customizing-Methodik meist relativ knapp aus.
- Einige Security-Frameworks veranschaulichen Customizing und Umsetzung anhand von **Beispielanwendungen**, in denen wiederum Bezug auf die motivierenden Szenarien oder – zur Vereinfachung – ausgewählte Teile davon genommen wird. In anderen Fällen ersetzt die exemplarische Anwendung des Security-Frameworks auch die explizite Dokumentation der Anpassungsmethodik.
- Wie ebenfalls für wissenschaftliche Arbeiten typisch schließen die meisten Security-Framework-Dokumentationen mit einem Überblick über noch offene bzw. nicht ausreichend behandelte Aspekte und einem Ausblick auf Möglichkeiten zur zukünftigen **Weiterentwicklung**. Eine vergleichbare selbstkritische Analyse fehlt den meisten der betrachteten nicht-wissenschaftlichen Arbeiten; anstelle eines Ausblicks auf weitere Forschungstätigkeiten finden sich vereinzelt grobe Pläne und entsprechende Zeitangaben (engl. *roadmap*) für die Weiterentwicklung.

Ohne die in Abschnitt 4.5 diskutierten Verbesserungsmöglichkeiten vorwegzunehmen ist erwähnenswert, dass sich auch in der betrachteten wissenschaftlichen Literatur Verweise auf andere Arbeiten verstärkt nur dort finden, wo Einzelkomponenten vorgeschlagen und miteinander verglichen werden. Hingegen fehlen vielfach eine Diskussion ähnlicher Lösungsansätze und das Aufzeigen von Analogien zu Security-Frameworks für andere Themenbereiche. Hierfür spielen die beiden folgenden Aspekte eine Rolle:

1. An neuen sicherheitsrelevanten Themen – beispielsweise nationale E-Health-Infrastrukturen – wird von mehreren Gruppen zunächst unabhängig voneinander parallel geforscht, so dass die Zwischenergebnisse der jeweils anderen noch nicht verfügbar sind und adäquat berücksichtigt werden können.
2. Bei einem nicht unerheblichen Teil der Arbeiten wird durch eine erkennbare Bottom-up-Vorgehensweise der Eindruck erweckt, die Idee zur Zusammenstellung als Framework sei erst nach der Beschäftigung mit den punktuellen Einzelkomponenten entstanden. In Kombination mit der in Kapitel 2 bereits diskutierten unscharfen Verwendung des Begriffs *Framework* findet im Anschluss jedoch keine intensive Auseinandersetzung mit der in dieser Arbeit postulierten Top-down-Vorgehensweise statt, bei der andere gesamtheitliche Ansätze mit einbezogen werden sollen.

Obwohl es wie oben erläutert bislang keine dokumentierten Richtlinien oder „Best Practices“ zur Erstellung von Security-Frameworks gibt, beschäftigen sich einige Arbeiten mit wichtigen Teilaspekten, die beim Design berücksichtigt werden sollten:

- [LSM+98] thematisiert durch die Forschung an sicheren Betriebssystemen motiviert das grundlegende Designprinzip, dass jegliche Schutzmechanismen auf höheren Schichten

und Abstraktionsebenen ausgehebelt werden können, wenn die Basis nicht ausreichend geschützt wird. Obwohl sich die Arbeit primär mit den Schwerpunkten Access Control und Kryptographie im Umfeld IP-basierter Kommunikation befasst und auf die Härtung von Betriebssystemkernen abzielt, werden die von den Autoren postulierten Designvorgaben bewusst verallgemeinert und auf andere Dienste und Architekturen übertragbar formuliert.

- [Ste06] befasst sich mit ausgewählten Aspekten der Umsetzung rein softwarebasierter Security-Frameworks in größeren Unternehmensumgebungen. In dem kompakten Journalartikel werden typische Schwierigkeiten, die den Frameworkeinsatz motivieren, und organisatorische Vorgehensweisen grob skizziert. Er gibt somit einen grundlegenden Einblick in den praktischen Einsatz und einen knappen Überblick über sicherheitsmanagementrelevante Themen wie Schulungen und IT-Governance, ohne daraus jedoch konkrete Schnittstellenanforderungen für Security-Frameworks abzuleiten.
- [TX07] untersucht am Beispiel von E-Commerce-Architekturen ausgewählte Anforderungen an Security-Frameworks in diesem Bereich. Neben sicherheitsfunktionalen Aspekten, die den Schwerpunkt bilden, werden auch Eigenschaften wie die Hochverfügbarkeit und die Berücksichtigung von Datenschutzaspekten diskutiert, die auch für Security-Frameworks in anderen Gebieten relevant sind.
- Verschiedene Kombinationen von Sicherheitsmechanismen, die sich in der Praxis zur Umsetzung von sicherheitsfunktionalen Anforderungen bewährt haben, wurden von verschiedenen Arbeits- und Standardisierungsgruppen zu so genannten Security Patterns zusammengefasst und dienen somit auch als Ansatzpunkte und Referenzen für die im Rahmen von Security-Frameworks eingesetzten Komponenten. Da ihre Verwendung auch in framework-übergreifenden, beispielsweise unternehmensweiten Sicherheitskonzepten nahe liegt, wird auf sie vertiefend in Abschnitt 5.2 eingegangen.

Insgesamt bleibt damit festzuhalten, dass bislang nur wenige Vorarbeiten zur strukturierten Gestaltung von Security-Frameworks existieren, die sich zudem auf unterschiedliche Teilbereiche fokussieren. Die in dieser Arbeit vorgenommene Anforderungsanalyse und die Aufbereitung z. B. in Form einer Checkliste für Frameworkautoren (siehe Abschnitt 3.9) liefert somit gezielt einen Beitrag zur Unterstützung bei der Konzeption und Dokumentation neuer und verbesserter Security-Frameworks.

4.3. Detaillierte Analyse ausgewählter Security-Frameworks

In diesem Abschnitt werden die Analysen von zwei Security-Frameworks ausführlich dargestellt. Damit soll zum einen die Anwendung des in Kapitel 3 erarbeiteten Kriterienkatalogs demonstriert werden; zum anderen werden sowohl Stärken als auch Ansatzpunkte für die weitere Verbesserung an konkreten Beispielen vorgestellt, die sich in ähnlicher Form auch in vielen der unten knapper behandelten Security-Frameworks finden.

Für diese detaillierten Analysen wurde jeweils ein Security-Framework für IT-Architekturen bzw. für IT-Dienste ausgewählt. Dabei wurden die folgenden grundlegenden Selektionskriterien angewandt:

- Die im Detail vorgestellten Security-Frameworks haben einen konkreten Bezug zu den in dieser Arbeit behandelten Szenarien. So lässt sich das *Framework für föderierte Sicherheit* [Rei08] auf das DEISA-Szenario (siehe Abschnitt 3.4) anwenden und das *Energy Efficient Security Framework for Wireless Local Area Networks* [Kir05] deckt einen der in Szenario 1 (siehe Abschnitt 3.2) vorgestellten Dienste ab.
- Der Umfang und damit möglicherweise auch der Inhalt sollte nicht durch eine Obergrenze für die Seitenzahl – wie in Journalartikeln und Tagungsbeiträgen üblich – beschränkt werden. Mit einer Habilitationsschrift und einer Dissertation wurden zwei Arbeitsformen ausgewählt, die den Autoren ausreichend Freiraum für die Darstellung ihrer Ideen gewähren. Dadurch wurde auch sichergestellt, dass sowohl in sich abgeschlossene Arbeiten vorliegen als auch Vorarbeiten und verwandte Arbeiten adäquat berücksichtigt werden können.

Die nachfolgenden Analysen haben den folgenden Aufbau: Zunächst werden der **Inhalt des Security-Frameworks** knapp zusammengefasst und seine **Schwerpunkte** skizziert. Ergänzend wird die **Struktur der Arbeit** untersucht und den in Abschnitt 4.2 erläuterten Designkonzepten gegenübergestellt. Anschließend werden die in Kapitel 3 erarbeiteten **Beurteilungskriterien** in alphabetischer Reihenfolge nach Kategorien getrennt angewandt und der Erfüllungsgrad der jeweiligen Anforderung begründet festgehalten. Abschließend werden die Beurteilung zusammengefasst und die ermittelten **Stärken und Verbesserungsvorschläge** resümiert.

4.3.1. Analyse des Frameworks für föderiertes Sicherheitsmanagement

In der Habilitationsschrift von Helmut Reiser [Rei08] wird ein Security-Framework für Föderationen, d. h. organisationsübergreifende Verbünde mit dem Teilziel der gemeinsamen Bereitstellung und Nutzung von IT-Ressourcen, erarbeitet. Dabei werden insbesondere virtuelle Organisationen und somit Grids als phänotypische Föderationen behandelt, wodurch sich der unmittelbare Bezug zu Szenario 3 dieser Arbeit ergibt.

Aufgrund eines Mangels an einschlägigen Vorarbeiten zur organisationsübergreifenden Sicherheit erarbeitet Helmut Reiser zunächst auf Basis einer Typisierung von interorganisationalen Kooperationen und Grids eine Liste von Sicherheitsanforderungen, die sowohl organisatorische Aspekte wie die Berechtigungsdelegation als auch technische Herausforderungen wie Single Sign-On, Logging und Sandboxing umfasst. Auf dieser Basis werden acht Sicherheitsdienstklassen spezifiziert und die diesen zuzuordnenden, rund 20 verschiedenen Sicherheitsdienste und deren gegenseitige Abhängigkeiten analysiert. Auf dieser Basis ergibt sich ein Grobkonzept für das von Helmut Reiser konzipierte Security-Framework, das wie in Abbildung 4.3 dargestellt auf die szenarienspezifische Auswahl und Kombination der verfügbaren Sicherheitsdienste hinführt und durch die Wahl geeigneter Sicherheitsmechanismen und deren Einfassung und Parametrisierung in Form von Policies abzielt.

Um die konkrete Beurteilung und Auswahl zu unterstützen, spezifiziert Helmut Reiser ein Klassifikations- und Bewertungsschema für interorganisational einsetzbare Sicherheitsmechanismen. Dabei werden auch Managementaspekte wie Delegationsfähigkeit und Administrierbarkeit umfassend berücksichtigt.

Auf Basis dieser Vorarbeiten werden anschließend existierende Sicherheitskonzepte und -mechanismen bewertet, wobei hierauf – bereits am Umfang klar erkennbar – der Schwer-

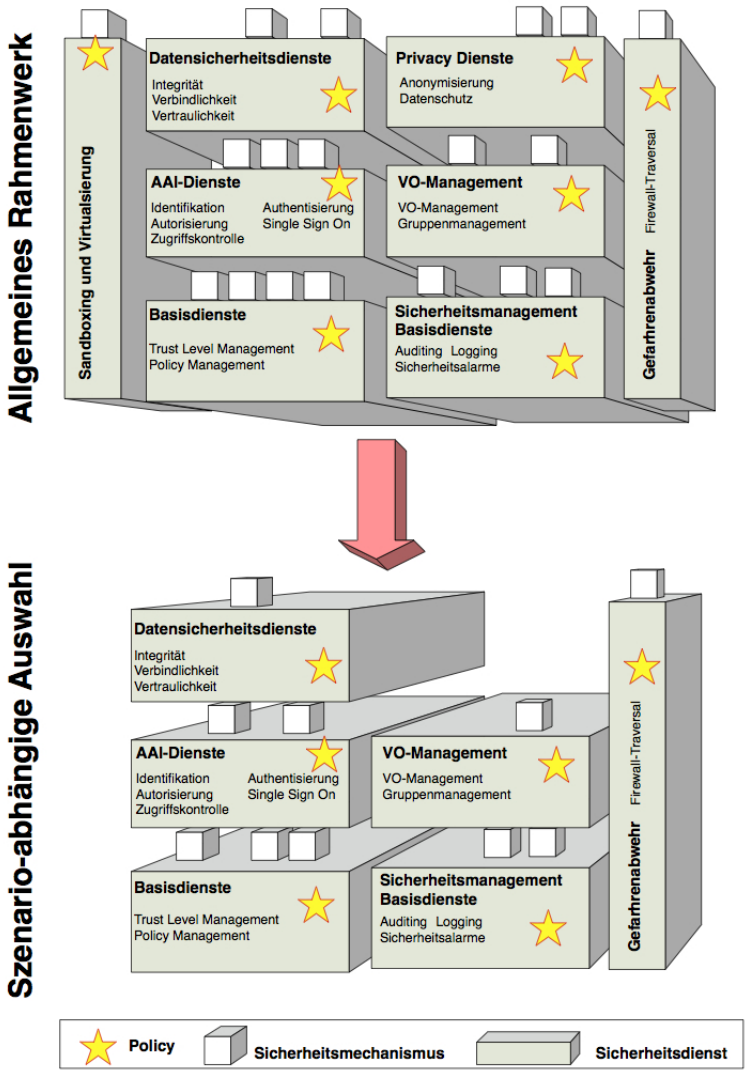


Abbildung 4.3.: Szenarienspezifische Auswahl von Sicherheitsdiensten beim Einsatz des Security-Frameworks von Helmut Reiser (Quelle: [Rei08, S. 29])

punkt der Arbeit liegt, in dem den Anwendern des Security-Frameworks ausführlich die zur Verfügung stehenden Optionen und die Facetten der jeweiligen Teillösungsansätze vermittelt werden. Da sich herausstellt, dass mit den existierenden Sicherheitsmechanismen nicht alle Anforderungen im Umfeld interorganisationaler Sicherheit abgedeckt werden können, erarbeitet Helmut Reiser im Anschluss neue Komponenten für das Trust Level Management und das verteilte, delegationsfähige Gruppen- und Autorisierungsmanagement, die ebenfalls auf Basis der ermittelten Anforderungen analysiert werden. Abschließend wird die Anwendung des gesamten Rahmenwerks vorgestellt, wobei zwischen einer Analyse- und einer Synthesephase unterschieden wird, so dass zunächst die erforderlichen Sicherheitsdienste ausgewählt und der Kriterienkatalog angepasst werden und daraufhin eine konkrete Mechanismenauswahl und -bewertung stattfindet, die im Hinblick auf eine kontinuierliche Verbesserung wiederholt

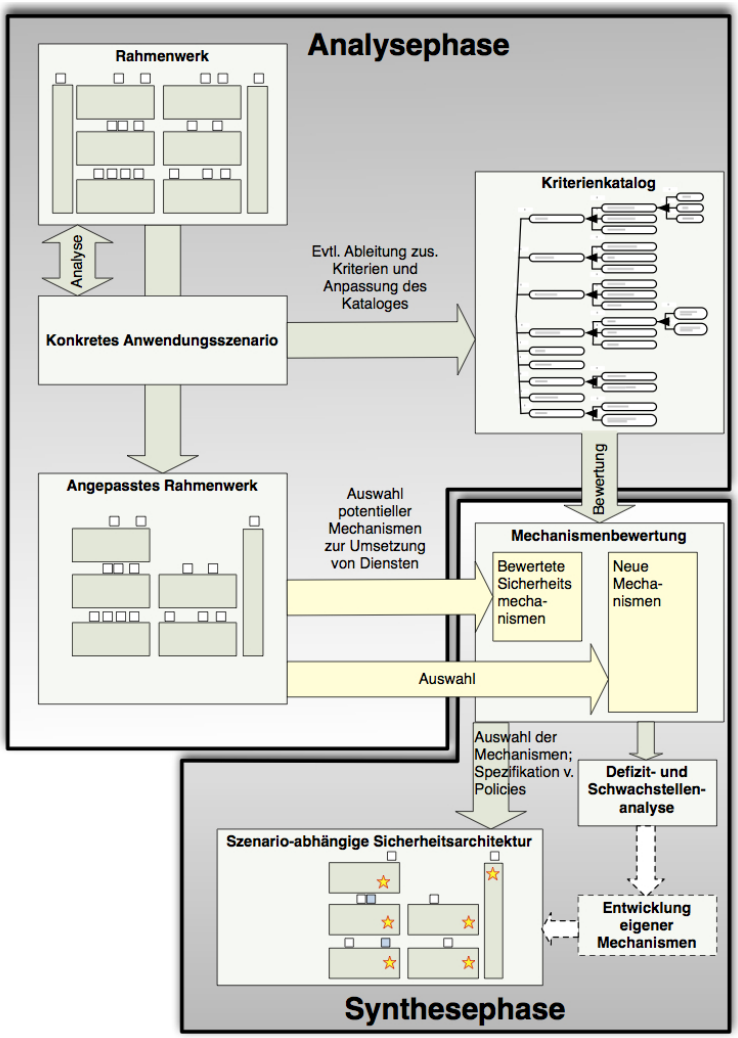


Abbildung 4.4.: Zusammenspiel von Analyse- und Synthesephase beim Einsatz des Security-Frameworks von Helmut Reiser (Quelle: [Rei08, S. 230])

angewendet werden kann. Diese Vorgehensweise ist in Abbildung 4.4 dargestellt.

Das Security-Framework von Helmut Reiser folgt damit im Wesentlichen dem in Abschnitt 4.2 erläuterten Design: Nach einer einleitenden Diskussion der Motivation für die Arbeit werden mit dem Identitätsmanagement bei der BMW Group und der verteilten IT-Ressourcennutzung in Grids zwei Szenarien und daraus resultierende Anforderungen analysiert, an die sich unmittelbar ein Überblick über die Gesamtarchitektur des erarbeiteten Security-Frameworks anschließt. Die darauffolgende Bewertung von Sicherheitsmechanismen fällt überdurchschnittlich breit und tiefgehend aus und stellt somit eines der herausragenden Merkmale dieses Security-Frameworks dar. Analog zum typischen Design von Security-Frameworks wird die Auswahl existierender Sicherheitsmechanismen durch die Spezifikation eigener, zusätzlicher Komponenten ergänzt; auch die Beschreibung der Anpassungsmethodik an eigene Szenarien fällt – vergleichbar mit den meisten der anderen betrachteten Arbei-

ten – bezüglich ihres Umfangs in Relation zu den übrigen Teilen der Arbeit relativ knapp aus. Eine Anwendung auf konkrete Szenarien findet im Rahmen der Habilitationsschrift von Helmut Reiser nicht statt; sie schließt – wie oben diskutiert für wissenschaftliche Arbeiten typisch – mit einem Überblick über offene Fragestellungen und mögliche weitere Arbeiten.

Nachfolgend wird auf Basis des in Abschnitt 3.7.1 beschriebenen Verfahrens der Erfüllungsgrad der in dieser Arbeit ermittelten Anforderungen an Security-Frameworks erläutert. Im Bereich der sicherheitsfunktionalen Anforderungen zeichnet sich folgendes sehr positives Bild ab:

- Die *wichtige* Anforderung **SF-FUNK-Abschottung** wird *vollständig* erfüllt, da die Autarkie der in einer Föderation bzw. an einem Grid beteiligten Organisationen von Anfang an berücksichtigt wird und sich durch das Design des gesamten Frameworks zieht.
- Die *wünschenswerte* Anforderung **SF-FUNK-Adaptivität** wird ebenfalls *vollständig* erfüllt; insbesondere die von Helmut Reiser selbst entwickelte Komponente zur verteilten Gruppenverwaltung und -autorisierung berücksichtigt die Notwendigkeit von dynamischen Anpassungen; darüber hinaus ist die Flexibilität eines der Kriterien, die im Framework zur Beurteilung von Lösungsbausteinen herangezogen wird.
- Die *wichtige* Anforderung **SF-FUNK-Angriffe** wird *zielführend partiell* erfüllt: Aufgrund der Breite der im Framework betrachteten Ressourcen und Komponenten werden einzelne Angriffe zwar nicht im Detail diskutiert; es wird jedoch konsequent auf entsprechende Vorarbeiten verwiesen, so dass sich der Leser eine umfassende Meinung über die Gefahrenlage und die Übertragbarkeit auf eigene Szenarien bilden kann.
- Die *essentielle* Anforderung **SF-FUNK-Assets** wird *vollständig* erfüllt, da sowohl in den im Framework analysierten Szenarien als auch den abstrakten Konzepten auf alle in aktuellen Grid-Projekten anzutreffenden Dienste, Komponenten und Ressourcen ausführlich eingegangen wird.
- Auch die *essentielle* Anforderung **SF-FUNK-Auditing** wird *vollständig* erfüllt, da es sich beim Auditing um einen der im Framework identifizierten Sicherheitsmanagement-Basisdienste handelt und die Einschränkungen, die beim organisationsübergreifenden Austausch entsprechender Informationen zu beachten sind, explizit berücksichtigt werden.
- Die *wichtige* Anforderung **SF-FUNK-Automatisierung** wird *zielführend partiell* erfüllt. Eine vollständige Erfüllung ist an vielen und im Framework mehrfach explizit dokumentierten Stellen insbesondere wegen Einschränkungen der verfügbaren Sicherheitslösungen, die ihrerseits keine Automatisierung bieten, nicht möglich; hieraus ergibt sich ein nachvollziehbar dokumentierter Kompromiss aus der Entwicklung eigener Komponenten und der effizienten Wiederverwendung existierender Lösungsbausteine.
- Die *essentielle* Anforderung **SF-FUNK-Maßnahmen** wird *vollständig erfüllt*, da eine umfassende Analyse und Bewertung in Frage kommender Sicherheitslösungen vorgenommen wird; die breite Auswahl bildet zudem eine solide Basis für die szenarienspezifische Anwendbarkeit des Frameworks.
- Schließlich wird die *wichtige* Anforderung **SF-FUNK-Schwachstellen** *zielführend partiell* erfüllt. Analog zur oben analysierten Behandlung von Angriffen werden die

Schwachstellen zwar nicht im Detail einzeln diskutiert; das Frameworkkonzept verweist jedoch auf entsprechende Vorarbeiten und stellt die Möglichkeit zur Beurteilung durch den Leser und die Übertragbarkeit auf eigene Szenarien sicher.

Auch bezüglich der Integrations- und Betriebsanforderungen schneidet das Security-Framework von Helmut Reiser überdurchschnittlich gut ab:

- Die *wichtige* Anforderung **SF-INT-Ausbauphasen** wird *zielführend partiell* erfüllt, da eine nachträgliche Erweiterung der szenarienspezifischen Frameworkinstanz im Anschluss an den Durchlauf der Synthesephase in der Anpassungsmethodik prinzipiell vorgesehen ist. Das entsprechende Vorgehen sollte jedoch noch weiterführend unterstützt werden, beispielsweise indem die bislang aus Analyse- und Synthesephase bestehende Anpassungsmethodik noch konsequenter als kontinuierlicher Verbesserungsprozess ausgelegt wird.
- Die *essentielle* Anforderung **SF-INT-Customizing** wird *vollständig* erfüllt, da das Framework einen methodisch unterstützten Anpassungsprozess beinhaltet, der alle wesentlichen Schritte umfasst. Allerdings ist anzumerken, dass die Anwendung dieser Anpassungsmethodik durch eine ausführlichere Dokumentation und begleitende Beispiele noch besser unterstützt werden könnte.
- Die *wichtige* Anforderung **SF-INT-Einführung** wird *partiell* erfüllt: Zwar wird auf Besonderheiten bei der Einführung im Kontext der Analyse einiger der verwendeten Komponenten eingegangen; die geforderte, über die Schritte des Adaptionsprozesses hinausgehende methodische Unterstützung der Einführung angepasster Frameworkinstanzen in den jeweiligen Szenarien wird jedoch nicht explizit thematisiert und verbleibt somit Aufgabe des Frameworkanwenders.
- Die *wichtige* Anforderung **SF-INT-Erweiterung** wird *zielführend partiell* erfüllt: Das Framework sieht zwar keine expliziten Schnittstellen oder Sollbruchstellen für Erweiterungen vor, deren Nutzung methodisch unterstützt wird. Die zur Verfügung gestellten Methoden, beispielsweise zur Analyse und Bewertung von technischen Sicherheitsmechanismen, lassen sich jedoch auf weitere bzw. eigene Ergänzungen anwenden; implizit kommt diese Vorgehensweise bei den im Rahmen des Frameworks neu konzipierten Komponenten zum Trust Level Management und zur Gruppenverwaltung zum Einsatz. Zudem werden die untersuchten Sicherheitsmechanismen unter anderem bezüglich ihrer eigenen Erweiterbarkeit bewertet.
- Die *wichtige* Anforderung **SF-INT-Hochverfügbarkeit** wird *partiell* erfüllt: Die Verfügbarkeit der Dienste und Daten wird vom Framework nicht explizit als Sicherheitsanforderung genannt und auch nicht bei der Bewertung potentieller Lösungsbausteine berücksichtigt. Aus dem Frameworkdesign ergeben sich jedoch auch keine Einschränkungen hinsichtlich der Umsetzung von Hochverfügbarkeitsmaßnahmen, die von den einzelnen Sicherheitskomponenten bereits geboten werden.
- Die *wichtige* Anforderung **SF-INT-Kompatibilität** wird *vollständig* erfüllt, da einerseits das Zusammenspiel zwischen den vom Framework vorgesehenen Komponenten und andererseits deren Integration in bestehende Systeme auch explizit als Design- und Bewertungskriterium herangezogen werden.
- Auch die *wichtige* Anforderung **SF-INT-Modularität** wird *vollständig* erfüllt: Die Modularität der Sicherheitsdienstklassen wird explizit hergeleitet, zieht sich durch das

gesamte Frameworkkonzept und fungiert als Basisgranularität für den Customizing-Prozess; auf die Zusammenhänge und Abhängigkeiten wird dabei explizit eingegangen.

- Die *essentielle* Anforderung **SF-INT-Parallelbetrieb** wird *zielführend partiell* unterstützt. Zwar wird die Koexistenz der framework-basierten Sicherheitslösung mit framework-externen Sicherheitsmaßnahmen nicht an allen Stellen explizit thematisiert; aufgrund der berücksichtigten großen Heterogenität der betrachteten Ressourcen und Schutzmechanismen wird die Koexistenz mit weiteren Sicherheitskomponenten jedoch nicht beeinträchtigt.
- Die *wünschenswerte* Anforderung **SF-INT-Polyinstanziierbarkeit** wird *zielführend partiell* unterstützt: Auf die Instanziierung des Frameworks an mehr als einem Standort wird in der Form eingegangen, dass der Anpassungsprozess gleichermaßen auf einzelne Domänen oder ganze Föderationen angewandt werden kann; eine explizite Differenzierung auf Basis standortspezifischer Anforderungen erfolgt dabei jedoch nicht. Wie bereits oben beim Kriterium SF-INT-Customizing angemerkt würde der Frameworkanwender von einer ausführlicheren Dokumentation des Anpassungs- und Instanziierungsprozesses profitieren.
- Die *essentielle* Anforderung **SF-INT-Skalierbarkeit** wird *vollständig* erfüllt. Auch hierbei handelt es sich um ein Kriterium, das sich durch das gesamte Framework zieht und zur Beurteilung der an der Lösung beteiligten Komponenten konsequent eingesetzt wird.
- Die *wichtige* Anforderung **SF-INT-Usability** wird ebenfalls *vollständig* erfüllt. Sie findet sich im Kontext des Security-Frameworks unter dem Begriff *Administrierbarkeit* und wird ebenfalls durchgängig als Beurteilungskriterium für analysierte Sicherheitsmechanismen angewandt.
- Schließlich wird die *wichtige* Anforderung **SF-INT-Wiederverwendbarkeit** auch *vollständig* erfüllt, da sich die Nutzung bereits vorhandener Dienstkomponenten explizit positiv auf die Bewertung der analysierten Sicherheitskomponenten auswirkt.

Im Bereich der Anforderungen an die Schnittstellen für Managementoperationen und -prozesse zeigt sich deutlich, dass zwar einerseits die explizit berücksichtigten Themen gut umgesetzt wurden, dass aber andererseits einige Aspekte nicht in das Design eingeflossen sind:

- Die *wichtige* Anforderung **SF-MGMT-Administrationskonzept** wird *vollständig* erfüllt, da die Administrierbarkeit der Lösung durchgängig berücksichtigt wird und dabei stets aktuelle Konzepte und Technologien zum Einsatz kommen.
- Die *wichtige* Anforderung **SF-MGMT-Berichtsdetails** wird *nicht* erfüllt, da auf Security-Reports nicht eingegangen und somit auch die Zielgruppenorientierung nicht erörtert wird.
- Die *essentielle* Anforderung **SF-MGMT-Compliance** wird *zielführend partiell* erfüllt. Dabei liegt der Schwerpunkt auf dem Schutz personenbezogener Daten, so dass die Breite relevanter gesetzlicher und anderer externer Auflagen je nach für den Frameworkanwender relevantem Szenario nicht vollständig diskutiert wird.
- Die *wichtige* Anforderung **SF-MGMT-Delegation** wird *vollständig* erfüllt, da es sich wiederum um ein durchgängig zur Beurteilung eingesetzter Komponenten verwendetes Kriterium handelt.

- Die *wünschenswerte* Anforderung **SF-MGMT-Events** wird *partiell* erfüllt: Zwar wird für die untersuchten Sicherheitsmechanismen eruiert, ob diese möglichst flexibel konfigurierbare Sicherheitsmeldungen generieren und ggf. von einer zentralen Stelle aggregieren lassen können; das Framework liefert jedoch kein komponentenübergreifendes Konzept oder Werkzeug zur gezielten Auswertung und Interpretation dieser Meldungen.
- Die *essentielle* Anforderung **SF-MGMT-ITSM-Schnittstellen** wird *nicht* erfüllt. Die Notwendigkeit entsprechender Betrachtungen wird jedoch als offener Punkt bzw. Ausblick auf weitere Forschungsarbeiten im Schlusskapitel des Frameworks dokumentiert.
- Die *wichtige* Anforderung **SF-MGMT-Kosten** wird *partiell* erfüllt. Die kosteneffiziente Umsetzung föderationsweiter Sicherheitskonzepte wird zwar als Motivation für das Framework angeführt und an mehreren Stellen erneut aufgegriffen; eine konkrete Auseinandersetzung mit Aufwendungen und Kosten, die je nach szenarienspezifischer Adaption des Frameworks anfallen, findet jedoch nicht statt. Allerdings wird bei ausgewählten technischen Komponenten auf den potentiell mit ihnen verbundenen erhöhten Betriebsaufwand hingewiesen.
- Die *wünschenswerte* Anforderung **SF-MGMT-KPIs** wird nur *partiell* erfüllt, da zwar eine Aussage mittels einer zentralen, als *quality of protection* bezeichneten Kennzahl gefordert wird, die jedoch von keiner im Framework untersuchten Komponente in der von diesem geforderten Qualität geliefert werden kann; vielmehr wird fast allen untersuchten Komponenten ein völliger Mangel attestiert. Darüber hinaus definiert das Framework auch keine eigenen KPIs.
- Die *wichtige* Anforderung **SF-MGMT-Mandantenfähigkeit** wird im Unterschied zur oben diskutierten Delegationsfähigkeit *nicht* erfüllt. Somit ist davon auszugehen, dass die sicherheitsspezifischen Kundenanforderungen innerhalb einer Föderation als homogen anzusehen sind; auch eine parallele Nutzung derselben Frameworkinstanz für die Teilnahme an mehreren Föderationen wird nicht thematisiert.
- Die *essentielle* Anforderung **SF-MGMT-Metriken** wird *partiell* erfüllt. Mit Ausnahme der oben im Kontext von KPIs diskutierten, lediglich postulierten *quality of protection* wird auf die Messung bzw. Quantifizierung der erreichbaren oder erreichten Sicherheit nur durch das Bewertungsverfahren für Sicherheitsmechanismen eingegangen; dieses dient jedoch der initialen Auswahl im Rahmen des Frameworks einzusetzender Komponenten und nicht zur Beurteilung der laufenden Frameworkinstanz bzw. als Basis für die kontinuierliche Überwachung des Sicherheitsniveaus und Sicherheitsberichte.
- Die *essentielle* Anforderung **SF-MGMT-Operationen** wird *zielführend partiell* erfüllt. Auf die zur Beurteilung wichtigen Managementoperationen wird im Framework bei der Diskussion der einzelnen Sicherheitsmechanismen eingegangen, wobei durchaus auch die zentralen Querbeziehungen thematisiert werden. Ein Gesamtmanagementkonzept für das resultierende Framework, in dem auf die Managementoperationen aus einer Top-down-Perspektive eingegangen wird, liegt hingegen nicht vor.
- Die *wichtige* Anforderung **SF-MGMT-Performanz** wird *partiell* erfüllt. Während die Skalierbarkeit wie oben erläutert durchgängig berücksichtigt wird, findet eine Auseinandersetzung mit der Performanz nur an einigen Stellen, u. a. bei der neu entwickelten Komponente für das Gruppenmanagement, statt.
- Die *wichtige* Anforderung **SF-MGMT-Policies** wird *zielführend partiell* erfüllt. Im

gesamten Framework spielen Policies, die zur Parametrisierung jedes der modularen Sicherheitsdienste dienen, eine zentrale Rolle; ein wesentlicher Aspekt ist dabei auch das Policy-Mapping zwischen den an der Föderation beteiligten Organisationen. Im Vordergrund stehen dabei jedoch einerseits die klar auf organisatorischer Ebene angesiedelten Certificate Authority Policies und die Acceptable Use Policies (Benutzerrichtlinien) und andererseits techniknahe Policies, die als maschinenlesbare Regelwerke zur Konfiguration der eingesetzten Sicherheitsmechanismen fungieren. Somit werden zwar die für die technischen Lösungen relevanten Bereiche gut abgedeckt, die im Rahmen von SF-MGMT-Policies geforderte Einbettung in eine Gesamtsicherheitsrichtlinie, die beispielsweise die von ISO/IEC 27000 vorgegebenen Aspekte abdeckt, sollte jedoch noch ausgebaut werden.

- Die *wichtige* Anforderung **SF-MGMT-Praxis** wird *partiell* erfüllt. So kommen zwar durchaus praxisbewährte Sicherheitsmechanismen zum Einsatz, es liegen jedoch bislang noch keine Berichte über praktische Erfahrungen zum Einsatz des Frameworks als Ganzes vor, die wiederum in seine Weiterentwicklung eingeflossen sind.
- Die *essentielle* Anforderung **SF-MGMT-Prozesse** wird *partiell* erfüllt, da im Kontext der Nutzung einiger der eingesetzten Sicherheitsmechanismen auch auf die damit verbundenen organisatorischen Prozessschritte eingegangen wird. Da das Frameworkkonzept jedoch größtenteils anhand der involvierten Sicherheitsmechanismen strukturiert ist, fehlt eine übergeordnete gesamtheitliche Betrachtung der zu seinem Management erforderlichen Abläufe.
- Die *wichtige* Anforderung **SF-MGMT-Quantifizierung** wird *zielführend partiell* erfüllt. Über das im Framework vorgegebene Bewertungsschema können die effektiv einzusetzenden Sicherheitsmechanismen identifiziert werden und somit z. B. die Maßnahmenpriorisierung wie gewünscht unterstützen. Wie oben im Bereich von Metriken bereits diskutiert beschränkt sich die Anwendbarkeit dieser Methodik jedoch auf die konzeptionelle Auswahl und bietet für den nachfolgenden praktischen Betrieb keine direkte Unterstützung. Ferner wären Vorgaben dazu, wie die Relevanz der einzelnen Sicherheitsdienstklassen in einem konkreten Szenario zu beurteilen ist, zur weiteren Konkretisierung des Customizing-Prozesses hilfreich.
- Die *wichtige* Anforderung **SF-MGMT-Releasezyklus** wird *nicht* erfüllt. Die methodische Unterstützung der Frameworkanwendung endet mit dem Abschluss des Customizing-Prozesses; die zur initialen Inbetriebnahme und für Aktualisierungen relevanten Rollout- und Rollback-Konzepte werden entsprechend nicht behandelt.
- Die *wichtige* Anforderung **SF-MGMT-Schulungen** wird *nicht* erfüllt, da entsprechende Aus- und Weiterbildungsmaßnahmen z. B. für Sicherheitsverantwortliche, Administratoren oder Benutzer im Frameworkkonzept nicht behandelt werden.
- Die *wünschenswerte* Anforderung **SF-MGMT-Support** wird *vollständig* erfüllt, da sich Frameworkanwender mit ihren Fragen an den „Hersteller“ bzw. die dahinterstehende Forschergruppe wenden können.
- Die *wünschenswerte* Anforderung **SF-MGMT-Tests** wird *nicht* erfüllt, da keine Schnittstellen, Methoden oder Ansatzpunkte für eine initiale bzw. kontinuierliche Funktionsüberprüfung spezifiziert werden. Der Frameworkanwender ist somit darauf angewiesen, die ggf. von den einzelnen ausgewählten Sicherheitsmechanismen mitgelieferten

Testverfahren zu verwenden oder dafür eigene Vorgehensweisen zu entwickeln.

- Die *essentielle* Anforderung **SF-MGMT-Verbesserung** wird *partiell* erfüllt. Zwar findet im wissenschaftlichen Umfeld des Frameworkautors eine durch Publikationen belegte aktive Weiterentwicklung und Ergänzung der behandelnden Themen statt. Bislang sind aber noch keine neuen Versionen des Frameworks erschienen, die beispielsweise auf die sich kontinuierlich weiterentwickelnde Technik eingehen.
- Schließlich wird die *wünschenswerte* Anforderung **SF-MGMT-Zuständigkeiten** *zielführend partiell* erfüllt. Im Frameworkkonzept wird grundlegend zwischen Rollen wie den Administratoren und dem Sicherheitsverantwortlichen unterschieden. Eine weitere Verbesserung könnte jedoch durch eine feinere Untergliederung erreicht werden.

Bezüglich der Anforderungen an die Dokumentation von Security-Frameworks ergeben sich folgende Bewertungen:

- Die *wichtige* Anforderung **SF-DOKU-Anforderungsanalyse** wird *vollständig* erfüllt, da die zur Ermittlung der Anforderungen analysierten Szenarien und auch die wissenschaftlichen Hintergründe wie die OSI-Sicherheitsarchitektur klar erläutert werden.
- Die *wichtige* Anforderung **SF-DOKU-Angreifermodelle** wird *zielführend partiell* erfüllt, da bei vielen der untersuchten Sicherheitsmechanismen skizziert wird, wie ein Angreifer vorgehen könnte. Wünschenswert bleibt jedoch eine von den einzelnen Lösungsbausteinen losgelöste, umfassende Diskussion der im vom Framework abgedeckten Bereich zu betrachtenden Angreifer und ihrer Eigenschaften.
- Die *wichtige* Anforderung **SF-DOKU-Ausrichtung** wird *zielführend partiell* erfüllt. Die Schwerpunkte des Frameworks insbesondere auf der Prävention von Angriffen und auch auf deren Erkennung – aber nicht auf der automatischen Reaktion – sind zwar anhand der vorgeschlagenen Sicherheitsmechanismen (z. B. Sandboxing bzw. Sicherheitsalarme) deutlich erkennbar, werden aber nicht durchgängig explizit diskutiert oder begründet.
- Die *wünschenswerte* Anforderung **SF-DOKU-Beurteilung** wird *nicht* erfüllt, da die Frameworkdokumentation nicht darauf eingeht, wie das Ergebnis des Anpassungsprozesses und die praktische Umsetzung der Frameworkinstanz beurteilt werden können.
- Die *wünschenswerte* Anforderung **SF-DOKU-Checkliste** wird *nicht* erfüllt, da in der Frameworkdokumentation keine entsprechende Aufbereitung der Zwischenschritte für die praktische Umsetzung enthalten ist.
- Die *wichtige* Anforderung **SF-DOKU-Designentscheidungen** wird *vollständig* erfüllt, indem der modulare Aufbau des Frameworkkonzepts analog zur Anforderungsanalyse hergeleitet und dokumentiert wird; zudem werden die Vor- und Nachteile der zur Auswahl gestellten Sicherheitsmechanismen umfassend analysiert und dargestellt.
- Die *wünschenswerte* Anforderung **SF-DOKU-Kontinuum** wird *partiell* erfüllt. Zwar wird zum Abschluss der Beschreibung des Customizing-Prozesses auf die Möglichkeit zur kontinuierlichen Verbesserung hingewiesen. Eine deutliche Verbesserung würde sich aber ergeben, wenn einerseits an dieser Stelle konkreter angegeben wäre, wozu die kontinuierliche Verbesserung dient und wie sie erreicht werden kann, und wenn sich andererseits der Ansatz dazu konsequent durch das gesamte Frameworkkonzept zöge.

- Die *wünschenswerte* Anforderung **SF-DOKU-Lifecyclephasen** wird *vollständig* erfüllt, da die beiden im Framework als *Analyse* und *Synthese* bezeichneten Phasen explizit benannt werden.
- Die *wichtige* Anforderung **SF-DOKU-Vollständigkeit** wird *vollständig* erfüllt, indem das Zustandekommen z. B. der betrachteten Anforderungen und Sicherheitsmechanismen erläutert und realen Szenarien gegenübergestellt wird; ferner wird erläutert, wie weitere szenarienspezifische Aspekte oder erst im Entstehen befindliche Lösungsansätze integriert werden können.
- Die *essentielle* Anforderung **SF-DOKU-Voraussetzungen** wird *vollständig* erfüllt, da die für reibungslose Integration und effizienten Betrieb erforderlichen Voraussetzungen bei der Bewertung jedes der vorgeschlagenen Sicherheitsmechanismen dokumentiert wurden.
- Die *wünschenswerte* Anforderung **SF-DOKU-Zertifizierung** wird *nicht* erfüllt; sofern eine Zertifizierung über die vom Framework abgedeckten Komponenten durchgeführt werden soll, muss der Frameworkanwender die erforderlichen Vorbereitungen von Grund auf selbst treffen.
- Die *essentielle* Anforderung **SF-DOKU-Ziele** wird *vollständig* erfüllt: Sowohl das Gesamtziel des Frameworks als auch seine Teilfragestellungen und das angewandte Vorgehensmodell werden bereits in der Einleitung der Frameworkdokumentation vorgestellt und konsequent umgesetzt.
- Schließlich wird auch die *wünschenswerte* Anforderung **SF-DOKU-Zielgruppe** *vollständig* erfüllt, da im Kontext der oben erwähnten Zieldeklaration auch die Zielgruppe des Frameworkkonzepts – Sicherheitsverantwortliche und Administratoren mit sicherheitsspezifischen Aufgaben – explizit spezifiziert wird.

Der Erfüllungsgrad der Anforderungen und die daraus resultierenden Bewertungszahlen auf Basis der in Abschnitt 3.7.1 vorgestellten Nutzwertanalyse sind in Abbildung 4.5 zusammengefasst.

Hierbei zeigt sich erneut deutlich, dass das Security-Framework von Helmut Reiser seine Stärken insbesondere im sicherheitsfunktionalen Bereich sowie im Hinblick auf die Integrations- und Betriebsanforderungen ausspielt. Wünschenswert ist mit Bezug auf die Frameworkdokumentation eine noch stärkere Ausrichtung auf den praktischen Einsatz, da einige hierfür relevante Anforderungen (wie SF-DOKU-Beurteilung und SF-DOKU-Checkliste) nicht erfüllt werden. Weiteres Verbesserungspotential ergibt sich – trotz des ebenfalls deutlich überdurchschnittlichen Abschneidens – im Bereich der Managementschnittstellen: Einerseits fehlen dem Frameworkkonzept Betrachtungen zu wichtigen Bereichen wie Sicherheitsberichten und ITSM-Schnittstellen. Andererseits werden zwar die meisten der aus Sicht dieser Arbeit relevanten Themen aufgegriffen, aufgrund der auch aus der thematischen Komplexität resultierenden Breite jedoch nicht im Detail behandelt; somit ist davon auszugehen, dass für die praktische Umsetzung und den nachhaltigen Betrieb in konkreten Szenarien noch ein erheblicher Eigenaufwand seitens der Frameworkanwender erforderlich ist. Diese Annahme deckt sich mit der bereits diskutierten Problematik, dass vom gesamten Security-Framework-Lebenszyklus mit der Analyse und der Synthese nur die beiden chronologisch ersten Phasen betrachtet werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**2**	4
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		57

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**3**	6
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**2**	8
SF-MGMT-Delegation	2	**3**	6
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**1**	2
SF-MGMT-KPIs	1	**1**	1
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**1**	4
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**1**	2
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**2**	4
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**3**	3
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**1**	4
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		61

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**2**	4
SF-INT-Customizing	4	**3**	12
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**1**	2
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**2**	2
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**3**	6
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		70

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**2**	4
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**1**	1
SF-DOKU-Lifecyclephasen	1	**3**	3
SF-DOKU-Vollständigkeit	2	**3**	6
SF-DOKU-Voraussetzungen	4	**3**	12
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**3**	3
Summe SF-DOKU	24		57

Bewertungszahlen:		SF-FUNK:	2,71
		SF-INT:	2,41
		SF-MGMT:	1,20
Gesamt:	**2,17**	SF-DOKU:	2,38

Abbildung 4.5.: Nutzwertanalyse des Frameworks für föderiertes Sicherheitsmanagement

4.3.2. Analyse des Energy Efficient Security Framework for Wireless Local Area Networks

Die an der University of Pittsburgh entstandene Dissertation von Phongsak Kiratiwintakorn (siehe [Kir05]) erarbeitet ein Security-Framework für IEEE 802.11-basierte Funknetze (vgl. Szenario 1 in Abschnitt 3.2) und zielt dabei auch auf Energieeinsparungen durch die adaptive Wahl u. a. der eingesetzten Verschlüsselungsalgorithmen ab. Für die Verlängerung der Laufzeit batterie- bzw. akkubetriebener Endgeräte und Access Points (z. B. mobile 802.11 Access Points mit GSM- bzw. UMTS-Uplink) wird dabei bewusst in Kauf genommen, dass je nach Nutzungsverhalten auch andere als ständig nur die stärksten kryptographischen Verfahren zum Einsatz kommen: Einerseits können beispielsweise Online-Zeitungslesen, E-Mail-Zugriff und Homebanking einen jeweils unterschiedlichen Schutzbedarf aufweisen; andererseits ist u. a. Homebanking anbieterseitig in der Regel zwingend mit einer starken Verschlüsselung auf Anwendungsebene verbunden, so dass eine zusätzliche Verschlüsselung der Datenpakete innerhalb des lokalen WLANs zu keiner signifikanten weiteren Steigerung des Gesamtsicherheitsniveaus führen würde.

Im Konzept des Security-Frameworks werden nach einer einleitenden Motivation und Beschreibung der Zielsetzung zunächst die Sicherheitsanforderungen und typischen Angriffe in drahtlosen Netzen sowie Protokollstandards und häufig eingesetzte kryptographische Algorithmen analysiert. Anders als bei der in Abschnitt 4.2 diskutierten typischen Struktur von

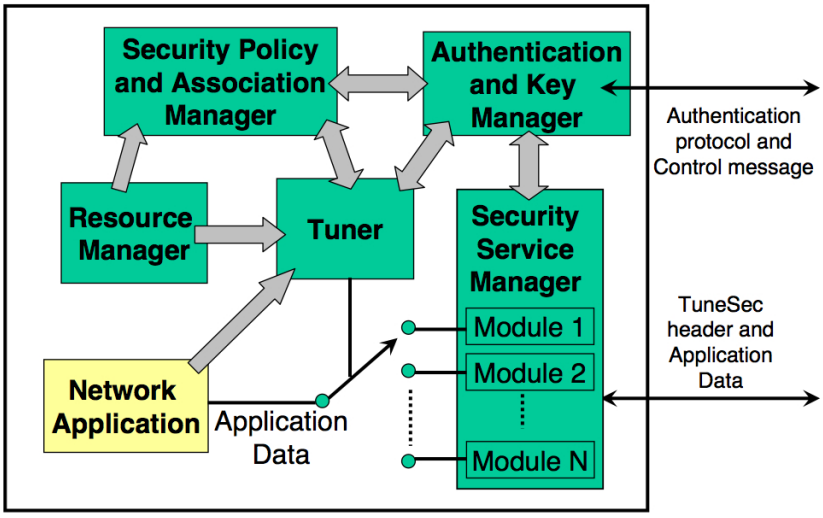


Abbildung 4.6.: TuneSec-Architektur des Energy Efficient Security Framework for Wireless Local Area Networks ([Kir05, S. 109])

Frameworkkonzepten wird dabei weder auf konkrete noch abstrakte Anwendungsszenarien eingegangen. Die einzelnen kryptographischen Operationen und ihre typische Verwendung im Rahmen der in WLANs zum Nachrichtenaustausch eingesetzten Protokolle werden anschließend sowohl auf Basis eines Modells als auch mit entsprechenden Messgeräten in einer Laborumgebung auf ihren Energieverbrauch hin analysiert; dieser erste von zwei wissenschaftlichen Schwerpunkten der Arbeit liefert dem Anwender des Security-Frameworks Hintergrundinformationen, die später für die konkrete Parametrisierung des instanziierten Frameworks benötigt werden.

Der zweite Schwerpunkt der betrachteten Arbeit geht nachfolgend auf das methodische Frameworkdesign und die resultierende, *TuneSec* genannte Architektur ein, die in Abbildung 4.6 dargestellt ist. Sie ist explizit auf Adaptivität sowie modular ausgelegt und verfolgt das Ziel, für den jeweils benötigten Schutz und den angestrebten Energieverbrauch die möglichst optimale Wahl bezüglich Protokollen, Algorithmen und zu deren Umsetzung erforderlichen kryptographischen Operationen zu treffen. Zu diesem Zweck lässt sich *TuneSec* über Policies und weitere Parameter zur Laufzeit konfigurieren.

Die Beschreibung der Architektur und ihrer Komponenten sowie der zur Anpassung notwendigen Schritte folgt somit wiederum dem typischen Aufbau von Frameworkkonzepten. Ferner decken sich damit die anschließende praktische Evaluation des Security-Frameworks in verschiedenen WLANs (Wohnräume, Bibliothek und Fakultätsgebäude eines Universitätscampus) und die Zusammenfassung des Konzepts mit einem Ausblick auf noch offene und weitere Fragestellungen.

Im Folgenden wird wiederum auf Basis des in Abschnitt 3.7.1 erläuterten Verfahrens der Erfüllungsgrad der in dieser Arbeit ermittelten Anforderungen bewertet. Beginnend mit den sicherheitsfunktionalen Anforderungen zeichnet sich ein insgesamt sehr positives Bild ab:

- Die *wichtige* Anforderung **SF-FUNK-Abschottung** wird *vollständig* erfüllt, da die

Autarkie der durch das Security-Framework geschützten WLANs ein explizites Ziel ist, das sich durch die gesamte Arbeit zieht.

- Die *wünschenswerte* Anforderung **SF-FUNK-Adaptivität** wird ebenfalls *vollständig* erfüllt: Die *TuneSec*-Architektur ist explizit auf die geforderten Anpassungen zur Laufzeit ausgelegt.
- Die *wichtige* Anforderung **SF-FUNK-Angriffe** wird *vollständig* erfüllt: Die in der Praxis erwarteten und beim Frameworkdesign berücksichtigten Angriffe werden in einem eigenen Kapitel des Frameworkkonzepts analysiert.
- Die *essentielle* Anforderung **SF-FUNK-Assets** wird *vollständig* erfüllt, da sich das Security-Framework explizit auf verschiedene WLAN-Geräte mit begrenzter Energiekapazität bezieht.
- Die *essentielle* Anforderung **SF-FUNK-Auditing** wird hingegen *nicht* erfüllt, da sich das Framework wie auch unten erläutert nur auf präventive Maßnahmen konzentriert und die Erkennung bzw. Nachverfolgbarkeit sicherheitsrelevanter Vorfälle nicht thematisiert.
- Die *wichtige* Anforderung **SF-FUNK-Automatisierung** wird *zielführend partiell* erfüllt. Zwar unterstützt die *TuneSec*-Architektur die durchgängige Umkonfiguration der eingesetzten Sicherheitsmechanismen in Abhängigkeit vom aktuellen Schutzbedarf; dieses Umschalten muss aber von einem Benutzer oder Administrator explizit manuell angestoßen werden, da in der vorliegenden Frameworkversion noch keine automatische Beurteilung des Schutzbedarfs vorgesehen ist.
- Die *essentielle* Anforderung **SF-FUNK-Maßnahmen** wird *vollständig* erfüllt, da die Wirksamkeit aller vom Security-Framework vorgesehenen Maßnahmen in Relation zum jeweils angestrebten Schutzniveau explizit analysiert wird.
- Schließlich wird die *wichtige* Anforderung **SF-FUNK-Schwachstellen** *vollständig* erfüllt, weil die relevanten Schwachstellen analog zu den möglichen Angriffen explizit analysiert und im Kontext der vorgeschlagenen Lösungsbausteine erneut aufgegriffen werden.

Auch bezüglich der Integrations- und Betriebsanforderungen schneidet das betrachtete WLAN Security-Framework überdurchschnittlich gut ab:

- Die *wichtige* Anforderung **SF-INT-Ausbauphasen** wird *vollständig* erfüllt, da ein dreistufiges Vorgehen vorgeschlagen wird, bei dem sich die Gesamtkomplexität der Umsetzung mit jeder Stufe steigert; einschränkend ist jedoch anzumerken, dass weite Teile des Frameworkkonzepts von einer vollständigen Umsetzung aller Konzeptbestandteile ausgehen.
- Die *essentielle* Anforderung **SF-INT-Customizing** wird *zielführend partiell* erfüllt: Zwar besteht bei der Anpassung beispielsweise bezüglich der eingesetzten Mechanismen und Algorithmen freie Auswahl, aber ein Großteil der *TuneSec*-Architektur wird zwingend vorausgesetzt und bietet praktisch keinen Anpassungsspielraum.
- Die *wichtige* Anforderung **SF-INT-Einführung** wird *zielführend partiell* erfüllt, weil für die Einführung zwar keine explizite methodische Unterstützung, aber eine Ablaufbeschreibung mit Beispielen gegeben wird.

- Die *wichtige* Anforderung **SF-INT-Erweiterung** wird *vollständig* erfüllt: Sowohl die zum Einsatz kommenden Algorithmen als auch die für die *TuneSec*-Komponente *Security Service Manager* eingesetzten Module können nach Bausteinprinzip flexibel ergänzt werden.
- Die *wichtige* Anforderung **SF-INT-Hochverfügbarkeit** wird *zielführend partiell* erfüllt: Die Verfügbarkeit der eingesetzten Komponenten wird überwacht und durch das Framework entstehen keine Einschränkungen z. B. bezüglich bereits vorhandener Redundanzkonzepte. Es sich jedoch keine expliziten Hochverfügbarkeitskonzepte vorgesehen.
- Die *wichtige* Anforderung **SF-INT-Kompatibilität** wird *zielführend partiell* erfüllt, da die Nutzung der bereits vorhandenen Infrastruktur vom Frameworkkonzept zwar gewünscht wird, an einigen Stellen zur Energieeinsparung jedoch bewusst Abweichungen z. B. von Standardprotokollen vorgesehen sind.
- Die *wichtige* Anforderung **SF-INT-Modularität** wird *vollständig* erfüllt: Die vom Security-Framework vorgeschlagene Architektur und die zur Parametrisierung angebotenen Sicherheitsmechanismen sind modular aufgebaut; wie im Kontext von SF-INT-Customizing bereits diskutiert ergibt sich jedoch die Einschränkung, dass ein Großteil dieser Bausteine für den praktischen Einsatz auch zwingend verwendet werden muss.
- Die *essentielle* Anforderung **SF-INT-Parallelbetrieb** wird *nicht* unterstützt: Einerseits wird die potentielle (partielle) Abdeckung der betrachteten Assets durch andere Sicherheitskonzepte nicht berücksichtigt; andererseits ergibt sich durch die im Kontext von SF-INT-Kompatibilität bereits erwähnte partielle Abweichung von Standards zwingend die Situation, dass der geforderte Parallelbetrieb mit anderen Sicherheitsmaßnahmen nicht mehr möglich ist.
- Die *wünschenswerte* Anforderung **SF-INT-Polyinstanziierbarkeit** wird *vollständig* unterstützt, da das Security-Framework in ggf. anderen Ausbaustufen und mit anderen Laufzeitparametern an beliebig vielen Standorten eingesetzt werden kann.
- Die *essentielle* Anforderung **SF-INT-Skalierbarkeit** wird *vollständig* erfüllt, da entsprechende Untersuchungen auch im Hinblick auf den Energieverbrauch durchgängig in das Frameworkkonzept einfließen.
- Die *wichtige* Anforderung **SF-INT-Usability** wird *nicht* erfüllt: Im Frameworkkonzept werden bislang keine Aspekte der praktischen Anwendbarkeit, z. B. im Kontext der *TuneSec*-Parametrisierung, thematisiert.
- Schließlich wird die *wichtige* Anforderung **SF-INT-Wiederverwendbarkeit** *vollständig* erfüllt, da trotz der zum Zweck der Optimierung des Energieverbrauchs bewusst in Kauf genommenen Abweichungen von Standardprotokollen weitestgehend auf bereits in der Infrastruktur vorhandene Komponenten und Verfahren zurückgegriffen wird.

Im Bereich der Anforderungen an die Schnittstellen für Managementoperationen und -prozesse zeigen sich wiederum Einschränkungen hinsichtlich der vom Security-Framework abgedeckten Aspekte:

- Die *wichtige* Anforderung **SF-MGMT-Administrationskonzept** wird *vollständig* erfüllt, da die für seinen Einsatz relevanten Konfigurations- und Optimierungsmöglichkeiten beschrieben werden und diese die nicht IT-sicherheitsspezifischen Administrationskonzepte komplementieren.

- Die *wichtige* Anforderung **SF-MGMT-Berichtsdetails** wird *nicht* erfüllt, da auf Security-Reports bzw. dafür erforderliche Roh-/Messdaten nicht eingegangen und somit auch die geforderte Zielgruppenorientierung nicht erörtert wird.
- Die *essentielle* Anforderung **SF-MGMT-Compliance** wird *partiell* erfüllt, da lediglich auf Datenschutz und auch darauf nur am Rande eingegangen wird.
- Die *wichtige* Anforderung **SF-MGMT-Delegation** wird *zielführend partiell* erfüllt, da zwar zur Laufzeit Anpassungen des Systems an den aktuellen Schutzbedarf vorgesehen sind, die sich jedoch innerhalb zentral vordefinierter Grenzen bewegen müssen.
- Die *wünschenswerte* Anforderung **SF-MGMT-Events** wird *partiell* erfüllt: Im Rahmen der *TuneSec*-Komponente *Resource Manager* sind zwar Schnittstellen vorgesehen, die zur Bewertung und Eskalation sicherheitsrelevanter Ereignisse genutzt werden könnten, auf deren konkrete Ausprägung und die weitere Verarbeitung wird jedoch nicht eingegangen.
- Die *essentielle* Anforderung **SF-MGMT-ITSM-Schnittstellen** wird *nicht* erfüllt, da eine entsprechende Einbettung ins oder Querbeziehungen zum IT Service Management im Frameworkkonzept weder explizit noch implizit thematisiert werden.
- Die *wichtige* Anforderung **SF-MGMT-Kosten** wird *partiell* erfüllt: Das Frameworkkonzept stellt die durch seinen Einsatz erreichbaren Energieeinsparungen auch unter dem Aspekt der Energiekosten dar; auf sämtliche darüber hinausgehenden Kosten, beispielsweise auch die zur Anpassung und Umsetzung sowie zum Betrieb des Frameworks erforderlichen Kosten, wird nicht eingegangen.
- Die *wünschenswerte* Anforderung **SF-MGMT-KPIs** wird *vollständig* erfüllt, da im Rahmen der Modellierung der relevanten Operationen und Protokolle auch eine einfache Quantifizierungsmethodik für die erreichte Sicherheitsstärke festgelegt wird, auf die beispielsweise in SLAs Bezug genommen werden kann; es gelten jedoch dieselben Einschränkungen, die unten bei der Anforderung SF-MGMT-Metriken diskutiert werden.
- Die *wichtige* Anforderung **SF-MGMT-Mandantenfähigkeit** wird *zielführend partiell* erfüllt. Zur nicht im Detail im Frameworkkonzept thematisierten Mandantentrennung ist jedoch der Einsatz verschiedener WLANs erforderlich, für die das Security-Framework entsprechend parametrisiert werden kann.
- Die *essentielle* Anforderung **SF-MGMT-Metriken** wird *partiell* erfüllt. Mit der vom Frameworkkonzept vorgeschlagenen Quantifizierung der Sicherheitsstärke können zwar vergleichende Aussagen über die für verschiedene Schutzniveaus ausgewählten Sicherheitsmechanismen getroffen werden; die geforderte kontinuierliche Überwachung des im praktischen Betriebs erreichten Sicherheitsniveaus findet aber nicht statt.
- Die *essentielle* Anforderung **SF-MGMT-Operationen** wird *vollständig* erfüllt, da die zum Management des Security-Frameworks bzw. zur Administration der zentralen *TuneSec*-Steuerkomponente relevanten Operationen in mehreren relevanten Variationen beschrieben werden.
- Die *wichtige* Anforderung **SF-MGMT-Performanz** wird *vollständig* erfüllt; entsprechende Messungen und Analysen werden in einem eigenen Kapitel des Frameworkkonzepts vorgestellt.

- Die *wichtige* Anforderung **SF-MGMT-Policies** wird *zielführend partiell* erfüllt: Der Einsatz von Security-Policies, mit denen Anforderungen an das zu erreichende Schutzniveau abgebildet werden, ist auf technischer Ebene explizit vorgesehen; die geforderte Schnittstelle, über die das Frameworkkonzept auch Einfluss auf Sicherheitsrichtlinien – im vorliegenden Fall z. B. bezüglich der Nutzung von WLANs durch Kunden und Anwender – nimmt, fehlt jedoch.
- Die *wichtige* Anforderung **SF-MGMT-Praxis** wird *zielführend partiell* erfüllt, da die Ergebnisse aus dem Einsatz an drei Standorten in die weitere Entwicklung des Frameworkkonzepts eingeflossen sind.
- Die *essentielle* Anforderung **SF-MGMT-Prozesse** wird *partiell* erfüllt, da die für das Management des Security-Frameworks erforderlichen organisatorischen Abläufe nicht explizit spezifiziert sind, in groben Zügen jedoch aus der Beschreibung u. a. des Administrationskonzept hervorgehen.
- Die *wichtige* Anforderung **SF-MGMT-Quantifizierung** wird *zielführend partiell* erfüllt: Der vorhandenen Modellierung und Messung von Sicherheitsstärken und Energieaufwendungen steht ein Mangel an Quantifizierung z. B. von Risiken und damit verbunden einer Möglichkeit zur Priorisierung der Umsetzungsschritte gegenüber, der somit mit Eigenaufwand spezifisch pro Einsatzszenario kompensiert werden muss.
- Die *wichtige* Anforderung **SF-MGMT-Releasezyklus** wird *nicht* erfüllt, da im Frameworkkonzept weder Rollout-/Rollbackkonzepte noch Frameworkaktualisierungen vorgesehen sind.
- Die *wichtige* Anforderung **SF-MGMT-Schulungen** wird *nicht* erfüllt, da entsprechende Aus- und Weiterbildungsmaßnahmen analog zu den bereits diskutierten Usability-Aspekten im Frameworkkonzept nicht thematisiert werden.
- Die *wünschenswerte* Anforderung **SF-MGMT-Support** wird *nicht* erfüllt, da das Security-Framework von keinem externen Dienstleister unterstützt wird und der Autor zwischenzeitlich an einer anderen Hochschule mit anderem Aufgabengebiet tätig ist und keine Auskünfte mehr zum Security-Framework erteilt.
- Die *wünschenswerte* Anforderung **SF-MGMT-Tests** wird *nicht* erfüllt, da keinerlei Schnittstellen, Methoden oder Ansatzpunkte für eine initiale bzw. kontinuierliche Funktionsüberprüfung spezifiziert werden.
- Die *essentielle* Anforderung **SF-MGMT-Verbesserung** wird *nicht* erfüllt, da sich das Frameworkkonzept noch auf seinem initialen Stand befindet und derzeit keine Weiterentwicklung absehbar ist.
- Schließlich wird auch die *wünschenswerte* Anforderung **SF-MGMT-Zuständigkeiten** *nicht* erfüllt, da zwischen verschiedenen Rollen und Zuständigkeiten in Bezug auf das Security-Framework nicht unterschieden wird.

Bezüglich der Anforderungen an die Dokumentation von Security-Frameworks ergeben sich folgende Bewertungen:

- Die *wichtige* Anforderung **SF-DOKU-Anforderungsanalyse** wird *zielführend partiell* erfüllt, da die Vorgehensweise bei der Anforderungsanalyse zwar nicht explizit beschrieben ist, aber aus dem Kontext und der Struktur des Frameworkkonzepts hervorgeht.

- Die *wichtige* Anforderung **SF-DOKU-Angreifermodelle** wird *vollständig* erfüllt: Auf die berücksichtigten Fähigkeiten potentieller Angreifer wird an vielen Stellen – nicht nur bei der Beschreibung möglicher Angriffe, sondern auch bei der Diskussion vorgeschlagener Lösungsansätze – eingegangen.
- Die *wichtige* Anforderung **SF-DOKU-Ausrichtung** wird *zielführend partiell* erfüllt: Bei der Beschreibung der einzelnen Sicherheitsmechanismen wird die Prävention – und nur diese – mehrmals aufgegriffen.
- Die *wünschenswerte* Anforderung **SF-DOKU-Beurteilung** wird *nicht* erfüllt, da die Dokumentation des Frameworks nicht auf Kriterien dafür eingeht, wie das Ergebnis von Anpassungsprozess bzw. praktischer Umsetzung beurteilt werden können.
- Die *wünschenswerte* Anforderung **SF-DOKU-Checkliste** wird *nicht* erfüllt, da im Frameworkkonzept keine Aufbereitung der Zwischenschritte stattfindet, mit der die praktische Umsetzung unterstützt wird.
- Die *wichtige* Anforderung **SF-DOKU-Designentscheidungen** wird *zielführend partiell* erfüllt, indem die meisten – jedoch nicht alle – Designentscheidungen unter den im Frameworkkonzept festgehaltenen Gesichtspunkten beurteilt werden.
- Die *wünschenswerte* Anforderung **SF-DOKU-Kontinuum** wird *nicht* erfüllt, da aus dem Frameworkkonzept weder ein prozessorientierter Charakter hervorgeht noch auf die kontinuierliche Weiterentwicklung eingegangen wird.
- Die *wünschenswerte* Anforderung **SF-DOKU-Lifecyclephasen** wird *partiell* erfüllt: Die vom Frameworkkonzept abgedeckten Lebenszyklusabschnitte (Design, Customizing und Pilotbetrieb) werden darin zwar nicht explizit erläutert, gehen aber aus dem Kontext hervor.
- Die *wichtige* Anforderung **SF-DOKU-Vollständigkeit** wird *nicht* erfüllt, da der dem Frameworkkonzept zugrunde liegende Betrachtungsraum nicht explizit nach außen abgegrenzt wird und keine Selbsteinschätzung bezüglich der Vollständigkeit der präsentierten Lösungsbausteine vorgenommen wird.
- Die *essentielle* Anforderung **SF-DOKU-Voraussetzungen** wird *zielführend partiell* erfüllt, da die bezüglich der vorhandenen Infrastruktur postulierten Anforderungen sowohl hardware- als auch softwareseitig aus den Beschreibungen im Frameworkkonzept indirekt hervorgehen.
- Die *wünschenswerte* Anforderung **SF-DOKU-Zertifizierung** wird *nicht* erfüllt. Auf entsprechende Zertifizierungsmöglichkeiten und -maßnahmen wird nicht eingegangen; in Anbetracht der bewussten Abweichung von Standardprotokollen an einigen Stellen bei voller Ausbaustufe des Security-Frameworks haben Zertifizierungsvorhaben jedoch offensichtlich nur eine geringe Priorität.
- Die *essentielle* Anforderung **SF-DOKU-Ziele** wird *vollständig* erfüllt: Die jeweiligen Ziele werden sowohl für das gesamte Security-Framework als auch viele der einzelnen beschriebenen Teile des Frameworks spezifiziert; allerdings sollte diese Zielsetzung nicht nur auf technischer, sondern auch auf organisatorischer Ebene erfolgen.
- Schließlich wird die *wünschenswerte* Anforderung **SF-DOKU-Zielgruppe** *zielführend partiell* erfüllt, da im Frameworkkonzept zwar keine explizite Zielgruppe genannt wird,

insgesamt aber deutlich erkennbar wird, dass es sich an Technologieexperten und Systemarchitekten (vgl. Rollendefinition in Abschnitt 2.2.1) wendet.

In Abbildung 4.7 sind der Erfüllungsgrad der Anforderungen und die sich daraus ergebenden Bewertungszahlen auf Basis der in Abschnitt 3.7.1 erläuterten Nutzwertanalyse zusammengefasst.

Aus dieser Bewertungsübersicht geht erneut deutlich hervor, dass das untersuchte Security-Framework konzeptionell zu einseitig auf die Prävention von Sicherheitsvorfällen und zu wenig auf den praktischen Einsatz ausgelegt ist: Das Fehlen jeglicher Protokollierungs- und Auditierungsmöglichkeiten erschwert die automatische Detektion von sicherheitsrelevanten Ereignissen signifikant und führt zu einer deutlichen Abwertung im ansonsten starken sicherheitsfunktionalen Bereich. Eine stärkere Ausrichtung auf den Produktiveinsatz des Security-Frameworks könnte erreicht werden, indem einerseits bislang vernachlässigte Aspekte wie Usability, Rollout-Konzept, Testmöglichkeiten sowie Schulungen und Support aufgegriffen werden. Andererseits ist sowohl im Hinblick auf die Managementschnittstellen als auch die Frameworkdokumentation eine stärkere Prozessorientierung anzuraten, bei der auch auf die Schnittstellen z. B. zu den ITSM-Prozessen eingegangen wird. In den beiden Anforderungskategorien SF-MGMT und SF-DOKU zeigt sich bei einem Großteil der nur *partiell* erfüllten Anforderungen zudem, dass die entsprechenden Überlegungen vertieft und im Frameworkkonzept expliziter und umfassender dargestellt werden sollten.

4.4. Ergebnisse der Analyse weiterer Security-Frameworks

In diesem Abschnitt werden die Ergebnisse der Analyse der mehr als 70 auf Basis des in Abschnitt 4.1.2.1 beschriebenen Verfahrens ermittelten weiteren Security-Frameworks kompakt vorgestellt.

Das dabei im Rahmen dieser Arbeit verfolgte Primärziel ist, eine Basis für die in Abschnitt 4.5 diskutierte Auswertung zu legen. Auf dieser Grundlage können die typischen Stärken und Schwächen bisheriger Security-Frameworks ermittelt werden, um daraus Konsequenzen für die weiteren Schwerpunkte dieser Arbeit abzuleiten.

Neben der zusammenfassenden Präsentation der Ergebnisse der Nutzwertanalyse in Form der bereits bekannten Tabellen werden pro Security-Framework dessen Ziele und Schwerpunkte skizziert. Daran anschließend werden jeweils die herausragenden Stärken sowie einige Verbesserungsmöglichkeiten, die sich unmittelbar aus der Anwendung des Bewertungsverfahrens ergeben, zusammengefasst. Sekundär ergibt sich somit ein umfassender Überblick über die aktuellen Security-Frameworks.

Bezüglich der Auswertung ist anzumerken, dass aus offensichtlichen Gründen nur das jeweils schriftlich vorliegende Frameworkkonzept beurteilt werden konnte: Sofern ein Security-Framework also beispielsweise nur als Konferenzbeitrag mit einstelliger Seitenzahl veröffentlicht wurde, ergeben sich Abwertungen bei Aspekten, die – möglicherweise nur aus Platzgründen – nicht adäquat dokumentiert wurden, obwohl sie bei der Entwicklung eventuell durchaus beachtet worden sind.

Die Analyseergebnisse werden nach Frameworkkategorie und darin alphabetisch nach Frameworknamen sortiert vorgestellt:

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**3**	6
Summe SF-FUNK	21		49

SF-MGMT-Adminkonzepte	2	**3**	6
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**1**	4
SF-MGMT-Delegation	2	**2**	4
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**1**	2
SF-MGMT-KPIs	1	**3**	3
SF-MGMT-Mandantenfähigkeit	2	**2**	4
SF-MGMT-Metriken	4	**1**	4
SF-MGMT-Operationen	4	**3**	12
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**2**	4
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		62

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**3**	6
SF-INT-Customizing	4	**2**	8
SF-INT-Einführung	2	**2**	4
SF-INT-Erweiterung	2	**3**	6
SF-INT-Hochverfügbarkeit	2	**2**	4
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		59

SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**3**	6
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**1**	1
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		41

Bewertungszahlen:		SF-FUNK:	2,33
		SF-INT:	2,03
		SF-MGMT:	1,22
Gesamt:	**1,82**	SF-DOKU:	1,71

Abbildung 4.7.: Nutzwertanalyse des Energy Efficient Security Framework for Wireless Local Area Networks

- Die Vorstellung der Analyseergebnisse der Security-Frameworks für das Software Engineering beginnt nachfolgend auf Seite 168.
- Die Analyseergebnisse der Security-Frameworks für IT-Dienste schließen sich ab Seite 181 an.
- Den Abschluss bilden die Analyseergebnisse der Security-Frameworks für IT-Architekturen ab Seite 206.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		23

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		26

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**3**	6
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**1**	2
SF-INT-Parallelbetrieb	4	**1**	4
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		31

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		34

Bewertungszahlen:			
		SF-FUNK:	1,10
		SF-INT:	1,07
		SF-MGMT:	0,51
Gesamt:	**1,02**	SF-DOKU:	1,42

Abbildung 4.8.: Nutzwertanalyse des generic framework for context-based distributed authorizations ([MB03])

Frameworkkategorie:	Software Engineering	Referenz: [MB03]
Frameworkname:	A generic framework for context-based distributed authorizations	
Frameworkautoren:	Mostéfaoui, G. K.; Brezillon, P.	

Das 2003 veröffentlichte Security-Framework dient als Grundlage für die Implementierung von Autorisierungsmechanismen in Ubiquitous-Computing-Anwendungen; dabei werden insbesondere auch Informationen über die Umgebung, in der sich der jeweilige Benutzer gerade aufhält, in die Entscheidungen mit einbezogen. Die vorgestellten Konzepte sind auf andere mobile Anwendungen übertragbar. Wie die in Abbildung 4.8 zusammengefasste Bewertung zeigt, stehen bei der untersuchten Arbeit die Adaptivität, die Erweiterbarkeit und der Einsatz technischer Policies im Vordergrund.

Eine Umsetzung des Frameworkkonzepts ist bislang nur in einer Testumgebung erfolgt. Durch den Schwerpunkt, Umgebungsinformationen als Eingabe für Policy Decision Points zur Verfügung zu stellen, erhält das gesamte Framework einen rein präventiven Charakter – Maßnahmen zur Erkennung von Sicherheitsvorfällen und auch Auditingmechanismen spielen bislang keine Rolle. Für die Weiterentwicklung ist wünschenswert, dass weitere technische wie auch organisatorische Maßnahmen, die über den reinen Autorisierungsprozess hinausgehen, erarbeitet und integriert werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		34

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**1**	2
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**1**	2
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**1**	1
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**3**	3
Summe SF-MGMT	51		38

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**2**	8
SF-INT-Einführung	2	**2**	4
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**3**	12
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**2**	4
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		63

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**2**	4
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**1**	1
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**3**	3
SF-DOKU-Lifecyclephasen	1	**2**	2
SF-DOKU-Vollständigkeit	2	**1**	2
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**3**	3
Summe SF-DOKU	24		51

Bewertungszahlen:			
		SF-FUNK:	1,62
		SF-INT:	2,17
		SF-MGMT:	0,75
Gesamt:	**1,67**	SF-DOKU:	2,13

Abbildung 4.9.: Nutzwertanalyse des Multi-Tier, Multi-Role Security Framework for E-Commerce Systems ([CM07])

Frameworkkategorie:	Software Engineering	Referenz: [CM07]
Frameworkname:	A Multi-Tier, Multi-Role Security Framework for E-Commerce Systems	
Frameworkautoren:	Cachia, E.; Micallef, M.	

Das 2007 von der Software Engineering Process Improvement Research Group der Universität Malta veröffentlichte Security-Framework geht explizit auf mehrere Aspekte ein, die von den meisten der hier analysierten Arbeiten noch nicht in der angestrebten Ausführlichkeit betrachtet werden: Zum einen spielt der Lebenszyklus der unter Zuhilfenahme des Frameworks erstellten Dienste eine wesentliche Rolle, wofür auch die Erstellung von Checklisten zumindest angedacht ist. Zum anderen wird auf die Wichtigkeit eines kontinuierlichen Ansatzes mit einer sukzessiven Verbesserung des Sicherheitsniveaus eingegangen. Darüber hinaus nimmt die Arbeit eine Kategorisierung der relevanten Angriffsbereiche vor und gibt – wie aus dem Titel bereits hervorgeht – die Zuständigkeiten in Form eines flexiblen Rollenmodells konkret vor.

Bei der Weiterentwicklung des Security-Frameworks, dessen Bewertung in Abbildung 4.9 zusammengefasst ist, sollten zum einen Möglichkeiten zur Werkzeugunterstützung der beschriebenen Abläufe konzipiert werden. Zum anderen sollten auch die über die unmittelbaren Framework-Managementoperationen hinausgehenden Schnittstellen zu weiteren Prozessen erläutert werden; beispielsweise sollten die Zusammenhänge zwischen den bereits beschriebenen Angreifermodellen und Angriffen mit dem Risikomanagement beschrieben werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		31

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**3**	6
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**1**	2
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**1**	2
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		30

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**0**	0
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**1**	2
Summe SF-INT	29		25

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**2**	2
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		34

Bewertungszahlen:		SF-FUNK:	1,48
		SF-INT:	0,86
		SF-MGMT:	0,59
Gesamt:	**1,09**	SF-DOKU:	1,42

Abbildung 4.10.: Nutzwertanalyse von: A Policy Language for Adaptive Web Services Security Framework ([Che07])

Frameworkkategorie:	Software Engineering	Referenz: [Che07]
Frameworkname:	A Policy Language for Adaptive Web Services Security Framework	
Frameworkautor:	Che, T.	

Das 2007 veröffentlichte Security-Framework beschränkt sich explizit auf das Thema Access Control und wendet sich implizit eher an Systemdesigner als an Softwareentwickler. Das vorgestellte Konzept, das eine Architektur zur Administration und Anwendung systemnaher Policies umfasst, wurde bislang nur im Rahmen einer Konzeptstudie in die Praxis umgesetzt.

Wie auch die in Abbildung 4.10 zusammengefasste Bewertung zeigt, fehlt für die praktische Umsetzung in eigenen Szenarien insbesondere eine prozessorientierte Beschreibung der Schnittstellen zu den Systemen, die von der policybasierten Zugriffskontrolle profitieren sollen. Für die Weiterentwicklung ist wünschenswert, dass über den rein präventiv steuernden Charakter der Policies auch auf die Überwachung der Policyeinhaltung – beispielsweise durch Auditmechanismen – und mögliche Sicherheitsvorfälle eingegangen wird.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**1**	1
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		23

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**1**	2
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**3**	6
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**1**	2
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**3**	3
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**3**	12
SF-MGMT-Zuständigkeiten	1	**1**	1
Summe SF-MGMT	51		38

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**2**	8
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**3**	12
SF-INT-Polyinstanziierbark.	1	**2**	2
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		54

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**0**	0
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**1**	1
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		33

Bewertungszahlen:			
		SF-FUNK:	1,10
		SF-INT:	1,86
		SF-MGMT:	0,75
Gesamt:	**1,27**	SF-DOKU:	1,38

Abbildung 4.11.: Nutzwertanalyse des Public Web Services Security Framework Based on Current and Future Usage Scenarios ([TM02])

Frameworkkategorie:	Software Engineering	Referenz: [TM02]
Frameworkname:	A Public Web Services Security Framework Based on Current and Future Usage Scenarios	
Frameworkautoren:	Thelin, J.; Murray, P. J.	

In der Arbeit von Thelin und Murray werden zunächst mehrere Szenarien, in denen Web Services zum Einsatz kommen, vorgestellt und bezüglich der zu ihrer grundlegenden Absicherung erforderlichen Maßnahmen untersucht. Das anschließend vorgestellte Framework befindet sich seit mehreren Jahren im Praxiseinsatz; über die Verbindung zur Firma Cape Clear Software steht auch entsprechender Support zur Verfügung.

Am 2002 veröffentlichten Framework fällt positiv auf, dass es explizit auf den parallelen Einsatz weiterer Sicherheitsmaßnahmen von Dritten ausgelegt ist. Das Customizing des Frameworks ist explizit vorgesehen, sollte jedoch noch ausführlicher beschrieben werden. Abbildung 4.11 zeigt die zusammengefasste Bewertung: Sowohl techniknahe Aspekte wie das Monitoring und Auditing als auch insbesondere die Prozesseinbettung und das Management der mit dem Framework geschützten Produkte sollten präzise erläutert werden. Weitere Verbesserungen würden sich auch durch Untersuchungen der Performance und durch Verfahrensbeschreibungen oder konzeptionelle Analysen der mit dem Frameworkeinsatz erzielten Verbesserungen des Sicherheitsniveaus ergeben.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**2**	4
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		35

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		10

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**1**	2
SF-INT-Parallelbetrieb	4	**1**	4
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**0**	0
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		24

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**1**	1
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**0**	0
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		29

Bewertungszahlen:		SF-FUNK:	1,67
		SF-INT:	0,83
		SF-MGMT:	0,20
Gesamt:	**0,97**	SF-DOKU:	1,21

Abbildung 4.12.: Nutzwertanalyse des Security Framework for a Mobile Agent System ([Bry00])

Frameworkkategorie:	Software Engineering	Referenz: [Bry00]
Frameworkname:	A Security Framework for a Mobile Agent System	
Frameworkautor:	Bryce, C.	

Das im Jahr 2000 veröffentlichte Security-Framework für mobile Agentensysteme legt seinen Schwerpunkt auf das Erreichen der beiden Eigenschaften *believability* und *survivability*. Es ist gut strukturiert und folgt dabei i. W. dem in Abschnitt 4.2 diskutierten Aufbau. Inhaltlich wendet es sich dabei nicht nur an Java-Entwickler, sondern durch die zusätzliche Verwendung von Pseudocode insbesondere auch an Wissenschaftler. Durch den Einsatz von Monitoring, Policies und Kryptographie wird neben den beiden primär gewünschten Eigenschaften auch der Schutz gegen Denial-of-Service-Angriffe und bösartige Hosts, auf denen mobiler Code ausgeführt werden soll, verbessert. Viele weitere Sicherheitseigenschaften, die für mobilen Code ebenfalls relevant sind, werden jedoch nicht erörtert, so dass sich auch im sicherheitsfunktionalen Bereich Defizite ergeben. Wie bei diversen anderen Security-Frameworks für das Software Engineering wird auf das Management der mit ihrer Hilfe erstellten Softwareprodukte nicht näher eingegangen, so dass die damit verbundenen Anforderungen wie in Abbildung 4.12 dargestellt insbesondere in der Kategorie SF-MGMT nicht zufriedenstellend erfüllt werden. Zur Verbesserung bietet sich deshalb an, entsprechende Erfahrungen aus der auf diesem Security-Framework basierenden Entwicklung und dem praktischen Einsatz in Folgeversionen einfließen zu lassen.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		18

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**3**	6
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**2**	4
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**3**	6
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		28

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**0**	0
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		25

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**1**	4
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		26

Bewertungszahlen:		SF-FUNK:	0,86
		SF-INT:	0,86
		SF-MGMT:	0,55
Gesamt:	**0,84**	SF-DOKU:	1,08

Abbildung 4.13.: Nutzwertanalyse des adaptable security framework for service-based systems ([YYCZ05])

Frameworkkategorie:	Software Engineering	Referenz: [YYCZ05]
Frameworkname:	An adaptable security framework for service-based systems	
Frameworkautoren:	Yau, S. S.; Yao, Y.; Chen, Z.; Zhu, L.	

Das Security-Framework befasst sich umfassend mit Maßnahmen zur Abbildung von in natürlicher Sprache formulierten Richtlinien auf rechnergestützt auswertbare Regelsätze und den damit verbundenen technischen Schwierigkeiten im Kontext von Diensten, die durch die Zusammenstellung unabhängiger Web Services in serviceorientierten Architekturen implementiert werden.

Wie die in Abbildung 4.13 zusammengefasste Bewertung zeigt, werden bereits die technischen bzw. sicherheitsfunktionalen Aspekte durch die ausschließliche Behandlung des Themenbereichs Access Control den gestellten Anforderungen und Zielen nicht gerecht, zumal lediglich auf die Spezifikation, nicht aber die Umsetzung bzw. das Policy Enforcement eingegangen wird. Auch die Anpassbarkeit des Frameworks selbst sowie die Betriebs- und Managementaspekte der mithilfe des Frameworks erstellten Dienste sollten bei der Weiterentwicklung stärker berücksichtigt werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**2**	4
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**1**	2
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		36

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		12

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**0**	0
SF-INT-Modularität	2	**0**	0
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**0**	0
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		2

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**1**	4
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		24

Bewertungszahlen:			
		SF-FUNK:	1,71
		SF-INT:	0,07
		SF-MGMT:	0,24
Gesamt:	**0,75**	SF-DOKU:	1,00

Abbildung 4.14.: Nutzwertanalyse des aspect-oriented security framework ([SH03])

Frameworkkategorie:	Software Engineering	Referenz: [SH03]
Frameworkname:	An aspect-oriented security framework	
Frameworkautoren:	Shah, V.; Hill, F.	

Das ursprünglich 2003 veröffentlichte Security-Framework beschreibt die Anwendung der aspektorientierten Programmierung auf ausgewählte IT-Sicherheitsthemen wie die Vermeidung von Buffer-Overflows. Die knapp gehaltene Beschreibung geht jedoch lediglich auf die konzeptionellen Aspekte, nicht aber auf die praktische Anwendung in beliebigen eigenen Szenarien ein. Auch der Nachfolgeartikel [SH04], in dem praktische Erfahrungen und einige Verbesserungen vorgestellt werden, vertieft weder die szenarienspezifische Anwendung noch das Spektrum der betrachteten Ansatzpunkte zur Verbesserung der Sicherheit von Anwendungen.

Wie sich auch in der Bewertung, die in Abbildung 4.14 zusammengefasst ist, niederschlägt, würde das Framework sowohl von einer gezielteren Darstellung seiner Umsetzung als auch von einer Diskussion der Auswirkungen auf den Betrieb der mit seiner Hilfe abgesicherten Anwendungen profitieren.

Frameworkkategorie:	Software Engineering	Referenz: [NSA04]
Frameworkname:	Guide to Microsoft .NET Framework Security	
Frameworkautor:	NSA	

Der 2004 von der NSA veröffentlichte Leitfaden zur IT-Sicherheit des Microsoft .NET-Frameworks geht detailliert auf die Sicherheitsaspekte von .NET allgemein sowie auf die spezifischen Sicherheitsfunktionen ein. Er beschreibt auch alle relevanten administrativen Aufgaben und wendet sich nicht nur an Programmierer, sondern auch an Systemadministratoren. Neben präventiven Maßnahmen werden auf technischer Ebene explizit auch Ereignisprotokolle und Auditmaßnahmen angesprochen, deren Auswertung z. B. im Rahmen von zielgruppenspezifischen Berichten jedoch nicht diskutiert wird. Positiv von vielen anderen der hier untersuchten Arbeiten hebt sich ab, dass sowohl pro Kapitel des Frameworkkonzepts als auch für den gesamten Inhalt mit Checklisten vergleichbare Empfehlungslisten dokumentiert wurden.

Zur Weiterentwicklung des Frameworks, dessen Bewertung in Abbildung 4.15 zusammengefasst ist, sind weitere, konkretere und ausführlichere Beispiele wünschenswert. Es sollte auch stärker auf Selektionsmechanismen oder Best Practices eingegangen werden, die Aufschluss darüber geben, wann welche der verfügbaren technischen Sicherheitsmaßnahmen eingesetzt werden sollen. Ebenso sollten typische Schwachstellen und Angriffe, für die sich die technischen Lösungsansätze eignen, benannt werden. Neben der Einordnung in systemadministrative Konzepte sollte auch eine Einbettung des .NET-Sicherheitsmanagements in die übrigen Managementprozesse vorgenommen werden.

Frameworkkategorie:	Software Engineering	Referenz: [Sun05]
Frameworkname:	Java™ security overview	
Frameworkautor:	Sun Microsystems	

Sun Microsystems hat 2005 in Form eines White Papers eine an Java-Programmierer gerichtete, mit Beispielen angereicherte Übersicht über die auf Basis der Java-Standardfunktionsbibliotheken bereitgestellten Sicherheitsfunktionen und -schnittstellen veröffentlicht. Sie deckt unter anderem die Themen kryptographische Algorithmen, Authentifizierung, abgesicherter Nachrichtenaustausch und Access Control ab. Dabei stehen jeweils verschiedene Implementierungsvarianten zur Auswahl; beispielsweise wird sowohl über SASL als auch über GSS-API eine Schnittstelle zur Benutzerauthentifizierung angeboten. Erwartungsgemäß orientieren sich die Ausführungen sehr eng an Technik und Programmiersprache. Wünschenswert sind deshalb ergänzende Informationen darüber, wie sich die Wahl der jeweiligen Implementierungsvariante z. B. auf den Administrationsaufwand im späteren Betrieb auswirkt. Abbildung 4.16 fasst die Bewertung dieses Security-Frameworks zusammen.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		42

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**3**	6
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**3**	3
SF-MGMT-ITSM-Schnittstellen	4	**1**	4
SF-MGMT-Kosten	2	**1**	2
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**3**	12
SF-MGMT-Performanz	2	**2**	4
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**2**	4
SF-MGMT-Schulungen	2	**2**	4
SF-MGMT-Support	1	**2**	2
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**3**	3
Summe SF-MGMT	51		68

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**2**	4
SF-INT-Customizing	4	**2**	8
SF-INT-Einführung	2	**2**	4
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**1**	2
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		57

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**3**	3
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**2**	2
SF-DOKU-Lifecyclephasen	1	**2**	2
SF-DOKU-Vollständigkeit	2	**2**	4
SF-DOKU-Voraussetzungen	4	**3**	12
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**3**	3
Summe SF-DOKU	24		52

Bewertungszahlen:			SF-FUNK:	2,00
			SF-INT:	1,97
			SF-MGMT:	1,33
	Gesamt:	**1,87**	SF-DOKU:	2,17

Abbildung 4.15.: Nutzwertanalyse des Guide to Microsoft .NET Framework Security ([NSA04])

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		22

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**3**	6
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**3**	6
SF-MGMT-Schulungen	2	**3**	6
SF-MGMT-Support	1	**3**	3
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**3**	12
SF-MGMT-Zuständigkeiten	1	**3**	3
Summe SF-MGMT	51		44

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**3**	12
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**3**	6
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		53

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**0**	0
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**0**	0
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**1**	2
SF-DOKU-Voraussetzungen	4	**3**	12
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**3**	3
Summe SF-DOKU	24		29

Bewertungszahlen:			SF-FUNK:	1,05
			SF-INT:	1,83
			SF-MGMT:	0,86
	Gesamt:	**1,24**	SF-DOKU:	1,21

Abbildung 4.16.: Nutzwertanalyse des Java^{TM} security overview ([Sun05])

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**0**	0
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		32

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**1**	1
Summe SF-MGMT	51		19

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		33

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		28

Bewertungszahlen:		SF-FUNK:	1,52
		SF-INT:	1,14
		SF-MGMT:	0,37
Gesamt:	**1,05**	SF-DOKU:	1,17

Abbildung 4.17.: Nutzwertanalyse von SAgent: A Security Framework for JADE ([GT06])

Frameworkkategorie:	Software Engineering	Referenz: [GT06]
Frameworkname:	SAgent: A Security Framework for JADE	
Frameworkautoren:	Gunupudi, V.; Tate, S. R.	

Das 2006 veröffentlichte Security-Framework SAgent thematisiert die Entwicklung von Agentensystemen in Java und dabei insbesondere den Schutz derjenigen Daten, die mit den mobilen Agenten auf potentiell bösartige oder kompromittierte Maschinen, auf denen sie ausgeführt werden, mitwandern. Dabei stellen die Entwicklungsplattform JADE und die für diese in Vorarbeiten bereits durchgeführten Sicherheitsuntersuchungen die konzeptionelle Basis des Frameworkkonzepts dar. Durch den expliziten Fokus auf dieser Art von Daten ist das Security-Framework nur bedingt auf die Entwicklung allgemeiner Agentensysteme anwendbar.

Für die Weiterentwicklung ist insbesondere wünschenswert, dass neben der Vorstellung der eigenen Implementierung verstärkt auf die Anwendung in eigenen Szenarien eingegangen wird, die sich sowohl aus Anpassungen als auch den Abläufen im Betrieb zusammensetzt. Die in Abbildung 4.17 zusammengefasste Bewertung verdeutlicht zudem, dass auch die Dokumentation des Security-Frameworks noch expliziter auf die zur Anwendung relevanten Aspekte eingehen sollte.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		49

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**2**	4
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**2**	4
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**3**	6
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**3**	6
SF-MGMT-Schulungen	2	**3**	6
SF-MGMT-Support	1	**3**	3
SF-MGMT-Tests	1	**1**	1
SF-MGMT-Verbesserung	4	**3**	12
SF-MGMT-Zuständigkeiten	1	**3**	3
Summe SF-MGMT	51		52

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**2**	4
SF-INT-Customizing	4	**2**	8
SF-INT-Einführung	2	**2**	4
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**2**	4
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		65

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**1**	1
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**3**	12
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**3**	3
Summe SF-DOKU	24		44

Bewertungszahlen:		SF-FUNK:	2,33
		SF-INT:	2,24
		SF-MGMT:	1,02
Gesamt:	**1,86**	SF-DOKU:	1,83

Abbildung 4.18.: Nutzwertanalyse des Generalized Security Framework ([DKM01])

Frameworkkategorie:	Software Engineering	Referenz: [DKM01]
Frameworkname:	The Generalized Security Framework	
Frameworkautoren:	Detry, R. J.; Kleban, S. D.; Moore, P. C.	

Das 2001 von den Sandia National Laboratories als technischer Bericht veröffentlichte Security-Framework wendet sich explizit an die Entwickler verteilter Anwendungen, ist konsequent modular aufgebaut und greift beim dargestellten Lösungsansatz nach einer klaren Darstellung der Ziele und Designentscheidungen auf Standardkomponenten wie die Generic Security Services (GSS) API zurück. Alle eingesetzten Mechanismen werden dabei explizit gekapselt und sind somit gut austauschbar. Positiv hervorzuheben ist neben diversen Anwendungsbeispielen, die auch die umfangreichen Erfahrungen im praktischen Einsatz aufzeigen, dass die sukzessive Weiterentwicklung des Security-Frameworks und ein entsprechender Release-Zyklus deutlich werden und auch ein entsprechender Support verfügbar ist.

Wie sich auch in der Bewertung, die in Abbildung4.18 zusammengefasst ist, zeigt, ist das Security-Framework in vielen Bereichen jedoch äußerst technisch ausgerichtet; beispielsweise sind zwar technische Schnittstellen zur Protokollierung und zum Auditing vorgesehen, auf die spätere Auswertung, z. B. in Form von Berichten, wird jedoch nicht eingegangen. Für zukünftige Version ist somit insbesondere eine Betrachtung, die über die einzelnen mit Hilfe des Security-Frameworks entwickelten verteilten Anwendungen hinausgeht und somit einen anwendungsübergreifenden Managementansatz beschreibt, wünschenswert.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		28

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**1**	2
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		14

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		35

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**0**	0
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		32

Bewertungszahlen:			
		SF-FUNK:	1,33
		SF-INT:	1,21
		SF-MGMT:	0,27
Gesamt:	**1,04**	SF-DOKU:	1,33

Abbildung 4.19.: Nutzwertanalyse der UDDI and WSDL extensions for Web services: a security framework ([AB02])

Frameworkkategorie:	Software Engineering	Referenz: [AB02]
Frameworkname:	UDDI and WSDL extensions for Web services: a security framework	
Frameworkautoren:	Adams, C.; Boeyen, S.	

Das 2002 von der Firma Entrust entwickelte und auf dem ACM Workshop on XML Security vorgestellte Security-Framework schlägt Erweiterungen der UDDI-Registry und der Sprache WSDL vor, um die Sicherheit von entfernten Web-Service-Aufrufen zu verbessern. Obwohl auf Unzulänglichkeiten von UDDI und WSDL eingegangen wird, fehlt dem Frameworkkonzept eine Beschreibung der relevanten Schwachstellen und Angriffe, vor denen geschützt werden soll. Als Lösungsansatz wird insbesondere der Einsatz von Policies in der Sprache XACML vorgeschlagen; allerdings gehen die Beschreibungen nicht auf die damit verbundenen operativen Managementabläufe im Betrieb ein. Auch die Übertragbarkeit auf bzw. die Anwendung in eigenen Szenarien wird nicht konkret behandelt. Vermutlich aufgrund der Standardisierung alternativer Lösungsansätze in den Folgejahren wurde das vorgestellte Security-Framework, dessen Bewertung in Abbildung 4.19 zusammengefasst ist, bislang nicht mehr weiterentwickelt.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**0**	0
SF-FUNK-Angriffe	2	**2**	4
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		28

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**1**	2
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**1**	1
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		18

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		35

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		36

Bewertungszahlen:			
		SF-FUNK:	1,33
		SF-INT:	1,21
		SF-MGMT:	0,35
Gesamt:	**1,10**	SF-DOKU:	1,50

Abbildung 4.20.: Nutzwertanalyse: Using aspects for security engineering of web service compositions ([CM05])

Frameworkkategorie:	Software Engineering	Referenz: [CM05]
Frameworkname:	Using aspects for security engineering of web service compositions	
Frameworkautoren:	Charfi, A.; Mezini, M.	

Die 2005 veröffentlichte Arbeit von Charfi und Mezini erläutert ein Framework, das die aspektorientierte Programmierung mit der Komposition von Web Services unter Berücksichtigung von IT-Sicherheitsaspekten verknüpft. Anhand eines Beispiels werden die vom Frameworkkonzept berücksichtigten Angriffe und die Anforderungen erläutert. Das Framework liegt auch als Implementierung vor, deren Verwendung vorgestellt wird.

Bezüglich der Prozesseinbettung geht das Security-Framework bislang lediglich auf die Abläufe beim Deployment der Java-Bibliotheken ein; insgesamt liegt der Fokus auf der sehr technisch orientierten Darstellung der Idee und Lösungsanwendung, wobei stärker auf die eigene Implementierung als auf die Übertragbarkeit auf andere Szenarien eingegangen wird. Wie die in Abbildung 4.20 zusammengefasste Bewertung zeigt, werden in jedem der vier Anforderungsbereiche diverse Aspekte bislang noch nicht berücksichtigt. Auch in den vom Security-Framework bereits abgedeckten Bereichen ist eine vertiefte und stärker auf die Übertragbarkeit ausgerichtete Darstellung wünschenswert.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**1**	1
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**1**	2
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		27

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**2**	8
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**1**	2
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		40

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**1**	2
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**1**	4
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		25

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**1**	1
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		31

Bewertungszahlen:		SF-FUNK:	1,29
		SF-INT:	0,86
		SF-MGMT:	0,78
Gesamt:	**1,06**	SF-DOKU:	1,29

Abbildung 4.21.: Nutzwertanalyse der dynamic, context-aware security infrastructure for distributed healthcare applications ([HW04])

Frameworkkategorie:	IT-Dienst	Referenz: [HW04]
Frameworkname:	A dynamic, context-aware security infrastructure for distributed healthcare applications	
Frameworkautoren:	Hu, J.; Weaver, A. C.	

Bei dem von den Autoren als *security infrastructure* bezeichneten Konzept handelt es sich in der in dieser Arbeit verwendeten Terminologie um ein Security-Framework zur Absicherung einzelner verteilter Anwendungen für das Gesundheitswesen bzw. für den Einsatz in größeren E-Health-Infrastrukturen. Durch die inhaltliche Beschränkung auf rollenbasierte Zugriffskontrolle deckt die vorgeschlagene Lösung jedoch nur einen Teil des Problembereichs ab. Die technische Unvollständigkeit zeigt sich auch darin, dass zwar ein formales Modell präsentiert wird, das z. B. bei der Zertifizierung der auf dem Framework aufbauenden Produkte helfen kann, und dass auch Compliance-Aspekte diskutiert werden, dass die technische Umsetzung z. B. mittels Monitoring-, Logging- und Auditingmechanismen aber nicht behandelt wird.

Obwohl bereits eine praktisch eingesetzte Implementierung vorliegt, werden wie auch aus der Bewertung in Abbildung 4.21 ersichtlich viele Aspekte der Umsetzung und des Managements im laufenden Betrieb nicht erörtert. Insgesamt sind deshalb sowohl eine breitere technische Basis als auch eine prozessorientierte Einbettung in E-Health-Umgebungen wünschenswert.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**1**	1
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**1**	4
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		33

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**1**	2
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**1**	1
Summe SF-MGMT	51		5

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**1**	2
SF-INT-Modularität	2	**0**	0
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**2**	2
SF-INT-Skalierbarkeit	4	**0**	0
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		8

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**3**	6
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		48

Bewertungszahlen:			
		SF-FUNK:	1,57
		SF-INT:	0,28
		SF-MGMT:	0,10
Gesamt:	**0,99**	SF-DOKU:	2,00

Abbildung 4.22.: Nutzwertanalyse des general framework for robust watermarking security ([BBF03])

Frameworkkategorie:	IT-Dienst	Referenz: [BBF03]
Frameworkname:	A general framework for robust watermarking security	
Frameworkautoren:	Barni, M.; Bartolini, F.; Furon, T.	

Das 2003 entstandene Security-Framework konzentriert sich auf den Einsatz von Wasserzeichen insbesondere in digitalem Bild- und Videomaterial. Es zeichnet sich durch ein umfassendes Angreifermodell aus, das verschiedene kryptoanalytische Methoden seitens der Angreifer vorsieht. Als Beispiel wird die Anwendung im Kopierschutz digitaler Medien erläutert.

Die Bewertung des Security-Frameworks ist in Abbildung 4.22 zusammengefasst. Sie verdeutlicht, dass die Stärken der untersuchten Arbeit bei der Technik und Dokumentation liegen. Durch die Fokussierung auf die Watermarking-Algorithmen wird auf betriebliche Aspekte wie die Umsetzung für und das Management in eigenen Szenarien überwiegend nicht und in den anderen Teilen nur sehr oberflächlich eingegangen. Bei der Weiterentwicklung sollte deshalb erheblich stärker auf die praktische Anwendung eingegangen werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**0**	0
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**1**	4
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**1**	2
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		32

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**1**	2
SF-MGMT-Compliance	4	**3**	12
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**1**	2
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**3**	6
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**3**	12
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**1**	1
SF-MGMT-Verbesserung	4	**1**	4
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		51

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**2**	4
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**1**	2
SF-INT-Kompatibilität	2	**1**	2
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**0**	0
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		25

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**1**	1
SF-DOKU-Checkliste	1	**2**	2
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**3**	3
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**1**	2
SF-DOKU-Voraussetzungen	4	**3**	12
SF-DOKU-Zertifizierung	1	**2**	2
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**3**	3
Summe SF-DOKU	24		51

Bewertungszahlen:		SF-FUNK:	1,52
		SF-INT:	0,86
		SF-MGMT:	1,00
Gesamt:	**1,38**	SF-DOKU:	2,13

Abbildung 4.23.: Nutzwertanalyse des new security framework for HIPAA-compliant health information systems ([TC03])

Frameworkkategorie:	IT-Dienst	Referenz: [TC03]
Frameworkname:	A new security framework for HIPAA-compliant health information systems	
Frameworkautoren:	Tulu, B.; Chatterjee, S.	

Das Security-Framework für Health Information Systems orientiert sich an den US-amerikanischen Vorgaben, die 1996 im Rahmen des Health Insurance Portability and Accountability Act (HIPAA) verabschiedet wurden. Es geht auf die Notwendigkeit der Aufstellung von Sicherheitsrichtlinien ein und stellt acht Schritte zur Einführung des Frameworks vor, die jedoch ausführlicher beschrieben werden sollten. Im Unterschied zu den meisten anderen hier analysierten Arbeiten geht das Frameworkkonzept explizit auf den Bedarf an einem kontinuierlichen Sicherheitsverbesserungsprozess ein; auch die Schnittstellen zu anderen Prozessen werden gut erläutert. In Teilen ist die Frameworkdokumentation auch als Checkliste zur Umsetzung geeignet.

Abbildung 4.23 zeigt die Zusammenfassung der Bewertung des 2003 veröffentlichten Security-Frameworks. Sie verdeutlicht einerseits den Bedarf an einer konkreteren Darstellung der technischen Aspekte; hier sollten insbesondere die abgedeckten Assets und die konkreten Angriffe und Gegenmaßnahmen ausführlicher behandelt werden. Andererseits sollten auch die Abläufe im operativen Betrieb, u. a. mit Bezug auf die durch den Frameworkeinsatz erzielten Verbesserungen, umfassender dargestellt werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		45

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**1**	2
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**2**	4
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**3**	12
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**3**	6
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**1**	4
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		44

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**2**	4
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**3**	6
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		47

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**1**	2
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		32

Bewertungszahlen:		SF-FUNK:	2,14
		SF-INT:	1,62
		SF-MGMT:	0,86
Gesamt:	**1,49**	SF-DOKU:	1,33

Abbildung 4.24.: Nutzwertanalyse des policy-based security framework for Web-enabled applications ([VCS03])

Frameworkkategorie:	IT-Dienst	Referenz: [VCS03]
Frameworkname:	A policy-based security framework for Web-enabled applications	
Frameworkautoren:	Ventuneac, M.; Coffey, T.; Salomie, I.	

Das Security-Framework für web-basierte Anwendungen wurde 2003 veröffentlicht; es verfolgt einen konsequent policyorientierten Ansatz und zielt auf eine Abdeckung der Bereiche Access Control, Security Management, Identity Management und Accounting ab. Der modulare Aufbau und die Workflows sowie die administrativen Operationen werden gut erläutert; auch die Erweiterbarkeit und Skalierbarkeit werden explizit behandelt. Für das Auditing ist ein explizit ereignisgesteuerter Lösungsweg vorgesehen, der ansatzweise auch in Richtung eines Berichtswesens ausgearbeitet wurde.

Die Bewertung dieses Security-Frameworks ist in Abbildung 4.24 zusammengefasst. Wünschenswert für eine Weiterentwicklung ist einerseits, dass die Designkriterien über eine Auflistung verwandter Arbeiten hinausgehend offengelegt werden, so dass z. B. auch die konkrete Maßnahmenauswahl besser nachvollzogen werden kann; in einigen Teilbereichen wie dem Identity Management sollte darüber hinaus eine stärkere Orientierung an etablierten Standards in Erwägung gezogen werden. Zahlreiche in der Kategorie SF-MGMT nicht erfüllte Anforderungen machen ferner deutlich, dass über die reine Technik hinaus noch verstärkt auf die Einbettung der mit dem Framework geschützten Web-Anwendungen in Managementsysteme und ITSM-Prozesse eingegangen werden sollte.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**1**	4
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		26

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**1**	4
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**1**	2
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**3**	6
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**1**	2
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		26

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**2**	4
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**2**	4
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**2**	4
SF-INT-Kompatibilität	2	**1**	2
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**0**	0
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		41

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**1**	1
SF-DOKU-Designentscheid.	2	**0**	0
SF-DOKU-Kontinuum	1	**2**	2
SF-DOKU-Lifecyclephasen	1	**2**	2
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**1**	1
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**3**	3
Summe SF-DOKU	24		33

Bewertungszahlen:		SF-FUNK:	1,24
		SF-INT:	1,41
		SF-MGMT:	0,51
Gesamt:	**1,13**	SF-DOKU:	1,38

Abbildung 4.25.: Nutzwertanalyse des security framework for an ERP system ([ML05])

Frameworkkategorie:	IT-Dienst	Referenz: [ML05]
Frameworkname:	A security framework for an ERP system	
Frameworkautoren:	Marnewick, C.; Labuschagne, L.	

Das an der Universität von Johannesburg entstandene, 2005 veröffentlichte Security-Framework für Enterprise Resource Planning Systeme ist eine der wenigen hier analysierten Arbeiten, die Policies nicht nur als technische Regelwerke einsetzen, sondern auch auf die Zusammenhänge mit organisatorischen Richtlinien auf Managementebene eingehen. Darüber hinaus werden diverse Fragestellungen rund um den Aufbau und die Inbetriebnahme des Systems, die sich auch zwangsweise bei der Übertragung auf eigene Szenarien ergeben, diskutiert.

Demgegenüber wird dieses Security-Framework bei der Auswahl technischer Maßnahmen nur wenig konkret; auch eine Betrachtung der Schnittstellen zu anderen Systemen, die im ERP-Umfeld offensichtlich essentiell sind, fehlt bislang. Neben entsprechenden Erweiterungen ist es für weitere Versionen dieses Frameworks wünschenswert, dass einige bereits angerissene Themen konsequenter fortgeführt werden: Beispielsweise wird zwar ein Überblick über relevante Standards gegeben, im Hinblick auf potentielle Zertifizierungen wird aber nicht darauf eingegangen, wie sich die vorgeschlagene Lösung diesen Standards gegenüber positioniert. Die Ergebnisse der Bewertung sind in Abbildung 4.25 zusammengefasst.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**1**	4
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		44

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		25

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**1**	2
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		39

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		38

Bewertungszahlen:			
		SF-FUNK:	2,10
		SF-INT:	1,34
		SF-MGMT:	0,49
Gesamt:	**1,38**	SF-DOKU:	1,58

Abbildung 4.26.: Nutzwertanalyse des Security Framework for Collaborative Distributed System Control at the Device-Level ([XKW+03])

Frameworkkategorie:	IT-Dienst	Referenz: [XKW+03]
Frameworkname:	A Security Framework for Collaborative Distributed System Control at the Device-Level	
Frameworkautoren:	Xu, Y.; Korba, L.; Wang, L.; Hao, Q.; Shen, W.; Lang, S.	

Das 2003 veröffentlichte Security-Framework thematisiert die exponierte Rolle von Zugangsgeräten zu verteilten Systemen und deren Administration. Im Rahmen der im Frameworkkonzept beschriebenen Anforderungsanalyse lehnt es sich explizit an mehrere für das Umfeld relevante Standards an. Als Maßnahmen zur Absicherung werden unter anderem Policies eingesetzt, die jedoch vorrangig als technisches Instrument fungieren; bei einer Weiterentwicklung sollte der Zusammenhang mit organisationsweiten Richtlinien stärker herausgearbeitet werden. Allgemein ist das Security-Framework, wie auch die in Abbildung 4.26 zusammengefasste Abbildung zeigt, bislang stark technisch ausgerichtet und geht nur unvollständig auf die übergeordneten Managementabläufe ein. Ferner sollten die relevanten Angreifermodelle und die vom Framework berücksichtigten Schwachstellen und Angriffe näher erläutert werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**2**	4
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		57

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**1**	4
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**1**	4
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**3**	6
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**2**	4
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		42

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**2**	8
SF-INT-Einführung	2	**2**	4
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**2**	4
SF-INT-Kompatibilität	2	**1**	2
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**2**	4
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		37

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**3**	6
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**3**	3
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**3**	6
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		49

Bewertungszahlen:			
		SF-FUNK:	2,71
		SF-INT:	1,28
		SF-MGMT:	0,82
Gesamt:	**1,71**	SF-DOKU:	2,04

Abbildung 4.27.: Nutzwertanalyse des security framework for mobile-to-mobile payment network ([DSG05])

Frameworkkategorie:	IT-Dienst	Referenz: [DSG05]
Frameworkname:	A security framework for mobile-to-mobile payment network	
Frameworkautoren:	Das, M. L.; Saxena, A.; Gulati, V. P.	

Das 2005 entstandene Security-Framework wendet sich implizit an Systemarchitekten und befasst sich mit der Nutzung mobiler Endgeräte zur bargeldlosen Zahlung; durch die Ein- und Ausgabemöglichkeiten, die z. B. Mobiltelefone bieten, kann ein besserer Schutz gegen Missbrauchsvarianten, die z. B. von Kreditkarten bekannt sind, erreicht werden. Das Security-Framework gibt hierzu einen festen, grundlegenden Ablauf vor, der z. B. durch die Wahl eines konkreten Authentifizierungsverfahren (beispielsweise PIN-Eingabe) angepasst werden kann. Da sie in vielen anderen Frameworkkonzepten fehlt, fällt die Selbsteinschätzung der mit dem Frameworkeinsatz erreichten Verbesserungen positiv auf. Wünschenswert ist jedoch ein noch stärkeres Eingehen auf organisatorische Maßnahmen und Managementaspekte sowie eine Einschätzung des Aufwands zur praktischen Umsetzung, der aufgrund notwendiger Anpassungen sowohl bei mobilen Geräten als auch bei den Händlerinfrastrukturen, die das vorgeschlagene Zahlungsverfahren unterstützen wollen, relativ hoch ausfallen dürfte. Abbildung 4.27 fasst die Bewertung zusammen.

Frameworkkategorie:	IT-Dienst	Referenz: [SLJ+07]
Frameworkname:	A software framework for autonomic security in pervasive environments	
Frameworkautoren:	Saxena, A.; Lacoste, M.; Jarboui, T.; Lucking, U.; Steinke, B.	

Das in einer Kooperation zwischen der France Télécom und dem Nokia Research Center entstandene und 2007 als 18 Seiten umfassender Konferenzbeitrag veröffentlichte Security-Framework erläutert die Einbettung einzelner, autonomer, abgesicherter Systeme, die dem *Sensor-Analyzer-Responder*-Modell folgen, in *pervasive computing* Architekturen. Wie für autonome Systeme charakteristisch liegt einer der Schwerpunkte auf der möglichst weitgehenden Automatisierung der zur Erhaltung der IT-Sicherheit relevanten Vorgänge. Das Security-Framework liefert sowohl eine für Nokia-Systeme spezifische Implementierung als auch eine wiederverwendbare Programmierschnittstelle.

Bei der Arbeit, deren Beurteilung in Abbildung 4.28 zusammengefasst ist, fällt positiv auf, dass im Unterschied zu den meisten anderen hier betrachteten Arbeiten die Bedeutung des Begriffs Security-Framework aus Sicht der Autoren knapp beschrieben wird. Auch die angewandten Designkriterien und die getroffenen Designentscheidungen werden ausführlich dargestellt. Darüber hinaus wird sowohl auf die Herausforderungen bei der Quantifizierung der erreichten IT-Sicherheit als auch auf die mit der Umsetzung verbundenen Kosten eingegangen, wenngleich diesbezüglich keine belastbaren Ergebnisse geliefert werden. Für die Weiterentwicklung ist wünschenswert, dass noch stärker auf konkrete Anwendungsgebiete und die relevanten Managementschnittstellen eingegangen wird; auch die Beschreibungen der Anpassung an eigene Szenarien und der stufenweisen Umsetzung sind noch ausbaufähig.

Frameworkkategorie:	IT-Dienst	Referenz: [AJ03]
Frameworkname:	A Unified Security Framework for Networked Applications	
Frameworkautoren:	Abendroth, J.; Jensen, Ch. D.	

Das Security-Framework thematisiert als Schwerpunkt die Zugriffssteuerung für netzbasierte Dienste. Durch sein auf Client-/Server-Kommunikation ausgelegtes vierstufiges Schichtenmodell erreicht es eine hohe Flexibilität; allerdings wird der explizit vorgesehene Customizing-Prozess nur sehr knapp skizziert, so dass die Übertragbarkeit auf eigene Szenarien nicht unmittelbar gegeben ist. An vielen Stellen der 2003 veröffentlichten Frameworkdokumentation wird deutlich, dass der Forschungsschwerpunkt der Autoren das Software Engineering ist, so dass die Einordnung der hier untersuchten Arbeit im Grenzbereich zwischen Software-Engineering- und IT-Dienst-Security-Frameworks liegt. Wie die in Abbildung 4.29 zusammengefasste Bewertung zeigt, verfolgt das Security-Framework einen durchaus prozessorientierten Ansatz; allerdings sind die Management-Schnittstellen durchaus noch ausbaufähig, da zwar beispielsweise technische Policies zur Entscheidung über erlaubte Benutzerzugriffe eingesetzt werden, aber auf den Zusammenhang mit unternehmensweiten Richtlinien nur unzureichend eingegangen wird. Bei einer Weiterentwicklung sollte zudem über die bislang rein präventive Ausrichtung des Security-Frameworks z. B. auf Detektions- und Auditmechanismen eingegangen werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**3**	6
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		43

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**2**	4
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**1**	2
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**1**	2
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		42

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		45

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**2**	2
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		40

Bewertungszahlen:		SF-FUNK:	2,05
		SF-INT:	1,55
		SF-MGMT:	0,82
Gesamt:	**1,52**	SF-DOKU:	1,67

Abbildung 4.28.: Nutzwertanalyse des software framework for autonomic security in pervasive environments ([SLJ+07])

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		26

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**1**	2
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		34

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		35

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**1**	1
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**1**	2
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		39

Bewertungszahlen:		SF-FUNK:	1,24
		SF-INT:	1,21
		SF-MGMT:	0,67
Gesamt:	**1,18**	SF-DOKU:	1,63

Abbildung 4.29.: Nutzwertanalyse des Unified Security Framework for Networked Applications ([AJ03])

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		32

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**1**	2
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		40

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		49

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**1**	1
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		35

Bewertungszahlen:			
		SF-FUNK:	1,52
		SF-INT:	1,69
		SF-MGMT:	0,78
Gesamt:	**1,36**	SF-DOKU:	1,46

Abbildung 4.30.: Nutzwertanalyse des Integrated Security Framework for XML based Management ([CSF05])

Frameworkkategorie:	IT-Dienst	Referenz: [CSF05]
Frameworkname:	An Integrated Security Framework for XML based Management	
Frameworkautoren:	Cridlig, V.; State, R.; Festor, O.	

Das Security-Framework von Cridlig, State und Festor behandelt die rollenbasierte Zugriffssteuerung für Netz- und Systemmanagementsysteme mittels XML-basierter Policies. Die in Abbildung 4.30 zusammengefasste Bewertung der 2005 veröffentlichten Arbeit zeigt, dass zwar bereits auf viele technische Aspekte und auch umfassend auf die Integrations- und Betriebsanforderungen eingegangen wird, dass die Schnittstellen zu den organisatorischen Managementprozessen und -abläufen, die über das Netz- und Systemmanagementsystem selbst hinausgehen, aber noch stärker ausgearbeitet werden sollten.

Auf technischer Ebene ist für die Weiterentwicklung darüber hinaus wünschenswert, dass über die bislang rein präventive Ausrichtung des Security-Frameworks auch auf die Erkennung bzw. das Auditing und mögliche Reaktionen eingegangen wird und dass die angekündigten Performancemessungen durchgeführt werden. Im Einklang mit der bereits starken Orientierung an existierenden Standards sollte auch eine Beurteilung der Vollständigkeit der Lösung und deren Rolle im Kontext von Zertifizierungen dokumentiert werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**1**	2
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		46

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**3**	6
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**1**	2
SF-MGMT-Support	1	**2**	2
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		48

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**3**	6
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		45

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**3**	12
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		42

Bewertungszahlen:		SF-FUNK:	2,19
		SF-INT:	1,55
		SF-MGMT:	0,94
Gesamt:	**1,61**	SF-DOKU:	1,75

Abbildung 4.31.: Nutzwertanalyse von iSecurity: A Security Framework for Interactive Workspaces ([STL+03])

Frameworkkategorie:	IT-Dienst	Referenz: [STL+03]
Frameworkname:	iSecurity: A Security Framework for Interactive Workspaces	
Frameworkautoren:	Song, Y. J.; Tobagus, W.; Leong, D. Y.; Johanson, B.; Fox, A.	

Das 2003 veröffentlichte Security-Framework ist für Installationen von *Interactive Workspaces* konzipiert; dabei handelt es sich um eine Ubiquitous-Computing-Umgebung derselben Autoren. Im Unterschied zu den meisten anderen hier analysierten Arbeiten geht dieses Framework explizit auf das Thema Benutzerfreundlichkeit ein und erläutert den Einsatz geeigneter graphischer Bedienoberflächen. Eine weitere Stärke liegt in der Implementierung, die auch in der Praxis erfolgreich eingesetzt wird.

Abbildung 4.31 fasst die Bewertung des Security-Frameworks zusammen und reflektiert, dass eine weitere Verbesserung beispielsweise noch durch eine Einbettung der Abläufe in die über das unmittelbare, technische Management der eingesetzten Komponenten hinaus relevanten Prozesse erzielt werden kann. Ebenso sollte analysiert werden, wie sich der Einsatz des Security-Frameworks auf das Sicherheitsniveau auswirkt und in welchem Verhältnis es zum zur Umsetzung notwendigen Aufwand steht.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**1**	4
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**3**	6
Summe SF-FUNK	21		43

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**3**	6
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**3**	6
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**3**	3
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**3**	12
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		49

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**2**	4
SF-INT-Erweiterung	2	**3**	6
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**3**	12
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		57

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**1**	2
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**3**	3
SF-DOKU-Lifecyclephasen	1	**1**	1
SF-DOKU-Vollständigkeit	2	**2**	4
SF-DOKU-Voraussetzungen	4	**3**	12
SF-DOKU-Zertifizierung	1	**1**	1
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**3**	3
Summe SF-DOKU	24		58

Bewertungszahlen:			
		SF-FUNK:	2,05
		SF-INT:	1,97
		SF-MGMT:	0,96
Gesamt:	**1,85**	SF-DOKU:	2,42

Abbildung 4.32.: Nutzwertanalyse von Linux Security Modules: General Security Support for the Linux Kernel ([WCS+02])

Frameworkkategorie:	IT-Dienst	Referenz: [WCS+02]
Frameworkname:	Linux Security Modules: General Security Support for the Linux Kernel	
Frameworkautoren:	Wright, C.; Cowan, C.; Smalley, S.; Morris, J.; Kroah-Hartman, G.	

Die 2002 veröffentlichte Arbeit beschreibt die im Linux-Kernel enthaltenen Sicherheitsfunktionen, die von beliebigen Linux-Anwendungen genutzt werden können; der Schwerpunkt liegt dabei auf dem Thema Zugriffssteuerung. Durch die kontinuierliche Weiterentwicklung des Linux-Kernels und der von ihm bereitgestellten Sicherheitsfunktionalität handelt es sich um ein gutes Beispiel für ein Security-Framework, das nicht nur implementiert ist, sondern auch einem expliziten Releasezyklus unterliegt und für das Supportdienstleistungen bedarfsorientiert abgerufen werden können. Zudem geht das Frameworkkonzept explizit auf typische Schwachstellen und Angriffe in Bezug auf das Zusammenspiel von Anwendungen und Kernel-Funktionen ein. Ebenso sind Maßnahmen für das reibungslose Zusammenspiel mit weiteren Access-Control-Frameworks explizit vorgesehen. Die Bewertung ist in Abbildung 4.32 zusammengefasst und zeigt, dass eine weitere Verbesserung insbesondere durch eine explizite Diskussion der zum Betrieb relevanten Managementabläufe erreicht werden könnte.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**1**	4
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**1**	4
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		29

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**1**	4
SF-MGMT-Delegation	2	**1**	2
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**1**	2
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		23

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**2**	8
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**0**	0
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**0**	0
SF-INT-Usablility	2	**2**	4
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		20

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**1**	2
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**1**	4
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		32

Bewertungszahlen:		SF-FUNK:	1,38
		SF-INT:	0,69
		SF-MGMT:	0,45
Gesamt:	**0,96**	SF-DOKU:	1,33

Abbildung 4.33.: Nutzwertanalyse des Location-based security framework for use of handheld devices in medical information systems ([HO06])

Frameworkkategorie:	IT-Dienst	Referenz: [HO06]
Frameworkname:	Location-based security framework for use of handheld devices in medical information systems	
Frameworkautoren:	Hansen, F.; Oleshchuk, V.	

Bei dem 2006 veröffentlichten Security-Framework, das die Nutzung mobiler Geräte zum Zugriff auf Patienteninformationen durch Ärzte thematisiert, handelt es sich im Wesentlichen um eine auf dieses Umfeld ausgelegte Erweiterung der klassischen rollenbasierten Zugriffssteuerung (RBAC), bei der der aktuelle Standort des Anwenders bei der Entscheidung über die Zugriffserlaubnis berücksichtigt wird. Somit wird ein wichtiger Lösungsbaustein für medizinische Informationssysteme vorgestellt, der die Gesamtproblematik jedoch nicht alleine lösen kann, so dass es wie in Abbildung 4.33 dargestellt bereits bezüglich der sicherheitsfunktionalen Anforderungen zu Abwertungen kommt. Ferner werden viele einführungs- und betriebsrelevante Aspekte trotz der Verwendung von Beispielen nicht oder nur knapp erläutert, so dass die Frameworkdokumentation im Hinblick auf die Anwendung in eigenen Szenarien überarbeitet werden sollte.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**3**	6
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		50

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**1**	2
SF-MGMT-Compliance	4	**2**	8
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**1**	4
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**3**	6
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**3**	3
SF-MGMT-Tests	1	**1**	1
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		58

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**2**	4
SF-INT-Customizing	4	**2**	8
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**1**	2
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**3**	12
SF-INT-Polyinstanziierbark.	1	**1**	1
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		59

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**1**	1
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**2**	2
SF-DOKU-Lifecyclephasen	1	**1**	1
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		36

Bewertungszahlen:		SF-FUNK:	2,38
		SF-INT:	2,03
		SF-MGMT:	1,14
Gesamt:	**1,76**	SF-DOKU:	1,50

Abbildung 4.34.: Nutzwertanalyse der Performance Analysis of Unified Enterprise Application Security Framework ([SSA05])

Frameworkkategorie:	IT-Dienst	Referenz: [SSA05]
Frameworkname:	Performance Analysis of Unified Enterprise Application Security Framework	
Frameworkautoren:	Shaikh, R. A.; Sharif, K.; Ahmed, E.	

Die hier analysierte Arbeit verknüpft das auf Seite 241 diskutierte *unified security framework* und die Vorarbeiten *application defense: next generation of unified enterprise security* [RH03] bzw. *modular approach for unified enterprise application security* [SZS04] mit einer prototypischen praktischen Umsetzung, deren Skalierbarkeit und Performanz untersucht werden. Dabei werden die wesentlichen Eckpunkte des architekturbezogenen Security-Frameworks rekapituliert und im Rahmen der Abbildung auf einen Beispieldienst konkretisiert sowie punktuell erweitert. Das Resultat ist somit nicht nur ein dienstbezogenes Security-Framework, sondern auch ein gelungenes Beispiel dafür, wie auf höherem Abstraktionsniveau spezifizierte Frameworks für IT-Architekturen auf die an diesen beteiligten einzelnen Dienste übertragen werden können. Die Arbeit sieht eine Querverbindung zum Incident Management zur Bearbeitung von Sicherheitsvorfällen vor und könnte insbesondere durch den Ausbau der ITSM-Schnittstellen und damit verbundener Aspekte wie dem Einsatz von Metriken und einer stärkeren Betonung des Prozesscharakters noch weiter verbessert werden. Die Bewertung ist in Abbildung 4.34 zusammengefasst.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**0**	0
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**1**	4
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**1**	2
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		24

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**2**	4
SF-MGMT-Support	1	**3**	3
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**3**	12
SF-MGMT-Zuständigkeiten	1	**1**	1
Summe SF-MGMT	51		34

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**0**	0
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**0**	0
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**1**	2
Summe SF-INT	29		12

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**1**	2
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**0**	0
SF-DOKU-Kontinuum	1	**2**	2
SF-DOKU-Lifecyclephasen	1	**2**	2
SF-DOKU-Vollständigkeit	2	**1**	2
SF-DOKU-Voraussetzungen	4	**0**	0
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**1**	4
SF-DOKU-Zielgruppe	1	**1**	1
Summe SF-DOKU	24		21

Bewertungszahlen:		SF-FUNK:	1,14
		SF-INT:	0,41
		SF-MGMT:	0,67
Gesamt:	**0,77**	SF-DOKU:	0,88

Abbildung 4.35.: Nutzwertanalyse des PITMA Security-Frameworks ([PIT08])

Frameworkkategorie:	IT-Dienst	Referenz: [PIT08]
Frameworkname:	PITMA Security Framework – Policy, Implementation, Training, Maintenance and Auditing	
Frameworkautor:	PITMA	

Das 2008 beschriebene PITMA Security-Framework beschreibt ein Vorgehensmodell bei der Absicherung von netzbasierten Diensten. Analog zum auf Seite 241 beschriebenen *universal security framework* handelt es sich bei [PIT08] um eine äußerst knappe Vorstellung des Security-Frameworks, zu dessen konkreter Umsetzung die Beratungsdienstleistungen des hinter den Autoren stehenden Unternehmens erworben werden können. Das Security-Framework wird hier betrachtet, da es neben verschiedenen technischen Komponenten zur Prävention und Detektion sicherheitsrelevanter Vorfälle auch explizit auf Schulungs- und Auditaspekte eingeht. Die zu PITMA frei verfügbare Literatur fällt jedoch äußerst knapp aus, so dass sich die meisten der in Abbildung 4.35 festgehaltenen Abwertungen dadurch ergeben, dass die entsprechenden Punkte nicht explizit oder nur sehr oberflächlich erwähnt werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**1**	4
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**3**	6
Summe SF-FUNK	21		41

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**1**	2
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		14

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**0**	0
SF-INT-Modularität	2	**0**	0
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		15

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**3**	6
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		44

Bewertungszahlen:			
		SF-FUNK:	1,95
		SF-INT:	0,52
		SF-MGMT:	0,27
Gesamt:	**1,14**	SF-DOKU:	1,83

Abbildung 4.36.: Nutzwertanalyse der Scalable multicast security with dynamic recipient groups ([MP00])

Frameworkkategorie:	IT-Dienst	Referenz: [MP00]
Frameworkname:	Scalable multicast security with dynamic recipient groups	
Frameworkautoren:	Molva, R.; Pannetrat, A.	

Der im Jahr 2000 erschienene Journalartikel bezeichnet sich selbst als *framework for multicast security* und zielt auf die Absicherung der Kommunikation mit den Empfängern von Multicast-Nachrichten und das Management dynamischer großer Empfängergruppen ab. Hierzu wird ein Angreifermodell präsentiert, das neben seiner Ausführlichkeit insbesondere auch durch seine gute Formalisierung besticht.

Wie auch in der Bewertung in Abbildung 4.36 deutlich wird, ist das Framework jedoch äußerst technisch ausgerichtet; es präsentiert den Lösungsansatz umfassend, geht jedoch nicht auf seine konkrete Anwendung ein. Von einer weiterführenden Aufbereitung der Konzepte in Hinblick auf die szenarienspezifische Umsetzung und den praktischen Einsatz würden weitere Versionen des Frameworks deshalb stark profitieren.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**0**	0
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		32

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		8

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**3**	6
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**0**	0
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		31

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		28

Bewertungszahlen:		SF-FUNK:	1,52
		SF-INT:	1,07
		SF-MGMT:	0,16
Gesamt:	**0,98**	SF-DOKU:	1,17

Abbildung 4.37.: Nutzwertanalyse von SecureTorrent: A Security Framework for File Swarming ([WM06])

Frameworkkategorie:	IT-Dienst	Referenz: [WM06]
Frameworkname:	SecureTorrent: A Security Framework for File Swarming	
Frameworkautoren:	Wilson, K.; Machanick, P.	

Das 2006 entwickelte Security-Framework stellt Konzepte zur Zugriffskontrolle, Vertraulichkeitssicherung und Auditierbarkeit für den Peer-to-Peer-Dateitransfer mittels Bittorrent vor. Den Schwerpunkt bilden dabei der Einsatz von Verschlüsselungsmechanismen und die damit verbundenen Auswirkungen auf die Performance. Wie die in Abbildung 4.37 zusammengefasste Bewertung zeigt, ist das gesamte Frameworkkonzept auf wenige, aber durchaus zentrale technische und integrationsspezifische Teilaspekte fokussiert. Eine Weiterentwicklung des Security-Frameworks sollte deshalb insbesondere stärker auf die praktische Anwendung der bereits vorhandenen Implementierung eingehen und trotz des dezentralen Peer-to-Peer-Ansatzes auch mindestens auf Managementaspekte wie die erforderlichen Administrationskonzepte eingehen.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**2**	4
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**3**	6
Summe SF-FUNK	21		51

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**1**	2
SF-MGMT-Compliance	4	**1**	4
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**2**	4
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**2**	4
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		51

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**1**	4
SF-INT-Usablility	2	**3**	6
SF-INT-Wiederverwend.	2	**1**	2
Summe SF-INT	29		33

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**1**	2
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**3**	3
Summe SF-DOKU	24		43

Bewertungszahlen:		SF-FUNK:	2,43
		SF-INT:	1,14
		SF-MGMT:	1,00
Gesamt:	**1,59**	SF-DOKU:	1,79

Abbildung 4.38.: Nutzwertanalyse von Security for Internet banking: a framework ([HW03])

Frameworkkategorie:	IT-Dienst	Referenz: [HW03]
Frameworkname:	Security for Internet banking: a framework	
Frameworkautoren:	Hutchinson, D.; Warren, M.	

Das 2003 veröffentlichte Security-Framework, dessen Bewertung in Abbildung 4.38 zusammengefasst ist, thematisiert die Sicherheit von Finanztransaktionen, die über Webseiten angestoßen werden, und unterscheidet zwischen verschiedenen Anwenderkategorien wie Privat- und Firmenkunden. Dabei wird sowohl auf die unterschiedlichen Anforderungen als auch auf das Thema Benutzerfreundlichkeit umfassend eingegangen. Die somit zugrunde gelegten Gestaltungskriterien und die getroffenen Designentscheidungen werden ausführlich dargelegt; auch die wesentlichen im Betrieb relevanten Abläufe werden diskutiert.

Bei einer Weiterentwicklung des Security-Frameworks sollten zum einen neben dem aktuellen Schwerpunktthema Authentifizierung auch die anderen sicherheitsrelevanten Problembereiche, die bislang nur am Rande thematisiert werden, umfassender erläutert werden. Zum anderen wird zwar die Notwendigkeit von Schulungen in bestimmten Bereichen diskutiert; diese sollte aber um die Angabe konkreter Inhalte für die jeweiligen Bereiche ergänzt werden. Wünschenswert sind darüber hinaus eine Beschreibung der praktischen Umsetzung, die über die bislang fiktiven Beispiele hinausgeht, und eine Einbettung der sicherheitsspezifischen Abläufe in den größeren Kontext des Internet-Bankings.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		29

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**2**	4
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		18

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**0**	0
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		24

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**0**	0
Summe SF-DOKU	24		28

Bewertungszahlen:			
		SF-FUNK:	1,38
		SF-INT:	0,83
		SF-MGMT:	0,35
Gesamt:	**0,93**	SF-DOKU:	1,17

Abbildung 4.39.: Nutzwertanalyse des Security Framework for DPWS Compliant Devices ([HLP+09])

Frameworkkategorie:	IT-Dienst	Referenz: [HLP+09]
Frameworkname:	Security Framework for DPWS Compliant Devices	
Frameworkautoren:	Hernández, V.; López, L.; Prieto, O.; Martínez, J.-F.; García, A.-B.; Da-Silva, A.	

Das 2009 veröffentlichte Security-Framework zielt auf die nahtlose Integration von Geräten, die die *Device Profile for Web Services* (DPWS) Spezifikationen erfüllen, in service-orientierte Architekturen unter Berücksichtigung von IT-Sicherheitsanforderungen ab. Der Schwerpunkt liegt dabei deutlich auf dem Zusammenspiel verschiedener kryptographischer Mechanismen und den damit verbundenen administrativen Abläufen.

Wie die in Abbildung 4.39 zusammengefasste Bewertung zeigt, ist für die Weiterentwicklung wünschenswert, dass die Übertragbarkeit der Konzepte auf eigene Szenarien noch stärker herausgearbeitet und auf die Einbettung in Managementkonzepte eingegangen wird. Auch die technischen Komponenten sollten um Monitoring- und Auditfunktionalität ergänzt werden. Insgesamt wird zwar bereits eine Reihe wichtiger Eigenschaften und Abläufe angesprochen; die Darstellung sollte an vielen Stellen aber noch expliziter und ausführlicher werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**3**	6
Summe SF-FUNK	21		45

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**2**	2
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**2**	8
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**3**	6
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**3**	6
SF-MGMT-Support	1	**3**	3
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		51

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**3**	6
SF-INT-Customizing	4	**2**	8
SF-INT-Einführung	2	**2**	4
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**1**	2
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**2**	2
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**3**	6
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		58

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**2**	4
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**3**	3
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**2**	4
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**3**	3
Summe SF-DOKU	24		48

Bewertungszahlen:		SF-FUNK:	2,14
		SF-INT:	2,00
		SF-MGMT:	1,00
Gesamt:	**1,79**	SF-DOKU:	2,00

Abbildung 4.40.: Nutzwertanalyse des Security Framework for IP Telephony ([Dad02])

Frameworkkategorie:	IT-Dienst	Referenz: [Dad02]
Frameworkname:	Security Framework for IP Telephony	
Frameworkautor:	Dadoun, N.	

Die Verfügbarkeit und die Vertraulichkeit bei der Kommunikation über Voice-over-IP sind die beiden Primärziele des 2002 entstandenen Security-Frameworks, dessen Dokumentation sich auch an VoIP-Anwender richtet und diese analog zu den VoIP-Infrastrukturbetreibern für die spezifischen Sicherheitsprobleme sensibilisieren soll. In der Beschreibung wird ausführlich auf typische Schwachstellen und spezifische Angriffsarten sowie auf verschiedene, zum Teil miteinander kombinierbare Lösungsansätze, deren Vor- und Nachteile diskutiert werden, eingegangen. Positiv fällt ferner ein wenngleich grobes Beurteilungsschema auf, mit dessen Hilfe das Sicherheitsniveau in Abhängigkeit von der Umsetzung der vorgeschlagenen Maßnahmen quantifiziert werden kann. Wie die Bewertung in Abbildung 4.40 reflektiert, bewegt sich das Security-Framework dennoch überwiegend auf der technischen Ebene. Somit werden beispielsweise die Aufgaben des Sicherheitsmanagements, notwendige oder empfehlenswerte Maßnahmen auf organisatorischer Ebene und die gezielte Vorgehensweise bei der schrittweisen Umsetzung der technischen Lösungsbausteine nicht erläutert und sollten bei einer Überarbeitung ergänzt werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**3**	6
Summe SF-FUNK	21		56

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**1**	2
SF-MGMT-Praxis	2	**3**	6
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**1**	2
SF-MGMT-Schulungen	2	**1**	2
SF-MGMT-Support	1	**2**	2
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**3**	12
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		45

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**2**	4
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**1**	4
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**2**	4
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		51

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**1**	2
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**2**	2
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**1**	2
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		44

Bewertungszahlen:		SF-FUNK:	2,67
		SF-INT:	1,76
		SF-MGMT:	0,88
Gesamt:	**1,79**	SF-DOKU:	1,83

Abbildung 4.41.: Nutzwertanalyse des Security Framework for Mobile Applications ([Pet08])

Frameworkkategorie:	IT-Dienst	Referenz: [Pet08]
Frameworkname:	Security Framework for Mobile Applications	
Frameworkautor:	Petersen, N. M.	

Das 2008 veröffentlichte Security-Framework für mobile Anwendungen wird in mehreren wissenschaftsnahen Projekten eingesetzt und betrachtet insbesondere auch die Benutzerfreundlichkeit. Die berücksichtigten Angriffe und die getroffenen Designentscheidungen werden umfassend dargestellt; auch die Skalierbarkeit des Frameworkeinsatzes und die Performance der genutzten Komponenten werden explizit untersucht.

Die in Abbildung 4.41 zusammengefasste Bewertung reflektiert, dass bei der zukünftigen Weiterentwicklung einerseits der Customizing-Prozess noch erweitert und detaillierter beschrieben sowie eine Möglichkeit zum stufenweisen Rollout geschaffen werden sollte. Andererseits sollte auch eine Einbettung in Enterprise-Security-Management-Konzepte vorgenommen werden, da sich viele der bereits eingesetzten technischen Sicherheitsmaßnahmen wie Kerberos und PKI überwiegend im Unternehmenskontext finden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**1**	4
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		32

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**1**	2
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		19

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**2**	4
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**1**	4
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		49

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**1**	1
Summe SF-DOKU	24		27

Bewertungszahlen:		SF-FUNK:	1,52
		SF-INT:	1,69
		SF-MGMT:	0,37
Gesamt:	**1,18**	SF-DOKU:	1,13

Abbildung 4.42.: Nutzwertanalyse des Security Framework in a Virtual Large-Scale Disk System ([Ueh08])

Frameworkkategorie:	IT-Dienst	Referenz: [Ueh08]
Frameworkname:	Security Framework in a Virtual Large-Scale Disk System	
Frameworkautor:	Uehara, M.	

Das 2008 entstandene Security-Framework zielt auf die Absicherung einer Variante verteilter Dateisysteme ab, mit der die auf Client-PCs ungenutzt bleibenden Festplattenkapazitäten gebündelt und von einem Fileserver zur Verfügung gestellt werden können. Dabei wird primär auf die sich durch die Ausgangsbasis gegebenen Besonderheiten eingegangen, beispielsweise die häufig nicht durchgängige Verfügbarkeit der einzelnen Knoten und die Notwendigkeit der Datenverschlüsselung, um unerlaubte Zugriffe durch die lokalen Nutzer der Client-PCs zu unterbinden. Obwohl der Ansatz bereits in die Praxis umgesetzt wurde und auf dieser Basis auch Aspekte der Inbetriebnahme und des Betriebs beschrieben werden, ist eine ausführlichere Beschreibung zur Übertragung auf eigene Szenarien wünschenswert. Zudem wird der Dienst bislang isoliert betrachtet, so dass die auf Schnittstellen und Verfahren, beispielsweise zur Kapazitätsplanung und zur Auswirkung z. B. von Kapazitätserweiterungen auf das operative Management, erläutert werden sollten. Die Bewertung ist in Abbildung 4.42 zusammengefasst.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**2**	4
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		38

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**1**	4
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**1**	2
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		14

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**1**	2
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**1**	4
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		42

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**1**	1
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**2**	4
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		43

Bewertungszahlen:		SF-FUNK:	1,81
		SF-INT:	1,45
		SF-MGMT:	0,27
Gesamt:	**1,33**	SF-DOKU:	1,79

Abbildung 4.43.: Nutzwertanalyse des Security-Frameworks für global verteilten Anwendungen ([Rub07])

Frameworkkategorie:	IT-Dienst	Referenz: [Rub07]
Frameworkname:	Sicherheitskonzepte in global verteilten Anwendungen	
Frameworkautor:	Rubarth, Th.	

Die 2007 entstandene Master-Arbeit von Thies Rubarth entwirft ein Security-Framework für global verteilte Anwendungen, die zur Kommunikation zwischen ihren Einzelkomponenten auf Web Services setzen. Sie ist durch die Vielzahl an einzelnen Sicherheitsbausteinen im Web-Service-Umfeld motiviert und setzt sich zum Ziel, deren Zusammenspiel und Anwendung strukturiert aufzubereiten. Das Security-Framework wendet sich an Architekten, Designer, Entwickler und Technologieexperten. Sein Schwerpunkt liegt auf der policyorientierten Zusammenstellung diverser Web-Service-Security-Protokolle. Wie aus der Bewertung in Abbildung 4.43 deutlich wird, ist die Vorgehensweise sehr stark technisch bzw. sicherheitsfunktional geprägt; auf das Management der mit Hilfe des Security-Frameworks gesicherten Anwendungen wird hingegen nicht explizit eingegangen, so dass insbesondere in der Anforderungskategorie SF-MGMT erhebliches Verbesserungspotential gegeben ist. Weitere Abstriche ergeben sich durch die fehlende Prozessorientierung und die Beschränkung auf die Security-Framework-Designphase, d. h. die Adaption und Umsetzung in eigenen Szenarien werden nicht methodisch unterstützt.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**0**	0
SF-FUNK-Angriffe	2	**2**	4
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		24

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**1**	2
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		6

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**1**	2
SF-INT-Kompatibilität	2	**0**	0
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**1**	4
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		10

	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**1**	2
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**0**	0
SF-DOKU-Kontinuum	1	**1**	1
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**3**	3
Summe SF-DOKU	24		34

Bewertungszahlen:			
		SF-FUNK:	1,14
		SF-INT:	0,34
		SF-MGMT:	0,12
Gesamt:	**0,76**	SF-DOKU:	1,42

Abbildung 4.44.: Nutzwertanalyse der Study on Security Framework in E-Commerce ([TX07])

Frameworkkategorie:	IT-Dienst	Referenz: [TX07]
Frameworkname:	Study on Security Framework in E-Commerce	
Frameworkautoren:	Tao, L.; Xue, L.	

Die 2007 veröffentlichte Arbeit von Tao und Xue setzt sich zum Ziel, einen umfassenden Überblick über für den E-Commerce spezifische Sicherheitsprobleme zu geben und ein *research framework for security in e-commerce* vorzuschlagen. Entsprechend handelt es sich um Vorarbeiten, die zu einem Security-Framework führen können, aber noch nicht den Anspruch haben, ein ebensolches darzustellen.

Entsprechend zeigt auch die in Abbildung 4.44 zusammengefasst Bewertung, dass zwar bereits einige Aspekte durchaus zielführend behandelt werden, unter dem Blickwinkel der meisten Anforderungen aber noch keine konkreten Lösungen vorliegen. Eine praktische Umsetzung auf Basis der bislang vorhandenen Konzepte erscheint nicht möglich.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**0**	0
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**3**	6
Summe SF-FUNK	21		38

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**3**	6
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**1**	2
SF-MGMT-Praxis	2	**3**	6
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**1**	2
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**3**	3
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		45

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**2**	4
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		33

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**3**	6
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**3**	12
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		44

Bewertungszahlen:			
		SF-FUNK:	1,81
		SF-INT:	1,14
		SF-MGMT:	0,88
Gesamt:	**1,42**	SF-DOKU:	1,83

Abbildung 4.45.: Nutzwertanalyse von: Towards an IPv6-based security framework for distributed storage resources ([BL03])

Frameworkkategorie:	IT-Dienst	Referenz: [BL03]
Frameworkname:	Towards an IPv6-based security framework for distributed storage resources	
Frameworkautoren:	Bassi, A.; Laganier, J.	

Die untersuchte Arbeit zielt auf die Absicherung des Internet Backplane Protocols beim Aufbau verteilter Speicherdienste in IPv6-basierten Netzen ab. Sie geht gut auf die bisherigen Schwächen beim Einsatz des Protokolls und mögliche spezifische Angriffe ein. Zur Lösung wird durchgängig auf Standardkomponenten wie IPsec gesetzt.

Das Security-Framework, dessen Bewertung in Abbildung 4.45 zusammengefasst ist, bietet umfassende Autorisierungskonzepte und unterstützt dabei explizit auch Delegationsmechanismen. Eine praktische Umsetzung mit mehr als 150 beteiligten Einrichtungen erfolgte im Rahmen des US-amerikanischen Forschungsnetzes Internet2. Für die Weiterentwicklung ist zum einen wünschenswert, dass über den bislang rein präventiven Charakter des Frameworks hinaus auch Audit- und Angriffserkennungsmechanismen erarbeitet werden. Zum anderen ist das Frameworkkonzept bislang sehr techniklastig, so dass verstärkt auch die notwendigen organisatorischen Maßnahmen und die Einbettung in Managementprozesse dokumentiert werden sollten.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		31

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**3**	6
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**2**	8
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**1**	2
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**3**	3
Summe SF-MGMT	51		45

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**3**	6
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		37

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**2**	2
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**3**	12
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		40

Bewertungszahlen:			
		SF-FUNK:	1,48
		SF-INT:	1,28
		SF-MGMT:	0,88
Gesamt:	**1,33**	SF-DOKU:	1,67

Abbildung 4.46.: Nutzwertanalyse der Context-Aware Security Architecture for Emerging Applications ([CFZA02])

Frameworkkategorie:	IT-Architektur	Referenz: [CFZA02]
Frameworkname:	A Context-Aware Security Architecture for Emerging Applications	
Frameworkautoren:	Covington, M. J.; Fogla, P.; Zhan, Z.; Ahamad, M.	

Zwar zielt die 2002 als Konferenzbeitrag veröffentlichte Arbeit vom Titel her auf einzelne kontextsensitive Dienste ab und bezeichnet den Inhalt selbst als *Sicherheitsarchitektur*; inhaltlich bezieht sie sich jedoch auf das Zusammenspiel mehrerer Anwendungen in Smart-Home-Szenarien und stellt insgesamt ein Security-Framework für Smart-Home-Architekturen dar. Besonders hervorzuheben sind die Gewichte, die der Benutzerfreundlichkeit und der Unterstützung hoher Szenariendynamik mit einem entsprechend adaptiven Ansatz eingeräumt werden. Wie aus der Bewertung in Abbildung 4.46 ersichtlich ist, wird jedoch nur partiell auf Aspekte der Inbetriebnahme und des Managements im laufenden Betrieb eingegangen. Trotz des Fokus auf Heimanwenderszenarien wie *Smart Homes* könnte das Security-Framework bei seiner Weiterentwicklung von einer stärkeren Orientierung an Standards und durch das Abdecken von Aspekten wie Monitoring/Auditing sowie einer Analyse der mit seinem Einsatz konkret zu erzielenden Verbesserungen profitieren.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**1**	4
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		44

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**1**	2
SF-MGMT-Compliance	4	**3**	12
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**3**	6
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**1**	1
Summe SF-MGMT	51		45

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**2**	4
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**1**	4
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		43

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**1**	2
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**1**	1
SF-DOKU-Checkliste	1	**3**	3
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**2**	2
SF-DOKU-Lifecyclephasen	1	**1**	1
SF-DOKU-Vollständigkeit	2	**2**	4
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**1**	1
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		46

Bewertungszahlen:		SF-FUNK:	2,10
		SF-INT:	1,48
		SF-MGMT:	0,88
Gesamt:	**1,59**	SF-DOKU:	1,92

Abbildung 4.47.: Nutzwertanalyse des Framework for an Institutional High Level Security Policy for the Processing of Medical Data and their Transmission through the Internet ([PI01])

Frameworkkategorie:	IT-Architektur	Referenz: [PI01]
Frameworkname:	A Framework for an Institutional High Level Security Policy for the Processing of Medical Data and their Transmission through the Internet	
Frameworkautoren:	Pangalos, G.; Ilioudis, Ch.	

Das im Rahmen des internationalen Projekts *Intranet Health Clinic* entstandene Framework unterscheidet sich von fast allen hier betrachteten anderen Arbeiten dadurch, dass es keine konkreten technischen Lösungsbausteine vorgibt. Vielmehr wird aus einer Top-Down-Perspektive spezifiziert, welche Charakteristika IT-Systeme, die in medizinischen Einrichtungen bzw. E-Health-Infrastrukturen eingesetzt werden, aufweisen müssen und wie diese zusammenzuspielen haben, um die für das Umfeld spezifischen Sicherheitsanforderungen und gesetzlichen Auflagen zu erfüllen. Dabei wird durchgängig stärker auf das Sicherheitsmanagement als die technische Umsetzung der einzelnen Anforderungen eingegangen. Die analysierte Arbeit geht adäquat auf Einführungs- und Betriebsaspekte ein und unterstützt die Beurteilung zur Auswahl stehender Systeme unter anderem durch ihren als Checkliste nutzbaren Aufbau. Eine weitere Verbesserung könnte insbesondere durch die Beschreibung von Schnittstellen nach außen, z. B. zu Geschäfts- und ITSM-Prozessen, und durch die Dokumentation eines Verfahrens, wie das erreichte Sicherheitsniveau beurteilt werden kann, erreicht werden. Die Bewertung ist in Abbildung 4.47 zusammengefasst.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**0**	0
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		34

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		8

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**0**	0
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		21

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**3**	6
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		48

Bewertungszahlen:			
		SF-FUNK:	1,62
		SF-INT:	0,72
		SF-MGMT:	0,16
Gesamt:	**1,13**	SF-DOKU:	2,00

Abbildung 4.48.: Nutzwertanalyse des framework for security on NoC technologies ([GG03])

Frameworkkategorie:	IT-Architektur	Referenz: [GG03]
Frameworkname:	A framework for security on NoC technologies	
Frameworkautoren:	Gebotys, C. H.; Gebotys, R. J.	

Das 2003 veröffentlichte Security-Framework betrachtet die Sicherheit auf Transport- und Anwendungsebene für Networks-on-Chip (NoC), die beispielsweise für Smartcards verwendet werden. Das Konzept geht ausführlich auf spezifische, insbesondere hardwarenahe Angreifermodelle ein; es umfasst sowohl eine ausführliche formale Basis als auch Simulationen und praktische Messungen, bei denen auch die Performance analysiert wurde.

Einhergehend mit der äußerst technischen und sehr hardwarenahen Ausrichtung werden die Auswirkungen des vorgestellten Ansatzes auf den praktischen Einsatz und die Aspekte des zentralen Managements z. B. einer größeren Anzahl eingesetzter NoCs nicht thematisiert; auch auf Kostenaspekte, die u. a. aufgrund der hohen Stückzahlen bei Smartcards durchaus ins Gewicht fallen, sollte bei einer Weiterentwicklung des Security-Frameworks eingegangen werden. Die Bewertung ist in Abbildung 4.48 zusammengefasst.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**0**	0
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		38

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**2**	8
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**1**	4
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**2**	4
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**1**	2
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**2**	4
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**1**	1
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**1**	1
Summe SF-MGMT	51		38

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**1**	2
SF-INT-Kompatibilität	2	**1**	2
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**1**	4
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**1**	4
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**1**	2
Summe SF-INT	29		24

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**2**	4
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**1**	1
SF-DOKU-Designentscheid.	2	**1**	2
SF-DOKU-Kontinuum	1	**1**	1
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**1**	4
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		32

Bewertungszahlen:			
		SF-FUNK:	1,81
		SF-INT:	0,83
		SF-MGMT:	0,75
Gesamt:	**1,18**	SF-DOKU:	1,33

Abbildung 4.49.: Nutzwertanalyse des hierarchical framework model of mobile security ([SHKS01])

Frameworkkategorie:	IT-Architektur	Referenz: [SHKS01]
Frameworkname:	A hierarchical framework model of mobile security	
Frameworkautoren:	Sun, J. Z.; Howie, D.; Koivisto, A.; Sauvola, J.	

Vergleichbar mit dem auf Seite 207 analysierten Framework für E-Health-Infrastrukturen bereitet die hier untersuchte Arbeit die Architekturkomponenten für die IT-Sicherheit mobiler Geräte und Anwendungen systematisch auf, ohne für den jeweiligen Teilbereich konkrete Produkte vorzuschlagen bzw. zur Auswahl zu stellen; stattdessen werden die jeweiligen Eigenschaften näher beschrieben und können bei einer Evaluation entsprechender Komponenten als Kriterien herangezogen werden. Während folglich eine direkte Instanziierung des Frameworks weder vorgesehen noch möglich ist, wird ein breites Spektrum relevanter Aspekte – auch im Hinblick auf die praktische Anwendung und das dafür notwendige operative Management – diskutiert. Obwohl die Arbeit explizit auf die Notwendigkeit zur Evaluation und Beurteilung des erreichten Sicherheitsniveaus hinweist, könnte sie durch die Nennung entsprechender Messverfahren und Beurteilungskriterien noch verbessert werden. Darüber hinaus werden viele Anforderungen wie die Dokumentation der Designentscheidungen zwar ansatzweise erfüllt, eine ausführlichere Darstellung wäre für die Übertragung auf eigene Szenarien jedoch sehr hilfreich. Abbildung 4.49 fasst die Bewertung des 2001 entstandenen Frameworks zusammen.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		53

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**1**	4
SF-MGMT-Delegation	2	**1**	2
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**3**	6
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		25

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**1**	4
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		33

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		32

Bewertungszahlen:			
		SF-FUNK:	2,52
		SF-INT:	1,14
		SF-MGMT:	0,49
Gesamt:	**1,37**	SF-DOKU:	1,33

Abbildung 4.50.: Nutzwertanalyse des multi-agent security framework for e-health services ([SSMT07])

Frameworkkategorie:	IT-Architektur	Referenz: [SSMT07]
Frameworkname:	A multi-agent security framework for e-health services	
Frameworkautoren:	Sulaiman, R.; Sharma, D.; Ma, W.; Tran, D.	

Das 2007 veröffentlichte Security-Framework ordnet die Verwendung von Agentensysteme umfassend in die größeren Zusammenhänge von E-Health-Architekturen ein und führt eine gute Klassifikation des jeweiligen Schutzbedarfs durch. Allerdings werden Konzepte vorgestellt, deren Implementierung als zukünftiges Aufgabenpaket beschrieben wird, so dass bislang weder auf praktische Erfahrungen noch auf die Managementeigenschaften im laufenden Betrieb eingegangen wird. Auch die Maßnahmen zur Anpassung an eigene Umgebungen werden nur rudimentär beschrieben. Bei der Weiterentwicklung sollte ferner auf die für den Bereich E-Health relevanten Standards und Compliance-Aspekte eingegangen werden. Die Bewertung ist in Abbildung 4.50 zusammengefasst.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**1**	4
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**3**	6
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		41

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**1**	2
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**1**	2
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		11

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**1**	2
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**1**	4
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		33

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**1**	2
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**1**	2
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**3**	12
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**0**	0
Summe SF-DOKU	24		30

Bewertungszahlen:		SF-FUNK:	1,95
		SF-INT:	1,14
		SF-MGMT:	0,22
Gesamt:	**1,14**	SF-DOKU:	1,25

Abbildung 4.51.: Nutzwertanalyse des New Grid Security Framework with Dynamic Access Control ([XGLQ04])

Frameworkkategorie:	IT-Architektur	Referenz: [XGLQ04]
Frameworkname:	A New Grid Security Framework with Dynamic Access Control	
Frameworkautoren:	Xie, B.; Gui, X.; Li, Y.; Qian, D.	

Die 2004 entstandene Arbeit nimmt auf die zu diesem Zeitpunkt aktuellen Grid-Middleware-Implementierungen Bezug und erweitert die statischen Authentifizierungs- und Autorisierungsmechanismen um eine dynamische Komponente, die neben Access Control Lists auch auf die Laufzeitanalyse der von Benutzern abgeschickten Grid-Jobs setzt, um Missbrauch nicht nur durch Autorisierungsregeln vorzubeugen, sondern gegebenenfalls auch erkennen und darauf reagieren zu können. Grid-Benutzer werden dabei ähnlich zu Vertraulichkeitsstufen im militärischen Bereich in sechs verschiedene Sicherheitsstufen eingeteilt, zwischen denen sie auf Basis einer automatischen Auswertung ihres Nutzungsverhaltens im Laufe der Zeit verschoben werden. Bei der in Abbildung 4.51 zusammengefassten Bewertung ist zu berücksichtigen, dass sie sich der analysierten Arbeit entsprechend auf den sicherheitsfunktionalen Bereich Access Control beschränkt und somit inhaltlich nicht direkt mit der in Abschnitt 4.3.1 vorgestellten Arbeit vergleichen lässt. Neben der Ergänzung des Frameworkkonzepts auf Basis der bislang nicht berücksichtigten Anforderungen ist eine ausführlichere Darstellung des Lösungsansatzes wünschenswert, da zahlreiche Aspekte zwar angerissen, aber nicht in adäquatem Umfang erläutert werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**2**	4
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**1**	4
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		26

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**3**	6
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**3**	6
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**3**	6
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**3**	6
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		36

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		23

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**1**	1
SF-DOKU-Lifecyclephasen	1	**1**	1
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		40

Bewertungszahlen:			
		SF-FUNK:	1,24
		SF-INT:	0,79
		SF-MGMT:	0,71
Gesamt:	**1,10**	SF-DOKU:	1,67

Abbildung 4.52.: Nutzwertanalyse des policy based approach to security for the semantic web ([KFJ03])

Frameworkkategorie:	IT-Architektur	Referenz: [KFJ03]
Frameworkname:	A policy based approach to security for the semantic web	
Frameworkautoren:	Kagal, L.; Finin, T.; Joshi, A.	

Die 2003 an der University of Maryland in Zusammenarbeit mit den Hewlett-Packard Labs entstandene Arbeit setzt sich zum Ziel, ein Security-Framework für Webressourcen, -agenten und -dienste zu spezifizieren. Zur Erläuterung werden Beispiele wie Supply Chain Management Systeme herangezogen. Der Schwerpunkt liegt auf dem Einsatz von Policies bzw. Regelwerken zur Konfiguration der Zugriffssteuerung und deren Management; eine zentrale Rolle spielen dabei die delegierte und somit verteilte Policy-Erstellung und die damit verbundenen Mechanismen zur Erkennung und Behebung von zueinander widersprüchlichen Policies.

Die in Abbildung 4.52 zusammengefasste Bewertung verdeutlicht, dass sich die untersuchte Arbeit auf ausgewählte Bereiche des Problemraums beschränkt. Einige dieser Einschränkungen des Umfangs werden explizit genannt, so dass die vorgeschlagenen Maßnahmen, obwohl sie über die Policysprache und das Management der Policies nicht hinausgehen und damit nicht als umfassende Sicherheitslösung für Webanwendungen gelten können, die gesteckten Zielsetzungen voll erfüllen. Zur weiteren Verbesserung sollte stärker auf die Umsetzung der Lösungsansätze in der Praxis und die damit verbundenen Betriebsaufwendungen eingegangen werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**3**	6
Summe SF-FUNK	21		48

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**3**	6
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**3**	12
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		43

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		29

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**3**	3
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**3**	6
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		47

Bewertungszahlen:		SF-FUNK:	2,29
		SF-INT:	1,00
		SF-MGMT:	0,84
Gesamt:	**1,52**	SF-DOKU:	1,96

Abbildung 4.53.: Nutzwertanalyse des Policy-based Security Framework for Ad-hoc Networks ([Keo05])

Frameworkkategorie:	IT-Architektur	Referenz: [Keo05]
Frameworkname:	A Policy-based Security Framework for Ad-hoc Networks	
Frameworkautoren:	Keoh, S. L.	

Das im Rahmen einer Dissertation entstandene Security-Framework thematisiert Ad-hoc Netze unter Berücksichtigung der Skalierbarkeit bezüglich der Anzahl der beteiligten Geräte, deren Heterogenität und des Bedarfs an partieller Out-of-Band-Kommunikation durch die Gerätebesitzer. Die Arbeit erläutert die mit der Umsetzung der vorgeschlagenen Sicherheitsmechanismen verbundenen administrativen Konzepte und operativen Managementabläufe ausführlich und nimmt eine kritische Beurteilung der mit dem Frameworkeinsatz erzielbaren Verbesserungen vor. Darüber hinaus werden Konzepte zur Umsetzung in verschiedenen Szenarien vorgelegt.

Wie die Bewertung in Abbildung 4.53 zeigt, könnten bei einer Weiterentwicklung insbesondere noch die Integrations- und die Managementeigenschaften verbessert werden. Einerseits wird bislang nicht auf Maßnahmen zur Anpassung des Security-Frameworks an eigene Szenarien eingegangen und auch die Umsetzung wird nicht methodisch unterstützt. Zum anderen werden zwar beispielsweise auftretende Ereignisse erläutert, die jedoch nicht auf ihre Sicherheitsrelevanz untersucht werden und für die keine Auswertungsmechanismen vorgesehen sind. Zudem sollten die eingesetzten Policies über ihre Rolle als technischer Steuermechanismus hinaus stärker in den Kontext übergreifender Sicherheitsrichtlinien und -ziele gestellt werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**3**	6
Summe SF-FUNK	21		60

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**3**	6
SF-MGMT-Berichtsdetails	2	**1**	2
SF-MGMT-Compliance	4	**1**	4
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**1**	2
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**2**	4
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**1**	2
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**1**	2
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**2**	2
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		60

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**2**	4
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		33

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**3**	6
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**2**	2
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**3**	12
SF-DOKU-Zertifizierung	1	**1**	1
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		55

Bewertungszahlen:		SF-FUNK:	2,86
		SF-INT:	1,14
		SF-MGMT:	1,18
Gesamt:	**1,87**	SF-DOKU:	2,29

Abbildung 4.54.: Nutzwertanalyse des Security Framework for Card-Based Systems ([Tsi02])

Frameworkkategorie:	IT-Architektur	Referenz: [Tsi02]
Frameworkname:	A Security Framework for Card-Based Systems	
Frameworkautor:	Tsiounis, Y.	

Tsiounis' 2002 veröffentlichtes Security-Framework zielt auf das sichere Bezahlen mit Kredit-, Debit- und Prepaid-Karten insbesondere bei Online-Anwendungen ab; es wendet sich implizit an Systemarchitekten bei Banken sowie an Händler (vgl. das in Abschnitt 3.3 diskutierte Szenario 2). Vor diesem Hintergrund werden sowohl die spezifischen Angreifermodelle als auch die relevanten Angriffe ausführlich erläutert, wohingegen die gesetzlichen Randbedingungen ausführlicher berücksichtigt werden könnten. Positiv fallen neben der gelungenen Untersuchung des Umfelds und der Modellierung der Abläufe insbesondere die Ansätze zur Quantifizierung des erreichten Sicherheitsniveaus auf, die jedoch noch vertieft werden sollten. Darüber hinaus muss der präsentierte Lösungsansatz vollständig umgesetzt werden, so dass bislang kein stufenweiser Rollout möglich ist. Wie auch die Bewertung in Abbildung 4.54 zeigt, wäre darüber hinaus eine noch vertiefte Betrachtung insbesondere der Aspekte des operativen Managements wünschenswert.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**1**	4
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		46

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**3**	6
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**2**	4
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**1**	2
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		44

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		37

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**2**	4
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**1**	1
Summe SF-DOKU	24		37

Bewertungszahlen:			
		SF-FUNK:	2,19
		SF-INT:	1,28
		SF-MGMT:	0,86
Gesamt:	**1,47**	SF-DOKU:	1,54

Abbildung 4.55.: Nutzwertanalyse des security framework for distributed brokering systems ([PPF+03])

Frameworkkategorie:	IT-Architektur	Referenz: [PPF+03]
Frameworkname:	A security framework for distributed brokering systems	
Frameworkautoren:	Pallickara, S.; Pierce, M.; Fox, G.; Yan, Y.; Huang, Y.	

In Anlehnung an Web-Service-Standards und die in Peer-to-Peer-Systemen und Grids angewandten Kommunikationskonzepte stellt das 2003 entstandene Framework Lösungsansätze für die sichere Kommunikation über Vermittlungsstationen in großen, inhärent unsicheren Netzen vor. Dabei wird ausführlich auf verschiedene Angriffe und deren Prävention und Erkennung sowie Reaktionen auf erfolgreiche Angriffe eingegangen. In einer Folgepublikation wird eine Implementierung des Frameworks vorgestellt, deren Performanz ausführlich analysiert wird (siehe [YHF+03]).

Obwohl wie in Abbildung 4.55 ersichtlich Teile der Betriebsaspekte bereits beschrieben werden, würde das Framework von einer explizit erläuterten Methodik zu seiner Anpassung und seiner Einführung in eigenen Szenarien stark profitieren. Darüber hinaus fehlen Prozess-Schnittstellen u. a. zum Sicherheitsmanagement, wodurch die im Kern sehr technische Ausrichtung des Security-Frameworks unterstrichen wird.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**2**	4
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**1**	4
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		36

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**2**	4
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		20

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**2**	4
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		23

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**1**	2
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**0**	0
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**0**	0
Summe SF-DOKU	24		26

Bewertungszahlen:		SF-FUNK:	1,71
		SF-INT:	0,79
		SF-MGMT:	0,39
Gesamt:	**1,00**	SF-DOKU:	1,08

Abbildung 4.56.: Nutzwertanalyse des Security Framework for Personal Networks ([SKI08])

Frameworkkategorie:	IT-Architektur	Referenz: [SKI08]
Frameworkname:	A Security Framework for Personal Networks	
Frameworkautoren:	Shin, S.; Kobara, K.; Imai, H.	

Das 2008 veröffentlichte Security-Framework entstand im Rahmen eines vom japanischen Wirtschaftsministerium geförderten Projekts; es zielt auf die Absicherung von Funknetzen ab, an denen überwiegend Geräte desselben Benutzers angeschlossen sind – neben tragbaren Rechnern und Smartphones beispielsweise auch Autos und Haushaltsgeräte.

Der Schwerpunkt des Security-Frameworks liegt auf der Spezifikation von Protokollen für den sicheren Austausch von kryptographischen Schlüsseln, die zur Absicherung der Kommunikation zwischen den beteiligten Geräten dienen; weitere technische Maßnahmen werden nicht vorgestellt, so dass die Vollständigkeit des Frameworks im Hinblick auf den praktischen Einsatz fraglich erscheint. Zudem ist das gesamte Frameworkkonzept sehr technisch orientiert; für die Weiterentwicklung bleibt es entsprechend wünschenswert, dass auch die Betriebs- und Managementaspekte untersucht und konkretere Hilfsmittel zum Umsetzung in eigenen Szenarien bereitgestellt werden. Die Bewertung ist in Abbildung 4.56 zusammengefasst.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**1**	2
SF-FUNK-Adaptivität	1	**1**	1
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**1**	4
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**1**	2
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		23

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		4

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**2**	4
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**1**	4
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**1**	2
Summe SF-INT	29		18

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**1**	2
SF-DOKU-Voraussetzungen	4	**1**	4
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		30

Bewertungszahlen:		SF-FUNK:	1,10
		SF-INT:	0,62
		SF-MGMT:	0,08
Gesamt:	**0,76**	SF-DOKU:	1,25

Abbildung 4.57.: Nutzwertanalyse des security framework for service oriented architectures ([Can07])

Frameworkkategorie:	IT-Architektur	Referenz: [Can07]
Frameworkname:	A security framework for service oriented architectures	
Frameworkautor:	Candolin, C.	

Das 2007 beim finnischen Militär entstandene Security-Framework konzentriert sich auf den Übergang von klassischen Client-/Server-Architekturen hin zum Einsatz von SOA für intensiv über unsichere Netze kommunizierende Anwendungen. Es wendet sich implizit an Systemarchitekten und diskutiert eine Reihe von Sicherheitsanforderungen sowie die vorgeschlagene Lösungsarchitektur, die aus den Ebenen *network*, *communication* und *content security* besteht. Aus diesem Aufbau und dem Abstraktionsgrad des Konzepts resultiert die Schwierigkeit, dass diverse Eigenschaften zwar vom erstellten Frameworkkonzept gefordert werden, dass aber auf Möglichkeiten zu ihrer konkreten Umsetzung nicht eingegangen wird. Hieraus ergibt sich wie in Abbildung 4.57 dargestellt eine ganze Reihe von nur mit einem Punkt bewerteten sicherheitsfunktionalen Anforderungen; das Framework würde folglich von einer ausführlicheren Diskussion dieser bereits berücksichtigten Aspekte deutlich profitieren. Ferner zielt die untersuchte Arbeit zwar bereits explizit auf die Spezifikation eines Security-Frameworks ab, stellt jedoch die im Rahmen des Designs angewandte Anforderungsanalyse in den Vordergrund, so dass nahezu alle Anforderungen rund um die Umsetzung und den Betrieb des Frameworks in eigenen Szenarien nicht erfüllt werden. Insgesamt handelt es sich somit um einen typischen Vertreter der stark technisch geprägten Security-Frameworks.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**1**	2
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		52

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**3**	3
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**1**	2
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**1**	4
SF-MGMT-Zuständigkeiten	1	**1**	1
Summe SF-MGMT	51		36

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**3**	6
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**2**	4
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		47

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**3**	6
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**1**	1
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**3**	12
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**1**	1
Summe SF-DOKU	24		48

Bewertungszahlen:			
		SF-FUNK:	2,48
		SF-INT:	1,62
		SF-MGMT:	0,71
Gesamt:	**1,70**	SF-DOKU:	2,00

Abbildung 4.58.: Nutzwertanalyse des security framework for wireless sensor networks ([Zia08])

Frameworkkategorie:	IT-Architektur	Referenz: [Zia08]
Frameworkname:	A security framework for wireless sensor networks	
Frameworkautor:	Zia, T. A.	

Das 2008 als Dissertation veröffentlichte Security-Framework für Funksensornetze unterstützt als eine von wenigen der hier analysierten Arbeiten den stufenweisen Ausbau durch das sukzessive Ausrollen seiner Komponentengruppen; davon unabhängig empfiehlt es als mittelfristiges Ziel für die Umsetzung aber klar den kombinierten Einsatz aller bereitgestellten Komponenten. Das Framework selbst besteht aus der Zusammenstellung mehrerer bereits verfügbarer Komponenten sowie aus diversen eigenen Beiträgen. Gegenüber den meisten der anderen betrachteten Arbeiten fällt auch die Definition von Sicherheitsereignissen und die gute Analyse spezifischer Angriffsarten positiv auf. Abbildung 4.58 zeigt die zusammengefasste Bewertung. Für die Weiterentwicklung ist zum einen wünschenswert, dass die Kosten nicht nur unter dem Stichwort Energieeffizienz aufgegriffen, sondern dass auch die übrigen zur Bereitstellung und zum Betrieb notwendigen Mittel berücksichtigt werden. Zum anderen wird zwar auf das Thema Sensornetze im Allgemeinen eingegangen und eine grundlegende Einbettung ins Umfeld vorgenommen, allerdings wird auf das Management der bereits im Einsatz befindlichen und vom vorgeschlagenen Security-Framework geschützten Sensoren nicht eingegangen. Zur Verbesserung sollten beispielsweise neben den Sicherheitsereignissen selbst auch deren Auswertung und die resultierenden Handlungsempfehlungen zur weiteren Erhöhung des Sicherheitsniveaus beschrieben werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**2**	4
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**3**	6
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		41

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**2**	4
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**1**	2
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**1**	2
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		29

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**1**	2
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**1**	4
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		37

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		38

Bewertungszahlen:			
		SF-FUNK:	1,95
		SF-INT:	1,28
		SF-MGMT:	0,57
Gesamt:	**1,35**	SF-DOKU:	1,58

Abbildung 4.59.: Nutzwertanalyse des security framework with trust management for sensor networks ([YKL+05])

Frameworkkategorie:	IT-Architektur	Referenz: [YKL+05]
Frameworkname:	A security framework with trust management for sensor networks	
Frameworkautoren:	Yao, Z.; Kim, D.; Lee, I.; Kim, K.; Jang, J.	

Abbildung 4.59 fasst die Bewertung des 2005 veröffentlichten Security-Frameworks für Sensornetze zusammen. Es konzentriert sich auf die sichere Kommunikation zwischen autarken, beliebig verteilten Sensoren und greift, da sich die Kommunikationspartner nicht alle a priori gegenseitig kennen, stark auf Trust-Level-Management-Konzepte zurück. Entsprechend liegt die technische Stärke insbesondere in der guten Adaptivität zur Laufzeit; den damit einhergehenden Abläufen wird alles andere jedoch untergeordnet, so dass sogar einige der im Framework vorgesehenen Komponenten nicht näher erläutert werden.

Damit eng verbunden ist die stark technische Ausrichtung des gesamten Frameworkkonzepts, so dass auch die bereits aufgegriffenen Integrations- und Managementaspekte bei einer Weiterentwicklung des Frameworks noch deutlich vertieft werden sollten. Beispielsweise werden die verarbeiteten Trust-Level zwar quantifiziert, eine Übertragung auf das Gesamtsicherheitsniveau findet aber nicht statt. In weitere Versionen des Frameworks sollten vor allem in der Praxis gewonnene Betriebserfahrungen stärker einfließen, die über die bislang dargestellten einfachen Beispiele hinausgehen.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**1**	1
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**1**	4
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**1**	4
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		11

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		4

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**0**	0
SF-INT-Modularität	2	**1**	2
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**0**	0
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		4

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**0**	0
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**0**	0
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		16

Bewertungszahlen:		SF-FUNK:	0,52
		SF-INT:	0,14
		SF-MGMT:	0,08
Gesamt:	**0,35**	SF-DOKU:	0,67

Abbildung 4.60.: Nutzwertanalyse des extended security framework for e-government ([AAAK08])

Frameworkkategorie:	IT-Architektur	Referenz: [AAAK08]
Frameworkname:	An extended security framework for e-government	
Frameworkautoren:	Al-Ahmad, W.; Al-Kaabi, R.	

Die Bewertung des 2008 veröffentlichten Security-Frameworks für E-Government-Architekturen ist in Abbildung 4.60 zusammengefasst. Die Arbeit wählt zwar einen explizit prozessorientierten Ansatz, geht unter anderem aufgrund ihrer Kompaktheit aber nur sehr allgemein und oberflächlich auf die Basisziele der IT-Sicherheit im E-Government-Kontext ein. In der vorliegenden Form ist die Frameworkdokumentation trotz der Vorarbeiten derselben Autoren, in denen beispielsweise eine grundlegende Anforderungsanalyse durchgeführt wird, für die praktische Umsetzung zu knapp gehalten und erzielt keinen erkennbaren Mehrwert. Für die Weiterentwicklung ist deshalb vorrangig wünschenswert, dass die erarbeiteten Konzepte in einer angemessenen Ausführlichkeit dargestellt werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**2**	4
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		47

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**1**	2
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		16

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**0**	0
SF-INT-Parallelbetrieb	4	**1**	4
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		29

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**2**	4
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**1**	1
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		39

Bewertungszahlen:		SF-FUNK:	2,24
		SF-INT:	1,00
		SF-MGMT:	0,31
Gesamt:	**1,29**	SF-DOKU:	1,63

Abbildung 4.61.: Nutzwertanalyse des Identity-Based Security Framework For VANETs ([KBT06])

Frameworkkategorie:	IT-Architektur	Referenz: [KBT06]
Frameworkname:	An Identity-Based Security Framework For VANETs	
Frameworkautoren:	Kamat, P.; Baliga, A.; Trappe, W.	

Die 2006 veröffentlichte Beschreibung des Security-Framework für Vehicular Ad-hoc Networks (VANETs) ist äußerst kompakt und reißt viele Aspekte deshalb nur sehr knapp an. Aufgrund der mit Pseudocode beschriebenen Algorithmen wenden sich die Autoren primär an VANET-Systemdesigner und -architekten. Diesem Ansatz entsprechend wird vorrangig auf die technischen Eigenschaften eingegangen, so dass sich Verbesserungen insbesondere durch die Darstellung der Einführungs- und Betriebsaspekte bei der konkreten Anwendung des Security-Frameworks ergeben würden. Die Bewertung ist in Abbildung 4.61 zusammengefasst.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**1**	4
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**3**	6
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		38

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**3**	3
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**1**	1
Summe SF-MGMT	51		24

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**3**	6
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**1**	4
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**1**	2
Summe SF-INT	29		41

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**1**	4
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		34

Bewertungszahlen:			
		SF-FUNK:	1,81
		SF-INT:	1,41
		SF-MGMT:	0,47
Gesamt:	**1,28**	SF-DOKU:	1,42

Abbildung 4.62.: Nutzwertanalyse des Integrated Security Framework for Assisting in the Defense of Computer Networks ([OLH06])

Frameworkkategorie:	IT-Architektur	Referenz: [OLH06]
Frameworkname:	An Integrated Security Framework for Assisting in the Defense of Computer Networks	
Frameworkautoren:	Onwubiko, C.; Lenaghan, A. P.; Hebbes, L.	

Das 2006 an der Kingston University entstandene Security-Framework behandelt unternehmensweite Rechnernetze. Es zeichnet sich zum einen durch seine explizit vorgesehene Erweiterbarkeit und zum anderen dadurch aus, dass es auf die größtmögliche Automatisierung abzielt, die auch Reaktionen auf erkannte Angriffe umfasst. Viele der zur nahtlosen Integration erforderlichen Schnittstellen und die damit verbundenen Kompatibilitätsaspekte werden zumindest ansatzweise behandelt.

Wie auch die in Abbildung 4.62 zusammengefasste Bewertung widerspiegelt, überträgt das Security-Framework zwar den von autonomen Systemen bekannten Ansatz *messen – auswerten – reagieren* auf die IT-Sicherheit, nimmt dabei jedoch keine Einbettung in einen gesamtheitlichen Managementansatz vor. In die Weiterentwicklung sollten deshalb insbesondere die mit der praktischen Umsetzung gemachten Erfahrungen im laufenden Betrieb einfließen und neben den für die eingesetzten Komponenten spezifischen Abläufen auch das Prozessumfeld vorgestellt werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**2**	4
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		44

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**1**	4
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**1**	2
SF-MGMT-Policies	2	**1**	2
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**1**	2
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**1**	4
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		34

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**1**	2
Summe SF-INT	29		33

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**1**	2
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**1**	1
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**2**	2
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**1**	2
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		43

Bewertungszahlen:			
		SF-FUNK:	2,10
		SF-INT:	1,14
		SF-MGMT:	0,67
Gesamt:	**1,42**	SF-DOKU:	1,79

Abbildung 4.63.: Nutzwertanalyse der Study on Security Framework for Ambient Intelligence Environment ([KR09])

Frameworkkategorie:	IT-Architektur	Referenz: [KR09]
Frameworkname:	A Study on Security Framework for Ambient Intelligence Environment	
Frameworkautoren:	Ko, H.; Ramos, C.	

Das 2009 veröffentlichte Security-Framework thematisiert die IT-Sicherheit für Umgebungen, in denen die von der europäischen IST Advisory Group konzipierten Ambient Intelligence (AmI) Systeme eingesetzt werden. Dabei werden zunächst die Sicherheitsdefizite beim Einsatz des AmI-Frameworks aufgezeigt und verschiedene spezifische Angriffe erläutert, für die geeignete Schutzmechanismen erarbeitet werden müssen.

Wie die in Abbildung 4.63 zusammengefasste Beurteilung zeigt, werden zwar bereits viele Aspekte der Umsetzung in eigenen Szenarien angerissen; insgesamt sollte auf die Integration der mit dem Security-Framework geschützten Systeme in die betrieblichen Umgebungen jedoch noch tiefer eingegangen werden. Darüber hinaus ist eine Beschreibung des Zusammenspiels mit den anderen in entsprechenden Umgebungen anzutreffenden Managementabläufen wünschenswert; ebenso sollten die kontinuierliche Überwachung und die Beurteilung der mit Hilfe des Security-Frameworks erreichten Verbesserung des Sicherheitsniveaus thematisiert werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		51

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**1**	2
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**2**	4
SF-MGMT-Policies	2	**1**	2
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		32

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**2**	4
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		33

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**2**	4
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**1**	1
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**1**	1
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		42

Bewertungszahlen:			
		SF-FUNK:	2,43
		SF-INT:	1,14
		SF-MGMT:	0,63
Gesamt:	**1,49**	SF-DOKU:	1,75

Abbildung 4.64.: Nutzwertanalyse von Attack analysis & bio-inspired security framework for IP multimedia subsystem ([AFJ08])

Frameworkkategorie:	IT-Architektur	Referenz: [AFJ08]
Frameworkname:	Attack analysis & bio-inspired security framework for IP multimedia subsystem	
Frameworkautoren:	Awais, A.; Farooq, M.; Javed, M. Y.	

Das 2008 veröffentlichte Security-Framework geht insbesondere auf die Angriffe, die für *next generation all-IP networks* relevant sind, und dafür geeignete Erkennungsmöglichkeiten ein. Insgesamt liegt der Schwerpunkt somit klar bei Mechanismen und Maßnahmen zur Intrusion Detection, worunter die Vollständigkeit des technischen Lösungsansatzes für das Themengebiet als Ganzes etwas leidet. Positiv fällt jedoch die hohe Adaptivität der vorgeschlagenen Lösung zur Laufzeit auf, zu denen die Autoren die Analogie zu Immunsystemen ziehen.

Die in Abbildung 4.64 dargestellte Bewertung verdeutlicht, dass der technische Lösungsansatz bei der Beschreibung des Security-Frameworks im Vordergrund steht. Für neue Versionen des Frameworks sind deshalb insbesondere sowohl eine Beschreibung der Schritte zur szenarienspezifischen Umsetzung als auch eine umfassendere Diskussion der Managementaufgaben im Betrieb wünschenswert.

Frameworkkategorie:	IT-Architektur	Referenz: [All04]
Frameworkname:	Building a Practical Framework for Enterprise-Wide Security Management	
Frameworkautor:	Allen, J. H.	

Die 2004 an der Carnegie Mellon University in Kooperation mit dem US Department of Defense entstandene Arbeit betrachtet unternehmensweite Sicherheit vorrangig aus der Managementperspektive; entsprechend wird jedoch nur relativ knapp auf konkrete technische Lösungsansätze eingegangen. Wie die in Abbildung 4.65 zusammengefasste Bewertung zeigt, werden die meisten der untersuchten Kriterien zumindest grundlegend erfüllt; an vielen Stellen bleibt eine deutlich ausführlichere Behandlung des jeweiligen Themas wünschenswert – beispielsweise wird zwar erwähnt, dass mit der Einführung von Sicherheitsmaßnahmen Investitions- und Betriebskosten anfallen, auf deren Konkretisierung, Abschätzung oder Einfluss auf die Priorisierung von Maßnahmen wird aber nicht näher eingegangen.

Die hier untersuchte Arbeit sticht durch ihre explizite Forderung nach Schnittstellen zu den ITSM-Prozessen heraus; ebenso findet sich die Forderung nach einer Umsetzung eines kontinuierlichen Sicherheitsverbesserungsprozesses an mehreren Stellen. Für die Umsetzung in eigenen Szenarien sollte bei einer Weiterentwicklung der Arbeit darauf geachtet werden, noch stärker auf das Vorgehen beim Customizing und auf die Einführung in bestehenden Infrastrukturen einzugehen; die Lesbarkeit könnte z. B. durch konkrete Beispiele noch weiter verbessert werden.

Frameworkkategorie:	IT-Architektur	Referenz: [PGSP07]
Frameworkname:	Context-Sensitive Security Framework for Pervasive Environments	
Frameworkautoren:	Pigeot, C. E.; Gripay, Y.; Scuturici, M.; Pierson, J. M.	

Das 2007 veröffentlichte Security-Framework verfolgt explizit einen integrierenden Ansatz, der nicht nur auf eine formale Basis gestellt, sondern auch implementiert und in der praktischen Anwendung analysiert wurde. Das Konzept geht zudem auf Anforderungen mit Bezug auf die Benutzerfreundlichkeit ein und ist modular aufgebaut, wobei neben den jeweils berücksichtigten Anforderungen auch die gegenseitigen Abhängigkeiten zwischen den Modulen ausführlich dargestellt werden.

Zur weiteren Verbesserung des Security-Frameworks, dessen Bewertung in Abbildung 4.66 zusammengefasst ist, sollte angestrebt werden, über die technischen Lösungskomponenten hinaus noch stärker auf die Prozesse und Arbeitsabläufe beim Einsatz einzugehen. Ferner sollten Methoden bereitgestellt werden, mit denen sich die Ergebnisse des Frameworkeinsatzes und die Auswirkungen auf das erreichte IT-Sicherheitsniveau im jeweiligen Szenario untersuchen lassen.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**1**	2
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**1**	4
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**1**	4
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		28

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**2**	4
SF-MGMT-Compliance	4	**3**	12
SF-MGMT-Delegation	2	**2**	4
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**3**	12
SF-MGMT-Kosten	2	**1**	2
SF-MGMT-KPIs	1	**1**	1
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**1**	4
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**1**	2
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**3**	6
SF-MGMT-Prozesse	4	**3**	12
SF-MGMT-Quantifizierung	2	**1**	2
SF-MGMT-Releasezyklus	2	**1**	2
SF-MGMT-Schulungen	2	**1**	2
SF-MGMT-Support	1	**2**	2
SF-MGMT-Tests	1	**1**	1
SF-MGMT-Verbesserung	4	**3**	12
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		93

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**2**	4
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**2**	4
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		59

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**2**	4
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**2**	2
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**3**	3
SF-DOKU-Lifecyclephasen	1	**2**	2
SF-DOKU-Vollständigkeit	2	**2**	4
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**2**	2
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**3**	3
Summe SF-DOKU	24		60

Bewertungszahlen:			
		SF-FUNK:	1,33
		SF-INT:	2,03
		SF-MGMT:	1,82
	Gesamt:	**1,92**	SF-DOKU: 2,50

Abbildung 4.65.: Nutzwertanalyse von: Building a Practical Framework for Enterprise-Wide Security Management ([All04])

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**0**	0
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		34

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**3**	6
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**1**	2
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**3**	12
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**3**	6
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		43

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**1**	4
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		43

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**1**	1
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		37

Bewertungszahlen:			
		SF-FUNK:	1,62
		SF-INT:	1,48
		SF-MGMT:	0,84
	Gesamt:	**1,37**	SF-DOKU: 1,54

Abbildung 4.66.: Nutzwertanalyse des Context-Sensitive Security Framework for Pervasive Environments ([PGSP07])

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**1**	4
SF-FUNK-Automatisierung	2	**3**	6
SF-FUNK-Maßnahmen	4	**1**	4
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		30

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**2**	4
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		5

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		24

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**0**	0
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**1**	1
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**1**	2
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**0**	0
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		19

Bewertungszahlen:			
		SF-FUNK:	1,43
		SF-INT:	0,83
		SF-MGMT:	0,10
Gesamt:	**0,79**	SF-DOKU:	0,79

Abbildung 4.67.: Nutzwertanalyse von Distributed Intrusion Detection and Attack Containment for Organizational Cyber Security ([BRS06])

Frameworkkategorie:	IT-Architektur	Referenz: [BRS06]
Frameworkname:	Distributed Intrusion Detection and Attack Containment for Organizational Cyber Security	
Frameworkautoren:	Batsell, S. G.; Rao, N. S.; Shankar, M.	

Das 2006 veröffentlichte *integrated cyber security framework* zielt auf die Angriffserkennung und -eindämmung in Unternehmensnetzen ab. Der Schwerpunkt liegt dabei einerseits auf dem Einsatz von Intrusion Detection Systemen und andererseits auf der möglichst weitgehenden Automatisierung insbesondere auch der Reaktionen auf erkannte Angriffe. Auf die hierfür relevanten Angriffstypen wird umfassend eingegangen.

Die Bewertung des Security-Frameworks ist in Abbildung 4.67 zusammengefasst. Für die praktische Umsetzung der Frameworkkonzepte erweist sich als hinderlich, dass nur ein grober Überblick gegeben wird, aber die Details des Frameworks und seine Anwendung nicht diskutiert werden. Entsprechend werden die eingangs erwähnten Schwerpunktthemen zwar sehr gut und verständlich dargestellt, auf den Großteil der für die Gesamtbeurteilung relevanten Aspekte wird jedoch gar nicht oder nur ansatzweise eingegangen. Für eine Weiterentwicklung sind deshalb eine umfassendere Betrachtung und detailliertere Beschreibungen wünschenswert.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**2**	4
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**1**	4
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		26

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**1**	2
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**1**	2
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**1**	1
Summe SF-MGMT	51		26

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**1**	2
Summe SF-INT	29		23

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		28

Bewertungszahlen:		SF-FUNK:	1,24
		SF-INT:	0,79
		SF-MGMT:	0,51
Gesamt:	**0,93**	SF-DOKU:	1,17

Abbildung 4.68.: Nutzwertanalyse des Grid Security Framework for Managing the Certificate ([TN06])

Frameworkkategorie:	IT-Architektur	Referenz: [TN06]
Frameworkname:	Grid Security Framework for Managing the Certificate	
Frameworkautoren:	Thein, T.; Naing, T. T.	

Der 2006 veröffentlichte Konferenzbeitrag verwendet zum im Titel eingesetzten Begriff *Security Framework* noch weitere synonyme Bezeichnungen wie *authenticating framework*. Sein Schwerpunkt liegt dementsprechend auch klar auf der zertifikatsbasierten Authentifizierung und den zum Zertifikatsmanagement notwendigen Prozessen.

Trotz der nur knappen Darstellung wird eine Reihe wichtiger Aspekte angesprochen; wie die in Abbildung 4.68 zusammengefasste Bewertung zeigt, sollten jedoch nahezu alle Aspekte wesentlich ausführlicher diskutiert werden, um einen auf andere Szenarien übertragbaren Mehrwert zu erzielen. Dabei sollten sich die Betrachtungen nicht auf die vorgeschlagene technische Lösung beschränken, sondern eine umfassendere Einbettung in das Grid-Umfeld vornehmen.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		36

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**1**	2
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		30

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**1**	2
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		29

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**1**	2
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		34

Bewertungszahlen:		SF-FUNK:	1,71
		SF-INT:	1,00
		SF-MGMT:	0,59
Gesamt:	**1,18**	SF-DOKU:	1,42

Abbildung 4.69.: Nutzwertanalyse der Implementation of a Security Framework for Wireless Multi-hop Networks ([PC09])

Frameworkkategorie:	IT-Architektur	Referenz: [PC09]
Frameworkname:	Implementation of a Security Framework for Wireless Multi-hop Networks	
Frameworkautor:	Paris, S.; Capone, A.	

Das 2009 veröffentlichte Security-Framework basiert auf mehrjährigen Vorarbeiten im Umfeld drahtloser Ad-Hoc-Netze; als Basis dient die Plattform MobiMESH [CNP06]. Sie ist ein typischer Vertreter von Architekturen, bei denen zunächst vorrangig auf die Funktionalität Wert gelegt und die erst sukzessive um Sicherheitseigenschaften erweitert wurden. Damit verbunden ist ein auf Pilotprojekte begrenzter praktischer Einsatz, der auch zur kontinuierlichen Weiterentwicklung und Verbesserung der eingesetzten Sicherheitsmechanismen geführt hat.

Mit der hier analysierten Arbeit liegt ein Zwischenstand vor, der zwar auf die eigene praktische Umsetzung des Security-Frameworks eingeht, aber die kozeptionelle Anpassung an eigene Szenarien bislang noch nicht explizit vorsieht. Wie die Bewertung in Abbildung 4.69 zeigt, wird auch über die technischen Maßnahmen hinaus noch nicht auf die für das operative Management im laufenden Betrieb relevanten Abläufe eingegangen. Insofern gibt die Arbeit den aktuellen Entwicklungsstand zwar gut wieder, sollte aber insbesondere in Bezug auf die praktische Verwertbarkeit noch erweitert werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		26

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		36

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		39

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**2**	4
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		42

Bewertungszahlen:			
		SF-FUNK:	1,24
		SF-INT:	1,34
		SF-MGMT:	0,71
Gesamt:	**1,26**	SF-DOKU:	1,75

Abbildung 4.70.: Nutzwertanalyse des Interoperable Internet-Scale Security Framework for RFID Networks ([Mao09])

Frameworkkategorie:	IT-Architektur	Referenz: [Mao09]
Frameworkname:	Interoperable Internet-Scale Security Framework for RFID Networks	
Frameworkautor:	Mao, T.	

Die 2008 am MIT abgeschlossene und 2009 veröffentlichte Dissertation von Mao thematisiert die Anwendung von Ontologien, um die IT-Sicherheit und insbesondere den Datenschutz beim Einsatz von RFID-Tags zu verbessern; die technischen Schwerpunkte liegen dabei auf der Authentifizierung und dem Trust Management. Als Anwendungsbeispiel werden Zulieferketten verwendet, bei denen der Weg von mit RFID-Tags versehenen Werkstücken durchgängig vom Hersteller bis zum Endabnehmer verfolgt werden und logistische Teilprozesse maßgeblich vereinfachen können. Die in Abbildung 4.70 zusammengefasste Abbildung zeigt, dass zunächst eine noch ausführlichere Darstellung der technischen Eigenschaften des Frameworks wünschenswert ist; beispielsweise wird in der Arbeit nur auf die allgemeinen Ziele der IT-Sicherheit, nicht aber auf spezifische Schwachstellen und Angriffe bzw. Angreifermodelle beim RFID-Einsatz eingegangen. Darüber hinaus werden die Managementabläufe und Administrationskonzepte zwar mit Bezug auf die vorgestellten technischen Maßnahmen erläutert, eine Einbettung in den Kontext – beispielsweise durch die Darstellung der Schnittstellen zu den anderen Prozessen – würde die Anwendung in eigenen Szenarien jedoch ebenso erleichtern wie die nähere Erläuterung der vorgesehenen Customizing-Maßnahmen.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**1**	2
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**3**	6
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		51

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		2

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**0**	0
SF-INT-Modularität	2	**2**	4
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**0**	0
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		4

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**0**	0
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**0**	0
Summe SF-DOKU	24		26

Bewertungszahlen:		SF-FUNK:	2,43
		SF-INT:	0,14
		SF-MGMT:	0,04
Gesamt:	**0,92**	SF-DOKU:	1,08

Abbildung 4.71.: Nutzwertanalyse des Network Security Framework ([GR06])

Frameworkkategorie:	IT-Architektur	Referenz: [GR06]
Frameworkname:	Network Security Framework	
Frameworkautoren:	Gupta, K. K.; Ramamohanarao, K.	

Das 2006 entstandene *Network Security Framework* verdeutlicht sowohl die bereits diskutierte bislang unscharfe Verwendung des Begriffs Security-Framework als auch die fließenden Übergänge zwischen dienst- und architekturbezogenen Frameworks. Es diskutiert im Wesentlichen den Einsatz von Intrusion Detection Systemen zur Absicherung von (unternehmensweiten) Netzen. Somit handelt es sich um kein umfassendes Security-Framework für Netze, da hierfür neben IDS offensichtlich noch weitere Komponenten benötigt werden; andererseits wird nicht auf die Sicherheit des IDS an sich oder genau eines damit geschützten Dienstes, sondern durchaus auf ein breiteres, netzweites Schutzgebiet eingegangen. Da auf diese thematische Einschränkung gegenüber dem anhand des Titels zu erwartenden Inhalt im Artikel eingegangen wird, bezieht sich die in Abbildung 4.71 zusammengefasste Bewertung hinsichtlich der Sicherheitsfunktionalität nur auf den IDS-spezifischen Umfang. Davon unabhängig liegt jedoch ein Frameworkkonzept vor, das zwar technische Stärken aufweist und ausgewählte Aspekte gut dokumentiert, bezüglich nahezu sämtlicher Anforderungen im Hinblick auf die Einführung und den Betrieb in der Praxis jedoch noch stark erweitert werden sollte.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**3**	6
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		55

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		30

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**0**	0
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**0**	0
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**0**	0
Summe SF-INT	29		21

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**1**	2
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		32

Bewertungszahlen:			
		SF-FUNK:	2,62
		SF-INT:	0,72
		SF-MGMT:	0,59
Gesamt:	**1,32**	SF-DOKU:	1,33

Abbildung 4.72.: Nutzwertanalyse von Phyllo: a peer-to-peer overlay security framework ([HK05])

Frameworkkategorie:	IT-Architektur	Referenz: [HK05]
Frameworkname:	Phyllo: a peer-to-peer overlay security framework	
Frameworkautoren:	Heinbockel, W.; Kwon, M.	

Das 2005 veröffentlichte Security-Framework Phyllo dient dem Selbstschutz von Peer-to-Peer-Netzen durch das Erkennen von kompromittierten oder bösartigen Nodes und automatisierte reaktive Maßnahmen. Der Kernbeitrag liegt in der Definition des Protokolls, das zur logischen Restrukturierung des Netzes eingesetzt wird, um als unerwünscht eingestufte Nodes zu isolieren. Das Framework geht explizit auf diverse spezifische Angriffsvarianten ein und liegt als Referenzimplementierung vor, die auch zur Performanceanalyse verwendet wurde.

Die in Abbildung 4.72 zusammengefasste Bewertung macht deutlich, dass das Security-Framework zwar ausgeprägte technische Stärken hat, dass aber über die algorithmischen Beiträge hinaus noch auf viele weitere Aspekte eingegangen werden sollte. Zwar spielen in den vom Framework betrachteten Peer-to-Peer-Netzen zentrale Managementkonzepte nur eine untergeordnete Rolle; insbesondere die Aspekte der szenariengetriebenen Umsetzung und die Vollständigkeit der Dokumentation sollten bei einer Weiterentwicklung aber stärker berücksichtigt werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**1**	2
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**2**	4
Summe SF-FUNK	21		52

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**1**	2
SF-MGMT-Praxis	2	**3**	6
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**1**	2
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		35

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**3**	6
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		47

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**1**	2
SF-DOKU-Ausrichtung	2	**3**	6
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**2**	2
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**2**	4
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		46

Bewertungszahlen:		SF-FUNK:	2,48
		SF-INT:	1,62
		SF-MGMT:	0,69
Gesamt:	**1,67**	SF-DOKU:	1,92

Abbildung 4.73.: Nutzwertanalyse von Secure SocialAware: A Security Framework for Mobile Social Networking Applications ([BGRH09])

Frameworkkategorie:	IT-Architektur	Referenz: [BGRH09]
Frameworkname:	Secure SocialAware: A Security Framework for Mobile Social Networking Applications	
Frameworkautor:	Beach, A.; Gartrell, M.; Ray, B.; Han, R.	

Das 2009 als Technical Report veröffentlichte Security-Framework thematisiert die IT-Sicherheit mit Schwerpunkt Datenschutz bei der Nutzung von sozialen Netzen mit mobilen Anwendungen, die beispielsweise den aktuellen Standort des Nutzers auswerten. Dabei steht die praktische Anwendbarkeit auf viele der aktuell populären *Internet Social Networking Sites* im Vordergrund, für die auch eine Reihe einschlägiger Angriffsvarianten untersucht wird.

Die Bewertung in Abbildung 4.73 zeigt zum einen, dass zwar bereits viele Integrations- und Betriebsaspekte adäquat berücksichtigt wurden, dass aber die Bereiche Anpassung, stufenweiser Aufbau und praktische Umsetzung noch methodisch unterstützt werden sollten. Zum anderen werden zwar bereits einige Managementschnittstellen und -eigenschaften beschrieben, die aber noch nicht alle Bereiche abdecken; die Autoren erwähnen jedoch explizit, dass der Ausbau der Managementschnittstellen Bestandteil der zukünftigen Arbeiten am Security-Framework sein wird. In diesem Kontext sollte auch eine Beurteilung der mit dem Einsatz des Frameworks erreichten Verbesserung des Sicherheitsniveaus vorgenommen werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**1**	2
SF-FUNK-Assets	4	**1**	4
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**1**	2
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		26

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**1**	2
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**1**	1
Summe SF-MGMT	51		21

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**1**	2
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**1**	4
SF-INT-Usablility	2	**1**	2
SF-INT-Wiederverwend.	2	**1**	2
Summe SF-INT	29		27

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**1**	2
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**1**	2
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		30

Bewertungszahlen:			
		SF-FUNK:	1,24
		SF-INT:	0,93
		SF-MGMT:	0,41
Gesamt:	**0,96**	SF-DOKU:	1,25

Abbildung 4.74.: Nutzwertanalyse des Security Framework for Home Network: Authentication, Authorization, and Security Policy ([KLH+07])

Frameworkkategorie:	IT-Architektur	Referenz: [KLH+07]
Frameworkname:	Security Framework for Home Network: Authentication, Authorization, and Security Policy	
Frameworkautoren:	Kim, G. W.; Lee, D. G.; Han, J. W.; Kim, S. C.; Kim, S. W.	

Das 2007 veröffentliche Security-Framework behandelt verschiedene Aspekte der IT-Sicherheit von privaten Hausnetzen, deren Dienstzusammensetzung sich entsprechend von Unternehmensnetzen unterscheidet und Haushaltsgeräte integriert, die im Zusammenhang mit der unternehmensweiten IT-Sicherheit bislang nicht wissenschaftlich aufbereitet wurden. Als Konsequenz aus diesen möglichen Anwendungsszenarien ergibt sich, dass – wie auch der Bewertung in Abbildung 4.74 entnommen werden kann – Managementabläufe nur am Rande und Schnittstellen zu anderen Prozessen nicht behandelt werden, da jedes Hausnetz als autark betrachtet und kein zentrales Management (z. B. für Hotels) in Erwägung gezogen wird.

Der Lösungsansatz ist zwar modular aufgebaut und durch die Erläuterungen der Abläufe verständlich, aber aufgrund der fehlenden Diskussion möglicher Angreifermodelle und der nur groben Skizzierung der betrachteten Angriffe und der getroffenen Designentscheidungen nicht ohne Einschränkungen nachvollziehbar. Eine Weiterentwicklung des Security-Frameworks sollte neben der Berücksichtigung dieser Aspekte insbesondere auch die Schritte zur Umsetzung des Konzepts in eigenen Szenarien behandeln.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**1**	2
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		26

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		19

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**0**	0
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**1**	2
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**1**	4
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**2**	8
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**1**	2
Summe SF-INT	29		27

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**3**	3
Summe SF-DOKU	24		39

Bewertungszahlen:			
		SF-FUNK:	1,24
		SF-INT:	0,93
		SF-MGMT:	0,37
Gesamt:	**1,04**	SF-DOKU:	1,63

Abbildung 4.75.: Nutzwertanalyse des Security framework for integrated networks ([AS03])

Frameworkkategorie:	IT-Dienst	Referenz: [AS03]
Frameworkname:	Security framework for integrated networks	
Frameworkautoren:	Alkassar, A.; Stüble, C.	

Das 2003 veröffentlichte Security-Framework thematisiert unternehmensweite und organisationsübergreifende Netze, die sich primär durch Client-/Server-Kommunikation charakterisieren lassen; dabei spielen auch die Möglichkeiten zur Zusicherung von Quality-of-Service-Parametern eine wesentliche Rolle. Das sehr technisch orientierte Frameworkkonzept sieht eine Multi-Layer-Architektur vor, für die jeweils die einzusetzenden Komponenten und technischen Sicherheitsmaßnahmen vorgestellt werden.

Wie auch in der in Abbildung 4.75 zusammengefassten Bewertung erkennbar ist, wird auf das Management der mit dem Security-Framework geschützten Netze jedoch nicht eingegangen. Auch hinsichtlich einer Implementierung und praktischen Umsetzung werden nur Grobkonzepte vorgestellt. Eine direkte Anwendung des Security-Frameworks in eigenen Szenarien ist somit nicht möglich. Bei der weiteren Entwicklung sollte neben der Diskussion der noch nicht berücksichtigten Aspekte auch noch detaillierter auf die bislang nur angerissenen Themen Erweiterbarkeit, Administrationskonzepte und sicherheitsrelevante Aktionen bzw. Ereignisse eingegangen werden.

Frameworkkategorie:	IT-Architektur	Referenz: [MP05]
Frameworkname:	Security Frameworks for Virtual Organizations	
Frameworkautoren:	Magiera, J.; Pawlak, A.	

Die 2005 als Buchkapitel veröffentlichte Arbeit von Magiera und Pawlak ist eine von wenigen, die den Begriff Security-Framework explizit beschreiben – in diesem Fall als Menge von Methoden, Werkzeugen und Richtlinien, die von einer virtuellen Organisation (VO) angewandt werden sollen, um die gesamte Infrastruktur inklusive Ressourcen, Diensten, Informationen und Benutzern zu schützen. Wie auch aus dem Titel hervorgeht, beschreibt die Arbeit nicht genau ein Security-Framework für VOs, sondern gibt zunächst einen Überblick über integrierte Sicherheitslösungen für VOs, führt anschließend darüber hinaus aber auch eigene Anforderungen und Lösungsansätze aus. Durch die Betrachtung mehrerer Grid-Projekte ergibt sich ein unmittelbarer und konkreter Praxisbezug, so dass einerseits auch explizit auf Aspekte des operativen Managements und andererseits auch ansatzweise auf Auswahlkriterien und Einführungsaspekte bei der szenarienspezifischen Umsetzung eingegangen wird.

Die in Abbildung 4.76 zusammengefasste Beurteilung zeigt, dass zwar bereits viele der bei der Analyse betrachteten Aspekte berücksichtigt wurden, aber noch weitere Verbesserungen anzustreben sind: Beispielsweise wurden die für das Management unmittelbar relevanten technischen Maßnahmen im Bereich Automatisierung und Auditing noch nicht angegangen, und die insbesondere für internationale Kooperationen relevante Compliance-Thematik wurde bislang explizit ausgeklammert. Wünschenswert ist darüber hinaus eine Einbettung der bereits beschriebenen, VO-spezifischen Managementprozesse in das Umfeld bei jeder beteiligten Organisation, die z. B. durch eine Beschreibung der Schnittstellen zu den lokalen ITSM-Prozessen erreicht werden könnte.

Frameworkkategorie:	IT-Architektur	Referenz: [Hua05]
Frameworkname:	Semantic policy-based security framework for business processes	
Frameworkautor:	Huang, D.	

Das 2005 an der Universität Karlsruhe entstandene Security-Framework befasst sich mit den Sicherheitsaspekten, die bei der Unterstützung von Abläufen auf Geschäftsprozessebene durch (z. B. BPEL-basierte) Workflow-Engines ergeben. Die Arbeit geht dabei nicht auf einzelne Dienste, sondern auf web-service- bzw. SOA-basierte Umgebungen im Allgemeinen ein. Der Schwerpunkt liegt auf der Steuerung und Kontrolle der Abläufe über Policies. Aufgrund des Abstraktionsgrads des Frameworkkonzepts fehlen an vielen Stellen Konkretisierungen und Beispiele, so dass eine direkte Anwendung bzw. Übertragung auf eigene Szenarien erheblich erschwert wird. Entsprechend zeigt auch die in Abbildung 4.77 zusammengefasste Bewertung, dass die von den Autoren gewählten Schwerpunkte sehr gut umgesetzt und diverse weitere Aspekte angerissen werden, dass sich jedoch eine größere Anzahl an Anforderungen – insbesondere im Hinblick auf den praktischen Einsatz – aus allen vier Kategorien nicht im Security-Framework wiederfinden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**1**	4
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		42

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**3**	6
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**1**	4
SF-MGMT-Delegation	2	**1**	2
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**1**	2
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**3**	6
SF-MGMT-Praxis	2	**3**	6
SF-MGMT-Prozesse	4	**3**	12
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**1**	2
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		59

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**1**	2
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		51

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**2**	2
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**3**	3
SF-DOKU-Lifecyclephasen	1	**2**	2
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		41

Bewertungszahlen:			
		SF-FUNK:	2,00
		SF-INT:	1,76
		SF-MGMT:	1,16
	Gesamt:	**1,66**	SF-DOKU: 1,71

Abbildung 4.76.: Nutzwertanalyse von Security Frameworks for Virtual Organizations ([MP05])

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**1**	4
SF-FUNK-Auditing	4	**0**	0
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		19

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**0**	0
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**1**	4
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**0**	0
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**3**	6
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**2**	8
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**0**	0
Summe SF-MGMT	51		18

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**0**	0
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**1**	4
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		22

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**1**	2
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**1**	1
SF-DOKU-Lifecyclephasen	1	**1**	1
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**1**	4
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**1**	1
Summe SF-DOKU	24		25

Bewertungszahlen:			
		SF-FUNK:	0,90
		SF-INT:	0,76
		SF-MGMT:	0,35
	Gesamt:	**0,76**	SF-DOKU: 1,04

Abbildung 4.77.: Nutzwertanalyse des semantic policy-based security framework for business processes ([Hua05])

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**2**	4
SF-FUNK-Adaptivität	1	**2**	2
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**3**	12
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**1**	2
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**3**	6
Summe SF-FUNK	21		52

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**1**	4
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**2**	8
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**0**	0
SF-MGMT-Praxis	2	**0**	0
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**1**	1
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		30

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**1**	2
SF-INT-Customizing	4	**2**	8
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		55

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**3**	6
SF-DOKU-Angreifermodelle	2	**3**	6
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**3**	3
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**1**	1
SF-DOKU-Vollständigkeit	2	**2**	4
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		52

Bewertungszahlen:		SF-FUNK:	2,48
		SF-INT:	1,90
		SF-MGMT:	0,59
Gesamt:	**1,78**	SF-DOKU:	2,17

Abbildung 4.78.: Nutzwertanalyse von: Sicherheit in Mobilen Ad hoc Netzwerken ([Kar03])

Frameworkkategorie:	IT-Architektur	Referenz: [Kar03]
Frameworkname:	Sicherheit in Mobilen Ad hoc Netzwerken	
Frameworkautoren:	Kargl, F.	

Die Dissertation von Frank Kargl ist eine der ersten Arbeiten, die sich umfassend mit der Sicherheit von mobilen Ad-hoc Netzen befasst hat. Sie deckt unter anderem die Authentifizierung von Teilnehmern, das Trust Management, die Gerätelokalisierung und die Kommunikationspfadwahl ab; dabei werden insbesondere die dynamischen Strukturen von MANETs und die typischen Ressourcenbeschränkungen der involvierten Geräte berücksichtigt. Das modular aufgebaute Security-Framework liefert diverse eigene Beiträge, unter anderem zur Pseudonymisierung und zum Datenschutz sowie zur Intrusion Detection. Von den vorgeschlagenen Verfahren werden sowohl der Rechen- und Speicheraufwand als auch die Performance analysiert.

Die in Abbildung 4.78 zusammengefasste Bewertung verdeutlicht, dass zwar sowohl die technischen Aspekte als auch die Integrationseigenschaften und die Frameworkdokumentation bereits sehr ausgereift sind, dass die Einbettung ins operative Management und die Betrachtung organisatorischer Aspekte jedoch noch weitestgehend fehlen. Für eine Weiterentwicklung ist darüber hinaus wünschenswert, dass die Lösungsbausteine einem kontinuierlichen Verbesserungsprozess unterzogen werden und dass stärker auf Szenarien bzw. die praktische Anwendung eingegangen wird.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**2**	4
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**1**	4
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**2**	8
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		31

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**1**	2
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**1**	2
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**1**	2
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**3**	12
SF-MGMT-Performanz	2	**3**	6
SF-MGMT-Policies	2	**3**	6
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**3**	12
SF-MGMT-Zuständigkeiten	1	**3**	3
Summe SF-MGMT	51		57

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**0**	0
SF-INT-Erweiterung	2	**2**	4
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**3**	6
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**2**	8
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		47

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**3**	6
SF-DOKU-Kontinuum	1	**2**	2
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		38

Bewertungszahlen:		SF-FUNK:	1,48
		SF-INT:	1,62
		SF-MGMT:	1,12
Gesamt:	**1,45**	SF-DOKU:	1,58

Abbildung 4.79.: Nutzwertanalyse von Toward a Usage-Based Security Framework for Collaborative Computing Systems ([ZCS08])

Frameworkkategorie:	IT-Architektur	Referenz: [ZCS08]
Frameworkname:	Toward a Usage-Based Security Framework for Collaborative Computing Systems	
Frameworkautor:	Zhang, X.; Nakae, M.; Convington, M.; Sandhu, R.	

Das 2008 als Journalartikel veröffentlichte Security-Framework ist auf verteilte Architekturen wie Grids anwendbar und präsentiert ein formales Modell mit den beiden Schwerpunkten Authentifizierung und Zugriffssteuerung. Wie aus dem Titel der untersuchten Arbeit hervorgeht, handelt es sich um ein noch in Entstehung befindliches Gesamtwerk, das beispielsweise vertiefende Administrationskonzepte explizit als Bestandteil der zukünftigen Arbeiten ausweist. Die seit früheren, im Frameworkkonzept referenzierten Arbeiten derselben Autoren vorgenommenen kontinuierlichen Weiterentwicklungen und Verbesserungen sind transparent nachvollziehbar dokumentiert.

Die in Abbildung 4.79 zusammengefasste Bewertung verdeutlicht, dass mehrere Aspekte in allen Anforderungskategorien noch weiter vertieft werden sollten, beispielsweise die Delegationsmechanismen und die Reportingstrukturen. Auch die Vorgehensweise bei der konzeptionellen Anpassung an eigene Szenarien und bei der praktischen Einführung sollten vertiefend erläutert werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**3**	6
SF-FUNK-Adaptivität	1	**3**	3
SF-FUNK-Angriffe	2	**3**	6
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**3**	12
SF-FUNK-Automatisierung	2	**0**	0
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**1**	2
Summe SF-FUNK	21		49

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**2**	4
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**0**	0
SF-MGMT-Delegation	2	**0**	0
SF-MGMT-Events	1	**2**	2
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**1**	2
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**1**	4
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**2**	4
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**0**	0
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**0**	0
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**0**	0
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		22

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0**	0
SF-INT-Customizing	4	**2**	8
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**3**	6
SF-INT-Hochverfügbarkeit	2	**3**	6
SF-INT-Kompatibilität	2	**2**	4
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**3**	3
SF-INT-Skalierbarkeit	4	**3**	12
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**2**	4
Summe SF-INT	29		51

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2**	4
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**2**	4
SF-DOKU-Kontinuum	1	**0**	0
SF-DOKU-Lifecyclephasen	1	**0**	0
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**2**	8
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**3**	12
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		34

Bewertungszahlen:			
		SF-FUNK:	2,33
		SF-INT:	1,76
		SF-MGMT:	0,43
Gesamt:	**1,48**	SF-DOKU:	1,42

Abbildung 4.80.: Nutzwertanalyse des flexible security framework for peer-to-peer based grid computing ([DGBC04])

Frameworkkategorie:	IT-Architektur	Referenz: [DGBC04]
Frameworkname:	Towards a flexible security framework for peer-to-peer based grid computing	
Frameworkautoren:	Detsch, A.; Gaspary, L. P.; Barcellos, M. P.; Cavalheiro, G. G. H.	

Das 2004 im Rahmen des *Workshops on Grid Computing Middleware* vorgestellte Security-Framework thematisiert stark verteilte, nach Peer-to-Peer-Konzepten ausgerichtete Grids; dementsprechend wird verstärkt auf eine dezentrale Selbstorganisation und weniger auf das zentrale Management eingegangen. Konzeptionell fallen insbesondere das klar beschriebene Schichtenmodell und die Schnittstelle zur Infrastruktur bzw. zu den Anwendungen positiv auf.

Zur weiteren Verbesserung des Security-Frameworks, dessen Bewertung in Abbildung 4.80 dargestellt ist, sollten neben noch nicht untersuchten technischen Aspekten wie der Automatisierung und der Performance auch die Auswirkungen des praktischen Einsatzes des Security-Frameworks diskutiert werden. Insbesondere für den Fall, dass sich auch „herkömmliche“ Grid Service Provider an den beschriebenen Peer-to-Peer-Grids beteiligen sollen, müssen die Managementeigenschaften und die Konzepte zur Integration in die vorhandenen Infrastrukturen noch erweitert werden.

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**0**	0
SF-FUNK-Adaptivität	1	**1**	1
SF-FUNK-Angriffe	2	**0**	0
SF-FUNK-Assets	4	**2**	8
SF-FUNK-Auditing	4	**2**	8
SF-FUNK-Automatisierung	2	**2**	4
SF-FUNK-Maßnahmen	4	**3**	12
SF-FUNK-Schwachstellen	2	**0**	0
Summe SF-FUNK	21		33

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1**	2
SF-MGMT-Berichtsdetails	2	**0**	0
SF-MGMT-Compliance	4	**1**	4
SF-MGMT-Delegation	2	**2**	4
SF-MGMT-Events	1	**1**	1
SF-MGMT-ITSM-Schnittstellen	4	**0**	0
SF-MGMT-Kosten	2	**0**	0
SF-MGMT-KPIs	1	**0**	0
SF-MGMT-Mandantenfähigkeit	2	**0**	0
SF-MGMT-Metriken	4	**0**	0
SF-MGMT-Operationen	4	**0**	0
SF-MGMT-Performanz	2	**0**	0
SF-MGMT-Policies	2	**1**	2
SF-MGMT-Praxis	2	**2**	4
SF-MGMT-Prozesse	4	**1**	4
SF-MGMT-Quantifizierung	2	**0**	0
SF-MGMT-Releasezyklus	2	**0**	0
SF-MGMT-Schulungen	2	**0**	0
SF-MGMT-Support	1	**3**	3
SF-MGMT-Tests	1	**0**	0
SF-MGMT-Verbesserung	4	**2**	8
SF-MGMT-Zuständigkeiten	1	**2**	2
Summe SF-MGMT	51		34

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**2**	4
SF-INT-Customizing	4	**1**	4
SF-INT-Einführung	2	**1**	2
SF-INT-Erweiterung	2	**1**	2
SF-INT-Hochverfügbarkeit	2	**0**	0
SF-INT-Kompatibilität	2	**0**	0
SF-INT-Modularität	2	**3**	6
SF-INT-Parallelbetrieb	4	**0**	0
SF-INT-Polyinstanziierbark.	1	**0**	0
SF-INT-Skalierbarkeit	4	**0**	0
SF-INT-Usablility	2	**0**	0
SF-INT-Wiederverwend.	2	**3**	6
Summe SF-INT	29		24

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**0**	0
SF-DOKU-Angreifermodelle	2	**0**	0
SF-DOKU-Ausrichtung	2	**2**	4
SF-DOKU-Beurteilung	1	**0**	0
SF-DOKU-Checkliste	1	**0**	0
SF-DOKU-Designentscheid.	2	**1**	2
SF-DOKU-Kontinuum	1	**2**	2
SF-DOKU-Lifecyclephasen	1	**1**	1
SF-DOKU-Vollständigkeit	2	**0**	0
SF-DOKU-Voraussetzungen	4	**1**	4
SF-DOKU-Zertifizierung	1	**0**	0
SF-DOKU-Ziele	4	**2**	8
SF-DOKU-Zielgruppe	1	**2**	2
Summe SF-DOKU	24		23

Bewertungszahlen:		SF-FUNK:	1,57
		SF-INT:	0,83
		SF-MGMT:	0,67
Gesamt:	**1,01**	SF-DOKU:	0,96

Abbildung 4.81.: Nutzwertanalyse des Unified Security Framework ([WT03])

Frameworkkategorie:	IT-Architektur	Referenz: [WT03]
Frameworkname:	Unified security framework	
Frameworkautoren:	Wilson, G.; Tharakan, U. O.	

Der 2003 entstandene Artikel gibt einen groben Überblick über den unternehmensweiten Einsatz von Security-Frameworks, zu dem die Autoren entsprechende Beratungsdienstleistungen anbieten. Das skizzierte Security-Frameworks wendet sich sowohl an Systemarchitekten als auch die Leitungsebene (z. B. CIO). Es zielt auf ein anwendungsübergreifendes, unternehmensweites Management ab und basiert auf dem systemübergreifenden Einsatz u. a. von Access Management, Firewalls und Anti-Virussoftware sowie der Nutzung von Delegationskonzepten. Positiv ist anzumerken, dass die Arbeit im Unterschied zu den meisten anderen explizit auf Ziele aus Managementperspektive eingeht. Die Abbildung 4.81 zu entnehmenden Abstriche ergeben sich vorrangig aus der Knappheit der Darstellung, durch die auf viele Aspekte nicht oder nur sehr oberflächlich eingegangen wird.

Kriterium	0 Punkte	1 Punkt	2 Punkte	3 Punkte	Summe	Durchschnitt
SF-FUNK-Abschottung	22	3	6	45	150	**1,97**
SF-FUNK-Adaptivität	10	6	34	26	152	**2,00**
SF-FUNK-Angriffe	20	19	10	27	120	**1,58**
SF-FUNK-Assets	0	13	30	33	172	**2,26**
SF-FUNK-Auditing	37	8	17	14	84	**1,11**
SF-FUNK-Automatisierung	24	11	33	8	101	**1,33**
SF-FUNK-Maßnahmen	0	7	26	43	188	**2,47**
SF-FUNK-Schwachstellen	32	18	16	10	80	**1,05**
Summe SF-FUNK	145	85	172	206	1047	**1,72**
SF-MGMT-Adminkonzepte	18	17	30	11	110	**1,45**
SF-MGMT-Berichtsdetails	66	9	1	0	11	**0,14**
SF-MGMT-Compliance	56	12	5	3	31	**0,41**
SF-MGMT-Delegation	57	8	7	4	34	**0,45**
SF-MGMT-Events	34	22	17	3	65	**0,86**
SF-MGMT-ITSM-Schnittstellen	71	4	0	1	7	**0,09**
SF-MGMT-Kosten	72	2	1	1	7	**0,09**
SF-MGMT-KPIs	62	13	1	0	15	**0,20**
SF-MGMT-Mandantenfähigkeit	67	3	4	2	17	**0,22**
SF-MGMT-Metriken	71	4	1	0	6	**0,08**
SF-MGMT-Operationen	18	17	35	6	105	**1,38**
SF-MGMT-Performanz	34	10	8	24	98	**1,29**
SF-MGMT-Policies	26	12	27	11	99	**1,30**
SF-MGMT-Praxis	17	21	27	11	108	**1,42**
SF-MGMT-Prozesse	29	25	19	3	72	**0,95**
SF-MGMT-Quantifizierung	65	8	2	1	15	**0,20**
SF-MGMT-Releasezyklus	68	4	1	3	15	**0,20**
SF-MGMT-Schulungen	60	9	4	3	26	**0,34**
SF-MGMT-Support	61	0	5	10	40	**0,53**
SF-MGMT-Tests	68	8	0	0	8	**0,11**
SF-MGMT-Verbesserung	45	5	18	8	65	**0,86**
SF-MGMT-Zuständigkeiten	21	10	39	6	106	**1,39**
Summe SF-MGMT	1086	223	252	111	1060	**0,63**

Kriterium	0 Punkte	1 Punkt	2 Punkte	3 Punkte	Summe	Durchschnitt
SF-INT-Ausbauphasen	44	19	10	3	48	**0,63**
SF-INT-Customizing	33	30	11	2	58	**0,76**
SF-INT-Einführung	25	40	11	0	62	**0,82**
SF-INT-Erweiterung	25	21	23	7	88	**1,16**
SF-INT-Hochverfügbarkeit	55	12	7	2	32	**0,42**
SF-INT-Kompatibilität	12	9	36	19	138	**1,82**
SF-INT-Modularität	7	3	19	47	182	**2,39**
SF-INT-Parallelbetrieb	46	12	14	4	52	**0,68**
SF-INT-Polyinstanziierbark.	14	1	4	57	180	**2,37**
SF-INT-Skalierbarkeit	10	9	25	32	155	**2,04**
SF-INT-Usablility	48	15	7	6	47	**0,62**
SF-INT-Wiederverwend.	16	10	31	19	129	**1,70**
Summe SF-INT	335	181	198	198	1171	**1,28**
SF-DOKU-Anford.-analyse	4	15	31	26	155	**2,04**
SF-DOKU-Angreifermodelle	46	13	8	9	56	**0,74**
SF-DOKU-Ausrichtung	0	1	56	19	170	**2,24**
SF-DOKU-Beurteilung	47	8	17	4	54	**0,71**
SF-DOKU-Checkliste	69	3	2	2	13	**0,17**
SF-DOKU-Designentscheid.	6	6	42	22	156	**2,05**
SF-DOKU-Kontinuum	48	10	13	5	51	**0,67**
SF-DOKU-Lifecyclephasen	57	11	7	1	28	**0,37**
SF-DOKU-Vollständigkeit	56	8	9	3	35	**0,46**
SF-DOKU-Voraussetzungen	6	8	50	12	144	**1,89**
SF-DOKU-Zertifizierung	69	5	2	0	9	**0,12**
SF-DOKU-Ziele	0	1	21	54	205	**2,70**
SF-DOKU-Zielgruppe	4	5	54	13	152	**2,00**
Summe SF-DOKU	412	94	312	170	1228	**1,24**

Hinweis:
In den einzelnen Spalten wird angegeben, wie oft 0, 1, 2 bzw. 3 Punkte für das jeweilige Kriterium vergeben wurden, welche Gesamtpunktezahl und welche durchschnittlich vergebene Punktezahl sich daraus ergeben.

Abbildung 4.82.: Pro Kriterium vergebene Punkte sowie deren gewichtete Summe und Durchschnitt

4.5. Auswertung der Security-Framework-Analyse

Nach der detaillierten Vorstellung der Analysen von zwei Security-Frameworks sowie der Kurzdarstellung der Untersuchungen von 74 weiteren Security-Frameworks in den vorherigen Abschnitten wird nachfolgend aufbereitet und diskutiert, welche Konsequenzen aus diesen Ergebnissen für die Schwerpunkte dieser Arbeit zu ziehen sind. Bevor in den Abschnitten 4.5.1 und 4.5.2 auf die pro Anforderungskategorie häufig anzutreffenden Stärken und Verbesserungsmöglichkeiten bzw. in Abschnitt 4.5.3 auf die Konsequenzen näher eingegangen wird, werden einleitend zur Verschaffung eines Überblick einige **grundlegende Auswertungen** vorgenommen.

Abbildung 4.82 zeigt zunächst zusammenfassend, wie oft jedes Beurteilungskriterium mit 0, 1, 2 bzw. 3 Punkten bewertet wurde. Wie als Selektionskriterium in Abschnitt 4.1.2.1 definiert wurde, wurden nur Security-Frameworks untersucht, die die Anforderungen *SF-FUNK-Assets* und *SF-FUNK-Maßnahmen* mindestens partiell erfüllen; darüber hinaus wurde – ohne dass dies ein Ausschlusskriterium gewesen wäre – kein Framework untersucht, dessen Ausrichtung oder Zielsetzung (vgl. entsprechende Kriterien in Kategorie SF-DOKU) gänzlich unklar waren. In der Abbildung sind darüber hinaus jeweils die gewichtete Punktesumme und die durchschnittliche Punktezahl pro Kriterium angegeben.

Die ebenfalls in Abbildung 4.82 für jede der vier Anforderungskategorien aufgeführten durchschnittlichen Punktezahlen zeigt bereits deutlich, dass der technische bzw. sicherheitsfunktionale Bereich (*SF-FUNK*) nicht nur derjenige ist, der die besten Bewertungen erhält, sondern als einziger auch eine über dem Erwartungswert (1,5 Punkte) liegende Gesamtbeurteilung erhält. Die beiden Anforderungskategorien *SF-INT* und *SF-DOKU* schneiden in etwa gleich und bezüglich ihrer Durchschnittspunktezahl knapp unter dem Erwartungswert ab. **Sehr deutliche Defizite** zeigen sich jedoch in der Anforderungskategorie *SF-MGMT*, in der auch

Kriterium	G-Faktor	Punkte	G * P
SF-FUNK-Abschottung	2	**1,97**	3,94
SF-FUNK-Adaptivität	1	**2,00**	2
SF-FUNK-Angriffe	2	**1,58**	3,16
SF-FUNK-Assets	4	**2,26**	9,04
SF-FUNK-Auditing	4	**1,11**	4,44
SF-FUNK-Automatisierung	2	**1,33**	2,66
SF-FUNK-Maßnahmen	4	**2,47**	9,88
SF-FUNK-Schwachstellen	2	**1,05**	2,1
Summe SF-FUNK	21		37,22

Kriterium	G-Faktor	Punkte	G * P
SF-MGMT-Adminkonzepte	2	**1,45**	2,9
SF-MGMT-Berichtsdetails	2	**0,14**	0,28
SF-MGMT-Compliance	4	**0,41**	1,64
SF-MGMT-Delegation	2	**0,45**	0,9
SF-MGMT-Events	1	**0,86**	0,86
SF-MGMT-ITSM-Schnittstellen	4	**0,09**	0,36
SF-MGMT-Kosten	2	**0,09**	0,18
SF-MGMT-KPIs	1	**0,20**	0,2
SF-MGMT-Mandantenfähigkeit	2	**0,22**	0,44
SF-MGMT-Metriken	4	**0,08**	0,32
SF-MGMT-Operationen	4	**1,38**	5,52
SF-MGMT-Performanz	2	**1,29**	2,58
SF-MGMT-Policies	2	**1,30**	2,6
SF-MGMT-Praxis	2	**1,42**	2,84
SF-MGMT-Prozesse	4	**0,95**	3,8
SF-MGMT-Quantifizierung	2	**0,20**	0,4
SF-MGMT-Releasezyklus	2	**0,20**	0,4
SF-MGMT-Schulungen	2	**0,34**	0,68
SF-MGMT-Support	1	**0,53**	0,53
SF-MGMT-Tests	1	**0,11**	0,11
SF-MGMT-Verbesserung	4	**0,86**	3,44
SF-MGMT-Zuständigkeiten	1	**1,39**	1,39
Summe SF-MGMT	51		32,37

Kriterium	G-Faktor	Punkte	G * P
SF-INT-Ausbauphasen	2	**0,63**	1,26
SF-INT-Customizing	4	**0,76**	3,04
SF-INT-Einführung	2	**0,82**	1,64
SF-INT-Erweiterung	2	**1,16**	2,32
SF-INT-Hochverfügbarkeit	2	**0,42**	0,84
SF-INT-Kompatibilität	2	**1,82**	3,64
SF-INT-Modularität	2	**2,39**	4,78
SF-INT-Parallelbetrieb	4	**0,68**	2,72
SF-INT-Polyinstanziierbark.	1	**2,37**	2,37
SF-INT-Skalierbarkeit	4	**2,04**	8,16
SF-INT-Usablility	2	**0,62**	1,24
SF-INT-Wiederverwend.	2	**1,70**	3,4
Summe SF-INT	29		35,41

Kriterium	G-Faktor	Punkte	G * P
SF-DOKU-Anford.-analyse	2	**2,04**	4,08
SF-DOKU-Angreifermodelle	2	**0,74**	1,48
SF-DOKU-Ausrichtung	2	**2,24**	4,48
SF-DOKU-Beurteilung	1	**0,71**	0,71
SF-DOKU-Checkliste	1	**0,17**	0,17
SF-DOKU-Designentscheid.	2	**2,05**	4,1
SF-DOKU-Kontinuum	1	**0,67**	0,67
SF-DOKU-Lifecyclephasen	1	**0,37**	0,37
SF-DOKU-Vollständigkeit	2	**0,46**	0,92
SF-DOKU-Voraussetzungen	4	**1,89**	7,56
SF-DOKU-Zertifizierung	1	**0,12**	0,12
SF-DOKU-Ziele	4	**2,70**	10,8
SF-DOKU-Zielgruppe	1	**2,00**	2
Summe SF-DOKU	24		37,46

Bewertungszahlen:		SF-FUNK:	1,77
		SF-INT:	1,22
		SF-MGMT:	0,63
Gesamt:	**1,30**	SF-DOKU:	1,56

Abbildung 4.83.: Nutzwertanalyse auf Basis der Durchschnittspunktezahlen pro Kriterium

elf Kriterien enthalten sind, die von 60 oder mehr Security-Frameworks bislang nicht erfüllt sind (0 Punkte). Die Abbildung zeigt darüber hinaus, dass es in den Kategorien *SF-INT*, *SF-MGMT* und *SF-DOKU* zusammen insgesamt sechs Kriterien gibt, die von keinem der untersuchten Security-Frameworks vollständig erfüllt werden (3 Punkte); in Abschnitt 4.5.2 wird deshalb nochmals auf die Relevanz dieser Kriterien und die praktischen Auswirkungen beim Einsatz der Security-Frameworks eingegangen.

In Abbildung 4.83 wurden die oben diskutierten durchschnittlichen Punktezahlen als Eingabe für die bereits pro Security-Framework durchgeführte Nutzwertanalyse verwendet. Sie zeigt somit die Analyseergebnisse unter Berücksichtigung der Gewichtung der einzelnen Anforderungen. Erwartungsgemäß erreicht die Kategorie *SF-FUNK* auch hierbei die höchste Bewertungszahl; allerdings schneidet bei dieser Auswertung auch *SF-DOKU* etwas über dem Erwartungswert von $1,5$ ab, d. h. die wichtigeren Dokumentationsaspekte werden von den Frameworkautoren insgesamt besser berücksichtigt als die im Rahmen der Anforderungsanalyse lediglich als *wünschenswert* eingestuften. Mit wiederum sehr deutlichem Abstand wird die Kategorie *SF-MGMT* jedoch am schlechtesten bewertet.

Schließlich zeigt Abbildung 4.84 alle Anforderungen absteigend nach ihrer Durchschnittspunktezahl sortiert. Bei dieser Tabelle, die somit über die am besten bzw. am wenigsten erfüllten Anforderungen Auskunft erteilt, fällt insbesondere auf, dass *SF-MGMT-Adminkonzepte*

als insgesamt am besten beurteilte Anforderung der Kategorie *SF-MGMT* abgeschlagen auf Platz 17 liegt. Somit zeigt sich bereits durchgängig, dass insbesondere im Bereich der Managementprozesse, -operationen und -schnittstellen ein umfassendes Verbesserungspotenzial identifiziert wurde.

Auf eine vertiefende, vergleichende Gegenüberstellung der Security-Frameworks, die Gesamtbewertungszahlen zwischen $0,35$ und $2,17$ erhalten haben, wird an dieser Stelle bewusst verzichtet, da das vorrangige Ziel der Untersuchungen ist, aus der Ermittlung bereits ausgeprägter Stärken und noch vorhandener Schwächen allgemeine **Maßnahmen zur Verbesserung zukünftiger Security-Frameworks** abzuleiten. Es muss jedoch angemerkt werden, dass in der Regel ausführlich dokumentierte Security-Frameworks mehr Kriterien erfüllen und somit auch insgesamt besser beurteilt werden als knapp gehaltene Frameworkkonzepte. Allerdings gibt es diesbezüglich auch Ausnahmen und im Hinblick auf die praktische Anwendbarkeit der analysierten Security-Frameworks liegt mit dem Umfang ihrer Dokumentation keine Kennzahl vor, aus der ein Korrekturfaktor für die Gesamtbeurteilung abgeleitet werden sollte. Vielmehr dient das einheitliche Bewertungsschema genau dazu, die im Einzelfall zu berücksichtigenden Verbesserungsmaßnahmen zu identifizieren, und kann bei der Vorauswahl zwischen mehreren ähnlichen Security-Frameworks uneingeschränkt herangezogen werden.

4.5.1. Häufige Stärken von Security-Frameworks

Erfreulicherweise lassen sich nicht nur vielen Security-Frameworks individuelle Stärken attestieren, sondern es gibt eine Reihe von Anforderungen, die über alle untersuchten Frameworks hinweg betrachtet überdurchschnittlich gut erfüllt werden. Im Folgenden werden diese Stärken nach Anforderungskategorie sortiert und ihre Auswirkungen auf die Auswahl und den Einsatz von Security-Frameworks kurz diskutiert.

Wie oben schon bei der allgemeinen Auswertung erläutert wurde, ist der technische, sicherheitsfunktionale Bereich **SF-FUNK** derjenige mit den insgesamt besten Bewertungen. Es ist zugleich der einzige, bei dem alle Anforderungen eine Durchschnittspunktezahl über $1,00$ erreicht haben. Die höchsten Bewertungen erreichen dabei *SF-FUNK-Maßnahmen* und *SF-FUNK-Assets*, so dass einerseits anhand des durch die angegebenen Assets spezifizierten Schutzbereichs effizient entschieden werden kann, ob das Security-Framework zum eigenen Szenario passt; andererseits werden solide, zum Schutzbereich passende Lösungsbausteine vorgegeben, woraus sich der unmittelbare technische Mehrwert des Einsatzes von Security-Frameworks ergibt. Die Durchschnittspunktezahl $2,00$ für *SF-FUNK-Adaptivität* verdeutlicht zudem, dass nicht nur starre Lösungsarchitekturen, sondern durchaus explizit flexible Lösungen, die während des Betriebs an sich ändernde Anforderungen angepasst werden können, geschaffen wurden. Insgesamt kann damit festgehalten werden, dass die Frameworkautoren im Allgemeinen durchaus mindestens technisch passende Lösungen für einen jeweils genauer umrissenen Problembereich liefern, ohne dabei auf konzeptioneller Ebene zu spezifisch oder zu starr zu werden.

Im Bereich der Integrations- und Betriebsanforderungen **SF-INT** zeigt sich mit der sehr guten Bewertung von *SF-INT-Modularität* zunächst, dass fast alle Security-Frameworks dem bereits diskutierten Baukastenprinzip folgen und vorhandene wie auch eigene neue Komponenten miteinander verbinden. Durch die Kapselung jedes Bausteins und die häufig angebotene Auswahl aus verschiedenen Implementierungen eines Moduls wird die szenarienspezifische

Kriterium	Durchschnittspunktezahl	Gesamtpunktezahl
SF-DOKU-Ziele	2,70	205
SF-FUNK-Maßnahmen	2,47	188
SF-INT-Modularität	2,39	182
SF-INT-Polyinstanziierbark.	2,37	180
SF-FUNK-Assets	2,26	172
SF-DOKU-Ausrichtung	2,24	170
SF-DOKU-Designentscheid.	2,05	156
SF-DOKU-Anford.-analyse	2,04	155
SF-INT-Skalierbarkeit	2,04	155
SF-DOKU-Zielgruppe	2,00	152
SF-FUNK-Adaptivität	2,00	152
SF-FUNK-Abschottung	1,97	150
SF-DOKU-Voraussetzungen	1,89	144
SF-INT-Kompatibilität	1,82	138
SF-INT-Wiederverwend.	1,70	129
SF-FUNK-Angriffe	1,58	120
SF-MGMT-Adminkonzepte	1,45	110
SF-MGMT-Praxis	1,42	108
SF-MGMT-Zuständigkeiten	1,39	106
SF-MGMT-Operationen	1,38	105
SF-FUNK-Automatisierung	1,33	101
SF-MGMT-Policies	1,30	99
SF-MGMT-Performanz	1,29	98
SF-INT-Erweiterung	1,16	88
SF-FUNK-Auditing	1,11	84
SF-FUNK-Schwachstellen	1,05	80
SF-MGMT-Prozesse	0,95	72
SF-MGMT-Events	0,86	65
SF-MGMT-Verbesserung	0,86	65
SF-INT-Einführung	0,82	62
SF-INT-Customizing	0,76	58
SF-DOKU-Angreifermodelle	0,74	56
SF-DOKU-Beurteilung	0,71	54
SF-INT-Parallelbetrieb	0,68	52
SF-DOKU-Kontinuum	0,67	51
SF-INT-Ausbauphasen	0,63	48
SF-INT-Usablility	0,62	47
SF-MGMT-Support	0,53	40
SF-DOKU-Vollständigkeit	0,46	35
SF-MGMT-Delegation	0,45	34
SF-INT-Hochverfügbarkeit	0,42	32
SF-MGMT-Compliance	0,41	31
SF-DOKU-Lifecyclephasen	0,37	28
SF-MGMT-Schulungen	0,34	26
SF-MGMT-Mandantenfähigkeit	0,22	17
SF-MGMT-Kosten	0,20	15
SF-MGMT-Quantifizierung	0,20	15
SF-MGMT-Releasezyklus	0,20	15
SF-DOKU-Checkliste	0,17	13
SF-MGMT-Berichtsdetails	0,14	11
SF-DOKU-Zertifizierung	0,12	9
SF-MGMT-Tests	0,11	8
SF-MGMT-ITSM-Schnittstellen	0,09	7
SF-MGMT-KPIs	0,09	7
SF-MGMT-Metriken	0,08	6

Abbildung 4.84.: Beurteilungskriterien nach Durchschnittspunktezahlen abnehmend sortiert

Umsetzung eines Security-Frameworks bereits grundlegend flexibilisiert. Die ebenfalls sehr guten Bewertungen von *SF-INT-Polyinstanziierbarkeit* und *SF-INT-Skalierbarkeit* belegen, dass die meisten Security-Frameworks den an sie gestellten Anforderungen gerecht werden, nicht nur für kleine lokale Beispielszenarien der Frameworkautoren maßgeschneidert zu sein, sondern in verschiedenen Ausprägungen auch in großen und komplexen Szenarien eingesetzt werden zu können. Schließlich wird – verdeutlicht durch die über dem Erwartungswert liegenden Bewertungen von *SF-INT-Kompatibilität* und *SF-INT-Wiederverwendbarkeit* – von den Security-Frameworks meist auch explizit Wert auf das technische Zusammenspiel der vorgeschlagenen Lösungskomponenten mit den zu erwartenden bereits vorhandenen Komponenten gelegt, die nach Möglichkeit nicht redundant aufgebaut werden müssen.

Obwohl es sich bei der Kategorie **SF-MGMT** um die insgesamt am schlechtesten bewertete handelt, werden einige Aspekte zumindest so weit berücksichtigt, dass ihre Durchschnittsbewertung nur knapp unter dem Erwartungswert liegt. Die gute Bewertung von *SF-MGMT-Administrationskonzepte* verdeutlicht zwar einerseits, dass für viele Security-Frameworks im Bereich des IT-Managements zwar die technisch-operativen Abläufe im Vordergrund stehen; andererseits werden den Frameworkanwendern damit aber auch wichtige Informationen für den laufenden Betrieb mit auf den Weg gegeben, deren Zusammenspiel mit den im jeweiligen Szenario bereits etablierten Administrationskonzepten durchaus ein zentrales Selektionskriterium sein kann. Dass es sich bei Security-Frameworks im Allgemeinen nicht um rein theoretische Konstrukte handelt, belegt die gute Bewertung von *SF-MGMT-Praxis*: Viele der untersuchten Frameworks sind in mindestens einem realen Szenario bereits erprobt worden und es liegen zumindest von den Frameworkautoren selbst knapp dokumentierte Erfahrungsberichte vor. Die organisatorische Umsetzung wird zumindest dadurch ein wenig erleichtert, dass die als *wünschenswert* gewichtete Anforderung *SF-MGMT-Zuständigkeiten* ebenfalls gut erfüllt wird: Bei mehr als der Hälfte der untersuchten Security-Frameworks bleiben keine Unklarheiten, welche Personenkreise fachlich für die einzelnen Bestandteile verantwortlich sind. Die ebenfalls noch gute Bewertung von *SF-MGMT-Operationen* wirkt sich insbesondere aufgrund der deutlich schlechteren Bewertungen von *SF-MGMT-Schulungen* und *SF-MGMT-Support* positiv darauf aus, dass zumindest die für das operative Management der Komponenten des Security-Frameworks Zuständigen auf definierte Abläufe zurückgreifen können.

Im Bezug auf die Dokumentation der Security-Frameworks (Kategorie **SF-DOKU**) sticht zunächst heraus, dass ausnahmslos alle Security-Frameworks die von ihnen verfolgten Ziele darstellen: Die Anforderung *SF-DOKU-Ziele* ist über alle Kategorien hinweg die mit Abstand am besten bewertete. Für die praktische Anwendung folgt daraus, dass im Allgemeinen sehr effizient bestimmt werden kann, ob sich ein Security-Framework prinzipiell für die vom Frameworkanwender im konkreten Szenario verfolgten Ziele eignet oder ob bereits vor einer vertiefenden Betrachtung auf Alternativen ausgewichen werden muss. Diese Entscheidung wird auch dadurch erleichtert, dass wiederum ausnahmslos klar wird, welche inhaltliche Ausrichtung das Security-Framework im Bezug auf den Lebenszyklus von Angriffen verfolgt: Durch die insgesamt sehr gute Bewertung von *SF-DOKU-Ausrichtung* kann im Allgemeinen mühelos bestimmt werden, ob ein Security-Framework nur einige oder alle Phasen von der Prävention über die Detektion bis hin zur Reaktion auf Angriffe abdeckt; allerdings ist anzumerken, dass diese positive Eigenschaft darauf beschränkt ist, dass diese Ausrichtung an sich erkenntlich wird – in vielen Fällen beschränken sich Security-Frameworks auf die Prävention von erfolgreichen Angriffen, bleiben Erkennungsmaßnahmen und insbesondere adäquate Reaktionen darauf jedoch schuldig. Die Anforderungskategorie *SF-DOKU* ist zudem diejenige, welche

die meisten Anforderungen mit einer Durchschnittspunktezahl von 2,00 oder höher enthält. Wie sich durch die sehr guten Bewertungen der beiden entsprechenden Anforderungen zeigt, werden auch die *Anforderungsanalysen* und die *Designentscheidungen* in den meisten Fällen sehr gut nachvollziehbar dokumentiert, so dass der potentielle Frameworkanwender seine eigenen Anforderungen den bereits berücksichtigten gut gegenüberstellen und prüfen kann, ob er für sein Szenario dieselben Konsequenzen gezogen hätte. Schließlich wird – untermauert durch die sehr gute Bewertung der Anforderung *SF-DOKU-Zielgruppe* – mit nur wenigen Ausnahmen immer deutlich, welcher Leserkreis vom Frameworkkonzept angesprochen wird, so dass auch effizient bestimmt werden kann, ob beispielsweise für die Genehmigungsphase der Frameworkumsetzung zunächst eine ans Management gerichtete Zusammenfassung der Ziele und Maßnahmen erstellt werden muss oder ob – wie durchaus in einigen Fällen gegeben – entsprechende Textabschnitte bereits vorhanden sind.

Zusammenfassend lässt sich verallgemeinern, dass Security-Frameworks auch bislang schon sehr gute und flexible technischen Lösungsansätze darstellen, die modular aufgebaut sind und sich aufgrund ihrer technischen Schnittstellen prinzipiell gut in vorhandene Infrastrukturen integrieren lassen. Die szenarienspezifische Beurteilung wird dabei durch eine klare Beschreibung der jeweiligen Zielsetzungen, Anforderungen und Designentscheidungen unterstützt; analog dazu werden einige zentrale Aspekte des operativen Managements wie die relevanten Managementoperationen und die zugrunde gelegten Administrationskonzepte mit einem erkennbaren Praxisbezug bereits relativ gut berücksichtigt.

Im folgenden Abschnitt wird erörtert, dass trotz dieses positiven Grundtenors eine Reihe von Aspekten identifiziert wurde, bei denen noch ein dringender Verbesserungsbedarf besteht.

4.5.2. Typische Schwächen von Security-Frameworks

In allen vier Kategorien gibt es Anforderungen, die von der Mehrheit der analysierten Security-Frameworks nicht oder nur partiell (0 bzw. 1 Punkte) erfüllt werden. Diese Anforderungen liefern folglich einerseits nunmehr offensichtliche Anregungen und Ansatzpunkte für die konkrete Verbesserung und Weiterentwicklungen der Security-Frameworks. Andererseits existieren Anforderungen, die bislang nur von so wenigen der untersuchten Arbeiten und nur ansatzweise erfüllt wurden, dass die Hintergründe dafür zu untersuchen sind – denn entweder handelt es sich um Aspekte, bei denen bislang tatsächlich fast alle Security-Frameworks erhebliche Defizite aufweisen, oder die praktische Relevanz der jeweiligen Anforderung ist nicht gegeben. Im Folgenden werden diese Punkte wiederum nach Anforderungskategorien getrennt diskutiert.

Im insgesamt am besten bewerteten Bereich **SF-FUNK** hat die Anforderung *SF-FUNK-Schwachstellen* die niedrigste Durchschnittspunktezahl und 20 der untersuchten Security-Frameworks erfüllen auch die damit relativ eng verbundene Anforderung *SF-FUNK-Angriffe* nicht. Insbesondere wenn diese Anforderungen beide nicht oder nicht ausreichend erfüllt sind, befindet sich der Frameworkanwender in der Situation, ein in der Regel sehr gut zu seinen Infrastrukturkomponenten (vgl. Durchschnittsbewertung von *SF-FUNK-Assets*) passendes Frameworkkonzept vorliegen zu haben, in dem umfassende und insbesondere technisch ausgereifte Maßnahmen vorgeschlagen werden (vgl. *SF-FUNK-Maßnahmen*), ohne aber unmittelbar beurteilen zu können, ob diese Maßnahmen zu den ihm bekannten Schwachstellen und den in seinem Szenario erwarteten Angriffen passen. In Abhängigkeit von anderen Faktoren wie der vom Frameworkkonzept untersuchten eigenen Vollständigkeit (vgl. *SF-DOKU-Vollständigkeit*) er-

höht sich damit der szenarienspezifische Aufwand zur Evaluation der Eignung des jeweiligen Security-Frameworks.

Auch die Anforderung *SF-FUNK-Auditing* wird von knapp der Hälfte der untersuchten Security-Frameworks nicht erfüllt (0 Punkte). Damit ist nicht nur verbunden, dass geeignete Maßnahmen zur Überwachung und Auswertung des Frameworkeinsatzes szenarienspezifisch sowohl konzeptionell als auch implementierungsseitig zu ergänzen sind. Vielmehr handelt es sich um ein Symptom für die rein technisch-präventive Ausrichtung vieler Security-Frameworks, d. h. dem Anwender werden Maßnahmen an die Hand gegeben, um viele Arten erfolgreicher Angriffe zu verhindern, es fehlen jedoch ergänzende Maßnahmen, um andere dennoch erfolgreiche Angriffe zu erkennen und geeignet – insbesondere also auch zum Framework passend – darauf zu reagieren. Analog dazu wird auch die Automatisierung der sicherheitsspezifischen Maßnahmen (vgl. *SF-FUNK-Automatisierung*) von knapp der Hälfte der untersuchten Security-Frameworks nur unzureichend thematisiert; in Kombination mit der völlig unzureichenden Untersuchung der mit dem Frameworkbetrieb verbundenen Kosten (vgl. *SF-MGMT-Kosten*) droht somit bei vielen Security-Frameworks die Gefahr, komplexe Sicherheitsmaßnahmen umzusetzen, von denen a priori nicht bekannt ist, in welchem Umfang sie dauerhaft manuellen Administrationsaufwand binden werden. Entsprechende konzeptionelle Untersuchungen und praktische Automatisierungsmaßnahmen müssen deshalb in vielen Fällen von Grund auf szenarienspezifisch erbracht werden.

In der Anforderungskategorie **SF-INT** fällt zunächst auf, dass jeweils rund zwei Drittel der Security-Frameworks nicht auf die Themen Hochverfügbarkeit und Benutzerfreundlichkeit (vgl. *SF-INT-Hochverfügbarkeit* und *SF-INT-Usability*) eingehen. Dabei überrascht die mangelhafte Berücksichtigung von Hochverfügbarkeitskonzepten besonders, zumal die Verfügbarkeit von Daten und Diensten eines der Grundziele der IT-Sicherheit ist und viele technische Teilaspekte hat (vgl. Abschnitt 2.1.1.1). Dies erschwert die praktische Umsetzung von Security-Frameworks insbesondere in solchen Szenarien, in denen die zu schützenden Dienste bereits geeignet hochverfügbar ausgelegt wurden und die Dienstqualität durch *single points of failure* der Sicherheitsmaßnahmen nicht beeinträchtigt werden darf. Bezüglich *SF-INT-Usability* bestätigt sich, dass sich insbesondere technische Sicherheitsmaßnahmen oft gegenläufig zur Benutzerfreundlichkeit verhalten (vgl. Abschnitt 2.3); als Konsequenz daraus muss jeweils szenarienspezifisch untersucht werden, ob die sich aus dem Einsatz des Security-Frameworks in den Abläufen ergebenden Einschränkungen den Administratoren und Benutzern zugemutet werden können.

Noch erheblich schwerwiegender ist jedoch, dass die Anforderungen *SF-INT-Customizing*, *SF-INT-Einführung* und *SF-INT-Ausbauphasen* nur unzureichend erfüllt werden; dabei ist *SF-INT-Einführung* eine der insgesamt sechs in dieser Arbeit postulierten Anforderungen, die von keinem einzigen der untersuchten Security-Frameworks vollständig erfüllt wird. Diese drei Defizite bilden zusammen das **größte Hindernis** dafür, dass die technisch-funktional häufig hervorragenden Security-Frameworks erfolgreich in die Praxis umgesetzt werden: Erstens kann die Implementierung in den meisten Fällen **nicht schrittweise** erfolgen, sondern es muss das gesamte, meist sehr komplexe Security-Framework vollständig in einem Stück umgesetzt werden. Zweitens werden für die einzelnen Module zwar verschiedene Lösungsvarianten vorgestellt, der zwingend durchzuführende **Anpassungsprozess wird aber nicht ausreichend unterstützt**. Schließlich erfährt der potentielle Frameworkanwender in keinem Fall eine vollständige, **methodische Unterstützung bei der Einführung** des letztlich angepassten Security-Frameworks. Dass kein einziges Framework die Anforderung *SF-INT-Einführung*

vollständig unterstützt, ist somit nicht auf deren vermeintliche Irrelevanz zurückzuführen, sondern vor allem dem Mangel geschuldet, dass bereits der einer praktischen Einführung zeitlich vorgelagerte Anpassungsvorgang in den meisten Frameworkkonzepten unzureichend behandelt wird und auf die weiteren Phasen im Lebenszyklus einer Security-Framework-Instanz nicht mehr adäquat eingegangen wird.

Diese Erkenntnis wird durch die vielen nur völlig unzureichend erfüllten Anforderungen in der Kategorie **SF-MGMT**, die auf verschiedene Aspekte des Managements instanziierter Security-Frameworks abzielen, umfassend bestätigt. Nicht nur durch die zwölf Anforderungen, deren Durchschnittspunktezahlen unter $0,50$ liegen, wird offensichtlich, dass es sich hierbei um denjenigen Bereich handelt, der bei nahezu allen Security-Frameworks noch umfassend verbessert werden muss. Da sich, wie auch nachfolgend in Abschnitt 4.5.3 diskutiert wird, ein unfassender weiterer Schwerpunkt dieser Arbeit mit den hier identifizierten Schwachpunkten auseinandersetzt, werden an dieser Stelle lediglich die vier Anforderungen diskutiert, die von keinem der untersuchten Security-Frameworks vollständig erfüllt wurden.

Zunächst liegt mit *SF-MGMT-Tests* eine als *wünschenswert* gewichtete Anforderung vor, die auf von den Frameworkautoren vorgeschlagene Maßnahmen zur Überprüfung der Frameworkumsetzung abzielt. Dadurch soll verhindert werden, dass aufgrund von Fehlern beim Customizing oder bei der Implementierung eine degenerierte Frameworkinstanz entsteht, mit der sich die ursprünglich gesetzten Ziele nicht mehr erreichen lassen. Mehr noch als *SF-INT-Einführung* wird dieser Aspekt von fast keinem der untersuchten Security-Frameworks auch nur ansatzweise berücksichtigt, ohne dass deshalb der mit der Anforderung beabsichtigte Mehrwert in Frage zu stellen wäre. Als praktische Konsequenz ergibt sich, dass initiale und kontinuierliche Funktionsüberprüfungen der Security-Framework-Instanzen zwingend szenarienspezifisch zu konzipieren und durchzuführen sind. Die drei weiteren von keinem Security-Framework vollständig erfüllten Anforderungen *SF-MGMT-Berichtsdetails*, *SF-MGMT-Metriken* und *SF-MGMT-KPIs* hängen sehr eng mit der Anforderung *SF-MGMT-ITSM-Schnittstellen* zusammen, die ebenfalls zu den drei insgesamt am schlechtesten bewerteten Kriterien zählt. Sie sind zum einen Symptome dafür, dass nahezu keines der Security-Frameworks Berichte über die aktuelle Sicherheitslage und seine Beiträge dazu vorsieht – weder intern für Administratoren oder das Management noch für externe Kunden und Anwender. Zum anderen lassen sich die Sicherheitseigenschaften der Security-Frameworks offensichtlich nur sehr schwer messen und quantifizieren, obwohl es sich bei dieser Quantifizierung – beispielsweise in Form von KPIs oder SLA-Parametern – um eine Anforderung handelt, die sich konsistent durch alle Standards und Best Practices zum IT Service Management zieht. Als Konsequenz werden diese Anforderungen, die im praktischen Betrieb unverzichtbar sind und durch szenarienspezifische Maßnahmen mit entsprechendem Mehraufwand umgesetzt werden müssen, im Rahmen dieser Arbeit uneingeschränkt aufrecht erhalten.

Schließlich zeigt sich in der Anforderungskategorie **SF-DOKU**, dass den meisten Frameworkkonzepten eine kritische Selbstbetrachtung fehlt, so dass ein potentieller Frameworkanwender ohne gezielte Unterstützung von Grund auf selbst prüfen muss, ob der Umfang des Security-Frameworks für seine Zwecke ausreichend ist (vgl. *SF-DOKU-Vollständigkeit*). Der in den obigen Diskussionen bereits mehrfach aufgegriffene Schwachpunkt, dass Anpassung, Umsetzung, Einführung und Betrieb nicht ausreichend unterstützt werden, zeigt sich auch in der schlechten Durchschnittsbewertung von *SF-DOKU-Lifecyclephasen*; sie bestätigt die dabei gewonnene Erkenntnis, dass häufig eine Beschränkung auf die Designphase stattfindet, die nicht wie durch diese Anforderung gewünscht explizit benannt wird. Auch die als

wünschenswert gewichtete Anforderung *SF-DOKU-Checkliste* wird nur von einem Bruchteil der untersuchten Security-Frameworks erfüllt; da sie auf die Erleichterung von Anpassung, Umsetzung und Einführung abzielt, korreliert dieses Ergebnis mit den bereits diskutierten und hat zur Folge, dass entsprechende Ablaufpläne von jedem Frameworkanwender szenarienspezifisch erstellt werden müssen. Letztlich handelt es sich bei *SF-DOKU-Zertifizierung* um die am schlechtesten bewertete Anforderung dieser Kategorie und um die sechste, die von keinem der untersuchten Security-Frameworks vollständig erfüllt wird. Diese Bewertung zeigt, dass bei der Konzeption von Security-Frameworks bislang auf das im industriellen Umfeld und verstärkt auch im öffentlichen Bereich relevante Thema der Organisations- und auch Personenzertifizierung, beispielsweise nach ISO/IEC 27001, zu wenig eingegangen wird. Aufgrund dieser praktischen Bedeutung wird an der als wünschenswert gewichteten Anforderung unverändert festgehalten.

Nach dieser Gegenüberstellung der durch die Untersuchung der Security-Frameworks identifizierten größten Stärken und Schwächen wird nachfolgend erläutert, welche Auswirkungen die gewonnenen Ergebnisse auf die weiteren Beiträge und Schwerpunkte dieser Arbeit haben.

4.5.3. Konsequenzen für diese Arbeit

Bereits in Kapitel 1 wurden die verschiedenen Aspekte der Gesamtzielsetzung dieser Arbeit, IT-Sicherheitsmanagement über die Abdeckungsgebiete einzelner Security-Frameworks hinausgehend zu betrachten, erläutert. Dieses übergeordnete Ziel kann, wie die Analysen in diesem Kapitel ergeben haben, nur durch die Bewältigung zweier großer Herausforderungen erreicht werden: Zum einen liegen bislang nur wenige Fragmente für das integrierte Management mehrerer parallel betriebener, zueinander komplementärer Security-Frameworks vor, da über die Grenzen jedes einzelnen Frameworks hinausgehende Konzepte noch fehlen. Zum anderen weisen, wie im vorhergehenden Abschnitt ausgeführt wurde, sehr viele Security-Frameworks eine ganze Reihe von Defiziten auf, so dass diese eine nur eingeschränkt taugliche Basis für weiterführende Konzepte darstellen. Aufgrund der Ergebnisse dieser Bestandsaufnahme muss deshalb an dieser Stelle konkretisiert werden, wie die gesteckten Zielsetzungen durch die in den folgenden Kapiteln dargelegten Konzepte erreicht werden können.

Zunächst ist festzuhalten, dass unter Berücksichtigung der bereits ausgeprägt vorhandenen Stärken der existierenden Security-Frameworks im sicherheitsfunktionalen Bereich auf die detaillierte Untersuchung technischer Sicherheitsmechanismen weitgehend verzichtet werden kann. Erheblich dringender benötigt werden Konzepte, durch die in einem **ersten Schritt** die Mängel der bestehenden Security-Frameworks bei ihrer szenarienspezifischen Anpassung, Umsetzung, Inbetriebnahme sowie im laufenden Betrieb kompensiert werden können. In einem **zweiten Schritt** muss anschließend untersucht werden, wie die einzelnen für ein Szenario relevanten Security-Frameworks zusammenspielen, in einen gesamtheitlichen Sicherheitsmanagementansatz integriert und nahtlos in die übergeordneten ITSM-Prozesse eingebettet werden können. Im erforderlichen **dritten Schritt** ist schließlich zu zeigen, wie diese Konzepte durch entsprechende Managementwerkzeuge erfolgreich in die Praxis umgesetzt werden können und wie diese konzeptionellen Beiträge wiederum mit den angestrebten Verbesserungen individueller Security-Frameworks zusammenhängen, um eine nachhaltige und durchgängige Verbesserung der Sicherheitsmanagementprozesse zu erzielen. Die Umsetzung dieser Schritte findet in den weiteren Kapiteln dieser Arbeit wie folgt statt:

- In Kapitel 5 wird der **Soll-Lebenszyklus von Security-Frameworks** nicht aus der Sicht der Autoren eines Security-Frameworks, sondern vielmehr aus der Perspektive von Frameworkanwendern spezifiziert, die in ihren Szenarien in der Regel mehr als ein Security-Framework parallel einsetzen wollen (vgl. Diskussion der Szenarien in Kapitel 3). Dieser Lebenszyklus muss mit der Auswahl geeigneter Security-Frameworks zeitlich früher ansetzen als die untersuchten Frameworkkonzepte und insbesondere **weit über die Design- und Ansätze der Customizingphase hinausgehen**, da beispielsweise auch laufende Verbesserungen im operativen Betrieb bis hin zur Außerbetriebnahme des Security-Frameworks zu betrachten sind. Ein Schwerpunkt muss dabei auf den Bereichen der Anforderungskategorie *SF-INT* liegen; darüber hinaus müssen zum einen auch ausgewählte Fragestellungen rund um die Defizite in *SF-FUNK*, beispielsweise die oft nur partiell vorhandene Beschreibung berücksichtigter Schwachstellen und Angriffe, berücksichtigt und zum anderen die Schnittstellen zu den nachfolgend im Detail zu betrachtenden Managementkonzepten spezifiziert werden.
- Kapitel 6 muss ein **integriertes Managementkonzept für Security-Frameworks** erarbeiten und dabei verstärkt auf die Anforderungen aus der von den existierenden Security-Frameworks bislang unzureichend behandelten Kategorie *SF-MGMT* eingehen. Es hat im Unterschied zu vielen der analysierten Arbeiten einen konsequent **prozessorientierten Ansatz** zu verfolgen, muss die erforderlichen **Interaktionen** des security-framework-orientierten Sicherheitsmanagements mit den anderen ITSM-Prozessen verdeutlichen, zu den vorhandenen technischen Lösungen komplementäre **organisatorische Maßnahmen** thematisieren und die **kontinuierliche Überwachung und Verbesserung** des Gesamtsicherheitsniveaus unter anderem auf Basis von Sicherheitskennzahlen sowie Sicherheitsberichten und deren Auswertung konkretisieren. Dabei ist insbesondere auch Bezug auf ausgewählte Teile der Kategorie *SF-FUNK*, beispielsweise hinsichtlich zu verbessernder Automatisierungsansätze, und Konsequenzen für der Kategorie *SF-DOKU* zugeordnete Aspekte von Security-Frameworks, z.B. bezüglich Zertifizierungsvorhaben, zu nehmen.
- In Kapitel 7 sind **Detailkonzepte und Prototypen von ausgewählten Werkzeugen**, die bestehende Managementarchitekturen ergänzen und zur Umsetzung einiger der vorgestellten Bestandteile des Managementkonzepts erforderlich sind, darzustellen. Neben dem von ihnen gebotenen Mehrwert muss dabei die enge **Verzahnung mit den Security-Frameworks**, zu deren Betrieb sie beitragen, betrachtet werden, so dass sich wiederum Bezüge zu den Aspekten der Kategorie *SF-FUNK* ergeben.

Insgesamt sind somit Beiträge anzustreben, die über die Schaffung übergeordneter Managementkonzepte hinausgehend auch zu Maßnahmen und Methoden führen, die zur gezielten Verbesserung der bestehenden Security-Frameworks genutzt werden können.

4.6. Zusammenfassung

In diesem Kapitel wurden zunächst die verschiedenen Arten und inhaltlichen Schwerpunkte von Security-Frameworks und die Recherchemethodik, mit der die relevanten Arbeiten ermittelt wurden, diskutiert. Nach einer Kurzübersicht über die so identifizierten Security-Frameworks wurde festgestellt, dass zwar bislang keine explizit dokumentierten Designrichtli-

nien für Security-Framework-Konzepte existieren, dass der Aufbau von Frameworkdokumentationen aber häufig einem Muster folgt, das näher erläutert wurde.

Anschließend wurde je ein Security-Framework für IT-Architekturen bzw. IT-Dienste auf Basis des im vorhergehenden Kapitel erarbeiteten Kriterienkatalogs beurteilt, um dessen Anwendung detailliert zu verdeutlichen und bereits einige typische Stärken sowie Optimierungspotenziale aufzuzeigen. Im Weiteren wurden analog, aber in der Darstellung wesentlich kompakter die Ergebnisse der Analyse von mehr als 70 weiteren Security-Frameworks vorgestellt, wobei neben der Nutzwertanalyse auch jeweils knapp auf die Schwerpunkte und wichtigsten Verbesserungsmöglichkeiten des jeweiligen Frameworkkonzepts eingegangen wurde.

Die Betrachtung der einzelnen Security-Frameworks abschließend wurden die Einzelbewertungen zusammengefasst und das Gesamtergebnis analysiert: Insbesondere im technischen bzw. sicherheitsfunktionalen Bereich weisen die meisten Security-Frameworks bereits klare Stärken auf. Fast der gesamte Bereich der Managementanforderungen wird bislang jedoch nur völlig unzureichend erfüllt und auch bezüglich der Anpassungs- und Integrationsabläufe sind ebenso noch umfangreiche Verbesserungen vorzunehmen wie in einigen Teilbereichen der Dokumentation von Security-Frameworks.

Schließlich wurden die Analyseergebnisse in den Kontext der Ziele dieser Arbeit eingebettet und die Schwerpunkte der Beiträge der nachfolgenden Kapitel festgelegt.

Kapitel 5.

Der Lebenszyklus von Security-Frameworks

Inhalt dieses Kapitels

Die Analyse existierender Security-Frameworks in Kapitel 4 hat sehr deutlich gezeigt, dass zwar technische Architekturen und IT-sicherheitsrelevante Eigenschaften meist sehr zielführend in den Frameworkkonzepten dargelegt werden, dass aber bereits die ersten notwendigen Schritte zur Anpassung und Implementierung der Security-Frameworks in eigenen Szenarien bislang häufig nur unzureichend konzeptionell unterstützt werden. Insbesondere fehlt eine methodische Auseinandersetzung mit den für den nachhaltigen Betrieb zwingend erforderlichen technischen und organisatorischen Managementeigenschaften fast durchgängig.

In diesem Kapitel wird deshalb – auch als Grundlage für die weiteren Betrachtungen der genauen Abläufe im Management von Security-Frameworks im nächsten Kapitel – eine **spezifische Darstellung des gesamten Lebenszyklus von Security-Frameworks** erarbeitet; hinsichtlich ihrer Breite und Tiefe existieren bislang keine vergleichbaren Arbeiten.

Die Betrachtungen in den vorangegangen Kapiteln konzentrierten sich auf einzelne Security-Frameworks und erfolgten, beispielsweise bei der Aufbereitung der Anforderungen zu einer Checkliste in Abschnitt 3.9, auf die Sichtweise von Frameworkautoren zugeschnitten. Demgegenüber liegt diesem Kapitel die Zielsetzung zugrunde, die **Perspektive von Frameworkanwendern** abzudecken. Erst dadurch wird es möglich, auch die für den operativen Einsatz der Security-Frameworks relevanten **Anforderungen an das jeweilige *Szenario*** herauszuarbeiten, um die bereits umfassend diskutierten Anforderungen an *Security-Frameworks* zu komplementieren.

Durch die in Kapitel 2 erläuterte duale Verwendung des Begriffs Security-Framework sowohl für das allgemeine **Frameworkkonzept** als auch die jeweils **szenarienspezifische Instanz** ergibt sich die Notwendigkeit, ebenso bei der Beschreibung des Lebenszyklus zwischen der kontinuierlichen Weiterentwicklung des Frameworkkonzepts und dem einem kontinuierlichen Verbesserungsprozess unterliegenden, nachhaltigen Betrieb der jeweiligen szenarienspezifischen Frameworkinstanz differenzieren zu müssen. Grundsätzlich wird dabei angenommen, dass die Frameworkautoren und -anwender im Allgemeinen – abgesehen von den in diesem Kapitel beschriebenen Schnittstellen – unabhängig voneinander agieren.

Hinzu kommt, dass es sich bei der **initialen Einführung** eines Security-Frameworks in einem konkreten Szenario oftmals um ein umfangreiches und komplexes Vorhaben handelt, das unter praktischen Gesichtspunkten in Form eines dedizierten Projekts durchgeführt wird; dieses kann wiederum in Teilprojekte und einzelne Phasen untergliedert werden, die zu berücksichtigende Schnittstellen aufweisen und in die Abläufe eingebettet werden müssen.

Betrachtet man zusätzlich noch die von einzelnen Security-Frameworks losgelösten Geschäfts- und ITSM-Prozesse, so ergibt sich bei jeder praktischen Instanziierung eines Security-Frameworks ein **komplexes Geflecht an Abhängigkeiten**, deren Berücksichtigung für den erfolgreichen Einsatz jedoch zwingend erforderlich ist und somit eine strukturierte Auseinandersetzung mit der gegenseitigen **Verzahnung der Lebenszyklus-, Projekt- und Prozessphasen** motiviert. Erst durch die Definition entsprechender Schnittstellen und die Einbettung in den Lebenszykluskontext können die in Kapitel 6 beschriebenen Managementziele, -aufgaben und -operationen fundiert erarbeitet werden.

Die Zielsetzung der vorangegangenen Kapitel, Maßnahmen zur weiteren Verbesserung von Frameworkkonzepten zu erarbeiten, wird dabei jedoch nicht aufgegeben; vielmehr wird bei der Analyse der verschiedenen Lebenszyklusphasen berücksichtigt, dass bei der Implementierung und im Betrieb eines Security-Frameworks gewonnene praktische Erfahrungen in die **Weiterentwicklung** des Frameworkkonzepts einfließen können und sollen.

Die nachfolgend vorgestellten Ergebnisse sind somit für zwei Zielgruppen unmittelbar relevant: Zum einen für die Autoren von Frameworkkonzepten, die Anregungen für zu berücksichtigende Aspekte erhalten bzw. vertiefen können, und zum anderen für Systemarchitekten und Projektleiter, die sich mit der Einführung und später mit der kontinuierlichen Verbesserung von Frameworkinstanzen in einem konkreten Szenario befassen.

In Abschnitt 5.1 werden zunächst die grundlegenden **Annahmen, Vorgehensweisen und**

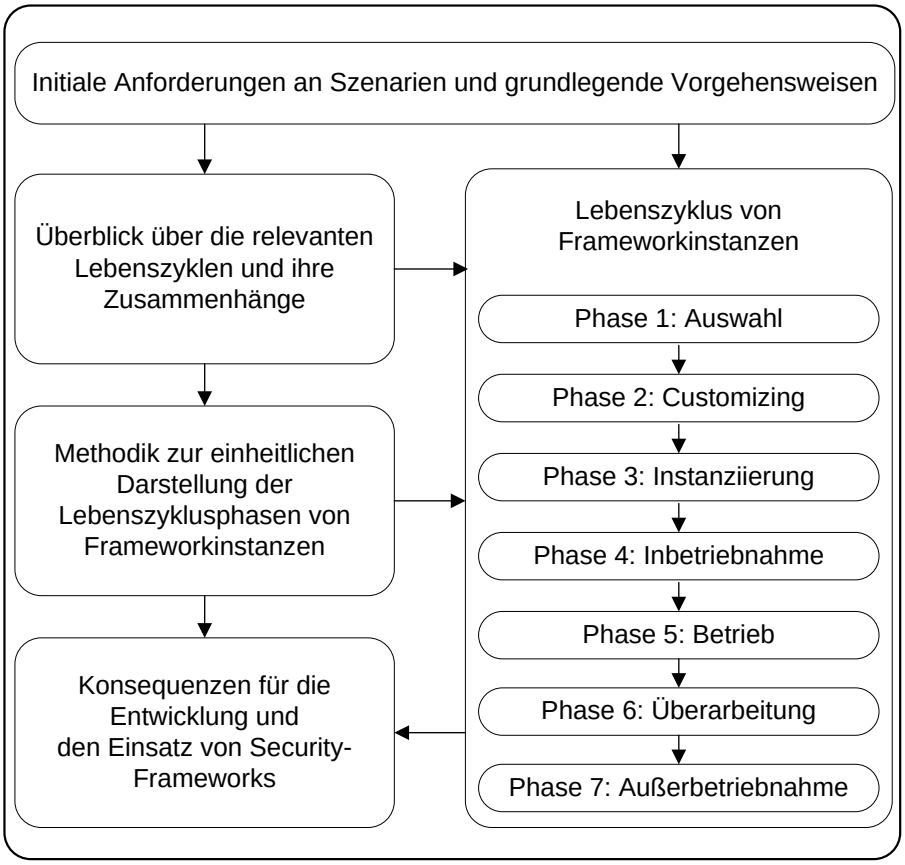


Abbildung 5.1.: Vorgehensmodell in diesem Kapitel

szenarienseitigen Voraussetzungen diskutiert, aus denen sich die Motivation und die Möglichkeit zum Einsatz von Security-Frameworks in konkreten Szenarien ergeben. Darauf aufbauend werden in Abschnitt 5.2 die für die weitere Betrachtung relevanten **Lebenszyklen und ihre gegenseitigen Abhängigkeiten** und Synergien in einem kurzen Überblick dargestellt. Dabei wird auf den Lebenszyklus der Frameworkkonzepte, aus dem sich mehrere zu berücksichtigende Schnittstellen ergeben, nur in kompakter Form eingegangen, da die umfassende Analyse und Diskussion des Lebenszyklus von Frameworkinstanzen explizit den Schwerpunkt bildet.

Anschließend werden in Abschnitt 5.3 die **Methodik** und die Struktur erläutert, die gewählt wurden, um die **Lebenszyklusphasen von Frameworkinstanzen einheitlich zu beschreiben**. Diese einzelnen **Phasen** von der initialen Auswahl bis hin zur Außerbetriebnahme werden in den Abschnitten 5.4 bis 5.10 mit ihren jeweiligen Schnittstellen und einigen ausgewählten, zu ihrer Durchführung geeigneten Methoden erörtert.

In Abschnitt 5.11 werden schließlich die **Konsequenzen**, die sich aus den Diskussionen der einzelnen Lebenszyklusphasen für die Entwicklung und den praktischen Einsatz von Security-Frameworks ergeben, erläutert. Das Kapitel, dessen Vorgehensmodell in Abbildung 5.1 zusammengefasst ist, schließt mit einer kurzen Zusammenfassung der Ergebnisse.

5.1. Szenarienspezifische Voraussetzungen und Entscheidungsgrundlagen

Die in diesem Kapitel vorgestellten Lebenszyklusphasen für die Konzepte und Instanzen von Security-Frameworks sind generisch in dem Sinn, dass sie – in individueller Ausprägung – von jedem Security-Framework bzw. in jedem Szenario durchlaufen werden. Um die getroffene Auswahl der in jeder Phase vorgestellten Methoden zu motivieren, werden im Folgenden zunächst die für Szenarien, in denen ein (weiteres) Security-Framework eingesetzt werden könnte, zugrunde gelegten Annahmen und Anfangsbedingungen skizziert. Damit wird das Ziel verfolgt, die nachfolgenden Ausführungen zu fokussieren, ohne zu implizieren, dass andere Szenarien nicht für den Einsatz von Security-Frameworks geeignet seien. Daran anschließend wird erläutert, wie die initiale Entscheidung zur Instanziierung eines Security-Frameworks szenarienspezifisch getroffen werden kann.

5.1.1. Initiale Voraussetzungen und prinzipielle Vorgehensweisen

An die Planung des Einsatzes von Security-Frameworks in einem bestimmten Szenario werden die folgenden drei Randbedingungen gestellt:

1. Es wird davon ausgegangen, dass ausreichend detailliertes *Wissen über das konkrete Szenario*, in dem ein Security-Framework eingesetzt wird, bereits a priori vorhanden ist, so dass bei der Beschreibung der einzelnen Phasen nicht auf grundlegende Schritte zur Erfassung und Analyse des Szenarios an sich eingegangen wird. Hierzu gehört beispielsweise, dass die zu schützenden Assets genauso bereits ermittelt wurden wie z. B. die für das Szenario relevanten Angreifermodelle. Entsprechende Vorarbeiten müssen folglich geleistet werden, bevor die Einführung des Security-Frameworks in die Wege geleitet wird.
2. Es muss prinzipiell unterschieden werden, ob Security-Frameworks *von Anfang an* gemeinsam mit den von ihnen zu schützenden Assets (z. B. Dienste oder Architekturen) aufgebaut und in Betrieb genommen oder ob Security-Frameworks *nachträglich* in die schon vorhandene Infrastruktur integriert werden sollen. Diese Unterscheidung hat insbesondere auf Abläufe und Randbedingungen in den beiden Phasen *Implementierung* und *Inbetriebnahme* größere Auswirkungen. Nicht explizit betrachtet wird jedoch der Ansatz, ein Security-Framework zu instanziieren, ohne dass die zu schützenden Assets bereits vorhanden sind. Diese zur genannten Fallunterscheidung komplementäre Vorgehensweise, IT-Dienste erst nachträglich in vorab geschaffene Sicherheitsarchitekturen zu integrieren, kann bei Bedarf über einen Einsprung in die in Abschnitt 5.9 beschriebene Lebenszyklusphase, die eine Überarbeitung der Frameworkinstanz z. B. aufgrund von größeren Änderungen an der zu schützenden Infrastruktur vorsieht, abgebildet werden. Im Vordergrund steht jedoch immer die Zielsetzung, die u. a. durch die Frameworkmodularität ermöglichte Flexibilität zu nutzen, um individuell an den *aktuell* konkret planbaren Schutzbedarf angepasste Sicherheitsmaßnahmen umzusetzen.
3. Es muss berücksichtigt werden, dass im Allgemeinen *mehr als ein Security-Framework pro Szenario* zum Einsatz kommen kann. Dies ist beispielsweise immer dann der Fall, wenn eine Organisation oder ein Verbund von Organisationen mehrere IT-Dienste betreibt, für die kein gemeinsames Security-Framework existiert. Dadurch ergeben sich

für das Szenario z. B. durch die frameworkübergreifend gemeinsame Nutzung von technischen Komponenten wie Firewalls einige Randbedingungen, die in den Phasen *Customizing* und *Betrieb* berücksichtigt werden müssen; diese haben sich auch bereits als Anforderungen an Security-Frameworks in der Kategorie SF-INT niedergeschlagen.

Bei den weiteren Betrachtungen wird ohne Beschränkung der Allgemeinheit davon ausgegangen, dass die genannten Randbedingungen erfüllt werden.

5.1.2. Entscheidungsgrundlagen für den Einsatz von Security-Frameworks

Während sich Frameworkkonzepte unabhängig von den konkreten Einsatzszenarien weiterentwickeln, hängt die Instanziierung des Lebenszyklus einer Frameworkinstanz offensichtlich von der Entscheidung ab, im jeweils vorliegenden Szenario zielgerichtet auf ein Security-Framework zurückzugreifen. Diese Entscheidung wird im Regelfall auf Basis einer Ermittlung und Auswertung der szenarienspezifischen IT-Sicherheitsanforderungen getroffen. Im Folgenden wird – die in Kapitel 6 erläuterten Abläufe im IT-Sicherheitsmanagement berücksichtigend – eine Einbettung dieser Entscheidung in an ISMS angelehnte Strukturen vorgenommen (vgl. Abschnitt 2.6).

Für die Vorbereitung einer Entscheidung zum Einsatz eines Security-Frameworks müssen die folgenden Voraussetzungen erfüllt sein:

- **Ziele**: Die im Szenario verfolgten technischen und organisatorischen Ziele der IT-Sicherheit sowie die zu schützenden Daten und Systeme (Assets) müssen bekannt sein. In Anlehnung an ISO/IEC 27001 werden *Scope*, *Assets* und *Ziele* in einer Informationssicherheitsleitlinie (engl. *security policy*) dokumentiert, auf deren Basis ein Gesamtsicherheitskonzept erstellt wird. Dieses Gesamtsicherheitskonzept muss wiederum durch dienstspezifische Betriebs- und Sicherheitskonzepte ergänzt werden, die später insbesondere auch eine Gegenüberstellung mit dem implementierten Security-Framework zur Analyse und Beurteilung der Zielerreichung ermöglichen.
- **Ist-Zustand**: Neben den zu schützenden Assets müssen die bereits eingesetzten technischen und organisatorischen Sicherheitsmaßnahmen bekannt sein. Diese wirken sich einerseits auf die Analyse des zusätzlichen Schutzbedarfs als auch auf die zu berücksichtigenden szenarienspezifischen Integrationseigenschaften der Security-Frameworks aus. Die erforderliche Gesamtsicht auf die Infrastruktur sowie deren Komponenten und Abhängigkeiten kann beispielsweise durch ITSM-Prozesse wie das Configuration Management im Zusammenspiel mit der Dokumentation des ISMS bereitgestellt werden (vgl. Abschnitt 2.2.3.3).
- **Verantwortlichkeiten**: Die für die technische Konzeption und die für das Treffen der Entscheidung zuständigen Personen müssen benannt sein. Entsprechende Gremien, Abläufe und deren Befugnisse werden ebenfalls im Rahmen der Informationssicherheitsleitlinie definiert; beim Übergang zwischen den unten diskutierten Lebenszyklusphasen der Frameworkinstanz müssen dabei zum Teil auch Ressourcen- und Budgetentscheidungen getroffen werden können, so dass beispielsweise die Leitung des betroffenen Unternehmens zu involvieren ist.

Der Bedarf an zusätzlichen technischen und organisatorischen Sicherheitsmaßnahmen ergibt sich auf dieser Basis aus einer Diskrepanz zwischen den Zielen und dem aktuellen Ist-Zustand,

die von den Verantwortlichen beispielsweise in folgenden Situationen diagnostiziert werden kann:

- Im Rahmen des ITSM-Prozesses Service Portfolio Management werden neue oder veränderte Dienste geplant, für die adäquate Schutzmaßnahmen vorgesehen werden müssen (vgl. Abschnitt 2.2.3.3).
- Bei Self Assessments, Management Reviews oder ISMS-Audits werden Defizite und Verbesserungsmaßnahmen identifiziert (vgl. [I27001, Kap. 8]).
- Durch die Anwendung von Methoden des Security Engineering wie proaktiven Sicherheitstests werden bis dahin unbekannte Risiken identifiziert (vgl. Abschnitte 2.3 und 2.4.2).
- Im operativen Management werden, z. B. durch konkrete IT-Sicherheitsvorfälle oder den Einsatz des Common Vulnerability Scoring Systems [MSR07], Verwundbarkeiten und Bedrohungen bekannt und bewertet, die nicht mit punktuellen Eingriffen in den betroffenen Systemen beseitigt werden können (hierauf wird in Kapitel 6 genauer eingegangen).

Die identifizierten Problembereiche und möglichen Maßnahmen müssen – üblicherweise im Zusammenspiel mit einem szenarienweiten Risikomanagement – analysiert und priorisiert werden (vgl. Abschnitte 2.2.3.1 und 6.1). Durch gegenseitige Abhängigkeiten und gemeinsame Eigenschaften wie beispielsweise den Bezug mehrerer Risiken auf denselben Dienst können in der Regel Gruppierungen vorgenommen werden, so dass die entsprechenden Risiken im weiteren Verlauf zusammenhängend bearbeitet werden können.

Eine Entscheidung für oder gegen die Einführung eines Security-Frameworks hängt ab diesem Zeitpunkt wesentlich davon ab, ob die bereits vorhandenen technischen und organisatorischen Maßnahmen nur geringfügig angepasst bzw. erweitert werden müssen oder ob sich die Notwendigkeit größerer Anpassungen abzeichnet, für die ein geeignetes Security-Framework ermittelt werden soll. In diesem Fall wird der Lebenszyklus der Frameworkinstanz wie in Abschnitt 5.4 beschrieben mit der Ermittlung geeigneter Security-Frameworks und der Auswahl des für das Szenario am besten geeigneten Frameworkkonzepts begonnen.

5.2. Überblick über die Lebenszyklen und ihre Zusammenhänge

Analog zu Softwareprodukten und IT-Diensten dient die Einteilung in Lebenszyklusphasen auch bei Security-Frameworks der strukturierten Auseinandersetzung mit den sich im Laufe der Entwicklung und des Einsatzes verändernden Teilzielen, Tätigkeitsschwerpunkten, Zuständigkeiten und relevanten Schnittstellen. Im Unterschied zu szenarienspezifischen Sicherheitskonzepten sind Security-Frameworks bereits per Definition für den Einsatz in mehr als einem Szenario geeignet; *ein Frameworkkonzept* wird somit im Allgemeinen *beliebig oft instanziiert*.

Sieht man von den relativ seltenen Fällen ab, in denen sich die Autoren von Frameworkkonzepten beispielsweise durch die Beschränkung auf Teilveröffentlichungen vorbehalten, die Instanziierung selbst vorzunehmen, so liegt eine klare Aufgaben- und Zuständigkeitstrennung zwischen Frameworkkonzepten und -instanzen vor. Diese führt dazu, dass die Frameworkkonzepte unabhängig von den entsprechenden szenarienspezifischen Frameworkinstanzen wei-

terentwickelt werden. Unter dieser Grundannahme wird im Folgenden zur Verbesserung der Übersichtlichkeit, aber unter Berücksichtigung der erforderlichen Schnittstellen der **Lebenszyklus eines Frameworkkonzepts getrennt vom Lebenszyklus einer Frameworkinstanz betrachtet**.

Im folgenden Abschnitt wird dazu auf den Lebenszyklus der Konzepte von Security-Frameworks eingegangen. In Abschnitt 5.2.2 wird ein kurzer Überblick über den Lebenszyklus von Frameworkinstanzen gegeben; die detaillierte Diskussion der einzelnen Lebenszyklusphasen ist Schwerpunkt der Abschnitte 5.4 bis 5.10. In Abschnitt 5.2.3 werden die Anknüpfungspunkte und Schnittstellen zwischen den beiden Lebenszyklen und zur Umgebung, in der das Security-Framework eingesetzt wird, diskutiert; auch diese werden bei der Diskussion der einzelnen Instanz-Lebenszyklusphasen vertieft.

5.2.1. Der Lebenszyklus von Konzepten für Security-Frameworks

Bei den Frameworkkonzepten handelt es sich im Allgemeinen – insbesondere auch unabhängig davon, ob es sich um ein Security-Framework für das Software Engineering, für IT-Dienste oder IT-Architekturen handelt – um eine zielorientierte Zusammenstellung technischer und organisatorischer Maßnahmen, bei der existierende Lösungsbausteine kombiniert und optional um eigene, meist von Grund auf neu spezifizierte Komponenten ergänzt werden. Dabei muss beachtet werden, dass im Rahmen des Frameworkkonzepts bereits szenarienunabhängige Referenzimplementierungen dieser neu spezifizierten Komponenten entstehen können. Diese über rein konzeptionelle Tätigkeiten hinausgehenden Implementierungsarbeiten werden aufgrund ihrer Unabhängigkeit von Frameworkinstanzen dennoch im Kontext des Frameworkkonzepts betrachtet, da sie aufgrund der gewünschten Modularität von Security-Frameworks und in Abhängigkeit von szenarienspezifischen Frameworkanpassungen nicht zwingend in jeder Frameworkinstanz zum Einsatz kommen.

In Abschnitt 4.2 wurde bereits diskutiert, dass die Konzeption der aktuellen, in dieser Arbeit untersuchten Security-Frameworks bislang keinen explizit dokumentierten Designrichtlinien folgt, aber in strukturell miteinander gut vergleichbaren Frameworkkonzepten mündet. Analog dazu existiert bislang kein Referenzlebenszyklus, an dem sich die Frameworkkonzepte bewusst orientieren könnten. Im Folgenden wird deshalb ein idealisierter, an den Systems Development Life Cycle des US-amerikanischen Department of Justice (DOJ SDLC, siehe [SDLC]) angelehnter Lebenszyklus für Frameworkkonzepte beschrieben, ohne jedoch auszuschließen, dass vergleichbare Ergebnisse auch mit einer anders strukturierten Vorgehensweise erreicht werden könnten. Da für die den Betrachtungsschwerpunkt bildenden Frameworkinstanzen im Wesentlichen die resultierenden Frameworkkonzepte und deren Schnittstellen zu den Frameworkinstanzen relevant sind, wird auf eine Diskussion möglicher Variationen in diesem Lebenszyklus verzichtet.

Der DOJ SDLC stellt die Design- und Entscheidungsprozesse in den Vordergrund, die einen unmittelbaren Bezug zum funktionalen Umfang und zu den Kosten des zu entwickelnden Gesamtsystems haben. Die einzelnen Phasen können sowohl sequenziell als auch z. B. iterativ angewandt werden, so dass die Entwicklung eines Security-Frameworks insgesamt oder in Teilen je nach aktuellen Anforderungen beispielsweise einem Wasserfall- oder Spiralmodell bzw. einem agilen Entwicklungsmodell folgen kann. Die nachfolgend beschriebenen Lebenszyklusphasen dienen deshalb vorrangig der Gruppierung von Aktivitäten, die auf den Ergebnissen

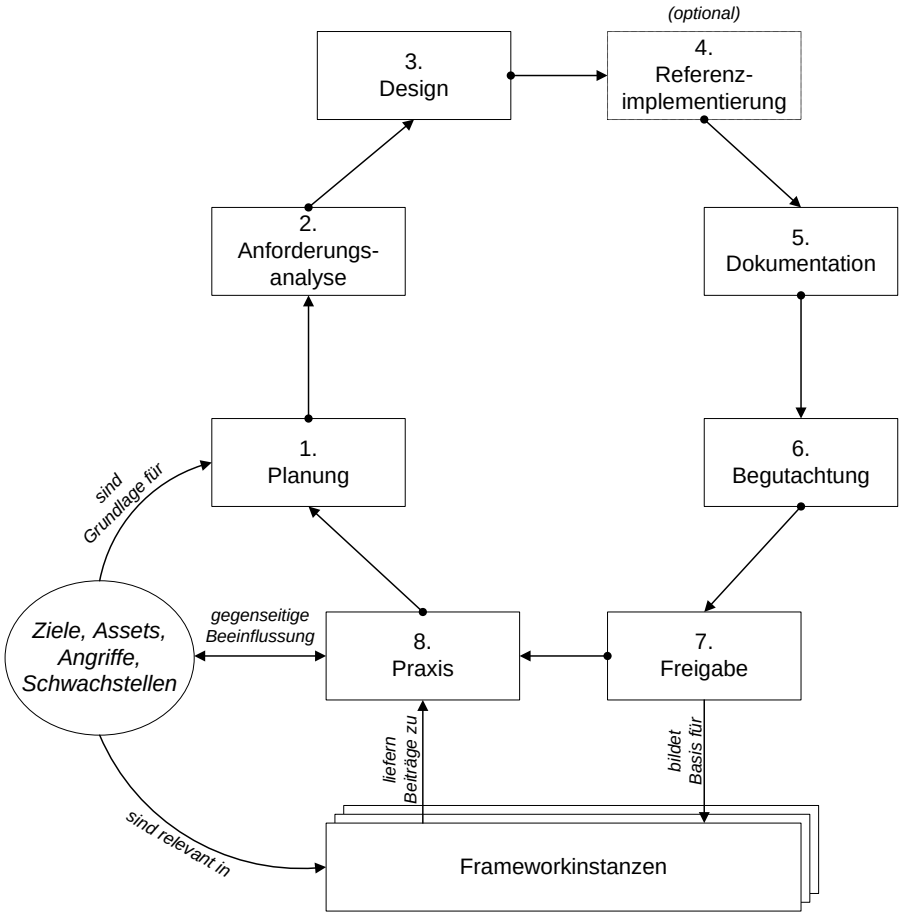


Abbildung 5.2.: Der Lebenszyklus von Frameworkkonzepten

der jeweils vorhergehenden Phase aufbauen.

Für die Konzepte von Security-Frameworks ergeben sich die folgenden, in Abbildung 5.2 dargestellten Phasen:

1. **Planung**: Zu Beginn der Konzeption eines neuen oder überarbeiteten Security-Frameworks müssen die Ziele spezifiziert und das weitere Vorgehen festgelegt werden. Mit Bezug auf die Definition von Security-Frameworks in Abschnitt 2.5 sind dabei insbesondere die zu schützenden Assets, die relevanten IT-Sicherheitsziele, die gewählten Ziele des IT-Sicherheitsmanagements sowie die relevanten Schwachstellen und Angriffe zu berücksichtigen.
2. **Anforderungsanalyse**: Die zum Erreichen der Ziele erforderlichen technischen und organisatorischen Maßnahmen müssen auf Anforderungen abgebildet werden. Die Disziplin *Requirements Engineering* stellt geeignete Methoden zur Verfügung, so dass sichergestellt werden kann, dass die unterschiedlichen Belange der involvierten Assets, IT-Sicherheitsrisiken und Zielgruppen (z. B. Administratoren und Anwender) ermittelt werden können. Im Allgemeinen sind die inhaltlichen Anforderungen an Frameworkkonzepte so vielfältig, dass eine Priorisierung vorgenommen werden muss. Neben den

fachspezifischen Zielen müssen in diesem Kontext auch die in dieser Arbeit ermittelten Anforderungen in den Kategorien *SF-FUNK*, *SF-INT* und *SF-MGMT* berücksichtigt werden.

3. **Design**: In der Designphase werden die zum Erfüllen der zu berücksichtigenden Anforderungen geeigneten technischen und organisatorischen Maßnahmen ausgewählt und zueinander in Beziehung gesetzt. Durch das Ziel, ein Security-Framework zu schaffen, motiviert steht dabei die Flexibilität im Vordergrund, so dass für einzelne Teilfragestellungen mehrere Lösungsansätze verfolgt werden können. Aspekte wie das spätere szenarienspezifische Anpassen des Security-Frameworks und die angestrebte Möglichkeit eines mehrstufigen Ausrollens müssen deshalb bereits beim Design beachtet werden.
4. **Referenzimplementierung**: Diese Phase ist optional. Eine Implementierung bietet sich insbesondere für die beim Frameworkdesign von Grund auf neu spezifizierten Komponenten an, wenn ohne sie eine spätere Umsetzung des Frameworkkonzepts in beliebigen Szenarien nicht möglich oder mit erheblichem Mehraufwand verbunden wäre. Eine vollständige Umsetzung des zu diesem Zeitpunkt noch nicht abgeschlossenen Frameworkkonzepts durch die Frameworkautoren ist als Sonderfall der ab Abschnitt 5.4 beschriebenen Frameworkinstanziierung möglich, wird im Folgenden aber nicht explizit betrachtet.
5. **Dokumentation**: Das in den vorhergehenden Phasen festgelegte und ggf. implementierte Security-Framework muss in Form des später zu veröffentlichenden Frameworkkonzepts dokumentiert werden. Über das schriftliche Fixieren des Designs hinausgehend müssen dabei u. a. die methodische Unterstützung der Customizing- und Rollout-Prozesse und der operativen Aufgaben wie Administration und Schulungen berücksichtigt werden. Die Anforderungen der Kategorie *SF-DOKU* und die in Abschnitt 3.9 erarbeitete Checkliste unterstützen die Frameworkautoren bei dieser Aufgabe.
6. **Begutachtung**: Nach Abschluss von Design, Referenzimplementierung und Dokumentation muss das als Ergebnis vorliegende Frameworkkonzept mit dem Ziel der Qualitätssicherung überprüft werden. Dabei muss wiederum sowohl auf die Gegenüberstellung der erreichten fachlichen Eigenschaften des Security-Frameworks mit den ursprünglichen Zielen als auch auf die geeignet aufbereitete Dokumentation des Frameworkkonzepts eingegangen werden. Identifizierte erforderliche Verbesserungen müssen vor dem Übergang zur nächsten Phase umgesetzt werden.
7. **Freigabe**: Die Arbeiten am Security-Framework werden für die aktuelle Version abgeschlossen und das Frameworkkonzept wird den potentiellen Anwendern geeignet zugänglich gemacht (vgl. Anforderung *SF-MGMT-Releasezyklus*). Diese Phase fungiert als primäre Schnittstelle zu den unten erläuterten Frameworkinstanzen.
8. **Praxis**: Der Freigabe des Frameworkkonzepts folgt der praktische Einsatz des Security-Frameworks in beliebigen Szenarien. Die Erfahrungen, die häufig auch von den Frameworkautoren selbst gewonnen werden können und – wie unten beschrieben – möglichst auch von anderen Frameworkanwendern kommuniziert werden sollen, liefern Hinweise zur weiteren Verbesserung (siehe auch Anforderungen *SF-MGMT-Support* und *SF-MGMT-Verbesserungen*). Neben diesen auf den Eigenschaften des Security-Frameworks basierenden Anregungen ergeben sich auch durch Weiterentwicklungen, z. B. seitens der zu schützenden Assets, Änderungen an den ursprünglich berücksichtigten Anforderungen, die beobachtet und bewertet werden müssen. Mit dem Erreichen einer kritischen

Masse an erforderlichen oder gewünschten Änderungen erfolgt der Übergang zur Planungsphase für die nächste Version des Security-Frameworks.

Bei vielen der in dieser Arbeit analysierten Security-Frameworks fällt auf, dass sie nach ihrer einmaligen Freigabe nicht mehr überarbeitet wurden. Der Ringschluss von der Praxis- zur Planungsphase für eine überarbeitete Version wird maßgeblich vom Vorliegen von Rückmeldungen der Frameworkanwender motiviert. Für den Lebenszyklus von Frameworkinstanzen sind Schnittstellen zur Meldung praktischer Erfahrungen an die Frameworkautoren deshalb von grundlegender Bedeutung.

5.2.2. Übersicht über den Lebenszyklus von Instanzen von Security-Frameworks

Analog zu den oben diskutierten Frameworkkonzepten ergibt sich auch für die Instanzen von Security-Frameworks die Schwierigkeit, dass keine verwandten Arbeiten existieren, die auf den vollständigen Lebenszyklus eingehen und somit als Basis für die weiteren Betrachtungen herangezogen werden könnten. Aus der Begriffsdefinition in Abschnitt 2.5 ergibt sich für Frameworkinstanzen die Aufgabe, organisatorische und technische Maßnahmen im Rahmen eines kontinuierlichen Verbesserungsprozesses für spezifische Szenarien umzusetzen. Bei den zu implementierenden Maßnahmen handelt es sich in der Regel um Sicherheitsmechanismen und -dienste sowie deren organisatorische Einbettung. In einer vereinfachten Betrachtung können Instanzen von Security-Frameworks deshalb zunächst als IT-Dienste aufgefasst werden, auf die existierende Lifecycle-Managementkonzepte übertragen werden können. Im Folgenden wird anhand des Beispiels ITIL v3 der grundlegende Service-Lebenszyklus skizziert, um anschließend auf die in dieser Arbeit erweiterte, für Security-Frameworks spezifische Lebenszyklusvariante einzugehen.

In Abschnitt 2.2.3.3 wurde bereits knapp auf die allgemeinen Zusammenhänge zwischen dem IT Service Management (ITSM) und dem IT-Sicherheitsmanagement eingegangen. ITSM-Rahmenwerke wie ITIL und MOF definieren Referenzprozesse zur Planung und Umsetzung sowie zum Betrieb und zur kontinuierlichen Verbesserung von IT-Diensten unter einer expliziten Dienst- und Kundenorientierung, d. h. losgelöst von rein technischen Betrachtungen. Die 2007 veröffentlichte dritte Version von ITIL verfolgt zur Gruppierung der Referenzprozesse eine stark am Lebenszyklus der IT-Dienste orientierte Struktur:

- Alle Aktivitäten müssen zunächst in eine *Servicestrategie* eingebettet werden. Auf den Einsatz von Security-Frameworks übertragen muss das in Abschnitt 5.1.2 geforderte szenarienspezifische Gesamtsicherheitskonzept als Rahmen vorliegen.
- Es folgt die Phase des *Serviceentwurfs*, in der die aus Geschäftsperspektive relevanten Ziele auf Funktionalität und Leistungsumfang des IT-Dienstes übertragen werden.
- Die Phase *Serviceüberführung* zielt auf die praktische Inbetriebnahme des IT-Dienstes ab; sie berücksichtigt neben den technischen Änderungen an der Infrastruktur auch die organisatorischen Auswirkungen.
- In der Phase *Servicebetrieb* werden operative Aufgaben wie das Management von Störungen und die Unterstützung von Kunden und Anwendern behandelt.
- Im Rahmen der *kontinuierlichen Serviceverbesserung* werden Methoden zur Identifikation und Umsetzung von Optimierungsmöglichkeiten behandelt. Diese fließen wiederum

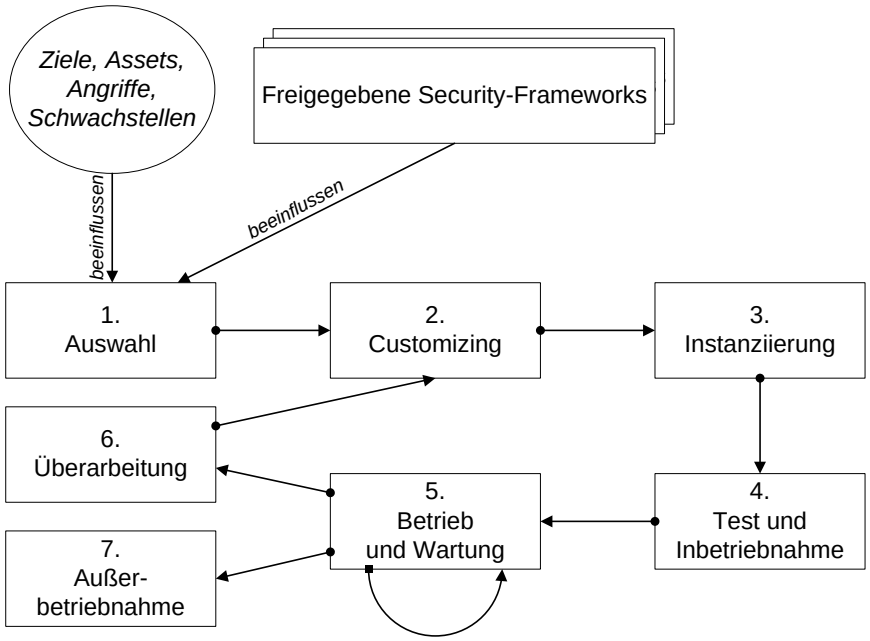


Abbildung 5.3.: Der Lebenszyklus von Frameworkinstanzen

in den weiteren *Serviceentwurf* mit ein, bis im Rahmen der *Servicestrategie* entschieden wird, dass der Dienst außer Betrieb genommen werden soll.

Wie IT-Dienste werden auch Security-Frameworks für eine möglicherweise sehr lange, letztlich aber immer begrenzte Lebensdauer instanziiert. Sie unterliegen somit einem Lebenszyklus, der mit planerischen Aktivitäten beginnt, seine szenarienspezifischen IT-Sicherheitsziele in der Betriebsphase unterstützt und nach einer meist nicht a priori festgelegten Anzahl an Verbesserungen und Überarbeitungen mit der Außerbetriebnahme endet.

Um die Besonderheiten von Security-Frameworks insbesondere in den Bereichen der szenarienspezifischen Adaption und der nahtlosen Integration in die vorhandene Infrastruktur besser berücksichtigen zu können, wird in dieser Arbeit das in Abbildung 5.3 dargestellte Lebenszyklusmodell für Frameworkinstanzen betrachtet:

1. **Auswahl des Security-Frameworks**: Wiederum im Unterschied zu szenarienspezifischen, auf konkrete einzelne IT-Dienste bezogene Sicherheitskonzepten setzt die Planung der Instanziierung eines Security-Frameworks voraus, dass ein als Basis geeignetes Frameworkkonzept existiert. Diese erste Phase befasst sich deshalb mit der Auswahl des zu verwendenden Security-Frameworks mittels eines szenarienspezifischen Anforderungskatalogs. Sie wird in Abschnitt 5.4 erläutert.
2. **Customizing des Security-Frameworks**: Die szenarienspezifische Adaption des Frameworkkonzepts entspricht der Designphase und ist per Definition vom Frameworkkonzept methodisch zu unterstützen. Wie in Abschnitt 5.5 dargelegt wird, erfordert diese Phase einen signifikanten szenarienspezifischen Aufwand, der sich zum einen aus der bislang überwiegend unzureichenden Betrachtung dieser Phase in den Frameworkkon-

zepten und zum anderen aus Randbedingungen durch den parallelen Einsatz mehrerer Security-Frameworks und anderer Sicherheitsmechanismen ergibt.

3. **Instanziierung des Security-Frameworks**: Die eigentliche Instanziierung des Security-Frameworks durch die Umsetzung seiner Komponenten und Maßnahmen entspricht der Implementierungsphase z. B. im Rahmen von Softwareentwicklungsprozessen. In dieser in Abschnitt 5.6 diskutierten Phase müssen nicht nur die im adaptierten Frameworkkonzept vorgesehenen Lösungskomponenten realisiert, sondern auch alle relevanten technischen und prozessorientierten Schnittstellen vorbereitet werden. Insbesondere können zur Integration in die vorhandene Umgebung auch die Konzeption und die Implementierung von Adaptern und anderen Schnittstellenkomponenten erforderlich werden; hieraus ergeben sich beispielsweise zusätzliche Software-Engineering-Teilprojekte.
4. **Parametrisierung, Testen und Inbetriebnahme des Security-Frameworks**: In Analogie zur ITIL v3-Phase *Serviceüberführung* und den Test- und Abnahmephasen in der Softwareentwicklung muss die Frameworkinstanz überprüft und auf die Inbetriebnahme vorbereitet werden. In Abschnitt 5.7 werden entsprechende Methoden vorgestellt, die beispielsweise auch die frameworkübergreifend einheitliche Wahl von Sicherheitsparametern thematisieren.
5. **Betrieb und Wartung des Security-Frameworks**: Die Zielsetzung der Betriebs- und Wartungsphase ist mit derjenigen von IT-Diensten vergleichbar; die Umsetzung unterscheidet sich inhaltlich und methodisch jedoch stark durch ihre IT-sicherheitsspezifische Ausprägung. In Abschnitt 5.8 werden die grundlegenden Aufgaben und Schnittstellen dieser Phase identifiziert; eine detaillierte Darstellung der Abläufe und Managementmethoden ist Gegenstand von Kapitel 6.
6. **Überarbeitung des Security-Frameworks**: Analog zur *kontinuierlichen Serviceverbesserung* in ITIL v3 kann sich im laufenden Betrieb der Bedarf zu grundlegenderen Anpassungen des Security-Frameworks, die über Routinewartungsarbeiten in der Betriebsphase hinausgehen, ergeben. In Abschnitt 5.9 wird zunächst auf mögliche Auslöser für und anschließend auf den Ablauf von größeren Änderungen an der Frameworkinstanz eingegangen.
7. **Außerbetriebnahme des Security-Frameworks**: Analog zu IT-Diensten endet der Lebenszyklus von Frameworkinstanzen mit der Außerbetriebnahme. Dabei muss jedoch differenziert werden, ob das Security-Framework nicht mehr benötigt wird, beispielsweise weil die von ihm geschützten Assets ebenfalls wegfallen sollen oder ob eine Ablösung durch ein anderes Security-Framework bzw. andere Sicherheitsmechanismen angestrebt wird. Durch die gemeinsame Nutzung von Lösungskomponenten durch mehrere Security-Frameworks ergeben sich Abhängigkeiten, die beim Rückbau der Frameworkinstanz berücksichtigt werden müssen. Die entsprechenden Abläufe werden in Abschnitt 5.10 diskutiert.

Diese Lebenszyklusphasen bauen offensichtlich aufeinander auf und können somit nicht gänzlich isoliert voneinander betrachtet werden. Als Konsequenz daraus ergibt sich zum einen, dass das in dieser Arbeit betrachtete Management von Security-Frameworks sich mit allen Phasen und nicht nur mit der den Schwerpunkt bildenden Betriebsphase auseinandersetzen muss. Zum anderen muss beim organisationsübergreifenden Einsatz von Security-Frameworks

unter Umständen auf geeignete Synchronisationsmechanismen, z. B. beim Übergang zur Betriebsphase, geachtet werden, so dass in den einzelnen Phasen entsprechende Schnittstellen vorgesehen werden müssen.

5.2.3. Verzahnung der Lebenszyklusphasen

Bei einer gesamtheitlichen Betrachtung des Lebenszyklus von Security-Frameworks müssen nicht nur die Zusammenhänge zwischen den Konzept- und Instanzlebenszyklen berücksichtigt, sondern auch weitere relevante Lebenszyklen, z. B. die der geschützten Assets, und in Phasen einteilbare Abläufe wie die kontinuierliche Verbesserung des szenarienspezifischen ISMS integriert werden.

Abbildung 5.4 veranschaulicht die sich beim praktischen Einsatz von Security-Frameworks ergebende Komplexität:

- Die **Konzeption von Security-Frameworks** kann wie in Abschnitt 5.2.1 dargestellt überwiegend autark betrachtet werden:
  - Mit der *Freigabe* einer neuen Version des Frameworkkonzepts liefert sie die Basis für die Instanziierung in beliebig vielen Szenarien.
  - In der *Praxis*-Phase des Frameworkkonzepts werden Verbesserungsmöglichkeiten identifiziert, die zusammen mit szenarienunabhängigen Änderungen im vom Security-Framework abzudeckenden Bereich in Form modifizierter und zusätzlicher Anforderungen in die Weiterentwicklung einfließen.
- Für die **Frameworkinstanzen** stellt die Verfügbarkeit eines freigegebenen Frameworkkonzepts eine essentielle Voraussetzung dar, da die Auswahlphase der Frameworkinstanz an die Freigabephase des Frameworkkonzepts anknüpft. Demgegenüber sollen Rückmeldungen an die Frameworkautoren nicht erst bei der Außerbetriebnahme einer Frameworkinstanz erfolgen. Vielmehr hängt die weitere Verbesserung des Frameworkkonzepts wesentlich davon ab, dass die Frameworkautoren Einblick in die in jeder Lebenszyklusphase gewonnenen Erfahrungen mit der Frameworkinstanz erhalten. Dies können beispielsweise die Gründe für oder gegen die Wahl eines Frameworkkonzepts in einem Szenario oder Berichte über Schwierigkeiten bei der szenarienspezifischen Anpassung sein. Auf für die Rückmeldung an Frameworkautoren relevante Aspekte wird unten bei der Beschreibung der einzelnen Lebenszyklusphasen eingegangen.
- Bei der Instanziierung von Security-Frameworks und auch bei größeren Änderungen an der Frameworkinstanz können umfangreiche Teilaufgaben anfallen, die in Form von **Projekten** realisiert werden; diese können wiederum in Phasen wie *Initiierung*, *Planung*, *Konzeption*, *Implementierung*, *Test* und *Bereitstellung* eingeteilt werden.
- Der Lebenszyklus einer Frameworkinstanz muss mit dem **Lebenszyklus der geschützten Assets** in Beziehung gesetzt werden. In Abhängigkeit davon, ob das Security-Framework zusammen mit dem zu schützenden IT-Dienst bzw. der zu schützenden IT-Architektur aufgebaut wird oder ob es nachträglich integriert werden soll, muss eine entsprechende Synchronisation spätestens in der Betriebsphase erreicht werden.
- Das **szenarienspezifische Umfeld** muss berücksichtigt werden; hierzu gehören unter anderem:

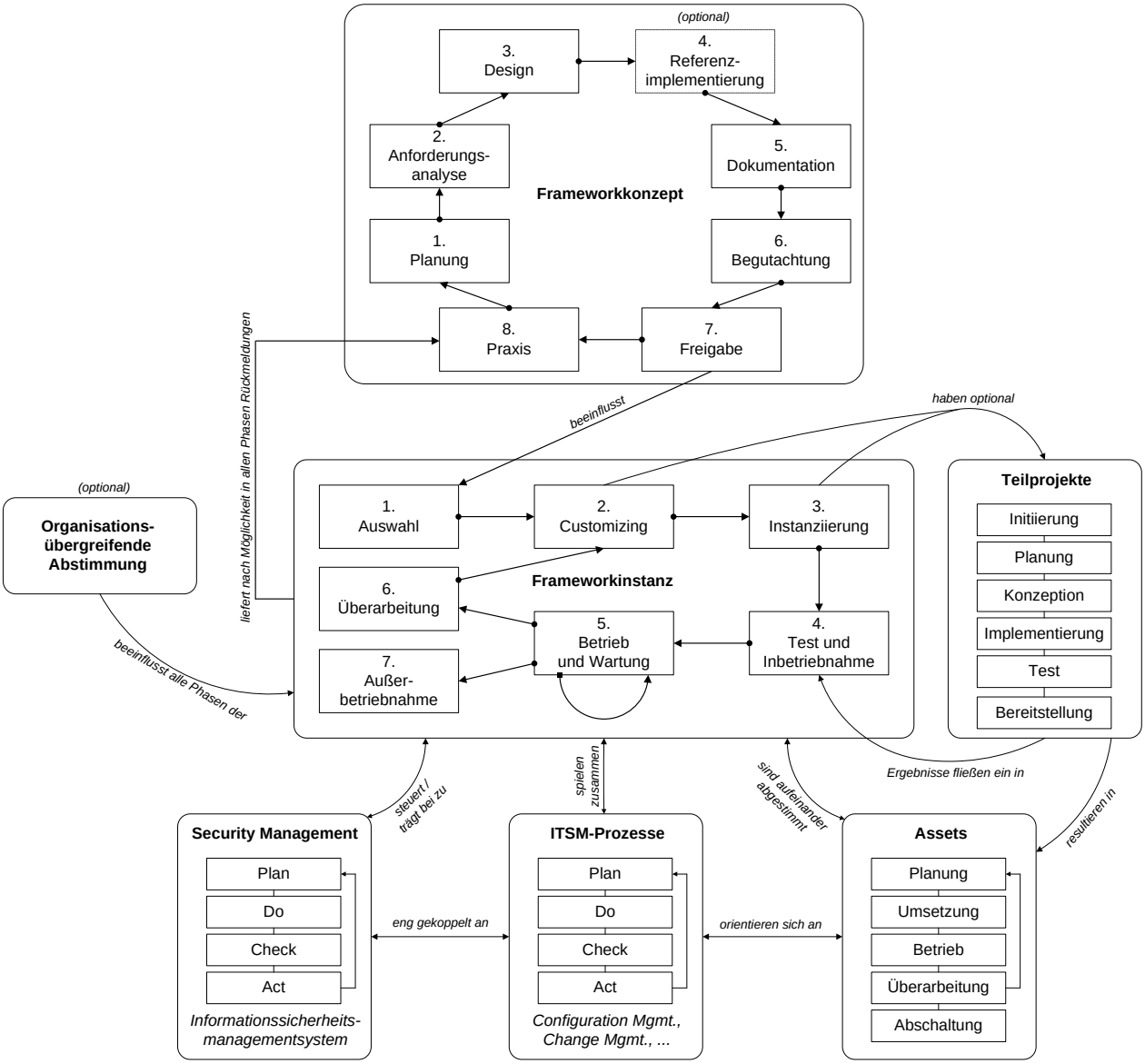


Abbildung 5.4.: Zusammenspiel der betrachteten Lebenszyklen

- Auswirkungen, die sich im Rahmen der *ITSM-Prozesse* ergeben, die als kontinuierliche Verbesserungsprozesse ebenfalls einem Lebenszyklus unterliegen.
- Konsequenzen aus den Abläufen im *Prozess IT-Sicherheitsmanagement*, beispielsweise bei Änderungen an der Informationssicherheitsleitlinie oder an Vorgaben zu frameworkübergreifend relevanten Sicherheitsparametern.
- Notwendige Abstimmungen, die sich aus dem *organisationsübergreifenden Einsatz* von Security-Frameworks ergeben und z. B. durch das Eintreten eines der genannten Aspekte bei Dritten ausgelöst werden.

Die aufgrund dieser Abhängigkeiten erforderlichen Schnittstellen werden bei der nachfolgenden Vertiefung der Instanz-Lebenszyklusphasen berücksichtigt.

5.3. Methodik zur Darstellung der Instanz-Lebenszyklusphasen von Security-Frameworks

Um den gesamten Lebenszyklus von Frameworkinstanzen durchgängig einheitlich beschreiben zu können und um die Gemeinsamkeiten und Unterschiede zwischen den einzelnen Lebenszyklusphasen – beispielsweise in Bezug auf die involvierten Personen bzw. Rollen – zu verdeutlichen, wird in den Abschnitten 5.4 bis 5.10 jeweils die folgende Struktur verwendet:

- **Zielsetzung**: Die mit der Lebenszyklusphase verfolgten qualitativen Ziele werden knapp zusammengefasst.
- **Voraussetzungen**: Neben Vorbedingungen, ohne die mit den Arbeiten der Phase nicht begonnen werden kann, werden auch Randbedingungen genannt, die für den erfolgreichen Abschluss erforderlich sind.
- **Tätigkeitsschwerpunkte**: Die Kernaufgaben und wesentlichen Abläufe, die zum Erreichen der genannten Ziele umgesetzt werden müssen, werden prägnant zusammengefasst.
- **Beteiligte Rollen**: Auf Basis der in Abschnitt 2.2.1 definierten Rollen werden die in der jeweiligen Lebenszyklusphase zu beteiligenden Personengruppen erläutert. Ohne Beschränkung der Allgemeinheit wird dabei von einem Unternehmensszenario ausgegangen, das organisationsübergreifende Abstimmungen vornehmen muss.
- **Schnittstellen**: Die gegenseitigen Abhängigkeiten und Einflüsse, die über die Komponenten und Maßnahmen der betrachteten Frameworkinstanz hinausgehen, werden skizziert. In Frage kommen dabei u. a.
  - externe Einflüsse wie die Abstimmung in organisationsübergreifenden Projekten, gesetzliche Rahmenbedingungen (Compliance) und Anforderungen, die sich beispielsweise aus Mandantenfähigkeit und Delegationsmechanismen ergeben,
  - die vom Security-Framework zu schützenden Assets,
  - ausgewählte Aspekte der bereits vorhandenen Infrastruktur, z. B. bezüglich bereits eingesetzte Sicherheitsmechanismen bzw. etablierte organisatorische Abläufe,
  - die Lebenszyklusphasen z. B. des Frameworkkonzepts,
  - die im Kontext der Diensterbringung relevanten ITSM-Prozesse,
  - die Abläufe im IT-Sicherheitsmanagement, beispielsweise im Zusammenspiel mit dem Informationssicherheitsmanagementsystem und
  - das Risikomanagement.
- **Relevante Anforderungen aus dem Kriterienkatalog**: Anhand des in Kapitel 3 erstellten Kriterienkatalogs wird erläutert, welche Anforderungen an die Security-Frameworks für die aktuelle Phase besonders bedeutsam sind. Aufgrund der anschließend in Abschnitt 5.11 vorgenommenen Auswertung wird auf diesen Aspekt jeweils relativ ausführlich eingegangen.

- **Ablauf und Methoden**: Die in der Lebenszyklusphase durchzuführenden Aktivitäten werden näher erläutert. Für einige Aktivitäten bieten sich ausgewählte Vorgehensweise und Methoden an, die ebenfalls skizziert werden.
- **Abnahmekriterien und Kontrollen**: Zur Qualitätssicherung und Sicherstellung der Zielerreichung werden phasenspezifische Abnahmekriterien definiert und beispielsweise Reviews vorgesehen.
- **Berichtswesen**: Die Phasenbeschreibung abschließend wird darauf eingegangen, welche internen und externen Stellen in geeigneter Form über den jeweils erreichten Zwischenstand informiert werden sollen. Hierzu gehören insbesondere auch die Rückmeldungen an die Frameworkautoren.

Der Umfang und die Ausprägung dieser Aspekte variieren mit ihrer Relevanz für die jeweils beschriebene Lebenszyklusphase.

5.4. Phase 1: Auswahl des Security-Frameworks

Ziele:
Die Instanziierung eines Security-Frameworks beginnt mit seiner Auswahl für ein konkretes Einsatzszenario. Der potentielle Frameworkanwender befindet sich zu Beginn in der Situation, dass der Bedarf an zusätzlichen IT-Sicherheitsmaßnahmen erkannt wurde, aber noch unklar ist, ob und welches Security-Framework für seine szenarienspezifischen Anforderungen geeignet ist. Das Ziel dieser ersten Lebenszyklusphase ist somit, ein zum Szenario passendes Security-Framework als Basis für die weiteren Phasen auszuwählen.

Voraussetzungen:
Da es sich um die erste Lebenszyklusphase handelt, muss sie von außen angestoßen werden. In Abschnitt 5.1.2 wurde eine entsprechende Vorgehensweise vorgestellt. Es kann somit davon ausgegangen werden, dass ein ausreichend detailliertes Wissen über das Umfeld im konkreten Szenario vorhanden ist und dass die mit dem Frameworkeinsatz verbundenen Ziele definiert worden sind. Diese Informationen sind für die Beurteilung in Frage kommender Security-Frameworks zwingend erforderlich.

Schwerpunkte:
Die primären Aktivitäten in dieser Phase umfassen eine Recherche, um eine Kandidatenmenge näher zu untersuchender Security-Frameworks zu bestimmen, den methodisch unterstützten Vergleich dieser Security-Frameworks und die Entscheidung, welches Security-Framework für das Szenario am besten geeignet ist bzw. ob auf alternative Sicherheitsmaßnahmen zurückgegriffen werden muss.

Rollen:
Bei der Auswahl und Beurteilung in Frage kommender Security-Frameworks handelt es sich zunächst um eine fachliche Tätigkeit, die ein *Systemarchitekt* durchzuführen hat. Um die Eignung für die zu schützenden Assets (IT-Dienste bzw. IT-Architekturen) zu beurteilen, können beispielsweise auch deren *Administratoren* hinzugezogen werden. Analog dazu sind *Designer* zu involvieren, wenn sich frühzeitig abzeichnet, dass Eigenleistungen z. B. für die Implementierung von Schnittstellenkomponenten erforderlichen werden. Zur Beratung und Beurteilung können ferner *Technologieexperten* und *Security Engineers* hinzugezogen werden.

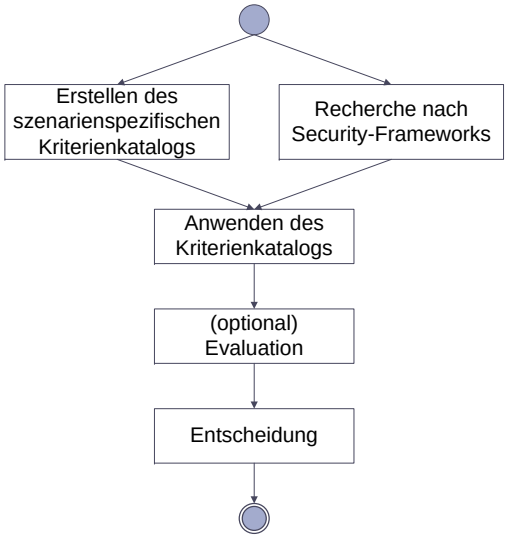
Die Planung und organisatorische Einbettung erfolgt über den *Projektleiter*, der das Vorhaben bis zur Produktivführung fachlich verantwortlich begleitet und sowohl an den *Prozesseigner*, in dessen Bereich die zu schützenden Assets fallen, als auch an den *CISO*, der stellvertretend für die Managementebene genannt wird, berichtet. Die Größe der Projektgruppe, auf deren Mitglieder diese Rollen verteilt werden, ist szenarienabhängig; gegebenenfalls sind auch weitere Interessenvertreter (Stakeholder), z. B. von Anwendern oder Kooperationspartnern, zu involvieren.

Schnittstellen:
In der Auswahlphase existieren außerhalb dieses Projektkontextes noch keine bidirektionalen Schnittstellen bzw. externe Stellen, die von den Ergebnissen unmittelbar abhängig sind. Das szenarienspezifische Umfeld liefert jedoch sämtliche Anforderungen und Randbedingungen, die zur Beurteilung der zu untersuchenden Security-Frameworks herangezogen werden müssen. So werden beispielsweise vom Risikomanagement Prioritäten vorgegeben, Teile der Assets werden eventuell bereits von anderen Security-Frameworks oder Sicherheitsmechanismen abgedeckt, durch ITSM- und andere Prozesse vorgegebene Abläufe müssen eingehalten werden und branchenspezifische Vorgeben müssen erfüllt werden. Diese Abhängigkeiten müssen bei der unten diskutierten Erstellung eines szenarienspezifischen Anforderungskatalogs berücksichtigt werden.

Relevante Anforderungen aus dem Kriterienkatalog:
Zur Unterstützung der szenarienspezifischen Auswahl passender Security-Frameworks spielen insbesondere die folgenden Anforderungen aus den beiden Kategorien *SF-FUNK* und *SF-DOKU* eine zentrale Rolle:

- Kategorie *SF-FUNK*: Über die grundlegende fachliche Eignung eines Security-Frameworks für das konkrete Szenario kann primär auf Basis der berücksichtigten *Assets* und der vorgeschlagenen *Sicherheitsmaßnahmen* entschieden werden. Die angestrebte sicherheitstechnisch-funktionale Vorauswahl ist darüber hinaus auch von den betrachteten *Schwachstellen* und *Angriffen* abhängig.
- Kategorie *SF-DOKU*: Die Aufgabe, die in Frage kommenden Security-Frameworks rasch auf eine gut handhabbare Menge zu reduzieren, wird essentiell durch die Dokumentation der *Ziele* und *Voraussetzungen* des Security-Frameworks unterstützt. Weiteren Einfluss haben die *Ausrichtung* des Security-Frameworks, die von ihm berücksichtigten *Angreifermodelle*, die im Frameworkkonzept festgehaltene *Anforderungsanalyse* und die Dokumentation der getroffenen *Designentscheidungen*. Im Frameworkkonzept enthaltene Aussagen zur *Vollständigkeit* erleichtern zudem die Identifikation zusätzlich benötigter Komponenten.

Ablauf und Methoden:
Zu Beginn der Auswahlphase, deren Ablauf in Abbildung 5.5 dargestellt ist, muss ein szenarienspezifischer Kriterienkatalog erstellt werden, anhand dessen die in Frage kommenden Security-Frameworks beurteilt werden können. In Abschnitt 3.8 wurde bereits erläutert, wie der in dieser Arbeit entwickelte Kriterienkatalog szenarienspezifisch erweitert und modifiziert werden kann, so dass hierauf nicht näher eingegangen wird. Analog dazu wurde in Abschnitt 4.1.2.1 eine Recherchemethodik vorgestellt, die unter Hinzunahme weiterer präzisierender Kriterien eine zu den im konkreten Szenario betrachteten Assets passende Kandidatenmenge von Security-Frameworks liefern kann. Sofern keine exakt passenden Security-Frameworks ermittelt werden können, muss geprüft werden, ob entweder mehrere Teillösungen



Beteiligte Rollen und ihre Zuständigkeiten (RASCI-Matrix)

	Administrator	CISO (Leitung)	Designer	Projektleiter	Prozesseigner	Security Engineer	System-architekt	Technologie-experte
Erstellen des Kriterienkat.	S	I	S	A	S	S	R	C
Recherche				A		S	R	C
Anwenden des Kriterienkat.	I	I	S	A	I	S	R	C
Evaluation	S			A		S	R	C
Entscheidung	I	A	I	R	C	C	C	C

Legende:
R – Responsible *(führt aus bzw. stößt an)*
A – Accountable *(ist verantwortlich für)*
S – Support *(unterstützt den Ausführenden bei)*
C – Consulted *(wird befragt zu)*
I – Informed *(wird informiert über Ergebnis von)*

Abbildung 5.5.: Ablauf und Zuständigkeiten in der ersten Lebenszyklusphase (Auswahl)

miteinander kombiniert werden können oder ob eine Umsetzung der szenarienrelevanten Teile eines umfassenderen Security-Frameworks möglich wären. Im Folgenden wird entsprechend davon ausgegangen, dass die Kriterien und die zu bewertenden Security-Frameworks bereits festgelegt wurden. Die Beurteilung der einzelnen Security-Frameworks erfolgt auf Basis des Kriterienkatalogs unter Berücksichtigung der folgenden Aspekte:

- Unzureichend erfüllte Kriterien bedeuten einen in Eigenleistung zu erbringenden Mehraufwand in den späteren Phasen und müssen über die Auswahl hinausgehend beim schließlich gewählten Security-Framework für die weitere Planung berücksichtigt werden.
- Bei Security-Frameworks, deren Dokumentation mangelhaft oder – beispielsweise bei kommerziellen Produkten – nicht frei zugänglich ist, muss der Erfüllungsgrad der Kriterien anderweitig, z. B. in geeigneter Abstimmung mit den Frameworkautoren ermittelt werden.
- Eigene Erfahrungen mit anderen Security-Frameworks sind insbesondere im Bereich überlappender Lösungskomponenten geeignet einzubeziehen, z. B. wenn Sicherheitsmechanismen wie Firewalls parallel für mehrere Dienste eingesetzt werden sollen.
- Sofern der Einsatz des Security-Frameworks in anderen Szenarien als Kriterium herangezogen wird (vgl. Anforderung *SF-MGMT-Praxis*), müssen entsprechende Erfahrungsberichte vorliegen; diese müssen wiederum geeignet recherchiert werden.
- Das Überprüfen der technisch-sicherheitsfunktionalen Eigenschaften des Security-Frameworks auf seine szenarienspezifische Eignung ist aufwendig und sollte durch einen Security Engineer erfolgen. Es muss sichergestellt werden, dass die im Frameworkkonzept vorgesehenen Maßnahmen die szenarienspezifischen IT-Sicherheitsanforderungen

vollständig abdecken bzw. dass alle noch fehlenden Komponenten identifiziert wurden und bei der weiteren Planung berücksichtigt werden können.

Um Unterschiede im Lösungsumfang der einzelnen Security-Frameworks zu berücksichtigen, muss in die Gegenüberstellung neben dem Ergebnis der Beurteilung mit dem Kriterienkatalog auch einfließen, welcher zusätzliche Aufwand zur Umsetzung der szenarienspezifischen Anforderungen anfällt. Mit Hilfe einer Bewertungsformel (vgl. Abschnitt 3.7.1) kann eine Rangliste erstellt werden, deren Stabilität beispielsweise im Rahmen einer Sensitivitätsanalyse geprüft werden sollte. Hierfür können z. B. alle niedrig priorisierten Anforderungen weggelassen werden; im Idealfall bleibt die Rangfolge zumindest in den vorderen Plätzen davon unberührt.

Optional schließt sich eine Evaluationsphase an, in der die Umsetzbarkeit des am besten geeigneten Security-Frameworks – oder ggf. einer kleinen Auswahl der nach Abschluss der Auswertung des Kriterienkatalogs verbleibenden Kandidaten – in einer Testumgebung untersucht wird. Hierbei kann einerseits überprüft werden, ob der bei der bereits durchgeführten Bewertung entstandene positive Eindruck auch in der Praxis aufrecht erhalten werden kann. Andererseits ergeben sich potentiell Korrekturen an den Bewertungen der einzelnen Kriterien, die auf Basis der Dokumentation unzutreffend beurteilt wurden. Im Allgemeinen ist die Aussagekraft der Evaluation in einer klassischen Testumgebung jedoch nicht besonders hoch, da die komplexen realen Anforderungen erst nach Durchlaufen der Customizingphase erfüllt werden könnten. Der Aufwand, eine realitätsnahe Testumgebung zu schaffen und das Security-Framework für eine Evaluation daran anzupassen, ist in der Regel jedoch äußerst hoch und wird in der Auswahlphase vermieden, so dass insbesondere kein praktischer Vergleich zwischen einer größeren Anzahl an Security-Frameworks durchgeführt werden kann. Erste praktische Gehversuche können jedoch dazu beitragen, den Aufwand für die nächsten Phasen noch besser planen zu können.

Auf der Grundlage der ermittelten Rangfolge und der optionalen Evaluationsergebnisse muss abschließend entschieden werden, ob ein für das Szenario passendes Security-Framework ermittelt werden konnte. Sofern dies nicht der Fall ist, muss entschieden werden, ob die Auswahlphase mit anderen Parametern erneut durchlaufen werden soll oder ob alternative Sicherheitslösungen analysiert werden müssen.

Abnahmekriterien und Kontrollen:
Die Auswahlphase kann beendet werden, sobald eine begründete und dokumentierte Entscheidung für *ein* Security-Framework sowie eine Übersicht über voraussichtlich zusätzlich benötigte Komponenten vorliegen, die von der Projektleitung genehmigt werden. Zur Qualitätssicherung empfiehlt es sich, die anhand des Kriterienkatalogs durchgeführte Bewertung durch einen Dritten nachvollziehen zu lassen, um potentielle subjektive Fehleinschätzungen auszuschließen. Falls sich herausgestellt hat, dass kein für das Szenario geeignetes Security-Framework verfügbar ist, wird der Lebenszyklus abgebrochen.

Berichtswesen:
Die Ergebnisse der Auswahl müssen primär szenarienintern kommuniziert werden. Neben dem CISO, der in Abstimmung mit den Prozesseignern und unter Berücksichtigung der Meinung der technischen Experten über die Fortführung des Vorhabens entscheidet, sind auch die Administratoren der mit dem Security-Framework zu schützenden Assets zu informieren, sofern sie nicht bereits zur Projektgruppe gehören, um die in den nächsten Phasen erforderlichen Planungen vornehmen zu können. Schließlich sollten auch die Autoren des gewählten bzw. der unterlegenen Security-Frameworks informiert werden; dabei sollten insbesondere die nicht

ausreichend erfüllten Anforderungen kommuniziert werden, um zukünftige Verbesserungen anzuregen.

5.5. Phase 2: Customizing des Security-Frameworks

Ziele:
Durch die Anpassung des Security-Frameworks sollen einerseits seine sicherheitsfunktionalen Eigenschaften auf die szenarienspezifischen Anforderungen abgebildet werden; andererseits muss auch seine nahtlose Integration in die bereits vorhandene Infrastruktur konzeptionell vorbereitet werden. Durch den parallelen Einsatz mehrerer Security-Frameworks kann es zu Redundanzen insbesondere bei den durch die Frameworkkonzepte vorgesehenen technischen Sicherheitsmechanismen kommen; diese müssen erkannt und nach Möglichkeit in Synergien gewandelt werden.

Voraussetzungen:
Die Customizingphase knüpft – von Schritten zur Genehmigung des weiteren Vorgehens abgesehen – nahtlos an die Auswahlphase an und arbeitet auf Grundlage des ausgewählten Security-Frameworks und der identifizierten zusätzlich erforderlichen Komponenten. Sie setzt jedoch auch das in Abschnitt 5.1.1 diskutierte Wissen über das Szenario voraus, um die Integration des Security-Frameworks sowohl in technischer als auch organisatorischer Hinsicht vorbereiten zu können.

Schwerpunkte:
Die Tätigkeitsschwerpunkte liegen in dieser rein konzeptionellen Phase auf der szenarienspezifischen Überarbeitung des Frameworkkonzepts und der Erstellung dafür spezifischer Betriebs- und Managementkonzepte.

Rollen:
Das Vorgehen involviert neben dem fachlich verantwortlichen *Projektleiter* wiederum *Systemarchitekten* und gegebenenfalls die *Administratoren* der vom Security-Framework zu schützenden Assets. Für die über die im Frameworkkonzept vorgesehenen hinausgehend erforderlichen Komponenten sind *System- bzw. Softwaredesigner* hinzuzuziehen. Die z. B. durch den *CISO* vertretene Leitungsebene entscheidet über die Umsetzung des Ergebnisses; die *Prozesseigner* werden ebenso wie *Security Engineers* und *Technologieexperten* beratend hinzugezogen.

Schnittstellen:
Aufgrund des planerischen Charakters der Customizingphase müssen bereits alle für den späteren Betrieb relevanten Schnittstellen berücksichtigt werden. Die Vorgehensweise bei der Anpassung hängt deshalb zum einen davon ab, ob und in welchem Umfang das Security-Framework seine szenarienspezifische Adaption methodisch unterstützt, und zum anderen davon, welche szenarienspezifischen Vorgaben beispielsweise im Rahmen des ITSM-Prozesses Change Management berücksichtigt werden müssen. Insbesondere muss berücksichtigt werden, dass die Integration des Security-Frameworks im Allgemeinen bilaterale Anpassungen, d. h. neben der Einführung frameworkspezifischer neuer Komponenten auch Modifikationen an der bestehenden Infrastruktur, z. B. den zu schützenden Assets, erfordert. Inhaltliche Aspekte der Anpassung unterliegen gegebenenfalls externen Einflüssen wie der organisationsübergreifenden Abstimmung der Frameworkarchitektur und müssen sich an den allgemeinen sicherheitsspezifischen Vorgaben, z. B. der Informationssicherheitsleitlinie, orientieren. Die

Schwerpunkte der sicherheitsfunktionalen Anpassungen richten sich nach den bereits in der Auswahlphase bekannten Anforderungen und werden somit in enger Kopplung mit dem Risikomanagement priorisiert.

Relevante Anforderungen aus dem Kriterienkatalog:
Auf die Customizingphase wirken sich in erster Linie die Anforderungen der Kategorie *SF-INT* aus: Neben Vorgaben zur Vorgehensweise bei der Anpassung, die dem Kriterium *SF-INT-Customizing* eine grundlegende Bedeutung verleihen, sind dabei zunächst die *Modularität* und die Möglichkeit, eigene *Erweiterungen* einzubringen, relevant. Darüber hinaus wirken sich auch die Optionen zur Planung von *Ausbauphasen*, die *Kompatibilität* mit und die *Wiederverwendbarkeit* von bereits vorhandenen Infrastrukturkomponenten sowie die *Skalierbarkeit* unmittelbar aus. In die Planungen müssen ferner die Möglichkeit zum *Parallelbetrieb* weiterer Sicherheitsmechanismen, Aspekte der *Hochverfügbarkeit* und die *Usability* der Frameworkkomponenten einbezogen werden. Im Kontext des organisationsübergreifenden Frameworkeinsatzes ist zudem die *Polyinstanziierbarkeit* zu beachten.

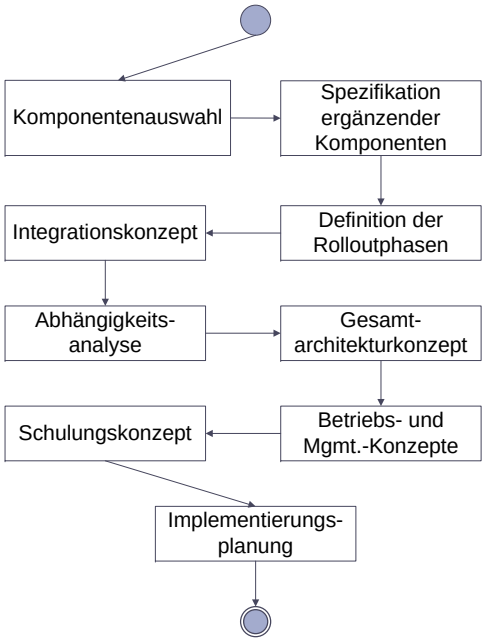
Die Dokumentation des Frameworkkonzepts unterstützt die Anpassung darüber hinaus, wenn die von ihm abgedeckten *Lifecyclephasen* benannt, *Checklisten* zu den Einzelschritten und Kriterien zur *Beurteilung* der Ergebnisse enthalten sind. Die direkte Übertragbarkeit des Frameworkkonzepts auf das eigene Szenario hängt ferner von der *Zielgruppe* des Frameworkkonzepts, seiner *Vollständigkeit* und der Dokumentation der *Ausrichtung*, *Angreifermodelle*, *Anforderungsanalyse* und *Designentscheidungen* ab (vgl. entsprechende Anforderungen in der Kategorie *SF-DOKU*).

Die resultierende technische Architektur ist abhängig von den vom Frameworkkonzept berücksichtigten *Assets*, von den vorgesehenen *Maßnahmen*, von der Unterstützung der *Automatisierung* im späteren Betrieb relevanter Abläufe und von den *Auditing*-Mechanismen. Für organisationsübergreifende Vorhaben muss zudem die Möglichkeit zur gegenseitigen *Abschottung* berücksichtigt werden (vgl. Anforderungskategorie *SF-FUNK*).

Die zu planenden Betriebs- und Managementkonzepte hängen von den im Frameworkkonzept vorgesehenen *Administrationskonzepten*, *Schulungen*, *ITSM-Schnittstellen* und *Prozessen* ab und profitieren davon, wenn die *Zuständigkeiten* für die *Managementoperationen* bereits definiert sind. Die Analyse von Aufwand und Mehrwert wird erleichtert, wenn Informationen über *Kosten* und Möglichkeiten zur *Quantifizierung* der Auswirkungen auf das Sicherheitsniveau, u. a. in Form von *Metriken* bekannt sind. Die Planung der Ausbaustufen kann mit dem *Releasezyklus* des Security-Frameworks verzahnt werden; in Abhängigkeit vom Szenario sind auch die *delegierte Administration*, die *Mandantenfähigkeit* und Aspekte der *Compliance* relevant (vgl. Anforderungskategorie *SF-MGMT*).

Ablauf und Methoden:
Zur Anpassung des Security-Frameworks an das Szenario müssen zunächst wie in Abbildung 5.6 dargestellt die umzusetzenden Frameworkkomponenten festgelegt werden. Diese können sich bei organisations- oder standortübergreifenden Vorhaben in jeder Instanz unterscheiden, so dass die gesamte Customizingphase gegebenenfalls – zumindest in Teilen – mehrfach durchgeführt werden muss; bei geeigneter Abstimmung kann dies parallel erfolgen. Die Auswahl der Module und deren nachfolgende szenarienspezifische Anpassung muss sich an den szenarienspezifischen Angreifermodellen, Angriffen und Schwachstellen orientieren und erfolgt somit risiko- bzw. prioritätsgetrieben.

Im nächsten Schritt müssen die Rollout-Phasen definiert werden, die sich sowohl auf die inkre-



Beteiligte Rollen und ihre Zuständigkeiten (RASCI-Matrix)

	Administrator	CISO (Leitung)	Designer	Projektleiter	Prozesseigner	Security Engineer	Systemarchitekt	Technologieexperte
Komponentenauswahl				A	I	S	R	C
Zusätzliche Komponenten			R	A	I	S	S	C
Rolloutphasen	C	I		A	S		R	
Integrationskonzept	S	I	S	A	C		R	
Abhängigkeitsanalyse	C		S	A	I		R	
Gesamtarchitektur	I	I	I	A	I	S	R	C
Betriebs- und Mgmt.-Konzept	S	I	C	A	S		R	
Schulungskonzept		I		A	R		S	C
Impl.-Planung	I	A	I	R	C		C	

Legende:
R – Responsible *(führt aus bzw. stößt an)*
A – Accountable *(ist verantwortlich für)*
S – Support *(unterstützt den Ausführenden bei)*
C – Consulted *(wird befragt zu)*
I – Informed *(wird informiert über Ergebnis von)*

Abbildung 5.6.: Ablauf und Zuständigkeiten in der zweiten Lebenszyklusphase (Customizing)

mentelle Umsetzung des Security-Frameworks an einem Standort als auch den organisations- bzw. standortübergreifenden Einsatz unter Berücksichtigung der sich daraus ergebenden Abhängigkeiten beziehen. Bei der Planung der Rollout-Phasen müssen jedoch auch die Pläne zur Weiterentwicklung der Infrastruktur, insbesondere der vom Security-Framework zu schützenden Assets, berücksichtigt werden.

Das weitere Vorgehen bezieht sich auf die als nächstes anzugehende Rollout-Phase unter geeigneter Berücksichtigung der geplanten finalen Ausbaustufe. Es beginnt mit der Integrationsplanung:

- Es muss festgelegt werden, welche der bereits in der Infrastruktur vorhandenen Komponenten (z. B. Firewalls oder Datenbankserver) für die Implementierung des Security-Frameworks genutzt werden können bzw. neu aufgebaut werden müssen.

  Hierfür sind die von vielen Security-Frameworks pro ausgewähltem Modul angebotenen Realisierungsalternativen auszuwerten. Neben einer Berücksichtigung der lokalen Gegebenheiten muss z. B. bei organisationsübergreifenden Projekten darauf geachtet werden, ob eine instanzenübergreifend einheitliche Lösung erforderlich oder möglich ist. Bei neu oder zusätzlich benötigten Komponenten ist auf deren Kompatibilität mit der vorhandenen Infrastruktur zu achten; gegebenenfalls sind vom Frameworkkonzept abweichende Alternativen zu ermitteln und untersuchen.

Sowohl die Wiederverwendung bereits vorhandener Komponenten als auch die Einführung neuer Komponenten muss frühzeitig im Rahmen des Change Managements berücksichtigt werden, über das weitere Prozesse wie z. B. die Erweiterung der Kapazität bestehender Dienste, der Aufbau neuer Dienste und die Ressourcenplanung angestoßen werden.

Bei den zusätzlich benötigten Komponenten muss berücksichtigt werden, dass u. U. komplexe Software- oder Systementwicklungsprojekte angestoßen werden müssen. In diesem Fall ist eine Spezifikation der Anforderungen, beispielsweise in Form eines Lastenhefts, erforderlich, bevor die Planungen zur Einführung und zum Betrieb durchgeführt werden können. Für den Fall, dass die Implementierung der somit spezifizierten Komponenten ebenfalls in Eigenregie durchgeführt werden soll, muss ein entsprechendes Implementierungsprojekt vorbereitet werden, das wiederum in Phasen wie die Erstellung des Pflichtenhefts (Planung), die Analyse der Anforderungen, das Design der Komponente, die Implementierung, Tests und Vorbereitungen zur Produktivführung eingeteilt werden kann. Auf diese Abläufe wird in den nachfolgenden Abschnitten näher eingegangen, da sie parallel zur übrigen Instanziierung des Security-Frameworks und dessen Vorbereitungen zur Produktivführung stattfinden.

- Die sich aus der Frameworkarchitektur ergebenden Abhängigkeiten, beispielsweise zwischen den zu schützenden Assets und den Frameworkkomponenten sowie deren Abhängigkeiten von der bereits vorhandenen Infrastruktur müssen dokumentiert und analysiert werden. Dabei muss insbesondere auf die Skalierbarkeit und bestehende Hochverfügbarkeitsanforderungen geachtet werden; ebenso müssen die Auswirkungen auf die Performanz des Gesamtsystems abgeschätzt werden.
- Als Vorlage für die technische Umsetzung in der nächsten Lebenszyklusphase muss ein Gesamtarchitekturkonzept erstellt werden, das mindestens die zu schützenden Assets, die in der geplanten Rollout-Phase relevanten Frameworkkomponenten und die Infrastrukturbestandteile, zu denen sich direkte Abhängigkeiten ergeben, umfasst.

  Auf dieser Basis müssen ferner die Auswirkungen des Security-Frameworks auf bestehende Ablaufbeschreibungen, Policies und Sicherheitsmechanismen dokumentiert werden und gegebenenfalls notwendige Änderungen an diesen über das Change Management eingebracht werden.

Neben dieser technikgetriebenen Einbettung muss durch die Erstellung szenarien- und frameworkspezifischer Betriebs- und Managementkonzepte auch die organisatorische Integration geplant werden. Hierbei sind u. a. die folgenden Aspekte, zu denen entsprechende Anforderungen an die Security-Frameworks bereits in Kapitel 3 diskutiert wurden, zu betrachten:

- Für die Komponenten des Security-Frameworks muss ein Administrationskonzept erstellt werden, aus dem die Betriebs- und Wartungsaufgaben hervorgehen. Sofern sich durch das Security-Framework Änderungen an den Administrationskonzepten für die geschützten Assets ergeben, sind auch diese mit einzubeziehen. Ebenso muss der jeweils szenarienspezifische Bedarf an delegierter Administration und Automatisierung berücksichtigt werden.
- Die mit dem Security-Framework neu eingeführten Komponenten sind konzeptionell über geeignete Werkzeuge in die bestehenden Managementarchitekturen zu integrieren.

Hierzu gehören beispielsweise die Planung der Überwachung über Monitoringsysteme und der Integration in Reportingwerkzeuge.

- Die in Kapitel 6 im Detail betrachteten Schnittstellen zu den ITSM-Prozessen müssen geplant werden. Hierzu gehören u. a. die Festlegung der IT-sicherheitsspezifischen SLA-Parameter und der Schnittstelle zum Incident Management.
- Für alle genannten Teilbereiche sind die Zuständigkeiten, z. B. durch Benennung entsprechender Betriebsgruppen, festzulegen.

Im Rahmen der Anpassung ist darüber hinaus zu ermitteln und festzulegen, in welchem Umfang Schulungen für verschiedene Zielgruppen (z. B. Administratoren oder Anwender) erforderlich werden und ob hierfür – beispielsweise aufgrund des Umfangs der durchgeführten Anpassungen – eigene Schulungsunterlagen erstellt werden müssen.

Auf Basis der technischen und organisatorischen Integrationskonzepte muss anschließend das weitere Vorgehen bei der Einführung des Security-Frameworks geplant werden. Dies umfasst eine Zeit- und Ressourcenplanung für die Implementierungs- und Testphasen sowie die frühzeitige Ankündigung angestrebter Rollout-Termine. Neben der damit verbundenen Ermittlung der voraussichtlichen Investitionskosten müssen darüber hinaus die Planungen für den späteren Betriebsaufwand angestoßen werden; die entsprechenden Schätzungen werden in den nächsten Lebenszyklusphasen verfeinert.

Abnahmekriterien und Kontrollen:
Bei der Abnahme des szenarienspezifisch adaptierten Security-Frameworks durch die Managementebene müssen die genannten drei Teilbereiche berücksichtigt werden:

1. *Fachliche Prüfung*: Es muss, beispielsweise unter Zuhilfenahme der im Frameworkkonzept gelieferten Checklisten, sichergestellt werden, dass alle relevanten Frameworkbestandteile angepasst wurden und die szenarienspezifischen IT-Sicherheitsziele mit der resultierenden, dokumentierten Frameworkarchitektur erreicht werden können. Diese Überprüfung kann beispielsweise von Security Engineers vorgenommen werden, die am Customizing nicht selbst beteiligt waren; es sollte darauf geachtet werden, dass Ähnlichkeiten zu im Szenario bereits erfolgreich eingesetzten vergleichbaren Sicherheitslösungen (z. B. andere Security-Frameworks) bestehen. Bei dieser Analyse müssen auch die Spezifikationen für im Rahmen von Softwareentwicklungsprojekten neu zu entwickelnde Komponenten berücksichtigt werden.
2. *Prüfung der organisatorischen Einbettung*: Die Vollständigkeit und Umsetzbarkeit der erarbeiteten Betriebs- und Managementkonzepte muss beurteilt werden. Neben der formalen Prüfung, beispielsweise anhand von Leitlinien zur Prozessdokumentation und zum Knowledge Management, ist eine inhaltliche Beurteilung vorzunehmen, in die beispielsweise das Change Advisory Board aus dem ITSM-Prozess Change Management herangezogen werden kann.
3. *Vorläufige Budgetprüfung*: Die mit dem szenarienspezifisch angepassten Security-Framework verbundenen, geschätzten Investitions-, Entwicklungs- und Betriebskosten müssen daraufhin geprüft werden, ob sie sich in einem akzeptablen Rahmen bewegen.

Gegebenenfalls müssen einzelne Aspekte der szenarienspezifischen Anpassung überarbeitet werden; sofern mit dem ausgewählten Security-Framework keine Lösung erarbeitet werden kann, mit der die fachlichen, organisatorischen und finanziellen Ziele erreicht werden können,

ist ein Rücksprung in die Auswahlphase erforderlich. In organisationsübergreifenden Projekten sollte die Entscheidung zur Fortführung der Aktivitäten gesamtheitlich getroffen werden, um die folgenden Implementierungskosten zu vermeiden, solange die szenarienweite Umsetzbarkeit noch nicht feststeht.

Berichtswesen:
Die erstellten technischen und organisatorischen Konzepte sind einerseits den unmittelbar davon betroffenen Zielgruppen, z. B. den Administratoren der Dienste, die das Security-Framework schützen soll, vorzulegen. Andererseits sollten auch Rückmeldungen von Gremien, die sich beispielsweise im Rahmen des IT-Sicherheitsmanagements mit Sicherheitsmechanismen und entsprechenden organisatorischen Maßnahmen auseinandersetzen, und Betriebsgruppen, die für die Überwachung und Wartung der vorgesehenen Lösungskomponenten zuständig sein werden, eingeholt werden.

Die Ergebnisse der szenarienspezifischen Anpassung sollten auch wiederum an die Frameworkautoren gemeldet werden; von Interesse sind dabei primär die Gründe, die zur Auswahl der pro Frameworkmodul angebotenen Lösungsalternativen geführt haben, und die zusätzlichen Komponenten, die zur Integration in die bestehende Infrastruktur erforderlich sind, aber im Frameworkkonzept bislang nicht vorgesehen waren. Die Frameworkautoren haben auf dieser Basis die Möglichkeit, die im Frameworkkonzept vorgesehenen Lösungsbausteine noch besser an den Bedarf in realen Szenarien anzupassen bzw. Vereinfachungen durch Weglassen praktisch oftmals nicht benötigter Bestandteile durchführen zu können.

5.6. Phase 3: Instanziierung des Security-Frameworks

Ziele:
In der Instanziierungsphase wird das in den vorhergehenden Phasen ausgewählte und an das Einsatzszenario angepasste Security-Framework implementiert. Dies umfasst die dokumentierte Bereitstellung der einzelnen Frameworkkomponenten und die Implementierung der Schnittstellen zu den vorhandenen Infrastrukturbestandteilen, die für eine nahtlose Integration erforderlich sind. Die Realisierung der Framework- und Schnittstellenkomponenten ist – dem in der Customizingphase ermittelten Bedarf entsprechend – gegebenenfalls mit System- bzw. Softwareentwicklungsprojekten verbunden, die bis zum Ende dieser Phase abgeschlossen werden.

Voraussetzungen:
Die in der Instanziierungsphase durchzuführenden Tätigkeiten hängen fachlich primär von den Ergebnissen der vorangegangenen Customizingphase ab; die Realisierbarkeit bedingt inhaltlich ferner die Korrektheit der Annahmen über das Umfeld des Szenarios – beispielsweise ergibt sich eine Abhängigkeit davon, ob Parallelprojekte wie etwa die erste Inbetriebnahme der vom Security-Framework zu schützenden Assets im Gesamtzeitplan liegen. Organisatorisch und fiskalisch ist diese Phase in der Regel mit dem höchsten Aufwand verbunden, da Investitions- und Implementierungskosten anfallen und mehr Personal pro Zeiteinheit gebunden wird als in den anderen Phasen.

Schwerpunkte:
Unabhängig von der Szenariengröße liegen die Schwerpunkte auf der Beschaffung bzw. Implementierung der benötigten Komponenten des Security-Frameworks und deren Inbetrieb-

nahme im Rahmen einer Testumgebung. Mit zunehmender Szenarienkomplexität bedeutet dies jedoch die i. A. parallele Realisierung vieler Frameworkkomponenten und somit einen erheblichen Koordinations- und Projektleitungsaufwand.

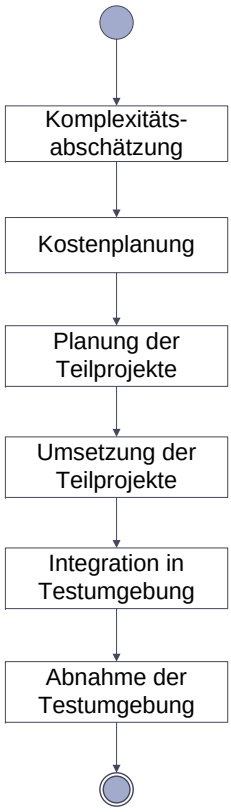
Rollen:
Alle Aktivitäten im Rahmen der Instanziierung werden von einem *Gesamtprojektleiter* koordiniert, der bei der Implementierung einzelner Frameworkkomponenten, insbesondere wenn diese durch eigene Entwicklungsprojekte umgesetzt werden, von *Teilprojektleitern* unterstützt wird. Die Zusammenstellung der einzelnen Komponenten zum Security-Framework als Ganzem wird weiterhin von einem *Systemarchitekten* begleitet. Bei der Umsetzung der Komponenten werden optional deren zukünftige *Administratoren* und eventuell auch *Anwender* hinzugezogen. Die Entwicklungsaufgaben im Rahmen der Instanziierung werden von *Designern* spezifiziert und von *Entwicklern* sowie ggf. *Security Engineers* ausgeführt. Der *CISO* wird ebenso wie die *Prozesseigner* über den Fortschritt der Umsetzung auf dem Laufenden gehalten und bildet zusammen mit dem Gesamtprojektleiter die Schnittstelle zur Entscheiderebene, von der z. B. die Teilprojektbudgets genehmigt werden müssen.

Schnittstellen:
Im Kontext des Projekts zur Frameworkeinführung ist gegebenenfalls zunächst wieder die organisations- bzw. standortübergreifende Abstimmung der einzelnen Implementierungsaktivitäten erforderlich. Der Schwerpunkt liegt jedoch auf der Realisierung der technischen und organisatorischen bzw. prozessualen Schnittstellen. Zum einen müssen die Schnittstellen, die die Frameworkkomponenten untereinander bzw. zu den weiteren Infrastrukturkomponenten benötigen, technisch umgesetzt werden, um beispielsweise das Zusammenspiel zwischen geschützten Assets und Security-Framework zu ermöglichen. Zum anderen müssen Anpassungen an den unternehmensinternen Abläufen vorgenommen werden, so dass z. B. die Komponenten des Security-Frameworks nicht nur im Monitoringsystem erfasst werden, sondern dass auch die Berichterstattung entsprechend ausgeweitet wird. Entsprechend sind Verknüpfungen zu vielen ITSM-Prozessen und insbesondere zum IT-Sicherheitsmanagement vorzusehen.

Relevante Anforderungen aus dem Kriterienkatalog:
Der in dieser Phase zu erbringende szenarienspezifische Eigenaufwand hängt technisch von den im Frameworkkonzept vorgesehenen *Maßnahmen* und ihren *Auditing*-Schnittstellen ab: Je konkreter diese beschrieben sind und falls z. B. Schnittstellenkomponenten bereits in Form einer Referenzimplementierung verfügbar sind, desto weniger eigene Konzeptions- und Implementierungsarbeiten sind erforderlich (vgl. Anforderungskategorie *SF-FUNK*).

Die technische Integration in die vorhandene Infrastruktur hängt von der *Kompatibilität* der Frameworkkomponenten ab. Darüber hinaus hat die Beschreibung des Vorgehens bei ihrer *Einführung* Einfluss auf die Umsetzung (vgl. Anforderungskategorie *SF-INT*).

Die organisatorische Einbettung ist hingegen primär auf die in der Anforderungskategorie *SF-MGMT* zusammengefassten Eigenschaften angewiesen: Zunächst ist maßgeblich relevant, ob die Auswirkungen auf die IT-Sicherheitsleitlinie und andere *Policies* bereits definiert sind. Im Idealfall werden vom Frameworkkonzept ferner die *ITSM-Schnittstellen*, *Managementprozesse* und *Managementoperationen* sowie die zu implementierenden *Metriken* und deren Auswirkungen auf das *Berichtswesen* vorgegeben. Vorgefertigte Spezifikationen bezüglich durchzuführender *Tests* tragen zur Sicherstellung der Qualität der entwickelten Komponenten bei und Anregungen zu *Schulungsinhalten* unterstützen das Vorhaben, das für die nachfolgende Inbetriebnahme und den späteren Betrieb erforderliche Personal geeignet fortzubilden.



Beteiligte Rollen und ihre Zuständigkeiten
(RASCI-Matrix)

	Administrator	Anwender	CISO (Leitung)	Designer	Entwickler	Gesamt-projektleiter	Prozesseigner	Security Engineer	System-architekt	Teilprojekt-leiter
Komplexitäts-abschätzung			I	S		A	I		R	S
Kostenplanung			A	S		R	C		S	S
Teilprojekt-planung			I	C	I	A	I		S	R
Umsetzung der Teilprojekte	C		I	S	S	A	I	S	S	R
Integration in Testumgebung	S	C	I		S	A	I	S	R	S
Abnahme	I		A	I	I	R	C	C	C	C

Legende:
R – Responsible *(führt aus bzw. stößt an)*
A – Accountable *(ist verantwortlich für)*
S – Support *(unterstützt den Ausführenden bei)*
C – Consulted *(wird befragt zu)*
I – Informed *(wird informiert über Ergebnis von)*

Abbildung 5.7.: Ablauf und Zuständigkeiten in der dritten Lebenszyklusphase (Instanziierung)

Ablauf und Methoden:
Der Ablauf der Instanziierungsphase hängt stark vom Umfang und der Komplexität des Szenarios und des daran angepassten Security-Frameworks ab. Während in einfachen Fällen nur wenige Komponenten hinzukommen, deren Einbettung in die Managementabläufe keine umfangreichen Änderungen erfordert, sind komplexe Szenarien möglich, in denen eine Vielzahl von Eigenentwicklungen erforderlich wird, die zum Teil zu bereits vorhandenen Komponenten im Widerspruch stehen und umfassende Anpassungen an den Managementabläufen erfordern. Im ersten Schritt ist deshalb wie in Abbildung 5.7 dargestellt eine *Komplexitätsabschätzung* erforderlich, wobei entsprechende Methoden aus der Softwareentwicklung i. d. R. nur für einzelne Teilbereiche eingesetzt werden können. In den übrigen Bereichen und insbesondere bei der Umsetzung der angepassten organisatorischen Abläufe muss meist auf die Schätzungen durch Experten zurückgegriffen werden, die einerseits das Szenario kennen und andererseits auf Erfahrungswerte zurückgreifen können, beispielsweise durch den Einsatz anderer Security-Frameworks im selben Szenario oder den Einsatz desselben Security-Frameworks in anderen Szenarien.

Im zweiten Schritt müssen die anfallenden *Kosten* ermittelt werden. Für die durch das Security-Framework neu hinzukommenden Komponenten müssen dabei u. a. die Investitionskosten für Hardware, beispielsweise Servermaschinen und Netzkomponenten, Softwarelizen-

zen, erforderliche Schulungsmaßnahmen und zur Implementierung benötigtes, ggf. externes Personal berücksichtigt werden. In die Gesamtkalkulation müssen darüber hinaus jedoch auch der Koordinations- und Projektleitungsaufwand, die Entwicklungs- und Implementierungskosten sowie den an anderen Stellen im Szenario durch Anpassungsaufgaben entstehenden Aufwand eingehen. Das Ergebnis dieser Planungen stellt eine Verfeinerung der am Ende der Customizingphase durchgeführten Schätzung dar und muss den Entscheidern zur Genehmigung der weiteren Schritte vorgelegt werden.

Als dritter Schritt erfolgt die detaillierte *Planung der Teilprojekte*, indem die jeweils zu erbringenden Ergebnisse (engl. *deliverables*) und Meilensteine festgelegt werden. Dementsprechend müssen die Modalitäten für Zwischenüberprüfungen, Abnahmeprozeduren und Eckpunkte des Berichtswesens festgelegt werden. Die Entwicklungs- und Implementierungsarbeiten sollten dabei generell anerkannten Methoden und Best Practices der Softwareentwicklung und des IT Service Management folgen. Hierzu gehört insbesondere die auch in ISO/IEC 27001 aus Perspektive des IT-Sicherheitsmanagements geforderte Trennung in Entwicklungs-, Test-, Integrations- und Produktivumgebungen, für die entsprechende Ressourcen eingeplant und bereitgestellt werden müssen. In der aktuellen Lebenszyklusphase ist somit vorzusehen, dass die Implementierung der einzelnen Frameworkkomponenten in dedizierten Entwicklungsumgebungen erfolgt und diese schließlich in einer gemeinsamen Testumgebung evaluiert werden können. Die Integrations- bzw. Produktivumgebungen sind entsprechend in den weiteren Phasen relevant. Für die Testumgebung muss die Möglichkeit geschaffen werden, ausreichend komplexe und realistische Anwendungsfälle umzusetzen, um eine für den späteren praktischen Einsatz brauchbare Bewertung der durchgeführten Entwicklungen vornehmen zu können.

Die *Umsetzung* der geplanten und genehmigten Teilprojekte wird als vierter Schritt vollzogen; dabei sind insbesondere die folgenden Kernaspekte zu berücksichtigen:

- Die Beschaffung der Frameworkkomponenten muss initiiert werden; hierzu gehört auch der Beginn der eigenen Entwicklungsprojekte.
- Beschaffte Hard- und Softwarekomponenten müssen installiert und grundlegend für den Einsatz in der Testumgebung konfiguriert werden. Die vollständige szenarienspezifische Konfiguration mit den später auch für den Produktivbetrieb erforderlichen Parametern erfolgt jedoch erst in Phase 4 (siehe Abschnitt 5.7).
- Parallel zu allen Entwicklungen müssen die unten als Abnahmekriterien definierten Dokumentationen erstellt werden. Zudem muss ebenfalls bereits in dieser Phase durch Schulungsmaßnahmen z. B. für die Administratoren der vom Framework geschützten Assets, die designierten Betreiber der Frameworkkomponenten, und die von den Schnittstellen zum IT-Sicherheitsmanagement und zu den ITSM-Prozessen Betroffenen sichergestellt werden, dass das für die weiteren Phasen relevante Fachwissen vermittelt wird.
- Im Rahmen der Projektleitung müssen neben der ggf. erforderlichen organisationsübergreifenden Abstimmung auch Steuerungs- und Kontrollmaßnahmen ergriffen werden, um einerseits sicherzustellen, dass die Zeit- und Budgetvorgaben eingehalten werden. Andererseits muss die Dynamik des Szenarios insbesondere bei länger dauernden Implementierungsvorhaben berücksichtigt werden, so dass beispielsweise auf sich verändernde Randbedingungen oder sich erst nachträglich herausstellenden oder zwischenzeitlich verändernden Anforderungen adäquat reagiert werden kann. Der Projektleitung kommt darüber hinaus die Aufgabe zu, über den Projektrahmen hinausgehend am Ergebnis

beteiligte Personengruppen z. B. im Rahmen von Koordinationstreffen zu involvieren. Die entsprechenden Vorgehensweisen unterscheiden sich jedoch nicht von anderen IT-(Sicherheits-)Projekten und werden deshalb an dieser Stelle nicht vertieft.

- Für jede bereitzustellende Komponente müssen die technischen, organisatorischen und prozessrelevanten Schnittstellen implementiert werden.

  Auf technischer Ebene umfasst dies beispielsweise Datenflüsse, über die Nutz- bzw. Metadaten ausgetauscht werden, um z. B. Informationen über erkannte sicherheitsrelevante Ereignisse propagieren zu können. Die Entwicklung der einzelnen Komponenten kann dabei beispielsweise in Anlehnung an den Security Development Lifecycle (SDL, [Mic10]) erfolgen, der in jeder Phase der Entwicklung ergänzende, sicherheitsspezifische Maßnahmen vorsieht und bei Bedarf auch auf agile Entwicklungsmethoden angewandt werden kann. Der SDL stellt einerseits die Einhaltung der in Abschnitt 2.3.2 diskutierten Eigenschaften *secure by design*, *secure by default* und *secure in deployment* sicher und berücksichtigt identifizierte Datenschutzaspekte. Andererseits sieht er vor, dass die Entwickler sicherheitsspezifische Schulungen erhalten und Werkzeuge einsetzen, mit denen die Implementierungsergebnisse nicht nur funktional, sondern auch hinsichtlich ihrer IT-Sicherheitseigenschaften getestet werden können. Auf die enge Verknüpfung zwischen SDL und Risikomanagement, aus der sich wiederum Prioritäten bei der Implementierung einzelner Sicherheitsmechanismen ergeben, setzen auch Softwareentwicklungsmethoden wie das Aspect-Oriented Risk-Driven Development (AORDD, [GAB+10]); AORDD ergänzt die Testphase der Entwicklung zudem durch den gezielten Einsatz formaler Analysemethoden, die auf den als Implementierungsgrundlage erstellten UML-Modellen der jeweiligen Frameworkkomponente aufsetzen.

  Auf organisatorischer Ebene können sich neben Auswirkungen auf bereits vorhandene Vorgaben wie das szenarienspezifische Gesamtsicherheitskonzept auch neue Prozesse und Abläufe ergeben, die mit den dafür zuständigen Stellen abgestimmt und gemeinsam umgesetzt werden müssen; u. U. müssen weitere Interessenvertreter wie beispielsweise der Datenschutzbeauftragte hinzugezogen werden. Aus der Perspektive des IT-Sicherheitsmanagements und der ITSM-Prozesse muss aufbauend auf den entsprechenden Dokumenten aus der Customizingphase pro Komponente spezifiziert werden, welche Abläufe beim Betrieb der Frameworkkomponente beispielsweise im Rahmen von Kapazitätsplanungen und Change Management erforderlich sind. Auf diese einzelnen Aspekte wird in Kapitel 6 im Detail eingegangen.

Die Instanziierungsphase endet, sobald alle Teilprojekte erfolgreich abgeschlossen, ihre Ergebnisse zur Testumgebung für das gesamte Security-Framework zusammengetragen und die unten genannten Abnahmekriterien erfüllt wurden. Die bei allen Aktivitäten gesammelten Erfahren sollten in Anlehnung an etablierte Projektmanagementmethoden und das Change Management nach ITIL beispielsweise in Form eines Post-Implementation-Reviews (PIR) zusammengetragen werden. Sie dienen nicht nur dem unten erläuterten Berichtswesen, sondern liefern potentiell auch Randbedingungen für die Betriebsphase sowie für später geplante weitere Rollout-Phasen des Security-Frameworks, die beim ursprünglichen Design in der Customizingphase noch nicht bekannt waren.

Abnahmekriterien und Kontrollen:
Die implementierten Frameworkkomponenten müssen sowohl einzeln als auch in ihrer Zusammenstellung im Rahmen der Testumgebung überprüft und genehmigt werden. Dies kann

beispielsweise als Audit im Rahmen einer Gegenüberstellung der erreichten mit den ursprünglich geplanten funktionalen und sicherheitstechnischen Eigenschaften erfolgen; darüber hinaus können weitere aus dem Software Engineering bekannte Methoden für System- und Integrationstests angewandt werden. Der Betrachtungsschwerpunkt liegt dabei auf dem frameworkinternen Zusammenspiel aller relevanten Komponenten, wohingegen die Schnittstellen zu und die Kompatibilität mit frameworkexternen Komponenten und Abläufen Gegenstand der nachfolgenden Phase 4 sind.

Bereits in der Customizingphase wurden Dokumentationen zu Administrationskonzepten, zur Managementintegration und über Prozessschnittstellen erstellt, die während dieser Phase spezifisch für die einzelnen Komponenten ergänzt und auf Basis der Implementierung verfeinert werden müssen. Auch die mit dem Abschluss der Implementierungsarbeiten vorzulegenden Dokumentationen der in Eigenentwicklung entstandenen Frameworkkomponenten fungieren als Planungsgrundlage für alle weiteren Phasen und müssen somit beispielsweise mit der Dokumentation von zugekauften Produkten vergleichbar sein.

Berichtswesen:
Um die nachfolgende Phase der Inbetriebnahme vorzubereiten, muss der Personenkreis, der die Auswahl und Instanziierung des Security-Frameworks in Auftrag gegeben hat, über den aktuellen Zwischenstand informiert werden. In Analogie zu Phase 1 betrifft dies insbesondere die Prozesseigner und Administratoren, in deren Bereiche die Komponenten des Security-Frameworks bzw. die von ihm geschützten Assets fallen, sowie den CISO, der über die Fortführung des Einführungsprojekts entscheidet. In organisationsübergreifenden Projekten muss der Abschluss der lokalen Implementierungsarbeiten geeignet szenarienweit kommuniziert werden.

Die bei der Implementierung mit dem Security-Framework gesammelten Erfahrungen sollten zudem an die Frameworkautoren übermittelt werden. Aus ihnen können einerseits Maßnahmen abgeleitet werden, wie beispielsweise durch eine ausführlichere Darstellung von Teilaspekten der vorgefundene Zusatzaufwand künftig besser vermieden werden kann. Andererseits kann auf dieser Basis analysiert werden, ob und welche szenarienspezifisch implementierten Schnittstellenkomponenten potentiell in abstrahierter Form ins Frameworkkonzept mit aufgenommen werden sollten.

5.7. Phase 4: Parametrisierung, Testen und Inbetriebnahme des Security-Frameworks

Ziele:
Die vierte Phase im Lebenszyklus der Frameworkinstanz zielt darauf ab, zunächst die praktische Eignung des szenarienspezifisch angepassten und implementierten Security-Frameworks sicherzustellen. Darauf aufbauend werden die für den Produktivbetrieb relevanten Konfigurationsparameter für die einzelnen Frameworkkomponenten festgelegt und das Security-Framework schließlich in den Produktivbetrieb überführt. Mit dem Abschluss dieser Phase endet auch das Einführungsprojekt für das Security-Framework, so dass dessen Regelbetrieb beginnen kann.

Voraussetzungen:
Der Test des gesamten Security-Frameworks setzt voraus, dass die beschafften bzw. entwickelten Einzelkomponenten wie oben diskutiert bereits in Phase 3 individuell getestet wurden.

Ebenso muss bereits im Rahmen der szenarienspezifischen Anpassung des Frameworkkonzepts als Bestandteil des Administrationskonzepts erarbeitet worden sein, welche szenarienspezifischen Parameter für welche Frameworkkomponenten benötigt werden und wie diese – beispielsweise auf Basis des szenarienspezifischen Gesamtsicherheitskonzepts (vgl. Abschnitt 5.1.2) ermittelt werden können.

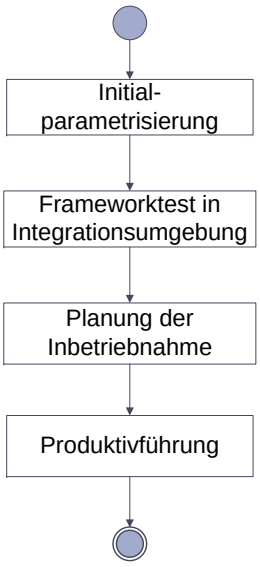
Der eigentliche Zeitpunkt der Inbetriebnahme hängt neben diesen Vorbereitungen einerseits von der internen Freigabe ab, die i. d. R. durch das Change Management und das Release Management erfolgt, und erfordert andererseits die Abstimmung z. B. für die Einkopplung in den Lebenszyklus der vom Security-Framework geschützten Assets und die organisationsübergreifende Koordination in entsprechenden Szenarien.

Schwerpunkte:
Die Tätigkeitsschwerpunkte liegen in dieser Phase auf der praktischen Evaluation des szenarienspezifisch angepassten Security-Frameworks und der Vorbereitung seines nachhaltigen praktischen Einsatzes. Der damit verbundene Rollout aller für die aktuelle Ausbaustufe vorgesehenen Frameworkkomponenten ist insbesondere in organisationsübergreifenden Szenarien potentiell mit einem erheblichen Koordinationsaufwand verbunden, der auch organisationsintern für die Aktivierung aller vorgesehenen Prozessschnittstellen erforderlich ist.

Rollen:
Die in Test- und Inbetriebnahmephase durchgeführten Aktivitäten werden wiederum vom für die Einführung des Security-Frameworks zuständigen *Projektleiter* gesteuert und vom *Systemarchitekt* umgesetzt. Für die Durchführung der Tests werden zusätzlich *Security Engineers* und – in Abhängigkeit von den szenarienspezifischen formalen Kriterien zur Inbetriebnahme neuer Komponenten – *Auditoren* eingesetzt, die im Rahmen der technischen Abnahme gegebenenfalls auch die Rolle von *Angreifern* annehmen, um noch verbleibende Schwachstellen zu identifizieren. In die Vorbereitungen zur Produktivführung sind die *Administratoren* sowohl der vom Security-Framework geschützten Assets als auch der Frameworkkomponenten einzubeziehen. Ausgewählte *Anwender* werden optional in die Tests eingebunden und müssen gesamtheitlich auf Änderungen, die sich durch die Produktivführung des Security-Frameworks ergeben, vorbereitet werden. Die Managementebene, zu der beispielsweise der *CISO* als Schnittstelle fungiert, muss die Inbetriebnahme in Abstimmung mit den betroffenen *Prozesseignern* genehmigen.

Schnittstellen:
In der Test- und Inbetriebnahmephase werden alle Schnittstellen aktiviert, die in den vorangegangenen Phasen konzipiert und implementiert wurden. Die Inbetriebnahme wird von den ITSM-Prozessen Change Management und Release Management gesteuert. Mit ihr werden die Lebenszyklen des Security-Frameworks und der von ihm geschützten Assets für den weiteren Betrieb aneinandergekoppelt. Das Security-Framework wird dabei auch zu einem *managed object* des IT-Sicherheitsmanagements; seine Komponenten werden zu Bestandteilen der bereits vorhandenen IT-Infrastruktur und z. B. bezüglich Monitoring und Reporting in die existierenden operativen Abläufe integriert. Die Inbetriebnahme muss in organisationsübergreifenden Szenarien in gegenseitiger Abstimmung erfolgen; in Abhängigkeit von den Auswirkungen auf den Benutzerbetrieb sind auch die Kunden und Anwender einzubeziehen.

Relevante Anforderungen aus dem Kriterienkatalog:
Die in dieser Lebenszyklusphase auszuführenden frameworkspezifischen Aktivitäten hängen wie bereits die Implementierungstätigkeiten von der im Rahmen der Kategorie *SF-INT* gefor-



Beteiligte Rollen und ihre Zuständigkeiten
(RASCI-Matrix)

	Administrator	Anwender	Auditor (z.T. als Angreifer)	CISO (Leitung)	Projektleiter	Prozesseigner	Security Engineer	Systemarchitekt
Initialparametr.	S			I	A	C	S	R
Test in Int.-Umgebung	S	C	S	I	A	C	S	R
Planung der Inbetriebnahme	C	I		I	A	C	C	R
Produktiv-führung	S	I	I	A	R	S	C	S

Legende:
R – Responsible *(führt aus bzw. stößt an)*
A – Accountable *(ist verantwortlich für)*
S – Support *(unterstützt den Ausführenden bei)*
C – Consulted *(wird befragt zu)*
I – Informed *(wird informiert über Ergebnis von)*

Abbildung 5.8.: Ablauf und Zuständigkeiten in der vierten Lebenszyklusphase (Parametrisierung, Test und Inbetriebnahme)

derten Beschreibung der *Einführung* des Security-Frameworks ab. Bei der Abnahme der Frameworkinstanz stehen ausgewählte Eigenschaften der Kategorie *SF-MGMT* im Vordergrund: Neben der Durchführung der vorgesehenen *Tests* ist auch die *Performanz* zu analysieren. Darüber hinaus muss sichergestellt werden, dass die *Compliance*-spezifischen Anforderungen im Szenario erfüllt werden; aus technischer Perspektive müssen dabei die für das *Auditing* vorgesehenen Mechanismen berücksichtigt werden. Im Idealfall unterstützt auch eine in der Frameworkdokumentation enthaltene *Checkliste* das Abarbeiten der zur Produktivführung erforderlichen Schritte (vgl. Anforderungskategorie *SF-DOKU*).

Ablauf und Methoden:
Nachdem in Phase 3 bereits jede Frameworkkomponente für sich und im frameworkinternen Zusammenhang getestet wurde, steht vor der Inbetriebnahme nun das Security-Framework als Ganzes im Mittelpunkt der Betrachtung. Realistische Tests setzen jedoch eine Konfiguration des Security-Frameworks und seiner Bestandteile voraus, die dem Realbetrieb möglichst nahe kommt. In Anlehnung an die Testphasen im Software Engineering werden die nachfolgend beschriebenen Maßnahmen deshalb wie in Abbildung 5.8 dargestellt in einer Integrationsumgebung durchgeführt, die keine isolierte Testumgebung mehr ist, in der Fehlschläge aber auch keine negativen Auswirkungen auf den Produktionsbetrieb haben.

Die Wahl der initialen Konfigurationsparameter beeinflusst die Wirksamkeit und Effizienz der vom Security-Framework eingebrachten IT-Sicherheitsmechanismen. Zur Parametrisierung gehört beispielsweise die Festlegung kryptographischer Mechanismen wie die Wahl von Verschlüsselungsalgorithmen, die Integration in eine PKI und die einheitliche Gestaltung von Firewallregeln ebenso wie das Einstellen management-, aber nur indirekt IT-sicherheitsrelevanter Parameter wie Zugriffsmöglichkeiten für Monitoringsysteme, zu ver-

wendende Datenbankserver bzw. Repositories, DNS-Server, Logging-Mechanismen und vieles mehr. Die Menge der insgesamt relevanten Parameter ergibt sich aus dem Security-Framework selbst und den szenarienspezifischen Administrations- und Managementkonzepten; ihre Belegung muss sich an folgenden Gesichtspunkten orientieren:

- Im Allgemeinen lässt sich ein Großteil der zu konfigurierenden Parameterwerte aus frameworkübergreifend bzw. szenarienweit gültigen Leitlinien und Administrationskonzepten ableiten.
- Für die Parametrisierung sollten nach Möglichkeit von Anfang an zentrale, integrierte Managementsysteme eingesetzt werden, so dass keine isolierte Konfiguration einzelner Frameworkkomponenten durchgeführt wird, deren Auswirkung auf andere Komponenten somit nicht automatisch erfasst werden würde.
- Die Begründung für die Wahl der Initialparameter muss dokumentiert werden; sie dient als Grundlage für spätere Konsistenzprüfungen und das Change Management.
- Die Testphase bietet die Möglichkeit, mit frameworkspezifischen Parametern, deren Wert nicht durch szenarienweite Vorgaben beeinflusst wird, zu experimentieren. Durch eine bewusst vom Optimum abweichende Wahl der Initialparameter können zum einen Frameworkeigenschaften wie die automatische dynamische Anpassung (vgl. Anforderung *SF-FUNK-Adaptivität*) evaluiert und zum anderen eine schrittweise Einführung vorbereitet werden, bei der das Security-Framework z. B. erst nach mehreren Tagen oder Wochen im Produktivbetrieb sein volles Wirkungsspektrum entfaltet.

Zur Parametrisierung kann auch der Import umfangreicher Datensätze gehören, beispielsweise wenn das Security-Framework die bislang eingesetzten Sicherheitsmechanismen ablösen soll oder z. B. Heuristiken verwendet, die mit realistischen Daten trainiert werden müssen. In organisationsübergreifenden Szenarien sind die Initialparameter geeignet abzustimmen, beispielsweise wenn sie standortübergreifende identisch oder komplementär zueinander gewählt werden müssen.

Nach Abschluss der Initialparametrisierung befindet sich das Security-Framework innerhalb der Integrationsumgebung in einem Zustand, der nach bisherigem Kenntnisstand für den Produktionseinsatz geeignet wäre. Durch die nachfolgende Testphase soll sichergestellt werden, dass das Security-Framework einerseits diesem Anspruch gerecht wird und dass sein Einsatz andererseits keine neuen, noch nicht berücksichtigten IT-Sicherheitsrisiken mit sich bringt. In den Tests werden deshalb insbesondere die folgenden Aspekte analysiert, die auf einen Vergleich zwischen der ursprünglich im Rahmen der Frameworkauswahl bzw. dem Customizing vorgegebenen Zielsetzung und der mit der Implementierung abgedeckten Anforderungen abzielt:

- *Sicherheitsfunktionalität:* Schützt das Security-Framework vor den berücksichtigten Angriffen? Hierzu können beispielsweise Penetrationstests oder die unten beschriebenen Evaluationsmethoden auf die zu schützenden Assets angewandt werden.
- *Sichere Implementierung:* Weist die Implementierung des Security-Frameworks eigene Schwachstellen auf? Zur Klärung können wiederum Methoden wie Penetrationstests eingesetzt werden, die jedoch auf das Security-Framework und seine Komponenten, also nicht die eigentlich zu schützenden Assets, abzielen.

- *Integration:* Wie verhält sich das Security-Framework im Realbetrieb u. a. im Hinblick auf Performance und Skalierbarkeit? Die Integrationsumgebung sollte, auch wenn sie die Produktionsumgebung nicht exakt nachstellen kann, auf den praktischen Einsatz übertragbare Aussagen zulassen.
- *Management:* Sind die definierten Managementkonzepte, u. a. bezüglich administrativer Abläufe und Prozessschnittstellen, praktikabel? Zu Testzwecken sollten beispielsweise Änderungen an den gewählten Initialparametern durchgeführt werden, die Prozesse wie das Change Management ähnlich zum späteren Produktionsbetrieb durchlaufen.
- *Dokumentation:* Sind die mit dem Security-Framework im Szenario verfolgten Ziele, alle durchgeführten Entwicklungs- und Implementierungstätigkeiten und deren Ergebnisse sowie die für den Betrieb relevanten Abläufe und Schnittstellen ausreichend dokumentiert?

Im Frameworkkonzept können weitere ergänzende Tests, die vor der Produktivführung durchgeführt werden sollen, vorgegeben sein. Im Allgemeinen dienen die Tests in dieser Phase zur Qualitätssicherung vor der Inbetriebnahme des Security-Frameworks in der Produktivumgebung. Sie dürfen jedoch nicht als einmalige Kontrolle missverstanden werden, sondern dienen auch im laufenden Betrieb zur Identifikation von Abweichungen vom Soll-Zustand. Um die Tests zielführend zu gestalten und ihre einfache Wiederholbarkeit sicherzustellen, kann beispielsweise auf folgende Methoden zurückgegriffen werden:

- Mit der *modellbasierten Sicherheitstestautomatisierung* [BBNC01] können Tests automatisch generiert werden, wenn die zu überprüfende Komponente und ihre sicherheitsfunktionalen Eigenschaften in Anlehnung an die Common Criteria modelliert worden sind (vgl. Abschnitt 2.2.3.2). Dieses Verfahren bietet sich deshalb insbesondere für Szenarien an, für die eine formale Zertifizierung angestrebt wird (vgl. Anforderung *SF-DOKU-Zertifizierung*). Für beispielsweise nicht selbst entwickelte Komponenten, von denen lediglich die Schnittstellen, aber nicht die internen Abläufe bekannt sind, kann ergänzend auf *Attack-Injection*-Konzepte wie AJECT zurückgegriffen werden [ANC+10].
- Das im Rahmen des IT-Sicherheitsmanagements anzuwendende risikoorientierte Vorgehen wird durch Ansätze wie das *bedrohungsmodellgetriebene Sicherheitstesten* [WWX07] unterstützt. Die in einem Szenario bekannten Bedrohungen (vgl. Anforderungen *SF-DOKU-Angreifermodelle* und *SF-FUNK-Angriffe*) werden dabei z. B. in UML als Aktivitätsdiagramme modelliert und den internen Abläufen im Security-Framework algorithmisch gegenübergestellt. Aufgrund des notwendigen Detailgrads der Modellierung bietet sich das Verfahren primär für die im Rahmen der Frameworkinstanziierung in Eigenentwicklung implementierten Komponenten an, wobei die modellierten Bedrohungen komponentenübergreifend wiederverwendet werden können.
- Aus den mit dem Security-Framework verfolgten Zielen und den im Frameworkkonzept oder im Rahmen der Customizingphase definierten Key Performance Indicators (KPIs) können nach [SAM08] Metriken für die Beurteilung der Sicherheitsmechanismen abgeleitet werden. Die dazu erforderliche Dokumentation der im Szenario verfolgten IT-Sicherheitsziele, der architekturspezifischen Abhängigkeiten und der Auswirkungen erfolgreicher Angriffe liegt mit dem Gesamtsicherheitskonzept und dem szenarienspezifisch angepassten Security-Framework bereits vor.

Durch die Tests werden potentielle Defizite im Security-Framework oder den gewählten Initialparametern ermittelt, die in Abhängigkeit ihrer Kritikalität entweder noch vor Inbetriebnahme behoben oder für die Bearbeitung im Rahmen der kontinuierlichen Verbesserung vorgemerkt werden müssen.

Nach dem Abschluss der Tests kann mit der Planung, Abstimmung und Durchführung der Inbetriebnahme des Security-Frameworks begonnen werden. Diese ist vergleichbar mit der Produktivführung anderer Assets und wird durch die ITSM-Prozesse gesteuert. Dadurch wird sichergestellt, dass z. B. andere in der Produktivumgebung erforderliche Anpassungen wie die Umstellung der vom Security-Framework geschützten Assets oder die Außerbetriebnahme bisher eingesetzter Sicherheitsmechanismen in der richtigen Reihenfolge und zum passenden Zeitpunkt erfolgen und alle betroffenen Personengruppen rechtzeitig informiert werden. Durch den formalen Rahmen wird insbesondere gewährleistet, dass potentiell nach der Inbetriebnahme des Security-Frameworks im Betrieb der anderen Dienste auftretende Störungen richtig zugeordnet werden können.

Die Inbetriebnahme kann bei Bedarf wiederum in mehreren Stufen erfolgen, z. B. in Form eines Pilotbetriebs für ausgewählte Teilbereiche. Nach jedem Schritt ist – beispielsweise durch die Wiederholung ausgewählter Tests – zu kontrollieren, ob die jeweils gesetzten Ziele im Betrieb erreicht werden.

Mit der erfolgreichen Inbetriebnahme des Security-Frameworks endet sein Einführungsprojekt und der Regelbetrieb (Phase 5) beginnt. Das Einführungsprojekt sollte einem Review unterzogen werden, um die gewonnenen Erfahrungen sowohl bei der späteren Verbesserung des vorliegenden Security-Frameworks als auch bei der Instanziierung weiterer Security-Frameworks nutzen zu können.

Abnahmekriterien und Kontrollen:
Als Ergebnis dieser Lebenszyklusphase ist das in den Produktionsbetrieb überführte Security-Framework vorzulegen. Zu diesem Zweck sind eine begründete Dokumentation der gewählten Initialparameter und ein Abnahmeprotokoll für die Frameworkkomponenten und das gesamte Security-Framework anzufertigen; darin müssen auch die durchgeführten Tests mit den jeweils erfüllten Kriterien, erkannten Abweichungen und daraus gezogenen Konsequenzen festgehalten werden. Die mit dem Security-Framework eingeführten neuen Komponenten müssen in die Betriebsumgebung aufgenommen worden sind; dies kann beispielsweise anhand der entsprechenden Einträge in der Configuration Management Database (CMDB) überprüft werden.

Berichtswesen:
Über den Abschluss der Vorbereitungen zur Inbetriebnahme muss die Managementebene informiert werden, um die Genehmigung für die Produktivführung einzuholen. Zur Vorbereitung dieser Produktivführung sind neben dem Durchlaufen der formalen Prozesse, z. B. durch die Erstellen entsprechender *Change Requests*, auch die betroffenen Prozesseigner und Administratoren über die gewählten Initialparameter, die Ergebnisse der Tests und die bevorstehende Inbetriebnahme zu informieren. Analog dazu ist über den Abschluss des Einführungsprojekts und eventuell noch verbliebene offene Punkte zu berichten. Auch die Frameworkautoren sollten über die Inbetriebnahme und möglicherweise bei den vorangegangenen Tests identifizierte Problembereiche informiert werden.

5.8. Phase 5: Betrieb und Wartung des Security-Frameworks

Ziele:
Das Ziel der Betriebs- und Wartungsphase ist es, den effizienten und effektiven Betrieb des Security-Frameworks durch die adäquate Anwendung von Managementmethoden sicherzustellen, bis Ereignisse eintreten, die eine umfassendere Überarbeitung oder die Außerbetriebnahme erforderlich machen.

Voraussetzungen:
Eine offensichtliche Voraussetzung für den operativen Betrieb des Security-Frameworks ist dessen Bereitstellung und Inbetriebnahme in den vorhergehenden Phasen, durch die sichergestellt wird, dass auch entsprechende Administrations- und Betriebskonzepte vorliegen. Darüber hinaus müssen die in Abschnitt 5.1 diskutierten Dokumente – beispielsweise das Gesamtsicherheitskonzept – und Verfahren, z. B. das Risikomanagement, fortgeführt und inhaltlich jeweils auf dem aktuellen Stand gehalten werden. Dies betrifft sowohl Änderungen, die sich aus dem Streben nach kontinuierlicher Verbesserung ergeben, als auch die Berücksichtigung sich verändernder Anforderungen, z. B. durch das Bekanntwerden neuer Verwundbarkeiten oder Angriffsvarianten.

Schwerpunkte:
Die Schwerpunkte beim Betrieb des Security-Frameworks liegen auf der Bearbeitung der mit seiner Hilfe erkannten Sicherheitsereignisse, dem Beitragen zur Überwachung des Gesamtsicherheitsniveaus u. a. durch Messungen und Berichte, der Identifikation zur kontinuierlichen Verbesserung erforderlicher Maßnahmen und der Durchführung von kleineren Anpassungs- und Wartungsarbeiten.

Rollen:
Die Betriebs- und Wartungsaufgaben werden von den *Administratoren* des Security-Frameworks in enger Abstimmung mit den Administratoren der von ihm geschützten Assets wahrgenommen. Die *Prozesseigner* für das IT-Sicherheitsmanagement und für die mit den geschützten Assets verknüpften Geschäftsprozessen entscheiden über die weiteren Arbeiten am Security-Framework und stellen zusammen mit dem Management, das beispielsweise durch den *CISO* repräsentiert wird, Zielgruppen für Berichte bzw. Eskalationsinstanzen bei der Bearbeitung von Sicherheitsvorfällen dar.

Durch *Security Engineers* wird die sicherheitstechnische Funktionalität des Security-Frameworks regelmäßig überprüft, wohingegen für *Auditoren* bei den regelmäßigen Kontrollen die organisatorische Einbettung im Vordergrund steht. *Technologieexperten* können diese Analysen z. B. mit Hinweisen auf neue oder veränderte Bedrohungen und Sicherheitsmechanismen ergänzen.

In den Betrieb sind auch die *Anwender* involviert, sofern die vom Security-Framework umgesetzten Sicherheitsmechanismen aus Nutzersicht nicht vollständig transparent sind. Die *Angreifer* sind die potentiellen Auslöser von Sicherheitsvorfällen, wobei in den szenarienspezifischen Angreifermodellen berücksichtigt werden muss, ob z. B. auch Mitarbeiter des Unternehmens oder reguläre Anwender als mögliche Angreifer zu berücksichtigen sind.

Schnittstellen:
Das Security-Framework ist als IT-Sicherheitsmaßnahme während seiner gesamten Betriebsdauer eng mit dem Prozess IT-Sicherheitsmanagement verknüpft. Durch seinen inhaltlichen

Bezug auf zu schützende Assets und da es selbst wiederum aus Einzelkomponenten besteht, die zu den im Einsatzgebiet verwalteten *Configuration Items* gehören, ergeben sich gegenseitige Abhängigkeiten zwischen dem Security-Framework und den ITSM-Prozessen. Dieser Schnittstelle sind u. a. auch die an Monitoringsysteme übermittelten und ins Berichtswesen einfließenden Messwerte und Sicherheitsmetriken zuzuordnen. Beim organisationsübergreifenden Einsatz erfordert auch der laufende Betrieb regelmäßige Abstimmungen, beispielsweise bei der anstehenden Änderung von Konfigurationsparametern.

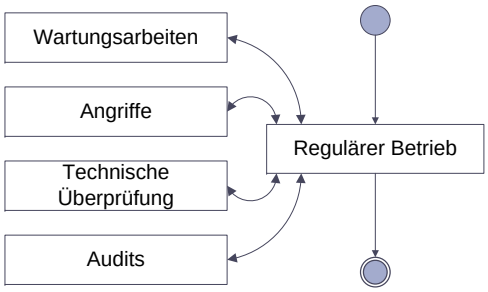
Relevante Anforderungen aus dem Kriterienkatalog:
Für den Betrieb sind aus offensichtlichen Gründen alle sicherheitsfunktionalen Eigenschaften (siehe Anforderungskategorie *SF-FUNK*) relevant. In dieser Phase wird beispielsweise auch die Forderung nach *Adaptivität* zur Laufzeit relevant, die zur Vermeidung längerer Wartungsintervalle beiträgt.

Aus dem Bereich der Integrations- und Betriebsanforderungen (Kategorie *SF-INT*) sind die *Skalierbarkeit* und die Möglichkeit zum *Parallelbetrieb* mit anderen Sicherheitsmechanismen ausschlaggebend. Darüber hinaus sind die *Hochverfügbarkeit* sowie die *Usability* zu berücksichtigen.

Schließlich sind fast alle Anforderungen der Kategorie *SF-MGMT* für den laufenden Betrieb relevant. Maßgeblichen Einfluss haben dabei die definierten *Managementprozesse* und *Managementoperationen* sowie die Schnittstellen zu den *ITSM-Prozessen*; die entsprechenden Vorgänge werden von den definierten *Security-Events* und den aus den Kennzahlen abgeleiteten *KPIs* unterstützt. Darüber hinaus zeigen sich die *Praxiserprobung* und die ins Security-Framework einfließenden *Verbesserungen* ebenso wie die Auswirkungen auf die *Compliance* deutlich. In den Wartungsintervallen ergibt sich potentiell der Bedarf an externem *Support* für das Security-Framework.

Ablauf und Methoden:
Auf die einzelnen Abläufe im operativen Management von Security-Frameworks und die zu ihrer Unterstützung geeigneten Methoden wird unter Berücksichtigung der jeweils relevanten Schnittstellen in Kapitel 6 detailliert eingegangen. Um eine durchgängige Darstellung des Instanzlebenszyklus zu erreichen, werden im Folgenden lediglich ausgewählte und in Abbildung 5.9 dargestellte Kernaspekte stichpunktartig vorgestellt:

- Das Security-Framework wird immer zusammen mit den Diensten bzw. Architekturen betrachtet, die von ihm geschützt werden. Der Bedarf an Änderungen und Anpassungen ergibt sich überwiegend aus extern ausgelösten Ereignissen wie neuen Angriffsvarianten oder aus an den geschützten Assets geplanten Änderungen, und ist aufgrund der Zweckbindung des Security-Frameworks nur in seltenen Fällen intrinsisch motiviert (z. B. vorab geplante Rolloutphasen).
- Analog zum Management der geschützten Assets deckt auch das Management des Security-Frameworks die Teilbereiche Fehlermanagement, Konfigurationsmanagement, Accounting, Performancemanagement und Sicherheitsmanagement (FCAPS, vgl. [HAN99, S. 75]) ab. Der Bereich Accounting ist insbesondere dann relevant, wenn sicherheitsspezifische Dienstgüteparameter in Service Level Agreements mit Kunden einfließen; im Rahmen des Sicherheitsmanagements muss damit umgegangen werden, dass das Security-Framework nicht nur Schutzmaßnahmen bereitstellt, sondern auch selbst zum Ziel von Angriffen werden kann.



Beteiligte Rollen und ihre Zuständigkeiten (RASCI-Matrix)

	Administrator	Angreifer	Anwender	Auditor	CISO (Leitung)	Prozesseigner	Security Engineer	Technologie-experte
Regulärer Betrieb	R		I		I	A		
Wartungs-arbeiten	R		I		I	A	S	C
Angriffe	I	R			I	A	I	I
Technische Überprüfung	S			I	I	A	R	C
Audits	I			R	A	C	I	

Legende:
R – Responsible *(führt aus bzw. stößt an)*
A – Accountable *(ist verantwortlich für)*
S – Support *(unterstützt den Ausführenden bei)*
C – Consulted *(wird befragt zu)*
I – Informed *(wird informiert über Ergebnis von)*

Abbildung 5.9.: Ablauf und Zuständigkeiten in der fünften Lebenszyklusphase (Betrieb und Wartung)

- Das Security-Framework liefert regelmäßig Messwerte, die in Kennzahlen zur Beurteilung des aktuell erreichten Sicherheitsniveaus einfließen; die Komponenten des Security-Frameworks sind zu diesem Zweck u. a. in Monitoring- und Reportingsystem eingebunden. Neben zielgruppenorientierten Berichten, die auf unerwartete Abweichungen zu untersuchen sind, werden Trendanalysen durchgeführt, aus denen Maßnahmen für die Verbesserung abgeleitet werden.
- Neben der passiven Überwachung finden auch aktive Tests statt, für die Methoden analog zu den in Phase 4 diskutierten eingesetzt werden; diese werden von regelmäßigen Reviews und Audits des gesamten Security-Frameworks und seines Umfelds ergänzt, wobei das ISMS den Gesamtrahmen bildet.
- Zusätzlich zu den genannten passiven und aktiven Überwachungsmethoden liefern eintretende Sicherheitsereignisse und -vorfälle Anregungen für die weitere Verbesserung des Security-Frameworks. Diese hängen u. a. davon ab, ob es präventiv, detektierend bzw. zur Unterstützung der Reaktion auf IT-sicherheitsspezifische Störungen ausgerichtet ist, so dass Verbesserungen ggf. über den Rahmen des Security-Frameworks hinaus umgesetzt werden müssen.
- In den Wartungszyklen werden kleinere Anpassungen des Security-Frameworks vorgenommen, die primär den folgenden Kategorien zugeordnet werden können:
  - Die *Parametrisierung* des Security-Frameworks muss angepasst werden, sofern dafür keine Automatismen vorgesehen sind.
  - *Routineaufgaben* wie die Erneuerung von Serverzertifikaten im Rahmen einer PKI fallen regelmäßig an.

  - *Dienstabhängige* Änderungen wie beispielsweise die Berücksichtigung neuer Kunden müssen im Zusammenspiel mit dem szenarienspezifischen Mandanten- und Delegationskonzept vorgenommen werden.

- Die Wartungsoperationen werden in enger Abstimmung mit dem IT-Sicherheitsmanagement und den ITSM-Prozessen durchgeführt, aus denen sich regelmäßig und bedarfsorientiert auch weitere Aufgaben ergeben, z. B. im Hinblick auf die Kapazitätsplanung.

Die Betriebsphase wird prinzipiell nur verlassen, wenn das Security-Framework umfassender überarbeitet oder außer Betrieb genommen werden soll; mögliche Gründe hierfür werden in den Abschnitten 5.9 und 5.10 diskutiert.

Abnahmekriterien und Kontrollen:
Da es sich beim Betrieb des Security-Frameworks um eine Daueraufgabe handelt, existieren keine Kriterien, die zum „erfolgreichen“ Verlassen dieser Phase führen. Das Security-Framework wird wie oben skizziert kontinuierlich überprüft; mit dem Eintreten von Ereignissen, auf die durch die genannten Wartungsarbeiten nicht ausreichend reagiert werden kann, erfolgt der Übergang zu einer der beiden nachfolgenden Lebenszyklusphasen. Der Betrieb wird dabei noch so lange im bisherigen Umfang aufrechterhalten, bis das Security-Framework abgeschaltet bzw. eine überarbeitete Version in Betrieb genommen wird.

Berichtswesen:
Das Security-Framework ist wie die anderen im Szenario eingesetzten Sicherheitsmechanismen in die Überwachungs- und Reportingabläufe mit den oben genannten Zielgruppen eingebunden. Auf die diesbezüglich für Security-Frameworks spezifischen Aspekte wird in Kapitel 6 eingegangen. Die im laufenden Betrieb gewonnenen Erfahrungen und die sich abzeichnenden Stärken und Schwächen des Security-Frameworks sowohl aus sicherheitsfunktionaler Sicht als auch bezüglich seines Managements sind auch für die Frameworkautoren von großem Interesse und sollten geeignet kommuniziert werden.

5.9. Phase 6: Überarbeitung des Security-Frameworks

Ziele:
In der Überarbeitungsphase werden größere Veränderungen an der Architektur bzw. der Konfiguration der Frameworkinstanz vorbereitet, ohne den laufenden Betrieb des Security-Frameworks zu beeinträchtigen.

Voraussetzungen:
Diese Lebenszyklusphase beginnt, wenn sich die Notwendigkeit eines Eingriffs in die Frameworkinstanz abzeichnet, der über die im Rahmen regulärer Wartungstätigkeiten durchführbaren Parameteranpassungen hinausgeht, zusätzliche Frameworkkomponenten erfordert oder in der Customizingphase nicht im benötigten Umfang vorgesehen wurde. Zu den typischen Auslösern gehören folgende Ereignisse:

- *Qualitative Einschränkungen:* Im laufenden Betrieb zeichnet sich ab, dass z. B. die Sicherheitsfunktionalität des Security-Frameworks, seine Managementeigenschaften oder die mit ihm verbundenen Betriebskosten nicht den ursprünglichen Erwartungen entsprechen, so dass größere Nachbesserungen erforderlich werden.

- *Zeitgesteuerte Ereignisse:* Die für das Security-Framework vereinbarte Betriebszeit läuft ab, beispielsweise weil seine nächste Ausbaustufe bzw. Rolloutphase bevorsteht.
- *Neues Frameworkkonzept:* Die Frameworkautoren geben eine neue Version des Frameworkkonzepts frei, die für das Szenario benötigte Neuerungen mit sich bringt.
- *Weitere Security-Frameworks:* Durch die geplante Inbetriebnahme weiterer Security-Frameworks im Szenario ergeben sich z. B. sicherheitsfunktionale Überlappungen, die eine Anpassung des bereits vorhandenen Security-Frameworks erforderlich machen.
- *Identifizierte Verbesserungsmöglichkeiten:* Beispielsweise im Rahmen der kontinuierlichen technischen Überprüfungen, der regelmäßigen Audits oder aus dem ITSM-Prozess Problem Management heraus wurde eine signifikante Menge an Change Requests für das Security-Framework gestellt, die nicht im Rahmen der Routinewartungsarbeiten umgesetzt werden können.
- *Veränderte Randbedingungen:* Durch die Weiterentwicklung des Szenarios und der technischen Möglichkeiten ändern sich Teile der mit dem Security-Framework verbundenen Zielsetzung, z. B. falls
  - weitere bzw. andere Assets vom Security-Framework geschützt werden sollen,
  - neue Kunden mit erhöhten IT-Sicherheitsanforderungen hinzukommen oder Kunden wegfallen,
  - Teile der Diensterbringung im Rahmen einer organisationsübergreifenden Kooperation neu geregelt werden und zu einer Umverteilung führen,
  - sich an den vom Security-Framework geschützten Assets, z. B. einem IT-Dienst, größere Änderungen ergeben, die eine Anpassung der Sicherheitsmaßnahmen erfordern,
  - im Szenario andere Angreifermodelle relevant werden bzw. neue Arten von Angriffen berücksichtigt werden müssen,
  - neue, bislang nicht berücksichtigte Verwundbarkeiten in den Assets bekannt werden,
  - sich die organisatorischen und rechtlichen Randbedingungen ändern, so dass beispielsweise neue Gesetze in Kraft treten, die sich auf die IT-Sicherheitslösungen auswirken,
  - im Szenario neue Technologien eingeführt werden, aus denen sich neue Risiken ergeben, beispielsweise im Rahmen der Virtualisierung bislang eigenständig physischer Komponenten.

Mit dem Eintritt in diese Lebenszyklusphase ist das Streben danach verbunden, die durch die o. g. Auslöser veränderte Zielsetzung durch eine Modifikation der Frameworkinstanz wieder zu erreichen. Alternativ kann auch eine Ablösung des Security-Frameworks in Betracht gezogen werden (siehe Abschnitt 5.10).

Schwerpunkte:
Die Hauptaufgaben in der Überarbeitungsphase bestehen in der Identifikation und Dokumentation der Auslöser für die geplante Überarbeitung, der szenarienweiten Auswirkungen und möglicher Maßnahmen, um die veränderte Zielsetzung zu erreichen.

Rollen:
Die Notwendigkeit einer Überarbeitung wird auf fachlicher Ebene von den *Administratoren* im Zusammenspiel mit den *Prozesseignern*, beispielsweise des IT-Sicherheitsmanagements oder der mit den geschützten Assets verbundenen Geschäftsprozesse, erkannt. Die Konzeption der Veränderungen am Security-Framework wird analog zu den früheren Lebenszyklusphasen von einem *Systemarchitekten* übernommen, der optional von *Security Engineers* und *Technologieexperten* unterstützt wird. Für die Realisierung der Überarbeitung wird ein Verantwortlicher ernannt, der die aus den Phasen 1–4 bekannte Rolle des *Projektleiters* übernimmt; der Grad der Verteilung dieser Rollen auf unterschiedliche Personen hängt vom geschätzten Umfang der erforderlichen Änderungen ab. Das Vorhaben muss auf Basis einer Schätzung des Aufwands und der anfallenden Kosten von der Managementebene genehmigt werden; die Koordination erfolgt beispielsweise über den *CISO*.

Schnittstellen:
Die in dieser Lebenszyklusphase zu berücksichtigenden Schnittstellen entsprechen im Wesentlichen denen der Auswahlphase, unterscheiden sich durch das bereits operativ betriebene Security-Framework inhaltlich jedoch in Bezug auf ihre Ausgangsbasis:

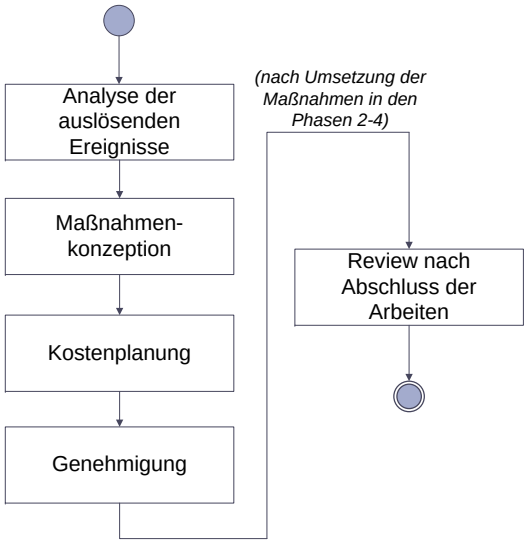
- Die Auswahl und Priorisierung der angestrebten Veränderungen erfolgt in Abstimmung mit dem szenarienweiten Risikomanagement.
- Gegebenenfalls sind organisationsübergreifende Abstimmungen erforderlich.
- Alle Änderungen müssen über den ITSM-Prozess Change Management abgewickelt werden.

Weitere Einflüsse ergeben sich aus der Art des Auslösers für den Eintritt in diese Phase, so dass sich beispielsweise auch Schnittstellen zu Einführungsprojekten für andere Security-Frameworks ergeben können oder eine enge Zusammenarbeit mit Projektgruppen erforderlich wird, die z. B. größere Änderungen an den geschützten Assets vornehmen.

Relevante Anforderungen aus dem Kriterienkatalog:
Die Frameworkkonzepte können die erforderlich werdenden Überarbeitungsphasen in verschiedenen Bereichen gezielt unterstützen. Aus der Perspektive der Managementanforderungen (Kategorie *SF-MGMT*) ist maßgeblich, dass *Verbesserungen* kontinuierlich identifiziert und über das Frameworkkonzept zur Umsetzung gelangen. Dabei wirken sich sowohl *Metriken*, die den konkreten Bedarf erkennbar machen, als auch ein definierter *Releasezyklus* für das Security-Framework positiv aus; in diesem Kontext ist ferner vorteilhaft, wenn das Ziel der kontinuierlichen Verbesserung bereits in der Frameworkdokumentation verankert ist und von Anfang an in die Planungen einbezogen werden kann (vgl. Anforderung *SF-DOKU-Kontinuum*).

Bei der Planung der Veränderungen sind wiederum die Integrationseigenschaften (Anforderungskategorie *SF-INT*) zu berücksichtigen. Neben bereits vorgesehenen *Ausbauphasen* sind die Schnittstellen für *Erweiterungen* relevant; bei jeder Überarbeitung muss jedoch auch der Aspekt der *Skalierbarkeit* beachtet werden.

Ablauf und Methoden:
Die in dieser Phase durchzuführenden und in Abbildung 5.10 dargestellten Tätigkeiten hängen maßgeblich davon ab, ob die durchzuführenden Änderungen bereits konkret bekannt sind und welchen Umfang sie haben. Im Allgemeinen muss davon ausgegangen werden, dass in



Beteiligte Rollen und ihre Zuständigkeiten (RASCI-Matrix)

	Administrator	CISO (Leitung)	Projektleiter	Prozesseigner	Security Engineer	System-architekt	Technologie-experte
Ereignis-analyse	S	I	A	C	S	R	C
Maßnahmen-konzeption	C	I	A	C	S	R	C
Kostenplanung		I	A	C		R	
Genehmigung	I	A	R	C	C	C	C
Review	I	A	R	C	C	C	C

Legende:
R – Responsible *(führt aus bzw. stößt an)*
A – Accountable *(ist verantwortlich für)*
S – Support *(unterstützt den Ausführenden bei)*
C – Consulted *(wird befragt zu)*
I – Informed *(wird informiert über Ergebnis von)*

Abbildung 5.10.: Ablauf und Zuständigkeiten in der sechsten Lebenszyklusphase (Überarbeitung)

der vorangegangenen Betriebsphase lediglich Symptome von Defiziten oder geschäftsprozessorientierter Änderungsbedarf erkannt wurden, die sich beispielsweise durch die Abweichung von Messwerten von ihren Sollwerten äußern, ohne dass die exakten Ursachen und mögliche Lösungswege bereits bekannt sind. In diesem Fall müssen beispielsweise durch die Analyse bereits praktizierter Workarounds, die nach Sicherheitsvorfällen oder als Reaktion auf Störungsmeldungen eingeführt wurden, und den Einbezug weiterer Experten, die z. B. bereits die Phasen 2–4 begleitet haben, die Fehler im szenarienspezifisch angepassten Frameworkkonzept bzw. in seiner Instanziierung sowie die ggf. veränderten Anforderungen und Zielsetzungen identifiziert werden.

Für die weitere Planung müssen die technischen und organisatorischen Maßnahmen bzw. Veränderungen am Security-Framework benannt werden. Die dazu erforderlichen Abläufe sind mit den in Abschnitt 5.1.2 genannten vergleichbar, haben jedoch den Unterschied, dass sich das Security-Framework bereits im Einsatz befindet und im Sinne des ITSM-Prozesses Configuration Management als *Baseline* für die Ist-Analyse herangezogen werden kann. Auf dieser Grundlage muss zunächst fachlich und wiederum unter Berücksichtigung der den Phaseneintritt auslösenden Ereignisse beurteilt werden, ob eine Überarbeitung des Security-Frameworks die beste Lösung darstellt oder z. B. außerhalb der Frameworkinstanz neue bzw. veränderte Maßnahmen umgesetzt werden sollten.

Nach der Neudefinition des Soll-Zustands für das Security-Framework und der Genehmigung des Vorhabens auf Basis einer Aufwands- und Kostenabschätzung, die sich aus der Gegenüberstellung mit der definierten Baseline ergibt, erfolgt im Allgemeinen ein Sprung in die Customizingphase (siehe Abschnitt 5.5) mit dem Ziel, die Änderungen im Detail zu planen und ihre Implementierung und Inbetriebnahme anzustoßen. In Abhängigkeit vom Umfang

der Änderungen und insbesondere, wenn sich an den bereits etablierten Betrieb- und Managementkonzepten sowie den Schnittstellen nur geringfügige Änderungen ergeben, kann die Customizingphase jedoch erheblich schneller durchlaufen werden als bei der initialen Anpassung des Security-Frameworks, so dass zügig zur Instanziierungsphase übergegangen werden kann. Nach Inbetriebnahme des modifizierten Security-Frameworks muss – beispielsweise in Form eines *Post Implementation Reviews* – überprüft werden, ob die mit der Überarbeitung angestrebten Ziele erreicht wurden; das Security-Framework befindet sich damit wieder in der Betriebs- und Wartungsphase.

Abnahmekriterien und Kontrollen:
Der Übergang von der Überarbeitungs- in die Customizingphase erfordert die Genehmigung des Änderungsvorhabens durch die Managementebene und setzt somit eine Dokumentation der zusätzlich benötigten bzw. zu modifizierenden Frameworkkomponenten und des damit voraussichtlich verbundenen Aufwands voraus. Analog zur Frameworkauswahlphase können Dritte zur fachlichen Beurteilung des entsprechenden Grobkonzepts hinzugezogen werden.

Die Genehmigung zum Übergang in die Customizingphase wird unter der Auflage erteilt, dass das schließlich zu liefernde Ergebnis in Form eines in den Produktivbetrieb überführten, überarbeiteten Security-Frameworks daraufhin untersucht wird, ob die gesteckten Ziele durch die Änderungen erreicht wurden. Gegebenenfalls müssen weitere Überarbeitungen geplant oder komplementäre Lösungsansätze außerhalb der Frameworkinstanz verfolgt werden.

Berichtswesen:
Die von den geplanten Änderungen betroffenen Personenkreise müssen geeignet informiert werden; neben den Administratoren und Prozesseignern gehören dazu auch diejenigen Stellen, die Änderungsanträge eingebracht haben bzw. hinter den die Änderungen auslösenden Ereignissen stehen. Darüber hinaus spielt die Dokumentation der Änderungen im Rahmen des Change Managements eine zentrale Rolle, da durch Trendanalysen und Reviews, die im Rahmen der ITSM-Prozesse regelmäßig durchgeführt werden, mittel- bis langfristige Konsequenzen gezogen werden – beispielsweise, falls ein Security-Framework durch einen überdurchschnittlich häufigen oder umfangreichen Änderungsbedarf auffällig wird. Informationen über die Hintergründe und den Umfang der geplanten Änderungen sollten wiederum an die Frameworkautoren kommuniziert werden.

5.10. Phase 7: Außerbetriebnahme des Security-Frameworks

Ziele:
Alle nicht mehr benötigten Komponenten und Schnittstellen des Security-Frameworks werden unter Berücksichtigung der gegenseitigen Abhängigkeiten strukturiert außer Betrieb genommen.

Voraussetzungen:
Analog zur Überarbeitungsphase wird auch die Außerbetriebnahmephase durch einzelne oder in Summe signifikante Ereignisse ausgelöst, die mit Zielen verknüpft sind, für die eine Überarbeitung des Security-Frameworks keine ausreichende Lösung darstellt. Hierzu gehören beispielsweise:

- *Qualitative Mängel:* Falls sich z. B. trotz wiederholter Überarbeitungsvorgänge herausstellt, dass das Security-Framework die an seine Sicherheitsfunktionalität oder Mana-

gementeigenschaften gestellten Anforderungen in der Praxis nicht erfüllt, muss seine Ablösung durch alternative Maßnahmen geplant werden. Hierzu kann auch gehören, dass das Frameworkkonzept von den Frameworkautoren zu lange nicht mehr weiterentwickelt wurde und der Aufwand für die in szenarienspezifischer Eigenleistung erbrachte Weiterentwicklung zu hoch ist.

- *Assetgesteuerte Ereignisse:* Das Security-Framework wird nicht mehr benötigt, da z. B. der von ihm geschützte IT-Dienst außer Betrieb genommen wird oder ein Kunde mit sicherheitsspezifischen Anforderungen wegfällt. Analog dazu ist der Fall zu betrachten, dass sich die geschützten Assets z. B. durch Umstieg auf eine andere Softwarebasis so stark verändern, dass das Security-Framework dazu generell nicht mehr kompatibel ist.
- *Veränderte Randbedingungen:* Der Bedarf für das Security-Framework oder die Voraussetzungen für seinen Betrieb sind nicht mehr gegeben. Dieser Fall tritt z. B. ein, wenn ein anderes Security-Framework eingeführt wird, das die Aufgaben des außer Betrieb zu nehmenden Security-Frameworks mit übernehmen kann, oder wenn vom Security-Framework benötigte Komponenten außer Betrieb und diese Abhängigkeiten und Konsequenzen in Kauf genommen werden.

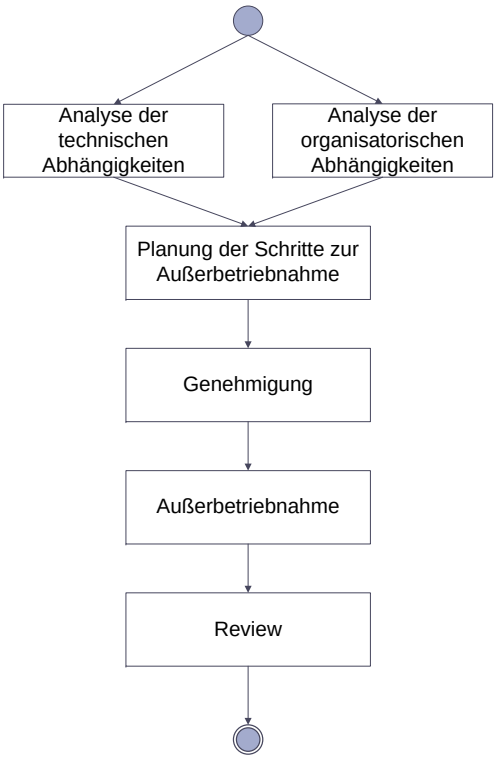
Analog zu anderen IT-Diensten und Assets kommen auch weitere Gründe wie der Ablauf der vereinbarten Betriebszeit oder unwirtschaftlich hohe Betriebskosten für die Außerbetriebnahme in Frage.

Schwerpunkte:
Die Tätigkeitsschwerpunkte liegen in dieser Lebenszyklusphase auf der Planung und der schrittweisen Durchführung der strukturierten Außerbetriebnahme der einzelnen Frameworkkomponenten.

Rollen:
Die Außerbetriebnahme der Frameworkkomponenten erfolgt durch deren *Administratoren* im Zusammenspiel mit den *Prozesseignern* und Administratoren der betroffenen Assets. Die Genehmigung der Außerbetriebnahme obliegt der Managementebene, beispielsweise dem *CISO*, in enger Abstimmung mit dem ITSM-Prozess Change Management. Zur Planung der nach der Außerbetriebnahme angestrebten Infrastruktur sind optional *Systemarchitekten* hinzuzuziehen. Gegebenenfalls hat die Außerbetriebnahme einzelner Sicherheitsmechanismen auch Auswirkungen auf die *Anwender*.

Schnittstellen:
Durch den erforderlichen Rückbau sind in dieser Phase alle Schnittstellen relevant, die das Security-Framework seit seiner Betriebsphase aufweist. Somit können organisationsübergreifende Abstimmungen ebenso erforderlich sein wie die Berücksichtigung der zwingend vorhandenen Schnittstellen zum IT-Sicherheitsmanagement, die beispielsweise eine Überarbeitung des szenarienspezifischen Gesamtsicherheitskonzepts erforderlich machen. Die Zusammenhänge mit den bislang vom Security-Framework geschützten Assets müssen auch im Rahmen der ITSM-Prozesse betrachtet werden, die über das Change Management die Außerbetriebnahme steuern. Mit dem Security-Framework entfallen zudem Maßnahmen, die sich potentiell auf externe Anforderungen im Rahmen des Compliance Managements und von Zertifizierungsaktivitäten auswirken.

Relevante Anforderungen aus dem Kriterienkatalog:
Die gezielte Unterstützung der Außerbetriebnahme des eigenen Security-Frameworks ist den



Beteiligte Rollen und ihre Zuständigkeiten (RASCI-Matrix)

	Administrator	Anwender	CISO (Leitung)	Prozesseigner	Systemarchitekt
Analyse der techn. Abh.	R		I	A	S
Analyse der org. Abh.	I		A	R	S
Planung	R		I	A	S
Genehmigung	I	I	A	R	I
Außerbetriebnahme	R	I	I	A	S
Review	C		A	R	C

Legende: R – Responsible *(führt aus bzw. stößt an)*
A – Accountable *(ist verantwortlich für)*
S – Support *(unterstützt den Ausführenden bei)*
C – Consulted *(wird befragt zu)*
I – Informed *(wird informiert über Ergebnis von)*

Abbildung 5.11.: Ablauf und Zuständigkeiten in der siebten Lebenszyklusphase (Außerbetriebnahme)

Frameworkautoren gegenüber aus offensichtlichen Gründen schwierig zu motivieren. Der Aufwand zur Planung der Außerbetriebnahme wird jedoch durch Aspekte wie die *Modularität* des Security-Frameworks und die *Wiederverwendbarkeit* von ihm benötigter Komponenten reduziert. Sofern alternative Sicherheitsmechanismen eingeführt oder erhalten bleiben sollen, spielt die Möglichkeit zu deren *Parallelbetrieb* in der Übergangszeit eine wichtige Rolle. Neben diesen Anforderungen aus der Kategorie *SF-INT* können zudem im Rahmen der Einführung des Security-Frameworks eingesetzte *Checklisten* Anhaltspunkte für die zur Außerbetriebnahme durchzuführenden Schritte geben (vgl. Kategorie *SF-DOKU*).

Ablauf und Methoden:
Im Allgemeinen resultieren aus der sich die im Laufe des Betriebs des Security-Frameworks ergebenden Mitbenutzung ausgewählter Komponenten durch andere Dienste und Prozesse gegenüber den Customizing- und Instanziierungsphasen neue Abhängigkeiten, so dass die Außerbetriebnahme nicht genau der Rückabwicklung der Inbetriebnahme entsprechen kann. Da es sich bei der Außerbetriebnahme zudem um ein höchstens einmaliges Ereignis handelt, wäre der Aufwand, sie bereits vorab zu konzipieren und diese Planungen bei allen Änderungen während der Betriebsphase aktuell zu halten, in der Praxis im Allgemeinen nicht gerechtfertigt; eine Ausnahme stellen beispielsweise a priori für einen nur relativ kurzen Betriebszeitraum geplante Frameworkinstanzen dar, für die ihre Außerbetriebnahme z. B. bereits im Betriebskonzept vorgesehen werden kann.

Aus diesem Grund müssen zunächst wie in Abbildung 5.11 dargestellt die Abhängigkeiten zwischen den Frameworkbestandteilen und dem restlichen Szenario ermittelt werden. Bezüglich der technischen Komponenten wird diese Analysephase durch den ITSM-Prozess Configuration Management auf Basis der CMDB unterstützt, die über entsprechende Verknüpfungen zwischen den *Configuration Items* Buch führt. Bezüglich der organisatorischen Abläufe und beispielsweise der Ermittlung der Auswirkungen auf die Betriebskonzepte für die bislang vom Security-Framework geschützten Assets müssen hingegen häufig manuelle Recherchen angestoßen werden, wobei sich je nach Anlass für die Außerbetriebnahme – beispielsweise die Ablösung durch ein anderes Security-Framework oder die gleichzeitige Außerbetriebnahme der betroffenen Dienste – Synergien ergeben und Werkzeuge wie Dokumenten- und Knowledge-Management-Systeme hilfreich sein können.

Bei der Planung der Schritte zur Außerbetriebnahme durch Auflösung der identifizierten Abhängigkeiten muss zudem sichergestellt werden, dass der Schutzbedarf der verbleibenden Assets nicht unbewusst verletzt wird, beispielsweise indem neue Sicherheitsmechanismen rechtzeitig in Betrieb genommen werden oder die Außerbetriebnahme der geschützten Assets vor derjenigen der Frameworkkomponenten durchgeführt wird.

Die Außerbetriebnahme der einzelnen Frameworkkomponenten beginnt nach Genehmigung des Vorhabens unter Steuerung des Change Managements, das auch die rechtzeitige Information der Betroffenen anstößt. Das Abschalten jeder Komponente ist mit einer entsprechenden Aktualisierung der Infrastrukturdokumentation, z. B. im Rahmen der CMDB, verbunden und führt zu einer Reihe von Folgeaktivitäten: Beispielsweise müssen die zuletzt verwendeten Konfigurationseinstellungen und Protokolldateien aus Gründen der Revisionssicherheit noch für eine Karenzzeit aufbewahrt werden, nicht mehr benötigte IT-Geräte und Speichermedien müssen sicher entsorgt oder ihrer Weiterverwendung im Rahmen anderer Dienste zugeführt werden und noch gültige, aber nicht mehr benötigte Serverzertifikate müssen über die PKI ungültig gemacht werden.

Nach dem Abschluss dieser Arbeiten, mit dem der Lebenszyklus der Frameworkinstanz endet, ist die verbleibende Infrastruktur auf ihre uneingeschränkte Funktionsfähigkeit hin zu untersuchen und es sollte ein Review des Einsatzes des Security-Frameworks durchgeführt werden, um die mit seinem Betrieb gesammelten Erfahrungen für zukünftige Vorhaben verwerten zu können.

Abnahmekriterien und Kontrollen:
Die Außerbetriebnahme muss beim Übergang von der Planung zur Durchführung genehmigt werden. Dabei muss sichergestellt werden, dass Risiken, die sich aus dem Wegfall der Sicherheitsfunktionalität des Security-Frameworks ergeben, adäquat berücksichtigt wurden, beispielsweise weil sich der Schutzbedarf reduziert hat oder die rechtzeitige Inbetriebnahme alternativer Maßnahmen geplant wurde. Darüber hinaus muss geprüft werden, ob die geplanten Schritte zur Außerbetriebnahme alle Frameworkkomponenten umfassen, die nicht noch weiterhin anderweitig benötigt werden, und ob sie nach erteilter Genehmigung vollständig und ohne weitere Beeinträchtigung der übrigen Dienste durchgeführt wurden.

Berichtswesen:
Die Planung, die Durchführung und der Abschluss der Außerbetriebnahme muss szenarienintern an die Managementebene und die auch während des Frameworkbetriebs relevanten Zielgruppen, zu denen z. B. auch die Administratoren der Dienste, die einzelne Frameworkkomponenten mit benutzen, gehören, kommuniziert werden. Abschließend sollten auch die

Frameworkautoren über die Motivation und den Verlauf der Außerbetriebnahme des Security-Frameworks informiert werden.

5.11. Konsequenzen für die Entwicklung und den Einsatz von Security-Frameworks

Der Lebenszyklus der Frameworkinstanzen weist wie oben für alle Phasen dargelegt eine Reihe szenarienspezifischer Schnittstellen auf, beispielsweise zum Gesamtsicherheitskonzept und den Abläufen im IT-Sicherheitsmanagement. Sowohl die Auswahl dieser szenarienspezifisch relevanten Schnittstellen als auch deren Umsetzung für ein Security-Framework verläuft jedoch immer wieder ähnlich, so dass die mit einem Security-Framework gewonnenen Erfahrungen auf die Planung des Einsatzes weiterer Security-Frameworks im selben Szenario Einfluss nehmen können. Diese Erfahrungen können insbesondere auch dazu beitragen, den zur Auswahl von Security-Frameworks angewandten Kriterienkatalog im Laufe der Zeit zu überarbeiten und veränderte Schwerpunktkriterien zu bilden. Dies ist beispielsweise dann der Fall, wenn bereits eine größere Anzahl potentiell wiederverwendbarer Sicherheitskomponenten angeschafft wurde, so dass die Integrations- und Managementkriterien gegenüber der reinen Sicherheitsfunktionalität zunehmend an Bedeutung gewinnen. Im Umkehrschluss ergibt sich daraus jedoch auch eine Abhängigkeit von der Reihenfolge, in der Security-Frameworks in einem Szenario eingeführt werden, die bei einer langfristigen Planung berücksichtigt werden müssen.

Für die Konzeption von Security-Frameworks ergibt sich somit einerseits die Auflage, Synergien mit anderen Security-Frameworks zu suchen und zu nutzen. Wie bereits bei der Analyse des Status Quo in Kapitel 4 diskutiert wurde, wird dieses praxisrelevante Umfeld des eigenen Security-Frameworks bislang jedoch von vielen Frameworkautoren nur unzureichend berücksichtigt. Andererseits bekräftigt die Diskussion des Lebenszyklus von Frameworkinstanzen in diesem Kapitel die Forderung, bereits im Frameworkkonzept möglichst alle Lebenszyklusphasen gezielt zu unterstützen. In den Abbildungen 5.12 bis 5.15 ist – die entsprechenden Ausführungen in jeder Phase zusammenfassend – dargestellt, welche der im Kriterienkatalog genannten Anforderungen in welchen Lebenszyklusphasen unmittelbar relevant sind. Daraus lassen sich die folgenden Schlüsse ziehen:

- Zunächst wird die naheliegende Annahme bestätigt, dass für die Auswahl eines Security-Frameworks seine sicherheitsfunktionalen Eigenschaften und seine Dokumentation ausschlaggebend sind. Die effiziente szenarienspezifische Auswahl kann durch eine übersichtliche Dokumentation der entsprechenden Eigenschaften im Frameworkkonzept erheblich erleichtert werden.
- Bereits in der Customizingphase, die – wie in Kapitel 4 dargestellt – bislang nur von einem kleinen Teil der Security-Frameworks umfassend methodisch unterstützt wird, sind rund zwei Drittel aller Anforderungen unmittelbar relevant. Vom Frameworkkonzept nicht ausreichend erfüllte Kriterien schlagen sich somit direkt in einem szenarienspezifischen Mehraufwand nieder, bei dem das Frameworkkonzept um die fehlenden Bestandteile ergänzt werden muss. Dieser Mehraufwand führt zunächst jedoch nur zu szenarienspezifischen Lösungen und kann erst nachfolgend durch geeignete Aufbereitung in das allgemeine Frameworkkonzept einfließen.

Kriterium	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7	Summe	Gewicht laut Kriterien-katalog
SF-FUNK-Abschottung		+			+			2	2
SF-FUNK-Adaptivität					+			1	1
SF-FUNK-Angriffe	+				+			2	2
SF-FUNK-Assets	++	+			+			4	4
SF-FUNK-Auditing		+	+	+	+			4	4
SF-FUNK-Automatisierung		+			+			2	2
SF-FUNK-Maßnahmen	++	+	+		+			5	4
SF-FUNK-Schwachstellen	+				+			2	2

Legende:

+	relevant (1 Punkt)
++	maßgeblich relevant (2 Punkte)
**	essentiell (4 Punkte)

Abbildung 5.12.: Relevanz der Kriterien aus Kategorie *SF-FUNK* in den Lebenszyklusphasen von Frameworkinstanzen

Kriterium	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7	Summe	Gewicht laut Kriterien-katalog
SF-INT-Ausbauphasen		+				+		2	2
SF-INT-Customizing		**						4	4
SF-INT-Einführung			+	+				2	2
SF-INT-Erweiterung		+				+		2	2
SF-INT-Hochverfügbarkeit		+			+			2	2
SF-INT-Kompatibilität		+	+					2	2
SF-INT-Modularität		+					+	2	2
SF-INT-Parallelbetrieb		+			++		+	4	4
SF-INT-Polyinstanziierbarkeit		+						1	1
SF-INT-Skalierbarkeit		+			++	+		4	4
SF-INT-Usablility		+			+			2	2
SF-INT-Wiederverwendbarkeit		+					+	2	2

Legende:

+	relevant (1 Punkt)
++	maßgeblich relevant (2 Punkte)
**	essentiell (4 Punkte)

Abbildung 5.13.: Relevanz der Kriterien aus Kategorie *SF-INT* in den Lebenszyklusphasen von Frameworkinstanzen

- Die hohe Relevanz einer Vielzahl von Anforderungen trifft analog dazu auch auf die Betriebsphase zu, wobei sich der Schwerpunkt dort von den Integrations- hin zu den Managementanforderungen und den sicherheitsfunktionalen Eigenschaften verschiebt. Die Lebenszyklusphasen 2 und 5 sollten aufgrund dieser Schwerpunktbildung entsprechend auch im Fokus der Frameworkdokumentation liegen. Dieser Bedarf wird von den bislang überwiegend anhand der technischen Frameworkarchitektur gegliederten Frameworkdo-

Kriterium	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7	Summe	Gewicht laut Kriterien-katalog
SF-MGMT-Adminkonzepte		+			+			2	2
SF-MGMT-Berichtsdetails			+		+			2	2
SF-MGMT-Compliance		+		+	++			4	4
SF-MGMT-Delegation		+			+			2	2
SF-MGMT-Events					+			1	1
SF-MGMT-ITSM-Schnittstellen		+	+		++			4	4
SF-MGMT-Kosten		+			+			2	2
SF-MGMT-KPIs					+			1	1
SF-MGMT-Mandantenfähigkeit		+			+			2	2
SF-MGMT-Metriken		+	+		+	+		4	4
SF-MGMT-Operationen		+	+		++			4	4
SF-MGMT-Performanz				+	+			2	2
SF-MGMT-Policies			++					2	2
SF-MGMT-Praxis					++			2	2
SF-MGMT-Prozesse		+	+		++			4	4
SF-MGMT-Quantifizierung		+			+			2	2
SF-MGMT-Releasezyklus		+				+		2	2
SF-MGMT-Schulungen		+	+		+			3	2
SF-MGMT-Support					+			1	1
SF-MGMT-Tests			+	+				2	1
SF-MGMT-Verbesserung					++	++		4	4
SF-MGMT-Zuständigkeiten		+						1	1

Legende:

+	relevant (1 Punkt)
++	maßgeblich relevant (2 Punkte)
**	essentiell (4 Punkte)

Abbildung 5.14.: Relevanz der Kriterien aus Kategorie *SF-MGMT* in den Lebenszyklusphasen von Frameworkinstanzen

kumentationen jedoch noch nicht erfüllt (vgl. die Strukturanalyse in Abschnitt 4.2).

- Die übrigen Phasen – Implementierung, Inbetriebnahme, Überarbeitung und Außerbetriebnahme – sind zwar deutlich erkennbar szenarienspezifisch geprägt, können in einigen Bereichen auf Basis der jeweils angegebenen Anforderungen aber gezielt vom Frameworkkonzept unterstützt werden und dürfen deshalb bei der Frameworkdokumentation nicht vernachlässigt werden.

In den Abbildungen wird die ermittelte Relevanz der Anforderungen in den Lebenszyklusphasen auch der Gewichtung im Kriterienkatalog (vgl. Abschnitt 3.7.3) gegenübergestellt. Dabei ergibt sich zu einem sehr großen Teil eine genaue Übereinstimmung, d. h. das Gewicht einer Anforderung korreliert im Regelfall mit der Anzahl der davon betroffenen Lebenszyklusphasen; lediglich bei den folgenden Anforderungen treten Abweichungen auf:

- *SF-FUNK-Maßnahmen:* Die vom Frameworkkonzept vorgeschlagenen IT-Sicherheitsmaßnahmen bilden den technischen Kern des Security-Frameworks. Aufgrund ihrer maßgeblichen Relevanz in der Auswahlphase und ihrer praktischen Bedeutung in drei weiteren Lebenszyklusphasen ergeben sich bei den Betrachtungen in

Kriterium	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Phase 7	Summe	Gewicht laut Kriterien-katalog
SF-DOKU-Anforderungsanalyse	+	+						2	2
SF-DOKU-Angreifermodelle	+	+						2	2
SF-DOKU-Ausrichtung	+	+						2	2
SF-DOKU-Beurteilung		+						1	1
SF-DOKU-Checkliste		+		+			+	3	1
SF-DOKU-Designentscheidungen	+	+						2	2
SF-DOKU-Kontinuum						+		1	1
SF-DOKU-Lifecyclephasen		+						1	1
SF-DOKU-Vollständigkeit	+	+						2	2
SF-DOKU-Voraussetzungen	**							4	4
SF-DOKU-Zertifizierung				+				1	1
SF-DOKU-Ziele	**							4	4
SF-DOKU-Zielgruppe		+						1	1

Legende:		
	+	relevant (1 Punkt)
	++	maßgeblich relevant (2 Punkte)
	**	essentiell (4 Punkte)

Abbildung 5.15.: Relevanz der Kriterien aus Kategorie *SF-DOKU* in den Lebenszyklusphasen von Frameworkinstanzen

diesem Kapitel 5 Punkte im Unterschied zum Gewichtsfaktor 4 im Kriterienkatalog, der dort das maximale Gewicht darstellt.

- *SF-MGMT-Schulungen:* Die Schulungen sind sowohl in der Einführungsphase als auch im späteren laufenden Betrieb, beispielsweise für neu hinzukommendes Personal, relevant. Die in Phase 2 vorzubereitenden Schulungen sind deshalb gleichermaßen für die Phasen 3 und 5 relevant, so dass im Frameworkkonzept diesbezüglich im Allgemeinen keine inhaltliche Differenzierung erforderlich ist. Diese Reduktion auf *Planung* und *Durchführung* von Schulungen deckt sich mit dem im Kriterienkatalog vergebenen Gewichtsfaktor 2.

- *SF-MGMT-Tests:* Die vom Frameworkkonzept vorgegebenen Tests sind sowohl für die Beurteilung der Einzelkomponenten am Ende der Implementierungsphase als auch für die Analyse des gesamten Security-Frameworks in der Test- und Inbetriebnahmephase relevant. Aufgrund der erläuterten, zwingend erforderlichen Spezifikation und Durchführung szenarienspezifischer Tests bleibt der Gewichtsfaktor 1 für die vom Frameworkkonzept vorgegebenen Tests gegenüber der Relevanz in 2 Phasen jedoch gerechtfertigt.

- *SF-DOKU-Checkliste:* Die als Bestandteil der Frameworkdokumentation geforderte Checkliste für die im Rahmen von Customizing und Inbetriebnahme anfallenden Tätigkeiten kann wie erläutert auch bei der Außerbetriebnahme herangezogen werden und ist somit in 3 Phasen der Frameworkinstanz relevant. Aufgrund der diskutierten Notwendigkeit szenarienspezifischer Ablaufspezifikationen, die von szenarienunabhängigen Checklisten nur teilweise antizipiert werden kann, ist der im Kriterienkatalog vergebene Gewichtsfaktor 1 jedoch weiterhin gerechtfertigt.

Durch die drei Teilergebnisse, dass

1. die Gewichte der einzelnen Kriterien weitgehend mit der Anzahl der Phasen, in denen die Kriterien relevant sind, korrelieren,
2. in den Phasen 2 und 5 Häufungen unmittelbar relevanter Kriterien auftreten, und
3. in Abschnitt 4.5.2 ermittelt wurde, dass insbesondere die Anforderungskategorien *SF-INT* und *SF-MGMT* bislang unzureichend erfüllt werden,

wird belegt, dass die meisten Security-Frameworks bislang sowohl die Customizing- als auch die Betriebsphase noch unzureichend unterstützen.

Für den Einsatz von Security-Frameworks bedeutet dies die praktische Einschränkung, dass sich beim beschriebenen Vorgehen – ähnlich zu anderen komplexen IT-Diensten und IT-Architekturen – viele Eigenschaften leider erst in der Customizingphase und zum Teil sogar erst im laufenden Betrieb vollständig entfalten. Um diesen Nachteil zu kompensieren, müssten die Auswahlphasen wesentlich umfangreicher gestaltet werden; beispielsweise müssten bereits viele der notwendigen szenarienspezifischen Anpassungen der Security-Frameworks vorgenommen und eine detaillierte praktische Evaluation durchgeführt werden. Dies ist wie bereits in Abschnitt 5.4 aufgrund des damit verbundenen Mehraufwands im Allgemeinen nicht realisierbar. Somit bestätigt sich erneut der Bedarf, über die Rückmeldung praktischer Erfahrungen auf die Weiterentwicklung und Verbesserung der Frameworkkonzepte Einfluss zu nehmen, um langfristig universeller einsetzbare Security-Frameworks zu erhalten und deren szenarienspezifische Beurteilung effizienter zu gestalten.

5.12. Zusammenfassung

In diesem Kapitel wurde als erstes erläutert, welche zu den Anforderungen an Security-Frameworks komplementären Voraussetzungen im jeweiligen Einsatzszenario erfüllt werden müssen, um die szenarienspezifische Instanziierung vornehmen zu können. Dieser allgemeinen Darstellung des Umfelds, in das Security-Frameworks integriert werden müssen, folgte ein Überblick über die Lebenszyklen von Frameworkkonzepten und Frameworkinstanzen sowie deren Schnittstellen zueinander und zu diesem Umfeld. Den Schwerpunkt des Kapitels bildete die einheitlich strukturierte Darstellung u. a. der Ziele, Schwerpunkte und Abläufe in jeder der sieben Phasen des Lebenszyklus von Frameworkinstanzen, der sich von der initialen Auswahl eines Security-Frameworks für ein Szenario bis hin zur Außerbetriebnahme der produktiv betriebenen Frameworkinstanz erstreckt. Ein Vergleich der Relevanz der in Kapitel 3 definierten Anforderungen für die einzelnen Lebenszyklusphasen mit deren Gewichtung und mit den Ergebnissen der Untersuchungen in Kapitel 4 hat schließlich gezeigt, dass sowohl die Customizing- als auch die Betriebsphase von Security-Frameworks noch besser unterstützt werden muss. Im nächsten Kapitel wird deshalb vertiefend auf die Betriebsphase und insbesondere die damit verbundenen operativen und organisatorischen Managementabläufe eingegangen.

Kapitel 6.

Security-Framework-Managementprozesse und -schnittstellen

Inhalt dieses Kapitels

Dieses Kapitel behandelt das integrierte Management von Security-Frameworks. Unter **Integration** werden dabei sowohl die frameworkübergreifende, skalierbare Anwendung einheitlicher Managementmethoden als auch die nahtlose Einbettung aller eingesetzten Security-Frameworks in die Prozesslandschaft in Unternehmensumgebungen verstanden. Für diese müssen, wie in Kapitel 2 diskutiert wurde, neben dem facettenreichen Prozess *Security Management* insbesondere die ITSM-Prozesse betrachtet werden. Insgesamt werden zahlreiche für die IT-Sicherheit relevante Managementprozesse aus der Perspektive von Security-Frameworks betrachtet, um die erforderlichen Schnittstellen definieren, vorhandene Methoden anpassen und deren Anwendbarkeit darlegen zu können.

Die vorangegangenen Kapitel haben wiederholt verdeutlicht, dass der Schwerpunkt aktueller Security-Frameworks eindeutig auf den technischen Sicherheitsmechanismen liegt. Diese Stärke ist prinzipiell zu begrüßen, da das Eintreten IT-sicherheitsrelevanter Vorfälle und ihre Auswirkungen letztlich direkt mit der Güte der technischen Sicherheitsmechanismen korrelieren. Die fundierte, systematische Auseinandersetzung mit dem Management von Security-Frameworks ist dennoch zwingend erforderlich; hierfür werden nachfolgend drei ausgewählte Gründe genannt, die sich auch als Motivation bzw. Zielsetzung bei allen in diesem Kapitel erörterten Themen wiederfinden: Erstens werden die technischen Infrastrukturen und die eingesetzten Sicherheitsmechanismen in der Praxis derart komplex, dass eine methodische Auseinandersetzung und ein **strukturiertes Vorgehen beim Betrieb** notwendig werden, um auch bei technischen Detailbetrachtungen nicht den Überblick über die Gesamtstruktur und die Zusammenhänge der beteiligten Komponenten zu verlieren. Zweitens können auch sehr umfangreiche technische Sicherheitsmechanismen das Eintreten IT-sicherheitsspezifischer Schadereignisse nicht völlig verhindern. Nachdem der a priori vorgesehene technische Schutz ausgehebelt wurde, sind jedoch die **definierten organisatorischen Abläufe** ausschlaggebend dafür, dass der Schaden begrenzt wird und schnellstmöglich zum regulären Betrieb zurückgekehrt werden kann. Auch wenn Teile dieser Abläufe wiederum durch Werkzeuge unterstützt oder teilautomatisiert werden, müssen diese zunächst auf einer konzeptionellen Ebene festgelegt worden sein. Drittens stellen sämtliche IT-Sicherheitsmaßnahmen keinen Selbstzweck dar, sondern müssen **auf die Geschäftsabläufe und die Erbringung von IT-Dienstleistungen abgestimmt** werden. Dies hat einerseits die Auswirkung, dass Security-Frameworks ebenso wie andere Komponenten der IT-Infrastruktur unter anderem bezüglich

ihres Kosten-/Nutzenverhältnisses beurteilt werden müssen. Andererseits muss erreicht werden, dass die IT-Sicherheit kein Thema ist, das in einer Organisation nur von einer separaten Expertengruppe behandelt wird; vielmehr müssen die mit der IT-Sicherheit verbundenen Fragestellungen auch zu einem festen Bestandteil der Betrachtungen in den Fachabteilungen werden. Diesbezüglich wird in diesem Kapitel erläutert, wie sich die durch Security-Frameworks erzielbare Bündelung IT-sicherheitsrelevanter Themen nutzen lässt, um diese gezielter kommunizieren und behandeln zu können.

Bei der Diskussion einzelner Security-Frameworks und des Lebenszyklus von Frameworkinstanzen wurden ferner zahlreiche Anforderungen genannt, die *im laufenden Betrieb* bzw. *für das Management* relevant sind. Die Behandlung der entsprechenden Abläufe setzt eine Differenzierung zwischen zwei komplementären Teilen des Sicherheitsmanagements voraus: Einerseits muss **Security Management als Prozess** und damit als organisatorisches Instrument betrachtet werden, in dem konzeptionelle Aufgaben wie das Risikomanagement und das Festlegen z. B. der Reaktionen auf IT-Sicherheitsvorfälle übernommen werden. Andererseits ist das **operative Sicherheitsmanagement** zu betrachten, bei dem Dienst- und Systemadministratoren sowie ggf. dediziertes IT-Sicherheitspersonal die vielfältigen Aufgaben rund um den Betrieb und die Wartung IT-sicherheitsrelevanter technischer Komponenten übernimmt. Beide Bereiche sind durch eine hohe Dynamik und kontinuierliche Weiterentwicklung geprägt: Die Anforderungen an und die Schwerpunkte des Sicherheitsmanagementprozesses, die in Abschnitt 6.1 auf Basis einer Literaturrecherche analysiert und den mit Security-Frameworks verfolgten Zielen gegenübergestellt werden, haben sich innerhalb der letzten 20 Jahre mehrfach komplett gewandelt und sind in ihrer Entwicklung noch bei Weitem nicht in einer stabilen Phase angekommen. So darf beispielsweise die wachsende Zahl nach ISO/IEC 27001 zertifizierter Unternehmen nicht darüber hinweg täuschen, dass die auf das Informationssicherheitsmanagement fokussierte Normenreihe ISO/IEC 27000 weiterhin noch im Entstehen ist und ISO/IEC 27001 lediglich Minimalanforderungen spezifiziert. Auch bei den in Abschnitt 6.2 diskutierten Aufgaben des operativen IT-Sicherheitsmanagements, für das zunächst eine Begriffsbildung und eine Zusammenstellung und Kategorisierung seiner Teilbereiche vorgenommen werden, handelt es sich um eine Momentaufnahme, mit der die Vielseitigkeit verdeutlicht wird, die Security-Frameworks sowohl sicherheitstechnisch-funktional als auch bezüglich ihrer Integration in die technischen Betriebsabläufe aufweisen müssen.

Nach diesem zweigeteilten Überblick über das Managementumfeld, in das Security-Frameworks eingebettet werden müssen, sind die weiteren Abschnitte dieses Kapitels der Vertiefung ausgewählter Schwerpunkte gewidmet, die die im Rahmen dieser Arbeit vorgenommenen, für Security-Frameworks spezifischen Anpassungen des Sicherheitsmanagements erforderlich machen. In Abschnitt 6.3 werden aktuelle wissenschaftliche und in der Praxis etablierte **Methoden für das Management von IT-sicherheitsbezogenen Risiken** vorgestellt, verglichen und bewertet sowie ihre Anpassung an die Spezifika der Security-Frameworks konzipiert und Möglichkeiten zur Kombination verschiedener Ansätze untersucht. Dieser Abschnitt bildet den Anfang der vertiefenden Betrachtungen, da das Risikomanagement in fast allen Standards und Best-Practice-Dokumenten als Schlüsselelement und treibende Kraft hinter dem Sicherheitsmanagement positioniert wird. Die von Security-Frameworks induzierte Aggregation von IT-sicherheitsrelevanten Konzepten und technischen Komponenten trägt dabei maßgeblich zur Vereinfachung und effizienten Umsetzung einiger der Kernkomponenten des Risikomanagements bei.

In Abschnitt 6.4 wird anschließend eine **integrierte Managementarchitektur für**

Security-Frameworks konzipiert. Die zentral betrachtete und im Rahmen dieser Arbeit gelöste Fragestellung ist dabei, welche Anpassungen vorgenommen werden müssen, um nicht nur ihre Einzelkomponenten, sondern um Security-Frameworks als Ganzes beispielsweise als *Managed Objects* oder *Configuration Items* auffassen und mit etablierten Managementmethoden handhaben zu können. Den Schwerpunkt bildet dabei die Erarbeitung eines auf den in diesem Kapitel betrachteten Konzepten basierendes Informationsmodell für eine Managementarchitektur. Ferner werden Auswirkungen, die sich durch die Anwendung der erarbeiteten Konzepte auf IT-Sicherheitswerkzeuge in ausgewählten Bereichen des operativen IT-Sicherheitsmanagements ergeben, analysiert.

Die **prozessrelevanten Schnittstellen von Security-Frameworks** sind Gegenstand von Abschnitt 6.5. Dabei wird zum einen anhand einer Analyse von ISO/IEC 27001 konzipiert, welche Subprozesse des Sicherheitsmanagements um welche Aspekte konzeptionell zu verfeinern sind, wenn Security-Frameworks eingesetzt werden sollen. Zum anderen werden unter Orientierung an ITIL v3 die Schnittstellen zu den als unmittelbar relevant identifizierten ITSM-Prozessen spezifiziert, um damit beispielsweise den Ablauf der Bearbeitung eines Sicherheitsvorfalls im Zusammenspiel mit dem Incident Management und dem Change Management darzustellen. Ebenso wird auf die Bereiche IT-Governance und Compliance Management, bei denen das Sicherheitsmanagement, die ITSM-Prozesse und das operative Management eng zusammenarbeiten müssen, eingegangen. Alle erarbeiteten Schnittstellenkonzepte werden zudem in den Kontext der in Kapitel 5 spezifizierten Lebenszyklusphasen eingeordnet.

Über alle betrachteten Bereiche hinweg zeigt sich dabei, dass für eine effiziente Steuerung der Abläufe rund um das Management von Security-Frameworks geeignete und spezifische Entscheidungsgrundlagen benötigt werden, die sich nicht nur aus den jeweiligen Frameworkkonzepten ergeben, sondern eine permanente, gezielte Überwachung der Security-Frameworks und der von ihnen geschützten Infrastruktur voraussetzen. In Abschnitt 6.6 stehen deshalb das **Messen und Beurteilen** der IT-sicherheitsrelevanten Eigenschaften von Security-Frameworks, die Verarbeitung der Messwerte in Form von IT-Sicherheitskennzahlen und deren Aufbereitung zu Berichten für verschiedene Zielgruppen wie z. B. Systemadministratoren oder das Risikomanagement im Vordergrund. Dabei werden durch eine Literaturrecherche die in dieser Disziplin noch vorherrschenden Defizite aufgezeigt und eine auf Security-Frameworks zugeschnittene Methodik zur Konzeption und Verwaltung von IT-Sicherheitskennzahlen spezifiziert. Sowohl für einzelne Kennzahlen als auch deren Aufbereitung in Form von Sicherheitsberichten werden Informationsmodelle und Verarbeitungsabläufe konstruiert. Als Beispiel für die praktische Anwendung von Sicherheitsberichten wird gezeigt, wie das Sicherheitsinvestitionsmodell von Gordon und Loeb auf Security-Frameworks übertragen werden kann.

Das Kapitel, dessen Struktur in Abbildung 6.1 zusammengefasst ist, schließt mit einer Rekapitulation der wesentlichen Ergebnisse und einem Ausblick auf die im nächsten Kapitel vertieften Werkzeugkonzepte.

6.1. Einbettung von Security-Frameworks in den Sicherheitsmanagementprozess

In Kapitel 3 wurde eine Reihe managementrelevanter Anforderungen an Security-Frameworks in der Kategorie *SF-MGMT* zusammengefasst, die somit bereits einen groben Rahmen der

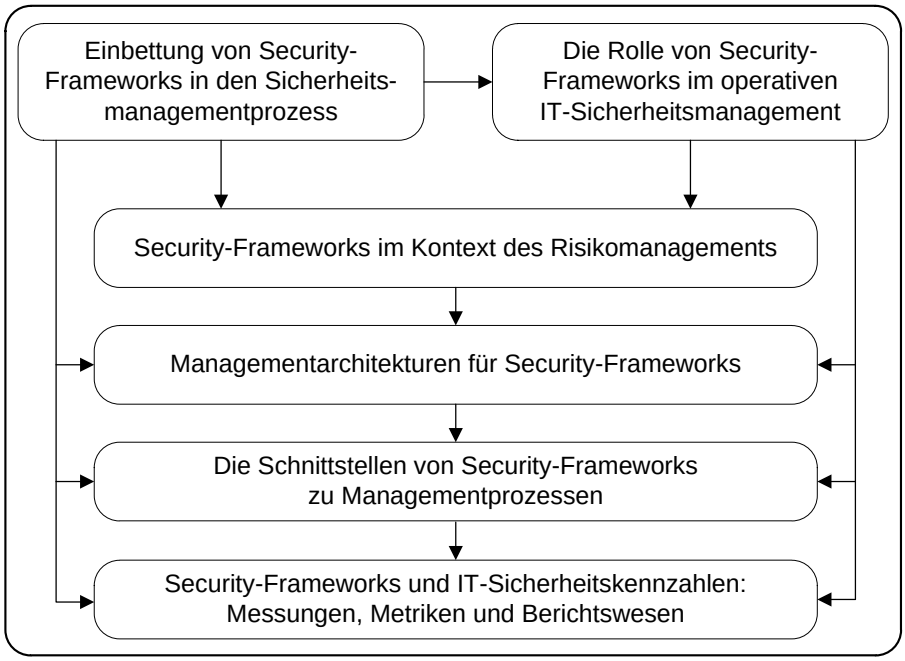


Abbildung 6.1.: Vorgehensmodell in diesem Kapitel

für Security-Frameworks spezifischen Schwerpunkte des Sicherheitsmanagements absteckt. In diesem Abschnitt wird darüber hinausgehend jedoch eine umfassende Einordnung der konzeptionellen und praktischen Teilaspekte von Security-Frameworks in den gesamten Sicherheitsmanagementprozess vorgenommen.

Hierzu werden nachfolgend die einzelnen Aufgabenbereiche des Sicherheitsmanagementprozesses auf Basis einer Literaturrecherche zusammengestellt und ihr Bezug zu Security-Frameworks erarbeitet. Dabei wird zur weiteren Differenzierung gegenüber dem in Abschnitt 6.2 thematisierten operativen IT-Sicherheitsmanagement knapp auf den anhaltenden Wandel dieses Prozesses und seiner Teilbereiche eingegangen. Daran anschließend werden im Kontext von Security-Frameworks relevante Standards und Best Practices zum Sicherheitsmanagementprozess vorgestellt, denen eine hohe praktische Verbreitung attestiert werden kann und auf die häufig in Publikationen zum Sicherheitsmanagement Bezug genommen wird. Der dabei analog zu ITSM-Referenzprozessen erkennbare Abstraktionsgrad zeigt sich noch deutlicher bei den in Abschnitt 6.1.3 im Überblick dargestellten gesetzlichen Auflagen zum Sicherheitsmanagement, die unter dem Stichwort *IT-Compliance* für einen großen Kreis an Organisationen relevant und häufig ausschlaggebend dafür sind, ob und in welchem Umfang die von einem Security-Framework vorgesehenen Maßnahmen praktisch umgesetzt werden können. Die Auswirkungen der diskutierten Aspekte auf das Management von Security-Frameworks werden in Abschnitt 6.1.4 abgeleitet und diskutiert.

6.1.1. Aufgaben des Sicherheitsmanagementprozesses und ihr Bezug zu Security-Frameworks

Nach von Solms [vS00] verlief die Ausbreitung der jeweils aktuellen Sicherheitsmanagementkonzepte bisher in drei Wellen: Die erste Welle, die ihren Höhepunkt in den 1980er Jahren hatte, deren Auswirkungen aber noch bis in die Mitte der 1990er Jahre spürbar waren, war demnach äußerst technisch geprägt, d. h. auf einzelne Infrastrukturkomponenten und technische Sicherheitsmechanismen konzentriert. Die zweite Welle, in den 1990ern bis zur Jahrtausendwende hin angesiedelt, stellte nach von Solms davon radikal abkehrend insbesondere die Interessen der höheren Managementebenen in den Vordergrund, vernachlässigte dabei aber essentielle Aspekte der praktischen Umsetzung: So wurden zwar IT-sicherheitsspezifische Policies top-down-orientiert vorgegeben; zur nachhaltigen Umsetzung dieses IT-Governance-Ansatzes fehlten jedoch Maßnahmen zur Überwachung der Umsetzung der notwendigen Sicherheitsmechanismen und entsprechende Berichtswege, so dass keine Rückkopplung stattfinden konnte. Erst in der nach wie vor aktuellen dritten Welle wurde damit begonnen, international anerkannte Best Practices und inzwischen verfügbare Standards zum Sicherheitsmanagement und einen bidirektionalen Informationsfluss umzusetzen.

6.1.1.1. Technischer Ursprung der Disziplin am Beispiel ISO/OSI Security Architecture

Einer der ersten und unter didaktischen Gesichtspunkten nach wie vor äußerst wertvollen Ansätze zur Festlegung der Aufgaben des Sicherheitsmanagements entstand Anfang der 1980er Jahre in den Entwürfen zum späteren Standard ISO 7498-2 [I7498] – *Open Systems Interconnection (OSI) – Basic reference model – Part 2: Security architecture*. Das OSI-Management wurde in die unter dem Akronym FCAPS bekannt gewordenen fünf Funktionsbereiche Fault, Configuration, Accounting, Performance und Security Management eingeteilt. Durch den Fokus auf das Management von verteilten Systemen und Netzen steht beim Security Management die Zugriffskontrolle auf an das Netz angeschlossene Komponenten und Endgeräte im Vordergrund. Die OSI-Sicherheitsarchitektur unterscheidet zwischen den folgenden drei Managementkategorien:

1. **System Security Management**: Hierunter wird das Management der Sicherheitseigenschaften des gesamten verteilten Systems, nicht das einer einzelnen Maschine bzw. eines einzelnen Endgeräts, unter Berücksichtigung von aktiven und passiven Angriffen verstanden.
2. **Security Services Management**: Die OSI-Sicherheitsarchitektur sieht Sicherheitsdienste für die Bereiche Authentisierung, Zugriffskontrolle, Vertraulichkeit, Datenintegrität und Verbindlichkeit vor. Bereits die direkte Gegenüberstellung dieser Bereiche mit den in Kapitel 2 erläuterten Zielen – einerseits der (technischen) IT-Sicherheit und andererseits des (organisatorischen) Sicherheitsmanagements – verdeutlicht die eindeutig technische Ausrichtung, die aus heutiger Sicht klar dem *operativen* Sicherheitsmanagement zugeordnet werden muss.
3. **Security Mechanisms Management**: Zur Umsetzung der Security Services wird vorrangig auf kryptographische Mechanismen wie Verschlüsselung, digitale Signaturen und kryptographische Prüfsummenverfahren zurückgegriffen, so dass sich auch in diesem Bereich die primär technische Ausprägung zeigt. In der Kategorie *Pervasive Security*

Mechanisms werden jedoch auch Mechanismen zur Umsetzung einer Informationsklassifizierung sowie zur Protokollierung und Auswertung von (sicherheitsbezogenen) Ereignissen spezifiziert, die auch nach aktueller Auslegung ein direktes Gegenstück im organisatorischen Ablauf mit sich bringen müssen.

Die Sicherheitsdienste stellen dabei eine Abstraktionsschicht dar, mit der die als Policies formulierten Zielsetzungen des Sicherheitsmanagements auf der Basis der verfügbaren Sicherheitsmechanismen umgesetzt werden. Die Zuordnung von Sicherheitsmechanismen zu Sicherheitsdiensten der ISO/OSI Security Architecture ist ein auch für die Analyse von Security-Frameworks nützliches Werkzeug, dessen Bedeutung in der Praxis seit der Verfügbarkeit neuerer Best-Practice-Referenzen wie CobiT, die eine ähnliche Abbildung vorsehen, jedoch abnimmt (vgl. Abschnitt 6.1.2).

6.1.1.2. Übergang von der technischen zur organisatorischen Ausprägung des Sicherheitsmanagements

Die bis ca. 1997 veröffentlichen Arbeiten verdeutlichen, dass sowohl in der Wissenschaft als auch der Industrie bis zu etwa diesem Zeitpunkt die technischen Aspekte des Sicherheitsmanagements klar im Vordergrund standen. Der damalige Status Quo zu diesem Zeitpunkt zeigt sich besonders gut am IETF RFC 2196 [RC2196], das 1997 von Barbara Frazer an der CMU aus zahlreichen Beiträgen anderer Autoren zusammengestellt wurde und aufgrund der weiten praktischen Verbreitung der IETF-Vorgaben weltweit eine Vielzahl von Sicherheitskonzepten und -werkzeugen beeinflusst hat. Als praktischer Leitfaden für Administratoren zur Absicherung ihrer Daten und Dienste konzipiert, stellt RFC 2196 eines der ersten umfassenden Best-Practice-Dokumente zum Sicherheitsmanagement dar. Charakteristisch für den Zeitpunkt der Veröffentlichung ist dabei aus heutiger Sicht und mit Bezug zur vorliegenden Arbeit, dass

- RFC 2196 *implizit risikogetrieben* vorgeht, d. h. es wird ein aus den Schritten Schutzbedarfsidentifikation, Bedrohungsidentifikation, Eintrittswahrscheinlichkeitsanalyse, Maßnahmenumsetzung und Maßnahmenüberwachung bestehender Prozess definiert, ohne dass der Begriff *Risikomanagement* verwendet oder auf eine der in Abschnitt 6.3 diskutierten Risikomanagementmethoden eingegangen wird. Das Risikomanagement entwickelt sich vielmehr bottom-up als notwendige Maßnahme zur Priorisierung von Zielen und Maßnahmen in Anbetracht der bereits zum damaligen Zeitpunkt stetig komplexer werdenden IT-Infrastrukturen.
- RFC 2196 eine relativ umfangreiche Liste technischer Sicherheitsmechanismen vorgibt, die durch die Nennung von Protokoll- und Produktnamen einen Grad an Konkretisierung erreicht, von dem in allen in Abschnitt 6.1.2 diskutierten aktuellen Standards und Best Practices bewusst Abstand genommen wurde.

Obwohl RFC 2196 damit für einzelne, punktuelle Problembereiche sehr spezifische Lösungen vorstellt, schlägt das Dokument zugleich eine Brücke zu den folgenden drei organisatorischen Bereichen, die zu den Eckpfeilern des modernen Sicherheitsmanagements zählen:

1. RFC 2196 fordert die Dokumentation von Richtlinien (Policies), die für alle Organisationsangehörigen verbindlich sind, unter anderem in den Bereichen Datenschutz, Zugriffskontrolle, Authentifizierung und (Informations- und Dienst-) Verfügbarkeit.

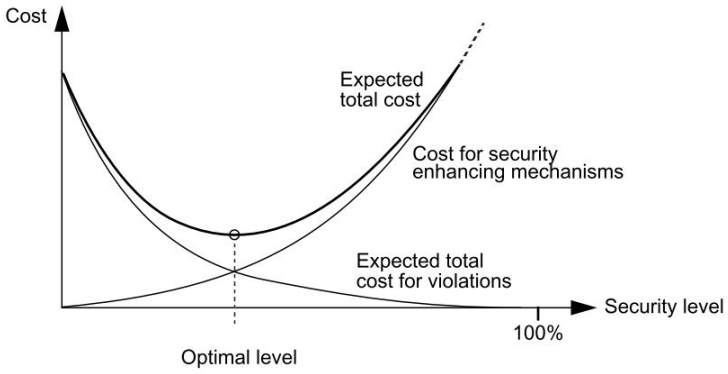


Abbildung 6.2.: Kosten für Sicherheitsmechanismen in Relation zu Kosten für Sicherheitsvorfälle (aus [Olo92])

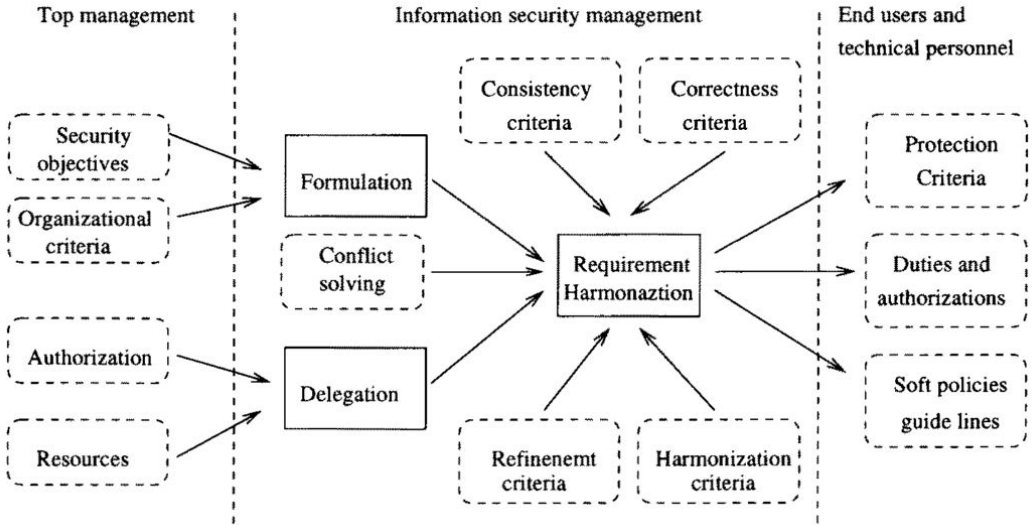


Abbildung 6.3.: Vorschlag für die Aufgabenverteilung im Sicherheitsmanagement aus dem Jahr 1997 (aus [LGZ97])

2. In RFC 2196 wird ein umfassender *Security Incident Handling* Prozess vorgestellt, der beispielsweise auch darauf eingeht, welche diesbezüglichen Aufgaben technische Administratoren bzw. das Management haben und bei welcher Art von Vorfällen beispielsweise auch Behörden eingeschaltet werden sollen.
3. RFC 2196 regt eine kontinuierliche Verbesserung des Sicherheitsmanagements an, beispielsweise indem die o. g. Policies mindestens jährlich auf notwendige Aktualisierungen überprüft werden.

Nachdem Anfang bis Mitte der 1990er Jahre auch eine intensive Auseinandersetzung mit den Kosten für die IT-Sicherheit stattfand, die auf den in Abbildung 6.2 dargestellten, anzustrebenden Kompromiss aus hohen Kosten für Sicherheitsvorfälle und hohen Kosten für

Sicherheitsmechanismen eingingen, wurde in der zweiten Hälfte der 1990er Jahre klar, dass in das Management der IT-Sicherheit auch die Führungsebene der Organisationen einbezogen werden muss. So stellten Leiwo und Zheng 1997 in [LGZ97], einer der ersten wissenschaftlichen Veröffentlichungen zum modernen Sicherheitsmanagement, die in Abbildung 6.3 dargestellte Aufgabenverteilung auf die drei Rollen *Top Level Management*, *Information Security Management* und *Technical Personnel* vor. Diese Dreiteilung, bei der eine dediziert mit der IT-Sicherheit betraute Expertengruppe Schnittstellen sowohl zum im Allgemeinen nicht IT-fokussierten Management als auch zu den mit dem operativen Betrieb betrauten Technik- und IT-Fachabteilungen pflegen muss, hat sich zwischenzeitlich auf breiter Basis durchgesetzt.

Im selben Zeitraum, in dem mit dieser Professionalisierung und Prozessorientierung des Sicherheitsmanagements begonnen wurde, kam auch der Begriff *Security-Framework* als Bezeichnung für die von konkreten Szenarien abstrahierte Zusammenstellung von Mechanismen und Maßnahmen auf, die sicherheitsrelevante Fragestellungen nicht mehr nur punktuell, sondern problem- und später dienstorientiert lösen sollten. Im nächsten Abschnitt werden die resultierenden Charakteristika der Security-Frameworks in die aktuellen Ansätze zum Sicherheitsmanagement eingeordnet.

6.1.1.3. Einordnung von Security-Frameworks in das aktuelle Verständnis des Sicherheitsmanagements

Mit dem Abkommen von rein technischen Betrachtungen in der oben erläuterten *zweiten Welle* des Sicherheitsmanagements ergaben sich durch den Einbezug des Managements neue Möglichkeiten, Geschäftspartnern und Kunden gegenüber zu demonstrieren, dass Informationssicherheit ein vom eigenen Unternehmen ernst genommenes Thema ist. Der Bedarf, die eigenen Bemühungen um das Sicherheitsmanagement auch nach außen wirksam zu dokumentieren, mündete in Forderungen nach einer mit ISO 9001 vergleichbaren Zertifizierung, die das Unternehmen gesamtheitlich bezüglich der Informationssicherheit auditiert (vgl. [vS96] und [Elo03]). Davon sind nach [vS00] insbesondere die folgenden drei Vorteile zu erwarten:

1. Durch die in Standards und Audits behandelten Teilbereiche des Sicherheitsmanagements kann verhindert werden, dass ein Unternehmen einen wichtigen Aspekt des Sicherheitsmanagements gänzlich übersieht.
2. Durch Zertifizierungen nach einheitlichen Kriterien kann die eigene Position gegenüber Kunden und Partnern verbessert werden.
3. Auf Basis von Standards können Kennzahlen definiert werden, die auch bei rein interner Verwendung Aufschluss darüber geben, wie gut die einzelnen Teilbereiche im Unternehmen bereits umgesetzt wurden.

Dadurch motiviert und im Zusammenspiel mit den in Abschnitt 6.1.3 genannten gesetzlichen Auflagen ist das aktuelle Sicherheitsmanagement, d. h. die *dritte Welle* nach von Solms, eng an Standards und Best Practices, die Zertifizierungsmöglichkeiten bieten, orientiert und nach [vS04] durch die folgenden drei Eigenschaften geprägt:

1. Es wird ein gesamtheitlicher, also in die Breite gehender Ansatz verfolgt. Dies führt – im Unterschied beispielsweise zum oben diskutierten RFC 2196 – dazu, dass die zur praktischen Umsetzung der einzelnen Aspekte notwendigerweise in die Tiefe gehenden Konzepte von den Organisationen selbst erarbeitet werden müssen.

2. Die grundlegende Bedeutung des Risikomanagements wird stark betont und stellt einen Anknüpfungspunkt zu den Geschäfts- und Managementprozessen dar, die sich auch mit nicht für die IT spezifischen Risiken auseinandersetzen.
3. Die Notwendigkeit, die Umsetzung von Richtlinien zu prüfen und geeignet zu erzwingen (engl. *policy monitoring and enforcement*), prägt die technische Umsetzung.

Analog dazu, dass der Standard ISO/IEC 20000-1 als Verfeinerung des Standards ISO 9001 im Kontext des IT Service Management aufgefasst werden kann, stellt ISO/IEC 27001 qualitätssichernde Mindestanforderungen an das Sicherheitsmanagement. Humphreys, einer der Autoren des Standards, erläutert diesbezüglich in [Hum08], dass ISO/IEC 27001 in Organisationen verschiedenster Größe eingesetzt werden kann, und betont wiederholt die Schlüsselrolle des Risikomanagements und der laufenden Überprüfung der Zielerreichung. Er demonstriert in dieser Arbeit jedoch auch, wie der Standard zu einer gezielten Untersuchung interner Bedrohungen, d. h. von den eigenen Mitarbeitern ausgehender Angriffe, maßgeschneidert betrachtet werden kann; eine damit vergleichbare Methodik wird bei der Betrachtung der prozessualen Schnittstellen von Security-Frameworks in Abschnitt 6.5 angewandt.

Obwohl sich die von ISO/IEC 27001 vorgegebene Einteilung des Sicherheitsmanagements in Teilbereiche (vgl. Abschnitt 2.1.2) inzwischen durchgesetzt hat und vergleichbare Ansätze zur Kategorisierung wie [HCCT03] und [Tud01] in sich vereint, wird die Weiterentwicklung der Disziplin in wissenschaftlichen Arbeiten unter anderem durch die folgenden drei Aspekte motiviert:

1. Standards und Best Practices zum Sicherheitsmanagement betonen die organisatorischen Aspekte so stark, dass die technische Umsetzung nicht ausreichend tief behandelt wird. Deshalb muss ein gesamtheitlicher Ansatz, der beide Aspekte ineinander vereint, erst noch erarbeitet werden; die Schwerpunkte aktueller Untersuchungen werden unten zu einer Übersicht zusammengestellt.
2. Es wurde zwar die Notwendigkeit zur Überprüfung der Umsetzung von organisatorischen und technischen Sicherheitsmaßnahmen erkannt, für die praktische Umsetzung stehen bislang jedoch nur sehr einfache technische Werkzeuge zur Verfügung. Dieser Aspekt wird, spezifisch für Security-Frameworks, in Abschnitt 6.6 behandelt.
3. Die Integration des Sicherheitsmanagements in die ITSM- und Geschäftsprozesse verläuft nach wie vor schleppend und muss gezielter methodisch unterstützt werden. Ansätze wie [WM08] und [Kla11] befassen sich dazu beispielsweise mit der Abbildung von Sicherheitszielen in der Modellierung von Geschäftsprozessen. In Abschnitt 6.5 wird auf die Verknüpfung der ITSM- und Sicherheitsmanagementprozesse unter dem Blickwinkel von Security-Frameworks eingegangen.

Aktuelle Arbeiten an einem nach wie vor stark prozessorientierten, aber techniknäheren Sicherheitsmanagement verfolgen unter dem Stichwort einer gesamtheitlichen *Security Architecture* die in Abbildung 6.4 dargestellte Zerlegung des Problembereichs (vgl. [AH08] und [Pet07]):

- Verschiedene Interessenvertreter (z. B. Unternehmensführung, Geschäftspartner und Kunden) geben die Ziele und Randbedingungen vor.
- Grundlage für alle technischen und organisatorischen Maßnahmen bilden aus den vorgegebenen Zielen und Randbedingungen abgeleitete Richtlinien (Policies), die sich an

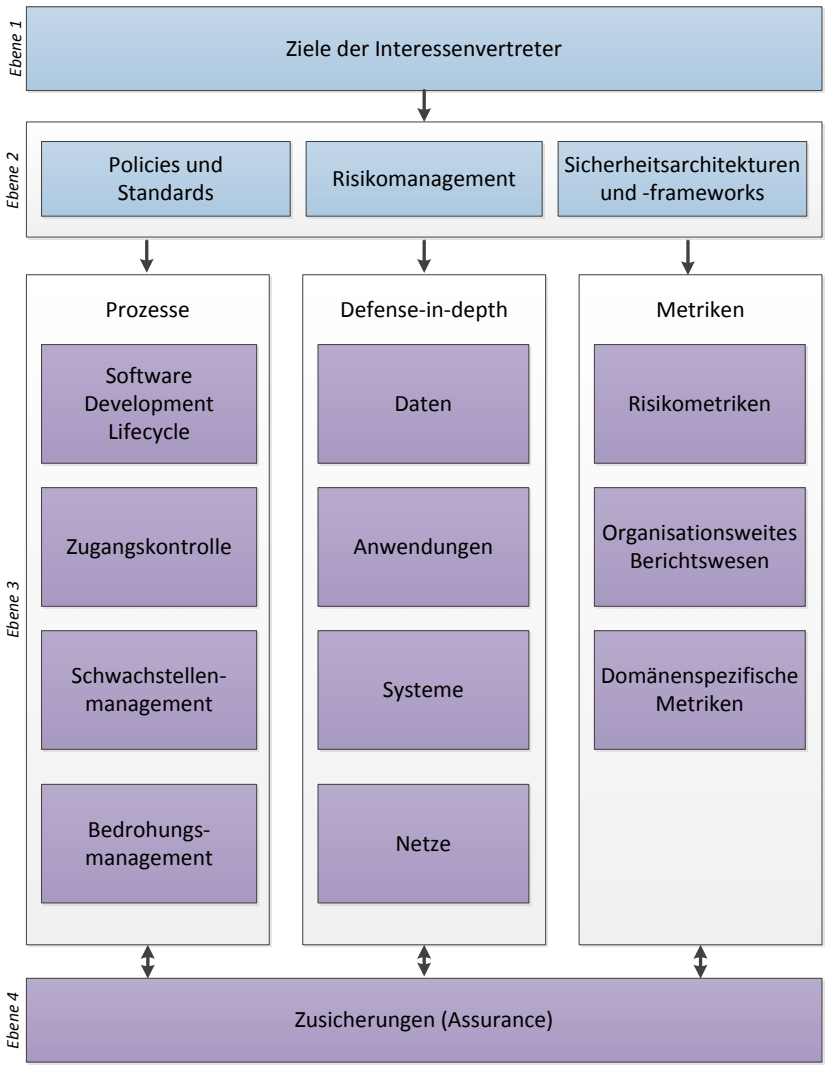


Abbildung 6.4.: Aufgabenbereiche eines techniknahen, aber prozessorientierten Sicherheitsmanagements (orientiert an [Pet07])

verfügbaren Standards zum Sicherheitsmanagement orientieren. Die Priorisierung der Umsetzung erfolgt auf Basis eines Risikomanagements, das nicht nur die reinen IT-Risiken betrachtet. Für die Umsetzung der Policies, Standards und Risikomanagement-entscheidungen wird auf bewährte Frameworks und Architekturen zurückgegriffen, die im Unterschied zur gesamtheitlichen *Security Architecture* als Sicherheitsarchitekturen im engeren Sinn bezeichnet werden.

- Die Umsetzung deckt drei komplementäre Bereiche ab:

  1. **Prozesse**: Die in Unternehmen zu etablierenden Prozesse müssen den gesamten Lebenszyklus der eingesetzten IT-Assets abdecken. Aktuelle Schwerpunkte in der Forschung und Praxis sind derzeit die Entwicklung sicherer Software über einen entsprechenden Software Development Lifecycle (SDL), die mit den Geschäftspro-

zessen gekoppelte Zugriffskontrolle und Verwaltung von Berechtigungen (beispielsweise über Identity Management) sowie das Management von Bedrohungen und Angriffen.

2. **Technik**: In die Tiefe gehende technische Schutzmaßnahmen (engl. *defense-in-depth*) müssen ebenfalls alle relevanten IT-Assets abdecken. Die Untergliederung erfolgt dabei in die vier Teilbereiche Daten, Anwendungen, Systeme und Netze; sie deckt sich mit der historischen Evolution technischer Schutzmaßnahmen und erlaubt deren direkte Zuordnung zu einem oder mehreren der vier Teilbereiche.
3. **Kontrolle**: Mittels Messungen und Kennzahlen kann überwacht werden, wie sich die umgesetzten Maßnahmen auf die identifizierten Risiken und die Geschäftsprozesse auswirken. Für Rückmeldungen an die Interessenvertreter ist ein entsprechendes Berichtswesen erforderlich.

- Als diese Bereiche übergreifende Zielsetzung wird verfolgt, belastbare Aussagen bis hin zu Garantien über die IT-Assets und ihre Sicherheit treffen zu können (engl. *assurance*), so dass die verfolgten Geschäftsziele auch bei akuten IT-Sicherheitsbedrohungen weiterhin erreicht werden können. In dieses Teilgebiet sind beispielsweise proaktive Sicherheitstests einzuordnen, die über Analysen einzelner IT-Assets (beispielsweise durch Penetrationstests einer ausgewählten Anwendung) hinausgehen.

Security-Frameworks lassen sich damit unter Berücksichtigung des prozessorientierten Sicherheitsmanagements, wie es beispielsweise von ISO/IEC 27000 postuliert wird, und der laufenden Weiterentwicklungen zu einem gesamtheitlich technischen und organisatorischen Ansatz wie folgt einordnen:

- Security-Frameworks stellen technische und organisatorische Maßnahmen zusammen und entsprechen von ihrer Zielsetzung her somit genau den in Abbildung 6.4 dargestellten Sicherheitsarchitekturen im engeren Sinn. Somit muss sich ihr Einsatz wie bereits im Kontext der Initiierung von Instanzlebenszyklen in Abschnitt 5.1 diskutiert mit der von übergeordneten Interessenvertretern vorgegebenen Zielsetzung decken; darüber hinaus muss es losgelöst von der technischen Realisierung organisatorische Schnittstellen innerhalb des Sicherheitsmanagements zu den beiden Bereichen *Policies* und *Risikomanagement* geben:
  - Die Einbettung des Security-Frameworks in die Unternehmensumgebung kann nur erfolgreich sein, wenn sowohl die vom Security-Framework vorgesehenen Komponenten den Vorgaben der bereits vorhandenen Richtlinien entsprechen als auch die erforderlichen Änderungen und Ergänzungen, die mit dem Einsatz des Security-Frameworks erforderlich werden, definiert sind. Durch die in der Praxis vorherrschenden engen Zusammenhänge zwischen Richtlinien und Standards bzw. Best Practices müssen auch Security-Frameworks unter dem Aspekt ihres Zusammenspiels mit ebendiesen betrachtet werden. Damit wird jedoch auch die deutliche Abgrenzung vorgenommen, dass es sich bei Security-Frameworks um Beiträge zur *Umsetzung* des Sicherheitsmanagements handelt und nicht um so genannte *Security Management Frameworks*, zu denen die in Abschnitt 6.1.2 behandelten Arbeiten gezählt werden können.
  - Die Security-Frameworks müssen in die vorhandenen Methoden zum Risikomanagement integriert werden können, um damit über die Grenzen der von ihnen

abgedeckten Bereiche hinausgehend eine organisationsweite Priorisierung aller Sicherheitsmaßnahmen zu ermöglichen. Analog zum im Abschnitt 6.3 beschriebenen, für Security-Frameworks spezifisch angepassten Verfahren zum Risikomanagement handelt es sich dabei um Erweiterungen und Modifikationen, aber nicht um einen vollständigen Ersatz der bereits eingesetzten Vorgehensweisen.

- Die Umsetzung von Security-Frameworks muss die drei komplementären Teilbereiche Prozesse, Technik und Kontrolle sowohl in der Breite als auch in der Tiefe möglichst vollständig abdecken:
  - Die Lebenszyklen der Frameworkkonzepte und der von ihnen vorgesehenen technischen Komponenten sind wie in Kapitel 5 erläutert eng an System- bzw. Softwareentwicklungslebenszyklen orientiert, die das Paradigma *security-by-design* umsetzen. Analog dazu umfassen Security-Frameworks per Definition und als treibende Kräfte für die kontinuierliche Weiterentwicklung die Behandlung von Schwachstellen und Bedrohungen. Ebenso weisen Security-Frameworks – wie in Abschnitt 6.5 systematisch behandelt wird – Schnittstellen zu allen Teilprozessen des Sicherheitsmanagements auf, indem sie beispielsweise darin etablierte Vorgehensweise und bereits zur technischen Umsetzung vorhandene Komponenten mit nutzen oder eigene Ergänzungen liefern. Für das in Abbildung 6.4 aufgrund seines Schwerpunktcharakters exemplarisch genannte Zugriffskontrollmanagement bedeutet dies beispielsweise, dass in der Organisation vorhandene Benutzer- und Berechtigungsverwaltungsinfrastrukturen genutzt werden sollten, wohingegen separate, nur auf das Security-Framework zugeschnittene Zugriffskontrollmechanismen zu vermeiden sind.
  - Security-Frameworks müssen bezüglich der von ihnen geschützten Assets und ihrer eigenen Komponenten das Paradigma *defense-in-depth* umsetzen, so dass zumindest bei Schlüsselkomponenten zueinander redundante Sicherheitsmechanismen auf unterschiedlichen Abstraktionsebenen realisiert werden; beispielsweise sollten einzelne Systeme Angriffen nicht schutzlos ausgeliefert sein, selbst wenn die für den Schutz des gesamten Netzes vorgesehenen Maßnahmen von einem Angreifer erfolgreich umgangen worden oder aus anderen Gründen ausgefallen sind. Der modulare Aufbau von Security-Frameworks trägt dazu bei, dass auch auf derselben Betrachtungsebene mehrere einander überlappende und sich im Angriffsfall gegenseitig ergänzende Sicherheitsmechanismen aufgebaut werden können. In Abschnitt 6.2 wird eine Abbildung auf die verschiedenen Bereiche des operativen Sicherheitsmanagements vorgenommen und in Abschnitt 6.4 werden die Auswirkungen auf Managementarchitekturen und -werkzeuge behandelt; die konkrete Auswahl technischer Schutzmechanismen ist Aufgabe des jeweiligen Frameworkkonzepts und wurde in Kapitel 4 für die untersuchten Security-Frameworks jeweils knapp zusammengefasst.
  - Um die Zielerreichung des Security-Frameworks zu überprüfen, müssen spezifische Kennzahlen und ein gegenüber der Überwachung einzelner Sicherheitskomponenten angepasstes Berichtswesen etabliert werden. In Abschnitt 6.6 werden entsprechende Verfahren entwickelt; wie aus der Zusammenfassung der historischen Entwicklung in den vorangegangenen Abschnitten und der Untersuchung aktueller Security-Frameworks in Kapitel 4 hervorgeht, handelt es sich hierbei sowohl im Allgemeinen

als auch bei Security-Frameworks im Speziellen um einen bislang nur unzureichend erschlossenen Bereich.

- Die Forderung nach konkreten, belastbaren Aussagen über ihre Wirksamkeit bis hin zu Garantien über erreichbare Sicherheitsniveaus ist für Security-Frameworks besonders relevant, da sie – wie bei der Diskussion von Szenarien und Anforderungen in Kapitel 3 gezeigt wurde – größere Teile der szenarienspezifischen Erarbeitung von Sicherheitskonzepten ersetzen sollen und somit eine zuverlässige Grundlage bilden müssen. Dieses Ziel kann für ein Security-Framework jedoch nur erreicht werden, wenn entsprechende Aussagen über alle seine dafür relevanten Komponenten getroffen werden können; beim aktuellen Stand der Technik können – beispielsweise durch den in Abschnitt 6.4 beschriebenen Werkzeugeinsatz – nur Annäherungen erreicht werden.

Die erarbeitete Einordnung verdeutlicht, dass Security-Frameworks zwar sehr gut in die sich weiterentwickelnden Sicherheitsmanagementkonzepte integriert werden können, aber eine Vielzahl von Teilaspekten berücksichtigt werden muss, die zur Gesamtkomplexität beiträgt; gegenüber der Betrachtung aller Einzelkomponenten muss deshalb insbesondere der Mehrwert, Security-Frameworks als Einheit betrachten zu können, genutzt werden, um effiziente Managementabläufe zu erreichen.

6.1.2. Standards und Best Practices zum Sicherheitsmanagementprozess

Der beschriebene Wandel des Sicherheitsmanagements vom Technischen ins prozessorientierte Organisatorische und der skizzierte Bedarf, eine möglichst objektive Vergleichbarkeit von Unternehmen im Bezug auf ihre Sicherheit zu erzielen, hat in den letzten rund zehn Jahren dazu geführt, dass von einer Reihe von Standardisierungsgremien, Behörden und Herstellerverbünden Dokumente zum Sicherheitsmanagementprozess erstellt wurden, die den Status von Industriestandards bzw. Best Practices (oder de-facto Standards) erlangt haben. Nachfolgend werden die sieben Werke, die sowohl die Forschung als auch die Industrie aktuell international und branchenübergreifend maßgeblich beeinflussen, vorgestellt, um in Abschnitt 6.1.4 ihre Relevanz für Security-Frameworks skizzieren zu können. Aufgrund des Umfangs jeder der genannten Arbeiten können nur wenige, unmittelbar für dieses Kapitel relevante Aspekte genannt werden. Bedingt durch ihre Grundausrichtung und die zeitlich überlappenden Gremienarbeiten sind die vorgestellten Werke insgesamt nicht redundanzfrei, durch deutlich erkennbare unterschiedliche Schwerpunkte aber als zueinander komplementär einzustufen:

- **ISO/IEC 27001:2005**: Die auch als DIN veröffentlichte internationale Norm ISO/IEC 27001 spezifiziert Minimalanforderungen an Informationssicherheitsmanagementsysteme. Wie bereits in Abschnitt 2.1.2 erwähnt wurde, verbindet sie das Risikomanagement als treibende Kraft mit der Organisation des Sicherheitsmanagements als kontinuierlichem Verbesserungsprozess auf Basis des PDCA-Zyklus und teilt über 130 Sicherheitsmaßnahmen in elf weitere Kategorien ein, die auch als Strukturierungsmittel in Abschnitt 6.5 verwendet werden.

  Für ISO/IEC 27001 werden sowohl Organisations- als auch Personenzertifizierungen angeboten, woraus sich neben dem Charakter als internationaler Standard eine hohe Attraktivität für und somit Verbreitung bei privatwirtschaftlichen Unternehmen ergibt. Die Reihe ISO/IEC 27000 umfasst bislang rund zwei Dutzend weiterer Standards, die

sich zum Teil jedoch noch im Vorschlags- und Entwurfsstadium befinden und somit noch nicht ratifiziert wurden. Hervorzuheben sind der Standard ISO/IEC 27002, bei dem es sich um einen Leitfaden zur Umsetzung von ISO/IEC 27001 handelt, der mit BS 7799-1 denselben Ursprung hat wie das Security Management nach ITILv2, und die geplanten Standards ISO/IEC 27030 bis ISO/IEC 27044, die auf konkrete technische Gebiete wie Netzsicherheit und VPNs eingehen sollen. Darüber hinaus existieren in der Reihe auch Standards mit branchenspezifischen Leitfäden, beispielsweise in den Bereichen Telekommunikation und Gesundheitswesen.

- **CobiT**: Die *Control Objectives for Information and Related Technology* positionieren sich als IT-Governance-Framework, das über das reine Sicherheitsmanagement hinausgehend sicherstellen soll, dass „die Unternehmens-IT dazu beiträgt, die Organisationsstrategie und -ziele zu erreichen und zu erweitern“ [C40DT, S. 21]. CobiT definiert in der aktuellen vierten Auflage insgesamt 34 Teilprozesse, zu deren Spezifikation auch eine Analyse der Auswirkungen auf die sieben *CobiT information criteria – effectiveness, efficiency, confidentiality, integrity, availability, compliance* und *reliability* – gehört. Dadurch, dass die drei IT-Sicherheitsgrundziele Vertraulichkeit, Integrität und Verfügbarkeit (vgl. Abschnitt 2.1.1.1) unmittelbar berücksichtigt werden, kann eine Abbildung der Organisations- und Prozessziele auf technische Sicherheitsmechanismen vorgenommen werden.

  Analog zu ISO/IEC 27001 sind das Risikomanagement und die Ausgestaltung als kontinuierlicher Verbesserungsprozess zwei der Schwerpunkte des CobiT-Frameworks. CobiT geht darüber hinaus jedoch unter dem Stichwort *performance measurement* auch auf das Messen der Zielerreichung der vorgeschlagenen Teilprozesse ein, indem es für jeden Teilprozess und darin ausgewählte Aktivitäten einige Metriken vorgibt, aus denen sich ableiten lässt, welche Teile der CobiT-Umsetzung in einer Organisation noch weiter verbessert werden können. Auf dieser Basis kann auch eine Einordnung in das CobiT-Reifegradmodell vorgenommen werden, das für jeden Teilprozess die Stufen 0 (Prozess wird nicht umgesetzt) bis 5 (optimierter, dokumentierter, im Unternehmen gelebter Prozess) umfasst. Neben der Frameworkdokumentation existieren über 20 weitere CobiT-Dokumente, die auf speziellere Aspekte wie die Anforderungen durch gesetzliche Auflagen (vgl. Abschnitt 6.1.3) eingehen. Die Information Systems Audit and Control Association (ISACA) bietet eine CobiT-Personenzertifizierung an; eine Zertifizierung von Organisationen nach CobiT ist derzeit nicht möglich.

- **BSI-Grundschutzkataloge**: Die Grundschutzkataloge vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) sind die derzeit umfangreichste strukturierte Zusammenstellung von IT-spezifischen Bedrohungen und Maßnahmen; ihr über 4.000 Seiten starker Umfang und die Verfügbarkeit ausgewählter Dokumente in englischer Übersetzung tragen zur internationalen Bedeutung in Forschung und Praxis maßgeblich bei. Die Bezeichnung als *Grundschutz* geht darauf zurück, dass auf Basis der empirischen 80-20-Regel Maßnahmen für die 80% der Systeme mit einer „üblichen“ Gefährdungslage empfohlen werden, wohingegen für die verbleibenden 20% der Systeme, die einen erhöhten Schutzbedarf aufweisen, mit dem BSI-Standard 100-3 [BSI08b] ein ergänzendes Dokument zur Risikoanalyse bereitgestellt wird.

  Die BSI-Grundschutzkataloge sind erheblich konkreter und techniklastiger ausgeprägt als die anderen hier betrachteten Werke; beispielsweise wird auf Sicherheitsmaßnahmen

für konkrete Protokolle und ausgewählte Softwareprodukte eingegangen. Trotz ausgewählter Querverweise zwischen den Spezifikationen der einzelnen Maßnahmen handelt es sich jedoch um punktuelle Lösungen, deren mögliche Zusammenstellung zu einem Gesamtkonzept (im Unterschied zu Security-Frameworks) der jeweiligen Organisation überlassen bleibt. Die Einordnung der Maßnahmen erfolgt in die Kategorien *Infrastruktur*, *Organisation*, *Personal*, *Hardware und Software*, *Kommunikation* und *Notfallvorsorge*.

Mit dem BSI-Standard 100-1 [BSI08a] stellt das BSI darüber hinaus eine zu ISO/IEC 27001 kompatible Spezifikation von Managementsystemen für Informationssicherheit zur Verfügung, auf deren Basis eine Zertifizierung von Organisationen nach BSI-Grundschutz angeboten wird, die eine ISO/IEC 27001-Zertifizierung beinhaltet. Ein weiteres Alleinstellungsmerkmal besteht in der Werkzeugunterstützung durch das so genannte *GSTOOL*, das die Erstellung von organisationsspezifischen IT-Sicherheitskonzepten unter Orientierung an den Grundschutzkatalogen ermöglicht und vom BSI kommerziell vertrieben wird.

- **NIST Handbooks**: Das US-amerikanische National Institute of Standards and Technology stellt im Rahmen seiner Publikationsreihe *Special Publications SP 800-x* zahlreiche Handbücher zu technischen und organisatorischen Aspekten der IT-Sicherheit bereit, die eine in den USA mit den BSI-Standards vergleichbare Stellung und internationale Anerkennung erlangt haben.

  Neben dem prozessorientierten Vorgehen, das in SP 800-12 [SP8H12] und SP 800-14 [SP8H14] spezifiziert wird und eine mit ISO/IEC 27001 vergleichbare Untergliederung vornimmt, kommt insbesondere SP 800-30 [SP8H30] eine Schlüsselrolle zu: Der darin beschriebene Risikomanagementprozess fungiert als Referenz und Messlatte für alle modernen Ansätze zum IT-Risikomanagement (vgl. Abschnitt 6.3). Die seit der Veröffentlichung von ISO/IEC 27001 erschienenen Dokumente der Reihe SP 800-x nehmen darauf Bezug und vertiefen ausgewählte technische Aspekte, beispielsweise zur Sicherheit der Servervirtualisierung und zu IT-forensischen Maßnahmen. Eine Zertifizierung ist für einzelne Systeme möglich, die in den USA den Status eines *Federal Information Systems* haben.

- **ISF Standard of Good Practice**: Der Standard of Good Practice (SoGP) des Information Security Forums (ISF) ist eine seit 1996 alle zwei bis drei Jahre aktualisierte Sammlung von Best Practices, in die sowohl aktuelle Forschungsergebnisse als auch praktische Erfahrungen der ISF-Mitgliedsorganisationen einfließen. Der SoGP besteht aus den sechs großen Kategorien *Enterprise-wide Security Management*, *Critical Business Applications*, *Computer Installations*, *Networks*, *Systems Development* und *End User Environment*. Diese Kategorien sind in insgesamt 36 Teilbereiche (engl. *areas*) und weiter in über 160 Abschnitte (engl. *sections*) untergliedert.

  Der Bereich Security Management besteht aus sieben Teilbereichen und 36 Abschnitten, in denen sowohl organisatorische (z. B. Engagement der Unternehmensführung), prozedurale (z. B. dokumentierter Softwareaktualisierungsprozess) als auch technische (z. B. Intrusion Detection Systeme) Anforderungen gestellt werden. Diese können sowohl bezüglich ihrer Auswahl als auch im Hinblick auf den Abstraktionsgrad und die Knappheit der Darstellung als Teilmenge der in ISO/IEC 27001 aufgeführten Maßnahmen angesehen werden. Ein konkreter Mehrwert ergibt sich jedoch aus der im SoGP enthaltenen

so genannten Themenmatrix, die für über 80 Schlagwörter wie beispielsweise *Information Security Incident Handling* aufzeigt, welche der sechs großen Kategorien von dem jeweiligen Thema mit welchen Teilbereichen und Abschnitten betroffen sind; somit können die ausgewählten Zusammenhänge über das Sicherheitsmanagement hinausgehend einfach erkannt und berücksichtigt werden. Eine Zertifizierung nach SoGP ist nicht möglich; das ISF bietet seinen Mitgliedern jedoch alle zwei Jahre eine als Benchmark bezeichnete Überprüfung an, die der Identifikation von Schwächen und dem anonymen Vergleich mit den anderen Mitgliedern dient.

- **Information Security Management Maturity Model**: Das von einem aus international tätigen IT-Sicherheitsberatungsunternehmen bestehenden Konsortium herausgegebene Information Security Management Maturity Model (ISM3) zielt auf die Übertragung der in ISO 9001 verankerten Qualitätsmanagementprinzipien auf das Sicherheitsmanagement ab; anders als ISO/IEC 27001 befasst es sich hierzu jedoch ausschließlich mit Teilprozessen und nicht mit Maßnahmen. Analog zu CobiT enthält ISM3 ein Reifegradmodell, das auch die Basis für die Zertifizierung von Organisationen darstellt, für seine Prozesse, die sich darüber hinaus durch eine sehr strukturierte Dokumentation auszeichnen: Jeder Prozess wird einheitlich tabellarisch beschrieben, wobei beispielsweise auch präzise Verantwortlichkeiten und abzuliefernde Berichte spezifiziert werden.

  Das Sicherheitsmanagement nach ISM3 basiert zum einen auf Risikomanagement und teilt die weiteren Prozesse in die drei Kategorien *Strategic*, *Tactical* und *Operational Management* ein. Unter dem strategischen Bereich werden dabei die Gesamtkoordination des Sicherheitsmanagements und das Berichtswesen an die übergeordneten Interessenvertreter verstanden; der taktische Bereich von ISM3 umfasst weitere organisatorische Aspekte wie die Erstellung von Richtlinien und Schulungsmaßnahmen für Mitarbeiter. Das mit 25 einzelnen Prozessen am umfangreichsten beschriebene *Operational Management* befasst sich mit stärker technisch orientierten Aspekten wie der Erstellung von Datensicherungen, dem Einspielen von Software-Updates und der Benutzerverwaltung.

- **IT Infrastructure Library**: Die IT Infrastructure Library (ITIL) ist eine der einflussreichsten Best Practice Sammlungen zum IT Service Management, die am gesamten Lebenszyklus von IT-Diensten orientiert auf relativ hohem Abstraktionsniveau eine umfassende Menge von ITSM-Referenzprozessen spezifiziert.

  ITIL enthielt in Version 2 eine separate Publikation zum Thema *Security Management*, die sich inhaltlich eng an BS 7799-1 orientierte und wie oben erläutert aufgrund dieses gemeinsamen Ursprungs starke Parallelen zu ISO/IEC 27002 aufwies. Mit ITIL v3 erfolgte eine noch stärkere Strukturierung anhand des IT-Service-Lebenszyklus und damit auch eine Aufteilung des Bereichs Sicherheitsmanagement in einen konzeptionellen und einen operativen Bestandteil: Das *Information Security Management* ist nunmehr Bestandteil der ITIL v3-Bücher zur Lebenszyklusphase *Service Design*, wodurch die gegebene Notwendigkeit der Berücksichtigung von Sicherheitsaspekten von Anfang an betont wird, und wird vom *Access Management* in den Spezifikationen zur Lebenszyklusphase *Service Operations* ergänzt.

  Aufgrund der nach wie vor engen Verwandtschaft mit ISO/IEC 27002 ergibt sich bei einer reinen Betrachtung des Sicherheitsmanagements kein Vorteil von ITIL gegenüber der ISO/IEC 27000-Normenreihe. Da ITIL das Sicherheitsmanagement jedoch als Querschnittsfunktion, die Schnittstellen zu allen anderen ITSM-Prozessen aufweist, auffasst,

ergibt sich der potentielle Mehrwert einer Darstellung der Zusammenhänge zwischen dem Sicherheitsmanagement und den weiteren ITSM-Prozessen. Diese Erwartung wird jedoch sowohl von ITILv2 als auch von ITIL v3 nur sehr eingeschränkt erfüllt, da nach wie vor deutlich erkennbar ist, dass die einzelnen ITIL-Publikationen parallel von verschiedenen Autoren erstellt wurden und viele konzeptionell und praktisch relevante Querverbindungen nicht explizit erwähnt werden (vgl. [Bre07]).

In der Praxis ergibt sich daraus das weit verbreitete Vorgehen, das Sicherheitsmanagement zwar bezüglich seiner Organisation und Dokumentation analog zu den anderen ITSM-Prozessen zu gestalten, inhaltlich und als Ausgangsbasis für die technische Umsetzung jedoch auf die anderen hier vorgestellten Arbeiten zurückzugreifen. ITIL sieht lediglich eine Personenzertifizierung vor; für Organisationen, die ITIL umsetzen, stellt die Zertifizierung nach der mit ITILv2 inhaltlich eng verwandten Norm ISO/IEC 20000 [I20k1] eine Option dar.

Bei diesen Standards und Best Practices handelt es sich jedoch nicht um unmittelbar praktisch umsetzbare Anleitungen zum Sicherheitsmanagement. Kritische Untersuchungen wie [SW09] kommen zum Schluss, dass einerseits der Anspruch dieser Werke, für ein möglichst breites Spektrum an Organisationen geeignet zu sein, nachweislich dazu führt, dass für verschiedene Größen von Unternehmen bzw. für unterschiedliche Branchen relevante Aspekte nicht behandelt werden. Andererseits werden viele der vorgeschlagenen Maßnahmen lediglich durch die Behauptung, sie seien allgemein üblich, als Best Practice positioniert, ohne dass hierfür Belege oder Alternativen aufgeführt werden. Die vorgestellten Werke sind deshalb als strukturierte Materialsammlungen und als Grundlage für eigene Sicherheitsmanagementkonzepte und die Planung ihrer Umsetzung geeignet; sie erfordern dabei aber erhebliche szenarienspezifische Anpassungen und Erweiterungen.

6.1.3. IT-Compliance: Gesetzliche und branchenspezifische Auflagen zum Sicherheitsmanagement

Durch die starke Abhängigkeit der Geschäftsprozesse vieler Unternehmen von der IT kann ein unzureichendes Sicherheitsmanagement zu erheblichen finanziellen Schäden führen, die sich mittelbar negativ auf die Interessen beispielsweise von Gläubigern, Aktionären, Beschäftigten und Kunden auswirken können. Aus diesem Grund entstanden in vielen Ländern gesetzliche Auflagen, die durch multinational tätige Unternehmen weltweite Relevanz erhalten haben. Sie haben insbesondere dazu geführt, dass zumindest ausgewählte Bereiche des Sicherheitsmanagements nicht mehr nur unternehmens- oder IT-abteilungsintern, sondern auch von außen motiviert werden und durch Haftungsauflagen auch im Eigeninteresse der Unternehmensführung liegen. Die im Folgenden aufgeführten Stichpunkte vermitteln einen groben Überblick über die aus der Perspektive deutscher Unternehmen relevanten Randbedingungen, die auch beim Management von Security-Frameworks berücksichtigt werden müssen:

- **EU-Datenschutzrichtlinie**: Die EU-Datenschutzrichtlinie 95/46/EG, die mit der Novellierung des Bundesdatenschutzgesetzes (BDSG) 2001 in Deutschland umgesetzt wurde und durch weitere Gesetze wie beispielsweise das Teledienstedatenschutzgesetz (TDDSG) verfeinert wird, betont die Notwendigkeit der Entwicklung und Umsetzung von Sicherheitskonzepten in Unternehmen. In Art. 17 Abs. 1 der Richtlinie werden

sowohl technische als auch organisatorische Maßnahmen postuliert, um die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten sicherzustellen.

- **GDPdU**: Die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) sind eine Verwaltungsanweisung, die die Aufbewahrung digitaler Unterlagen und die Mitwirkungspflicht bei Betriebsprüfungen regelt. Sie involviert den Umgang mit qualifiziert elektronisch signierten Dokumenten, deren Integrität geprüft und bewahrt werden muss. Bei Betriebsprüfungen muss dem Prüfer u. a. ein Lesezugriff auf die Daten gewährt werden. Die Umsetzung der GDPdU wirkt sich damit direkt auf zahlreiche organisatorische und technische Aspekte der IT-Sicherheit aus, beispielsweise die Nutzung von PKIs, die revisionssichere E-Mail-Archivierung und das Zugriffskontrollmanagement.
- **Basel II**: Die vom Basler Ausschuss für Bankenaufsicht festgelegten Eigenkapitalvorschriften, die unter der Bezeichnung Basel II bekannt sind und als Banken- und Kapitaladäquanzrichtlinie in deutsches Recht umgesetzt wurden, regeln Kreditentscheidungen auf Basis einer individuellen Bonitätseinschätzung. Bei der Beantragung von Krediten durch Unternehmen spielen deshalb neben Markt- und Kreditrisiken im Bankensektor auch operationelle Risiken des Kreditnehmers eine Rolle. Hierzu gehören explizit auch Risiken aus dem Einsatz von IT in den Unternehmensprozessen, so dass insbesondere ein aktives IT-Risikomanagement gefordert wird, das sich mit der IT-Sicherheit des Unternehmens befasst.
- **KonTraG**: Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) verpflichtet den Vorstand einer Aktiengesellschaft bzw. die Geschäftsführung einer GmbH zur Durchführung einer Risikoanalyse und zur Etablierung eines Sicherheitskonzepts inklusive eines Risikomanagements (§91 Abs. 2 AktG); die Gesetzesbegründung geht dabei auch auf die Notwendigkeit interner Überwachungs- und Frühwarnsysteme ein.
- **Sarbanes-Oxley Act**: Der US-amerikanische Sarbanes-Oxley Act (SOX), der inzwischen inoffiziell als EuroSOX und J-SOX bezeichnete europäische und japanische Äquivalente hat, ist eine verschärfte Regelung zur Finanzberichterstattung insbesondere von börsennotierten Unternehmen. Sie sieht vor, dass sowohl die Geschäftsleitung als auch unabhängige Wirtschaftsprüfer die Wirksamkeit des internen Kontrollsystems für die Rechnungslegung beurteilen. Da die Finanzberichterstattung nicht nur selbst mit IT-Systemen realisiert wird, sondern inhaltlich von einer Vielzahl weiterer IT-Systeme abhängt, deren Manipulation zu gefälschten Bilanzen führen kann, motiviert SOX ein Sicherheitsmanagement, das insbesondere unternehmensinterne Angreifermodelle berücksichtigt.

Ähnlich wirken sich gesetzliche, branchenspezifisch orientierte Regelungen in den USA aus: Der Federal Information Security Management Act (FISMA) schreibt Bundesbehörden u. a. die Einführung eines regelmäßig durchgeführten Risikomanagements, von Sicherheitsrichtlinien, IT-Sicherheitsschulungen für Mitarbeiter, technischen Sicherheitskonzepten sowie entsprechender Überprüfungen und Berichte vor; der Family Educational Rights and Privacy Act (FERPA) regelt den Datenschutz an Schulen, Hochschulen und anderen Ausbildungseinrichtungen; im Gesundheitswesen ist dies Bestandteil des Health Insurance Portability and Accountability Act (HIPAA); für die Finanzbranche spielt der Gramm-Leach-Bliley Act (GLBA) eine mit Basel II in Europa vergleichbare Rolle.

Als praktische Auswirkung auch außerhalb der USA ergibt sich, dass viele Hersteller von IT-Sicherheitslösungen direkten Bezug auf die amerikanische Gesetzgebung nehmen, ihre Produkte bislang aber nur relativ selten an europäische bzw. deutsche Gesetze anpassen. Es bleibt somit eine szenarienspezifische Aufgabe, zu überprüfen, ob die eingesetzten Produkte die jeweils relevanten gesetzlichen Anforderungen erfüllen bzw. zu ihrer Einhaltung beitragen.

Neben Gesetzen existieren branchenspezifische Auflagen, die sich meist dadurch auszeichnen, dass sie erheblich konkreter auf geforderte technische Sicherheitsmechanismen eingehen als Gesetzestexte und -erläuterungen. Ein Beispiel hierfür ist der Payment Card Industry Data Security Standard (PCI DSS); er ist für alle Organisationen verbindlich, die Kunden beispielsweise über Verkaufsstellen oder das Internet die Bezahlung per Kreditkarte ermöglichen wollen, und somit für Supermärkte ebenso relevant wie für E-Commerce-Webseiten. Der PCI DSS schreibt u. a. die Verwendung von Firewalls und Anti-Virus-Software, die Mindeststärke der Verschlüsselung z. B. beim Einsatz von WLAN, tägliche Logfile-Auswertungen und die Ausarbeitung einer Sicherheitsleitlinie sowie eines Reaktionsplans für Sicherheitsvorfälle verpflichtend vor. Die regelmäßigen Aktualisierungen des PCI DSS müssen von den Organisationen jeweils bis zu einem Stichtag umgesetzt werden, andernfalls drohen der Entzug der Möglichkeit zur Kreditkartenabrechnung und eine Vertragsstrafe.

Obwohl sich die Gesamtheit dieser Vorgaben positiv auf das IT-Sicherheitsbewusstsein der im Allgemeinen nicht IT-affinen Unternehmensführungen auswirkt, ergeben sich daraus nicht immer Verbesserungen für die von den Unternehmen erreichten Sicherheitsniveaus: Die ursprünglich intendierte Zielsetzung einer Erhöhung der IT-Sicherheit weicht in der Praxis verstärkt dem rein formalen Einhalten der Richtlinien, das bei Audits mit Hilfe von Checklisten überprüft wird. Nach [Hul08] wird sogar häufig das für IT-Sicherheitsmaßnahmen vorgesehene Budget umgewidmet, um formale Compliance-Anforderungen umzusetzen, so dass sich die de facto erzielte IT-Sicherheit sogar verschlechtert, da entsprechende Mittel zur Verbesserung fehlen.

6.1.4. Konsequenzen für die Konzeption des Managements von Security-Frameworks

Der praktische Einsatz von Security-Frameworks in Unternehmen erfolgt wie in diesem Kapitel einleitend dargestellt nicht unter ausschließlich technischen Gesichtspunkten, sondern setzt die Einbettung der Sicherheitsmechanismen in das zunehmend prozessorientierte und organisatorische Abläufe behandelnde Sicherheitsmanagement voraus.

In Abschnitt 6.1.1.3 wurde gezeigt, dass sich Security-Frameworks nahtlos in moderne Sicherheitsarchitekturen einfügen, sofern sie die drei Teilbereiche *Prozesse*, *Technik* und *Kontrolle* adäquat abdecken. Die Unternehmen stehen über diese grundlegende Orientierung des Sicherheitsmanagements hinausgehend jedoch auch unter dem direkten Einfluss von Standards und Best Practices; sie müssen zudem die Einhaltung gesetzlicher und branchenspezifischer Auflagen sicherstellen. Security-Frameworks müssen sich der Gesamtheit dieser Vorgaben einerseits unterordnen, tragen durch ihre technische Ausprägung andererseits aber maßgeblich zu deren Umsetzung bei.

Für die weiteren Betrachtungen in dieser Arbeit werden die folgenden Konsequenzen gezogen:

- Die Diskussion des Prozesses Sicherheitsmanagement, seiner Bestandteile und der Schnittstellen zu Security-Frameworks erfolgt am Beispiel von ISO/IEC 27001: Wie

in Abschnitt 6.1.2 dargestellt wurde, nehmen alle anderen Standards und Best Practices Bezug darauf, wodurch auch die praktische Dominanz dieser Norm zum Ausdruck kommt. Darüber hinaus wurde ISO/IEC 27001 für den Einsatz in Organisationen verschiedenster Größenordnungen konzipiert, woraus sich eine für die Betrachtung verschiedenster Security-Frameworks ausreichende Skalierbarkeit ergibt.

- Auf gesetzliche und branchenspezifische Auflagen wird nicht im Einzelnen eingegangen; die wiederholt auftretenden Schwerpunkte Risikomanagement, Datenschutz und Berichtswesen sowie das Zusammenspiel mit unternehmensinternen Policies werden im Kontext von Security-Frameworks jedoch vertieft.

Der zwischen Referenzprozessen für das Sicherheitsmanagement und den meisten, stärker technisch orientierten Security-Frameworks bestehende Unterschied im Abstraktionsgrad erschwert die unmittelbare Umsetzung des Sicherheitsmanagements für Security-Frameworks. Aus diesem Grund werden im nächsten Abschnitt als Zwischenschritt die für Security-Frameworks relevanten Aspekte des operativen Sicherheitsmanagements beleuchtet.

6.2. Security-Frameworks im operativen IT-Sicherheitsmanagement

Während in Abschnitt 2.4 häufig im Kontext von Security-Frameworks betrachtete Angriffe und einzelne Sicherheitsmechanismen behandelt wurden, wird im Folgenden auf die Aufgabenbereiche des operativen Sicherheitsmanagements eingegangen. Für jeden Aufgabenbereich werden dabei die allgemein vorzusehenden Schnittstellen zu Security-Frameworks erarbeitet. Dabei liegt allerdings wiederum die Schwierigkeit vor, dass eine einheitliche, anerkannte Definition des *operativen Sicherheitsmanagements* ebenso fehlt wie eine Taxonomie seiner Teilbereiche und Aufgaben. Einleitend werden deshalb die für diese Arbeit vorgenommene Begriffsdefinition und die Vorgehensweise vorgestellt, die zur Ermittlung der zu betrachtenden operativen Aufgaben und ihrer Einordnung in sieben Themenbereiche angewandt wurde.

Hyland und Sandhu definieren das operative Sicherheitsmanagement im Kontext der Netzsicherheit in [HS98] als *„real-time monitoring and control of active security applications that implement one or more security services“*. Für die vorliegende Arbeit wird davon abgeleitet die folgende allgemeinere Auffassung verwendet:

Definition 15 (Operatives IT-Sicherheitsmanagement)

Das operative IT-Sicherheitsmanagement umfasst alle beim Betrieb von IT-Systemen, IT-Diensten und IT-Infrastrukturen systemadministrativ durchgeführten Tätigkeiten, die der technischen Steuerung und Kontrolle IT-sicherheitsrelevanter Eigenschaften und Funktionen dienen.

Diese Definition charakterisiert das operative Sicherheitsmanagement zum einen als *systemadministrative* Tätigkeit, wodurch sie sich von der reinen Nutzung der Sicherheitsfunktionalität durch Anwender abhebt; zum anderen schränkt sie auf *technische* Maßnahmen im *Betrieb* ein, um gegenüber den organisatorisch-konzeptionellen Arbeiten bei der Gestaltung

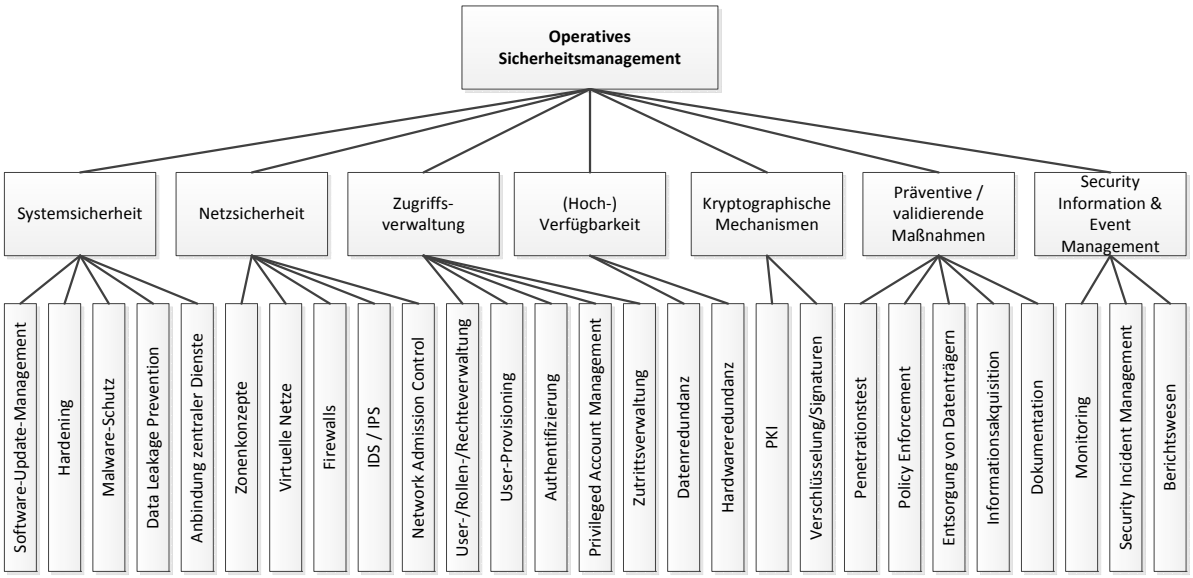


Abbildung 6.5.: Aufgabenbereiche im operativen Sicherheitsmanagement

des Sicherheitsmanagementprozesses zu differenzieren. Hinsichtlich der Zuständigkeiten werden jedoch keine Einschränkungen gemacht; im Allgemeinen kann davon ausgegangen werden, dass sowohl Systemadministratoren bzw. Dienstverantwortliche als auch dediziertes IT-Sicherheitspersonal mit Aufgaben des operativen Sicherheitsmanagements betraut werden; ebenso bleiben Delegationskonzepte uneingeschränkt möglich.

Um Zuordnungen sowohl zu den Prozessabläufen im Sicherheitsmanagement als auch zu den sicherheitsfunktionalen Bestandteilen von Security-Frameworks vornehmen zu können, ist eine detailliertere Betrachtung der Teilbereiche und Aufgaben im operativen Sicherheitsmanagement erforderlich. Die folgende Zusammenstellung wurde auf Basis einer Literaturrecherche erstellt; die inhaltlichen Schwerpunkte orientieren sich an [Ush03], [MB06] und [KK08]. Sie erstreckt sich von den klassischen Bereichen System- und Netzsicherheit ausgehend über die auch wissenschaftlich fundiert aufbereiteten Bereiche der Zugriffsverwaltung und der Anwendung kryptographischer Hilfsmittel hin zu weiteren operativen Aufgaben zum präventiven, detektierenden und reagierenden Handhaben von sicherheitsrelevanten Ereignissen. Dementsprechend kann das operative Sicherheitsmanagement derzeit wie in Abbildung 6.5 dargestellt unter Berücksichtigung des Einsatzes von Security-Frameworks untergliedert werden:

- **Systemsicherheit**: Der Bereich Systemsicherheit befasst sich mit technischen Maßnahmen zum Schutz einzelner Komponenten wie Servern oder mobilen Arbeitsplätzen; eine zentrale Herausforderung besteht in der Skalierbarkeit, da die entsprechenden Maßnahmen in größeren Unternehmen auf einer Vielzahl von Komponenten und ggf. mit individuellen Parametern durchgeführt werden müssen. Folgende Aufgabenbereiche können unterschieden werden:
  - Software-Update- bzw. Patch-Management: Das Einspielen der Aktualisierungen von Betriebssystembestandteilen und Anwendungen zur Behebung bekannt gewordener Sicherheitslücken hat sich in den letzten 15 Jahren als essentielle Sicher-

heitsmaßnahme etabliert. Sie wird u. a. durch vorab notwendige Kompatibilitätsprüfungen, mögliche Ausfallzeiten während der Aktualisierung und die z. B. durch Hardwaredefekte bedingte temporäre Nichtverfügbarkeit zu behandelnder Komponenten erschwert.

- Sicherheitsoptimierende Konfiguration (engl. *Hardening*): Nach der Installation von Betriebssystemen und Anwendungen muss deren Konfiguration geprüft und angepasst werden, um die Komponente gegenüber Angriffen zu schützen. Weit verbreitete Maßnahmen sind beispielsweise das Deaktivieren nicht benötigter Softwaremodule, die Verfeinerung der lokalen Zugriffskontrollkonfiguration gegenüber dem Auslieferungszustand und die Nutzung eines lokal installierten Firewalls.
- Schutz vor Malware: Hierzu gehören beispielsweise die Inbetriebnahme und Pflege von Anti-Virus-Software auf Clients und Servern sowie die Nutzung von hostbasierten Intrusion Detection Systemen.
- Data Leakage Prevention (DLP): Als Schutz gegenüber internen Angreifern, die Daten unerlaubt auf eigene Speichermedien kopieren oder z. B. über das Internet an Dritte weiterzugeben versuchen, werden zusätzliche Softwarewerkzeuge in Betrieb genommen, die beispielsweise die Nutzung von USB-Memorysticks an Arbeitsplatz-PCs verhindern.
- Anbindung an sicherheitsrelevante zentrale Netzdienste: Weitere Maßnahmen im Bereich der Systemsicherheit umfassen beispielsweise die Integration in Backup-Konzepte, die Aufnahme des Systems in Monitoringlösungen, den Anschluss an zentrale Logfile-Server und die Einbindung in unternehmensweite Zugriffskontrollkonzepte; dabei handelt es sich um die Schnittstellen der im Kontext der Systemsicherheit betrachteten Einzelsysteme zu den Sicherheitsdiensten in den anderen Bereichen des operativen Sicherheitsmanagements.

Für das Management eines Security-Frameworks ist folglich zu klären, ob es selbst aus mehreren Einzelkomponenten besteht bzw. ob es eigene Beiträge zu Systemsicherheitsmaßnahmen liefert. Alle Komponenten des Security-Frameworks, die selbst keine Maßnahmen zur Sicherheit einzelner Systeme darstellen, müssen analog zu anderen im Unternehmen eingesetzten Komponenten den Maßnahmen aus den vorhandenen Systemsicherheitskonzepten unterzogen werden. Die Sicherheitsfunktionalität der übrigen Komponenten des Security-Frameworks kann hingegen direkt einem oder mehreren der anderen Aufgabenbereiche zugeordnet werden.

- **Netzsicherheit**: Der Anschluss von Servern und Arbeitsplatzrechnern ans Unternehmensnetz mit Zugängen von und zu VPNs bzw. Internet ist inzwischen in den meisten Organisationen zum Normalfall geworden. Neben somit möglicherweise über das Netz auch von externen Dritten ausgehenden Angriffen muss sich der Bereich Netzsicherheit verstärkt mit dem Umgang mit privaten mobilen Endgeräten, beispielsweise von Mitarbeitern an den Arbeitsplatz mitgebrachte Smartphones, auseinandersetzen. Das operative Sicherheitsmanagement umfasst in diesem Bereich die folgenden Teilaufgaben:
  - Umsetzen von Zonenkonzepten: Durch die Zuweisung von Endgeräten in verschiedene Zonen können unterschiedliche Sicherheitsklassen, beispielsweise für weltweit

erreichbare Server, unternehmensinterne Server, Mitarbeiterarbeitsplätze, WLAN-Netze und Laborbereiche, realisiert werden.

- Virtuelle Netze: Durch die Virtualisierung von Netzen auf verschiedenen Ebenen des ISO/OSI-Modells können, beispielsweise durch den Einsatz von VLANs oder IPsec-VPNs, weiterführende Maßnahmen sowohl zur Isolation von Gruppen von Systemen als auch zur sicheren standortübergreifenden Kopplung physischer Netze getroffen werden.
- Firewalls: An Zonenübergängen können beispielsweise Paketfilter-Firewalls und Application Level Gateways eingesetzt werden, um den Aufbau unerwünschter Verbindungen zu verhindern. Die umgesetzten Regelsätze sind häufig asymmetrisch, so dass Arbeitsplatz-PCs beispielsweise Verbindungen zu Servern über das Internet aufbauen können, selbst aber nicht direkt über das Internet erreichbar sind.
- Intrusion Detection/Prevention Systeme: Die IDS-/IPS-Systeme dienen wie in Abschnitt 2.4.2 beschrieben der Erkennung und automatischen Reaktion auf netzbasierte Angriffe; im Betrieb ist dies mit einer laufenden Pflege und Aktualisierung der Regelsätze für die Erkennungsmechanismen verbunden (vgl. [MHR11]).
- Network Admission Control (NAC): NAC ist das Bindeglied zwischen der oben beschriebenen Systemsicherheit und der unten erläuterten Zugriffskontrolle. Über NAC wird sichergestellt, dass keine unerwünschten Endgeräte ans lokale Netz angeschlossen werden. Dazu findet zunächst eine Authentisierung des Endgeräts und ggf. seines aktuellen Benutzers statt; über auf dem Endgerät installierte Softwareagenten kann die Zulassung zur Netznutzung darüber hinaus von den aktuellen Systemsicherheitseigenschaften des Endgeräts abhängig gemacht werden: Falls beispielsweise Betriebssystem-Updates noch nicht eingespielt wurden, wird das Endgerät einem Quarantänenetz zugeordnet, aus dem heraus nur auf Software-Update-Dienste zugegriffen werden kann.

Für jede Netzsicherheitskomponente muss darüber hinaus ihre Systemsicherheit betrachtet werden. Bezüglich des Managements von Security-Frameworks ist analog zum Bereich Systemsicherheit zu überprüfen, welche Auswirkungen sich beispielsweise aus der Positionierung von Frameworkkomponenten in verschiedenen Netzzonen ergeben bzw. zu welchen Aufgabenbereichen das Security-Framework eigene Beiträge liefert. In Kapitel 4 wurde gezeigt, dass sich relative viele Security-Frameworks mit Maßnahmen für die Netzsicherheit beispielsweise ganzer Unternehmensnetze oder einzelner WLANs befassen. Demgegenüber unterstützen nur wenige Security-Frameworks die Anwendung von Netzsicherheitskomponenten zu ihrem eigenen Schutz methodisch; im Allgemeinen verhalten sie sich wie andere Systeme weitgehend agnostisch gegenüber entsprechenden frameworkexternen Maßnahmen.

- **Zugriffsverwaltung**: Der Bereich Access Management setzt die durch Policies festgelegten Authentifizierungs- und Autorisierungskonzepte unternehmensweit, d. h. dienst- und systemübergreifend, um. Durch auf Identity & Access Management spezialisierte Anbieter sind zwar häufig Komplettlösungen für diesen Bereich im Einsatz, es kann jedoch die folgende Untergliederung vorgenommen werden:
  - Benutzer-, Rollen- und Berechtigungsverwaltung: Alle zur Nutzung von IT-Diensten berechtigten Benutzer werden in der Regel zentral erfasst; durch die

direkte Kopplung der Benutzerverwaltung z. B. mit Personal- und Kundendatenbeständen wird sichergestellt, dass keine auf Ebene der Geschäftsprozesse Unbekannten unberechtigt Kennungen erlangen und Benutzerdatensätze beispielsweise beim Ausscheiden von Mitarbeitern zeitnah und automatisiert auch wieder gelöscht werden. Wie in Abschnitt 2.4.2 dargelegt wurde, werden in komplexen Unternehmensumgebungen oft Rollen modelliert, die einerseits organisatorische Zuordnungen (z. B. Mitarbeiter der IT-Abteilung) und andererseits technische Zuständigkeiten (z. B. Datenbankadministrator) widerspiegeln, um den Benutzern die Vielzahl einzelner technischer Berechtigungen strukturiert zuweisen zu können.

- User-Provisioning: Das User-Provisioning umfasst alle, nach Möglichkeit weitestgehend automatisierte Abläufe, um einzelne IT-Dienste und IT-Systeme an die zentrale Benutzerverwaltung und die damit verwalteten Autorisierungen anzubinden, so dass nach Vergabe einer Berechtigung beispielsweise eine lokale Kennung auf dem entsprechenden System angelegt und nach Entzug der Berechtigung wieder gelöscht wird.
- Authentifizierung: In diesen Aufgabenbereich fällt zum einen der Betrieb der Infrastruktur zur Authentifizierung u. a. von Benutzern und Endgeräten auf Basis von Wissen (z. B. Passwort), Besitz (z. B. Smartcard) bzw. Eigenschaften (z. B. biometrischer Fingerabdruckleser). Dem operativen Sicherheitsmanagement sind jedoch beispielsweise auch Supportanfragen zum Zurücksetzen vergessener Passwörter zuzuordnen.
- Privileged Account Management: Insbesondere durch die oben diskutierten gesetzlichen Auflagen motiviert finden Schutzmaßnahmen gegen potentielle interne Angreifer, die systemadministrative Berechtigungen haben, inzwischen auch außerhalb klassischer Anwendungsbereiche, zu denen beispielsweise das Militär und Banken gehören, immer weitere Verbreitung. Durch die Minimierung der nutzbaren administrativen Funktionalität und die durchgängige Aufzeichnung und Überwachung der als Administrator durchgeführten Tätigkeiten soll der Schaden, den „privilegierte“ Benutzer anrichten können, verhindert bzw. frühzeitig erkannt und somit minimiert werden. Sofern die administrierten Systeme keine entsprechenden Verfahren integriert haben, können die erforderlichen Restriktionen beispielsweise über Gateways umgesetzt werden, die zur Administration zwingend verwendet werden müssen.
- Zutrittsverwaltung: Der sichere Betrieb von IT-Infrastrukturen umfasst auch eine Regelung des physischen Zutritts, beispielsweise zu Netzkomponenten und zu Endgeräten wie Serverfarmen, auf denen die IT-Dienste betrieben werden. Dem operativen Sicherheitsmanagement ist in diesem Kontext über die Berechtigungsverwaltung hinausgehend der Betrieb der Zutrittskontrollsysteme zuzuordnen.

Beim Einsatz von Security-Frameworks ist zu unterscheiden, ob die von ihnen bereitgestellte Sicherheitsfunktionalität eine Verknüpfung mit der Berechtigungsverwaltung für reguläre Benutzer erfordert, beispielsweise weil sie eigene Komponenten zur Benutzerauthentifizierung enthalten, oder ob ihr Einsatz diesbezüglich transparent abläuft und keine Anbindung an die Berechtigungsverwaltung erfordert. Die Komponenten des Security-Frameworks sind selbst wiederum den Maßnahmen zum Privileged Account Management und zur Zutrittsverwaltung zu unterziehen.

- **Sicherstellung der (Hoch-)Verfügbarkeit**: Die Maßnahmen zur Gewährleistung der von Geschäftsprozessen benötigten und im Rahmen von SLAs vereinbarten, möglichst durchgängigen Verfügbarkeit von Diensten und Daten konzentrieren sich auf die Schaffung fehlertoleranter Infrastrukturen. Die Umsetzung erfolgt häufig durch Redundanz, um bei Teilausfällen ohne oder nur mit kurzer Unterbrechung wieder in den regulären Betrieb übergehen zu können. Dabei ist zwischen Daten- und Hardwareredundanz zu unterscheiden:

  – Datenredundanz: Durch das Vorhalten von Kopien aller relevanten Daten, beispielsweise durch Backups oder Spiegelsysteme, können die Auswirkungen von Datenträgerdefekten reduziert werden. Physische Schutzmaßnahmen – beispielsweise die Aufbewahrung der Kopien an anderen Standorten, um einem Verlust von Original und Kopie z. B. durch Brand vorzubeugen – müssen in der Regel mit den unten beschriebenen kryptographischen Mechanismen, z. B. einer Verschlüsselung aller Daten, kombiniert werden.

  – Hardwareredundanz: Redundante Hardware wird sowohl innerhalb eines Endgeräts, z. B. durch die Nutzung mehrerer Netzteile zur redundanten Stromversorgung, als auch in Form der Bereitstellung mehrerer nahezu identischer Endgeräte, die sich gegenseitig ersetzen können, genutzt. Während das Wiedereinspielen von Backups häufig manuell angestoßen werden muss, kommen bei Hardwareredundanz meist automatisierte Failover-Mechanismen zum Einsatz, die vom operativen Sicherheitsmanagement konfiguriert und regelmäßig getestet werden müssen.

  Neben Hardwaredefekten müssen auch gezielte Angriffe auf die Verfügbarkeit von Daten und Systemen betrachtet werden. So sind Backups beispielsweise auch dann relevant, wenn ein Angreifer Daten manipuliert oder gelöscht hat; ausreichende Hardwarekapazitäten dienen darüber hinaus der Abfederung von Denial-of-Service-Angriffen, die auf eine Überlastung der Infrastrukturkomponenten abzielen.

  Der Einsatz von Security-Frameworks erhöht die Komplexität dieses Teilbereichs des operativen Sicherheitsmanagements oft erheblich, weil die damit einhergehenden zusätzlichen Komponenten mindestens dieselben Verfügbarkeitscharakteristika aufweisen müssen wie die geschützten Assets, potentielle weitere Angriffsziele darstellen und sich damit potentiell negativ auf die Verfügbarkeit des Gesamtsystems auswirken.

- **Kryptographische Mechanismen**: Kryptographische Hashfunktionen und Verschlüsselungsverfahren haben sich als Bausteine zur Sicherstellung von Authentizität, Integrität und Vertraulichkeit von Daten während ihrer Übertragung und Hintergrundspeicherung durchgesetzt. Im operativen Sicherheitsmanagement sind zwei wichtige Anwendungsgebiete zu unterscheiden:

  – Public-Key-Infrastrukturen (PKI): Server- und Personenzertifikate ermöglichen die effiziente Authentisierung von Kommunikationspartnern und bilden die Grundlage für die nachfolgend beschriebenen digitalen Signaturen. Die zuverlässige und skalierende Überprüfung der Echtheit und Gültigkeit von Zertifikaten setzt jedoch wie in Abschnitt 2.4.2 skizziert die Nutzung einer PKI voraus. Aufgrund der zeitlich beschränkten Gültigkeit von Zertifikaten und der Notwendigkeit, Zertifikate z. B. nach Sicherheitsvorfällen, die zu einer Kompromittierung des zum Zertifikat passenden Private Keys geführt haben, vorzeitig zu erneuern, stellt die Verwal-

tung einer größeren Zahl an Zertifikaten einen nicht unerheblichen Aufwand für das operative Sicherheitsmanagement dar.

– Verschlüsselung und elektronische Signaturen: Die Verschlüsselung von E-Mails, weiten Teilen der netzbasierten Kommunikation, den Hintergrundspeichern mindestens mobiler Geräte und von Backups hat sich aufgrund der Verbesserungen in der Benutzungsfreundlichkeit entsprechender Werkzeuge inzwischen ebenso durchgesetzt wie die Sicherstellung des Datenursprungs durch elektronische Signaturen, beispielsweise bei der Distribution von Software-Updates und beim Versand von E-Mails. Neben der entsprechenden Konfiguration von Endgeräten ist es Bestandteil des operativen Sicherheitsmanagements, dem jeweiligen Schutzbedarf adäquate Mechanismen zu wählen und auf dem aktuellen Stand zu halten: Beispielsweise durch auf Verschlüsselungs- und Hashalgorithmen im Laufe der Jahre bekannt werdende Angriffe und durch ablaufende Zertifikate motiviert müssen nicht nur die jeweils aktuell eingesetzten Verfahren kontinuierlich angepasst, sondern es muss auch z. B. der Schutz von Daten im Rahmen der Langzeitarchivierung überarbeitet werden.

Für das Management von Security-Frameworks ist im Kontext der kryptographischen Maßnahmen somit einerseits ausschlaggebend, ob beispielsweise der Einsatz von Verschlüsselung im selben Umfang möglich ist, wie dies szenarienweit bereits üblich ist, oder ob in ausgewählten Bereichen darauf verzichtet werden muss, beispielsweise weil einzelne Sicherheitsmechanismen zwingend auf die Verfügbarkeit des Klartextes angewiesen sind, um beispielsweise eine genauere Analyse der Nutzdaten vorzunehmen. Andererseits ist insbesondere bei Security-Frameworks, die über Standardkomponenten hinausgehend eigene Mechanismen mitliefern oder die szenarienspezifische Implementierung zusätzlicher Komponenten erfordern, die Zukunftsfähigkeit zu betrachten, so dass beispielsweise auf neuere Verschlüsselungsverfahren umgestellt werden kann.

- **Präventive und validierende Maßnahmen**: Mit Ausnahme des auf Endgeräten eingesetzten Malware-Schutzes und der netzweit genutzten IDS-Systeme hatten alle bislang beschriebenen Tätigkeiten des operativen Sicherheitsmanagements einen präventiven Charakter, d. h. sie sollen Sicherheitsvorfälle von vornherein verhindern oder zumindest signifikant erschweren. Diese Eigenschaft trifft auch auf die folgenden Aufgaben zu, die keinem der o. g. Bereiche direkt zugeordnet werden können:

  – Penetrationstest: Einerseits wird durch den Einsatz von Vulnerability Assessment Scannern nach bekannten Verwundbarkeiten, z. B. in der für den Betrieb von IT-Diensten eingesetzten Software, gesucht; andererseits kann mit geplanten, kontrollierten Angriffe überprüft werden, ob ihnen die Infrastruktur standhält. Penetrationstests müssen sowohl nach Änderungen an der Infrastruktur als auch regelmäßig wiederholt werden, um erst zwischenzeitlich bekannt gewordene Angriffsvarianten und Sicherheitslücken zu berücksichtigen.

  – Policy Enforcement: Die Überprüfung der Einhaltung der im Rahmen des Sicherheitsmanagementprozesses vorgegebenen Policies obliegt dem operativen Sicherheitsmanagement. Beispielsweise kann analog zu Penetrationstests durch eigene Bemühungen, Benutzerpasswörter mit Brute-Force-Verfahren aufzudecken, die Einhaltung der Qualitätsanforderungen einer Passwort-Richtlinie analysiert werden.

Ein weiterer Anwendungsbereich ist die Informationsklassifizierung: Unterschiedliche Daten weisen einen unterschiedlichen Schutzbedarf auf; während bei öffentlich zugänglichen Daten, beispielsweise den über Webserver präsentierten Inhalten, die Integrität und Verfügbarkeit im Vordergrund stehen, haben z. B. unternehmensinterne Personalverwaltungsdaten einen erhöhten Bedarf an Vertraulichkeit. Die per Richtlinie vorgegebenen Klassifizierungsregeln müssen für die im praktischen Betrieb anfallenden Daten umgesetzt werden (vgl. dazu die Behandlung des Schutzbedarfs in Abschnitt 6.4.3).

- Sichere Entsorgung von Datenträgern: Nicht mehr benötigte oder defekte Datenträger und Speichermedien, die entsorgt oder umgetauscht werden sollen, enthalten im Allgemeinen noch Daten, die vernichtet werden müssen, bevor unberechtigte Dritte davon Kenntnis erlangen können. Obwohl die Vernichtung von Datenträgern häufig an Dritte delegiert wird, die über eine entsprechende technische Ausrüstung für die effiziente Umsetzung verfügen, bleibt der Auftraggeber für den Gesamtvorgang verantwortlich und muss ihn im Rahmen des operativen Sicherheitsmanagements zumindest überwachen.
- Aggregation von Sicherheitsinformationen: Durch die Vielzahl eingesetzter Komponenten und Softwareprodukte verschiedenster Hersteller sind viele der jeden Tag neu entdeckten und behobenen Sicherheitslücken für größere Organisationen an den entsprechenden Stellen relevant. Das Zusammenstellen und Analysieren der aus verschiedenen Quellen verfügbaren Sicherheitsinformationen ist deshalb eine zentrale planerische Tätigkeit im operativen Sicherheitsmanagement. Als Informationsquellen kommen beispielsweise entsprechende Meldungen von Herstellern und Zulieferern, einschlägige Mailinglisten und Sicherheitsforen im Internet, öffentliche und herstellerübergreifende Verwundbarkeitsdatenbanken wie CVE [MIT11b] sowie eigene Honeypots und Meldungen von Administratoren und Benutzern in Frage.
- Dokumentation sicherheitsrelevanter Tätigkeiten und Maßnahmen: Analog zur Dokumentation der organisatorischen Abläufe im Rahmen des Sicherheitsmanagementprozesses müssen auch die für einzelne IT-Dienste und IT-Systeme getroffenen Sicherheitsmaßnahmen in einer Form dokumentiert werden, die den betrieblichen Abläufen und von Externen durchgeführten Überprüfungen, beispielsweise im Rahmen von Zertifizierungsaudits, genügt.

Da es sich bei Security-Framework um auf zu schützende Assets abgestimmte technische und organisatorische Schutzmaßnahmen handelt, liefern Frameworkinstanzen im Allgemeinen keine direkten Beiträge zur Umsetzung dieses Aufgabengebiets; vielmehr sind ihre Komponenten selbst den vorhandenen Sicherheitsrichtlinien und aktiven Testverfahren zu unterziehen und ihr Einsatz muss entsprechend dokumentiert werden. Allerdings können die Frameworkkonzepte bzw. -dokumentationen herangezogen werden, die selbst eine themenspezifische Aggregation von Sicherheitsinformationen darstellen und somit die Dokumentation der praktischen Umsetzung erleichtern und gezielt auf das Zusammenspiel mit Policies sowie im Rahmen von Sicherheitstests zu berücksichtigende Aspekte hinweisen können.

- **Security Information & Event Management (SIEM)**: Das Informations- und Ereignismanagement umfasst alle Maßnahmen zur Aggregation und Auswertung der im

laufenden Betrieb anfallenden sicherheitsrelevanten Daten und die adäquate Reaktion auf erkannte Sicherheitsvorfälle. Dabei sind die folgenden Aufgabenbereiche zu unterscheiden:

- Monitoring und technisches Auditing: Das sicherheitsspezifische Monitoring beinhaltet alle Aktivitäten zur Überwachung von IT-Diensten und IT-Systemen, die zur Erkennung der Abweichung vom Soll-Zustand dienen. Zu seiner Umsetzung werden im Allgemeinen von den überwachten Komponenten verschickte Benachrichtigungen, die Ergebnisse regelmäßiger Abfragen durch Monitoringsysteme und erstellte Protokolldateien aggregiert, korreliert und ausgewertet; bei erkannten Sicherheitsvorfällen werden vorgegebene automatische Aktionen wie das Informieren der zuständigen Administratoren angestoßen. Technische Audits, die entweder regelmäßig zur Kontrolle der korrekten Funktionsweise des Monitorings oder kontinuierlich für Systeme mit hohen Schutzanforderungen durchgeführt werden, beinhalten darüber hinaus die manuelle Kontrolle und Bestätigung der Überwachungsergebnisse, auch wenn keine Sicherheitsvorfälle erkannt wurden.
- Security Incident Management: Nach dem Eintreten eines Sicherheitsvorfalls müssen einem definierten Security-Incident-Response-Prozess gemäß Maßnahmen ergriffen werden, um schnellstmöglich zum regulären Betrieb zurückkehren zu können. Die Aufgaben des operativen Sicherheitsmanagements umfassen dabei zunächst geeignete Erstreaktionen, z. B. die Isolation eines kompromittierten Endgeräts in einem Quarantänenetz, die Analyse des Vorfalls mit einer Bestimmung von Auswirkungen und Dringlichkeit (engl. *impact* und *urgency*), das Bestimmen und Ergreifen geeigneter Gegenmaßnahmen sowie ggf. weiterführende IT-forensische Analysen und die Sicherung von Beweismitteln.
- Reports und Analysen: Sowohl die Monitoringdaten als auch Kennzahlen der in allen beschriebenen Bereichen umgesetzten Sicherheitsmaßnahmen dienen als Grundlage für die Erstellung von Berichten über das operative Sicherheitsmanagement, die von den entsprechenden Zielgruppen ausgewertet werden, um gezielte Planungen für die Weiterentwicklung vornehmen zu können (vgl. Abschnitt 6.6).

Durch ihre Eigenschaft, diverse sicherheitsrelevante Komponenten konzeptionell zu aggregieren, wirken sich Security-Frameworks stark auf den Aufgabenbereich SIEM aus. Wie in den Abschnitten 6.4 und 6.6 gezeigt wird, eignet sich die durch Security-Frameworks induzierte Gruppierung von Komponenten zur Strukturierung des Monitorings und der Berichte; darüber hinaus ergänzen frameworkspezifische Kennzahlen die über die Einzelkomponenten ermittelten Informationen. Die sich aus dem Einsatz von Security-Frameworks ergebenden Zusammenhänge und Abhängigkeiten müssen jedoch auch bei der Reaktion auf Sicherheitsvorfälle berücksichtigt werden.

Analog zur Einordnung in den Sicherheitsmanagementprozess in Abschnitt 6.1.1.3 handelt es sich bei dieser Zusammenstellung um eine Momentaufnahme eines sich inhaltlich weiterentwickelnden Bereichs, der einerseits von technologischen Fortschritten getrieben wird und andererseits besser skalierende Methoden erarbeiten muss, um mit der kontinuierlich wachsenden Anzahl verschiedenster in der IT-Infrastruktur eingesetzter Komponenten effizient umgehen zu können.

Im Unterschied zum Sicherheitsmanagementprozess gibt es keine Standards für das opera-

tive Sicherheitsmanagement. Best Practices und andere Leitfäden behandeln überwiegend produkt- und versionsspezifisch einzelne Aufgabenbereiche innerhalb einer der oben genannten Kategorien. Eine Ausnahme stellen die BSI-Grundschutzkataloge dar, die wie oben erläutert auch Maßnahmen für eine größere Zahl von konkreten Softwareprodukten beinhalten und somit eine in der Praxis sowohl für den Prozess als auch die operative Umsetzung des Sicherheitsmanagements relevante Referenz darstellen.

Der Bedarf vieler Unternehmen, die Qualifikation ihres Personals für das operative Sicherheitsmanagement nachweisen zu können, wird seit einigen Jahren durch herstellerspezifische Ausbildungs- und Zertifizierungsprogramme abgedeckt. Administratoren werden dabei spezifisch bezüglich der Sicherheitsaspekte ausgewählter Produkte und Produktreihen geschult und geprüft; im Kontext der System- und Netzsicherheit gehören hierzu beispielsweise:

- Cisco CSSP: Die Zertifizierung als Cisco Certified Security Professional (CSSP) umfasst inhaltlich die sichere Konfiguration von aktiven Netzkomponenten, Firewalls, VPNs, Intrusion Detection Systemen und Network Admission Control auf Basis jeweils aktueller Cisco-Produkte; sie muss alle drei Jahre erneuert werden, so dass sichergestellt ist, dass Zertifizierte zu den aktuellen Produkten passende Kenntnisse aufweisen.

- Microsoft MCTS und MCITP: Die Schulungsprogramme zum Microsoft Certified Technology Specialist bzw. IT-Professional orientieren sich an den jeweils aktuellen Versionen z. B. der Serverbetriebssystem-, Groupware-, Datenbank- und Virtualisierungsprodukte von Microsoft und umfassen auch deren sicherheitsspezifische Konfiguration. Durch die Bindung des Zertifikats an die jeweilige Produktversion ergibt sich die Gültigkeit der Zertifizierung aus dem Releasezyklus bzw. von Microsoft angebotenen Supportzeitraum.

- Red Hat Certified Security Specialist (RHCSS): Das Ausbildungsprogramm des Linux-Distributors RedHat deckt die Administration und Härtung von Linux-Servern und ausgewählten unter Linux betriebenen Netzdiensten wie Web-, DNS-, E-Mail- und Fileservern ab; die praktischen Anteile sind stark an den Spezifika der hauseigenen Linux-Distribution RHEL ausgerichtet. Darüber hinaus werden vertiefende Kurse z. B. für das Zertifikatsmanagement und den Betrieb Linux-basierter Firewalls angeboten. Die Zertifizierung ist drei Jahre lang gültig.

Durch den wachsenden Markt mit Ausbildungs- und Zertifizierungsprogrammen motiviert entstehen inzwischen auch vermehrt herstellerunabhängige bzw. -übergreifende Schulungsangebote. Diese sind jedoch auch weiterhin dadurch geprägt, dass sie nahezu ausschließlich die systemnahe technische Umsetzung von Sicherheitsmechanismen betrachten und nur unzureichend auf die Zusammenhänge mit dem Sicherheitsmanagementprozess eingehen. Da die Zertifizierungsprogramme im Rahmen des Sicherheitsmanagementprozesses hierzu genau komplementär sind, verbleibt die Zusammenführung der organisatorischen und operativen Teilaspekte des Sicherheitsmanagements eine individuell szenarienspezifisch zu lösende Aufgabe.

Die für ein integriertes Management erforderliche Zusammenführung dieser beiden Bereiche des Sicherheitsmanagements wird in den weiteren Abschnitten dieses Kapitel auf Security-Frameworks zugeschnitten erarbeitet. Als erstes wird hierzu das Risikomanagement betrachtet.

6.3. Security-Framework-orientiertes Management von IT-Sicherheitsrisiken

Eine grundlegende Definition von Risiken wurde bereits in Abschnitt 2.2.3.1 vorgenommen: Das mit einem Ereignis e verbundene Risiko R_e hängt von seiner Eintrittswahrscheinlichkeit P_e und seiner Schadwirkung S_e ab: $R_e = P_e \cdot S_e$. In der Praxis ist es jedoch sehr schwierig, eine vollständige Liste aller relevanten und sich eventuell gegenseitig beeinflussenden Schadereignisse zu erstellen, deren Eintrittswahrscheinlichkeit und Schadwirkung exakt zu bestimmen und aus der resultierenden Quantifizierung konkrete Maßnahmen zum Umgang mit den Risiken abzuleiten. Verschiedene in Wissenschaft und Praxis etablierte Ansätze unterstützen das Risikomanagement deshalb methodisch und lassen sich bezüglich ihrer Schwerpunkte grob in die Phasen Risikoermittlung (engl. *risk identification*), Risikobewertung (engl. *risk assessment*) und Risikosteuerung (engl. *risk control*) untergliedern.

Security-Frameworks setzen sich konzeptionell mit zu schützenden Assets sowie bekannten Verwundbarkeiten und Angriffen auseinander; sie tragen somit in ihrem Bereich bereits zur Risikoermittlung bei. Darüber hinaus geben sie technische und organisatorische Maßnahmen vor, die sich auf Eintrittswahrscheinlichkeit und Schadwirkung dieser Risiken auswirken können, und leisten somit einen Beitrag zur Risikosteuerung.

Die hohe Bedeutung, die dem Risikomanagement wie in Abschnitt 6.1 beschrieben in Standards und gesetzlichen Auflagen beigemessen wird, und die relativ große Zahl an praktischen Leitfäden und wissenschaftlichen Publikationen zum IT-Risikomanagement deuten jedoch auf die nicht zu unterschätzende Komplexität dieser Disziplin hin. In die Risikomanagementmethoden und die sie beschreibende Literatur haben Security-Frameworks bislang noch keinen Eingang gefunden. In den folgenden Abschnitten werden deshalb die einzelnen Phasen und Aufgaben des Risikomanagements im Kontext von Security-Frameworks konzeptionell aufbereitet und um deren Spezifika ergänzt: In Abschnitt 6.3.1 wird zunächst auf die Methoden zur Ermittlung von Risiken eingegangen und es werden neue, spezifische Aspekte ihrer Nutzung im Zusammenspiel mit Security-Frameworks betrachtet. Anschließend wird in Abschnitt 6.3.2 die Vorgehensweise zur Bewertung von Risiken unter Berücksichtigung der Vorarbeiten in Security-Frameworks behandelt; dabei werden auch ausgewählte Bewertungsverfahren vorgestellt, die eng mit den in Abschnitt 6.4 vorgestellten Managementkonzepten zusammenspielen. Abschnitt 6.3.3 thematisiert mögliche Vorgehensweisen und Maßnahmen zur Risikosteuerung und Abschnitt 6.3.4 geht auf die konkrete Umsetzung der gewählten Risikosteuerungsmaßnahmen und deren Integration ins Prozessumfeld ein. Alle Betrachtungen orientieren sich an jeweils kurz vorgestellten Standards und Best Practices zum IT-Risikomanagement; in Abschnitt 6.3.5 wird eine abschließende Gegenüberstellung erarbeitet, die zudem zusammenfasst, an welchen Stellen für Security-Frameworks spezifische Ergänzungen der Aufgaben und Abläufe des Risikomanagements vorgenommen wurden.

6.3.1. Methoden zur Ermittlung von Risiken und ihre Nutzung im Kontext von Security-Frameworks

Die initiale Phase des Prozesses zum Risikomanagement zielt darauf ab, eine möglichst vollständige Liste der im konkreten Szenario relevanten Schadereignisse zu bestimmen, die aber noch nicht z. B. durch Priorisierung bewertet werden. Während das Risikomanagement im

Allgemeinen eine Zuordnung von Risiken zu geschäftsrelevanten Prozessen verlangt, werden IT-Risiken typischerweise Assets zugeordnet, die zum einen wiederum Geschäftsprozesse unterstützen, denen sie zugeordnet werden können, und zum anderen hierarchisch zueinander angeordnet werden können. Somit können Risiken, die z. B. für ein ganzes Rechenzentrum relevant sind, auch im Kontext einzelner Dienste und Systeme betrachtet werden. Darüber hinaus müssen Risiken auf verschiedenen Abstraktionsebenen bzw. in verschiedenen Kategorien betrachtet werden, für die beispielsweise eine Orientierung an der Untergliederung des Sicherheitsmanagementprozesses nach ISO/IEC 27001 möglich ist (vgl. Abschnitt 6.5). Somit sind im Allgemeinen physische Schadereignisse wie Stromausfälle und Wasserschäden, die sich auf die Verfügbarkeit von Diensten und Daten auswirken, ebenso zu betrachten wie Schwachstellen in unternehmensinternen Prozessabläufen, die von internen Angreifern ausgenutzt werden könnten, und Sicherheitslücken in eingesetzter Software. Aufgrund der Ausrichtung von Security-Frameworks auf IT-Dienste und IT-Architekturen und ihrer überwiegend an technischen Assets und deren spezifischen Schwachstellen orientierten Konzepte werden nachfolgend primär Risiken auf technischer Ebene betrachtet, zu denen die Security-Frameworks in den nachfolgenden Risikomanagementphasen relevante Beiträge liefern.

Die Ermittlung von IT-Risiken besteht nach NIST SP 800-30 aus den folgenden vier Teilaufgaben, die auch in den meisten anderen Risikomanagementansätzen betrachtet werden:

1. Identifizierung und Beschreibung der Assets.
2. Identifizierung der Bedrohungen.
3. Identifizierung der Schwachstellen bzw. Verwundbarkeiten.
4. Analyse der bereits vorhandenen Schutzmaßnahmen.

Die folgenden Abschnitte gehen näher auf diese vier Teilaufgaben und die jeweilige Rolle von Security-Frameworks ein.

6.3.1.1. Identifizierung und Beschreibung der Assets

Die strukturierte Erfassung der Assets erfolgt üblicherweise bereits im ITSM-Prozess Configuration Management (vgl. Abschnitt 6.5), so dass die Teilaufgabe 1 insbesondere darin besteht, die im Risikomanagement zu behandelnde Teilmenge aller Assets festzulegen. Nach [Ecke09, S. 167ff.] kann dies auf Basis einer Schutzbedarfsermittlung erfolgen; beispielsweise könnte festgelegt werden, dass in Laborumgebungen betriebene Testrechner nicht für das Risikomanagement relevant sind. Offensichtlich muss hierbei ein Kompromiss gefunden werden, der berücksichtigt, dass einerseits ein Betrachten sehr vieler Assets den Aufwand aller nachfolgenden Schritte stark in die Höhe treibt, andererseits das Vernachlässigen wichtiger Bereiche zu falschen Ergebnissen mit gravierenden Konsequenzen führen kann. Die OCTAVE-Methode [ADA01], ein wiederum an NIST SP 800-30 orientiertes Vorgehensmodell zum Risikomanagement, empfiehlt für große Unternehmen, eine geeignete Verteilung der Aufgaben des Risikomanagements z. B. anhand einer Aufteilung nach Standorten oder Abteilungen vorzunehmen, damit jeweils eine Konzentration der Aktivitäten auf die wirklich kritischen Assets erfolgen kann.

Die somit durchgeführte Festlegung des Einflussbereichs des Risikomanagements ist zwingend szenarienspezifisch und an den Assets, also den zu schützenden Werten, nicht an den bereits

eingesetzten oder potentiell in Frage kommenden Schutzmaßnahmen orientiert. Der Einfluss von Security-Frameworks ist für Teilaufgabe 1 deshalb auf die folgenden beiden Aspekte beschränkt: Erstens können Security-Frameworks analog z. B. zur Modellierung von Diensten im Configuration Management (vgl. Abschnitt 6.4) als Instrument zur Aggregation bzw. Gruppierung zusammenhängender Assets eingesetzt werden. Als Konsequenz können alle von einem Security-Framework berücksichtigten Assets als Einheit aufgefasst werden, wodurch sich die Anzahl der in den weiteren Risikomanagementschritten zu betrachtenden Assets gegenüber einer Betrachtung aller Einzelkomponenten reduziert. Sofern die hierfür herangezogenen Security-Frameworks die unten erläuterten Anforderungen, die sich aus den weiteren Schritten ergeben, aber nicht erfüllen, muss an entsprechender Stelle gegebenenfalls wieder eine Dekomposition vorgenommen werden. Zweitens liefern die Auswahl und der Detailgrad, mit dem Assets in Security-Frameworks behandelt werden, Kriterien für die eigene Auswahl der im Rahmen des Risikomanagements zu betrachtenden Assets. Somit sollten einerseits Assets, die in Security-Frameworks umfassend berücksichtigt werden, nicht ohne guten Grund in den szenarienspezifischen Betrachtungen fehlen; andererseits ist es im Allgemeinen erforderlich, von Security-Frameworks explizit ausgeschlossene, aber im Szenario vorhandene Assets in die Risikoanalyse mit aufzunehmen, um die Notwendigkeit über das Security-Framework hinausgehender Schutzmaßnahmen zu beurteilen.

Nach der Auswahl der Assets ist ihre Priorisierung der nächste wichtige Schritt (vgl. [WhMa09, S. 128]), um die weiteren Bemühungen zu fokussieren: Da in komplexen Unternehmensumgebungen im Allgemeinen sehr viele Assets und sehr viele mit ihnen verbundene Risiken betrachtet werden müssen, kann aufgrund der damit verbundenen Kosten und Aufwendungen nicht jeder Bereich umfassend geschützt werden. Stattdessen müssen bereits anhand der Geschäftsprozesse, die durch die Assets umgesetzt werden, geeignete Prioritäten vorgegeben werden; zunächst zurückgestellte Bereiche werden entsprechend in späteren Iterationen im Rahmen der kontinuierlichen Verbesserung behandelt. In der Regel korreliert die Priorität eines Assets mit seinem szenarienspezifischen Wert: Besonders teure Systeme oder sensible Daten werden vorrangig betrachtet.

Für jedes ausgewählte Asset müssen ferner diverse Informationen zusammengetragen werden, die in den weiteren Schritten beispielsweise zur Ermittlung der Schwachstellen oder zur Auswahl geeigneter Gegenmaßnahmen benötigt werden. Dabei ist im Allgemeinen davon auszugehen, dass das Risikomanagement von Personal durchgeführt wird, das nicht notwendigerweise fachlich tiefgehende Kenntnisse über die betrachteten Assets hat. Im Idealfall stellen beispielsweise das Configuration Management und andere unternehmensweite Dokumentationssysteme auch die für das Risikomanagement relevanten Informationen bereit. Nach NIST SP 800-30 gehören dazu unter anderem eine Beschreibung der Aufgaben des Assets, der Schutzbedarf der zum Asset gehörenden Systeme und Daten, eine Definition des regulären Nutzerkreise, eine Liste für das Asset relevanter Security-Policies, Abhängigkeiten zu anderen Assets und resultierende Datenflüsse, technische Informationen beispielsweise über Netztopologie und Datenspeicherorte, sowie bereits eingesetzte physische, technische und organisatorische Schutzmaßnahmen. Da der Idealfall, dass diese Informationen jederzeit aktuell und einfach abrufbar gehalten werden, in der Praxis noch zu selten eintritt, liefern viele Risikomanagement-Ansätze Vorschläge zur Informationsermittlung beispielsweise über Fragebögen, Interviews und Auto-Discovery-Tools, auf die hier jedoch nicht näher eingegangen wird.

6.3.1.2. Identifizierung der Bedrohungen

Die zweite Teilaufgabe besteht in der Bestimmung und Ordnung einer möglichst vollständigen Liste der im weiteren Verlauf des Risikomanagements zu betrachtenden Bedrohungen, zu denen im Allgemeinen alle Arten von Ereignissen gehören, die sich z. B. negativ auf die Vertraulichkeit, Integrität oder Verfügbarkeit von Assets auswirken können. Entsprechend müssen generell Schadereignisse, die verschiedensten Bereichen des Sicherheitsmanagements zugeordnet werden können, betrachtet werden, da sich beispielsweise hypothetisch ein Wasserrohrbruch genauso auf die Verfügbarkeit eines IT-Dienstes auswirken kann wie ein von einem Angreifer über das Internet ausgenutzte Sicherheitslücke in der zur Erbringung des IT-Dienstes eingesetzten Software. Dem klar erkennbaren Fokus aktueller Security-Frameworks entsprechend werden ohne Beschränkung der Allgemeinheit nachfolgend primär technikspezifische Bedrohungen behandelt.

Die erfolgreiche Identifikation möglichst aller relevanten Bedrohungen wird grundlegend über Angreifermodelle gesteuert, die wie in Abschnitt 2.4 skizziert unter anderem die Motivation und Fähigkeiten von Angreifern beschreiben. Beispielsweise könnte bei einem über das Internet nutzbaren Dienst der Schwerpunkt des Risikomanagements auf externen Angreifern liegen, so dass Bedrohungen und Risiken, die sich durch organisationsinterne Angreifer ergeben, bewusst ausgeklammert werden. Die Konkretisierung zu betrachtender Bedrohungen ist folglich abhängig von den Angreifermodellen, muss somit szenarienspezifisch erfolgen und setzt entsprechendes Wissen über die Assets und die szenarienspezifische Infrastruktur voraus.

In den meisten Fällen wäre es jedoch nicht praktikabel, die Liste relevanter Bedrohungen für jedes Asset von Grund auf neu zu erarbeiten. Ein effizienteres Vorgehen macht sich deshalb einerseits zunutze, dass Mengen von Bedrohungen festgelegt werden können, die auf ganze Gruppen oder Kategorien von Assets zutreffen: Beispielsweise könnten für *Webanwendungen* oder für *über das Internet von außen erreichbare Server* allgemein relevante Bedrohungen festgelegt werden, die dann pro konkreter Webanwendung bzw. pro einzelnem Server lediglich spezifisch ergänzt werden müssen. Andererseits existieren für viele Bereiche bereits gut gepflegte Listen potentieller Bedrohungen, aus denen die im Szenario relevanten mit minimalem Aufwand ausgewählt werden können; so geben die oben diskutierten BSI-Grundschutzkataloge zahlreiche Bedrohungen in einem sehr breiten Spektrum vor und die OWASP-Community (vgl. [OWASP]) stellt beispielsweise einen äußerst umfangreichen Katalog webanwendungsspezifischer Bedrohungen bereit.

Security-Frameworks tragen über die von ihnen berücksichtigten Angriffe, sofern diese explizit im Frameworkkonzept dokumentiert sind, dazu bei, eine Vorauswahl relevanter Bedrohungen treffen zu können und unterstützen im Idealfall auch deren unten beschriebene Priorisierung. Die Untersuchungen in Kapitel 4 haben jedoch gezeigt, dass dadurch in den meisten Fällen keine ausreichende Annäherung an eine vollständige Liste aller Bedrohungen erreicht werden kann. Mindestens zur Identifikation von Bedrohungen, die eine Besonderheit des Szenarios darstellen, da sie sich auf Komponenten beziehen, die weder im Security-Framework noch in den allgemeinen Bedrohungsdatenbasen thematisiert werden, sind deshalb eigene Untersuchungen anzustellen.

Analog zur Identifikation von Assets schlagen Standards und Best Practices zum Risikomanagement deshalb einerseits Maßnahmen wie Fragebögen und Interviews zum Eruieren spezifischer Bedrohungen vor; andererseits existieren für die Analyse von IT-Diensten Leitfäden,

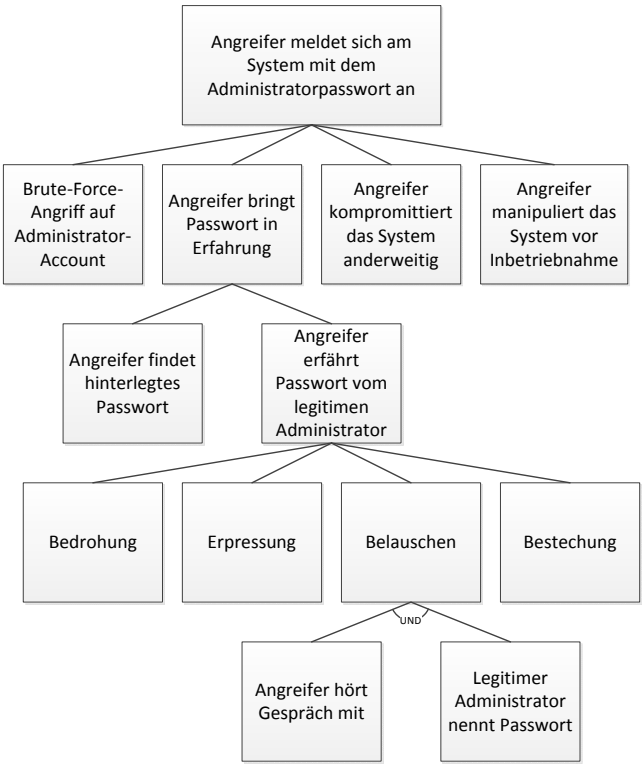


Abbildung 6.6.: Beispiel für einen Angriffsbaum (angelehnt an [Sch99])

die eine systematische, technikzentrierte Ermittlung relevanter Bedrohungen ermöglichen. Die von Microsoft propagierte STRIDE-Vorgehensweise (vgl. [Mic05]) betrachtet beispielsweise die Bedrohungsbereiche *Spoofing identity*, *Tampering with data*, *Repudiation*, *Information disclosure*, *Denial of service* und *Elevation of privilege*, aus deren Anfangsbuchstaben sich der Name des Verfahrens ableitet.

Eine detaillierte Auswertung der Eintrittswahrscheinlichkeit und Auswirkungen der somit ermittelten Bedrohungen findet erst in der nächsten Phase des Risikomanagements statt (siehe Abschnitt 6.3.2) und kann zuverlässig auch erst dann durchgeführt werden, wenn in den nächsten beiden Schritten dieser ersten Phase auch die Schwachstellen und die schon vorhandenen Sicherheitsmaßnahmen betrachtet wurden. Als pragmatisches Vorgehen hat sich in der Praxis jedoch herausgestellt, dass analog zur Auswahl betrachteter Assets auch eine Priorisierung und Reduktion betrachteter Bedrohungen notwendig werden kann, um den Aufwand für die nachfolgenden Schritte zu begrenzen.

Als Hilfsmittel können hierzu beispielsweise Bedrohungs- und Angriffsbäume (engl. *threat trees* und *attack trees*) eingesetzt werden, über die auch Abhängigkeiten zwischen Bedrohungen erfasst werden, die später u. a. zur Beurteilung der Eintrittswahrscheinlichkeit von Schadereignissen herangezogen werden können. Angriffsbäume sind eine auf Bruce Schneier zurückgehende Modellierungsmethodik, die die ursprünglich von Edward Amoroso geprägten Bedrohungsbäume (siehe [Amo94]) verfeinern und dabei berücksichtigen, dass dieselbe Bedrohung durch unterschiedliche Angriffe eintreten kann, die ebenso unterschiedliche Ge-

	Angreifer-modell	Unzufriedener Mitarbeiter	Script Kiddie	Industriespion
Security-Framework	**Asset**			
E-Commerce-Security-Framework	Mailserver	---	*versendet Spam über*	*liest ein- und ausgehende E-Mails*
	Webserver	*manipuliert öffentlich zugängliche Informationen*	*manipuliert öffentlich zugängliche Informationen*	*nutzt Maschine als Einfallstor*
	Datenbank	*löscht oder manipuliert Datensätze*	*liest vertrauliche Datensätze aus*	*liest vertrauliche Datensätze aus*
	Firewall	*deaktiviert Schutzregeln*	*überlastet mittels DoS-Angriff*	---
	Fileserver	*löscht wichtige Dateien*	---	*liest vertrauliche Dateien*
Storage-Security-Framework	Backup auf Band	*stiehlt oder zerstört*	---	*stiehlt oder kopiert*

Abbildung 6.7.: Einfaches Beispiel für eine Bedrohungsmatrix mit Kennzeichnung eingesetzter Security-Frameworks

genmaßnahmen erforderlich machen können (vgl. [Sch99]). Wie in Abbildung 6.6 dargestellt ist, bildet eine Bedrohung in einem solchen Modell die Wurzel des Baums und wird durch Teilbäume und Blätter in Teilbedrohungen bzw. Voraussetzungen für das Eintreten untergliedert. Für jeden Knoten ist dabei festzulegen, ob die in seinen Kindern verzeichneten Teilbedrohungen gemäß einer UND- bzw. ODER-Verknüpfung eintreten müssen, damit die Bedrohung eintritt. Die Tiefe eines Teilbaums wirkt sich somit auf die Anzahl der Zwischenschritte aus, die bis zum Eintritt der Wurzelbedrohung durchlaufen werden müssen. Aussagen zu Eintrittswahrscheinlichkeiten können als Knotenannotationen festgehalten werden. Sowohl auf Basis entsprechender Annotationen als auch durch die praktisch schnell anwachsende Größe des Baums können Grenzen gezogen werden, ab denen keine noch tiefergehende Bedrohungsidentifikation durchgeführt wird.

Die Zuordnung von Bedrohungen zu potentiellen Angreifern wird häufig in Form von Bedrohungsmatrizen dokumentiert. Dabei handelt es sich wie in Abbildung 6.7 dargestellt um Tabellen, in deren Zeilen die Assets und in deren Spalten die Bezeichnungen für Angreifermodelle eingetragen werden; jedes Element der Matrix wird mit einer Beschreibung der entsprechenden Bedrohungen gefüllt. Für den Einsatz von Bedrohungsmatrizen im Zusammenspiel mit Security-Frameworks wird im Rahmen dieser Arbeit die einfache Maßnahme vorgeschlagen, eine Erweiterung um Zeilengruppen durchzuführen, um darüber wie in der Abbildung dargestellt eine ggf. überlappende Zuordnung von Assets zu den Security-Frameworks, von denen sie geschützt werden, vorzunehmen.

6.3.1.3. Identifizierung der Schwachstellen und Verwundbarkeiten

Als dritter Schritt in dieser ersten Phase des Risikomanagements sind die Schwachstellen und Verwundbarkeiten der betrachteten Assets festzustellen; da jeder Verwundbarkeit eine Schwachstelle zugrunde liegt, wird im Folgenden vereinfachend nur der Begriff Schwachstelle verwendet (vgl. Abschnitt 2.2.2). Ihre Dynamik ist inhärent höher als die der Bedrohungen, da es sich im Wesentlichen um eine Momentaufnahme handelt, deren Ergebnis sich z. B. durch das routinemäßige Einspielen von Softwareaktualisierungen und das Bekanntwerden neuer Sicherheitslücken kontinuierlich wandeln kann.

Das Identifizieren der Schwachstellen stellt im Allgemeinen eine Konkretisierung der Bedrohungen und eine praktische Prüfung der Assets dar. Beispielsweise könnte als Bedrohung identifiziert worden sein, dass Angreifer potentiell von außen über eine Sicherheitslücke in einer Webanwendung weitreichende Kontrolle über einen Webserver erlangen können; zur Identifizierung der Schwachstellen kann folglich beispielsweise geprüft werden, ob über die aktuell eingesetzte Version der Webanwendung Sicherheitslücken bekannt sind, und ergänzend ein eigener Penetrationstest durchgeführt werden. Neben entsprechenden Datenbasen allgemein bekannter Schwachstellen, die sich bei Herstellern, CERTs und anderen Anbietern finden, und werkzeugunterstützten proaktiven Untersuchungen der Infrastruktur können wiederum mit dem konkreten Szenario vertrauten Experten befragt werden, welche Schwachstellen ihnen bekannt sind bzw. in welcher Form sie ein Eintreten der Bedrohungen für denkbar halten.

Security-Frameworks tragen implizit zur Identifizierung von Schwachstellen bei, da sie letztlich Maßnahmen bieten, die vor der Ausnutzung der beim Design des Security-Frameworks berücksichtigten Schwachstellen schützen und diese im Idealfall im Frameworkkonzept dokumentiert haben. Im Allgemeinen handelt es sich dabei aufgrund der Entkopplung zwischen den szenarienunabhängigen Security-Frameworks und den im Szenario konkret eingesetzten Komponenten und Softwareversionen jedoch um eine Zusammenstellung angenommener, typischerweise vorhandener Schwachstellen, die für das szenarienspezifische Risikomanagement validiert und präzisiert werden müssen.

Die Dokumentation ermittelter Schwachstellen erfolgt üblicherweise in Form einer tabellarischen Gegenüberstellung mit den Assets und den für diese zusammengestellten Bedrohungen. Wie in den vorherigen Schritten bietet sich eine Auswahl und Priorisierung an, um die Handhabbarkeit in den nächsten Schritten zu gewährleisten.

Bis zu diesem Schritt des Risikomanagements sind zwei weitere Aspekte zu beachten:

- Die Identifikation von Assets und Schwachstellen lässt sich zumindest für netzbasierte Bedrohungen und Angriffe weitgehend automatisieren. Dabei werden aus dem Netz- und Systemmanagement bekannte Auto-Discovery-Verfahren eingesetzt, um die über ein Netz erreichbaren Systeme zu ermitteln, und mit Penetrationstest- bzw. Vulnerability-Scan-Werkzeugen kombiniert, um zum einen eine Typisierung der gefundenen Systeme vorzunehmen und andererseits die Schwachstellen darauf betriebener Netzdienste automatisch zu analysieren. Beispielsweise wird die an der Universität Wien entwickelte und an NIST SP 800-30 orientierte AURUM-Methode [EFN09] durch ein Werkzeug unterstützt, das nach einem netzweiten Auto-Discovery über Internet frei zugängliche Vulnerability-Datenbanken nutzt, um die szenarienspezifischen Schwachstellen zu bestimmen. Unter Federführung des NIST wird zudem das Security Content Automation Protocol (SCAP, [Lab11]), das maßgeblich dazu beitragen soll, das Datenformat und

Vokabular zu standardisieren, mit dem Schwachstellen dokumentiert werden, um eine zuverlässige maschinelle Auswertung zu ermöglichen. Aufgrund der aktiven Beteiligung zahlreicher renommierter System- und Softwarehersteller ist davon auszugehen, dass sich die Automatisierung über das netzbasierte Auto-Discovery hinausgehend in den nächsten Jahren erheblich ausdehnen wird.

- Einige Risikomanagementmethoden fassen die Identifizierung der Schwachstellen und die Berücksichtigung der schon vorhandenen bzw. geplanten Sicherheitsmechanismen (siehe nachfolgender Schritt 4) zusammen, da Schwachstellen, für die bereits ausreichende Maßnahmen getroffen wurden, in der zweiten Phase des Risikomanagements nicht mehr zwingend berücksichtigt werden müssen. Die auch in dieser Arbeit verfolgte Trennung beider Schritte unterstützt jedoch beispielsweise die explizite Ermittlung von Sicherheitsmechanismen, die nicht mehr benötigt werden, falls die zugehörigen Schwachstellen inzwischen, z. B. aufgrund einer neuen Softwareversion, nicht mehr vorhanden sind. Darüber hinaus können die Beiträge von Frameworkkonzepten in dieser Phase differenzierter dargestellt werden.

Als letzter Schritt zur Ermittlung der Risiken müssen wie nachfolgend beschrieben die bereits vorhandenen Schutzmaßnahmen betrachtet werden.

6.3.1.4. Analyse der bereits vorhandenen Schutzmaßnahmen

Während viele im Rahmen des Sicherheitsmanagements zu betrachtende Schwachstellen im Laufe der Zeit wegfallen, beispielsweise durch Patches für Sicherheitslücken in Softwareprodukten, sind in der Praxis zahlreiche Bedrohungen und Schwachstellen inhärent mit Assets verbunden und erfordern separate Schutzmaßnahmen. Im Allgemeinen dienen Schutzmaßnahmen entweder der Reduktion der Wahrscheinlichkeit, mit der ein Schadereignis eintritt, oder reduzieren dessen negative Auswirkung auf die geschützten Assets.

Schutzmaßnahmen können sowohl technisch als auch organisatorisch ausgeprägt sein; die Umsetzung des Vier-Augen-Prinzips für die Arbeit von Administratoren an besonders kritischen Systemen ist beispielsweise zunächst eine organisatorische Vorgabe, deren Einhaltung jedoch nur durch den Einsatz entsprechender technischer Mechanismen sichergestellt werden kann. Zu den in diesem Schritt zu ermittelnden vorhandenen Schutzmaßnahmen gehören in der Praxis sowohl die produktiv eingesetzten als auch die bereits zur Umsetzung geplanten. Einzelne Schutzmaßnahmen können zudem bewusst nicht berücksichtigt werden, um im weiteren Verlauf des Risikomanagements zu prüfen, ob sie noch benötigt werden bzw. nach wie vor die beste Option zu Behandlung eines Risikos darstellen.

Die Dokumentation der identifizierten Schutzmaßnahmen erfolgt üblicherweise tabellarisch, um eine Zuordnung zu Assets und deren spezifischen Bedrohungen und Schwachstellen vornehmen zu können. Die Beschreibung jeder Schutzmaßnahme sollte dabei eine Einordnung enthalten, ob sie präventiv, detektierend oder reaktiv bezüglich relevanter Angriffe ausgerichtet ist. Die Umsetzung des oben erläuterten Paradigmas *defense-in-depth* äußert sich dabei in der Regel durch die Kombination mehrerer präventiver Schutzmaßnahmen für dieselben Bedrohungen und Schwachstellen.

Die effiziente Handhabung aller identifizierten Schutzmaßnahmen setzt im Allgemeinen zwei Formen von Gruppierungen voraus:

1. Eine einzelne Schutzmaßnahme kann sich auf Gruppen von Assets auswirken: Auf *technischer Ebene* schützt beispielsweise ein Firewall alle in einem Subnetz enthaltenen Endgeräte; analog dazu bezieht sich ein spezifizierter Security-Incident-Response-Prozess als *organisatorische Maßnahme* typischerweise auf mehrere oder gar alle Assets.
2. Mehrere Schutzmaßnahmen können gruppiert werden, um einzelne oder Gruppen von Assets gegen möglichst viele ihrer spezifischen Bedrohungen abzusichern. Hierzu gehören insbesondere Security-Frameworks, die bereits szenarienspezifisch instanziiert wurden. Die Berücksichtigung solcher Zusammenhänge zwischen zueinander komplementären und gruppierbaren Schutzmaßnahmen erfordert wie in Abschnitt 6.4 erarbeitet eine entsprechende Modellierung, die das Security-Framework als Einheit greifbar macht.

Bei der praktischen Anwendung muss berücksichtigt werden, dass insbesondere technische Schutzmaßnahmen, die z. B. wie netzweite Firewalls über dedizierte Hardwarekomponenten realisiert werden, selbst wiederum Assets darstellen, die Bedrohungen ausgesetzt und Schwachstellen aufweisen können, die Angreifer ausnutzen, um die Schutzmaßnahme zu umgehen. Durch qualitative Anforderungen bei der Auswahl technischer Sicherheitsmechanismen kann der Bedarf an *Schutzmaßnahmen für Schutzmaßnahmen* jedoch begrenzt werden, so dass eine aufwendige rekursive Betrachtung im Allgemeinen vermieden werden kann.

Mit dem Abschluss dieses Schrittes liegen Informationen über die im Szenario relevanten bzw. vorhandenen Assets, Bedrohungen, Schwachstellen und Schutzmaßnahmen und somit eine Beschreibung ausgewählter Teilaspekte von Risiken vor, die in der zweiten Phase des Risikomanagements bewertet werden.

6.3.2. Bewertung von Risiken unter Berücksichtigung der Vorarbeiten in Security-Frameworks

Die Bewertung der Risiken zielt darauf ab, die Reihenfolge festzulegen, in der alle im konkreten Szenario vorliegenden Risiken durch die Auswahl geeigneter Risikosteuerungsmaßnahmen in der nächsten Phase bearbeitet werden sollen. Große Risiken, die entsprechend als erste angegangen werden müssen, zeichnen sich dadurch aus, dass sie signifikante Auswirkungen haben und ihnen ein vermutlich eintretendes Ereignis zugrunde liegt. Die drei Schritte in dieser Phase sind entsprechend:

1. Einschätzung der Wahrscheinlichkeit, mit der jedes Schadereignis im konkreten Szenario eintritt.
2. Einschätzung der Auswirkung, die jedes potentiell eintretende Schadereignis hat.
3. Gegenüberstellung jedes betrachteten Risikos mit den anderen Risiken durch Quantifizierung und Ordnung.

Sie werden im Folgenden näher erläutert und in Bezug zu Security-Frameworks gesetzt.

6.3.2.1. Einschätzung der Eintrittswahrscheinlichkeit

Die Bestimmung der Eintrittswahrscheinlichkeit erfolgt im Bezug auf einen festzulegenden Betrachtungszeitraum, so dass beispielsweise abgeschätzt werden muss, mit welcher Wahrscheinlichkeit ein weltweit erreichbarer Webserver von einem externen Angreifer innerhalb

eines Jahres kompromittiert wird. Zur Beurteilung müssen die identifizierten Bedrohungen, Schwachstellen und vorhandenen Schutzmaßnahmen zueinander in Bezug gesetzt werden. Eine präzise, realistische Schätzung ist nur möglich, wenn entsprechende Erfahrungswerte und Statistiken vorliegen; [Ecke09] betont die starke Abhängigkeit zwischen Eintrittswahrscheinlichkeiten und szenarienspezifischen Angreifermodellen, so dass sich von Dritten veröffentlichte Statistiken nur für grobe Annäherungen eignen. Da sich alle der vier genannten Teilaspekte von IT-Risiken jedoch ständig weiterentwickeln, gestaltet sich eine szenarienspezifische Langzeitbeobachtung praktisch jedoch häufig unmöglich. Um eine ausreichend zuverlässige Einschätzung zu erzielen, führen die meisten Risikomanagementmethoden eine qualitative Beurteilung von Eintrittswahrscheinlichkeiten ein, die im weiteren Verlauf als diskrete Werte quantifiziert werden können. NIST SP 800-30 sieht beispielsweise die folgenden drei Wahrscheinlichkeitsstufen (engl. *likelihood levels*) vor:

- **High**: Die Bedrohung wird von einem sehr motivierten und qualifizierten Angreifer ausgeübt und es gibt keine ausreichenden Schutzmaßnahmen für die vorhandene Schwachstellen.
- **Medium**: Die Bedrohung geht von einem durchaus motivierten und qualifizierten Angreifer aus, aber es sind Schutzmaßnahmen vorhanden, die ein Ausnutzen der vorhandenen Schwachstelle verhindern können.
- **Low**: Motivation oder Fähigkeit potentieller Angreifer sind gering oder es existieren Schutzmaßnahmen, die ein Ausnutzen der Schwachstelle zuverlässig verhindern.

Diese Vorgaben des NIST sind dabei bewusst keine präzise formulierte, vollständige und disjunkte Einteilung; vielmehr soll eine szenarienspezifische Anzahl von Wahrscheinlichkeitsstufen und eine dazu passende Klassifizierung angeregt werden, die einen guten Kompromiss aus einfacher Anwendbarkeit und für die weiteren Schritte hinreichender Differenzierung der IT-Risiken ermöglicht. Diesem Ansatz entsprechend sieht der Risk Management Guide von Microsoft [DPR06] beispielsweise vor, die qualitative Einteilung in die Stufen *low*, *medium* und *high* durch die Verwendung einer Skala mit den Werten 0–10 zu verfeinern, so dass eine weitere Untergliederung niedriger und mittlerer Eintrittswahrscheinlichkeiten in jeweils vier Stufen (0–3 und 4–7) bzw. der hohen Eintrittswahrscheinlichkeiten in drei Stufen (8–10) vorgenommen wird.

Eine schwerpunktmäßig an den identifizierten Schwachstellen orientierte Unterstützung bei der Einordnung von Bedrohungen ermöglicht beispielsweise das in Abschnitt 6.3.2.3 beschriebene Verfahren CVSS2. Alle derzeit praxisrelevanten Ansätze kommen dabei mit maximal rund einem Dutzend qualitativer Einstufungen aus. Die außerhalb des IT-Risikomanagements bekannte Bestimmung exakter Prozentangaben für die Eintrittswahrscheinlichkeit liefert in der Praxis zu selten zuverlässige Werte: Nach [Ande08, S. 846f.] droht dabei vielmehr die Gefahr, dass die Wahrscheinlichkeiten nachträglich wieder angepasst werden müssen, um überhaupt plausible Ergebnisse des gesamten Risikomanagementprozesses erzielen zu können.

Die Konzepte von Security-Frameworks können im Rahmen der von ihnen betrachteten Assets, Angreifermodelle, Angriffe und Schwachstellen durch Hintergrundinformationen und die Erläuterung von Prioritäten dazu beitragen, die Bedrohungen in einem konkreten Szenario besser bezüglich ihrer Eintrittswahrscheinlichkeit beurteilen zu können. Da Security-Frameworks jedoch explizit szenarienunabhängig und die Eintrittswahrscheinlichkeiten zwingend szenarienspezifisch sind, führt kein Weg an szenarienspezifischen Analysen vorbei.

6.3.2.2. Einschätzung der Auswirkungen eines Schadereignisses

In diesem Schritt müssen möglichst alle Auswirkungen eines erfolgreichen Angriffs bzw. des Eintretens eines Schadereignisses ermittelt und bewertet werden; die Bewertung umfasst dabei nach Möglichkeit die Quantifizierung in Form des zu erwartenden finanziellen Schadens für ein einmaliges Eintreten des Schadereignisses. Zur Bestimmung muss im Allgemeinen zwischen *unmittelbaren Schäden* und *Folgeschäden* differenziert werden.

Der aus einem Schadereignis resultierende unmittelbare Schaden setzt sich prinzipiell wiederum aus zwei Bestandteilen zusammen:

- Schaden während des Angriffs: Fällt ein IT-System beispielsweise aufgrund eines Denial-of-Service-Angriffs mehrere Stunden lang aus, so können sowohl andere IT-Systeme als auch die von allen betroffenen IT-Systemen abhängigen Geschäftsprozesse davon in Mitleidenschaft gezogen werden. Die damit verbundenen finanziellen Schäden können im Allgemeinen gut abgeschätzt bzw. quantifiziert werden; Anhaltspunkte können beispielsweise eine Abschätzung der Anzahl der in diesem Zeitraum nicht arbeitsfähigen Mitarbeiter oder der mit dem Ausfall einer E-Commerce-Webseite im Durchschnitt entgangenen Neuaufträge liefern.
- Analyse- und Reparaturkosten: Im unmittelbaren Zusammenhang mit dem Angriff müssen Maßnahmen durchgeführt werden, um beispielsweise durch die Neuinstallation von Systemen die Schäden des Angriffs beseitigen, IT-forensische Aktivitäten durchzuführen und die betroffenen Kunden und Anwender zu informieren. Dadurch werden Kosten verursacht, die im Allgemeinen ebenfalls noch vergleichsweise einfach konkret quantifiziert werden können.

Ein Folgeschaden tritt hingegen im Allgemeinen erst unbestimmte Zeit nach Abschluss des Angriffs und insbesondere dann ein, wenn die Integrität oder Vertraulichkeit von IT-Systemen und Daten verletzt wurde. Fertigt ein Angreifer beispielsweise eine Kopie der Kundendatenbank an, so steht diese dem betroffenen Unternehmen nach wie vor zur Verfügung, so dass kein unmittelbarer finanzieller Schaden entstanden ist. Die Auswirkungen des Vorfalls beispielsweise im Hinblick auf den Datenschutz und das damit verbundene Vertrauen der Kunden verursachen jedoch Folgeschäden, deren genaue Abschätzung häufig sehr schwierig ist. Analog dazu kann eine unbemerkte Integritätsverletzung, die z. B. daraus resultiert, dass der Angreifer gezielte Modifikationen am Datenbestand vornimmt, ohne dass diese Aktionen protokolliert werden, zu Folgeschäden führen, wenn die entsprechenden Daten später unter der falschen Annahme ihrer Korrektheit weiterverarbeitet werden.

Diese Beurteilung steht somit vor den Schwierigkeiten, einerseits eine möglichst vollständige Liste möglicher Folgeschäden pro Schadereignis definieren und andererseits jeden einzelnen Folgeschaden möglichst exakt quantifizieren zu müssen. Aufgrund des damit verbundenen Aufwands und der häufig bewussten, aber unvermeidlichen Ungenauigkeit der Quantifizierung werden in der Praxis häufig entweder pauschale Obergrenzen für den zu erwartenden finanziellen Schaden verwendet oder es wird wiederum eine qualitative Kategorisierung vorgenommen, die den Ereignissen beispielsweise *geringen*, *mittleren* oder *hohen* Folgeschaden zuordnet. Analog zur qualitativen Beurteilung der Eintrittswahrscheinlichkeit muss die Anzahl der Kategorien ausreichend groß gewählt werden, um im nächsten Schritt eine ausreichende Differenzierung zwischen den betrachteten Risiken zu ermöglichen. Insbesondere sollte auch

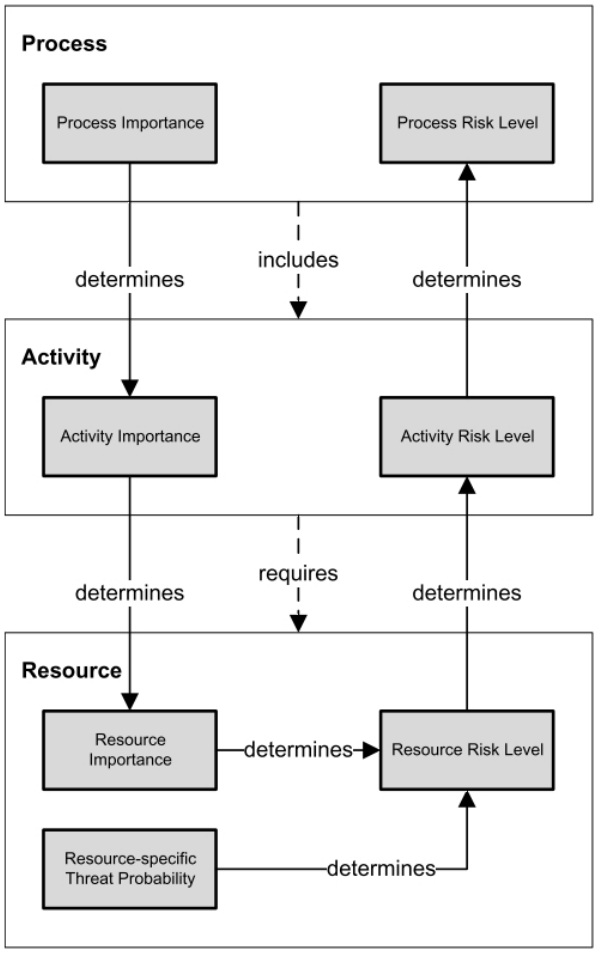


Abbildung 6.8.: Zusammenhänge zwischen Prozessen und IT-Ressourcen im Kontext des Risikomanagements (Quelle: [Fen10])

beachtet werden, dass eine Kosten-/Nutzenanalyse zur Beurteilung möglicher Gegenmaßnahmen (vgl. Abschnitt 6.3.3) nur durchgeführt werden kann, wenn die Kosten für Schadereignisse zumindest grob bekannt sind. Falls die Folgeschäden nicht ausreichend genau quantifizieren werden können, können lediglich die unmittelbaren Schäden herangezogen werden.

Die in Abbildung 6.8 dargestellten grundlegenden Zusammenhänge zwischen Geschäftsprozessen, deren Teilaktivitäten und den wiederum zu deren Umsetzung notwendigen IT-Ressourcen werden beispielsweise im Ansatz von Fenz [Fen10] genutzt, um aus technischen Bedrohungen für Assets auf die potentiell auf Ebene der Geschäftsprozesse entstehenden Schäden zu schließen. Dazu wird die Bedeutung jedes Assets A pro Geschäftsprozess P durch ein Gewicht G_{A_P} bewertet, so dass ein einmalig eintretendes Schadereignis in Relation zum finanziellen Wert des Geschäftsprozesses quantifiziert werden kann. Komplexere Abhängigkeiten können über die Gegenüberstellung von Angriffsbäumen mit so genannten *Mission Trees* abgebildet und ausgewertet werden [CDH05]; Geschäftsprozesse bzw. -ziele werden dabei analog zu Fenz auf die relevanten IT-Assets und deren Schwachstellen abgebildet, für die Dekomposition können

dabei jedoch beliebig viele Hierarchiestufen genutzt werden.

Da die zu betrachtenden Geschäftsprozesse szenarienspezifisch sind, können Security-Frameworks keinen expliziten Beitrag zu dieser Analyse leisten, der über einen Vorschlag, welche IT-Assets zusammenhängend betrachtet werden sollen, hinausgeht. Diese Informationen müssen in der Praxis jedoch auch unabhängig vom Einsatz von Security-Frameworks vorliegen und werden beispielsweise durch das Configuration Management bzw. eine CMDB zur Verfügung gestellt; in Abschnitt 6.4.4.3 wird vorgestellt, wie zu diesem Zweck auch an Security-Frameworks angepasste Managementplattformen eingesetzt werden können.

6.3.2.3. Quantifizierung von IT-Risiken

Mit der Bestimmung der Eintrittswahrscheinlichkeit im Betrachtungszeitraum und der Schätzung der beim Eintreten entstehenden Schäden werden die Voraussetzungen geschaffen, um die IT-Risiken quantifizieren zu können. Nach Baskerville fungiert das Risikomanagement damit auch als Kommunikationswerkzeug, das spezialisiertes, IT-sicherheitsspezifisches Wissen auf fiktive Geldwerte abbildet, die den Denkweisen der Investitionsentscheider auf Managementebene besser entsprechen (vgl. [Bas91]).

Im einfachsten Fall wurden die Wahrscheinlichkeiten und Schäden in den beiden vorangegangenen Schritten bereits quantitativ ermittelt. Das Risiko wird in diesem Fall durch die eingangs auf Seite 6.3 bereits erwähnte Multiplikation von Wahrscheinlichkeit und Schaden als so genannte *Single Loss Expectancy* (SLE, finanzieller Verlust beim einmaligen Eintreten eines Schadereignisses) ausgedrückt; durch Normierung des Betrachtungszeitraums auf ein Jahr bei der Bestimmung der Eintrittswahrscheinlichkeit kann die praktisch oft verwendete *Annual Loss Expectancy* (ALE, jährlich erwarteter finanzieller Verlust aufgrund des vorliegenden Risikos) abgeleitet werden.

Aufgrund ungenauer Schätzungen sowohl der Wahrscheinlichkeiten als auch der resultierenden Schäden eignet sich die ALE primär zur Priorisierung der IT-Risiken, die wie in Abschnitt 6.3.3 beschrieben zur gezielten Auswahl zu treffender Gegenmaßnahmen benötigt wird. Für die Weiterverwendung der Ergebnisse der Risikoanalyse im Rahmen des Finanzwesens wird hingegen beispielsweise eine Erweiterung zum *Perceived Composite Risk* (PCR, siehe [BGL08]) vorgenommen, das bei der Betrachtung aller Risiken eines Assets eine Differenzierung zwischen den insgesamt *erwarteten Verlusten* mit dem Mittelwert $E[X]$ und dem Anteil der *schwerwiegenden Verlusten* mit dem Mittelwert $E[X|X \geq T]$ vornimmt und zusätzlich die Standardabweichung σ aller Einzelverluste X berücksichtigt; diese Werte werden linear kombiniert:

$$\mathrm{PCR} = E[X] + \tfrac{b}{a}E[X|X \geq T] + \tfrac{c}{a}\sigma$$

Der Schwellenwert T und die Gewichte a, b und c, deren Summe 1 ergeben muss, müssen szenarienspezifisch gewählt werden und reflektieren die unternehmensspezifische Risikoneigung.

Sofern in mindestens einem der beiden vorangegangenen Risikomanagementschritten lediglich qualitative Einschätzungen vorgenommen wurden, können z B. *niedrige*, *mittlere* und *hohe* Wahrscheinlichkeiten bzw. Schäden auf zum Szenario passende diskrete Werte abgebildet werden. NIST SP 800-30 empfiehlt bezüglich der Wahrscheinlichkeiten beispielsweise die

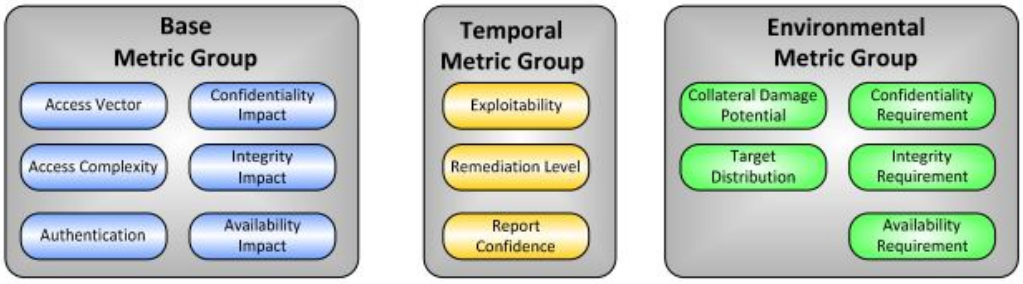


Abbildung 6.9.: Metriken zur Analyse von Schwachstellen nach CVSS2 (Quelle: [MSR07])

Quantifizierung mit 10%, 50% und 100%, so dass ein Risiko mit der Wahrscheinlichkeit *hoch* durchschnittlich genau einmal im Betrachtungszeitraum eintritt.

Für den Fall, dass sowohl Eintrittswahrscheinlichkeiten als auch zu erwartende Schäden ausschließlich qualitativ beurteilt werden konnten, eignet sich die resultierende Quantifizierung aufgrund der inhärenten Ungenauigkeit nicht für Anwendungen im Finanzwesen. Um die IT-Risiken in diesem Fall dennoch vergleichbar zu machen, bieten sich Methoden an, die eine bessere Differenzierung unter Hinzunahme weiterer qualitativer Kriterien ermöglichen. Im Folgenden werden dazu mit CVSS2 [MSR07] bzw. DREAD [MMD+03] zwei Verfahren skizziert, die sich an den für die Assets identifizierten Schwachstellen bzw. Bedrohungen orientieren und auf die Erstellung einer Rangfolge der betrachteten Risiken abzielen.

Die Anwendbarkeit des Common Vulnerability Scoring Systems (CVSS) basiert darauf, dass Verwundbarkeiten auf technischer Ebene bereits in sehr vielen Fällen – beispielsweise über die Common Vulnerabilities and Exposures (CVE) Datenbasis [MIT11b] – öffentlich zugänglich dokumentiert werden. Die korrekte Interpretation der somit einheitlich dokumentierten Schwachstellen erfordert jedoch wiederum technisches Fachwissen und eine gute Kenntnis der szenarienspezifischen Gegebenheiten. Um das Risikomanagement zu unterstützen und eine nachvollziehbare Interpretation bekannter Schwachstellen zu ermöglichen, wurden in der Forschung und von einigen Herstellern Bewertungsschemata entwickelt, von denen sich CVSS, das 2007 in seiner zweiten Version veröffentlicht wurde, als Referenz in der Wissenschaft und als de facto Standard in der Praxis durchgesetzt hat. Das von NIST und CMU gemeinsam entwickelte Verfahren betrachtet für jede Schwachstelle die drei in Abbildung 6.9 dargestellten Metrikgruppen (engl. *CVSS metric groups*):

1. **Base Metric Group**: Die erste Gruppe umfasst sechs Angaben, die die Art des zur Ausnutzung der Schwachstelle erforderlichen Angriffs, den dafür notwendigen Aufwand, Einschränkungen relevanter Angreifermodelle auf legitime Benutzer sowie die Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit bewerten. Die ersten drei Angaben korrelieren im Allgemeinen direkt mit den Eintrittswahrscheinlichkeiten, da ein von anonymen Angreifern einfach über das Internet durchzuführender Angriff aus offensichtlichen Gründen häufig wahrscheinlicher eintritt als ein nur von eigenen Mitarbeitern mit erheblichem Aufwand im lokalen Netz ausführbarer Angriff. Alle sechs Metriken sind qualitativ, wobei für jede Metrik eine von drei Optionen auf Basis eines in der CVSS2-Dokumentation beschriebenen Verfahrens zu wählen ist. Die Metriken in dieser Gruppe

sind szenarienunabhängig und konstant; sie werden beispielsweise in Herstellerberichten über neu entdeckte Schwachstellen genannt und müssen somit nicht im Rahmen des szenarienspezifischen Risikomanagements bestimmt werden, woraus sich die mit dem Verfahren häufig assoziierte Arbeitserleichterung ergibt.

2. **Temporal Metric Group**: Die zweite Gruppe umfasst drei Metriken und berücksichtigt zeitliche Abhängigkeiten bei der Behandlung von Schwachstellen. Sie beurteilt erstens den aktuellen Grad der Ausnutzbarkeit (engl. *exploitability*) der Schwachstelle, die unter anderem davon abhängt, ob entsprechende Schadsoftware nur Insidern oder bereits weltweit frei zugänglich ist. Zweitens wird untersucht, wie die Schwachstelle behoben werden kann, beispielsweise indem szenarienspezifische Workarounds implementiert werden müssen oder indem zwischenzeitlich durch den Hersteller zur Verfügung gestellte Softwareaktualisierungen eingespielt werden. Schließlich wird noch die Zuverlässigkeit des Berichts über die Schwachstelle ausgewertet; hierbei wird beispielsweise zwischen noch unbestätigten Gerüchten und einer offiziellen Bestätigung der Schwachstelle durch den Hersteller unterschieden. Die entsprechenden qualitativen Einstufungen stellen eine Momentaufnahme verschiedener Faktoren der allgemeinen Eintrittswahrscheinlichkeit dar und müssen entsprechend während des Risikomanagements bestimmt werden; sie sind also zeitpunkt-, aber nicht szenarienspezifisch.
3. **Environmental Metric Group**: Die dritte Gruppe bezieht über fünf weitere Metriken die szenarienspezifischen Gegebenheiten in die Bewertung von Schwachstellen ein. Sie beziehen sich jedoch stark auf die szenarienspezifischen Auswirkungen und orientieren sich nicht an den Eintrittswahrscheinlichkeiten. So ist einerseits der Kollateralschaden, der sich aus der erfolgreichen Ausnutzung einer Schwachstelle ergibt, abzuschätzen; so ist beispielsweise anzugeben, ob durch den Angriff Ausfälle im Produktivbetrieb entstehen. Andererseits spielt die (physische oder logische) Verteilung verwundbarer Systeme eine Rolle, beispielsweise in Abhängigkeit davon, ob sich mehrere betroffene Server im selben Subnetz befinden. Schließlich werden auch die szenarienspezifischen Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit der verwundbaren Systeme durch qualitative Einordnungen berücksichtigt.

Wie in Abbildung 6.10 dargestellt ist, werden die bislang rein qualitativen Beurteilungen anschließend zu einem als CVSS-Score bezeichneten quantitativen Ergebnis zusammengeführt. Hierzu gibt CVSS2 sowohl zu jeder qualitativen Stufe jeder Metrik einen konkreten Zahlenwert als auch Gewichte für die Aggregation der Metriken und Metrikgruppen vor. Dabei gelten die folgenden Randbedingungen:

- Jeder resultierende Score liegt zwischen 0.0 und 10.0 und wird auf eine Nachkommastelle gerundet verwendet.
- Die als *Base Score* bezeichnete Gesamtwertung der Basismetriken muss auf jeden Fall bestimmt werden; sie wird wie bereits erläutert für viele Schwachstellen öffentlich dokumentiert.
- Die Gesamtwertung der zeitabhängigen Metriken (*Temporal Score*) ist optional und wird auf Basis des *Base Score* so skaliert, dass der *Temporal Score* nicht höher wird als der *Base Score*, diesen aber auch nicht um mehr als ein Drittel unterschreitet.
- Die Gesamtwertung der umgebungsspezifischen Metriken (*Environmental Score*) ist wiederum optional und wird auf Basis des *Temporal Score* skaliert, so dass der *Environ-*

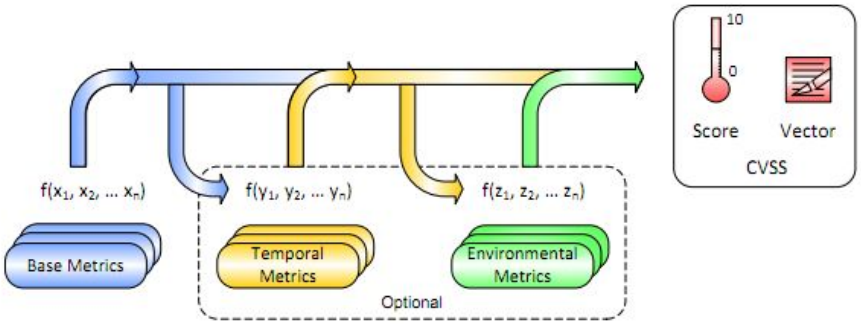


Abbildung 6.10.: Zusammenführen der Metriken nach CVSS2 (Quelle: [MSR07])

mental Score nicht größer als der *Temporal Score* wird.

Diese Randbedingungen zielen darauf ab, dass der veröffentlichte *Base Score* als Obergrenze aufgefasst werden kann. Er kann zu jedem Zeitpunkt durch den *Temporal Score* verfeinert werden, wobei auch diese Aktivität szenarienunabhängig von Dritten als Dienstleistung durchgeführt werden kann; die Risikoquantifizierung reduziert sich dabei im Laufe der Zeit auf bis zu zwei Drittel des *Base Score*. Eine weitere Reduzierung kann sich im Anschluss nur noch szenarienspezifisch durch die Bestimmung des *Environmental Score* ergeben. Der CVSS-Score entspricht somit zunächst dem *Base Score*, der durch *Temporal Score* bzw. *Environmental Score* ersetzt bzw. präzisiert wird. Die verwendeten Quantifizierungen und Gewichte wurden von der CVSS2-Forschungsgruppe empirisch festgelegt, machen zur effizienten praktischen Anwendung entsprechende Werkzeugunterstützung erforderlich und sind Gegenstand einer kontinuierlichen praktischen Bewertung und Weiterentwicklung.

Eine vollständige Anwendung von CVSS2 im Rahmen des Risikomanagements entspricht somit der Bestimmung des *Environmental Scores* für alle identifizierten Schwachstellen; falls jedoch selbst die qualitative Beurteilung der Teilaspekte von Eintrittswahrscheinlichkeiten und Schäden beispielsweise aufgrund des damit verbundenen Aufwands nicht möglich sein sollte, kann der *Base Score* als grobe Näherung verwendet werden.

Demgegenüber stellt das von Microsoft entwickelte DREAD-Verfahren ein besonders einfach anzuwendendes, in der Praxis etabliertes Bewertungsschema dar, das sich an Bedrohungen bzw. Angriffen orientiert und bewusst eine szenarienspezifisch, rein technische Beurteilung vornimmt. Es betrachtet die folgenden Aspekte, aus deren Anfangsbuchstaben sich der Name des Verfahrens ableitet:

- **Damage potential**: Werden durch einen erfolgreichen Angriff a) nur unkritische Daten, b) schützenswerte Daten oder c) administrationsrelevante Daten offengelegt?
- **Reproducibility**: Ist eine Situation, in der ein Angriff erfolgreich sein kann, a) nur sehr aufwändig, b) in wenigen Schritten oder c) mit einfachsten Werkzeugen (z. B. Webbrowser) herbeizuführen?
- **Exploitability**: Kann der Angriff a) nur von Experten, b) mithilfe automatisierender Werkzeuge oder c) auch von Anfängern erfolgreich ausgeführt werden?

- **Affected users**: Sind von einem erfolgreichen Angriff a) nur sehr wenige, b) zahlreiche oder c) alle Benutzer betroffen?
- **Discoverability**: Ist der Angriff a) nur intern, b) einigen Benutzern oder c) öffentlich bekannt?

Zur Auswertung werden die mit *a*, *b* bzw. *c* beantworteten Fragen jeweils mit 0, 5 bzw. 10 Punkten bewertet und anschließend der Mittelwert berechnet; somit ergibt sich analog zu CVSS2 eine Bewertung zwischen 0 und 10, die zur Sortierung aller betrachteten Risiken herangezogen werden kann.

Obwohl CVSS2 in der Praxis häufig dazu eingesetzt wird, Schwachstellen in Softwareprodukten zu dokumentieren, die durch Patches und neue Versionen im Laufe der Zeit behoben werden, eignet sich das Verfahren auch zur Dokumentation inhärenter Schwachstellen, die sich z. B. aus der Systemarchitektur ergeben: Beispielsweise ist ein öffentlich zugänglicher Webserver immer für Denial-of-Service-Angriffe anfällig und benötigt ihm vorgelagerte Schutzmechanismen, da andere Maßnahmen wie eine Abschottung von öffentlichen Netzen dem dahinterstehenden Geschäftsprozess widersprechen würden. Entsprechend bietet es sich an, auch die im Rahmen von Security-Frameworks betrachteten Schwachstellen z. B. mit CVSS2 festzuhalten (vgl. Abschnitt 6.4.3). Das DREAD-Verfahren eignet sich aufgrund seiner einfachen Anwendbarkeit insbesondere für die schnelle Überprüfung szenarienspezifischer Bedrohungen, die z. B. nicht im Rahmen eines in Frage kommenden Security-Frameworks berücksichtigt wurden oder sich möglicherweise durch eigenentwickelte Komponenten, die Security-Frameworks ergänzen sollen, ergeben (vgl. Abschnitt 5.5). Auf diese Weise als hoch eingestufte Risiken sollten im Allgemeinen jedoch zusätzlich quantitativ oder zumindest feiner granuliert mittels CVSS2 analysiert werden.

6.3.3. Maßnahmen zur Risikosteuerung im Kontext von Security-Frameworks

Nach der Bewertung bzw. Quantifizierung von Risiken müssen Maßnahmen zum Umgang mit ihnen festgelegt werden. Dazu wird entweder jedes Risiko einzeln betrachtet, wobei in der Regel vom größten Risiko, das das dringendste Problem darstellt, zum geringsten Risiko vorgegangen wird; oder es werden Gruppen gebildet, die beispielsweise alle mit einem Asset verbundenen Risiken umfassen und somit auf das Erarbeiten einer Gesamtlösung abzielen.

Mögliche Maßnahmen zum Umgang mit (IT-)Risiken lassen sich prinzipiell in die folgenden Kategorien einteilen (vgl. [SP8H30, Ecke09, BSI08b]):

- **Risikoakzeptanz**: Das Risiko wird zur Kenntnis genommen, es wird aber bewusst keine der anderen Maßnahmen ergriffen, beispielsweise weil die damit verbundenen Kosten in keinem brauchbaren Verhältnis zur Verringerung des Risikos stehen. Das langfristige Ziel des Risikomanagements im Zusammenspiel mit einer kontinuierlichen Verbesserung liegt genau darin, möglichst alle Risiken so weit zu reduzieren, dass sie ein akzeptables Niveau erreichen.
- **Risikovermeidung**: Das Risiko wird umgangen, beispielsweise indem die von einer Schwachstelle betroffenen Systeme oder deren diesbezüglich relevante Teile abgeschaltet werden. Diese Maßnahme ist offensichtlich nur dann sinnvoll, wenn der durch das Risiko erwartete Schaden höher ist als derjenige, der sich aus der Umsetzung der Risikovermeidungsstrategie ergibt.

- **Risikoreduktion**: Es werden technische und organisatorische Maßnahmen getroffen, um die Eintrittswahrscheinlichkeit und/oder die Auswirkung des jeweiligen Schadereignisses zu reduzieren. Ein Beispiel zur Umsetzung ist die Inbetriebnahme eines passenden Security-Frameworks. Wie bei der Risikovermeidung ist darauf zu achten, dass die Kosten für die getroffenen Maßnahmen niedriger sein sollten als der erwartete Schaden bei der Akzeptanz des Risikos.
- **Risikoübertragung**: Das Risiko wird beispielsweise über eine Versicherung an einen Dritten übertragen, der für tatsächlich entstehende Schäden aufkommt. Aufgrund sehr teurer Versicherungsprämien ist diese Variante für die meisten Unternehmen zumindest bei IT-spezifischen Risiken jedoch nicht besonders attraktiv (vgl. [Ande08, S. 847]).

Bis zu welcher Obergrenze ein Risiko noch akzeptiert wird, hängt maßgeblich von der generellen unternehmensweiten Einstellung zu dieser Thematik ab, die als Risikoneigung (engl. *risk appetite*) bezeichnet wird. Für ein konkretes Risiko ist somit die Risikotoleranz (engl. *risk tolerance*) zu bestimmen, die sich aus der Abweichung von der Risikoneigung in Bezug auf die potentiell betroffenen Assets ergibt. Die Möglichkeit zur Risikovermeidung bietet sich im Allgemeinen lediglich bei IT-Systemen, die bislang mit unnötiger Zusatzfunktionalität betrieben wurden, die ohne Auswirkungen auf die Geschäftsprozesse deaktiviert werden kann. Die Außerbetriebnahme von Systemen zur Risikovermeidung ist jedoch im Allgemeinen keine längerfristig akzeptable Lösung bzw. würde es erfordern, zusammen mit den betroffenen IT-Assets auch die Geschäftsprozesse umzustrukturieren. Da auch die Risikoübertragung an Dritte in der Praxis meist kein ökonomisch sinnvoller Weg ist, stellt die Risikoreduktion im Allgemeinen das Mittel der Wahl dar, die in einem Umfang betrieben werden muss, bis sich ein im Rahmen der Risikotoleranz akzeptables Restrisiko ergibt.

Security-Frameworks unterstützen das Risikomanagement in diesem Bereich dadurch signifikant, dass sie für definierte Mengen von Assets, Angriffen und Schwachstellen darauf genau abgestimmte Maßnahmen vorschlagen, die der Risikoreduktion dienen. Sie bieten durch ihre Modularität zudem die Möglichkeit, den Umfang der Schutzmaßnahmen auf das szenarienspezifisch akzeptable Restrisiko abzustimmen, um auch das Kosten-/Nutzverhältnis beachten zu können.

Das Vorgehen in dieser Phase des Risikomanagements entspricht nach NIST SP 800-30 dem folgenden, aus sieben Teilschritten bestehenden Ablauf, der anschließend unter dem Aspekt des Einsatzes von Security-Frameworks modifiziert wird:

1. Priorisierung der Risiken durch Anordnung in absteigender Reihenfolge, d.h. die größten Risiken werden zuerst behandelt.
2. Untersuchung in Frage kommender Maßnahmen im Hinblick auf ihre Realisierbarkeit im konkreten Szenario und ihre Effektivität.
3. Erstellen einer Kosten-/Nutzenabschätzung durch Bestimmung der Implementierungs- und sonstigen Bereitstellungskosten und deren Gegenüberstellung mit dem aktuellen bzw. nach Implementierung weiterhin verbleibenden Risiko.
4. Verbindliche Auswahl der umzusetzenden Maßnahmen.
5. Zuweisung der Verantwortlichkeit für das Umsetzen der Maßnahmen an entsprechende Personenkreise.

6. Dokumentation der Risiken, der getroffenen Entscheidungen und der Eckpunkte des Umsetzungvorhabens.
7. Umsetzung der ausgewählten Maßnahmen und Bestimmung des verbleibenden Risikos.

Die Schritte 2–7 lassen dabei direkt auf den Einsatz von Security-Frameworks abbilden und umfassen dabei jeweils Kernaspekte der in Kapitel 5 diskutierten Phasen der Instanzlebenszyklen von Security-Frameworks:

- Die von NIST SP 800-30 in Schritt 2 geforderte Untersuchung in Frage kommender Maßnahmen deckt sich mit der Auswahl geeigneter Security-Frameworks (Lebenszyklusphase 1, siehe Abschnitt 5.4), die auf einer Gegenüberstellung der im Frameworkkonzept berücksichtigten Assets, Angriffe, Schwachstellen und Gegenmaßnahmen mit den szenarienspezifischen Anforderungen – konkret also mit den aktuell betrachteten Risiken – beruht.
- Die im obigen Schritt 3 geforderte Kosten-/Nutzenabschätzung entspricht der Budgetanalyse im Rahmen der in Abschnitt 5.5 beschriebenen Customizingphase. Sie setzt voraus, dass im Rahmen der szenarienspezifischen Anpassungen des Frameworkkonzepts in denjenigen Bereichen, für die das Security-Framework mehr als eine Implementierungsvariante anbietet, bereits eine entsprechende szenarienspezifische Auswahl getroffen wurde und bereitet somit den vierten Schritt der NIST-Vorgehensweise fachlich vor; sie umfasst über die von NIST genannten Forderungen hinausgehend auch eine Betrachtung der später anfallenden laufenden Betriebskosten.
- Die Schritte 4–7 überlappen sich mit den Lebenszyklusphasen 2–4 von Frameworkinstanzen, die eine Genehmigung des szenarienspezifisch angepassten Frameworkkonzepts sowie seine Implementierung und Inbetriebnahme mit den in Kapitel 5 jeweils genannten Dokumenten umfassen (vgl. Abschnitte 5.5–5.7).

Die Beurteilung des verbleibenden Restrisikos entspricht einem erneuten Durchlaufen der Risikoanalyse unter Berücksichtigung der auf Basis des Security-Frameworks geplanten Schutzmaßnahmen und somit einem Rücksprung zum in Abschnitt 6.3.1.4 beschriebenen letzten Schritt in der ersten Phase des Risikomanagementablaufs. Dabei muss überprüft werden, ob die durch das ans Szenario angepasste Security-Framework geplanten Maßnahmen ausreichen, so dass das Restrisiko unterhalb der Risikoakzeptanzschwelle liegt, oder ob noch zusätzliche Maßnahmen ergriffen werden müssen.

6.3.4. Umsetzung der Risikosteuerung und prozessuale Einbettung

Unter anderem aufgrund der laufenden Weiterentwicklung der szenarienspezifischen IT-Infrastruktur, sich wandelnder Bedrohungen und neu entdeckter Schwachstellen ist das Risikomanagement keine einmalige Tätigkeit, sondern ein immer wieder durchlaufener Prozess, der die bereits vorhandenen Ergebnisse auf den jeweils aktuellen Stand bringt. In Abhängigkeit von der Größe und Komplexität des Szenarios wird er typischerweise mindestens einmal pro Jahr organisationsweit durchlaufen und bei Bedarf für Teilbereiche, z. B. bei Asset-spezifischen lokalen Änderungen oder nach Änderungen an dienstspezifischen Policies, häufiger angestoßen. Durch die Bestimmung des aktuell vorhandenen (Rest-)Risikos nimmt dieser Prozess eine Kontrollaufgabe wahr, die sich sowohl auf die Einhaltung der sicherheitsspezifischen Policies als auch die Umsetzung der ausgewählten Gegenmaßnahmen bezieht.

Wie auch bei anderen Prozessen hängt der Erfolg des Risikomanagements von einer Reihe von Faktoren ab, die von den Standards und Best Practices stark betont werden: So sind beispielsweise die klare Unterstützung durch die Unternehmensführung, die Kompetenz der damit beauftragten Mitarbeiter und die Unterstützung durch die Geschäftsprozesseigner und IT-Administratoren zwingende Voraussetzungen für die Effektivität des Risikomanagements. Neben den für die Informationsakquisition und -bewertung relevanten fachlichen Schnittstellen, die bei den einzelnen Schritten bereits genannt wurden, ergeben sich analog zur Darstellung in Abschnitt 6.5 prozessuale Schnittstellen, von denen die folgenden drei besonders zu betonen sind:

1. **Change Management**: Änderungen an der IT-Infrastruktur, beispielsweise durch die Integration weiterer IT-Dienste oder die Umkonfiguration bestehender IT-Systeme, können mit Auswirkungen auf die IT-Sicherheit verbunden sein. Im Rahmen des Change Management ist beispielsweise das Change Advisory Board dafür zuständig, die Auswirkungen von Änderungen im Rahmen ihrer Genehmigung zu berücksichtigen. Die Bestimmung IT-sicherheitsrelevanter Auswirkungen entspricht dabei genau dem Durchlaufen des IT-Risikomanagements mit dem Ziel, notwendige Anpassungen der Sicherheitsmaßnahmen rechtzeitig anzustoßen, so dass durch die geplante Änderung keine inakzeptabel hohen IT-Risiken entstehen.

2. **Event Management** bzw. **Security Incident Management**: Durch den planerischen Charakter des Risikomanagements und die zunächst mangels praktischer Erfahrung oft ungenauen Schätzungen sind sicherheitsrelevante Vorfälle kontinuierlich auszuwerten; sofern sich signifikante Abweichungen z. B. von den geschätzten Eintrittswahrscheinlichkeiten oder Auswirkungen von Schadereignissen abzeichnen, müssen die Ergebnisse des Risikomanagements entsprechend korrigiert werden.

3. **Financial Management**: Da die Umsetzung von IT-Schutzmaßnahmen ökonomisch nur dann sinnvoll ist, wenn Schäden in einem Umfang verhindert oder reduziert werden, der über die damit verbundenen Kosten hinausgeht, kommt dem IT-Risikomanagement eine Schlüsselposition im Bezug auf das IT-Sicherheitsbudget zu. Trotz der anhaltenden Bemühungen zahlreicher Hersteller von IT-Sicherheitsprodukten, den aus Investitionskalkulationen bekannten *Return on Invest* (RoI) auf eine als *Return on Security Invest* (RoSI) bezeichnete Kennzahl auszudehnen, muss berücksichtigt werden, dass das Sicherheitsmanagement generell nur Schäden eingrenzen, aber keine direkten Umsatzsteigerungen generieren kann.

Insbesondere die beiden letzten Aspekte wirken sich unmittelbar auf den Einsatz und das Management von Security-Frameworks aus: Zum einen müssen die mit der Bereitstellung und dem Betrieb des Security-Frameworks verbundenen Kosten kalkulierbar sein, wobei sich durch die gezielte Bündelung und die angestrebte Vollständigkeit seiner Schutzmaßnahmen im Allgemeinen auch finanzielle Vorteile gegenüber einer Reihe von Einzelmaßnahmen ergeben. Zum anderen spielt die bereits in Kapitel 3 geforderte Überwachung sicherheitsrelevanter Ereignisse und deren Aufbereitung, z. B. in Form von zielgruppenspezifischen Berichten, eine wesentliche Rolle bei der kontinuierlichen Beurteilung der Effektivität und Rentabilität von Security-Frameworks.

6.3.5. Zusammenfassende Einordnung Security-Framework-spezifischer Aspekte in Risikomanagementstandards

Die in den Abschnitten 6.3.1 bis 6.3.4 vorgestellten Aufgaben und Abläufe im Risikomanagement orientieren sich an der Strukturierung von NIST SP 800-30; in diesem Abschnitt werden die Beiträge, die Security-Frameworks zum Risikomanagement liefern können, ergänzend in eine Gegenüberstellung aktueller Standards und Best Practices zum Risikomanagement eingeordnet. Die vorgestellten Ansätze verfolgen zwar alle dasselbe wesentliche Ziel, unterstützen ihre Anwender aber jeweils unterschiedlich und geben über die Beschreibung des Ablaufs hinaus weitere Anregungen für die unternehmensspezifische Umsetzung des Risikomanagements; diese lassen sich, wie nachfolgend gezeigt wird, auf Security-Frameworks übertragen bzw. an diese anpassen.

Abbildung 6.11 zeigt das Ergebnis einer im Rahmen dieser Arbeit durchgeführten Gegenüberstellung der einzelnen Phasen und Schritte des Risikomanagements, für die neben NIST SP 800-30 die folgenden Standards und Best Practices ausgewertet wurden:

- **ISO/IEC 27005**: Die ISO/IEC-Norm zum *Information Security Risk Management* [I27005] wurde 2008 und damit drei Jahre nach ISO/IEC 27001 ratifiziert. Sie umfasst 55 Seiten und präzisiert die bereits in ISO/IEC 27001 geforderten Risikomanagement-Schritte, indem sie wiederum in Anlehnung an den PDCA-Zyklus einen Risikomanagementprozess definiert und auf Risikobehandlungsmethoden, die unternehmensinterne Risikokommunikation und die kontinuierliche Überwachung der Risiken eingeht. Analog zu den anderen Normen der Reihe ISO/IEC 27000 liegt der Fokus auf der Einführung und kontinuierlichen Verbesserung eines formalen, dokumentierten Prozesses; im Anhang der Norm werden jedoch auch Beispiele für typische Bedrohungen sowie exemplarische Methoden zur Bewertung von Schwachstellen vorgestellt.
- **Microsoft Security Risk Management Guide**: Der Risikomanagement-Leitfaden von Microsoft [DPR06] beschreibt unabhängig von den hauseigenen Produkten das Zusammenspiel zwischen IT und Risikomanagement in Unternehmen. Es wendet sich dabei sowohl an die Techniker, die fachliche Inhalte zum Risikomanagement beitragen müssen, als auch an die Entscheiderebene, die IT-spezifische Risiken mit berücksichtigen muss. Die beiden vorrangigen Ziele sind somit, Entscheidungshilfen bezüglich des Einsatzes technischer Sicherheitsmaßnahmen zu liefern und deren Effektivität zu überwachen (vgl. Phasenbezeichnungen *Conducting decision support* und *Measuring program effectiveness*). Die praktische Anwendung der beschriebenen Verfahren wird durch eine Reihe frei zugänglicher Dokumentenvorlagen, beispielsweise zur Erfassung und Auswertung von Bedrohungen sowie zur Erstellung von so genannten *Risk Scorecards*, unterstützt.
- **ISACA Risk IT Framework**: Das Risk IT Framework [ISA09] der ISACA hat, analog zum oben bereits diskutierten CobiT, das IT-Management und die Geschäftsleitungsebene als Zielgruppe. In den beschriebenen Prozessabläufen werden technische Aspekte wie die Analyse von Schwachstellen nur beiläufig erwähnt; die Schwerpunkte liegen auf der Analyse möglicher Auswirkungen auf Geschäftsprozesse und den Zuständigkeiten des Managements. Das Risk IT Framework stellt jedoch auch einige Methoden bereit, um IT-Risiken unternehmensweit gut verständlich zu kommunizieren: Über so genannte Bedrohungsszenarien werden die wesentlichen Aspekte von identifizierten Bedrohungen dokumentiert (vgl. Abbildung 6.12) und *Key Risk Indicators* übertragen das z. B. aus

Phase (wie in dieser Arbeit verwendet)	Arbeitsschritt	Standards bzw. Best Practices NIST SP 800-30	ISO/IEC 27005	Microsoft Security Risk Management Guide	ISACA Risk IT Framework	OCTAVE
Risikoermittlung	**Risk Assessment**	**Risk Identification**	**Assessing Risk**			**Organizational/technical view**
	Identifizieren von Assets	System characterization	Identification of assets	Planning	Descr. business impact	Asset profile/containers
	Identifizieren von Bedrohungen	Threat identification	Identification of threats	Data gathering	IT risk scenarios	Threat scenarios
	Identifizieren von Schwachstellen	Vulnerability identification	Identification of vulnerabilities	Priorization		Identify risks
	Identifizieren von Schutzmaßnahmen	Control analysis	Identification of existing controls			Current practices
Risikobewertung	**Bewertung der Eintrittswahrscheinlichkeiten**	(Risk Assessment)	**Risk Estimation**	**Decision Support**	**Risk Evaluation**	**Analyze risks**
	Bewertung der Auswirkungen	Likelihood determination	Assessment of incident likelihood	Probability	Data gathering	Probability
	Risikoquantifizierung	Impact analysis	Assessment of consequences	Impact	Analysis	Impact value
		Risk determination	**Risk Evaluation**	Requirements	Risk profile	Risk score
		Control recommendations		Solutions		
		Results documentation		Cost-benefit analysis		
Risikosteuerung	**Risk Mitigation**	**Risk Treatment**	**Implementing Controls**		**Risk Response**	
	Vorgehensmöglichkeiten	Mitigation options	Risk treatment options	Holistic approach	Communication	Strategy and plan
	Maßnahmenauswahl	Mitigation strategy	Risk treatment plan	Mitigation strategy	Response selection	Select mitigation approach
	Maßnahmenumsetzung	Control implementation	Risk treatment	Organize solutions	Manage risks	Mitigation plan
		Cost-benefit analysis	Risk acceptance		React to events	Residual risk
		Residual risk			Key risk indicators	
Prozessuale Einbettung	**Evaluation and Assessment**	**Risk Management Process**	**Measuring Effectiveness**		**Risk Governance**	**Using OCTAVE**
	Risikomanagementprozess	Good security practice	Risk monitoring and review	Measure controls	Process model	Resources, responsibilities
	Schnittstellen zu anderen Prozessen	Keys for success	Risk communication	Risk scorecard	Common risk view	Assessment workshops
				Integration with non-IT risks	Business integration	

Abbildung 6.11.: Vergleich der Phasen und Arbeitsschritte von Standards und Best Practices zum Risikomanagement

Abbildung 6.12.: Bestandteile von Risikoszenarien laut ISACA Risk IT Framework (Quelle: [ISA09])

ITIL bekannte Konzept von KPIs auf das Risikomanagement, so dass die aktuellen Ausprägungen ausgewählter IT-Risiken immer im Blick behalten werden und beispielsweise auch als Dienstgütemerkmale in SLAs integriert werden können.

- **OCTAVE**: Die Methode *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE, [ADA01]) wurde von der CMU zunächst für das Risikomanagement in großen Unternehmen entwickelt, bietet inzwischen mit den Varianten OCTAVE-S und OCTAVE Allegro aber auch Vereinfachungen für kleinere Organisationen und Arbeitsgruppen an. Trotz des Fokus auf IT-Risiken zeichnet sich OCTAVE dadurch aus, dass es sich nicht auf bereits elektronisch erfasste Informationen über die IT-Infrastruktur verlässt, wie dies beispielsweise beim Einsatz von netzbasierten Vulnerability-Scannern der Fall wäre, sondern das Risikomanagement als Reihe von Workshops organisiert, in denen zueinander komplementäre Sichten auf die IT-Risiken erfasst, bewertet und aufbereitet werden. Dadurch sollen auch Unternehmen, die keine IT-Sicherheitsexperten involvieren können, mit möglichst geringem Aufwand zu brauchbaren Analyseergebnissen gelangen können. Der Schwerpunkt von OCTAVE liegt somit auf der Ermittlung der zur Risikobewertung notwendigen Informationen; demgegenüber wird auf die Auswahl, Umsetzung und Abnahme von Schutzmaßnahmen nicht näher eingegangen. Die Anwendung von OCTAVE wird durch eine sehr umfangreiche Sammlung von Dokumentenvorlagen für schriftliche Interviews und die Durchführung der OCTAVE-Workshops unterstützt.

Analog zu den Standards und Best Practices zum Sicherheitsmanagementprozess weisen auch die Dokumentationen dieser Risikomanagementmethoden unterschiedliche Abstraktionsgrade auf: Während ISO/IEC 27005 im Kern aus der abstrakten Beschreibung eines Referenzprozesses besteht und im Anhang Beispiele in Form von Aufzählungen unter anderem typischer Bedrohungen gibt, demonstriert OCTAVE die Anwendung seiner Dokumentenvorlagen anhand eines fiktiven Szenarios, für das diverse konkrete Bedrohungen analysiert und Schritt für

Schritt mit der OCTAVE-Methode bewertet werden. Dennoch wird in vielen Organisationen der pragmatische Ansatz verfolgt, dass die Risikomanagementmethoden lediglich Anregungen für die Planung und Umsetzung eines eigenen, szenarienspezifischen Risikomanagementprozesses dienen und nicht exakt befolgt werden. Als Vorteil erweist sich dabei die flexible Kombinierbarkeit der Verfahren: Während sich die stark interview- und gruppenarbeitsbasierte Vorgehensweise OCTAVE besonders für die Ersterfassung von Risiken eignet, ergänzen sich die Schwerpunkte des Microsoft Security Risk Management Guide – IT-Risikomanagement zwischen technischer Ebene und IT-Management – und des ISACA Risk IT Frameworks, das das Zusammenspiel zwischen unternehmensweitem und IT-spezifischen Risikomanagement aufzeigt, gegenseitig; ferner liegt bei Unternehmen, die ihr Sicherheitsmanagement an ISO/IEC 27001 ausrichten, nahe, ihren Risikomanagementprozess gemäß ISO/IEC 27005 zu spezifizieren, da es sich dabei um eine Verfeinerung des bereits in ISO/IEC 27001 geforderten Vorgehens handelt, das auch für die Zertifizierung relevant ist.

Security-Frameworks tragen, wie bereits in den Abschnitten 6.3.1 bis 6.3.4 dargestellt wurde, im Allgemeinen keine eigenen Risikomanagementschritte bei, sondern ermöglichen eine effiziente Bündelung und Auswertung der in den einzelnen Phasen benötigten Informationen. Im Folgenden wird eine Einordnung anhand zweier generischer Anwendungsfälle vorgenommen, die beim Einsatz von Security-Frameworks relevant sind: Zunächst wird betrachtet, wie in einem Szenario, in dem noch kein umfassender Schutz besteht, Security-Frameworks im Rahmen des Risikomanagements zur Initialplanung eingesetzt werden können. Anschließend werden die Abläufe im Risikomanagement skizziert, wenn Frameworkinstanzen bereits im Einsatz sind und eine kontinuierliche Überwachung und Verbesserung erreicht werden soll.

Bei der initialen Instanziierung des Risikomanagementprozesses für ein konkretes Szenario können Security-Frameworks auf Basis der in dieser Arbeit vorgestellten Konzepte wie folgt genutzt werden:

- Die Festlegung des Anwendungsbereichs der aktuellen Risikoanalyse (engl. *Scoping*) durch Auswahl der szenarienspezifischen Assets kann sich an den vom Security-Framework konzeptionell berücksichtigten Assets orientieren. Diese Form der Zusammenfassung aller von einem Security-Framework behandelten Assets entspricht einer Anwendung der von OCTAVE vorgeschlagenen Bildung so genannter Asset-Container. Durch die Betrachtung einer Menge zusammenhängender Assets als Einheit kann die von OCTAVE im weiteren Verlauf angestrebte Vereinfachung durch Umsetzung von Schutzmaßnahmen auf Containerebene statt in der Granularität einzelner Assets erreicht werden (vgl. [CSYW07, S. 11]). Bei Bedarf können die Assets aber wie von den anderen Risikomanagementmethoden impliziert auch einzeln betrachtet werden.
- Bei der Identifizierung relevanter Bedrohungen sind generell sowohl allgemein bekannte als auch szenarien- und assetspezifische Bedrohungen bzw. Angriffe zu berücksichtigen. Security-Frameworks tragen hierzu im Allgemeinen partiell bei, da sie ausgewählte Angreifermodelle und Angriffe berücksichtigen, die, als Ausgangsbasis verwendet, um weitere szenarienspezifische Bedrohungen ergänzt werden müssen. Die Überprüfung der weitestgehenden Vollständigkeit berücksichtigter Angriffe gestaltet sich einfacher, wenn Bedrohungen auch in Frameworkkonzepten einheitlich, beispielsweise auf Basis des in ISO/IEC 27005 verwendeten Vokabulars, benannt werden. Die in Frameworkkonzepten dokumentierten Angreifermodelle können zudem in die vom ISACA Risk IT Framework postulierten Risikoszenarien übernommen werden.

- Analog dazu sind in den Frameworkkonzepten die vom Security-Framework berücksichtigten Schwachstellen dokumentiert und können als Ausgangsbasis für die szenarienspezifische Vervollständigung eingesetzt werden. Die zur Priorisierung notwendige grundlegende Bewertung kann durch Kennzahlen wie den CVSS-Score vereinfacht werden; Frameworkkonzepte können dadurch Obergrenzen für die Risikoeinstufung nennen, die durch die szenarienspezifische Berücksichtigung der lokalen Gegebenheiten präzisiert werden können.
- Bei der Betrachtung vorhandener bzw. geplanter Schutzmaßnahmen kann auf Basis von Security-Frameworks eine Gegenüberstellung der Ausgangssituation, in der das Security-Framework noch nicht eingesetzt wird, mit einer möglichen Zielkonfiguration vorgenommen werden. Da zu diesem Zeitpunkt die Risiken noch nicht quantifiziert wurden und noch keine Entscheidung über das weitere Vorgehen getroffen werden kann, ergibt sich analog zu den Ausführungen über die Auswahl von Security-Frameworks in Abschnitt 5.4 die Herausforderung, dass der Aufwand für ein vollständiges Durchlaufen der Customizingphase zur exakten Bestimmung der passenden Schutzmaßnahmen signifikant hoch wäre. Entsprechend muss eine vorläufige Schätzung vorgenommen werden; optional ist auch die Orientierung an im Frameworkkonzept dokumentierten Anwendungsbeispielen in Erwägung zu ziehen.
- Die zur Bewertung der betrachteten Risiken erforderlichen Beurteilungen von Eintrittswahrscheinlichkeit und Auswirkungen sind szenarienspezifisch und können von Security-Frameworks nur indirekt unterstützt werden, beispielsweise durch Hintergrundinformationen zu Angriffen, deren Zusammenstellung zu *Attack Trees*, die bei der Abschätzung der Eintrittswahrscheinlichkeit herangezogen werden können, und durch die Dokumentation der beim Design des Security-Frameworks zugrunde gelegten, meist qualitativen Priorisierung der Angriffe und Schwachstellen.
- Die von NIST SP 800-30 und dem Microsoft Security Risk Management Guide bereits für die Risikobewertungsphase vorgesehene vorläufige Empfehlung von zu treffenden Maßnahmen wird durch Security-Frameworks vollständig abgedeckt, da es sich genau um im weiteren Verlauf noch zu präzisierende Maßnahmensammlungen handelt, die zumindest einem Teil der im Szenario relevanten Risiken entgegenwirken. Bei einem an Security-Frameworks orientierten Risikomanagement liegen Teilergebnisse der zweiten Phase bereits von Anfang an vor und können ähnlich zum Vorgehensmodell bei CVSS durch die Ergänzung szenarienspezifischer Aspekte verfeinert werden; dieser Aufwand ist für die Korrektheit einer später durchgeführten Kosten-/Nutzenanalyse jedoch zwingend erforderlich, da anderweitig nicht sichergestellt werden kann, dass genau alle szenarienspezifischen Risiken adäquat behandelt werden.
- Insbesondere durch diese Spezifikation von Maßnahmen tragen Security-Frameworks auch dazu bei, die grundlegende Vorgehensweise bei der Risikosteuerung zu wählen. Dabei wird entweder implizit angenommen, dass die verbleibenden Restrisiken akzeptabel sind, oder es wird explizit im Frameworkkonzept bzw. spätestens beim Durchlaufen der Customizingphase dokumentiert, in welchen Bereichen weitere Maßnahmen ergriffen werden müssen. Die beiden dazu alternativen Vorgehensweisen, Risikovermeidung und Risikoübertragung, sind nicht mit der Zielsetzung von Security-Frameworks vereinbar und wie in Abschnitt 6.3.3 erläutert praktisch meist keine effiziente Option.
- Die konkrete Maßnahmenauswahl deckt sich bei der Orientierung an Security-

Frameworks mit den ersten beiden Lebenszyklusphasen ihrer Instanziierung: Auswahl und Anpassung. Diese Vorgehensweise geht davon aus, dass ein Großteil der erforderlichen Maßnahmen aus dem Frameworkkonzept abgeleitet werden kann und zusätzlich benötigte Maßnahmen für weitere Risiken analog zu szenarienspezifisch zur Integration erforderlichen Schnittstellenkomponenten im Rahmen der Anpassungsphase spezifiziert werden können. Andernfalls liefert das Security-Framework zwar Anregungen für zu ergreifende Maßnahmen, im weiteren Verlauf wird jedoch keine im Rahmen des Sicherheitsmanagements zu betrachtende Frameworkinstanz, sondern eine Reihe von Einzelmaßnahmen implementiert.

- Analog zur Maßnahmenauswahl entsprechen die von den Risikomanagementmethoden geforderten Schritte Maßnahmenumsetzung, Kosten-/Nutzenanalyse und Bestimmung des Restrisikos Teilen der Aufgaben, die in Kapitel 5 für die Phasen 2–4 des Lebenszyklus von Frameworkinstanzen spezifiziert wurden.
- Die prozessuale Umsetzung des Risikomanagements unter Orientierung an Security-Frameworks wurde in diesem Kapitel erarbeitet.

Als Zwischenergebnis für die weiteren Betrachtungen liegt somit vor, dass ein am jeweiligen Frameworkkonzept orientierter Durchlauf des Risikomanagementprozesses dazu geführt hat, dass zur Minderung der identifizierten Risiken ein ans jeweilige Szenario angepasstes Security-Framework instanziiert wird. Weitere Iterationen des Risikomanagements mit demselben Anwendungsbereich erfolgen somit wie folgt auf Basis der vorhandenen Frameworkinstanz:

- Neu oder verändert zu betrachtende Assets, Bedrohungen und Schwachstellen ergeben sich entweder durch das Security-Framework komplementierende szenarienspezifische Analysen oder durch das Erscheinen einer neuen Version des Frameworkkonzepts (vgl. Abschnitt 5.2.1). Nur im letzteren Fall wird die Betrachtung in Frage kommender zusätzlicher Maßnahmen direkt vom Security-Framework unterstützt.
- Die Quantifizierung der überarbeiteten Risiken variiert darüber hinaus in Abhängigkeit von Änderungen an deren Eintrittswahrscheinlichkeiten. Insgesamt können größere Änderungen oder Erweiterungen der Frameworkinstanz erforderlich werden (vgl. Abschnitt 5.9).
- Die Durchführung einer Kosten-/Nutzenanalyse kann ebenso wie die Bestimmung des Restrisikos und eine Verfeinerung der Eintrittswahrscheinlichkeiten und Auswirkungen auf Basis der zwischenzeitlich mit dem Betrieb des Security-Frameworks gesammelten Erfahrungen verbessert werden. Hierzu sind insbesondere die in Abschnitt 6.6 behandelten Kennzahlen und Berichte über die Effektivität und Effizienz der eingesetzten Frameworkinstanz heranzuziehen.

Die beschriebenen Abläufe bleiben auch dann gültig, wenn sich der Anwendungsbereich des Risikomanagementdurchlaufs nicht genau mit dem von einem Security-Framework abgedeckten Bereich deckt. Beispielsweise können für eine organisationsweite IT-Risikoanalyse die Beiträge mehrerer Security-Framework aggregiert und mit der herkömmlichen Vorgehensweise für das Risikomanagement auf Basis einzelner Assets und individueller Schutzmaßnahmen kombiniert werden. Zur Reduktion der damit im Allgemeinen verbundenen Komplexität bietet sich wiederum die gebündelte Betrachtung der von jeden Security-Framework geschützten Assets und Maßnahmen als Einheit an.

Zusammenfassend bleibt damit festzuhalten, dass insbesondere die *Konzepte* von Security-Frameworks umfassende Beiträge zum szenarienspezifischen Risikomanagement liefern können, da sie einen großen Teil der benötigten Informationen beitragen, aus denen auch ohne szenarienspezifische Verfeinerungen Zwischenergebnisse und Maßnahmen abgeleitet werden können. Da die Qualität der vom Risikomanagement erarbeiteten Ergebnisse jedoch stark von der Vollständigkeit und Präzision der betrachteten Risiken abhängt, sind ergänzende szenarienspezifische Analysen aber weiterhin unabdingbar.

6.4. Integration von Security-Frameworks in Managementplattformen und -architekturen

Die bisherigen Abschnitte in diesem Kapitel haben gezeigt, wie das Management von Security-Frameworks in den Sicherheitsmanagementprozess und das operative Sicherheitsmanagement eingebettet werden kann und mit einem unternehmensweiten Risikomanagement zusammenspielt. Genau an der Schnittstelle dieser drei Bereiche sind sicherheitsspezifische **Managementplattformen** anzusiedeln: Sie stellen offene, über definierte Schnittstellen erweiterbare Systemumgebungen dar, die verschiedenste so genannte Managementobjekte (engl. *managed objects*, MOs) einheitlich verwalten können. Mit ihrer Hilfe kann auch für komplexe, heterogene unternehmensweite und interorganisationale Infrastrukturen ein gesamtheitlicher Ansatz für das Management der Infrastrukturkomponenten umgesetzt werden, ohne eine Vielzahl einzelner, hersteller- bzw. produktspezifischer Managementwerkzeuge mit jeweils sehr ähnlicher Zielsetzung verwenden zu müssen. Managementplattformen setzen **Managementarchitekturen** um, bei denen es sich um konzeptionelle Rahmenwerke handelt, die vier komplementäre Aspekte spezifizieren: Sie beschreiben die zu verwaltenden MOs in Form eines *Informationsmodells*, legen Rollen und Kooperationsformen in einem *Organisationsmodell* fest, beschreiben den managementspezifischen Nachrichtenaustausch mittels eines *Kommunikationsmodells* und strukturieren die managementspezifische Funktionalität auf Basis eines *Funktionsmodells* (vgl. [HAN99, S. 100]).

Im Kontext des Managements von Security-Frameworks besteht eine nicht unerhebliche Schwierigkeit darin, dass *integrierte* Managementansätze für sicherheitsspezifische Infrastrukturkomponenten noch nicht annähernd so ausgereift sind wie beispielsweise diejenigen für das Netz- und Systemmanagement. Zwar behandeln einerseits viele Managementarchitekturen sicherheitsrelevante Aspekte der verwalteten MOs auf der funktionalen Ebene, die sich beispielsweise durch die Fünfteilung des OSI-Funktionsmodells in Fault, Configuration, Performance, Accounting und *Security* Management (FCAPS) ergibt. Andererseits werden viele Sicherheitsprodukte wie Firewalls und Anti-Virus-Software mit dedizierter Managementsoftware ausgeliefert, die durchaus für den unternehmensweiten Einsatz ausgelegt ist. Aber es fehlen hersteller- und produktübergreifende Managementplattformen, die für alle Belange des Sicherheitsmanagements eingesetzt werden können und dabei funktional über die Aggregation und Korrelation von Sicherheitsalarmen verschiedener Komponenten hinausgehen (vgl. SIEM-Systeme in Abschnitt 6.2).

Im Folgenden wird deshalb zunächst der Bedarf an einer schutzmaßnahmen- und sicherheitsmechanismenübergreifenden Managementlösung unter Berücksichtigung der Spezifika von Security-Frameworks motiviert. In Abschnitt 6.4.2 wird über Analogien sowohl zum Netz-

und Systemmanagement als auch zum in ITSM-Frameworks spezifizierten Configuration Management hergeleitet, welche Ziele mit der Auffassung von Security-Frameworks und ihrer Umgebung als MOs bzw. Configuration Items (CIs) zu verfolgen sind, und gezeigt, dass die in diesem Bereich etablierten Managementkonzepte auch auf Security-Frameworks übertragen werden können. Bei den weiteren Betrachtungen stellt das in Abschnitt 6.4.3 vorgestellte, im Rahmen der vorliegenden Arbeit von Grund auf unter Berücksichtigung der Spezifika von Security-Frameworks erarbeitete Informationsmodell den Schwerpunkt dar, da die durch es vorgegebenen Objekte und Attribute die Basis für das Zusammenspiel mit den ebenfalls in diesem Kapitel erläuterten prozessualen Schnittstellen und die Erhebung von sicherheitsrelevanten Kennzahlen bilden. In Abschnitt 6.4.4 werden die durch Security-Frameworks notwendig werdenden Änderungen und Erweiterungen an den Organisations-, Kommunikations- und Funktionsmodellen konzipiert. Schließlich werden in Abschnitt 6.4.5 eine Analyse und eine Beurteilung durchgeführt, wie sich die Anwendung der erarbeiteten Konzepte auf die zur Unterstützung des operativen Sicherheitsmanagements verwendeten Managementwerkzeuge auswirkt.

6.4.1. Notwendigkeit integrierter Sicherheitsmanagementsysteme für Security-Frameworks

Sowohl der Sicherheitsmanagementprozess als auch das operative Sicherheitsmanagement behandeln nicht nur dedizierte Sicherheitsmechanismen wie Firewalls, sondern die sicherheitsrelevanten Eigenschaften aller Komponenten der IT-Infrastruktur. Anders als beim Risikomanagement, das bedarfsorientiert für verschiedene Anwendungsbereiche mit jeweils begrenztem Umfang instanziiert werden kann, darf das operative Management der Sicherheitseigenschaften im Allgemeinen keinen Bereich gänzlich ausklammern, ohne dass sowohl der Anspruch auf ein integriertes Management aufgegeben werden müsste als auch Herde unzureichend schnell bemerkter Sicherheitsprobleme entstehen würden. Dies führt in der Praxis dazu, dass sich IT-Sicherheitsexperten häufig nicht auf die Absicherung einiger weniger Systeme konzentrieren können, sondern sich parallel um Serverdienste wie E-Mail-, Datei- und Webserver, Endgeräte wie Arbeitsplatz-PCs, Notebooks, VoIP-Telefone und Smartphones sowie die zugrunde liegende Netzinfrastruktur inklusive Routern und Switches kümmern müssen. Je nach Größe des Szenarios sind somit mehrere hundert oder tausend Einzelkomponenten zu betrachten, die im Allgemeinen aufgrund unterschiedlicher Hersteller und Anschaffungszeitpunkte zudem eine erhebliche Heterogenität aufweisen.

Neben der Skalierbarkeit des Sicherheitsmanagements und der Heterogenität der zu verwaltenden Komponenten ergibt sich als weitere Herausforderung, dass viele Produkte nur unzureichend auf die nahtlose Integration in die szenarienspezifisch bereits vorhandenen Sicherheitskonzepte ausgelegt sind. Beispielsweise sind viele IT-Dienste mit eigenen Benutzerdatenbasen, Authentifizierungsmodulen und Zugriffskontrollmechanismen ausgestattet, die zwar einen autarken Betrieb ermöglichen, schon vorhandene Verwaltungsmechanismen aber nicht aufgreifen. Analog dazu ist die Konfiguration sicherheitsspezifischer technischer Parameter – beispielsweise die Auswahl zu verwendender kryptographischer Hashfunktionen und das Einspielen von X.509v3-Zertifikaten – häufig nur möglich, indem lokale Konfigurationsdateien auf den Komponenten bearbeitet oder komponentenspezifische, häufig webbasierte Managementoberflächen genutzt werden. Hieraus resultiert zum einen das Manko, dass eine Vielzahl verschiedener Managementwerkzeuge mit sehr ähnlicher Funktionalität eingesetzt werden muss, die

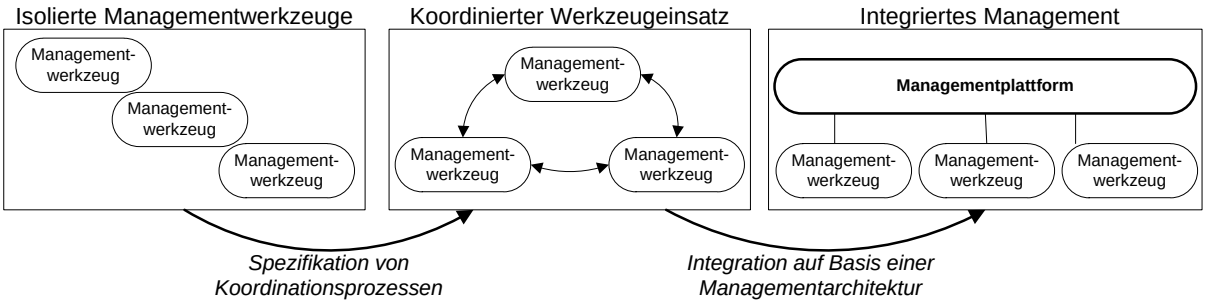


Abbildung 6.13.: Vom isolierten Werkzeugeinsatz zum integrierten Management (angelehnt an [HAN99, S. 98])

ihrerseits wiederum Betriebsaufwand verursachen und beispielsweise auch Schulungen erforderlich machen. Zum anderen führt die werkzeuginduzierte Fragmentierung der Tätigkeiten zu einem deutlich erhöhten Koordinationsaufwand, wenn bestimmte Änderungen möglichst zeitgleich und konsistent über eine Vielzahl unterschiedlicher Komponenten durchgeführt werden sollen.

Wie in Abbildung 6.13 dargestellt ist, stellt eine Reihe voneinander isolierter Managementwerkzeuge die Ausgangsbasis dar. Ein erster Schritt zur Verbesserung ist das Festlegen von Prozessen und Arbeitsabläufen, in denen das Zusammenspiel der nach wie vor autarken Werkzeuge beschrieben wird. Einen wirklich integrierten Ansatz können jedoch nur Managementplattformen liefern, die eine Vielzahl relevanter Managementwerkzeuge über offene Schnittstellen einbinden können und wie in Abbildung 6.14 gezeigt eine einheitliche Oberfläche für das Management praktisch beliebig vieler verwalteter Komponenten bieten. Über diese zentrale Oberfläche ist es im Anschluss möglich, Änderungen sicherheitsspezifischer Parameter produkt-, hersteller- und werkzeugübergreifend konsistent umzusetzen.

Trotz dieser erheblichen Verbesserung gegenüber dem Einsatz isolierter Managementwerkzeuge muss ein geeigneter Kompromiss aus Sicherheitsfunktionalität und Managementeigenschaften gefunden werden: Einerseits ist es auch mit integrierten Managementansätzen komplexer, viele verschiedenartige Komponenten zu verwalten als eine größere Zahl identischer Komponenten. Andererseits bietet die Kombination von Sicherheitsmechanismen verschiedener Hersteller den Vorteil, dass in einem Produkt bekannt werdende Schwachstellen nicht notwendigerweise zur Gefährdung der gesamten Infrastruktur führen; beispielsweise sehen Best Practices zum Schutz von Netzzonen für Firewallarchitekturen, die wie z. B. sog. demilitarisierte Zonen aus mehreren Firewalls bestehen, häufig entsprechend die Kombination von Firewallprodukten verschiedener Hersteller vor. Die Nutzbarkeit offener, standardisierter Schnittstellen zur Integration herstellerspezifischer Werkzeuge ist deshalb ein wesentlicher Aspekt bei der Auswahl insbesondere von kommerziellen Sicherheitskomponenten, deren Konzepte und Dokumentationen nicht frei verfügbar sind (vgl. Abschnitt 4.1.2.1).

Security-Frameworks haben insbesondere die folgenden drei in den vorangegangenen Kapiteln bereits ermittelten Eigenschaften, die einen integrierten Managementansatz nicht nur erforderlich machen, sondern auch zu seiner Umsetzung beitragen: Erstens stellen sie im Allgemeinen hersteller- und produktübergreifende Kompositionen von Schutzmechanismen dar, für die einheitliche Managementkonzepte benötigt werden. Zweitens thematisieren Security-

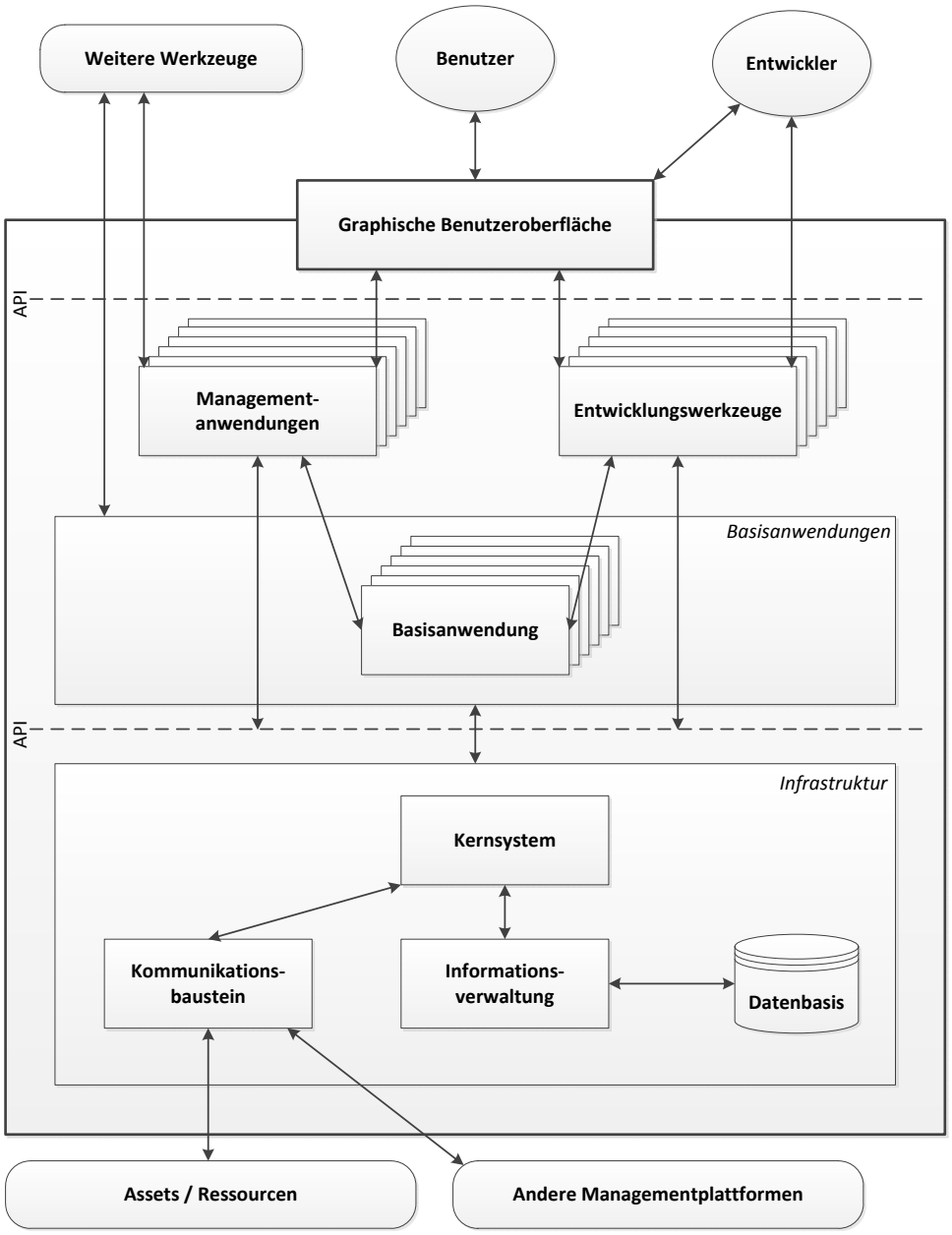


Abbildung 6.14.: Prinzipielle Architektur von Managementplattformen (angelehnt an [HAN99, S. 278])

Frameworks nicht nur technische Schutzmechanismen, sondern befassen sich mit einer Reihe weiterer Aspekte, die für das Sicherheitsmanagement relevant sind, beispielsweise mit Schwachstellen, Angriffen, Meldungen von Sicherheitsereignissen und organisatorischen Randbedingungen; reine Administrationswerkzeuge für sicherheitsrelevante Konfigurationsparameter würden somit zu kurz greifen. Drittens stellen Security-Frameworks den Bezug zu geschützten Assets und damit IT-Diensten und den von ihnen unterstützten Geschäftsprozessen her.

Durch diesen großen Abdeckungsbereich, der mit einem einzelnen, isolierten Werkzeug, das nur dem Management der Sicherheitsparameter des Security-Frameworks dient, nicht adäquat berücksichtigt werden könnte, und dem häufig möglichen und anzustrebenden parallelen Einsatz mehrerer Security-Frameworks werden die nachfolgenden Betrachtungen motiviert, inwieweit bestehende Konzepte zum integrierten Management auf Security-Frameworks angewandt bzw. um dafür spezifische Aspekte erweitert werden können.

6.4.2. Analogien zum Netz- und Systemmanagement und ITSM Configuration Management

Security-Frameworks bestehen aus zusammenhängenden und interagierenden Einzelkomponenten, deren Zusammenstellung und Parametrisierung einem oder mehreren gemeinsamen Zielen folgen. Nicht nur beim Customizing und im Rahmen des Risikomanagements, sondern auch zur Verwaltung mithilfe von Managementplattformen muss es deshalb das Ziel sein, jedes Security-Framework als Ganzes und nicht nur alle Einzelkomponenten separat steuern und überwachen zu können: Security-Frameworks sollen folglich als MOs bzw. CIs aufgefasst werden können.

Bei jeder konkreten Managementplattform handelt es sich um die Implementierung einer Managementarchitektur, die ein Rahmenwerk darstellt, das die in Abschnitt 6.4 genannten vier Teilmodelle (Informations-, Organisations-, Kommunikations- und Funktionsmodell) spezifiziert. Dabei bildet das Informationsmodell das Herzstück der gesamten Managementarchitektur [HAN99, S. 101]; es muss also festgelegt werden, welche für das Management relevanten Charakteristika und Parameter in Form von MOs betrachtet werden müssen, welche Arten von MOs benötigt werden und wie deren Interna sowie Zusammenhänge modelliert werden können. Vorrangig sind hierzu ein Modellierungsansatz und eine eindeutige Syntax für die Beschreibung der Managementinformationen festzulegen; für die Spezifikation der Semantik einzelner Managementinformationen wird im Allgemeinen auf natürliche Sprache zurückgegriffen.

Die nachfolgenden Abschnitte befassen sich deshalb zunächst mit der Fragestellung, wie Security-Frameworks im Kontext von Managementarchitekturen modelliert werden können, um darauf aufbauend im Anschluss die Spezifika der Organisations-, Kommunikations- und Funktionsmodelle aufzuzeigen. Dieses Vorhaben wird durch zwei Teilprobleme erschwert: Zum einen behandeln Security-Frameworks ihr Management bislang entweder überhaupt nicht oder beschreiben es nur uneinheitlich strukturiert und in natürlicher Sprache, liefern aber keine explizite Modellierung von MOs (vgl. Kap. 4). Zum anderen existieren bislang weder in wissenschaftlicher Literatur noch in der Praxis anerkannte Ansätze zur spezifischen Modellierung der spezifischen Eigenschaften für das hersteller- und produktübergreifende Management von Sicherheitsmechanismen (vgl. hierzu die in Abschnitt 2.3.2 skizzierten Ansätze für die Softwareentwicklung unter Sicherheitsgesichtspunkten). Die im Rahmen dieser Arbeit durchgeführte Modellierung orientiert sich deshalb an den im Folgenden skizzierten, bewährten Ansätzen, die einerseits aus dem integrierten Netz- und Systemmanagement und andererseits aus dem Einsatz von Configuration Management Databases (CMDBs) im Rahmen des organisationsinternen ITSM-Prozesses Configuration Management stammen.

Als Referenzarchitektur im Netzmanagement ist das OSI-Management [ISO89] anzuführen, das die Basis für das Telecommunications Management Network (TMN) bildet und als ers-

te Architektur alle vier Teilmodell ausgeprägt hat [HAN99, S. 113]. Sein Informationsmodell basiert auf einem objektorientierten Ansatz, so dass Objektklassen und deren Attribute, Operationen, Benachrichtigungen und Verhalten beschrieben werden, ohne implementierungsspezifische Details vorzuschreiben. Als Attribute kommen einfache und strukturierte Datentypen sowie Mengen davon zum Einsatz. Zusammenhänge zwischen MOs ergeben sich zunächst implizit aus der Vererbungshierarchie und dem als Management Information Tree bezeichneten Enthaltenseinsbaum; sie können auch in der meist natürlichsprachlichen Beschreibung des Verhaltens von MOs benannt werden. Eine explizite Modellierung kann durch Attribute von MOs erfolgen, die auf andere MOs verweisen, so dass insbesondere auch explizite Objektklassen zur Abbildung von Relationen modelliert werden können. Für die einzelnen Attribute und die Instanziierung der Objektklassen sind allgemeine Operationen wie *get*, *set*, *create* und *delete* vorgesehen. Benachrichtigungen dienen insbesondere dem asynchronen Melden managementrelevanter Ereignisse, die auch versandt werden, wenn sie von der Managementplattform nicht vorher explizit angefordert wurden. Das Informationsmodell des OSI-Managements wird seinem Ursprung entsprechend primär zur Modellierung aktiver und passiver Netzkomponenten angewandt. Eine sicherheitsspezifische Anwendung erfolgte beispielsweise durch die ansatzweise Spezifikation einer so genannten Security-MIB für Paketfilterfirewalls (siehe [HS98]); diese Vorgehensweise konnte sich bislang jedoch nicht durchsetzen und wurde noch nicht auf andere Schutzmechanismen übertragen.

Demgegenüber wird die Internet-Managementarchitektur der IETF, die in mehreren RFC-Dokumenten beschrieben ist, häufig mit dem in der Praxis dominierenden Managementprotokoll SNMP assoziiert. Das ihm zugrunde liegende Informationsmodell wurde bewusst möglichst einfach gehalten, so dass ein Großteil der Funktionalität über die in der Managementplattform hinterlegte Programmlogik erzielt werden muss. Obwohl das Internet-Informationsmodell keine Objekte im Sinne der objektorientierten Modellierung unterstützt, stehen MOs zur Verfügung, deren Granularität jedoch mit den Attributen von Objektklassen gemäß dem OSI-Informationsmodell entsprechen. Obwohl mehrere solcher MOs zu Management Information Bases (MIBs) zusammengestellt werden können und über das reine Netzmanagement hinausgehend auch MIBs für das Systemmanagement definiert wurden, eignen sich die Granularität und die beschränkten Möglichkeiten zur Modellierung von Zusammenhängen zwischen Komponenten nicht zur Abbildung komplexer komponentenübergreifender Zusammenhänge im Kontext von Security-Frameworks.

Im Gegensatz dazu haben das objektorientierte Common Information Model (CIM, [DMTF11]), das Netze, Dienste und Systeme abbildet, aber unzureichende Möglichkeiten zur Verknüpfung mit ITSM- und Geschäftsprozessen aufweist, und das sehr eng an den telekommunikationsspezifischen eTOM-Prozessen gekoppelte Shared Information/Data Model (SID, [For11]) jeweils einen Fokus und eine Komplexität, unter denen eine Anpassung an die Spezifika von Security-Frameworks nicht zielführend wäre. Unter der Berücksichtigung der Eigenschaft von Security-Frameworks, Assets zu schützen und aus Teilkomponenten zu bestehen, die selbst wiederum als Assets aufgefasst werden können, sind jedoch auch die aus dem ITSM bekannten CMDB-Konzepte zu betrachten. Eine CMDB speichert dabei sowohl CIs, die in einem szenarienspezifisch frei wählbaren Detaillierungsgrad modelliert werden können, als auch beliebige Beziehungen zwischen Paaren von CIs; als CIs werden dabei neben Assets beispielsweise auch IT-Dienste, SLAs und Dokumentationen aufgefasst.

Wie in [BGS06] dargelegt wird, ist das für eine CMDB zu verwendende Datenmodell im Allgemeinen schlank zu halten, so dass zwar die für alle daran angebundenen ITSM-Prozesse

relevanten Informationen bereitgehalten werden, aber nicht alle für das operative Management benötigten Attribute enthalten sind. Eine CMDB stellt darüber hinaus eine Sammlung von Kopien managementrelevanter Daten dar, bietet aber keine jederzeit aktuelle Sicht im Sinne eines Abrufs der Daten von den verwalteten Ressourcen zur Laufzeit. Analog dazu wirken sich auch Schreibzugriffe auf CIs nicht ohne weitere Maßnahmen auf die verwalteten Komponenten an sich aus, so dass eine graphische CMDB-Benutzeroberfläche keine Managementplattform gemäß Abschnitt 6.4.1 darstellt. Allerdings können in CIs auch Lebenszyklusinformationen hinterlegt werden, so dass CIs bereits in der Planungsphase eingesetzt werden können, also noch bevor eine implementierte und produktiv eingesetzte Ressource vorliegt. Eine enge Abstimmung zwischen der CMDB-Modellierung und der Modellierung von Security-Frameworks ist auch aufgrund der in Abschnitt 6.5 beschriebenen Schnittstellen zu den ITSM-Prozessen erforderlich, da wiederum Teile der für das Management von Security-Frameworks relevanten Informationen auch in der CMDB benötigt werden.

Die Schwierigkeiten, dass für CIs keine standardisierten Modellierungssprachen und keine szenarienübergreifenden Standardmodelle existieren und eine CMDB nicht ausreichend Funktionalität für eine Managementplattform besitzt, löst Sailer in [Sai07] am Beispiel der Modellierung einer Service-MIB. Er bringt hierzu Anforderungen, die sich aus ausgewählten ITSM-Prozessen ergeben, durch Aggregations- und Abbildungsregeln in Einklang mit den von den am Service beteiligten Ressourcen bereitgestellten Parametern. Die daraus resultierenden Managementinformationen werden anschließend in etablierte Managementarchitekturen integriert, so dass diverse wesentliche Arbeitsschritte des Service-Managements auf Basis vorhandener Managementplattformen durchgeführt werden können. Das Ziel, ein Informationsmodell zu erarbeiten, das sowohl die Anforderungen der ITSM-Schnittstellen erfüllt als auch zum operativen Management der Security-Frameworks eingesetzt werden kann, wird auch im folgenden Abschnitt verfolgt.

6.4.3. Informationsmodell zum Management von Security-Frameworks

Bislang sind in der wissenschaftlichen Literatur keine allgemeinen, d. h. für mehr als nur einige spezifische Sicherheitskomponenten geeigneten, Sicherheitsmanagementarchitekturen bekannt, die die vier Teilmodelle ausgeprägt haben; insbesondere fehlen bereits Konzepte für Informations- und Datenmodelle, die festlegen, welche Arten von MOs existieren und wie diese jeweils auszuprägen sind. Analog dazu existiert für den praktischen Einsatz zwar eine Vielzahl von Werkzeugen zur Unterstützung des operativen Sicherheitsmanagements, die sich jedoch überwiegend auf einzelne Teilbereiche konzentrieren, also keinen gesamtheitlichen Ansatz verfolgen, und deren Konzepte, die beispielsweise den werkzeugintern verwendeten Datenstrukturen zugrunde liegen, nicht offengelegt wurden. Somit ist es nicht möglich, bestehende Ansätze gezielt um für Security-Frameworks spezifische Aspekte zu ergänzen. Vielmehr wird im Folgenden das im Rahmen dieser Arbeit konzipierte Informationsmodell vorgestellt, das von Anfang an auf die Unterstützung von Security-Frameworks ausgerichtet ist.

Abbildung 6.15 gibt einen Überblick über die im Kontext des Management von Security-Frameworks relevanten Arten von MOs, die im Folgenden objektorientiert als Klassen modelliert werden, und ihre wichtigsten Zusammenhänge. Die grundlegende Auswahl und Zusammenstellung der Klassen basiert einerseits auf den in Abschnitt 2.2.2 definierten und in Abbildung 2.9 illustrierten Basisentitäten des Sicherheitsmanagements. Andererseits wurden

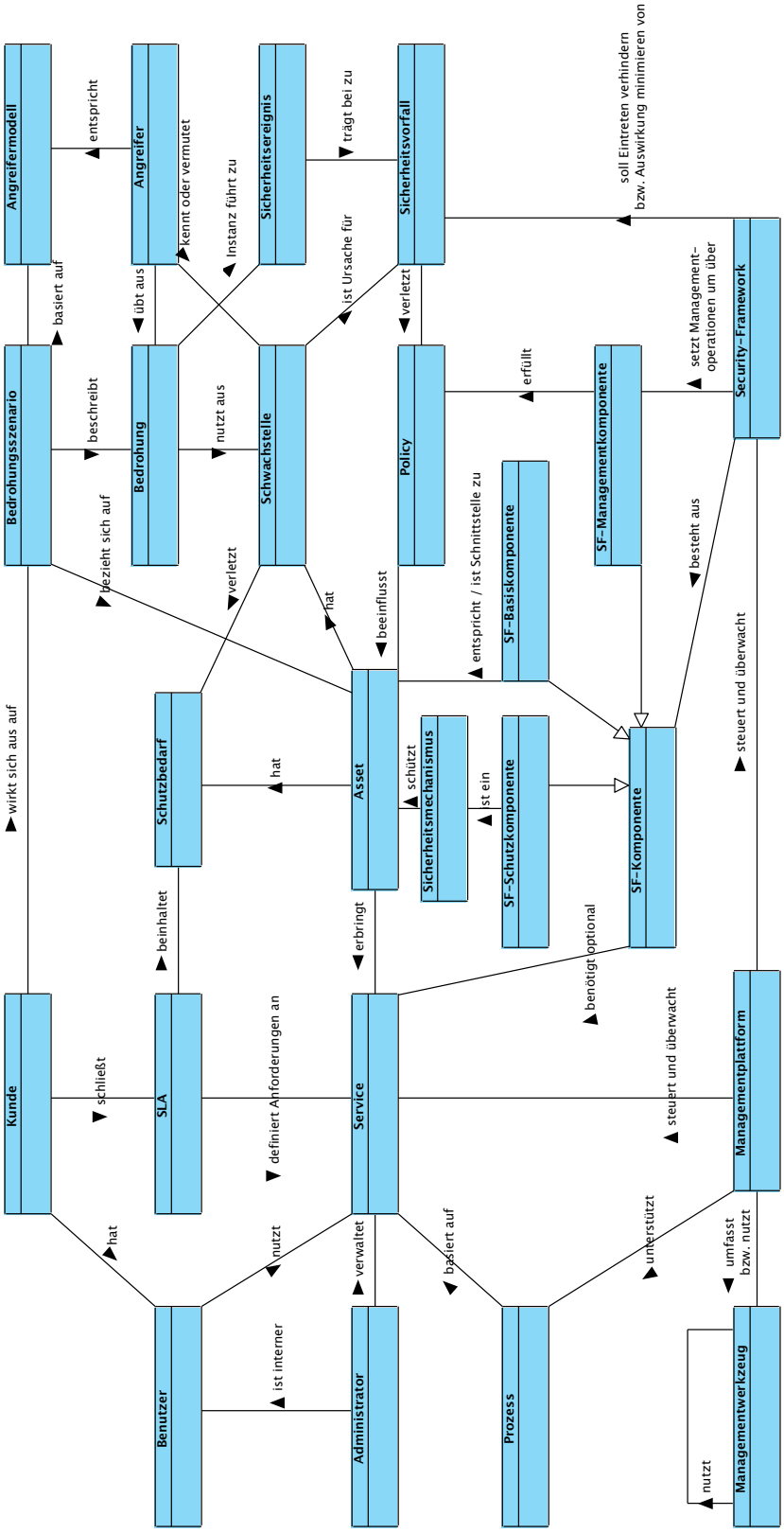


Abbildung 6.15.: Übersicht über das Informationsmodell der Managementarchitektur für Security-Frameworks

grundlegende Konzepte aus dem ITSM-Umfeld berücksichtigt, so dass beispielsweise zwischen Prozessen, Services und Assets sowie zwischen Kunden, Benutzern und privilegierten Benutzern unterschieden wird. Analog zur daraus resultierenden Datenschnittstelle zu ITSM-Managementplattformen wird durch die Modellierung u. a. von Bedrohungen und Schwachstellen der Bezug zum bereits diskutierten Risikomanagement hergestellt.

Als übergeordnete Designziele werden dabei verfolgt:

- Beliebig viele Security-Frameworks müssen unter Berücksichtigung ihrer Modularität bzw. ihrer Zusammensetzung aus mehreren Einzelkomponenten im Regelfall von einem, bei organisationsübergreifenden Szenarien ggf. jedoch auch von mehreren Managementplattformen verwaltet werden.
- Im Hinblick auf die Verknüpfung mit den ITSM-Prozessen ist der Bezug zwischen von den Security-Frameworks geschützten Assets und IT-Services und damit Prozessen bzw. Kunden herzustellen.
- Die Komponenten von Security-Frameworks können der Detektion von sicherheitsrelevanten Ereignissen dienen, die zusammen mit den Ereignismeldungen anderer Schutzmechanismen korreliert werden müssen und ins Security Incident Management einfließen.
- Zur Unterstützung sowohl des operativen Managements als auch des Risikomanagements müssen bekannte Bedrohungen und Schwachstellen verwaltet werden.

Security-Frameworks werden somit als aus einzelnen Komponenten bestehend modelliert, die jeweils wiederum wie folgt unterschieden werden können:

- SF-Schutzkomponenten sind Sicherheitsmechanismen, d. h. sie bieten Sicherheitsfunktionalität und dienen somit dem Schutz von Assets. Ein Beispiel für eine SF-Schutzkomponente ist ein Firewall.
- SF-Basiskomponenten haben die Aufgabe, den anderen SF-Komponenten frameworkintern benötigte Funktionalität bereitzustellen. Beispielsweise unterstützt ein Policy-Repository, das Filterregeln für den Netzverkehr enthält, die SF-Schutzkomponente Firewall. Bei SF-Basiskomponenten kann es sich auch um Schnittstellen oder Gateways zu bereits vorhandenen Assets handeln. Im Allgemeinen sind SF-Basiskomponenten deshalb wie Assets bzw. Subservices zu behandeln, decken sich jedoch nicht mit den vom Security-Framework geschützten Assets.
- SF-Managementkomponenten erbringen eine für das Security-Framework spezifische Funktionalität, die sich jedoch nur indirekt auf die Sicherheitsfunktionalität bzw. die Schnittstellen zu den übrigen Infrastrukturkomponenten auswirken. Beispiele umfassen Berichtswerkzeuge und eventuell explizit vorhandene Steuerkomponenten für das Security-Framework, die z. B. eine komponentenübergreifend einheitliche Parametrisierung vornehmen.

Diese Dreiteilung deckt sich wiederum mit der Kategorisierung von Anforderungen in Sicherheitsfunktionalität (SF-FUNK), Integrationseigenschaften (SF-INT) und Management (SF-MGMT). Die Nutzung einer Managementplattform für das Management von Security-Frameworks erfolgt unter der Annahme, dass neben den im jeweiligen Szenario eingesetzten Security-Frameworks noch weitere Sicherheitsmechanismen zum Tragen kommen, auf die jedoch nicht vertiefend eingegangen wird. Für einen integrierten Ansatz ist jedoch neben dem

Einbezug weiterer Managementwerkzeuge ausschlaggebend, dass eine Orientierung an den Prozessen (z. B. Geschäfts-, Sicherheitsmanagement- und ITSM-Prozessen) erfolgt und ausreichende Managementinformationen über Services vorliegen, um die Effektivität der Security-Frameworks und ihrer Parametrisierung beurteilen zu können.

Im Rahmen dieses Einbezugs von IT-Diensten, die auf Basis von Assets erbracht werden, sind auch Kunden und Benutzer zu betrachten, da insbesondere über SLAs Mindestanforderungen an die Sicherheitseigenschaften von Diensten und Assets vertraglich geregelt werden können. Der somit vorgegebene Schutzbedarf kann durch Schwachstellen, die einzelne Assets aufweisen, verletzt werden. Auf Basis von Angreifermodellen können Bedrohungsszenarien und konkrete Bedrohungen modelliert werden, die beim Vorhandensein entsprechender Schwachstellen zu sicherheitsrelevanten Ereignissen und damit zu Sicherheitsvorfällen führen können.

Für die weiteren Betrachtungen werden o. B. d. A. die folgenden beiden Vereinfachungen vorgenommen:

1. Die Modellierung der Attribute der festgelegten Objektklassen beschränkt sich auf das für das Management von Security-Frameworks Wesentliche. Beispielsweise werden die Attribute für Assets und Services ohne Anspruch auf Vollständigkeit im Sinne einer Anwendbarkeit auch außerhalb der hier betrachteten Managementarchitektur beschrieben; entsprechende Ergänzungen der Attribute können bei Bedarf auf Basis von Methoden zur Servicemodellierung vorgenommen werden (vgl. [Sai07]).
2. Die näher beschriebenen Objektklassen und ihre Attribute beschränken sich auf Managementinformationen, deren Erfassung und Verarbeitung in Managementplattformen praktikabel erscheint. Beispielsweise wird auf die detaillierte Modellierung von Angreifern verzichtet, da einerseits offensichtlich ist, dass diese den erstellten Angreifermodellen entsprechen und die modellierten Bedrohungen ausüben; andererseits stünde der Aufwand für eine genaue Erfassung aller (potentiellen) Angreifer in einer Managementplattform in keinem brauchbaren Verhältnis zum damit verbundenen praktischen Mehrwert und wäre insbesondere bei über das Internet eingehenden netzbasierten Angriffen mangels genauerer Kenntnis des Angreifers häufig schlichtweg nicht möglich (häufig als Problem der *Non-Attribution* bezeichnet).

Abbildung 6.16 zeigt die erarbeiteten Objektklassen und ihre wichtigsten Attribute, bei denen es sich um einfache Datentypen (z. B. für *Name* und *Beschreibung*), Verweise auf andere MOs bzw. beliebig komplex strukturierte Datentypen handeln kann, auf die nachfolgend näher eingegangen wird. Während die eine Verknüpfung mit anderen Objekten beschreibenden Attribute aus dem bereits diskutierten Überblick über alle Objektklassen abgeleitet sind, wurde bei der Zusammenstellung aller anderen Attribute wie folgt vorgegangen:

Sofern in der Praxis weit verbreitete (de facto) Standards existieren, wurden diese wie angegeben verwendet – beispielsweise IDMEF für Sicherheitsereignisse. In den meisten Fällen wurden die in Kapitel 2 bzw. die an anderen Stellen in diesem Kapitel verwendeten Verfahren aufgegriffen; beispielsweise wird das im Kontext des Risikomanagements beschriebene CVSS2 zur Modellierung von Schwachstellen herangezogen. Die übrigen Attribute – beispielsweise ITSM-Metadaten – stellen Platzhalter dar, für die jeweils exemplarische Ausprägungen genannt werden, deren explizite, detaillierte Datenmodellierung jedoch z. B. im Rahmen der Implementierung einer konkreten Managementplattform durchgeführt werden muss; sie werden primär verwendet, um ihren Bedarf an verschiedenen Stellen und den damit verbundenen

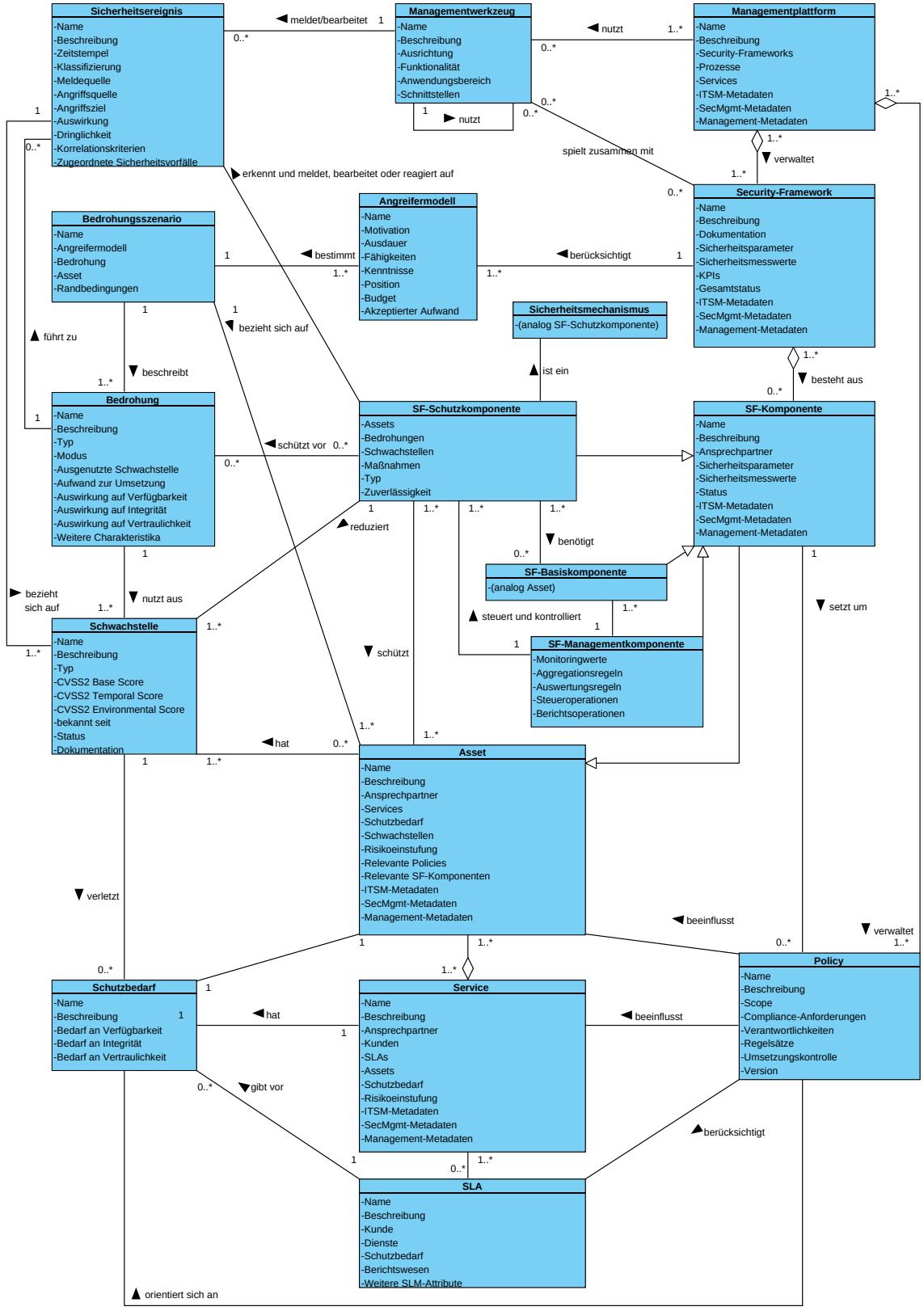


Abbildung 6.16.: Übersicht über die Objektklassen und Attribute im Informationsmodell

Datenfluss zu verdeutlichen.

Attribute zur MO-Verwaltung, beispielsweise die Erfassung der Person oder Schnittstelle, von der das MO angelegt wurde, des Zeitstempels der letzten Änderung oder zur Steuerung von Zugriffsrechten auf MOs, sind der besseren Übersicht wegen nicht explizit angegeben. Hierfür kann beispielsweise auf die Metadaten nach Dublin Core zurückgegriffen werden (siehe [DuCo10]).

Die vorgestellten Attribute decken mit den genannten Randbedingungen alle in Abschnitt 6.5 behandelten prozessualen Schnittstellen und damit die in diesem Kapitel erarbeiteten Konzepte ab. Bei der Ableitung konkreter Datenmodelle für die Implementierung einer Managementplattform können ggf. Ergänzungen der Objektklassen und Attribute vorgenommen werden, die sich aus weiteren, z. B. szenarienspezifischen Prozessen ergeben.

Der Ausgangspunkt für die folgenden Betrachtungen ist die Objektklasse *Managementplattform*:

- Wie alle Objektklassen hat auch die *Managementplattform* einen als eindeutigen Identifikator dienenden Namen und eine in natürlicher Sprache verfasste Beschreibung, aus der u. a. der Aufgabenbereich und die Funktionalität hervorgehen.
- Die hier betrachtete Hauptaufgabe der *Managementplattform* ist die Verwaltung von *Security-Frameworks*. Dies erfordert jedoch auch die Nutzung von *Managementwerkzeugen* und die autoritative Verwaltung von *Policies*, die unten erläutert werden.
- Die modellierte *Managementplattform* enthält Attribute, die auf die für ihren Einsatz relevanten *Prozesse* und *Services* verweisen, wie sie beispielsweise auch in CMDBs modelliert werden. Die damit implizierte Einschränkung des Anwendungsbereichs ist insbesondere dann erforderlich, wenn beispielsweise in organisationsübergreifenden Szenarien mehrere Managementplattforminstanzen vorliegen.
- Für die *Managementplattform* sind ferner drei Kategorien von Attributen vorgesehen, die als Metadaten bezeichnet werden, da sie bei diesem und anderen Objekten gespeichert und im Rahmen von Managementprozessen verwendet werden, sich aber nicht direkt auf die letztlich verwaltete Sicherheitsfunktionalität auswirken. Es handelt sich dabei um
  - ITSM-Metadaten, mit deren Hilfe die *Managementplattform* beispielsweise mit Changes, Incidents, Problems und weiteren Artefakten der ITSM-Prozesse assoziiert wird (siehe auch Abschnitt 6.5).
  - Sicherheitsmanagement-Metadaten, zu denen beispielsweise Verweise auf relevante *Policies*, zu liefernde Sicherheitsberichte und die Ergebnisse von Reviews bzw. Audits der *Managementplattform* gehören.
  - Management-Metadaten, unter denen alle Informationen verstanden werden, die mit dem praktischen Einsatz der *Managementplattform* zu Managementzwecken verknüpft sind, also beispielsweise Authentifizierungs- und Autorisierungsinformationen für die Benutzung der Managementfunktionalität.

In die *Managementplattform* integriert oder zumindest geeignet mit ihr verknüpft sind (insbesondere sicherheitsspezifische) *Managementwerkzeuge*:

- Bezüglich ihrer *Ausrichtung* ist zu unterscheiden, ob sie für proaktive Sicherheitstests (z. B. Penetration-Testing-Tools), die Erkennung von Sicherheitsereignissen (z. B. durch Logfile-Analyse) oder deren Bearbeitung (z. B. zur Isolation auffällig gewordener Systeme) konzipiert sind.
- Ihre *Funktionalität* wird im Allgemeinen in natürlicher Sprache beschrieben und soll die Beurteilung ihrer Eignung für im Rahmen des operativen Managements anfallende Aufgaben ermöglichen; sie kann z. B. durch die Zuordnung zu Kategorien des operativen Sicherheitsmanagements zur Verbesserung der automatisierten Auswertung strukturiert beschrieben werden.
- Der *Anwendungsbereich* schränkt beispielsweise über die Zuordnung zu *Assets* und *Services* das Einsatzgebiet der *Managementwerkzeuge* geeignet ein (z. B. Penetration-Testing-Tool für Web-Anwendungen).
- Über erfasste *Schnittstellen* können Verarbeitungsketten über mehrere *Managementwerkzeuge* hinweg gebildet und Anforderungen an die jeweiligen Ein- und Ausgabedaten erfasst werden.

In diese Klasse fallen beispielsweise auch Werkzeuge, die wie in Abschnitt 6.6 beschrieben das für Security-Frameworks spezifische Berichtswesen unterstützen. Security-Frameworks werden in ihrer Gesamtheit als MOs betrachtet, die in UML-Notation eine Aggregation einzelner Frameworkkomponenten darstellen.[1] Die Objektklasse *Security-Framework* umfasst die folgenden spezifischen Attribute:

- *Sicherheitsparameter* umfassen sämtliche sicherheitsrelevanten Konfigurationsparameter, die konsistent über alle *SF-Komponenten* umgesetzt werden müssen und damit einen Einfluss entweder auf die für *Assets* erbrachte Schutzfunktionalität haben oder die Sicherheitseigenschaften der *SF-Komponenten* selbst beeinflussen. Beispiele umfassen die Festlegung zu verwendender zentraler Authentifizierungs- und Logfileserver, Maschinen- und Dienstzertifikate, Schnittstellen z. B. zu Monitoringsystemen und relevanter Policies bzw. Regelsätze sowie die Auswahl kryptographischer Parameter wie Hash- und Verschlüsselungsalgorithmen, Schlüssellängen, Rekeying-Intervalle, etc.
- *Sicherheitsmesswerte* aggregieren in *Security-Framework*-MOs die entsprechenden Messwerte der *SF-Komponenten*; sie können dabei optional auch die in Abschnitt 6.6 beschriebenen Verarbeitungsschritte durchlaufen und somit zu Indikatoren beitragen. Welche Messwerte konkret geliefert werden, ist stark abhängig von den vom Security-Framework bereitgestellten Sicherheitsmechanismen sowie von den betrachteten Angriffen und Schwachstellen. Allgemein ist zwischen Messwerten zum regulären Betrieb (z. B. Anzahl beobachteter, aber unauffälliger Transaktionen), zu Sicherheitsereignissen (z. B. Zähler, wie oft welche Sicherheitsmechanismen oder Regelsätze zum Einsatz kamen) und zur Verfügbarkeit (z. B. Einschränkungen aufgrund von Störungen, die nicht auf aktive Angriffe zurückzuführen sind) zu unterscheiden.
- Als *KPIs* werden ausgewählte *Sicherheitsmesswerte* oder von diesen abgeleitete Kennzahlen benannt, die eine hervorgehobene Aussagekraft oder Relevanz besitzen und beispielsweise in Form von Dienstgüteparametern in SLAs aufgenommen werden und somit

[1] Da Security-Frameworks auch organisatorische bzw. konzeptionelle Bestandteile haben, handelt es sich in UML-Notation nicht um eine Komposition.

nicht nur in technischen Monitoringlösungen, sondern auch im Rahmen des ITSM kontinuierlich überwacht werden müssen.

- Der *Gesamtstatus* reflektiert die Statusinformationen der einzelnen *SF-Komponenten*; er gibt Auskunft darüber, ob alle Komponenten aktuell frei von Störungen sind oder ob aufgrund von Ausfällen oder erkannten akuten Sicherheitsereignissen eine erhöhte Aufmerksamkeit für das Security-Framework im operativen Sicherheitsmanagement erforderlich ist.
- Die im Kontext der *Managementplattform* erläuterten *Metadaten* werden über das *Security-Framework*-MO an seine *SF-Komponenten* propagiert. Dabei können erforderliche Einschränkungen oder Erweiterungen vorgenommen werden. Für das gesamte Security-Framework wird zudem eine Verknüpfung mit seiner *Dokumentation*, z. B. dem entsprechenden Frameworkkonzept, hergestellt.

Die Objektklasse *SF-Komponente* ist eine abstrakte Superklasse für die Subklassen *SF-Basiskomponente*, *SF-Schutzkomponente* und *SF-Managementkomponente*; sie übernimmt die pro Frameworkkomponente relevanten Attribute des *Security-Framework*-MOs. Wie *Assets* und *Services* werden auch die *SF-Komponenten* von *Policies* beeinflusst bzw. müssen diese umsetzen; pro Komponente wird zudem eine Menge von *Ansprechpartnern* festgelegt. Wie oben bereits erläutert dienen *SF-Basiskomponenten* der Erbringung frameworkinterner Funktionalität oder fungieren als Schnittstelle zu nicht frameworkspezifischen *Assets* bzw. *Diensten*. Sie können daher analog zu Assets bzw. rein intern verwendeten IT-Diensten modelliert werden und werden hier nicht näher betrachtet. Demgegenüber umfassen *SF-Schutzkomponenten* die folgenden zusätzlichen Attribute:

- Die Erfassung der *Assets*, die von der Komponente geschützt werden, dient neben ihrer unmittelbaren Relevanz für das operative Sicherheitsmanagement u. a. dazu, die Verbindungen zwischen den Geschäftsprozessen bzw. IT-Diensten und den eingesetzten Security-Frameworks herzustellen, wie sie z. B. im Rahmen des Risikomanagements benötigt werden.
- Die *SF-Schutzkomponente* wird zudem den für die von ihr geschützten *Assets* relevanten *Bedrohungen* und *Schwachstellen* zugeordnet, da mit ihr das Ziel verfolgt wird, vor der Ausnutzung von Schwachstellen durch die bekannten Bedrohungen zu schützen.
- Über das Attribut *Maßnahmen* werden die von der *SF-Schutzkomponente* bereitgestellten technischen Sicherheitsmechanismen erfasst; je nach Granularität der Module des Security-Frameworks liegt eine *1:1*- oder *1:n*-Zuordnung von Komponenten zu Mechanismen vor. Diese Maßnahmen sind in der Regel in natürlicher Sprache beschrieben, wodurch die stärker strukturierten *Sicherheitsparameter* komplementiert werden.
- Der *Typ* ordnet die *SF-Schutzkomponente* einer der in Abschnitt 6.2 diskutierten Kategorien des operativen Sicherheitsmanagements zu.
- Über die *Zuverlässigkeit* können bekannte Einschränkungen der *SF-Schutzkomponente* im Bezug auf die Reduktion der *Bedrohungen* ausgedrückt werden, beispielsweise falls nicht alle Arten von Angriffen korrekt erkannt werden können oder Authentifizierungsmechanismen eine Falschakzeptanz- bzw. Falschzurückweisungsrate aufweisen. Dieses Attribut ist für die Beurteilung des erreichten Gesamtsicherheitsniveaus erforderlich, wenn z. B. das Paradigma *defense-in-depth* umgesetzt wird, also auf verschiedenen tech-

nischen Ebenen zueinander redundante Schutzmaßnahmen für dieselben Schwachstellen und Bedrohungen ergriffen werden.

SF-Schutzkomponenten können ähnlich zu anderen *Managementwerkzeugen* präventiv bzw. detektierend zu Angriffen positioniert sein oder zur Reaktion darauf eingesetzt werden. Sie emittieren oder verarbeiten zu diesem Zweck bei Bedarf die ebenfalls über die Managementplattform verwalteten *Sicherheitsereignisse*. Diese können in Anlehnung an das im Umfeld von Intrusion Detection Systemen weit verbreitete IDMEF-Format wie folgt modelliert werden (vgl. [RC4765]):

- Jedes *Sicherheitsereignis* hat einen eindeutigen *Identifikator* und eine natürlichsprachliche *Beschreibung*, die im Allgemeinen von dem Werkzeug, das das Ereignis erkannt hat, vorgegeben und im Rahmen der weiteren Bearbeitung ggf. manuell ergänzt werden kann.
- Der Zeitpunkt des Eintretens des *Sicherheitsereignisses* wird über einen *Zeitstempel* erfasst. Zudem wird eine grundlegende *Klassifizierung* vorgenommen, die nach RFC 4765 Klassen wie *Portscan* und *Login Policy Violation* umfasst. Zu jedem Ereignis wird auch die Meldequelle, beispielsweise also eine *SF-Schutzkomponente*, ein *Managementwerkzeug* oder ein *Asset* festgehalten.
- Sofern das *Sicherheitsereignis* in Bezug zu einem konkreten Angriff steht, werden die *Angriffsquelle* und das *Angriffsziel* erfasst. Für den Fall, dass es sich dabei um szenarieninterne und über die Managementplattform erfasste Systeme handelt, können Verknüpfungen z. B. mit den entsprechenden *Assets* hergestellt werden; ansonsten sind beispielsweise die IP-Adressen als Identifikatoren zu verwenden.
- Von jedem Ereignis werden seine *Auswirkung* (engl. *impact*) und seine *Dringlichkeit* (engl. *urgency*) erfasst. Sie dienen der Priorisierung der Bearbeitung aller *Sicherheitsereignisse* und sind an die entsprechenden Parameter bei der Bearbeitung von Störungsmeldungen im Rahmen des ITSM-Prozesses Incident Management angelehnt (siehe Abschnitt 6.5).
- Für den Fall, dass möglicherweise mehrere *Sicherheitsereignisse* einer gemeinsamen Ursache zugeordnet werden könnten, sich jedoch nicht auf dieselben Angriffsquellen und -ziele beziehen, können weitere *Korrelationskriterien*, beispielsweise charakteristische Details von Angriffen oder Regelsätze zum Vergleich der von Netzüberwachungssystemen analysierten Datenpakete, separat festgehalten werden.
- Jedes Ereignis kann optional einem oder mehreren *Sicherheitsvorfällen* zugeordnet werden, die im Rahmen des Security Incident Management bearbeitet werden (vgl. Abschnitt 6.5). In der Praxis ist die Anzahl der *Sicherheitsvorfälle* jedoch um mehrere Größenordnungen kleiner als die Anzahl der *Sicherheitsereignisse*.

Die gemeldeten und verarbeiteten *Sicherheitsereignisse* können nur dann gezielt analysiert und bearbeitet werden, wenn bekannt ist, auf welche vorhandenen *Schwachstellen* sie sich beziehen. Hierzu und auch zur Unterstützung des Risikomanagements lassen sich die den einzelnen *Assets* zuzuordnenden *Schwachstellen* wie folgt erfassen:

- Jeder Schwachstelle wird einer bestimmter *Typ* zugeordnet; beispielsweise können Implementierungsfehler zu Buffer-Overflow-Angriffen oder Ressourcenengpässe zur Anfälligkeit für Überlastungen im Rahmen von Denial-of-Service-Angriffen führen.

- Zur Beurteilung der Auswirkungen von *Schwachstellen* und der Dringlichkeit ihrer Beseitigung bzw. der Einführung entsprechender Schutzmaßnahmen kann analog zum Risikomanagement auf Verfahren wie CVSS2 zurückgegriffen werden; dabei sind der konstante *Base Score*, der vom aktuellen Zeitpunkt abhängige *Temporal Score* und der *Asset*- bzw. szenarienspezifische *Environmental Score* separat zu erfassen. Die Orientierung an CVSS2 hat den bereits erläuterten Vorteil, dass die szenarienunabhängigen Eigenschaften vieler Verwundbarkeiten aus frei zugänglichen Datenbasen importiert werden können und somit nicht von Grund auf neu bzw. manuell erfasst werden müssen.
- Für jede *Schwachstelle* ist zudem festzuhalten, seit wann sie bekannt ist und welchen *Status* sie derzeit hat; hierüber kann der Lebenszyklus von Verwundbarkeiten abgebildet werden: Wie in Abschnitt 2.2.2 beschrieben wurde, kann sich die Verwundbarkeit beispielsweise in der Phase befinden, in der sie bekannt ist, aber noch keine Gegenmaßnahmen verfügbar sind, oder sie kann bereits für alle relevanten Assets erfolgreich behoben worden sein. Diese beiden Attribute bilden somit zusammen mit den CVSS2-Scores z. B. die Grundlage für statistische Auswertungen im Rahmen von Sicherheitsberichten (vgl. Abschnitt 6.6).
- Pro *Schwachstelle* können zudem Verweise auf Dokumentationen angegeben werden. Dabei kann es sich beispielsweise um Ergebnisse der Risikoanalyse handeln, aus denen hervorgeht, dass das mit der Schwachstelle verbundene Risiko akzeptabel ist; zudem kann auf detailliertere Beschreibungen, die beispielsweise über die CVE-Datenbank verfügbar sind, verwiesen werden.

Das Ausnutzen der *Schwachstellen* basiert auf *Bedrohungen*, die im Rahmen von *Bedrohungsszenarien* verwaltet werden und letztlich auf *Angreifermodellen* beruhen, über die sich wiederum der Bezug zu den *Security-Frameworks* ergibt. Über das *Angreifermodell* werden in Anlehnung an Abschnitt 2.4 die folgenden Attribute potentieller Angreifer erfasst:

- Die *Motivation*, *Ausdauer* und *Fähigkeiten* beschreiben die von Individuen ausgehende Gefährdung zunächst szenarienunabhängig in natürlicher Sprache.
- Über die *Kenntnisse* wird abgebildet, welches Wissen der modellierte Angreifer über das Szenario hat, also beispielsweise, ob er die technische Infrastruktur und deren Schwachstellen bereits kennt.
- Die *Position* des Angreifers dient einer groben Vorauswahl, welche Bedrohungen überhaupt erfolgreich ausgeübt werden können; beispielsweise ist zu unterscheiden, ob es sich um einen organisationsinternen Mitarbeiter mit physischen Zutrittsberechtigungen handelt oder um einen externen Angreifer, der z. B. Teile des Internet-Datenverkehrs der Organisation abhören kann. Eine entsprechende Unterscheidung fließt beispielsweise auch in den CVSS2-Score von *Schwachstellen* ein.
- Das angenommene *Budget* des Angreifers trägt zusammen mit den anderen Attributen dazu bei, dass eine als *akzeptierter Aufwand* bezeichnete Kennzahl abgeleitet werden kann, die als Vereinfachung dient und als Schwellenwert letztlich darüber entscheidet, welche konkreten Bedrohungen der Angreifer dem Modell nach erfolgreich ausüben kann.

Über die verwalteten *Bedrohungsszenarien* werden die Angreifermodelle, Bedrohungen und Assets einander zugeordnet (vgl. Abschnitt 6.3.5). Neben diesen Beziehungen werden in *Be-*

drohungsszenarien mögliche *Randbedingungen* erfasst, die im Wesentlichen zeitbezogene Verfeinerungen von Bedrohungen abbilden: Beispielsweise können sich Unterschiede daraus ergeben, wann eine Bedrohung eintritt (z. B. außerhalb der Geschäftszeiten), wie lange sie anhält (z. B. nur kurzer oder stundenlanger Denial-of-Service-Angriff) und wie lange es dauert, bis sie zuverlässig bemerkt wird. Bei den *Bedrohungen* sind die folgenden Attribute zu berücksichtigen:

- Über den *Typ* wird eine grobe Klassifizierung der *Bedrohung* vorgenommen; in Anlehnung an die oben diskutierten BSI-Grundschutzkataloge kann beispielsweise zwischen höherer Gewalt, organisatorischen Mängeln, menschlichen Fehlhandlungen, technischem Versagen und vorsätzlichen Handlungen unterschieden werden. Während alle Kategorien im Rahmen des Risikomanagements relevant sind, beziehen sich die meisten von Security-Frameworks explizit berücksichtigten Bedrohungen auf vorsätzliche Handlungen.
- Der *Modus* legt fest, ob ein die Bedrohung ausübender Angriff aktiv oder passiv ist; für den Fall netzbasierter Angriffe ist beispielsweise zu betrachten, ob der Angreifer den Netzverkehr nur passiv mithört oder auch aktiv eigene Datenpakete sendet. Dies wirkt sich u. a. darauf aus, ob und mit welchen Werkzeugen Angriffe erkannt und gemeldet werden können.
- Für jede Bedrohung muss bekannt sein, welche *Schwachstellen* sie ausnutzt und wie hoch der *Aufwand* zu ihrer Umsetzung ist; Bedrohungen, die sich auf bereits behobene Schwachstellen beziehen (vgl. Attribut *Status* in der Klasse *Schwachstelle*), bleiben weiterhin erfasst, lösen jedoch keine neuen Sicherheitsereignisse aus.
- Die *Auswirkungen* auf die *Verfügbarkeit*, *Integrität* und *Vertraulichkeit* der *Assets*, die die entsprechende *Schwachstelle* aufweisen, werden ebenfalls erfasst. Hierfür kann dieselbe Syntax verwendet werden wie in der nachfolgend beschriebenen Objektklasse für den *Schutzbedarf*.
- Für jede *Bedrohung* können *weitere Charakteristika* festgehalten werden, die beispielsweise für die Risikoanalyse auf Basis der oben beschriebenen Verfahren, z. B. DREAD, benötigt werden.

Die Kritikalität der Ausnutzung einer Verwundbarkeit eines *Assets* im Rahmen einer *Bedrohung* hängt maßgeblich vom *Schutzbedarf* des *Assets* bzw. der darauf aufbauenden *Services* und deren jeweiliger *Risikoeinstufung* ab. Analog zum Risikomanagement nach ISO/IEC 27000 kann der Schutzbedarf anhand der drei Grundziele der IT-Sicherheit *Verfügbarkeit*, *Integrität* und *Vertraulichkeit* bestimmt werden; beispielsweise haben die Informationen auf einem öffentlich zugänglichen Webserver hohe Anforderungen an Verfügbarkeit und Integrität, sind aber offensichtlich nicht vertraulich zu behandeln. Die Anforderungen können analog zu den Risikomanagementmethoden entweder qualitativ (z. B. niedrig, mittel, hoch) oder auf eine quantitative Skala (z. B. 0–10) abgebildet werden. Ein Angriff ist genau dann erfolgreich, wenn sich durch eine *Bedrohung* negative Auswirkungen auf die Verfügbarkeit, Integrität bzw. Vertraulichkeit ergeben, so dass der für ein *Asset* definierte *Schutzbedarf* nicht mehr erfüllt werden kann. Bei Bedarf können weitere Teilaspekte wie die Nicht-Abstreitbarkeit und die Authentizität ergänzt werden.

Die Festlegung des *Schutzbedarfs* setzt im Allgemeinen eine Klassifikation der von *Services* bzw. *Assets* gespeicherten und verarbeiteten Informationen voraus. Sie kann somit beispiels-

weise im Rahmen von *SLAs* vertraglich mit den Kunden und damit den Anwendern der *Services* festgelegt werden. Für *SLAs* ist im Kontext des Managements von Security-Frameworks deshalb relevant,

- auf welche *Kunden* und auf welche *Dienste* es sich bezieht,
- welcher *Schutzbedarf* dabei jeweils vereinbart wurde, und
- welche Kennzahlen und Modalitäten für das *Berichtswesen* erforderlich sind (siehe Abschnitt 6.6).

Darüber hinaus können weitere *SLM-Attribute* gespeichert werden, die Verknüpfungen zu anderen Systemen aufbauen, die im Rahmen des Service Level Managements benötigt werden; beispielsweise können Bezüge auf verschiedene Versionen des Dienstleistungskatalogs, Verweise auf andere Kennzahlen, Verweise auf SLA-Verletzungen, etc. hinterlegt werden (vgl. [Sch08]).

Die Anwendung der *SLAs*, die sich auf einzelne *Services* und darüber deren *Assets* beziehen, erfolgt über *Policies*, die wiederum von der *Managementplattform* verwaltet werden. Jede *Policy* umfasst dabei die folgenden Attribute:

- Über ihren *Scope* wird festgelegt, für welche *Services*, *Assets* und Benutzer sie gilt.
- *Compliance-Anforderungen* beschreiben in natürlicher Sprache, welche Ziele mit der jeweiligen *Policy* erreicht werden sollen; Beispiele umfassen die Einhaltung gesetzlicher Vorgaben und Verträge bzw. SLAs mit Kunden.
- Über *Verantwortlichkeiten* wird definiert, wer die Einhaltung der *Policy* kontrolliert und wer dafür verantwortlich ist; diese Angaben werden im Rahmen der prozessualen Schnittstellen z. B. für Eskalationen und das Berichtswesen benötigt (vgl. Abschnitt 6.5).
- Die *Regelsätze* beschreiben die mit der Policy umzusetzenden Gebote und Verbote. Je nach Abstraktionsebene der *Policy* können sie in natürlicher Sprache formuliert sein oder in maschinell verarbeitbaren Regelsprachen vorliegen, die z. B. von *SF-Komponenten* und anderen Schutzmechanismen ausgewertet werden können.
- Über das Attribut *Umsetzungskontrolle* wird auf *Managementwerkzeuge* oder Verfahren verwiesen, die zum Einsatz kommen, um die Einhaltung der Policy zu kontrollieren und ggf. zu erzwingen (engl. *policy enforcement*). Analog zu SLAs werden Maßnahmen für den Fall der Verletzung von Policies hier jedoch nicht weiter betrachtet.
- Policies können in verschiedenen *Versionen* vorliegen, so dass festgehalten werden muss, welche anderen MOs mit jeweils welcher Version der Policy verknüpft worden sind.

Die Einhaltung und technische Umsetzung der Policies obliegt allen an der IT-Infrastruktur beteiligten Komponenten. Für *Security-Frameworks* sind dabei die *SF-Managementkomponenten* ausschlaggebend: Entweder steuern und kontrollieren sie die anderen *SF-Komponenten* oder sie erbringen eine sich nicht direkt auf Schwachstellen bzw. Bedrohungen auswirkende frameworkspezifische Managementfunktionalität, beispielsweise für das Berichtswesen; sie umfassen dazu die folgenden zusätzlichen Attribute:

- *Monitoringwerte* umfassen über die *Sicherheitsmesswerte* hinausgehende Attribute, die eine Beurteilung aller betriebsrelevanten Eigenschaften der *SF-Komponenten* ermöglichen.

- *Aggregationsregeln* beschreiben, welche *Monitoringwerte* wie oft erfasst und ihren historischen Daten gegenübergestellt bzw. mit anderen *Monitoringwerten* kombiniert werden sollen, um beispielsweise die Auslastung im n-Minuten-Mittel zu erfassen.
- Die *Auswertungsregeln* legen fest, wie die durch Erfassung und Aggregation vorverarbeiteten Messwerte auszuwerten sind, um sie beispielsweise mit den in *Policies* vorgegebenen Schwellenwerten vergleichen und ggf. unerwünschte Zustände kommunizieren und eskalieren zu können.
- Über die *Steueroperationen* wird angegeben, welche Aspekte der Gesamtfunktionalität des *Security-Frameworks* mit der vorliegenden *SF-Managementkomponente* beeinflusst werden können. Dies ist einerseits beim Vorliegen mehrerer komplementärer oder zum Teil überlappender *SF-Managementkomponenten* relevant; andererseits müssen nicht über *SF-Managementkomponenten* erbrachte Managementoperationen direkt auf alle davon betroffenen *SF-Basis-* und *SF-Schutzkomponenten* angewendet werden, wodurch sich der Gesamtaufwand bei der Nutzung der Managementplattform erhöht.
- Die *Berichtsoperationen* spezifizieren die von der vorliegenden *SF-Managementkomponente* angebotenen Operationen bei der Erfassung von Messwerten und deren Verarbeitung zu Sicherheitsberichten (siehe Abschnitt 6.6).

Durch den Einsatz von Versionierungssystemen können neben den aktuellen auch die früheren Konfigurations- und Messwerte gespeichert und z. B. zur Historienbildung und Trendanalyse ausgewertet werden. Bei der Implementierung einer Managementplattform für Security-Frameworks müssen insbesondere die beschriebenen strukturierten Attribute konkretisiert werden, beispielsweise indem maschineninterpretierte Regelsprachen ausgewählt werden, die zur Formulierung von Policies eingesetzt werden. Dabei sind Synergien mit bereits vorhandenen Managementplattformen und -werkzeugen für andere Anwendungsbereiche zu berücksichtigen, beispielsweise indem auf offene, standardisierte Policysprachen zurückgegriffen wird.

6.4.4. Weitere Auswirkungen auf Managementarchitekturen

Mit dem vorgestellten Informationsmodell wird ein Rahmen dafür vorgegeben, wie die von einer für Security-Frameworks geeigneten Sicherheitsmanagementplattform zu verwaltenden Informationen grob zu strukturieren sind. Die konkrete Ausprägung einer solchen Managementplattform und der in sie zu integrierenden, zum Teil für einzelne Security-Frameworks spezifischen Werkzeuge, muss sich jedoch auch daran orientieren, wie diese Informationen und die Komponenten, die sie repräsentieren, verwaltet werden sollen und welche Arbeitsabläufe unterstützt werden müssen. Zu diesem Zweck sind neben dem Informationsmodell auch die Organisations-, Funktions- und Kommunikationsmodelle zu betrachten.

Vor dem Hintergrund der vielfältigen Einsatzszenarien für Security-Frameworks, deren mögliche Ausprägungen in Abschnitt 3.1.1 erörtert wurden und bei denen u. a. zwischen organisationsweiten und organisationsübergreifenden Ausprägungen sowie branchenspezifischen Besonderheiten zu unterscheiden ist, wird im Folgenden nicht das Ziel verfolgt, Ausprägungen dieser drei Teilmodelle mit einem Anspruch auf Vollständigkeit im Detail zu erarbeiten. Der dafür erforderliche Umfang, den beispielsweise [HAN99] für das integrierte Netzmanagement und [Mar11] für das organisationsübergreifende Fehlermanagement zeigen, würde den

Rahmen dieser Arbeit sprengen. Vielmehr werden die grundlegenden Eigenschaften und Rahmenbedingungen konzipiert, deren Einhaltung maßgeblich dazu beiträgt, dass flexible Managementlösungen für verschiedenste Security-Frameworks und Umgebungen entworfen werden können.

6.4.4.1. Grundlegendes Organisationsmodell für das Management von Security-Frameworks

Managementarchitekturen verfolgen allgemein das Ziel, die Aufbau- und Ablauforganisation des Betreibers nicht vorzugeben, sondern anpassbar an eine Vielzahl praktisch relevanter Ausprägungsformen zu sein (vgl. [HAN99, S. 103f.]). Somit müssen insbesondere die Aspekte der Bildung von Managementdomänen und der Festlegung der beteiligten Akteure bzw. Rollen betrachtet werden.

Die Bildung von Managementdomänen dient der Gruppierung von MOs anhand prinzipiell frei wählbarer Kriterien; vorrangig zu betrachten sind dabei die folgenden beiden Kategorien:

- *Funktionale Domänen* fassen MOs anhand ihrer Funktionalität zusammen (vgl. *Organisationsdomänen* im OSI-Management). Somit kann eine rudimentäre Einteilung beispielsweise unter Orientierung an Anwendungsfällen für Sicherheitsmanagementplattformen in ITSM-relevante, das Sicherheitsberichtswesen unterstützende, risikomanagementspezifische, einem bestimmten Dienst zugeordnete, bestimmten Aufgaben des operativen Sicherheitsmanagements zugeordnete oder ähnliche Sicherheitsfunktionalität bietende MOs vorgenommen werden.

  Diese Gruppierung kann durch Subdomänenbildung weiter verfeinert werden. Sie kann sich dabei selbstverständlich nicht nur auf MOs beziehen, die Systeme wie SF-Komponenten oder Assets darstellen, sondern sich z. B. auch über Policies und Angreifermodelle erstrecken. Auch Security-Frameworks selbst stellen Gruppierungen ihrer Komponenten und der sie beeinflussenden anderen MOs wie Assets und Policies dar.

- *Administrative Domänen* ordnen MOs ihren jeweiligen Verwaltungsautoritäten zu (vgl. *Verwaltungsdomänen* im OSI-Management). Hieraus ergeben sich Aufgaben und Berechtigungen, die ihrerseits durch Bildung funktionaler Domänen unterstützt werden können.

Für die konkrete Ausbildung von funktionalen Domänen ist deshalb neben Szenarienspezifika ausschlaggebend, welche administrativen Domänen berücksichtigt werden müssen. Für diese können die folgenden drei Kategorien unterschieden werden:

1. *Organisationsübergreifende Domänen* legen Verwaltungsbereiche fest, die bei interorganisationalen Szenarien jeweils konzertiert, beispielsweise durch ein gemeinsames Betreibergremium, bearbeitet werden.
2. *Organisationsinterne Domänen* bilden die Verwaltungsbereiche innerhalb einzelner Organisationen ab. Wie in Abschnitt 3.1.1 diskutiert wurde, sind die Verantwortlichkeiten für das Sicherheitsmanagement nicht notwendigerweise zentral bzw. decken sich nicht zwingend mit der übrigen Organisationsstruktur von Unternehmen und müssen unter Berücksichtigung der Delegationskonzepte auf (Sub-)Domänen abgebildet werden.

3. *Kundenspezifische Domänen* ermöglichen insbesondere beim Einsatz mandantenfähiger Security-Frameworks die gezielte Nutzung von Teilen der über die Managementplattform angebotenen Funktionalität durch Kunden.

Neben der logischen Strukturierung, die durch die Domänenbildung ermöglicht wird, dient diese auch als Basis für Berechtigungskonzepte, die festlegen, welche Akteure im Rahmen ihres Aufgabenumfangs welche Managementfunktionalität in welchem Umfang nutzen dürfen. Bereits in Abschnitt 2.2.1 wurde ein allgemeiner Überblick über die im Umfeld von Security-Frameworks relevanten Rollen gegeben, die sich den beschriebenen Domänen wie folgt zuordnen lassen:

- *Administratoren* sind für die Konfiguration und den laufenden Betrieb der MOs in den Domänen, denen sie zugeordnet sind, zuständig. Eine weitere Untergliederung kann wiederum beispielsweise anhand funktionaler Bereiche – unter Anlehnung an das OSI-Management beispielsweise in Fehler-, Konfigurations-, Abrechnungs-, Performance- und Sicherheitsmanagement (FCAPS) – vorgenommen werden. Auch die Managementplattform selbst stellt ein zu administrierendes MO dar. Administrative Rollen können in allen drei Kategorien administrativer Domänen eingesetzt werden; eine Häufung ist typischerweise in organisationsinternen Domänen anzutreffen, da auf dieser Ebene die meisten administrativen Aufgaben anfallen und eine Spezialisierung durchgeführt wird.
- *Anwender* kommen mit von Managementplattformen gebotenen Funktionalität in der Regel ausschließlich über dedizierte Self-Service-Portals in Kontakt, die eine Delegation managementrelevanter Aufgaben an einzelne Dienstnutzer vorsehen. Beispiele umfassen das dienstübergreifende Passwort- und Benutzerzertifikatsmanagement. Die Rolle ist im Allgemeinen fest an kundenspezifische Domänen gebunden.
- *Auditoren* haben die zu Administratoren und Security Engineers komplementäre Aufgabe, die Ergebnisse der von diesen durchgeführten Tätigkeiten zu überprüfen und auf dieser Basis einen Soll-Ist-Abgleich der MOs in ihren Domänen durchzuführen. Im Allgemeinen haben zumindest organisationsinterne Auditoren einen breiteren, aber auf lesenden Zugriff beschränkten Zugang zu MOs als Administratoren. Audits können jedoch auch in organisationsübergreifenden Szenarien und von Kunden, beispielsweise in Form so genannter Lieferantenaudits, durchgeführt werden und müssen entsprechend unterstützt werden.
- Das *Management*, hier im Sinne der Leitung einer Organisation oder eines Unternehmensverbunds verwendet, nutzt die Managementplattform primär im Rahmen des Berichtswesens. Im Unterschied zu Auditoren ist zwar die Menge der dabei betrachteten MOs noch größer, der Abstraktionsgrad aber ebenfalls höher. Über die Konformität hinausgehend werden dabei auch die Effektivität und Effizienz beurteilt.
- *Entwickler* sind zum einen für die Weiterentwicklung der Managementplattform zuständig, beispielsweise wenn Fehler bekannt werden, veränderte Anforderungen vorliegen oder weitere Werkzeuge integriert werden müssen. Zum anderen nutzen sie die Managementplattform zur Analyse von Abhängigkeiten zwischen MOs beispielsweise bei der Planung der Einführung neuer Security-Frameworks (vgl. Abschnitt 5.6). Analog zu Administratoren können auch Entwickler in allen drei Arten administrativer Domänen eingesetzt werden.
- *Prozesseigner* verfolgen bei der Nutzung der Managementplattform eine mit derjenigen

von Auditoren und Managern vergleichbare Zielsetzung, orientieren sich hinsichtlich der Zusammenstellung der für sie relevanten MOs jedoch an den Prozessen, für die sie zuständig sind. Sie delegieren ihre Aufgaben und Berechtigungen im Rahmen der in Abschnitt 6.5 diskutierten Prozesse üblicherweise an *Prozessmanager* oder andere mit der operativen Verantwortung betraute Rollen. Der Schwerpunkt der Betrachtung liegt dabei auf der organisationsinternen Umsetzung, die für jeden Prozess spezifisch organisationsübergreifend erweitert werden kann.

- *Security Engineers* übernehmen alle operativen Aufgaben, beispielsweise bei der Aufklärung von mit Security-Frameworks in Verbindung stehenden Sicherheitsvorfällen. Sie sind damit bezüglich ihrer Berechtigungen mit auf das Sicherheitsmanagement spezialisierten Administratoren vergleichbar, haben dabei jedoch einen mit Auditoren vergleichbaren Bereich von MOs, für die sie zuständig sind.

Die Zuweisung von Akteuren zu Rollen ist im Allgemeinen dynamisch und dem aktuellen Bedarf anzupassen. Beispielsweise kann im Rahmen des ITSM-Prozesses Incident Management auch der Service Desk bzw. First Level Support die Rolle eines Security Engineers einnehmen und bei akuten Sicherheitsvorfällen erste Notfallmaßnahmen veranlassen. Die Rollenverwaltung selbst unterliegt dabei wieder Policies, die z. B. sicherstellen, dass sich die Mengen Administratoren und Auditoren eines Bereichs nicht überlappen (engl. *separation of duties*).

Als Akteure, die in den genannten Rollen auftreten, sind neben natürlichen Personen auch Softwarewerkzeuge bzw. MOs zu betrachten, sofern diese ausgewählte Aufgaben automatisieren. Denkbar sind beispielsweise die Zuordnungen von Monitoringwerkzeugen zu Auditoren, Intrusion Prevention Systemen zu Security Engineers und Datenaustauschwerkzeugen zu anderen Managementsystemen mit Administratoren.

Analog zu den Zuständigkeiten im Rahmen des Lebenszyklus von Security-Frameworks (vgl. Kapitel 5) ergänzen sich die Rollen bezüglich ihrer Verantwortlichkeiten für einzelne Aufgaben. Für konkrete Anwendungsfälle kann deshalb beispielsweise über RASCI-Matrizen abgebildet werden, dass Administratoren für eine Aufgabe operativ verantwortlich sind, hierbei von Security Engineers unterstützt und von Auditoren kontrolliert werden, über deren Ergebnisse die Prozesseigner informiert werden und für die das Management rechenschaftspflichtig ist. Zur Unterstützung der Automatisierung dieser Abläufe und der damit verbundenen Informationsflüsse kann eine solche RASCI-Matrix beispielsweise Bestandteil einer Policy sein.

6.4.4.2. Vorgehen für die Spezifikation eines Kommunikationsmodells für das Management von Security-Frameworks

Mit dem Kommunikationsmodell wird das Ziel verfolgt, die Eckdaten für den Informationsfluss zwischen den identifizierten Akteuren bzw. Rollen und den im Rahmen der Managementarchitektur betrachteten MOs festzulegen. Es umfasst somit nicht nur atomare Steuer- und Kontrollanweisungen, sondern dient auch der Abbildung komplexer Arbeitsabläufe auf zwischen beteiligten Entitäten auszutauschende Nachrichten.

Basierend auf den in der Praxis vorherrschenden und zum Teil von den Security-Frameworks antizipierten Managementarchitekturen wird im Folgenden als grundlegende Entscheidung vom klassischen Manager-Agenten-Modell, wie es sich bereits beim oben diskutierten OSI-Management findet, und nicht etwa von einem Peer-to-Peer-Managementansatz ausgegangen.

Analog zum Client-/Servermodell wendet sich die Entität mit der Rolle *Manager* dabei an eine Entität mit der Rolle *Agent* mit dem Auftrag, bestimmte Informationen bereitzustellen oder Operationen auszuführen. Es ist allgemein von einer m:n-Beziehung zwischen Managern und Agenten auszugehen (vgl. [HAN99, S. 105f.]). Dieselbe Entität kann im Rahmen verschiedener Kommunikationsbeziehungen in unterschiedlichen Rollen agieren.

Bei der Festlegung und Implementierung konkreter Datenaustauschprotokolle wurde im Rahmen dieser Arbeit eine schrittweise verfeinernde Vorgehensweise gewählt. Im ersten Schritt wurde festgelegt, welche **Arten von Einzelnachrichten** prinzipiell zwischen Entitäten ausgetauscht werden können; dies umfasst:

- Nachrichten zur Ereignismitteilung (Signalisierung): Eine Entität wie eine SF-Schutzkomponente informiert eine andere Entität – beispielsweise ein Managementwerkzeug – über ein eingetretenes Ereignis, z. B. einen ausgelösten Sicherheitsvorfall. Die zu modellierenden Nachrichteninhalte hängen eng mit der Funktionalität der die Nachricht emittierenden Entität und dem Informationsmodell zusammen; für Sicherheitsereignisse kann beispielsweise wie oben erläutert auf das Format IDMEF zurückgegriffen werden.
- Nachrichten zur Datenweitergabe im Rahmen von Arbeitsabläufen (Steuerung): Zur Bildung von Bearbeitungsketten müssen Daten von einer Entität an andere Entitäten übergeben werden können; beispielsweise muss eine SF-Managementkomponente einen vom Managementsystem vorgegebenen Konfigurationsparameter in allen relevanten SF-Schutzkomponenten umsetzen.
- Nachrichten im Rahmen von Request-Response-Operationen, die beispielsweise dazu genutzt werden können, dass der Manager vom Agenten Informationen, beispielsweise einen Messwert zum aktuellen Status oder zur Überprüfung des korrekten Werts eines Konfigurationsparameters, abruft.

Neben den **Nachrichteninhalten** sind generell auch die für jede Nachricht **notwendigen Metadaten** festzulegen, die sich wiederum z. B. aus Sicherheitsanforderungen ergeben können: Beispielsweise könnte für Ereignismitteilungen eine digitale Signatur zur Sicherstellung der Authentizität der Absenderentität und für Request-Response-Nachrichten eine Ende-zu-Ende-Verschlüsselung gefordert werden; der zu erfüllende Schutzbedarf hängt auch von der szenarienspezifischen Klassifizierung der ausgetauschten Informationen ab.

Der syntaktischen Spezifikation der möglichen Nachrichten folgt in einem zweiten Schritt die Festlegung der am Nachrichtenaustausch beteiligten Kommunikationspartner im Rahmen der unterstützten **Kommunikationsbeziehungen**, die wiederum eng mit dem Funktionsmodell zusammenhängen. Generell ist zu unterscheiden, ob eine Nachricht an einen einzelnen Empfänger gerichtet werden soll oder ob Multicast- und Broadcastmechanismen benötigt werden: Insbesondere Ereignismitteilungen sind im Allgemeinen für mehrere Empfänger relevant, die dem Absender nicht zwingend a priori bekannt sind, so dass zur Umsetzung auf Kommunikationsmedien wie Service-Bus-Architekturen zurückgegriffen werden muss.

Im dritten Schritt erfolgt über die Bildung so genannter **Profile** die Definition der Abläufe beim Nachrichtenaustausch. Jedes Profil umfasst die Angaben,

- Für welche Kommunikationspartner (Absender; Menge der Empfänger)
- welche Nachrichten in welcher Reihenfolge zur Abbildung der entsprechenden Abläufe (Signalisierung, Steuerung bzw. Dialog) inklusive eines Austausches von Metadaten,

beispielsweise zur gegenseitigen Authentifizierung der Kommunikationspartner, auszutauschen sind,

- wie dabei eine Fehlerbehandlung erfolgen soll, beispielsweise falls die Gegenseite nicht verfügbar ist, beim Metadatenaustausch Fehler auftreten (z. B. fehlgeschlagene Authentifizierung) oder die Informationen vom Agenten nicht entgegengenommen bzw. bereitgestellt werden können, und
- wie über den Verlauf des Nachrichtenaustausches und dabei aufgetretene Fehler Protokoll geführt wird, um z. B. technische Audits zu unterstützen.

Im abschließenden vierten Schritt werden die Profile mit konkreten **Transportmechanismen** verknüpft (engl. *Binding*). In der Regel erfolgt die Kommunikation datennetzgebunden, beispielsweise über Web-Services (z. B. SOAP, XML-RPC), IP-basierte Netzmanagementprotokolle wie SNMP, per E-Mail (z. B. SMTP) oder über Message Queues bzw. Service-Busse.

Mit steigender Anzahl beteiligter Entitäten werden zur Unterstützung der sicheren Kommunikation zusätzliche Dienste benötigt; hierzu gehören beispielsweise:

- Eine *Authentifizierungs- und Autorisierungsinfrastruktur*, die von Agenten und Managern genutzt werden kann, um die Authentizität ihres Kommunikationspartners zu überprüfen und mit deren Hilfe die Berechtigungen der Manager zentral verwaltet werden können.
- Ein *Registrierungsdienst*, bei dem Manager und Agenten ihre Kommunikationsendpunkte hinterlegen und für potentielle Kommunikationspartner auffindbar machen können.
- Ein *Subskriptionsdienst*, über den sich Manager und Agenten in die Verteilerlisten für Multicasts und Broadcasts eintragen können, z. B. um die Sicherheitsereignismeldungen ausgewählter Sicherheitsmechanismen zu erhalten.

Wie in Abschnitt 6.4.1 dargestellt wurde, existieren bislang keine einheitlichen Schnittstellen und Protokolle zum Management von Sicherheitsmechanismen. Analog dazu sind einheitliche Formate für Protokolldateieinträge mit sicherheitsrelevanten Ereignissen erst seit kurzer Zeit Gegenstand von Standardisierungsbemühungen (vgl. [MIT11a]). Bei der Implementierung von Managementplattformen sind deshalb ggf. Gatewaykomponenten erforderlich (vgl. SF-Basiskomponenten im Informationsmodell), um die über Managementprotokolle übertragenen Steuerbefehle automatisiert in die erforderlichen Operationen, beispielsweise die Modifikation von Konfigurationsdateien, umsetzt. Hierzu können Managementwerkzeuge wie cfEngine [Bur05] eingesetzt werden, die z. B. im Rahmen des Customizings von Security-Frameworks als Schnittstellenkomponenten vorgesehen werden (vgl. Abschnitt 5.5).

6.4.4.3. Systematik des Funktionsmodells für das Management von Security-Frameworks

Das Funktionsmodell hat die Aufgabe, den Gesamtkomplex des Managements von Security-Frameworks in Bereiche zu untergliedern, für die generische Managementfunktionen definiert werden können. Diese können von Managementanwendungen genutzt werden, ohne Implementierungsspezifika vorwegzunehmen oder die Anwendungsbereiche einzuschränken.

Die Festlegung der Funktionsbereiche entspricht einer Gruppierung bzw. Strukturierung, die unter verschiedenen Gesichtspunkten durchgeführt werden kann; beispielsweise sieht das OSI-Management die Einteilung in die fünf FCAPS-Bereiche vor. Um die Rolle einer Managementplattform für Security-Frameworks im Rahmen des gesamtheitlichen Sicherheitsmanagements zu betonen, wird nachfolgend jedoch eine an denjenigen Managementprozessen orientierte Einteilung vorgenommen, die in diesem Kapitel bezüglich ihrer Relevanz für Security-Frameworks diskutiert werden. Auf dieser Basis erfolgt die Grobstrukturierung anhand folgender Prozesskategorien:

- Operatives Sicherheitsmanagement
- Risikomanagement
- IT Service Management
- Security Reporting

In jeder dieser Prozesskategorien können die in den anderen Abschnitten in diesem Kapitel beschriebenen Prozesse zur weiteren Untergliederung herangezogen werden; beispielsweise sind das technische Konfigurationsmanagement und die Zugriffsverwaltung Bestandteile des operativen Sicherheitsmanagements und das IT Service Management besteht u. a. aus Incident Management und Change Management. Abbildung 6.17 gibt einen Überblick über die resultierenden Prozesse und Funktionskategorien.

Eine Managementplattform muss Funktionalität zur Unterstützung der in diesen Prozessen relevanten Abläufe bereitstellen. Somit können die Inhalte des Funktionsmodells durch die Verallgemeinerung von Anwendungsfällen (engl. *Use Cases*) abgeleitet werden, die beschreiben, wie die Managementplattform im Rahmen des jeweiligen Prozesses genutzt werden sollte. Diese Methodik wird nachfolgend exemplarisch für ausgewählte Aspekte des in Abschnitt 6.3 beschriebenen Risikomanagements beim Einsatz von Security-Frameworks demonstriert. Eine vollständige Beschreibung aller Anwendungsfälle in allen Prozesskategorien könnte beispielsweise auf Basis von Szenarienanalysen erfolgen, liegt jedoch nicht im Fokus dieser Arbeit; vielmehr wird im Anschluss an das Beispiel gezeigt, wie sich bereits aus wenigen Anwendungsfällen generische Funktionen ableiten lassen.

Das hier exemplarisch betrachtete Risikomanagement besteht wie oben erläutert aus nur einem Prozess, der drei Phasen bzw. Teilprozesse umfasst:

1. Risikoermittlung
2. Risikobewertung
3. Risikosteuerung

Die **Risikoermittlung** (RE) erfolgt durch als Risikomanager bezeichnete Akteure, die die hier skizzierte Managementplattform in der Rolle *Security Engineer* im Rahmen der folgenden Anwendungsfälle nutzen können:

- Anwendungsfall RE1: Der Risikomanager muss den Anwendungsbereich für die aktuelle Prozessinstanz des Risikomanagements festlegen. Hierzu liegt ihm eine Liste von Diensten oder Assets vor, die im Kern seiner Betrachtung liegen; von diesen ausgehend benötigt er jedoch Informationen über deren jeweiliges Umfeld wie z. B. Dienstabhängigkeiten oder involvierte Sicherheitsmechanismen. Über die in der Management-

Prozesskategorie	Funktionskategorien gemäß (Teil-)Prozessen und Phasen
Operatives Sicherheitsmanagement	Systemsicherheit
	Netzsicherheit
	Zugriffsverwaltung
	(Hoch-)Verfügbarkeit
	Kryptographische Mechanismen
	Präventive/validierende Maßnahmen
	Security Information & Event Management
Risikomanagement	Risikoermittlung
	Risikobewertung
	Risikosteuerung
Sicherheitsmanagement	Policy Management
(nach ISO/IEC 27001)	Verwaltung von Rollen und Zuständigkeiten
	Asset Management
	Personelle Sicherheit
	Physische Sicherheit
	Betriebs- und Kommunikationssicherheit
	Zugangskontrolle
	Beschaffungs-, Entwicklungs- und Wartungsmanagement
	Security Incident Management
	Business Continuity Management
	Compliance Management
IT Service Management	Demand Management
	Portfolio Management
	Financial Management
	Service Catalogue Management
	Service Level Management
	Capacity Management
	Availability Management
	Supplier Management
	Transition Planning and Support
	Change Management
	Configuration Management
	Release and Deployment Management
	Service Validation and Testing
	Evaluation
	Knowledge Management
	Event Management
	Incident Management
	Request Fulfillment
	Problem Management
Security Reporting	Messen
	Metrikdefinition
	Ist-/Soll-Vergleich
	Kosten-/Nutzen-Analyse
	Berichtswesen

Abbildung 6.17.: Übersicht über die zu betrachtenden Funktionskategorien

plattform verwalteten MOs und Verknüpfungen kann er eine Liste der relevanten Assets generieren. Security-Frameworks fungieren dabei als Aggregatoren für die von SF-Schutzkomponenten implementierten Sicherheitsmechanismen und halten somit die Anzahl zu betrachtender einzelner Assets gering.

- Anwendungsfall RE2: Der Risikomanager muss die ermittelten Assets priorisieren. Die Managementplattform liefert ihm hierfür die Werte und den Schutzbedarf der Assets. Ferner kann in den Konzepten der eingesetzten Security-Frameworks recherchiert werden, welche Schwerpunkte szenarienunabhängig zu setzen sind.
- Anwendungsfall RE3: Der Risikomanager muss die für die auf Basis der Priorisierung ausgewählten Assets relevanten Bedrohungen bestimmen. Über die Managementplattform hat er Zugriff auf die bereits bekannten Angreifermodelle, Bedrohungsszenarien

und Bedrohungen; diese können das Ergebnis früherer Instanzen des Risikomanagementprozesses oder beispielsweise durch neue Versionen von Security-Frameworks eingespeist worden sein. Über in die Managementplattform integrierte Werkzeuge kann der Risikomanager zur besseren Übersicht beispielsweise Attack-Trees konstruieren. Aktualisierte und ergänzte Informationen können über die Managementplattform gespeichert werden.

- Anwendungsfall RE4: Der Risikomanager muss die aktuell vorliegenden Schwachstellen bestimmen. Über die Managementplattform hat er die Möglichkeit, auf die bereits bekannten Schwachstellen und deren Auswirkungen auf den Schutzbedarf zuzugreifen. Darüber hinaus kann er über integrierte Managementwerkzeuge beispielsweise Penetrationstests, Vulnerability-Scans und Selbsttests der Security-Frameworks anstoßen, die CVSS2-Scores auf den aktuellen Stand bringen und überprüfen, welche Schwachstellen seit der letzten Prozessinstanziierung hinzugekommen sind.
- Anwendungsfall RE5: Der Risikomanager muss die bereits vorhandenen Sicherheitsmechanismen bestimmen. Die Managementplattform stellt ihm hierzu – über die Security-Framework-MOs aggregiert – Informationen über die von den SF-Schutzkomponenten erbrachten Maßnahmen in Relation zu den vom Security-Framework betrachteten Bedrohungen und Schwachstellen zur Verfügung; analog dazu können Informationen über die anderen, von Security-Frameworks unabhängigen Sicherheitsmechanismen abgerufen werden.

Ein schreibender Zugriff auf die jeweils benötigten MOs wie in Anwendungsfall RE4 findet auch im Rahmen anderer Prozesse statt; beispielsweise wird der Schutzbedarf in Abstimmung mit Kunden im Rahmen des Service Level Management festgelegt. Daten, die originär in anderen Managementsystemen verwaltet werden, können über Automatismen mit dem Datenbestand dieser Managementplattform abgeglichen oder geeignet verknüpft werden.

Im Rahmen der **Risikobewertung** (RB) sind die folgenden Anwendungsfälle für die Managementplattform zu betrachten:

- Anwendungsfall RB1: Der Risikomanager muss die Eintrittswahrscheinlichkeit eines Schadereignisses bestimmen. Er kann hierzu über die Managementplattform sowohl auf umgebungsspezifische Informationen wie den CVSS2 Environmental Score als auch auf Daten früherer Sicherheitsvorfälle, die sich aus den betrachteten Bedrohungen ergeben haben, zugreifen. Ebenso kann die bei SF-Komponenten erfasste Zuverlässigkeit berücksichtigt werden.
- Anwendungsfall RB2: Der Risikomanager muss die Auswirkungen eines Schadereignisses bestimmen. Mit Hilfe der Managementplattform kann er neben der Analyse der Abhängigkeiten zwischen Assets und deren Werten auch ermitteln, welche Kunden und somit welcher Benutzerkreis potentiell betroffen ist; diese Angaben können beispielsweise mit Risikomanagementwerkzeugen im Rahmen des erläuterten DREAD-Verfahrens ausgewertet werden.
- Anwendungsfall RB3: Der Risikomanager muss die Risiken quantifizieren und dokumentieren. Als Bestandteil der Risikodokumentation werden die quantifizierten Risiken bzw. die ermittelten Risikoklassen über die Managementplattform festgehalten. Zur Beurteilung veränderter Risiken kann eine Gegenüberstellung mit früheren Werten durchgeführt werden.

Schließlich müssen bei der **Risikosteuerung** (RS) die folgenden Anwendungsfälle berücksichtigt werden:

- Anwendungsfall RS1: Der Risikomanager muss beurteilen, ob das Risiko ausreichend gering für eine Risikoakzeptanz ist. Diese Entscheidung kann von Variablen abhängen, beispielsweise welche oder wie viele Kunden den betroffenen Dienst aktuell mit welchem Schutzbedarf beziehen, und ist über Policies abgebildet, die ebenfalls über die Managementplattform zur Verfügung gestellt werden.
- Anwendungsfall RS2: Der Risikomanager muss beurteilen, wie stark eine zur Auswahl stehende Maßnahme das betrachtete Risiko reduziert. Zu diesem Zweck kann er in die Managementplattform integrierte Planungswerkzeuge nutzen, die beispielsweise auch beim Customizing von Security-Frameworks zum Einsatz kommen, um beispielsweise verschiedene Einsatzvarianten zusätzlicher Sicherheitswerkzeuge oder entsprechender Erweiterungen bestehender Security-Frameworks zu evaluieren.
- Anwendungsfall RS3: Der Risikomanager stößt die Umsetzung einer Maßnahme zur Risikoreduktion an. Er knüpft dabei an den vorstehenden Anwendungsfall RS2 an, indem er in Abstimmung mit dem Change Management im Rahmen der Evaluation ausgewählte Mechanismen als MOs mit dem Status „*in Planung*“ anlegt, diesen die entsprechenden Verantwortlichkeiten zuweist und einen Verweis auf die Dokumentation der Ergebnisse des Risikomanagements einträgt.
- Anwendungsfall RS4: Der Risikomanager muss über die erfolgte Umsetzung einer Maßnahme zur Risikoreduktion informiert werden. Er kann sich dazu automatisch benachrichtigen lassen, beispielsweise wenn der Status einer im Rahmen des Risikomanagements vorgeschlagenen zusätzlichen Komponente für ein Security-Framework auf „*in Betrieb*“ ändert.
- Anwendungsfall RS5: Der Risikomanager erstellt einen Bericht über die Wirksamkeit der vorhandenen Schutzmaßnahmen und verbleibende Risiken. Er nutzt hierfür über die Managementplattform die Reporting-Funktionalität u. a. der Security-Frameworks, die über die in den vorangegangenen Anwendungsfällen eingetragenen Informationen zur Risikobeurteilung hinausgehend auch Daten z. B. über erkannte Sicherheitsvorfälle sowie die reguläre Nutzung bereitstellt.

Obwohl das Risikomanagement nur einer von vielen Nutzern der Managementplattform ist, lassen sich aus den beschriebenen Anwendungsfällen die folgenden Basisfunktionen ableiten, die ggf. noch MO-spezifisch weiter zu verfeinern sind:

- Managed Objects müssen erzeugt (*create*), gelesen (*read*) und gelöscht (*delete*) werden können.
- Attribute von Management Objects müssen hinzugefügt (*add*), gelesen (*read*), modifiziert (*write*) und gelöscht (*delete*) werden können. Über Attribute müssen auch Verknüpfungen zwischen Managed Objects gepflegt werden können.
- Managed Objects müssen Benachrichtigungen über Zustandsänderungen senden können (*notify*).
- Managed Objects müssen Testmöglichkeiten bereitstellen, mit denen die Auswirkungen z. B. von Änderungen oder Angriffen evaluiert werden können, ohne den Produktivbetrieb einzuschränken (*test*).

- Managed Objects müssen die Erstellung von Berichten unterstützen, indem sie Gruppen dafür relevanter Attribute zu vorgegebenen Zeitpunkten bereitstellen (*report*).

Die Nutzung dieser grundlegenden sowie darauf aufbauender Funktionen wird über ein Berechtigungskonzept gesteuert, das festlegt, welche Akteure bzw. Rollen (Subjekte) für welche MOs (Objekte) welche Funktionen (Aktionen) nutzen dürfen. Weitere Einschränkungen können sowohl anhand der übergebenen Parameter, so dass beispielsweise nur bestimmte Attributwerte gesetzt werden dürfen, als auch anhand des aktuellen Zustands der MOs vorgenommen werden, so dass beispielsweise bei komplexen Datentypen nur Teile von Attributen ausgelesen werden dürfen, für die das Subjekt eine Freigabe enthalten hat. Der Funktionsaufruf kann zudem mit Obligationen verbunden sein, die beispielsweise dazu führen, dass die Managementoperation von der jeweiligen Managementanwendung protokolliert wird, um eine technische Auditierung zu ermöglichen. Entsprechende Regelsätze können beispielsweise als XACML-Policies formuliert und von in die Managementplattform integrierten Policy Decision Points und Policy Enforcements Points ausgewertet bzw. umgesetzt werden (vgl. [XACML3]).

Sowohl zur Anwendung als auch zur Bereitstellung dieser Funktionalität sind auch die in die Managementplattform zu integrierenden Sicherheitswerkzeuge zu betrachten; dies ist Gegenstand des folgenden Abschnitts.

6.4.5. Zusammenspiel mit sicherheitsspezifischen Managementwerkzeugen

Zu den Zielen der in dieser Arbeit konzipierten Managementarchitektur für Security-Frameworks gehört auch, existierende, relevante Sicherheitsmanagementwerkzeuge in die Managementplattform zu integrieren. Zu diesem Zweck ist es nicht nur erforderlich, diese Werkzeuge über die Nutzung der oben beschriebenen Schnittstellen in einer gemeinsamen Benutzeroberfläche zusammenzufassen, sondern sie müssen sich auch stärker an den Charakteristika und Spezifika von Security-Frameworks ausrichten. Hierzu gehören insbesondere die folgenden Aspekte:

- Die technischen Komponenten von Security-Frameworks bilden z. T. sehr umfangreiche und komplexe verteilte Systeme; die dabei auftretenden systemübergreifenden Abhängigkeiten sind auf Basis des Informationsmodells erfasst und müssen, beispielsweise durch eine enge Kopplung mit Configuration-Management-Werkzeugen wie einer CMDB, geeignet berücksichtigt werden.
- Security-Frameworks sind modular aufgebaut und im Allgemeinen mit dem Ziel einer einfachen Erweiterbarkeit konzipiert. Managementwerkzeuge müssen mit der resultierenden Dynamik der Architektur der Frameworkinstanz umgehen können und dürfen sich nicht auf das Vorfinden fest vorgegebener Ausprägungen verlassen.
- Durch die Ausrichtung auf hohe Adaptivität zur Laufzeit trifft die beschriebene Dynamik nicht nur auf die Komponenten, sondern auch auf deren jeweils aktuelle Parametrisierung zu. Insbesondere können durch Automatismen zur Laufzeit Änderungen an SF-Schutzkomponenten eintreten, die z. B. von Überwachungs- und Testwerkzeugen während deren Einsatz berücksichtigt werden müssen, so dass diese nicht von einem festen Soll-Zustand ausgehen.
- Security-Frameworks verknüpfen technische und organisatorische Sicherheitsmaßnahmen eng miteinander. Entsprechend müssen auch zur Unterstützung eingesetzte Werk-

zeuge nicht nur unter rein technischen Kriterien, sondern auch mit Bezug auf die organisatorischen Abläufe ausgewählt und eingesetzt werden. Hierzu gehört beispielsweise auch die Unterstützung des für Security-Frameworks spezifischen Berichtswesens, so dass beispielsweise framework- und werkzeugübergreifend einheitliche Messungen und Indikatoren angewandt werden (vgl. Abschnitt 6.6).

- Unter der Orientierung an einem kontinuierlichen Verbesserungsprozess werden bekannte Defizite u. U. zunächst bewusst in Kauf genommen und erst mittelfristig behoben. In die Managementplattform integrierte Werkzeuge müssen darüber verfügbare Informationen berücksichtigen und zur Priorisierung der jeweils nächsten Schritte beitragen.

Diese Charakteristika von Security-Frameworks haben zwei allgemeine Auswirkungen auf unterstützende Managementanwendungen und -werkzeuge, die unabhängig von deren spezifischer Funktionalität sind:

- Änderungen, z. B. an der eingesetzten Software, deren Konfiguration oder den verarbeiteten Daten müssen konsistent über alle betroffenen Komponenten des Security-Frameworks umgesetzt werden.
- Die Werkzeuge müssen die bereits vorhandenen Informationen, z. B. über Assets, den jeweiligen Schutzbedarf und die spezifischen Risiken, verwenden und sich an den auch die Security-Frameworks steuernden Policies orientieren. Insbesondere müssen die für Security-Frameworks spezifischen Parameter auch von den Werkzeugen berücksichtigt bzw. von diesen übernommen werden, um ihren Einsatz auf die vorhandene Sicherheitsinfrastruktur abzustimmen.

Insgesamt wird die Zielsetzung verfolgt, sicherheitsspezifische Managementwerkzeuge über die Grenzen einzelner Security-Frameworks hinweg zu konsolidieren und in die Managementplattform zu integrieren, so dass sie einerseits über eine gemeinsame Oberfläche genutzt werden können und auf Basis der diskutierten Programmierschnittstellen operieren. Andererseits soll erreicht werden, dass auch die Ergebnisse ihrer Anwendung, soweit sie die über die Managementplattform verwalteten MOs betreffen, dort hinterlegt bzw. mit diesen verknüpft werden können. Für die Werkzeuge in den einzelnen Bereichen des operativen Sicherheitsmanagements wurden insbesondere die folgenden Auswirkungen ermittelt:

- Bezüglich der **Systemsicherheit** müssen Werkzeuge für das Management von Software-Updates und Patches, die auf die verwalteten MOs und damit auch auf die Security-Frameworks angewendet werden sollen, die komponentenübergreifende Konsistenz gewährleisten, beispielsweise indem Aktualisierungen im Rahmen desselben Wartungszeitraums eingespielt werden. Bei der werkzeugunterstützten Systemhärtung (*Hardening*) sollte eine Orientierung an den bekannten bzw. über die Managementplattform hinterlegten Risiken erfolgen. Die Härtung sollte insbesondere auch auf solche SF-Komponenten angewandt werden, die auf separaten Systemen laufen, deren Absicherung konzeptionell jedoch nicht betrachten. Die Managementplattform sollte generell Gebrauch von verfügbaren zentralen Diensten wie Authentifizierungs- und Autorisierungsinfrastrukturen, Logfile-Servern, etc. machen und diese auch dahingehend verwalten, dass die verwalteten MOs ebenfalls einfach angebunden werden können.
- Im Bereich der **Netzsicherheit** sind einerseits die von IDS-/IPS-Systemen bereitgestellten Sensoren zur Detektion von Sicherheitsvorfällen bezüglich ihres Abdeckungsbereichs

und ihrer Erkennungsfunktionalität auf die SF-Schutzkomponenten abzustimmen. Andererseits stellen Schutzmechanismen wie Firewalls die auch von Security-Frameworks mit am häufigsten eingesetzten Komponenten dar, so dass eine einheitliche Managementlösung für alle entsprechenden MOs umgesetzt werden sollte.

- Die Werkzeuge zum **Access Management** gehören zu denjenigen zentralen Diensten, die sowohl bei der Nutzung der Managementplattform als auch bei der Konfiguration der von ihr verwalteten MOs zum Tragen kommen sollten. Analog dazu sind die Konzepte zum Privileged Account Management auf die Managementplattform und alle MOs anzuwenden.
- Bei Werkzeugen zur Anwendung *kryptographischer Maßnahmen* ist primär die komponentenübergreifende Konsistenz der dafür relevanten Metadaten zu berücksichtigen; beispielsweise sollten Schlüsselpaare, Zertifikate, Algorithmen und Schlüssellängen frameworkübergreifend einheitlich verwendet werden, um den Mehraufwand für die parallele Verwaltung mehrerer Sätze an Metadaten zu vermeiden.
- Der Bereich der **präventiven und validierenden Maßnahmen** umfasst die meisten Werkzeuge, deren Integration in die Managementplattform einen unmittelbaren Mehrwert für die Anwendung darstellt. Beispielsweise können integrierte Werkzeuge für Penetrationstests wie oben beschrieben im Rahmen des Risikomanagements eingesetzt werden; sie können dazu bereits in der Managementplattform gespeicherte Informationen über Schwachstellen nutzen und diese aktualisieren. Zudem können sie auf Informationen über die Zusammenhänge zwischen den Komponenten zurückgreifen und dadurch gezieltere Untersuchungen durchführen.

  Zum Policy-Enforcement eingesetzte Werkzeuge können auf die in Policies hinterlegten Zielvorgaben zurückgreifen und die aktuellen Attributbelegungen der MOs auswerten, um unerwünschte Abweichungen zu identifizieren. Zudem können sie auf die vorgegebenen Alarmierungswege zurückgreifen, ohne die entsprechende Funktionalität dort separat implementiert und konfiguriert werden muss.

  Bezüglich der Akquisition von Sicherheitsinformationen sind Automatismen vorzusehen, die eine Übernahme aktueller Sicherheitsmeldungen in die Managementplattform ermöglichen und dabei die eventuell erforderlichen Transformationen durchführen. Über diesen Meldeweg können auch unabhängig von aktualisierten Frameworkkonzepten Hinweise zu erforderlichen Maßnahmen an SF-Komponenten eingehen, beispielsweise falls Implementierungsfehler in Standardkomponenten bekannt werden.

  Die Managementplattform trägt darüber hinaus maßgeblich zur Dokumentation der Sicherheitsmechanismen bei, beispielsweise indem sie die strukturierte Erfassung der Ergebnisse einzelner Arbeitsschritte unterstützt, durch Versionierung Aufschluss über frühere Zustände der einzelnen MOs gibt und die Verknüpfung der MOs mit weiteren Dokumenten und anderen Managementsystemen ermöglicht. Sie kann somit zum Festhalten der Entwicklungen seit dem Abschluss der Customizing- und Inbetriebnahmephasen bei Security-Frameworks genutzt werden.
- Analog dazu kann auch bei der Integration von **SIEM-Werkzeugen** auf die in der Managementplattform verwalteten Policies zurückgegriffen werden, um Diskrepanzen zwischen Ist- und Sollzuständen zu ermitteln und ggf. Alarmmeldungen zu generieren. Die Durchführung technischer Audits wird durch das Zusammenlaufen von Protokol-

len und Sicherheitsmeldungen erleichtert. Die Ergebnisse der Behandlung von Sicherheitsvorfällen im Rahmen des Security Incident Managements können wiederum in der Managementplattform abgelegt und mit den betroffenen MOs verknüpft werden. Auch bei der Erstellung von Berichten und weiterführenden Analysen können entsprechende Abläufe über Managementwerkzeuge abgebildet werden und auf den integrierten Datenbestand zugreifen.

Der Einsatz der Managementplattform und ihrer Werkzeuge erfolgt jedoch nicht nur im Rahmen des operativen Sicherheitsmanagements, sondern zu einem großen Teil auch aus anderen Managementprozessen heraus, auf die im folgenden Abschnitt eingegangen wird.

6.5. Security-Framework-Schnittstellen zu den Managementprozessen

Ein *integriertes* Management muss sich nicht nur über alle in einem Szenario eingesetzten Security-Frameworks erstrecken, sondern auch nahtlos mit den anderen darin relevanten Prozessen und Abläufen harmonieren. Die für Security-Frameworks spezifischen Managementaspekte müssen deshalb über die obige Betrachtung einer entsprechenden Managementarchitektur hinausgehend auch für weitere Prozesse analysiert werden.

Den in Kapitel 5 und in Abschnitt 6.1 identifizierten Schwerpunkten gemäß werden im Folgenden die Teilprozesse des Informationssicherheitsmanagements nach ISO/IEC 27001, die IT-Service-Management-Prozesse nach ITIL v3 und ergänzende, im Kontext der IT-Governance und Compliance relevante CobiT-Prozesse betrachtet, um die gegenseitigen Einflüsse zwischen Security-Frameworks und den jeweiligen Referenzprozessen darzustellen. Insgesamt handelt es sich dabei um Prozesse, die in fast allen Szenarien, in denen Security-Frameworks zum Einsatz kommen, essentiell sind, da zum einen die durch Security-Frameworks bereitgestellte Sicherheitsfunktionalität nicht nur technisch, sondern auch organisatorisch integriert werden muss und sich aufgrund der engen Bindung zwischen Security-Frameworks und den von ihnen geschützten Diensten bzw. Architekturen zwangsweise die im Rahmen von ITSM thematisierten komplexen Abhängigkeiten zwischen den Infrastrukturkomponenten ergeben.

Eine Betrachtung der *Spezifika* für Security-Framework wird dadurch erschwert, dass in der Literatur bislang noch nicht die dafür als Grundlage heranziehbaren *allgemeinen* Schnittstellen zwischen dem Sicherheitsmanagement und den ITSM-Prozessen umfassend systematisch erarbeitet wurden. Trotz der Auffassung des Security-Managements als Querschnittsprozess beispielsweise in ITIL fehlt dort, wie bereits in Abschnitt 2.2.3.3 angedeutet wurde, eine explizite und präzise Benennung der jeweiligen Schnittstellen und der zwischen dem Sicherheitsmanagement und den anderen Prozessen jeweils auszutauschen Informationen. Ebenso werden die ITSM-relevanten Schnittstellen, wie in Kapitel 4 ermittelt wurde, bislang nur von einem kleinen Teil der Frameworkkonzepte und auch von diesem nicht in der erforderlichen Breite berücksichtigt. Die in dieser Arbeit im Folgenden fokussierte Kernfragestellung ist deshalb, wie sich die jeweils betrachteten Managementprozesse und der Einsatz von Security-Frameworks gegenseitig beeinflussen und welche expliziten Schnittstellen in den Abläufen bzw. Lebenszyklen der Prozessinstanzen und Security-Frameworks berücksichtigt werden müssen. Diese Fragestellung wurde in der Literatur bisher nicht in der vorliegenden Breite und Vollständigkeit bezüglich der Prozesse untersucht.

ISO/IEC 27001 (Annex A) CONTROLS	NIST SP 800-53 CONTROLS *	AUP V5.0 CONTROLS
A.6 Organization of information security		
A.6.1 Internal		
A.6.1.1 Management commitment to information security	XX-1 controls, PM-2; SP 800-39, SP 800-37	B.3, C.1
A.6.1.2 Information security coordination	CP-2, CP-4, IR-4, PL-1, PL-6, PM-2, SA-2; SP 800-39, SP 800-37	
A.6.1.3 Allocation of information security responsibilities	XX-1 controls, AC-5, AC-6, CM-9. PM-2; SP 800-39, SP 800-37	
A.6.1.4 Authorization process for information processing facilities	CA-1, CA-6, PM-10; SP 800-37	
A.6.1.5 Confidentiality agreements	PL-4, PS-6, SA-9	C.1
A.6.1.6 Contact with authorities	Multiple controls with contact reference (e.g., IR-6, SI-5); SP 800-39; SP 800-37	
A.6.1.7 Contact with special interest groups	AT-5	
A.6.1.8 Independent review of information security	CA-2, CA-7; SP 800-39, SP 800-37	
A.6.2 External Parties		
A.6.2.1 Identification of risks related to external parties	CA-3, PM-9, RA-3, SA-1, SA-9, SC-7	
A.6.2.2 Addressing security when dealing with customers	AC-8 , AT-2, PL-4	
A.6.2.3 Addressing security in third party agreements	CA-3, PS-7, SA-9	C.2

Abbildung 6.18.: Prozesszuordnung am Beispiel ISO/IEC 27001 A.6, NIST SP 800-53 und AUP v5 (Quelle: [AICP10])

Die kombinierte Betrachtung von ISO/IEC 27001 bzw. seinem Vorgänger ISO/IEC 17799 als Rahmen für das Sicherheitsmanagement, ITIL als ITSM-Framework und CobiT als Referenz für das Governance- und Compliance-Management hat sich trotz der fehlenden Betrachtung expliziter Schnittstellen sowohl in wissenschaftlicher Literatur als auch Best Practices bewährt; über ebenfalls in verwandten Arbeiten erstellte Prozesszuordnungen (engl. *process mappings*) kann der Bezug zu anderen Prozessrahmenwerken hergestellt werden, so dass die hier erarbeiteten Ergebnisse auf andere Sicherheitsmanagement- bzw. ITSM-Ansätze übertragbar sind (vgl. dazu [Har06], [Sal04], [HC04], [CSTT06] und [SSA08]). Abbildung 6.18 zeigt dies exemplarisch am Beispiel des in Abschnitt 6.5.1.2 diskutierten Anhangs A.6 von ISO/IEC 27001, der NIST Special Publication SP 800-53 und den *Agreed Upon Procedures* (AUP), die von Auditoren häufig zur Evaluation eingesetzt werden.

Für alle nachfolgenden Unterabschnitte wurde eine einheitliche Struktur gewählt: Zunächst werden aus dem jeweils angegebenen Abschnitt der Spezifikation des Prozesses, wie sie sich in ISO/IEC 27001, ITIL v3 bzw. CobiT findet, die im Kontext von Security-Frameworks relevanten Ziele extrahiert und knapp beschrieben. Davon werden jeweils die Zusammenhänge mit dem Management von Security-Frameworks abgeleitet und die zu berücksichtigenden Randbedingungen und Schnittstellen konzipiert.

Diese Schnittstellen werden in einheitlich strukturierten Abbildungen aufbereitet, um das Zusammenspiel zwischen den extern spezifizierten Prozessen und deren Teilaufgaben zu den einzelnen Phasen des Lebenszyklus von Frameworkinstanzen darzustellen und damit den Kreis zu den in Kapitel 5 konzipierten Inhalten jeder Lebenszyklusphase zu schließen.

6.5.1. Security-Framework-Managementschnittstellen zu ISO/IEC 27001

Auf Basis der in [Hum08] von Humphreys vorgestellten Methode wird nachfolgend eine auf die für Security-Frameworks relevanten Managementschnittstellen maßgeschneiderte Betrachtung der im normativen Anhang A (Abschnitte A.5 bis A.15) von ISO/IEC 27001 bzw. in den Kapiteln 5–15 von ISO/IEC 27002 postulierten Maßnahmen und Abläufe vorgestellt. Diese bilden, wie in Abschnitt 2.1.2 diskutiert wurde, den Schwerpunkt der Norm und teilen die von ihr vorgesehenen Maßnahmen systematisch in elf Kategorien ein. Bei den nachfolgenden Betrachtungen wird auf eine erneute Behandlung des allen Kategorien zugrunde gelegten Aspekts Risikomanagement verzichtet, da er bereits in Abschnitt 6.3 vertieft wurde. Die Beschreibung enthält dabei einheitlich zunächst die mit dem jeweiligen Prozess verfolgten Ziele, die Einflüsse von und auf das Management von Security-Frameworks und die zu berücksichtigenden Schnittstellen zum Lebenszyklus von Frameworkinstanzen.

6.5.1.1. Schnittstellen zu ISO/IEC 27001 A.5: Sicherheitsleitlinie

Die von ISO/IEC 27001 geforderten Maßnahmen rund um die Sicherheitsleitlinie einer Organisation haben die folgenden ausgewählten Ziele, aus denen sich wie nachfolgend erläutert Berührungspunkte mit dem Management von Security-Frameworks ergeben:

- Die Sicherheitsleitlinie definiert das Anwendungsgebiet und die Ziele des Informationssicherheitsmanagements einer Organisation.
- Sie regelt das Zusammenspiel zwischen dem organisatorischen und technischen Sicherheitsmanagement mit den Geschäftsprozessen.
- Sie benennt die für die Organisation im Kontext der Informationssicherheit relevanten gesetzlichen und vertraglichen Anforderungen.
- Sie regelt das Vorgehen bei der Zuweisung von Verantwortlichkeiten im Umfeld der Informationssicherheit und legt einen Rahmen für Sicherheitsausbildungen und Trainingsprogramme fest.
- Sie definiert die bei Verstößen gegen die Leitlinie und die anderen Richtlinien bzw. Policies drohenden Konsequenzen.
- Sie verweist auf weitere Richt- und Leitlinien sowie andere, sicherheitsspezifische Dokumente mit relevanten Informationen.
- Sie wird regelmäßig überprüft und bei Bedarf überarbeitet; die Basis dafür bilden Audits, sich im Laufe der Zeit ergebende Änderungen an Bedrohungen und Schwachstellen sowie Berichte über Informationssicherheitsvorfälle und externe Empfehlungen.

Somit bestehen zwischen dem Management von Security-Frameworks und den Arbeiten an der organisationsweiten Sicherheitsleitlinie die folgenden Zusammenhänge:

- Security-Frameworks decken die Sicherheitseigenschaften größerer, komplexer Teile der gesamten Infrastruktur ab, so dass der Anwendungsbereich jedes Security-Frameworks eine Teilmenge des Anwendungsbereichs der Sicherheitsleitlinie darstellt. Security-Frameworks können somit einerseits als Strukturierungsmittel eingesetzt werden; andererseits ist in der Leitlinie zu berücksichtigen, dass das Paradigma *defense-in-depth* z. B. durch einander partiell überlappende Security-Frameworks umgesetzt werden kann.

- Die von Security-Frameworks bereitgestellten Sicherheitsmechanismen liefern Hinweise auf Verstöße und Sicherheitsvorfälle; ihre regelmäßig überarbeiteten Konzepte gehen auf die Weiterentwicklungen von Bedrohungen und Schwachstellen ein. Security-Frameworks leisten somit Beiträge, die bei der Fortschreibung der Sicherheitsleitlinie berücksichtigt werden müssen.
- In den Konzepten von Security-Frameworks werden Schulungsaspekte für verschiedene Zielgruppen wie Administratoren und Benutzer betrachtet; diese sind in die allgemeinen Konzepte für Informationssicherheitsschulungen zu integrieren.
- Die Frameworkkonzepte bzw. die zu Frameworkinstanzen erstellten Dokumentationen können zum Kreis der Dokumente zählen, auf die in der Sicherheitsleitlinie verwiesen wird.
- Bei der Auswahl von Security-Frameworks muss auf eine Vereinbarkeit mit den Anwendungsgebieten und Zielen des organisationsweiten Sicherheitsmanagements, den bekannten gesetzlichen und vertraglichen Auflagen, den als relevant erachteten Bedrohungen und Schwachstellen sowie den Anforderungen an die bereitzustellenden Informationen über Sicherheitsvorfälle etc. geachtet werden.
- Der Betrieb von Security-Frameworks hat unter der Maßgabe zu erfolgen, die Vorgaben der Leitlinie kontinuierlich umzusetzen. Neben der operativen Unterstützung durch bereitgestellte Sicherheitsfunktionalität müssen folglich auch Compliance-Aspekte berücksichtigt werden.

Als Randbedingungen und Schnittstellen zwischen den beiden Prozessen sind folglich vorzusehen:

- O. B. d. A. kann davon ausgegangen werden, dass die Leitlinie bereits existiert, bevor in einem Szenario Security-Frameworks eingeführt werden sollen.
- Die Einführung oder die umfassendere Überarbeitung eines Security-Frameworks kann inhaltliche Anpassungen der Leitlinie oder mit ihr verknüpfter Dokumente erforderlich machen; hierzu inverse Änderungen werden bei der Außerbetriebnahme von Security-Frameworks erforderlich.
- Security-Frameworks liefern im laufenden Betrieb Informationen, die zur Weiterentwicklung der Leitlinie beitragen.
- Änderungen an der Leitlinie müssen geeignet im Security-Framework umgesetzt werden, beispielsweise durch eine Überarbeitung der Parametrisierung im Rahmen von Wartungsarbeiten oder durch größere Überarbeitungen des gesamten Security-Frameworks.

Diese Zusammenhänge sind in Abbildung 6.19 mit Bezug auf die jeweiligen Lebenszyklusphasen dargestellt.

6.5.1.2. Schnittstellen zu ISO/IEC 27001 A.6: Organisation der Informationssicherheit

ISO/IEC 27001 fordert eine Reihe von Maßnahmen, um die verschiedenen Abläufe und Zuständigkeiten für alle Aspekte der Informationssicherheit zu organisieren. Dabei werden die folgenden Ziele verfolgt, die sich auch auf das Management von Security-Frameworks auswirken:

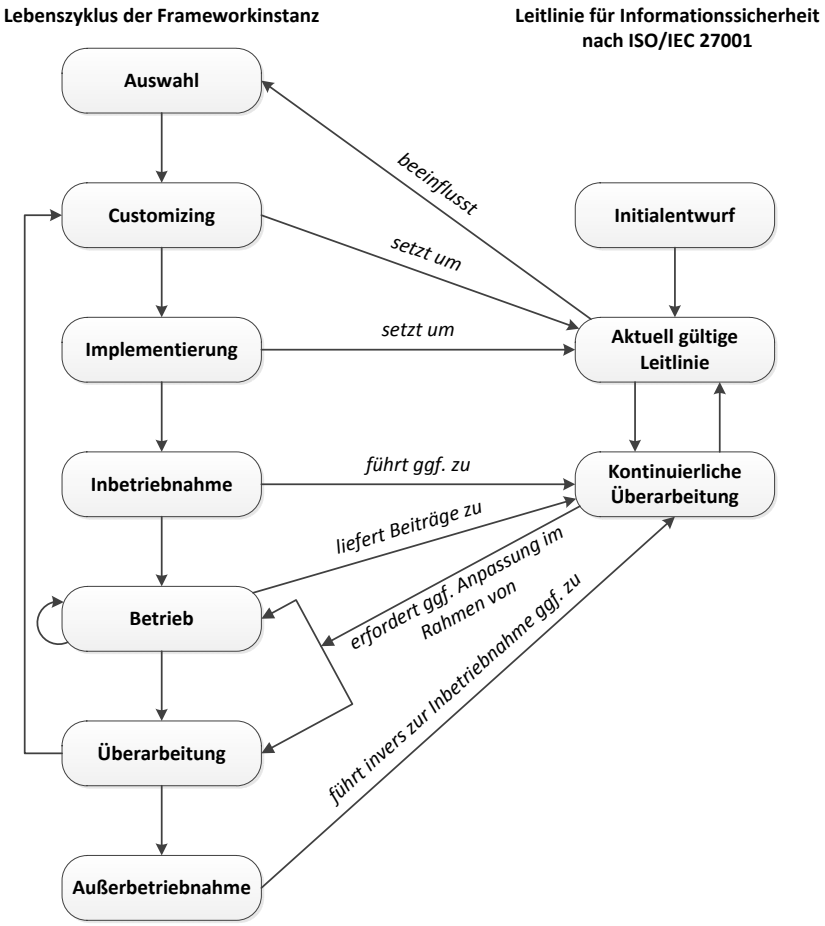


Abbildung 6.19.: Schnittstellen zwischen Security-Frameworks und der in ISO/IEC 27001 A.5 spezifizierten Informationssicherheitsleitlinie

- Das Engagement der Unternehmensleitung und der leitenden Angestellten für die Informationssicherheit soll sichergestellt und durch Sicherheitsprojekte und -initiativen ausgedrückt werden.
- Die Maßnahmen für die Informationssicherheit sollen u. a. dadurch koordiniert eingesetzt werden, dass ihr Ressourcenbedarf definiert und ihre Angemessenheit beurteilt werden.
- Die Zuständigkeiten und Verantwortlichkeiten für die verschiedenen Bereiche der Informationssicherheit müssen genau geregelt werden.
- Es muss ein Genehmigungsverfahren geben, um über den Einsatz informationsverarbeitender Infrastrukturkomponenten zu entscheiden.
- Der Kontakt zu aus Perspektive der Informationssicherheit relevanten Dritten soll gepflegt werden.
- Die Informationssicherheit der Organisation soll unabhängigen Überprüfungen unterzogen werden.

- Die Informationssicherheit muss auch im Rahmen der vertraglichen Vereinbarungen mit Dritten und Kunden berücksichtigt werden.

Diese organisatorischen Aspekte stehen mit dem Management von Security-Frameworks wie folgt in Wechselwirkung:

- Die mit Security-Frameworks erreichte konzertierte Einführung von Sicherheitsmaßnahmen entspricht den vom Standard geforderten Sicherheitsinitiativen. Komplementär dazu erfolgt die Umsetzung von Security-Frameworks im Rahmen der Organisations- und Projektstrukturen, die im Rahmen dieses Teilprozesses definiert wurden; dies trifft auch auf die Organisation z. B. von Schulungsmaßnahmen zu.
- Von Frameworkkonzepten und den Ergebnissen ihres Customizings werden wie von ISO/IEC 27001 gefordert die für die Verbesserung der Informationssicherheit benötigten Ressourcen vorgegeben.
- Analog dazu tragen die Security-Frameworks zur Vervollständigung des unternehmensweiten Rollen- und Berechtigungsmodells bei, an dem sie sich andererseits eng orientieren müssen. Zur Verwaltung kann beispielsweise auf eine entsprechende Access-Management-Anwendung in der in Abschnitt 6.4.4.3 skizzierten Managementplattform zurückgegriffen werden.
- Security-Frameworks dienen der Umsetzung der mit Kunden und Dritten vereinbarten Sicherheitsmaßnahmen. Auf Basis von Kennzahlen, KPIs und Berichten unterstützen sie den auch im Umgang mit Dritten geforderten Soll-/Ist-Abgleich und stellen Triggermechanismen bereit, um z. B. spezifizierte Eskalationsprozesse anzustoßen.
- Security-Frameworks müssen die durch diesen Teilprozess festgelegten Delegations- und Mandantenkonzepte umsetzen, die sich dabei wiederum an den Fähigkeiten der eingesetzten Schutzmechanismen orientieren müssen.
- Beim Customizing von Security-Frameworks sind sowohl die Beurteilungsmaßstäbe anzuwenden als auch die Genehmigungsverfahren zu durchlaufen, die von diesem Teilprozess vorgegeben werden.
- Security-Frameworks müssen die erforderlichen Messwerte liefern und aggregieren bzw. korrelieren können, die z. B. für den organisationsübergreifenden Informationsaustausch festgelegt wurden. Hierzu gehören auch die Inhalte und Formate entsprechender Berichte.
- Im Rahmen der unabhängigen Bewertungen werden auch die Security-Frameworks überprüft bzw. tragen Werkzeuge zur Durchführung entsprechender Audits bei.
- Die in Kapitel 5 für viele Lebenszyklusphasen empfohlenen Rückmeldungen an die Autoren von Security-Frameworks ist im Rahmen des Kontakts zu relevanten Externen zu berücksichtigen.

Analog zu den Schnittstellen, die im Rahmen der Pflege der Sicherheitsleitlinie erforderlich sind, ergeben sich auch hier Schnittstellen zu allen Phasen des Lebenszyklus von Security-Frameworks:

- Die Auswahl, Anpassung und Implementierung des Security-Frameworks folgen den organisationsweit festgelegten Anforderungen und Abläufen.

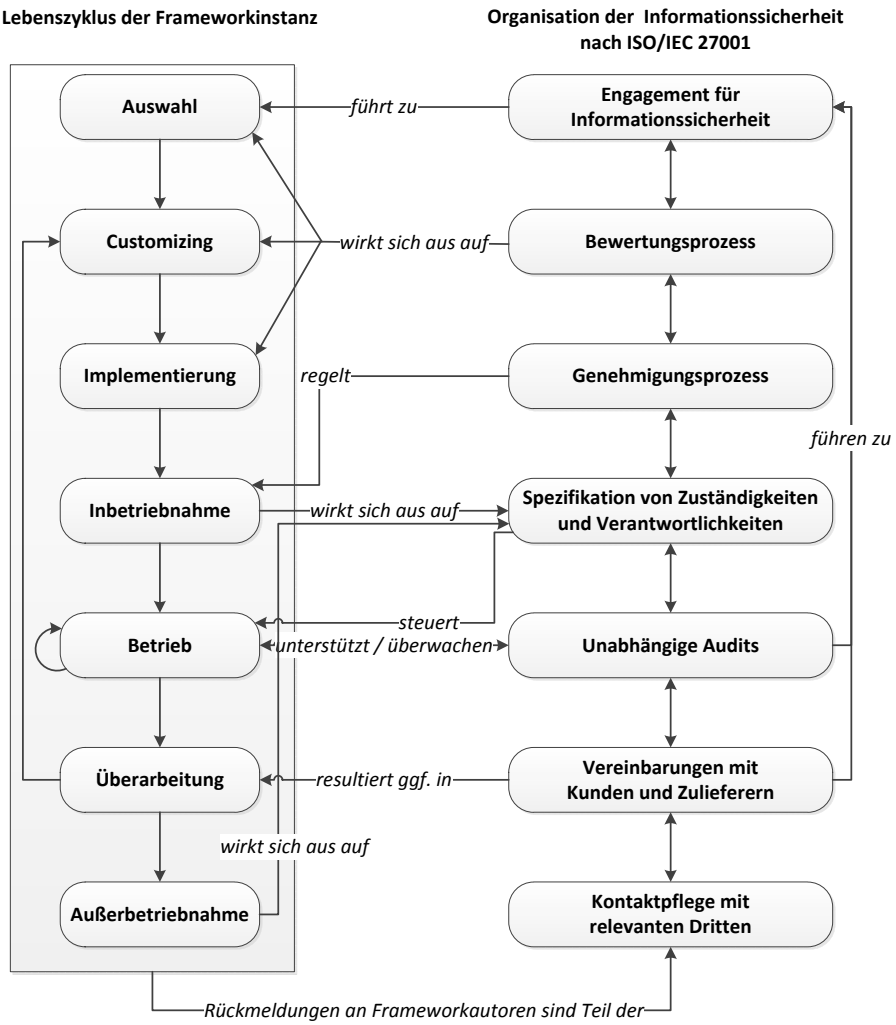


Abbildung 6.20.: Schnittstellen zwischen Security-Frameworks und der in ISO/IEC 27001 A.6 spezifizierten Organisation der Informationssicherheit

- Die Vorbereitung der Inbetriebnahme umfasst eine Abnahme gemäß dem definierten Genehmigungsprozess. Mit der In- und Außerbetriebnahme von Security-Frameworks können sich entsprechende Änderungen beispielsweise an den Zuständigkeiten, Rollenmodellen, Eskalationswegen und benötigten Ressourcen ergeben.
- Im laufenden Betrieb werden die für diesen Teilprozess erforderlichen Messwerte und Kennzahlen geliefert und in Abhängigkeit der definierten Schwellenwerte die definierten Eskalationsprozesse angestoßen.
- Änderungen der organisatorischen Regelungen müssen auch im Betrieb des Security-Frameworks umgesetzt werden; dabei handelt es sich im Regelfall um kleinere bzw. vorhersehbare Anpassungen, die sich z. B. aus Kunden- oder Zuliefererfluktuationen und somit SLA- bzw. Vertragsänderungen ergeben.

Eine Zusammenfassung dieser Schnittstellen ist in Abbildung 6.20 dargestellt.

6.5.1.3. Schnittstellen zu ISO/IEC 27001 A.7: Management von organisationseigenen Werten

Das in ISO/IEC 27001 aus Sicherheitsperspektive erläuterte Management der organisationseigenen Werte (Assets) ist eng mit dem *Service Asset and Configuration Management* nach ITIL verwandt (vgl. Abschnitt 6.5.2.3). Es verfolgt die folgenden vier im Zusammenspiel mit Security-Frameworks relevanten Ziele:

- Die Assets müssen inventarisiert werden; hierzu werden sie beispielsweise in einer CMDB oder Managementplattform erfasst, so dass andere Prozesse wie das Risikomanagement auf die jeweils relevanten Informationen zurückgreifen können.
- Als Konkretisierung der oben beschriebenen Organisation der Informationssicherheit müssen für jedes Asset die Zuständigkeiten und Verantwortlichkeiten festgehalten werden.
- Es müssen Richtlinien erstellt werden, die den zulässigen Gebrauch von Assets regeln.
- Die zu verarbeitenden Informationen müssen klassifiziert und entsprechend gekennzeichnet werden.

Diese Aktivitäten haben die folgenden unmittelbaren Auswirkungen auf das Management von Security-Frameworks:

- Die technischen Komponenten von Security-Frameworks sind wie in Abschnitt 6.4.3 dargestellt selbst Assets, die im Rahmen dieses Prozesses verwaltet werden müssen; dabei sind Gruppierungskriterien und Verknüpfungen, z. B. mit den vom Security-Framework geschützten Assets, zu berücksichtigen. Informationen über für das Sicherheitsmanagement relevante Assets müssen der entsprechenden Managementplattform verfügbar gemacht werden.
- Die Regelungen des zulässigen Gebrauchs von Assets führen zu Policies, deren Umsetzung auch von den Security-Frameworks erzwungen werden muss. Im Umkehrschluss bleiben Regelungen, deren Einhaltung nicht technisch kontrolliert oder erzwungen werden kann, potentiell wirkungslos.
- Die Klassifizierung von Informationen ist am jeweiligen Schutzbedarf auszurichten und auch von den Security-Frameworks zu berücksichtigen; insbesondere müssen Daten, die von Security-Frameworks erzeugt werden, ebenfalls entsprechend eingeordnet und gekennzeichnet werden.
- Die Zuständigkeiten und Verantwortlichkeiten müssen wie in Abschnitt 6.5.1.2 beschrieben beispielsweise über die Managementplattform zugewiesen und verwaltet werden.

Mit Bezug auf den Lebenszyklus von Frameworkinstanzen ergeben sich die folgenden Schnittstellen:

- Beim Customizing des Security-Frameworks muss auf die vorhandenen Klassifikations- und Gebrauchsregelungen Rücksicht genommen werden, beispielsweise indem frameworkspezifische und szenarienweite Rollenmodelle in Einklang gebracht werden.
- Mit der Inbetriebnahme eines Security-Frameworks können sich neue technische Möglichkeiten ergeben, die zu Veränderungen an den Gebrauchsregelungen führen. Die Außerbetriebnahme verhält sich dazu invers.

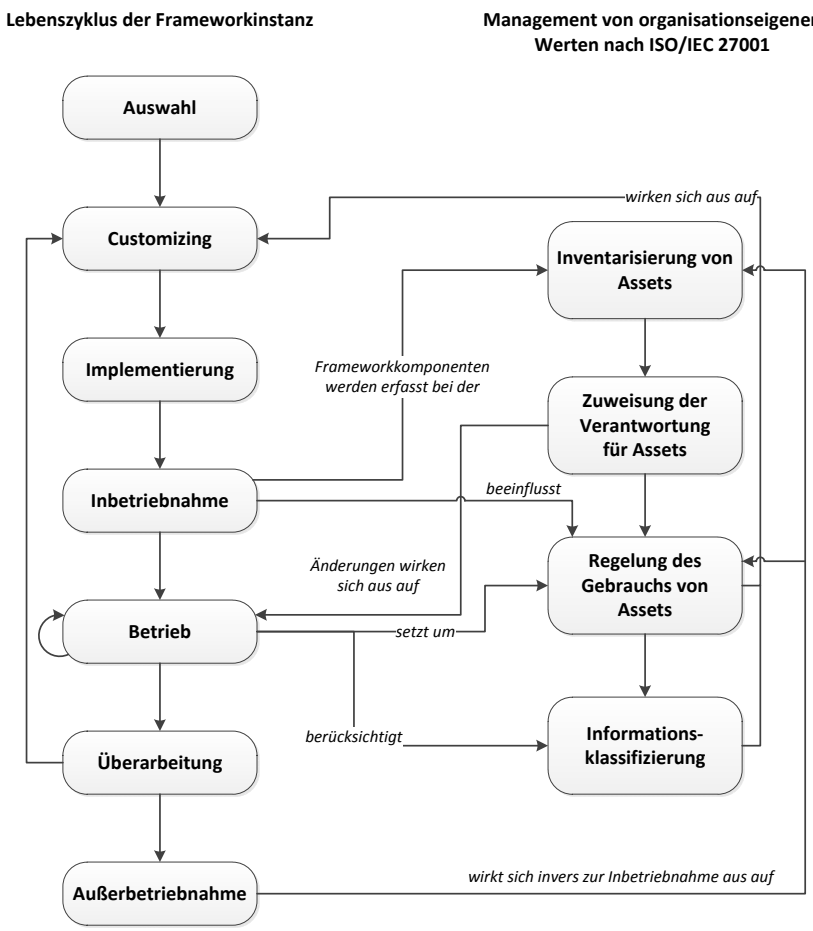


Abbildung 6.21.: Schnittstellen zwischen Security-Frameworks und dem in ISO/IEC 27001 A.7 spezifizierten Management organisationseigener Werte

- Im laufenden Betrieb trägt das Security-Framework zur Einhaltung der Zuständigkeiten und Regelungen bei.
- Änderungen an Zuständigkeiten, Verantwortlichkeiten, Klassifikations- und Gebrauchsregelungen müssen für die davon betroffenen Frameworkkomponenten umgesetzt werden. Im Allgemeinen handelt es sich dabei um Wartungstätigkeiten, die keine grundlegende Überarbeitung der Frameworkarchitektur erforderlich machen; komplexe Änderungen z. B. an Rollenmodellen können jedoch auch zur Notwendigkeit größerer Anpassungen führen.

Abbildung 6.21 fasst diese Interaktionen zusammen.

6.5.1.4. Schnittstellen zu ISO/IEC 27001 A.8: Personelle Sicherheit

Der Bereich der personellen Sicherheit regelt in ISO/IEC 27001 die sicherheitsrelevanten Aspekte *vor*, *während* und *zum Ende* der Beschäftigung von eigenen und externen Mitar-

beitern in einer Organisation. Im Zusammenspiel mit Security-Frameworks ist dabei primär der Zeitraum, in dem ein Mitarbeiter legitim mit Frameworkkomponenten arbeitet, relevant; hierbei verfolgt dieser Prozess die folgenden Ziele:

- Angestellte müssen im Bezug auf die Informationssicherheit sensibilisiert, ausgebildet und geschult werden. Diese Maßnahmen sollen nicht nur zum routinierten Umgang mit technischen Sicherheitsmechanismen beitragen, sondern z. B. auch eine Festigung gegenüber Social-Engineering-Angriffen bewirken.
- Bei Verstößen gegen Sicherheitsregelungen sind geeignete disziplinarische Maßnahmen zu ergreifen.
- Nicht mehr benötigte Berechtigungen müssen zeitnah entzogen werden.

Security-Frameworks leisten dabei die folgenden Beiträge zur Umsetzung:

- In den Frameworkkonzepten werden Anforderungen an und Inhalte von Schulungen genannt.
- Die Schutzkomponenten von Security-Frameworks tragen zur Erkennung von Verstößen gegen Policies bei und unterstützen die Beurteilung der jeweiligen Schwere des Vergehens.
- Security-Frameworks ermöglichen eine dynamische Berechtigungsverwaltung, die konsistent über alle Frameworkkomponenten und die geschützten Assets umgesetzt wird, so dass beispielsweise auf Verstöße oder die Beendigung von Anstellungsverhältnissen rasch mit dem (ggf. temporären) Entzug von Berechtigungen reagiert werden kann.

Im Lebenszyklus der Frameworkinstanzen sind somit folgende Schnittstellen zu berücksichtigen:

- Die Inbetriebnahme von Security-Frameworks kann sowohl initial als auch nach größeren Überarbeitungen die Durchführung entsprechender Schulungen erforderlich machen.
- Im laufenden Betrieb trägt das Security-Framework zur Überwachung der Nutzungsaktivitäten auf Verstöße bei und wirkt an der dynamischen Umsetzung resultierender Berechtigungsänderungen mit.

Diese sind zusammenfassend in Abbildung 6.22 darstellt.

6.5.1.5. Schnittstellen zu ISO/IEC 27001 A.9: Physische und umgebungsbezogene Sicherheit

ISO/IEC 27001 regelt auch die im Bereich der physischen Sicherheit zu ergreifenden Maßnahmen, beispielsweise indem sie fordert, dass Anlieferzonen und der Zutritt zu Serverräumen kontrolliert werden. Im Zusammenhang mit dem Einsatz von Security-Frameworks sind zwei Teilziele hervorzuheben:

- Es müssen Sicherheitsbereiche bzw. Sicherheitszonen definiert werden.
- Die physische Sicherheit der Betriebsmittel muss sichergestellt werden; unter dem Aspekt der Verfügbarkeit von informationsverarbeitenden Anlagen gehören hierzu beispielsweise auch unterbrechungsfreie Stromversorgungen.

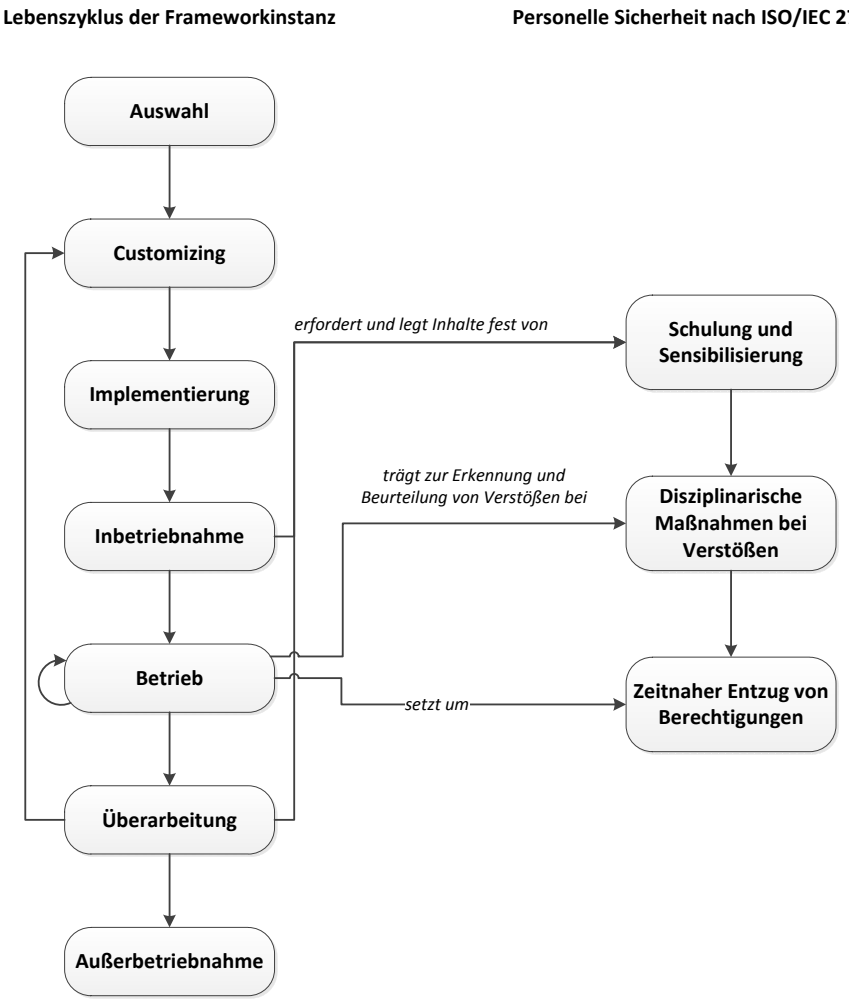


Abbildung 6.22.: Schnittstellen zwischen Security-Frameworks und der in ISO/IEC 27001 A.8 spezifizierten personellen Sicherheit

Daraus ergeben sich die folgenden Auswirkungen auf den Einsatz von Security-Frameworks:

- Die Anforderungen an die Aufstellungsorte von Frameworkkomponenten müssen spezifiziert werden; entsprechende Zonen mit entsprechenden Versorgungseinrichtungen müssen verfügbar sein.
- Die physische Sicherheit von dezentral betriebenen Frameworkkomponenten, beispielsweise mobilen Sensoren, muss auf Basis der szenarienspezifischen Gegebenheiten geregelt werden.

Die Komponenten von Security-Frameworks verhalten sich diesbezüglich somit vergleichbar zu anderen Assets, die beim Sicherheitsmanagement betrachtet werden. Als Schnittstelle zum Lebenszyklus von Frameworkinstanzen ist folglich wie in Abbildung 6.23 dargestellt bereits beim Customizing zu berücksichtigen und bei der Inbetriebnahme bzw. bei einer eventuellen Relokalisierung von Frameworkkomponenten umzusetzen, dass eine Zuordnung zu Sicherheits-

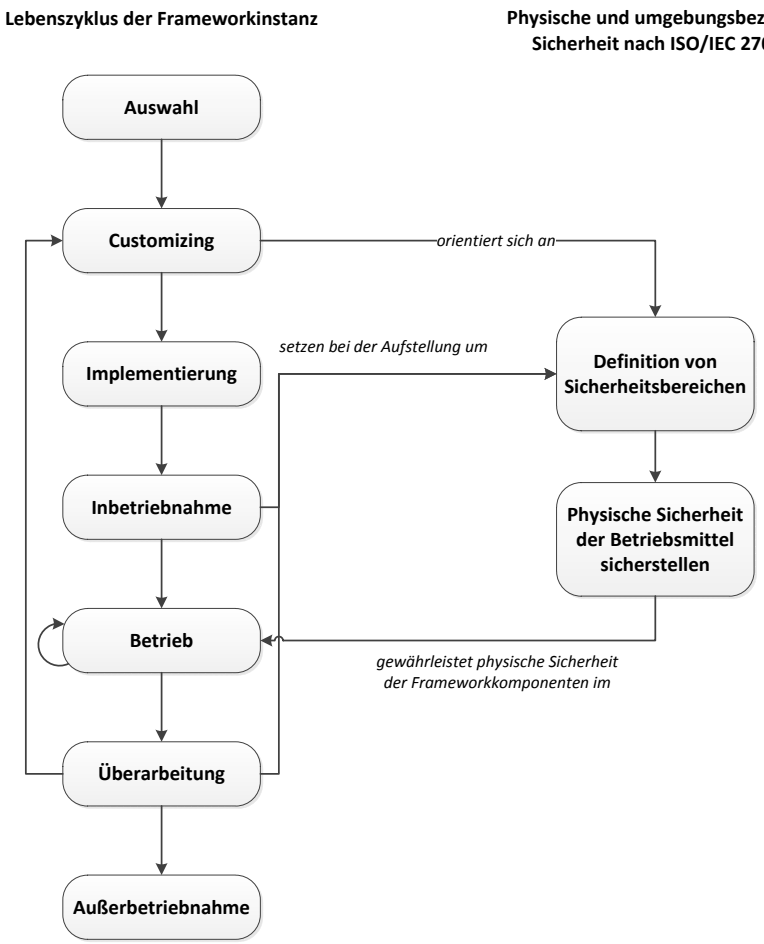


Abbildung 6.23.: Schnittstellen zwischen Security-Frameworks und der in ISO/IEC 27001 A.9 spezifizierten physischen und umgebungsbezogenen Sicherheit

zonen erfolgt. Im laufenden Betrieb wird die physische Sicherheit der Frameworkkomponenten gewährleistet.

6.5.1.6. Schnittstellen zu ISO/IEC 27001 A.10: Betriebs- und Kommunikationssicherheit

Der normative Anhang A.10 von ISO/IEC 27001 schlägt die Brücke zum operativen Sicherheitsmanagement und hierbei insbesondere zu den Bereichen *Systemsicherheit*, *Netzsicherheit*, *kryptographische Mechanismen* und *SIEM*. Er enthält eine Vielzahl von Zielen und Maßnahmen, von denen insbesondere die folgenden auch für das Management von Security-Frameworks unmittelbar relevant sind:

- Die Betriebsprozesse (aller Assets und Schutzmechanismen) sind zu dokumentieren.
- Alle Modifikationen am Aufbau der Infrastruktur und der Konfiguration ihrer Bestandteile sind einer Änderungsverwaltung zu unterziehen.

- Verantwortlichkeiten müssen geeignet aufgeteilt werden, z. B. durch die Umsetzung des Vier-Augen-Prinzips für besonders kritische Systeme.
- Entwicklungs-, Test- und Produktivumgebungen sind strikt voneinander zu trennen.
- Von Dritten erbrachte Sicherheitsdienstleistungen sind zu regeln und zu kontrollieren.
- Neu anzuschaffende Systeme sind zu planen und anhand spezifizierter Kriterien abzunehmen.
- Es müssen Maßnahmen zum Schutz vor Schadsoftware und Datenverlust ergriffen werden.
- Es muss ein Management für die Netzsicherheit geben.
- Der Umgang mit Speichermedien und der Austausch von Informationen mit Externen müssen geregelt werden.
- Maßnahmen zur Überwachung der Sicherheit der Infrastrukturkomponenten und Dienste müssen umgesetzt werden.

Diese Zielsetzungen decken sich zu einem großen Teil mit den funktionalen Schwerpunkten von Security-Frameworks und beeinflussen die Umsetzung wie folgt:

- Security-Frameworks enthalten wie in Kapitel 4 dargestellt sehr häufig eigene Komponenten zur Verbesserung der Netzsicherheit und untermauern somit die geforderten Maßnahmen durch technische Sicherheitsmechanismen.
- Die Frameworkkonzepte dienen als Ausgangsbasis für die Erstellung szenarienspezifischer Dokumentationen der Betriebsabläufe, die ihrerseits beispielsweise wiederum über eine Managementplattform einfach zugänglich gemacht werden; dabei müssen administrative Konzepte wie das Vier-Augen-Prinzip umgesetzt werden.
- Die von Security-Frameworks vorgesehenen Monitoring- und Überwachungsmöglichkeiten müssen sich in szenarienweite Konzepte integrieren.
- Protokolle über Änderungen, Tests, Genehmigungen, Wartungen, Überarbeitungen etc. müssen erstellt und z. B. in einer Managementplattform hinterlegt werden.
- Entwicklungs- und Testumgebungen müssen vorgesehen und dabei möglichst eng an der Produktivumgebung ausgerichtet werden, ohne deren sensible Daten zu verwenden.
- Für den Fall, dass einzelne Frameworkkomponenten von Dritten betrieben werden, sind entsprechende vertragliche Regelungen vorzusehen, deren Einhaltung technisch überwacht wird.
- Auch Frameworkkomponenten, die selbst eine Schutzwirkung entfalten, sind beispielsweise durch den Einsatz von Antiviren- und Backupsoftware gegen Schadsoftware bzw. Ausfälle zu schützen.
- Bei der Außerbetriebnahme von Frameworkkomponenten muss auf die sichere Entsorgung der entsprechenden Datenträger und Speichermedien geachtet werden.
- Beim Austausch der von Security-Frameworks generierten Daten mit Dritten ist beispielsweise durch die Anwendung adäquater kryptographischer Methoden auf entsprechende Sicherheitsregelungen Rücksicht zu nehmen.

- Die Überwachung, das Monitoring und die Durchführung von Sicherheitsaudit wird unter Berücksichtigung der datenschutzrelevanten Aspekte von Security-Frameworks unterstützt, indem sie Auditprotokolle über Benutzer- und Administratortätigkeiten generieren, geeigneten Korrelationsmechanismen zuführen und die Integrität dieser Protokollinformationen z. B. mit kryptographischen Hilfsmitteln schützen.

Als Schnittstellen zwischen dem Prozess zum Management der Betriebs- und Kommunikationssicherheit und dem Lebenszyklus von Security-Frameworks sind folglich zu betrachten:

- Bereits bei der Auswahl und beim Customizing von Security-Frameworks muss die Integration in die vorhandenen Betriebskonzepte und die dazu bereits eingesetzte Infrastruktur berücksichtigt werden. Sie unterliegen zudem dem Prozess zur Planung von Systemen.
- Die Inbetriebnahme kann nur erfolgen, wenn die erforderliche Dokumentation der Betriebsprozesse vorliegt und eine entsprechende Abnahme durchgeführt wurde.
- Änderungen an diesen Konzepten und frameworkexternen Komponenten können auch umfassendere Überarbeitungen der Frameworkinstanzen erforderlich machen und unterliegen den entsprechenden Verwaltungs- und Genehmigungsprozessen.
- Im laufenden Betrieb, der ebenfalls den definierten Regelungen unterliegt, tragen die Security-Frameworks maßgeblich zur Umsetzung der Sicherheitsmechanismen bei und liefern entsprechende Überwachungsinformationen.

Abbildung 6.24 stellt diese Wechselwirkungen graphisch dar.

6.5.1.7. Schnittstellen zu ISO/IEC 27001 A.11: Zugangskontrolle

Die in der Norm geforderte Regelung der Zugangskontrolle stellt die Schnittstelle zum entsprechenden Funktionsbereich des operativen Sicherheitsmanagements dar und umfasst die folgenden auch für das Management von Security-Frameworks relevanten Ziele:

- Die Ziele und Maßnahmen der Zugangskontrolle müssen in einer Leitlinie beschrieben werden.
- Die Benutzer und ihre Berechtigungen müssen auf Basis eines dokumentierten Prozesses verwaltet werden; dieser muss auch die Verwaltung von Sonderrechten, z. B. für Administratoren, und die regelmäßige Überprüfung der vergebenen Berechtigungen umfassen.
- Für den Anschluss von Systemen an Netze soll eine auf Geräteidentifikation basierte Zugangskontrolle umgesetzt werden.
- Verbindungen zu Systemen sollen nicht dauerhaft aufrecht erhalten werden können; vielmehr sollen Session-Timeouts zum Einsatz kommen, so dass längere Zeit nicht aktiv genutzte Verbindungen automatisiert wieder abgebaut werden.

Dadurch, dass viele Security-Frameworks eigene Authentifizierungs- und Autorisierungskomponenten vorsehen, ergeben sich folgende Einflüsse dieses Prozesses von und auf Frameworkinstanzen:

- Die Security-Frameworks setzen die szenarienweit festgelegten Berechtigungskonzepte für ihre eigenen Komponenten sowie die geschützten Dienste und Assets gebündelt um;

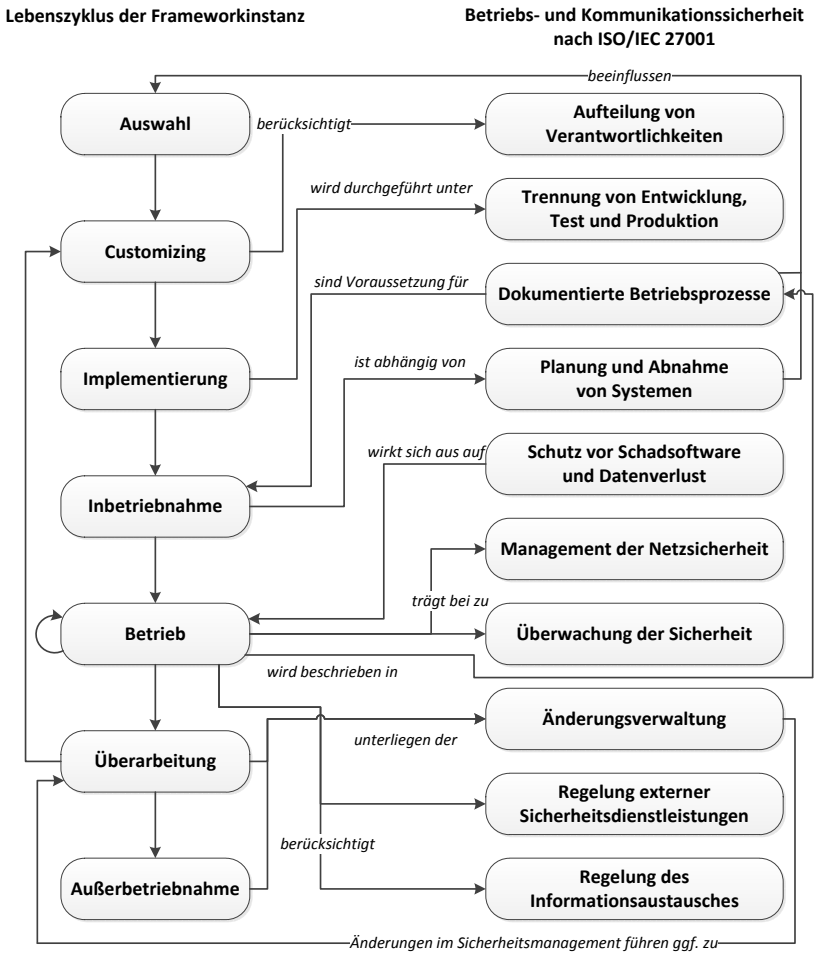


Abbildung 6.24.: Schnittstellen zwischen Security-Frameworks und der in ISO/IEC 27001 A.10 spezifizierten Betriebs- und Kommunikationssicherheit

sie nehmen dabei z. B. die Rolle von Gateways ein und schotten die geschützten Assets von direkten Zugriffen ab.

- Die regelmäßige Überprüfung der Zugangsberechtigungen wird über entsprechende Berichte gezielt unterstützt (vgl. Abschnitt 6.6).
- Die Integration in szenarienweite Netzzugangskonzepte kann beispielsweise über den Einsatz von Server- bzw. Komponentenzertifikaten erreicht werden.
- Die Komponenten des Security-Frameworks müssen mit Angaben beispielsweise zu Session-Timeouts parametrisiert werden können und diese im Anschluss umsetzen.

Hieraus ergeben sich die folgenden Schnittstellen zum Lebenszyklus von Frameworkinstanzen:

- Die Anforderungen an die Integration der Frameworkkomponenten in die szenarienweiten Zugangskontrollkonzepte müssen bereits beim Customizing berücksichtigt werden; hierzu gehört beispielsweise die Anbindung an eine zentrale Benutzer- und Berechtigungsverwaltung, die implementiert werden muss.

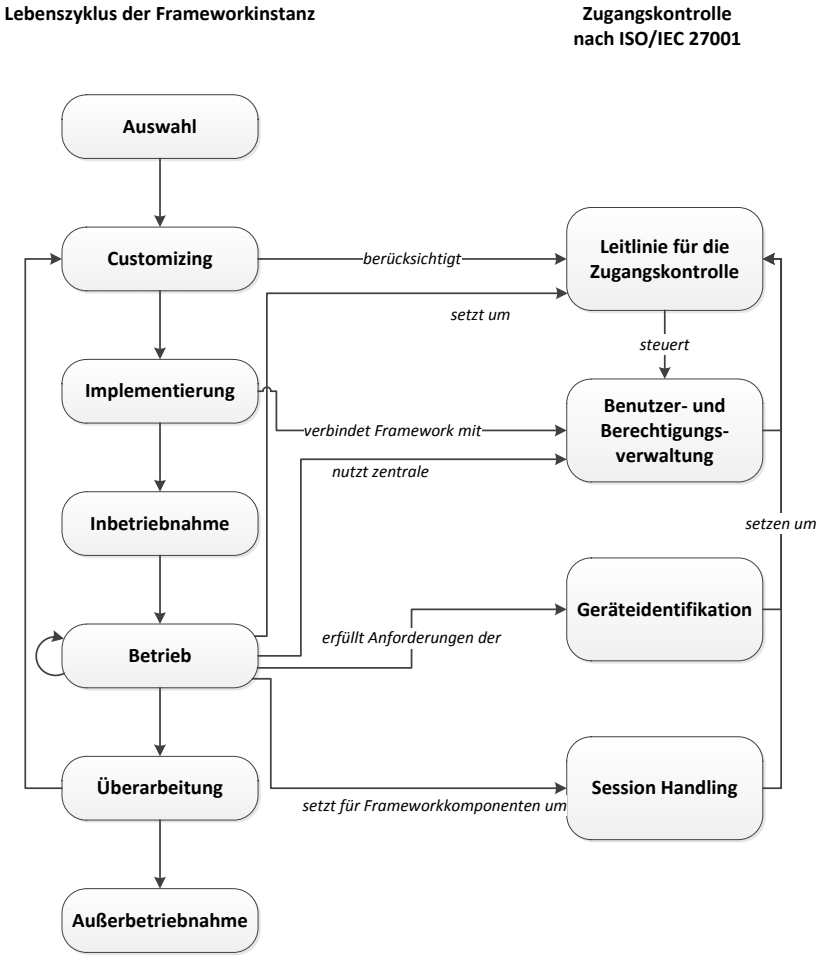


Abbildung 6.25.: Schnittstellen zwischen Security-Frameworks und der in ISO/IEC 27001 A.11 spezifizierten Zugangskontrolle

- Im laufenden Betrieb unterstützen die Security-Frameworks die Zugangsverwaltung durch die Umsetzung der entsprechenden Policies für die geschützten Assets und die Übermittlung entsprechender Monitoring- und Auditinformationen an die Überwachungs- und Kontrollwerkzeuge.

Abbildung 6.25 fasst dies zusammen.

6.5.1.8. Schnittstellen zu ISO/IEC 27001 A.12: Beschaffung, Entwicklung und Wartung von Informationssystemen

Die Zielsetzung, den Themenkomplex Informationssicherheit nicht nur punktuell, sondern über den ganzen Lebenszyklus der Assets hinweg zu betrachten, erfüllt ISO/IEC 27001 durch eine Reihe von Maßnahmen, die sich mit der Beschaffung, Entwicklung und Wartung von Informationssystemen befassen. Im Kontext von Security-Frameworks sind dabei die folgenden Teilziele wichtig:

- Sicherheitsanforderungen müssen bereits vor der Entwicklung und Implementierung von Informationssystemen identifiziert und anschließend dabei berücksichtigt werden.
- Entwickelte Anwendungen müssen die korrekte Verarbeitung der Daten sicherstellen, beispielsweise indem Eingabedaten auf Plausibilität überprüft werden.
- Es muss eine verbindliche Leitlinie geben, die regelt, welche kryptographischen Maßnahmen einzusetzen sind.
- Die Sicherheit von Systemdateien muss gewährleistet werden.
- Die Informationssicherheit muss bei Entwicklungs- und Wartungsprozessen berücksichtigt werden.
- Der Umgang mit Schwachstellen muss geregelt werden; insbesondere sind Fristen für die Reaktion auf bzw. die Behandlung von neu bekannt werdenden Schwachstellen zu setzen und ggf. Notfallmaßnahmen vorzusehen.

In den Teilbereich *Wartung von Informationssystemen* ist somit der Prozess *Vulnerability Management* integriert, der häufig eng mit dem Einspielen von Softwareaktualisierungen zusammenhängt. Insgesamt ergeben sich aus diesem Teil von ISO/IEC 27001 die folgenden Zusammenhänge mit dem Management von Security-Frameworks:

- Security-Frameworks stellen zu beschaffende und ggf. durch eigene Entwicklungen zu ergänzende Systeme dar, deren Konzepte im Rahmen der Anforderungsermittlung herangezogen werden können und auch Aufschluss über bei der Frameworkkonzeption berücksichtigte Schwachstellen geben.
- Die in Security-Frameworks eingesetzten Schutzkomponenten, die beispielsweise die von den geschützten Assets verarbeiteten Nutzdaten kontrollieren, müssen selbst gegen Angriffe, die wie beispielsweise Buffer-Overflows manipulierte Nutzdaten als Trägermedium verwenden, abgesichert werden.
- Security-Frameworks tragen dazu bei, die Leitlinie für den Einsatz kryptographischer Maßnahmen komponentenübergreifend in ihrem Einflussgebiet umzusetzen.
- Die Maschinen, auf denen Komponenten von Security-Frameworks betrieben werden, müssen analog zu anderen Assets z. B. auf Betriebssystemebene einem geeigneten Aktualisierungsprozess unterzogen werden.
- Security-Frameworks müssen mit definierten Notfallprozessen zusammenspielen; beispielsweise ist der Umgang mit neu bekannt werdenden Schwachstellen, die vom Security-Framework aktuell noch nicht berücksichtigt werden, festzulegen.

Entsprechend sind die folgenden Schnittstellen zum Lebenszyklus von Frameworkinstanzen vorzusehen:

- Im laufenden Betrieb und bei Überarbeitungen sind die aktuell bekannten Schwachstellen und Änderungen daran zu berücksichtigen; diese können beispielsweise über eine Vulnerability-Management-Anwendung in der oben diskutierten Managementplattform verwaltet werden und sich externe Informationsquellen zunutze machen.
- Beim Customizing und bei der Implementierung eigener Komponenten im Rahmen der Frameworkinstanziierung sind die Vorgaben an die sichere Softwareentwicklung und aus der Kryptographierichtlinie zu berücksichtigen.

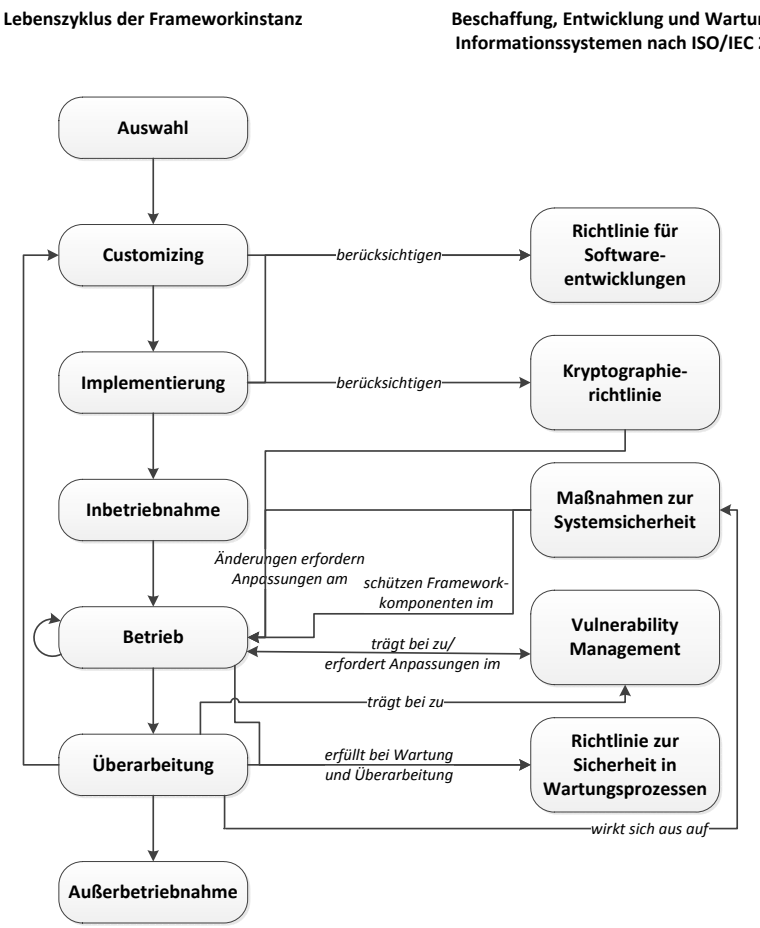


Abbildung 6.26.: Schnittstellen zwischen Security-Frameworks und der in ISO/IEC 27001 A.12 spezifizierten Beschaffung, Entwicklung und Wartung von Informationssystemen

- Im Betrieb müssen Änderungen, die sich z. B. an den Kryptographie- und Systemsicherheitsrichtlinien ergeben, berücksichtigt werden.

- Mit neuen Frameworkgenerationen oder Weiterentwicklungen der Kryptographierichtlinie müssen die szenarienweiten Konzepte fortgeschrieben bzw. entsprechende Umkonfigurationen der Schutzmaßnahmen vorgenommen werden.

Der hier betrachtete Prozess nach ISO/IEC 27001 stellt folglich eine Schnittstelle zu den Funktionsbereichen *Systemsicherheit* und *kryptographische Maßnahmen* dar. Die in der jeweiligen Lebenszyklusphase der Frameworkinstanz zu betrachtenden Schnittstellen sind in Abbildung 6.26 veranschaulicht.

6.5.1.9. Schnittstellen zu ISO/IEC 27001 A.13: Umgang mit Informationssicherheitsvorfällen

ISO/IEC 27001 fordert einen dokumentierten Prozess zum Umgang mit Informationssicherheitsvorfällen; dieser muss sich im Allgemeinen eng am im Rahmen von ITSM vorgesehenen Incident-Management-Prozess orientieren oder in diesen integriert werden (siehe dazu Abschnitt 6.5.2.4). Mit direktem Bezug auf das Management von Security-Frameworks liegen die folgenden Zielvorgaben vor:

- Sicherheitsvorfälle müssen geordnet gemeldet, bearbeitet und ggf. eskaliert werden; der Bearbeitungsverlauf ist im Berichtswesen zu berücksichtigen.
- Im Rahmen der Bearbeitung von Sicherheitsvorfällen sind Beweise geeignet zu sammeln und zu sichern.
- Aus Sicherheitsvorfällen muss gelernt werden, d. h. es sollen sowohl technische als auch organisatorische Verbesserungsmaßnahmen abgeleitet werden.

Der Einsatz von Security-Frameworks und die Instanziierung dieses Security-Incident-Response-Prozesses wirken sich wie folgt aufeinander aus:

- Die von Security-Frameworks vorgesehenen detektierenden Sicherheitsmechanismen tragen maßgeblich zur Erkennung und Erstanalyse von Sicherheitsvorfällen bei.
- Security-Frameworks müssen entsprechende Triggermechanismen vorsehen und Schnittstellen zur automatisierten Weitergabe der entsprechenden Daten haben; diese können beispielsweise auf dem in Abschnitt 6.4.3 vorgestellten Informationsmodell für Sicherheitsereignisse beruhen und müssen z. B. durch den Einsatz kryptographischer Maßnahmen gegen Manipulation geschützt werden.
- Über den kontinuierlichen Verbesserungsprozess werden Änderungen am Security-Incident-Response-Prozess durchgeführt, die z. B. zu einer Umkonfiguration der Security-Frameworks führen können.

Die Analyse von Sicherheitsvorfällen zur Prozessverbesserung impliziert auch eine Schnittstelle zum Risikomanagement, über die beispielsweise Abweichungen von der geschätzten Eintrittswahrscheinlichkeit bzw. den prognostizierten Auswirkungen tatsächlich eingetretener Schadereignisse korrigiert werden können. Insgesamt sind somit die folgenden Schnittstellen im Lebenszyklus von Frameworkinstanzen zu berücksichtigen:

- Bereits beim Customizing sind die vorhandenen Meldewege und -schnittstellen umzusetzen.
- Im laufenden Betrieb instanziieren Security-Frameworks den Security-Incident-Response-Prozess oder tragen Informationen zu anderweitig erkannten Sicherheitsvorfällen bei. Sie liefern Informationen für das Berichtswesen und stellen ggf. Analyse- und Forensikwerkzeuge bereit.
- Nach dem Abschluss der Bearbeitung eines Sicherheitsvorfalls kann es zu Änderungen an der Spezifikation des Prozesses oder einer veränderten Beurteilung der vorhandenen und noch benötigten Sicherheitsmaßnahmen durch das Risikomanagement kommen, so dass u. U. größere Änderungen am Security-Framework erforderlich werden.

Diese Zusammenhänge sind in Abbildung 6.27 zusammengestellt.

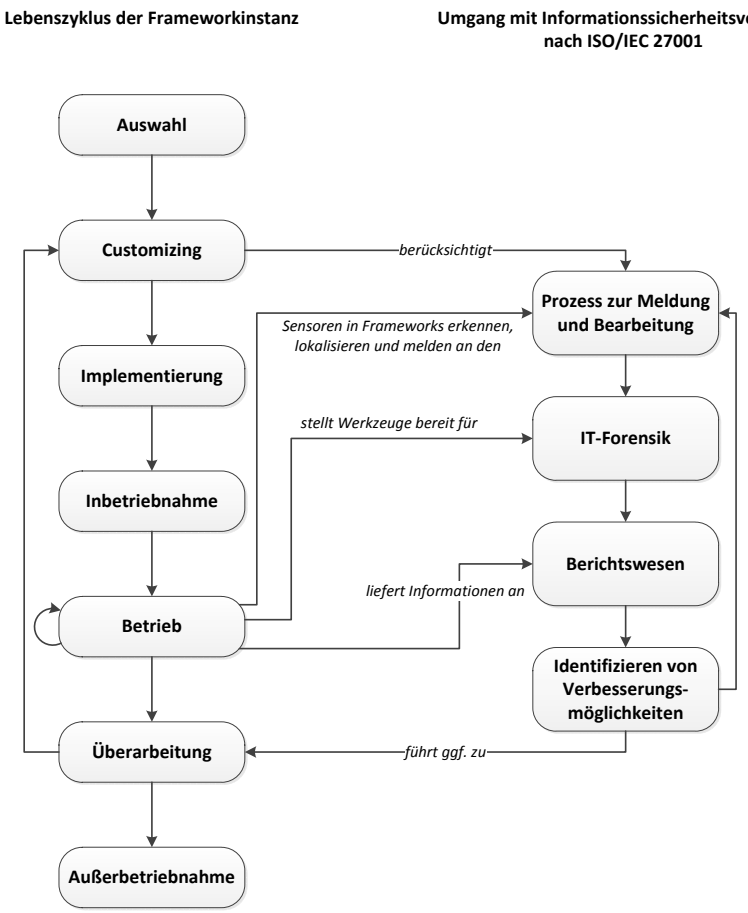


Abbildung 6.27.: Schnittstellen zwischen Security-Frameworks und dem in ISO/IEC 27001 A.13 spezifizierten Umgang mit Informationssicherheitsvorfällen

6.5.1.10. Schnittstellen zu ISO/IEC 27001 A.14: Sicherstellen des Geschäftsbetriebs

Ähnlich zur Überlappung von ITSM Incident Management und dem Security Incident Response Prozess stellt der Bereich *Sicherstellen des Geschäftsbetrieb* von ISO/IEC 27001 die Schnittstelle zum ITSM-Prozess *IT Service Continuity Management* dar und befasst sich mit der Reaktion auf äußerst unwahrscheinliche, aber existenzbedrohende Schadereignisse wie z. B. die Zerstörung eines Standorts durch eine Naturkatastrophe. Er hängt somit eng mit dem Risikomanagement zusammen und verfolgt u. a. die folgenden beiden auch für den Einsatz von Security-Frameworks relevanten Ziele:

- Die Kernfragen der Informationssicherheit müssen bei der Planung der Sicherstellung des Geschäftsbetriebs berücksichtigt werden.
- Notfallpläne und -maßnahmen müssen regelmäßig getestet und kontinuierlich verbessert werden.

In diesem Kontext ergibt sich die folgende Wechselwirkung mit Security-Frameworks:

- Für den Einsatz von Security-Frameworks werden Prioritäten vorgegeben, beispielsweise welche Schutzmaßnahmen auch im Rahmen eines Notfallbetriebs aufrecht erhalten werden müssen.
- Security-Frameworks müssen somit einerseits mit einem Wegbruch von Teilen der Infrastruktur umgehen können, worauf sich der im Allgemeinen modulare Aufbau positiv auswirkt. Andererseits müssen Security-Frameworks die zu ihrem Minimalbetrieb erforderlichen Komponenten vorgeben, um den Betrieb bzw. die Wiederherstellung der entsprechenden Ressourcen im Katastrophenfall planen zu können.

Im Lebenszyklus von Frameworkinstanzen sind somit die folgenden Schnittstellen zu berücksichtigen:

- Bereits beim Customizing müssen Vorkehrungen getroffen werden, damit – falls dies für erforderlich gehalten wird – ein Minimal- bzw. Notfallbetrieb der Frameworkinstanz im erforderlichen Umfang möglich ist, bei der beispielsweise auf einen Teil der Schutzfunktionalität und Redundanzeigenschaften verzichtet wird.
- Die In- und Außerbetriebnahme von Security-Frameworks macht u. U. eine Anpassung der Notfallpläne erforderlich.
- Im laufenden Betrieb müssen regelmäßige Tests der Notfallfunktionalität durchgeführt und dabei erkannte Defizite ausgemerzt werden.

Abbildung 6.28 fasst die Einbettung von Security-Frameworks in die Sicherstellung des Geschäftsbetriebs zusammen.

6.5.1.11. Schnittstellen zu ISO/IEC 27001 A.15: Einhaltung von Vorgaben

Der letzte Themenbereich von ISO/IEC 27001 widmet sich dem Thema Compliance. Die auch für Security-Frameworks relevanten Ziele sind dabei:

- Es muss sichergestellt werden, dass gesetzliche Vorgaben eingehalten werden.
- Der Datenschutz und die Vertraulichkeit von personenbezogenen Informationen müssen technisch und organisatorisch gewährleistet werden.
- In der Organisation definierte Sicherheitsleitlinien und technische Vorgaben müssen nachweislich eingehalten werden.
- Es müssen Maßnahmen spezifiziert werden, um Informationssysteme zu auditieren.

Das Erreichen dieser Ziele und der Einsatz von Security-Frameworks beeinflussen sich dabei wie folgt gegenseitig:

- Die Konzepte von Security-Frameworks können Hinweise darauf enthalten, welche externen Auflagen beim Betrieb von Schutzmaßnahmen für die entsprechenden Assets zu berücksichtigen sind.
- Security-Frameworks tragen zur Umsetzung der Compliance-Vorgaben durch entsprechende technische, gebündelte Sicherheitsmechanismen bei.
- Security-Frameworks unterstützen z. B. durch Monitoring- und Reportingschnittstellen die Auditierung der Sicherheitseigenschaften der geschützten Dienste.

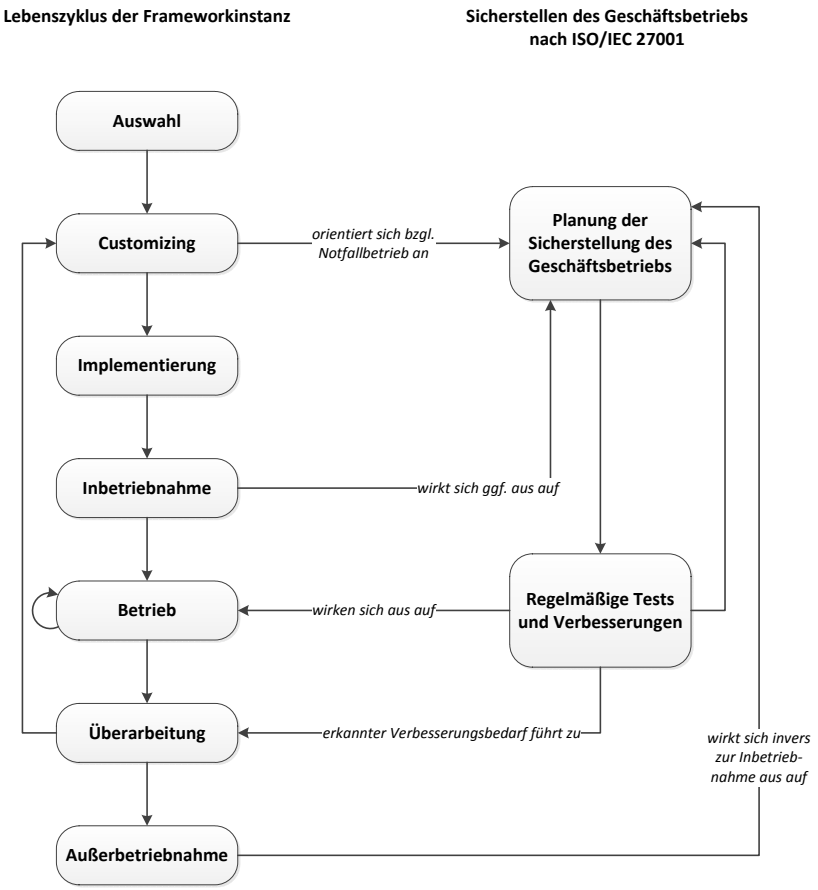


Abbildung 6.28.: Schnittstellen zwischen Security-Frameworks und dem in ISO/IEC 27001 A.14 spezifizierten Sicherstellen des Geschäftsbetriebs

Daraus ergeben sich folgende im Lebenszyklus von Frameworkinstanzen zu berücksichtigende Schnittstellen:

- Compliance-Anforderungen können den Einsatz von Security-Frameworks motivieren und sind bereits beim Customizing und der Implementierung der szenarienspezifischen Frameworkinstanz zu berücksichtigen.
- Bei der Implementierung müssen zudem die geltenden Datenschutzkonzepte umgesetzt werden.
- Im laufenden Betrieb tragen sie zur Umsetzung dieser Anforderungen und zum Erkennen von Abweichungen vom Soll-Zustand bei.
- Änderungen an den Compliance-Anforderungen können entsprechende Überarbeitungen bzw. Reparametrisierungen des Security-Frameworks erforderlich machen.

Diese Schnittstellen sind zusammenfassend in Abbildung 6.29 dargestellt.

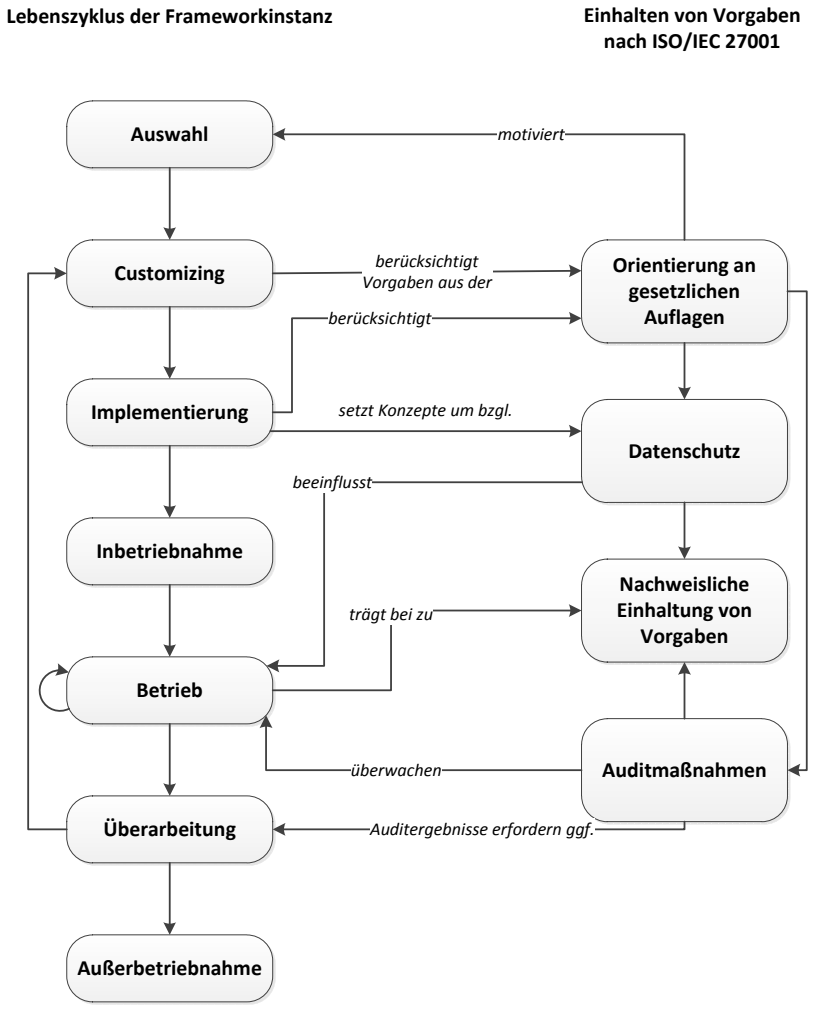


Abbildung 6.29.: Schnittstellen zwischen Security-Frameworks und dem in ISO/IEC 27001 A.15 spezifizierten Einhalten von Vorgaben

6.5.2. Security-Framework-Managementschnittstellen zu ITIL v3

In Abschnitt 2.2.3.3 wurden die mit der Anwendung von ITSM-Prozessen im Allgemeinen verfolgten Ziele und der grundsätzliche Bezug ausgewählter ITIL-Prozesse zum Sicherheitsmanagement bereits skizziert. Zur Verdeutlichung der beim Einsatz von Security-Frameworks spezifischen Schnittstellen zwischen den jeweiligen Managementabläufen werden nachfolgend die fünf von ITIL v3 zur Prozessgruppierung eingesetzten Service-Lebenszyklusphasen – Strategy, Design, Transition, Operation und Improvement – analysiert. Analog zur Betrachtung der Prozesse nach ISO/IEC 27001 werden dabei jeweils die Einflüsse von und die Auswirkungen auf Security-Frameworks herausgearbeitet und die bei der Implementierung und Nutzung der Schnittstellen relevanten Verbindungen zu den Lebenszyklen von Frameworkinstanzen hergestellt.

6.5.2.1. Schnittstellen zur ITIL v3 Service Strategy

Die Ausrichtung der Servicestrategie eines IT-Dienstleisters hängt nach ITIL maßgeblich von seinen avisierten Kunden ab; zu unterscheiden ist beispielsweise, ob es sich um die IT-Abteilung eines kleinen oder eines sehr großen Unternehmens handelt bzw. ob IT-Dienste auch für externe Dritte angeboten werden sollen. ITIL unterscheidet dabei drei eng zusammenhängende Prozesse:

- Das **Demand Management** ist für die Erfassung, Analyse und kontinuierliche Aktualisierung sowohl des eigenen als auch des kundenseitigen Bedarfs an IT-Diensten zuständig. Zu den dabei zu berücksichtigenden Dienstgüteparametern sind auch die Sicherheitseigenschaften zu zählen, die sich Bestandskunden und potentielle Neukunden von den IT-Diensten erwarten.
- Das **Portfolio Management** legt fest, welche IT-Dienste welchen (potentiellen) Kunden in welchem Umfang bzw. in welchen Ausprägungen angeboten werden. Es hat somit die Aufgabe, unter Anwendung ökonomischer Grundprinzipien einen praktikablen Kompromiss aus dem vom Demand Management ermittelten Bedarf und den u. a. vom Financial Management vorgegebenen Ressourceneinschränkungen zu ermitteln und dabei eine der Organisation angemessene Stabilität und Nachhaltigkeit der angebotenen Dienste zu gewährleisten. Hierzu gehört jedoch auch, dass nicht mehr benötigte oder mit akzeptablen Aufwand betreibbare Dienste wieder eingestellt werden.
- Der ITSM-Prozess **Financial Management** bildet die Schnittstelle zum organisationsweiten Finanzwesen und verfolgt somit kontinuierlich das Ziel, ein adäquates Budget für den gesamten IT-Betrieb zu akquirieren und dieses auf die einzelnen IT-Dienste und die dafür notwendige Infrastruktur, zu der auch die IT-Sicherheitsmechanismen gehören, zu verteilen. ITIL beschreibt im Rahmen des IT Service Management keinen separaten Risikomanagement-Referenzprozess, fordert jedoch im Rahmen des Financial Management einen entsprechenden Einbezug von IT-spezifischen Risiken, denen auch die Sicherheitsrisiken zuzuordnen sind.

Aus der Perspektive dieser drei Prozesse stellt der Einsatz von Security-Frameworks eine sehr attraktive Vorgehensweise dar, da diese einerseits explizit auf konkrete IT-Dienste bzw. größere Teile ganzer Dienstleistungsinfrastrukturen zugeschnitten sind und andererseits mehrere Maßnahmen und Mechanismen bündeln, so dass ökonomisch auf in der Regel günstige Komplettlösungen für den Aufgabenkomplex IT-Sicherheit zurückgegriffen werden kann. Die resultierenden gegenseitigen Einflüsse lassen sich wie folgt charakterisieren:

- Security-Frameworks unterstützen die Kostenplanung für Sicherheitslösungen, da sie die für einen Dienst bzw. die für eine Infrastruktur benötigten Sicherheitsvorkehrungen aufeinander abstimmen und eine Gesamtkostenabschätzung zulassen, die bei isolierten Betrachtung einzelner Lösungsbausteine wesentlich aufwendiger und ggf. unschärfer wäre. Diese Problematik der Planung von Sicherheitsinvestitionen wird in Abschnitt 6.6 vertieft. Auch für den Fall, dass sich ein konkretes Security-Framework als unzureichend geeignet für ein spezifisches Szenario erweisen sollte, kann es als Referenz bei der Planung eigener Lösungen herangezogen werden.
- Die von einem Security-Framework als Ganzes gebotene Sicherheitsfunktionalität geht aus den Frameworkkonzepten im Allgemeinen klar hervor und kann somit dem ermit-

telten Bedarf einfacher gegenüber gestellt werden als wenn eine Sicherheitsarchitektur von Grund auf aus Einzelbausteinen zusammengestellt werden muss. Durch in Frage kommende Security-Frameworks nicht abgedeckte Anforderungen müssen ggf. jedoch bewertet und durch ergänzende Maßnahmen erfüllt werden.

- Über das Demand Management, das Portfolio Management und das Financial Management werden Kriterien und Randbedingungen vorgegeben, die sich grundlegend auf die Auswahl von Security-Frameworks, den Umfang ihres Einsatzes und die Möglichkeiten zur Implementierung eigener, ergänzender Frameworkkomponenten auswirken. Somit werden Ziele und Grenzen des Einsatzes von Security-Frameworks vorgegeben, die nicht nur mit der von diesen gebotenen Sicherheitsfunktionalität zusammenhängen.
- Durch die Weiterentwicklung des Bedarfs und der angebotenen IT-Dienste sowie durch die Zielsetzung des Financial Management, nach Möglichkeit nur ökonomisch angemessene Sicherheitsmaßnahmen umzusetzen, bedingt müssen Security-Frameworks kontinuierlich der dynamischen Infrastruktur angepasst werden und eine Beurteilung ihres Nutzens ermöglichen.

Diese Zusammenhänge führen dazu, dass die folgenden Schnittstellen berücksichtigt werden müssen:

- Änderungen an sicherheitsspezifischen Anforderungen sowie am Dienstleistungsportfolio motivieren die initiale Auswahl bzw. größere Überarbeitungen von eingesetzten Security-Frameworks und steuern deren Umfang, Ausprägung und schließlich die Dekommissionierung.
- Das Demand Management und das Financial Management geben grundlegende Kennzahlen und KPIs vor, die zur Beurteilung der Sicherheitsfunktionalität und Kosten des Security-Frameworks im Betrieb benötigt werden. Für den Fall, dass Sicherheitsanforderungen nicht ausreichend erfüllt werden, sind ergänzende Sicherheitsmaßnahmen oder ggf. ein Überdenken der Servicestrategie erforderlich.
- Durch den planerischen Charakter der ITSM-Prozesse im Bereich Service Strategy ergibt sich an die Auswahl und das Customizing von Security-Frameworks die Anforderung, ebenso vorausschauend und nicht nur rein am aktuellen Bedarf orientiert zu handeln.

Abbildung 6.30 veranschaulicht diese Schnittstellen anhand des Lebenszyklus von Frameworkinstanzen.

6.5.2.2. Schnittstellen zum ITIL v3 Service Design

Der ITIL-Bereich Servicedesign konkretisiert die Vorgaben des Portfoliomanagements und verfolgt als übergeordnetes Ziel, zu Bedarf und Budget passende IT-Dienste unter Berücksichtigung der vier Aspekte *Architektur*, *Prozesse*, *Policies* und *Dokumentation* zu spezifizieren. Die unter diesen Gesichtspunkten vollständige Spezifikation eines IT-Dienstes wird als *Service Design Package* bezeichnet. Diese vier Aspekte werden auch von Security-Frameworks behandelt, so dass das Service Design Hand in Hand mit dem Customizing von Security-Frameworks gehen kann.

Dem Servicedesign sind die folgenden Prozesse primär zugeordnet:

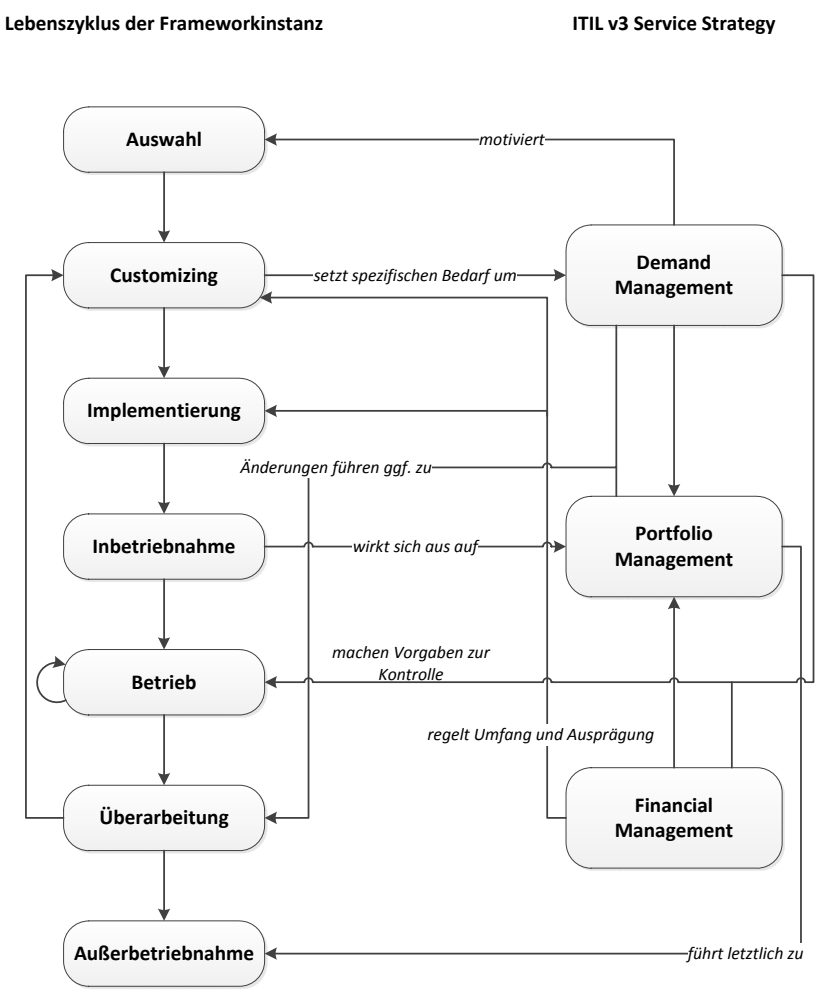


Abbildung 6.30.: Schnittstellen zwischen Security-Frameworks und den in ITIL v3 beschriebenen Service Strategy Prozessen

- Das **Service Catalogue Management** erarbeitet und pflegt einen Dienstleistungskatalog (DLK), der das Serviceportfolio derart in einzelne Dienste und deren Varianten aufteilt, dass diese von den einzelnen Kunden in Auftrag gegeben werden können. Der DLK ist somit einerseits beispielsweise aufgrund von Preisangaben und Informationen zu Ansprechpartnern konkreter als die organisationsinterne Dokumentation des Portfolios; andererseits kann auf die explizite Nennungen von auslaufenden Diensten verzichtet werden, die für Bestandskunden zwar noch erbracht werden und somit zum Portfolio gehören, aber nicht mehr weiter ausgebaut werden sollen. In der Regel enthält der DLK Angaben über Dienstgüteparameter und somit u. a. auch Aussagen über ausgewählte Sicherheitseigenschaften; je nach Dienst und Flexibilität des Dienstleisters sind diese entweder als fest vorgegeben zu betrachten oder können individuell pro Kunde angepasst werden. In jedem Fall bildet der DLK die Grundlage für die vertragliche Regelung der Diensterbringung in Form von Service Level Agreements (SLAs).

- Das **Service Level Management** umfasst alle Maßnahmen zur Pflege der vertraglichen Vereinbarungen zwischen dem IT-Dienstleister und seinen Kunden. Hierzu gehören beispielsweise auch Abläufe, um kundenseitige Interessenvertreter (Stakeholder) zu identifizieren und in Form eines Business Relationship Management regelmäßig positive wie auch negative Rückmeldungen der Kunden zum Dienstbetrieb einzuholen. Im Kern des Prozesses stehen jedoch die auch im Zusammenhang mit Security-Frameworks relevanten SLAs. Diese Verträge regeln den Umfang der für den jeweiligen Kunden erbrachten IT-Dienste und enthalten dazu so genannte SLA-Parameter, die auf Basis des im DLK spezifizierten Dienstes u. a. Dienstgütemerkmale wie seine Soll-Verfügbarkeit und die gewünschten Sicherheitseigenschaften, für die Kunden relevante technische Schnittstellen, Monitoring- und Reportingverfahren, kundenspezifische KPIs, Policies und Vertragsstrafen bei Verstößen gegen diese Vereinbarungen festlegen. Aus der Zielsetzung, diese Vereinbarungen unter Berücksichtigung der drohenden Vertragsstrafen einzuhalten, ergeben sich Prioritäten, die sich u. a. auf den operativen Betrieb sowie das Incident Management und das Risikomanagement auswirken: Führt beispielsweise ein Angriff auf ein Asset zum Ausfall eines Dienstes und somit zu einem Verstoß gegen die mit einem Kunden vereinbarte Dienstverfügbarkeit, so sind die Vertragsstrafen ein ggf. nicht unerheblicher Beitrag zu den fiskalischen Auswirkungen des Schadereignisses, so dass ein erhöhtes Risiko vorliegt. Mit den Kunden vereinbarte Dienstgütemerkmale müssen entsprechend auch bei Vereinbarungen mit Zulieferern bzw. bei unternehmensinterner Unterauftragsvergabe berücksichtigt werden.
- Das **Capacity Management** hat die Aufgabe, die für die Diensterbringung in der vereinbarten Qualität notwendigen Ressourcen wie Rechen- und Speicherkapazitäten sicherzustellen. Dabei muss berücksichtigt werden, dass sich durch den Einsatz der in Security-Frameworks enthaltenen Schutzmaßnahmen eventuell der Durchsatz oder die Antwortzeiten von Diensten verschlechtern können. Ebenso müssen Spitzenlasten, die beispielsweise auch durch aktive Angriffe (Denial-of-Service u. ähnl.) zustande kommen können, abgefedert werden. Der planerische Charakter des Capacity Management muss durch entsprechende organisationsinterne Monitoring- und Reportingmöglichkeiten sowie durch Trendanalysen unterstützt werden.
- Das **Availability Management** stellt die Verfügbarkeit der erbrachten IT-Dienste sicher und hat dabei eine zu Incident Management und Capacity Management komplementäre Rolle. In seinen Aufgabenbereich fällt es beispielsweise, darauf zu achten, dass die Ausfallsicherheit von Frameworkkomponenten, die den Zugriff auf Assets regeln, mindestens genauso hoch ist wie diejenige der Assets selbst.

ITIL v3 sieht noch drei weitere Prozesse vor, auf die im Folgenden nicht näher eingegangen wird, da sie bereits in einem anderen Kontext behandelt worden sind: Das **IT Service Continuity Management** entspricht bezüglich der Relevanz für das Management von Security-Frameworks den entsprechenden Abhandlungen in ISO/IEC 27001 A.14 (vgl. Abschnitt 6.5.1.10) und geht dabei auf weitere, nicht IT-sicherheitsspezifische Aspekte ein. Das **Information Security Management** nach ITIL kann als Teilmenge der Regelungen in ISO/IEC 27001 aufgefasst werden und hat zu diesen in BS 7799-2 eine gemeinsame Wurzel. Schließlich regelt das **Supplier Management** die Zusammenarbeit mit Zulieferern und kann für die hier betrachteten Aspekte als analog zum Service Level Management angesehen werden; im Kontext des Risikomanagements eröffnet es darüber hinaus die Möglichkeit, un-

ter Beibehaltung der Gesamtverantwortung gegenüber den Kunden ausgewählte Risiken an Dritte zu übertragen.

Insgesamt bestehen im Bereich Servicedesign die folgenden Wechselwirkungen mit dem Einsatz und Management von Security-Frameworks:

- Die Servicedesignprozesse regeln die Servicestrategie vertiefend den konkreten Bedarf an Schutzmaßnahmen und definieren somit Anforderungen an den Umfang und die Schutzfunktionalität von Security-Frameworks, die im Szenario eingesetzt werden. Durch Kundenrückmeldungen wird die kontinuierliche Verbesserung und Weiterentwicklung mit angetrieben. Andererseits stellen Security-Frameworks überwachbare und messbare Sicherheitsfunktionen bereit, die ihrerseits wiederum zur Aufwertung des Dienstangebots eingesetzt werden können.
- Neben der SLA-basierten Priorisierung der Schutzziele, die von den Security-Frameworks umgesetzt werden müssen und deren Parametrisierung somit zumindest in Teilen von der Kundenfluktuation abhängig ist, werden durch vertragliche Vereinbarungen auch bereitzustellende Messwerte, KPIs und Berichte vorgegeben, die von den Betreibern der Security-Frameworks geliefert werden müssen. Im Gegenzug wird durch die von Security-Frameworks implementierten Monitoringschnittstellen vorgegeben, welche sicherheitsspezifischen Kennzahlen und KPIs ohne zusätzlichen Implementierungsaufwand bereitgestellt werden können.
- Von Kunden benannte Vertreter nehmen Rollen bei der Nutzung und beim Management von Security-Frameworks ein, um beispielsweise Delegationskonzepte umzusetzen. In Abhängigkeit von der Mandantenfähigkeit der Security-Frameworks müssen ggf. kundenspezifische Frameworkinstanzen implementiert werden.
- Security-Frameworks müssen den durch Availability Management und Capacity Management vorgegebenen Anforderungen an die Hochverfügbarkeit und Performanz der Dienste genügen. Sie tragen jedoch durch den Schutz vor Angriffen auch aktiv dazu bei, Ausfälle der Dienste zu minimieren.
- Die Zusammenarbeit mit Frameworkautoren ist insbesondere beim Einsatz kommerzieller Security-Frameworks in den Kontext des Supplier Management einzubetten.

Somit sind die folgenden Schnittstellen zwischen den hier betrachteten ITSM-Prozessen und Security-Frameworks zu berücksichtigen:

- Die durch das Service Level Management definierten Anforderungen motivieren die Auswahl von Security-Frameworks und geben dafür Kriterien vor. Mit der Auswahl eines Security-Frameworks kann sich eine im Rahmen des Supplier Management zu berücksichtigende Verbindung zu den Frameworkautoren ergeben, die sich über den gesamten Lebenszyklus der Frameworkinstanz erstreckt.
- Bereits beim Customizing des Security-Frameworks müssen die von Service Level Management, Capacity Management und Availability Management definierten Vorgaben umgesetzt werden. Ebenso muss die Implementierung eng mit dem Availability Management abgestimmt werden.
- Durch die Inbetriebnahme des Security-Frameworks ergeben sich ggf. Verbesserungen bzw. Erweiterungen der im DLK anzubietenden Dienste und Dienstgüteparameter.

- Im laufenden Betrieb unterstützt das Security-Framework die Servicedesignprozesse durch jeweils aktuelle Messwerte und Berichte, auf deren Basis auch Trendanalysen durchgeführt werden können.
- Durch Kundenrückmeldungen kann sich der Bedarf an Überarbeitungen der Frameworkinstanz ergeben.
- Die Außerbetriebnahme eines Security-Frameworks wirkt sich invers zur Inbetriebnahme auf den DLK und somit das Service Level Management sowie das Supplier Management aus.

Diese Zusammenhänge sind in Abbildung 6.31 dargestellt.

6.5.2.3. Schnittstellen zur ITIL v3 Service Transition

Die am Dienstlebenszyklus orientierte Prozesskategorisierung nach ITIL ordnet in den Bereich Service Transition alle diejenigen Prozesse primär ein, die der geordneten Überführung neuer und geänderter Dienste in den Produktivbetrieb dienen:

- Der Prozess **Transition Planning and Support** sieht die Konzeption so genannter Releasezyklen vor, die bereits im Kontext der Konzepte von Security-Frameworks diskutiert wurden und bei ITIL dazu dienen, organisationsweit für alle Dienste strategisch festzulegen, in welchen typischen Zeitabständen neue *major* bzw. *minor* Releases freigegeben werden. Er regelt zudem die Durchführung der nachfolgend beschriebenen Prozesse unter der Zielsetzung, für alle neuen und geänderten Dienste Tests zu planen und durchzuführen, den Support kurz nach der Inbetriebnahme dieser Dienste bedarfsorientiert zu verstärken und die Einhaltung von Serviceakzeptanzkriterien zu gewährleisten.
- Das **Change Management** fungiert als Planungs-, Genehmigungs- und Kontrollprozess für sämtliche Änderungen an der Dienstinfrastruktur und ist somit in die Einführung neuer Dienste, alle kleineren und größeren Änderungen an bestehenden Diensten und die Umsetzung kurzfristig dringender Modifikationen zu involvieren, die beispielsweise auch bei akuten, anhaltenden Sicherheitsvorfällen erforderlich werden können. Ein als Change Advisory Board bezeichnetes Gremium bezieht fachlich und organisatorisch Betroffene mit ein, um gewünschte Änderungen zu prüfen, genehmigen und priorisieren; die Dokumentation genehmigter *Changes* umfasst auch die rechtzeitige Ankündigung ihres Durchführungszeitpunkts und der absehbaren Auswirkungen gegenüber Kunden und anderen Interessenvertretern.
- Als zentrales Werkzeug des **Service Asset and Configuration Management** ist das Configuration Management System (CMS) anzusehen, das im Kern aus *einer* logischen Configuration Management Database (CMDB) besteht, die ihrerseits in der Praxis meist aus einer Verknüpfung mehrerer Datenbestände – beispielsweise auch der diskutierten Managementplattform für Security-Frameworks – aufgebaut wird. Die Bereitstellung der darin kontinuierlich gepflegten und durch Soll-/Ist-Abgleiche kontrollierten Informationen für alle anderen Prozesse ist die Hauptaufgabe des Configuration Management. Das CMS kann insbesondere auch zu Planungszwecken eingesetzt werden, da Configuration Items (CIs) erfasst werden können, die noch nicht existierende Infrastrukturkomponenten abbilden; zudem wird die Versionierung individueller CIs und die Zusammenfassung

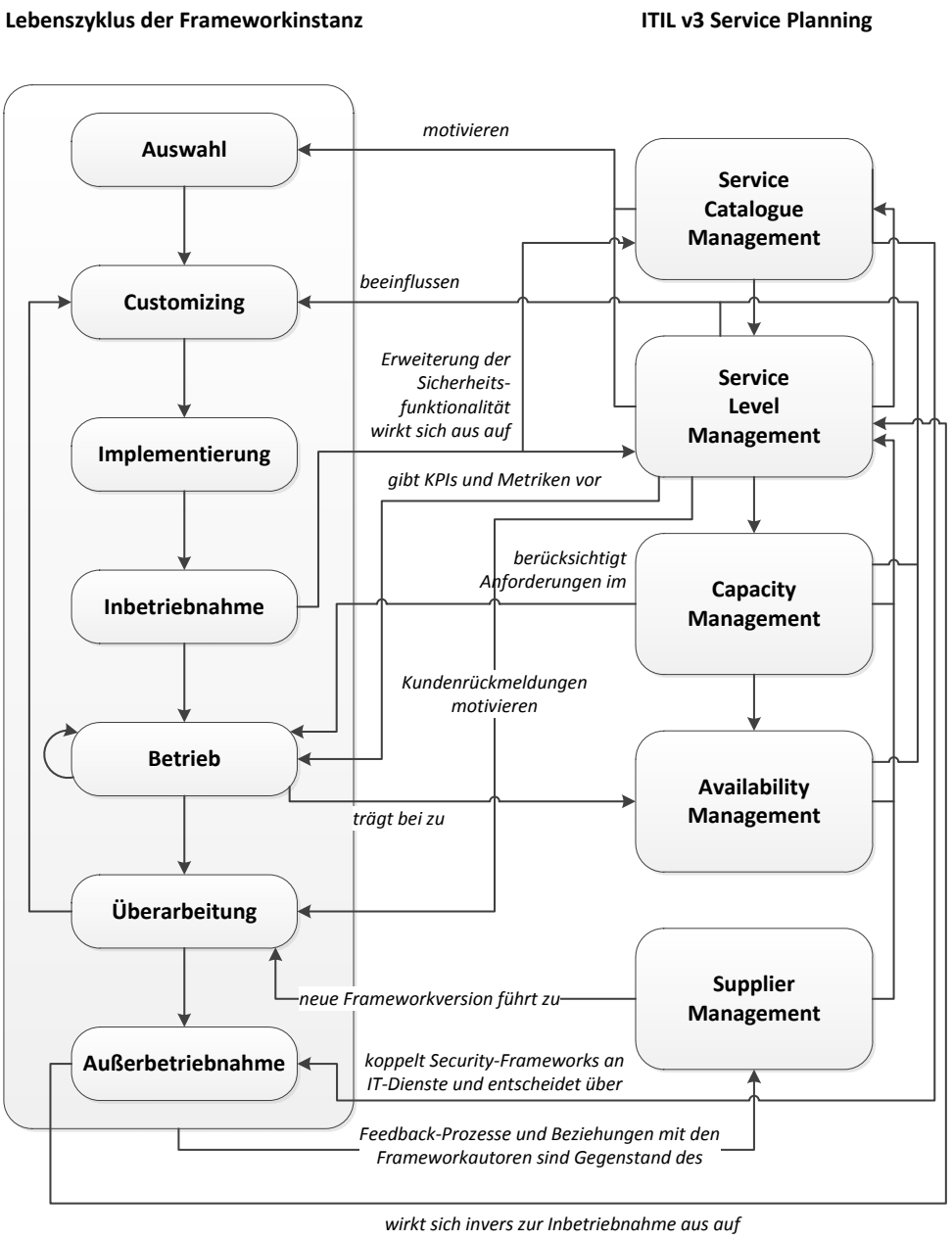


Abbildung 6.31.: Schnittstellen zwischen Security-Frameworks und den in ITIL v3 beschriebenen Service Design Prozessen

des aktuellen Zustands mehrerer CIs zu so genannten Baselines unterstützt, um einen Überblick über die Situation vor bzw. nach komplexen Änderungen zu schaffen und ggf. nach einem fehlgeschlagenen Change wieder auf einen konsistenten früheren Zustand zurückgehen zu können.

- Das **Release and Deployment Management** fasst ggf. mehrere zusammenhängende Änderungen zu einem neuen Release zusammen und führt dessen praktische Umset-

zung durch. Über Tests nach der Inbetriebnahme und eine Erfolgsprüfung anhand vorab definierter Akzeptanzkriterien wird sichergestellt, dass die durchgeführten Änderungen keine unerwarteten negativen Auswirkungen haben; über ein jeweils festzulegendes Rollback-Verfahren kann ggf. zum ursprünglichen Zustand zurückgekehrt werden.

- ITIL v3 sieht darüber hinaus drei unterstützende Prozesse vor, die konzeptionelle und empirische Zuarbeiten liefern:
  - Das **Service Validation and Testing** wirkt qualitätssichernd für neue und geänderte Dienste. Es wird primär vor dem Deployment neuer Releases angewandt und muss somit in die entsprechenden Entwicklungsprojekte eingebunden werden; darüber hinaus können jedoch auch Kontrollvorgänge für die produktiven Dienste in diesen Bereich eingeordnet werden, beispielsweise die Durchführung von regelmäßigen Penetrationstests im operativen Sicherheitsmanagement.
  - Der Prozess **Evaluation** dient der Bewertung potentiell anzuschaffender Assets. Neben der kontinuierlichen Marktbeobachtung und Berücksichtigung der technologischen Weiterentwicklungen ist diesem Prozess auch beispielsweise die Auswahl von Security-Frameworks zuzuordnen.
  - Das **Knowledge Management** hat die Aufgabe, das zum effizienten Betrieb der Infrastruktur erforderliche Wissen verfügbar zu halten und geeignet an die relevanten Personen zu kommunizieren, um u. a. eine fundierte Basis für Entscheidungen und Weiterentwicklungen aufzubauen. Es beinhaltet somit das bereits im Kontext von ISO/IEC 27001 diskutierte Schulungsmanagement und verwaltet beispielsweise auch die Dokumentationen von Frameworkkonzepten und -instanzen.

In Kapitel 5 wurde bereits auf die engen Zusammenhänge zwischen den einzelnen Phasen des Lebenszyklus von Frameworkinstanzen und dem Change Management eingegangen. Darüber hinaus sind folgende gegenseitige Einflüsse zu berücksichtigen:

- Security-Frameworks bestehen im Allgemeinen aus mehreren Komponenten und stellen somit Verbünde von CIs dar, die im Configuration Management entsprechend berücksichtigt werden müssen. CMDBs sehen szenarienspezifische festzulegende Verknüpfungen zwischen CIs vor, so dass beispielsweise auch die Beziehungen zwischen den Komponenten von Security-Frameworks und den von ihnen geschützten Assets modelliert werden können. Dabei muss insbesondere auch auf die Konsistenz der Informationen in einer für das operative Management von Security-Frameworks eingesetzten Managementplattform und dem Configuration Management System geachtet werden, d. h. es müssen entweder ein gemeinsamer Datenbestand verwendet oder Synchronisationsmechanismen implementiert werden.
- Der in Abschnitt 5.2.1 erläuterte Freigabevorgang für Frameworkkonzepte muss mit den szenarienspezifischen ITSM-Releasezyklen abgestimmt werden. Neben der erforderlichen zeitlichen Koordination, die sicherstellen soll, dass neue Versionen des Security-Frameworks zeitnah implementiert und produktivgeführt werden, ist dabei auch zu beachten, dass der Inhalt und Umfang von Releases zu einem durch das szenarienspezifische Customizing festgelegten Grad quasi von außen vorgegeben wird, so dass vom Deployment Management auszurollende Releases nicht aus einzeln zu ermittelnden Changes bestehen.

- Während sich somit der szenarienspezifische Aufwand für das Deployment reduziert, werden vorgelagerte Prozesse wie die Evaluation und das Testen aufwendiger, da nicht nur einzelne Komponenten, sondern z. T. komplexe Architekturen beurteilt und ggf. mit Spezialwerkzeugen getestet werden müssen.
- Im Gegenzug müssen Security-Frameworks anhand der szenarienspezifisch festgelegten Akzeptanzkriterien beurteilt werden und Prozeduren, beispielsweise für das Baselining, die Durchführung von Rollbacks und Soll-/Ist-Vergleiche umsetzen können.

Zwischen den für Security-Frameworks spezifischen Managementabläufen und den vorgenannten ITSM-Prozessen sind somit die folgenden Schnittstellen zu berücksichtigen:

- Die Auswahl, das Customizing, die Inbetriebnahme sowie Wartungsarbeiten, Überarbeitungen und die Außerbetriebnahme von Security-Frameworks unterliegen den planerischen Aufgaben des Change Management (vgl. Abschnitte 5.4 bis 5.10).
- Die Auswahl von Security-Frameworks erfolgt im Rahmen des Prozesses *Evaluation*; Customizing, Implementierung und Inbetriebnahme werden durch den Prozess *Transition Planning and Support* unterstützt.
- Die Inbetriebnahme neuer und geänderter Security-Frameworks erfolgt nach Durchlaufen der vorgegebenen Testprozeduren durch das *Release and Deployment Management*.
- Im Betrieb wird der aktuelle Zustand im Rahmen des *Configuration Management* im Zusammenspiel mit *Service Validation and Testing* überwacht. Betriebserfahrungen werden über das *Knowledge Management* aufbereitet.

Diese Schnittstellen sind in Abbildung 6.32 veranschaulicht.

6.5.2.4. Schnittstellen zur ITIL v3 Service Operation

Zum Bereich Service Operation fasst ITIL alle Aufgaben zusammen, die im laufenden Betrieb von IT-Diensten anfallen. Die einzelnen Prozesse werden durch auslösende Ereignisse angestoßen, zu denen einerseits Störungsmeldungen z. B. durch Benutzer bzw. Monitoringsysteme oder andere Formen von Benutzeranfragen und andererseits Schnittstellen zu anderen ITSM-Prozessen gehören: Während das *Incident Management* durch automatisch oder manuell berichtete Störungen initiiert wird, muss das *Access Management* beispielsweise auch bei Kundenfluktuation und damit auf Basis des *Service Level Management* aktiv werden. ITIL v3 unterscheidet die folgenden Prozesse:

- Das **Event Management** betrachtet alle Arten von managementrelevanten Ereignissen, wie sie beispielsweise von Systemüberwachungsmechanismen gemeldet werden. Es stellt somit auf technischer Ebene funktional eine Teilmenge des Monitorings dar. Analog zur Unterscheidung von Sicherheitsereignissen und Sicherheitsvorfällen können auch *Events* einen rein informativen oder bestätigenden Charakter haben, d. h. bei Weitem nicht jeder *Event* ist als *Incident* aufzufassen. Dienste und Systeme müssen eine entsprechende Instrumentierung aufweisen, um vom Event Management zu verarbeitende Ereignisse generieren zu können. Im Allgemeinen ist die Anzahl gemeldeter Events szenarienweit so groß, dass sie von einzelnen Administratoren nicht mehr überblickt werden kann. Eine wichtige Aufgabe ist deshalb die automatische Filterung und Klassifizierung

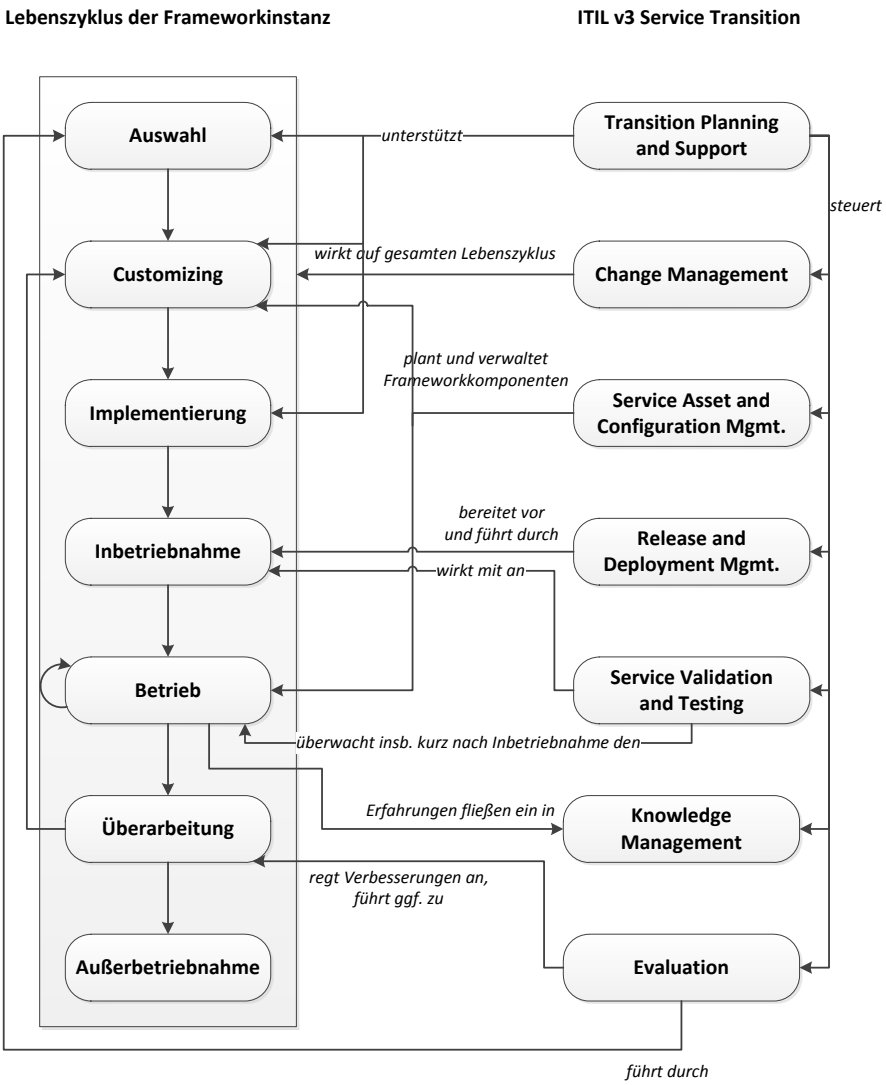


Abbildung 6.32.: Schnittstellen zwischen Security-Frameworks und den in ITIL v3 beschriebenen Service Transition Prozessen

von Events auf Basis zu spezifizierender, konfigurierbarer Regelsätze, so dass sich Administratoren auf die wesentlichen Meldungen konzentrieren können und ggf. über besonders dringende oder wichtige Meldungen auch über weitere Kommunikationskanäle, z. B. per E-Mail oder SMS, benachrichtigt werden.

- Das **Incident Management** behandelt alle ungeplanten Qualitätseinschränkungen der betriebenen IT-Dienste. Es wird durch automatische oder manuelle Störungsmeldungen, die eine Teilmenge der im Event Management behandelten Ereignisse darstellen, angestoßen. Der Prozess verfolgt im Unterschied zum unten beschriebenen Problem Management nicht vorrangig das Ziel, die Ursache für die gemeldete Störung zu beseitigen, sondern soll primär größere Beeinträchtigungen vermeiden und sicherstellen, dass aus Kunden- und Anwendersicht schnellstmöglich wieder zum Regelbetrieb übergegangen

werden kann; als Behelfslösungen können temporär so genannte Workarounds implementiert werden.

Da in komplexen Infrastrukturen häufig mehrere noch ungelöste Störungen parallel vorkommen, müssen diese priorisiert werden. Die Priorität wird dabei aus den Auswirkungen (engl. *impact*) der Störung auf den Geschäftsbetrieb und der Dringlichkeit (engl. *urgency*) ihrer Behebung abgeleitet; die Dringlichkeit hängt dabei maßgeblich davon ab, welche Entstörzeiten mit den Kunden im Rahmen von SLAs vereinbart wurden und welche Vertragsstrafen drohen, wenn diese Vorgaben nicht eingehalten werden. Störungen, deren Auswirkungen und Dringlichkeit vorgegebene Schwellenwerte überschreiten, werden als Major Incidents bezeichnet, die so große Betriebseinschränkungen darstellen, dass hierfür meist eine gesonderte Form des Incident-Management-Prozesses zum Einsatz kommt. Störungen können auch anhand anderer Kriterien kategorisiert werden; ist der Auslöser einer Störung beispielsweise eine Menge von Sicherheitsereignissen, so liegt ein Sicherheitsvorfall vor, für den es in Anlehnung an ISO/IEC 27001 eine als Security-Incident-Response-Prozess bezeichnete Variante des Incident Management geben kann.

Im Rahmen der Bearbeitung von Störungen, die zunächst vom so genannten First-Level-Support durchgeführt wird, kann eine fachliche Eskalation an den Second-Level-Support notwendig werden, beispielsweise wenn die Mitarbeiter des Servicedesks die Störung nicht selbst beseitigen können, sondern auf die eigentlichen Dienstbetreiber zurückgreifen müssen. Eine hierarchische Eskalation, d. h. ein Bericht über die Störung an die organisatorisch Vorgesetzten, wird beispielsweise dann erforderlich, wenn abzusehen ist, dass Störungen nicht in der mit Kunden vereinbarten Zeit behoben werden können. Die Störungen selbst und die dafür gefundenen Workarounds und Lösungen müssen dokumentiert werden; bei von Kunden bzw. Anwendern gemeldeten Störungen wird in der Regel nachgefragt, ob die Störung auch aus ihrer Sicht zufriedenstellend behoben wurde, bevor die Bearbeitung abgeschlossen wird. Über Statistiken und Trendanalysen auf Basis der dokumentierten Incidents können Verbesserungsmaßnahmen auf technischer und organisatorischer Ebene abgeleitet werden, beispielsweise indem instabile Dienstkomponenten oder Defizite im Knowledge Management, das auch die zur Störungsbeseitigung relevanten Informationen verwaltet, identifiziert werden.

- Ein als **Request Fulfillment** bezeichneter Prozess verarbeitet Benutzeranfragen, die keine Störungsmeldungen sind, sondern z. B. Auskunftsersuchen oder Bitten um die Durchführung eines typischerweise präautorisierten Changes, z. B. das Zurücksetzen eines vergessenen Passworts durch den Servicedesk. Beispielsweise über webbasierte Self-Service-Portale kann eine Semiautomatisierung erreicht werden.
- Der Prozess **Problem Management** hat zum einen die reaktive Aufgabe, die Ursachen von Störungen zu ermitteln und nachhaltig zu beheben. Darüber hinaus werden im Rahmen dieses Prozesses jedoch auch proaktive Maßnahmen durchgeführt, um Störungen möglichst a priori zu verhindern. Die Umsetzung dieser Verbesserungen muss eng mit dem Change Management und dem Release Management abgestimmt werden.
- Das **Access Management** umfasst die zentrale Koordination und die dezentrale Umsetzung von Benutzerberechtigungen. Der Prozess wurde beim Übergang von ITIL v2 zu ITIL v3 eingeführt und ist in den ITIL-Dokumenten bislang nur sehr knapp spezifiziert. Seine Zielsetzung ist mit dem in Abschnitt 6.5.1.7 diskutierten Bereich *Zugangskontrolle* von ISO/IEC 27001 vergleichbar, so dass an dieser Stelle auf eine nähere Betrachtung

verzichtet wird.

Die ITIL-Prozesse im Bereich Service Operation stehen mit dem Management von Security-Frameworks in folgendem Zusammenhang:

- Security-Frameworks enthalten zur Erkennung und Meldung von sicherheitsrelevanten Ereignissen benötigte Sensoren und ermöglichen eine genaue Zuordnung z. B. zu den von Angriffen betroffenen Assets. Sie setzen damit wesentliche technische Aspekte des Event Management um.
- Für den Fall, dass ein Security-Framework einen Angriff nicht nur erkennen, sondern auch verhindern kann, trägt es dazu bei, die Anzahl von (Security) Incidents zu reduzieren; andernfalls wirkt es an der Störungslokalisierung und -beurteilung im Rahmen des Incident Management mit. Hierzu trägt wie in Abschnitt 6.4.3 beschrieben beispielsweise bei, dass die Auswirkung einzelner Bedrohungen bereits analysiert wurden und somit zur Incident-Priorisierung herangezogen werden können.
- Über die Prozesse Event Management, Incident Management und Problem Management werden Melde- und Eskalationswege vorgegeben, die von den Automatismen im Security-Framework unterstützt bzw. über Schnittstellen und Triggermechanismen genutzt werden müssen.
- Zur Unterstützung des Request Fulfillment müssen Security-Frameworks Schnittstellen anbieten, die entweder dazu genutzt werden können, die mandantenspezifische Konfiguration z. B. vom Servicedesk durchführen zu können, oder über Self-Service-Portal genutzt werden können.
- Für den Fall, dass ein Security-Framework fehlerhaft ist, so dass es nicht nur zu vereinzelten Störungen kommt, sondern dass das Problem Management ein systematisches Defizit erkennt, wird das Change Management angestoßen, um entsprechende Anpassungen des Security-Frameworks zu veranlassen.

Daraus ergeben sich die folgenden zu berücksichtigenden Schnittstellen im Lebenszyklus von Frameworkinstanzen:

- Bereits beim Customizing müssen die Meldewege und Schnittstellen zur Propagation von Sicherheitsmeldungen und -vorfällen berücksichtigt werden.
- Kurz nach der Inbetriebnahme eines Security-Frameworks können eventuell vermehrt Störungsmeldungen auftreten, da technische Probleme vorliegen oder Benutzer ein bewusst verändertes Verhalten eines von einem Security-Framework geschützten Dienstes falsch interpretieren und den Servicedesk kontaktieren. Diese Übergangsphase wird vom Prozess *Transition Planning and Support* berücksichtigt.
- Im laufenden Betrieb liefern Security-Frameworks über Sensoren und Protokolle Ereignisse und ggf. Sicherheitsvorfallsmeldungen an das Incident Management.
- Das Problem Management kann Wartungsarbeiten und größere Überarbeitungen von Security-Frameworks mittelbar über das Change Management anstoßen.
- Über implementierte Self Services wird das Request Fulfillment unterstützt, das wiederum Änderungen durchführt, die sich auf den laufenden Betrieb auswirken.

Abbildung 6.33 fasst diese Schnittstellen zusammen.

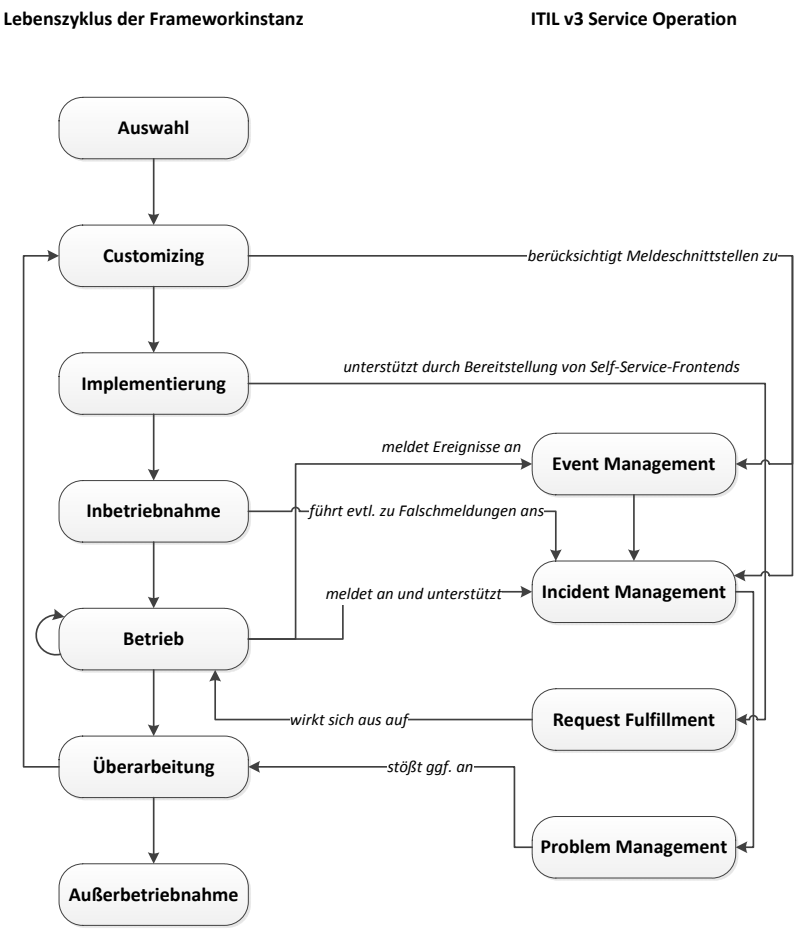


Abbildung 6.33.: Schnittstellen zwischen Security-Frameworks und den in ITIL v3 beschriebenen Service Operation Prozessen

Durch die Einbettung von Security-Frameworks in die Betriebs- und Managementprozesse soll auch das Ziel erreicht werden, Redundanzen und dienst- bzw. schutzmaßnahmenspezifische Arbeiten zu vermeiden. Ein dabei zentraler Vorgang ist der Umgang mit Sicherheitsvorfällen, die von einem Security-Framework erkannt wurden und durch ein Zusammenspiel des operativen Sicherheitsmanagements und des Incident Management verarbeitet werden sollen. Abbildung 6.34 gibt ein Beispiel für den erfolgreichen Ablauf eines von einem Security-Framework angestoßenen Security-Incident-Response-Prozesses:

- Für den Betrieb einer E-Commerce-Website wird ein Security-Framework eingesetzt, das den Webserver und die darunterliegende Datenbank schützen soll und u. a. ein Intrusion Detection System verwendet, um den gesamten Nutzdatenverkehr auf bekannte Angriffe zu analysieren. Optional besteht die Möglichkeit einer Deep-Packet-Inspection, um beispielsweise SQL-Injection-Angriffe erkennen zu können, die im Regelbetrieb aus Performanzgründen jedoch deaktiviert ist. Das IDS erkennt den Beginn eines Denial-of-Service-Angriffs, bei dem von außen eine große Menge von Datenpaketen mit unbrauchbarem Inhalt an den Webserver geschickt wird.

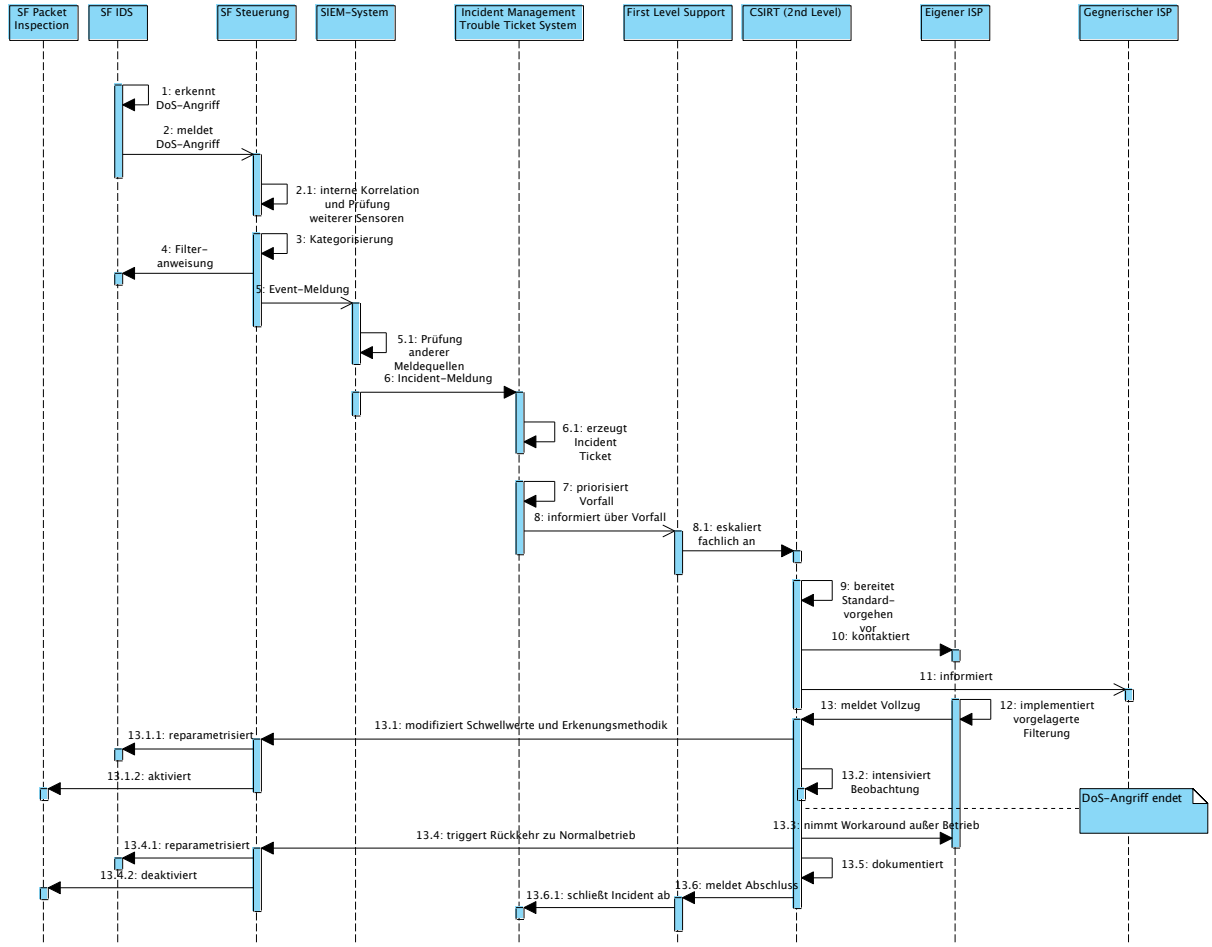


Abbildung 6.34.: Beispiel für das Zusammenspiel von Security-Frameworks, Security Management und Incident Management

- Das IDS sendet eine Nachricht an die Steuerkomponente des Security-Frameworks. Diese prüft, ob weitere Sensoren im Abdeckungsbereich des Security-Frameworks ebenfalls Sicherheitsereignisse melden. Da dies nicht der Fall ist, liegt aus Perspektive des Security-Frameworks ein Denial-of-Service-Angriff gegen den Webserver vor.

  Die Steuerkomponente weist das IDS an, den von der Quelladresse des DoS-Angriffs eingehenden Datenverkehr nicht an den Webserver weiterzugeben, so dass dieser und die Datenbank von den unerwünschten Anfragen dieser Quelle nicht überlastet werden.

- Trotz dieser Reaktion des Security-Frameworks und der dynamischen Aktivierung eines Sicherheitsmechanismus wird die Dienstqualität dennoch eingeschränkt, da ein erheblicher Teil der Uplink-Bandbreite vom Angriff aufgebraucht wird. Ein in der Steuerkomponente des Security-Frameworks vorkonfigurierter Regelsatz gibt vor, dass das Eintreten solcher Ereignisse an ein zentrales Security Information & Event Management System zu melden ist.

- Da das SIEM-System weitere Meldequellen, beispielsweise andere Security-Frameworks,

autarke Sensoren, Monitoringwerkzeuge und manuelle Eintragungen, auswerten kann, prüft es, ob neben dem Webserver noch weitere Dienste, beispielsweise der ebenfalls aus dem Internet zu erreichende Mailserver, ebenfalls betroffen sind. Da dies nicht der Fall ist, bleibt die Kategorisierung des Ereignisses als Denial-of-Service-Angriff gegen den Webserver erhalten.

Aufgrund der Qualitätsdegradierung und der Problematik, dass lokal keine Sicherheitsmechanismen und keine zuschaltbaren Ressourcen vorhanden sind, durch die die Auswirkung des laufenden Angriffs reduziert werden könnte, meldet das SIEM-System einen DoS-Sicherheitsvorfall, der im Rahmen des Incident Management bearbeitet wird.

- Bei der Meldung des Vorfalls an das Incident Management wird zunächst ein Incident-Datensatz generiert, dem im Verlauf der Bearbeitung weitere Informationen hinzugefügt werden können. Durch die vom Security-Framework weitergegebenen Daten können die meisten Angaben zum Incident automatisch vorbelegt werden: Es handelt sich um einen Sicherheitsvorfall, der auf einen Denial-of-Service-Angriff von einer bekannten Quelladresse, der ein unbekannter externer Angreifer zuzuordnen ist, gegen den Webserver gerichtet ist; dabei wurde bislang keine Maschine kompromittiert, aber die Dienstgüte ist durch die eingeschränkte Bandbreite anhaltend beeinträchtigt. Zudem wird der Incident-Datensatz mit den protokollierten Sicherheitsmeldungen verknüpft.
- Auf Basis vorgegebener Auswertungsregeln wird dem Incident eine hohe Priorität eingeräumt. Der First Level Support hat für den Fall hoch priorisierter Sicherheitsvorfälle die Anweisung erhalten, den Incident funktional an den Second Level Support eskalieren; deshalb wird das lokale CSIRT (Computer Security Incident Response Team) eingeschaltet. Dabei handelt es sich um ausgewählte Mitarbeiter im operativen Sicherheitsmanagement, die neben ihren Regeltätigkeiten für die schnelle Reaktion auf akute Vorfälle zuständig sind.
- Das CSIRT nimmt auf Basis einer Empfehlung im Frameworkkonzept, die in das Betriebskonzept eingeflossen ist, als Workaround Kontakt mit dem Internet-Provider auf, der den Uplink betreibt, und bittet ihn, den gesamten Datenverkehr von der bekannten Angreiferadresse bereits zu verwerfen, bevor er in Richtung der Organisation weitergeleitet wird, um die Bandbreitenbelastung zu reduzieren. Zudem wird der Angriff an den Internet-Provider des Angreifers gemeldet, von dem jedoch keine sofortige Reaktion erwartet wird.
- Um zeitnah erkennen zu können, ob der Angreifer eventuell auf eine andere Quelladresse ausweicht, um seinen Angriff fortzuführen oder zu verstärken, werden über das Security-Framework die Schwellenwerte zur DoS-Erkennung temporär reduziert und das SIEM-System, an das das Security-Framework seine aktuellen Messwerte liefert, einer verstärkten Beobachtung unterzogen. Bei der Reparametrisierung handelt es sich dabei um einen so genannten *preauthorized Change*, der zwar dokumentiert, aber nicht vorab von einer anderen Instanz genehmigt werden muss. Dabei stellt sich jedoch heraus, dass aktuell keine weiteren Angriffe erkennbar sind.
- Der Dienstbetrieb kann somit nach wenigen Minuten ohne weitere Qualitätseinbußen aufrecht erhalten werden.
- In Rücksprache mit dem eigenen Internet-Provider wird nach einigen Stunden, nachdem der DoS-Angriff von selbst abgeklungen ist oder der Internet-Provider des Angreifers

reagiert hat, der Workaround wieder außer Betrieb genommen. Die durchgeführten Maßnahmen und deren Erfolg werden im Incident-Dokument festgehalten und der Incident abgeschlossen.

Die bei vergleichbaren Vorfällen anfallenden Tickets können später ausgewertet werden, um systematisch Rückschlüsse auf weitere sinnvolle Schutzmaßnahmen ziehen zu können. Neben Verfahrensanweisungen für den First und Second Level Support kann beispielsweise geprüft werden, ob die Koordination mit dem Internet-Provider zum vorgelagerten Filtern des Internet-Datenverkehrs über technische Schnittstellen automatisiert werden kann.

6.5.2.5. Schnittstellen zum ITIL v3 Continual Service Improvement

Die Einbettung des IT Service Management in einen kontinuierlichen Verbesserungsprozess und damit die Aufgaben in den Check- und Act-Phasen des Demingzyklus beschreibt ITIL v3 als **7-step improvement process**. Dieser Prozess besteht im Wesentlichen aus Schritten zum Messen und Auswerten des aktuellen Zustands, um daraus Verbesserungsmaßnahmen ableiten zu können, die anschließend umgesetzt werden. Die Hauptschwierigkeit besteht dabei darin, festzulegen, was gemessen werden *soll* und was davon auch mit akzeptablem Aufwand gemessen werden *kann*. Diese Fragestellung wird auf Security-Frameworks bezogen in Abschnitt 6.6 behandelt.

ITIL v3 sieht im Bereich *Continual Service Improvement* vier weitere, den kontinuierlichen Verbesserungsprozess unterstützende Prozesse vor, auf die die ITIL-Dokumentation jedoch jeweils nur knapp eingeht: Im Rahmen des **Service Reporting** wird im Wesentlichen festgelegt, dass es verschiedene Zielgruppen für Berichte geben kann, mit denen Frequenz und Umfang der Berichte abgestimmt werden sollte; zudem wird zwischen prozess-, technologie- und servicespezifischen Metriken unterschieden. Das **Measurement** skizziert die technische Umsetzung der Datenerfassung für das Erstellen von Berichten über IT-Dienste. Schließlich dienen die Prozesse **Return on Invest for CSI** und **Business Questions for CSI** der Durchführung von Kosten-/Nutzenanalysen der angebotenen IT-Dienste und der Berücksichtigung geschäftlicher Entwicklungen bei der Weiterentwicklung der IT-Dienste.

Diese Prozesse treten mit dem Management von Security-Frameworks wie folgt in Wechselwirkung:

- Die Konzepte und Implementierungen von Security-Frameworks legen fest bzw. liefern Vorschläge dafür, welche Status- und Verlaufsinformationen im Betrieb gemessen und im Rahmen von Berichten verwertet werden können und sollen. Sie unterstützen das Reporting folglich aus Perspektive des Sicherheitsmanagements und ermöglichen eine Gruppierung nach geschützten Assets.
- Die Frameworkkonzepte liefern, sofern sie die entsprechenden Anforderungen erfüllen, Aussagen zum Kosten-/Nutzenverhältnis der von ihnen vorgeschlagenen Maßnahmen und geben in ihrer Dokumentation Beispiele für Anwendungsfälle und -gebiete.
- Da die ITIL-Prozesse in diesem Bereich insbesondere eine Weiterentwicklung und Verbesserung der angebotenen IT-Dienste anstoßen sollen, liefern sie indirekt neue Anforderungen an die technischen und organisatorischen Schutzmaßnahmen, die wiederum bei der Weiterentwicklung der Security-Frameworks berücksichtigt werden müssen.

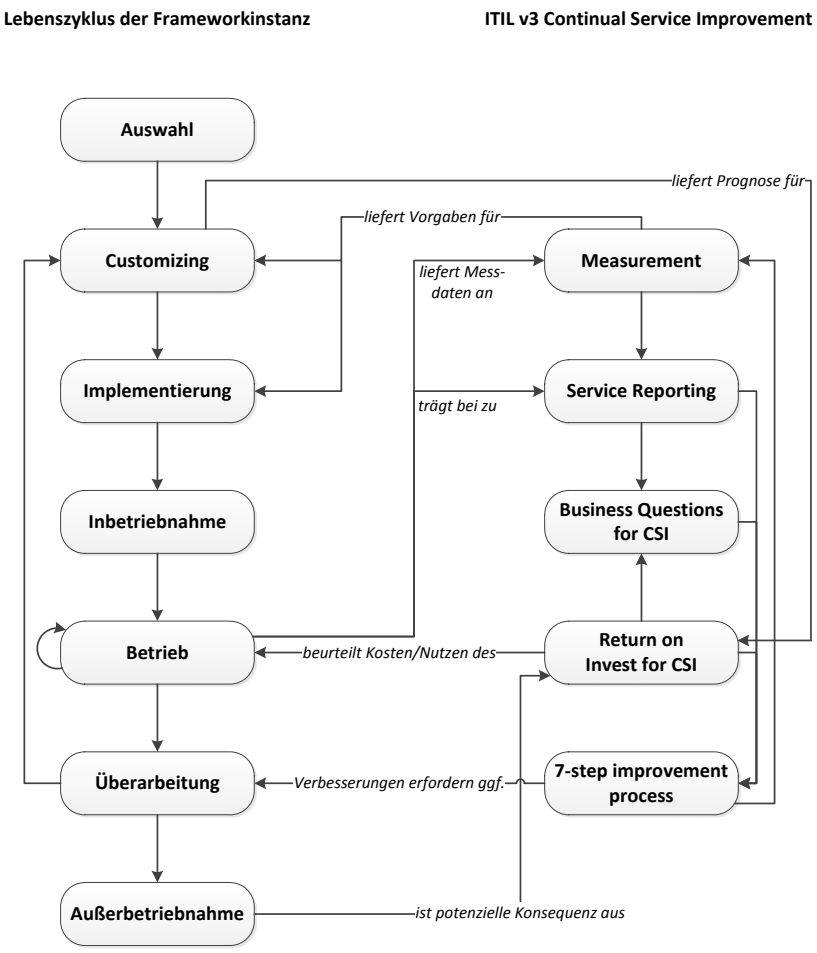


Abbildung 6.35.: Schnittstellen zwischen Security-Frameworks und den in ITIL v3 beschriebenen Continual Service Improvement Prozessen

- Die Durchführung von Return-on-Invest-Analysen wirkt sich auch in Form von Überprüfungen des Kosten-/Nutzenverhältnisses von Security-Frameworks und deren Komponenten aus.

Als Schnittstellen zu den einzelnen Phasen des Lebenszyklus von Frameworkinstanz sind somit festzuhalten:

- Beim Betrieb von Security-Frameworks müssen Messwerte geliefert und Berichte erstellt werden, die den organisationsweiten Regelungen entsprechen.
- Die Überarbeitung von Security-Frameworks und die Maßnahmen zur Verbesserung der IT-Dienste müssen aufeinander abgestimmt sein.
- Als Ergebnis einer Kosten-/Nutzenanalyse können größere Änderungen eines Security-Frameworks bis hin zu seiner Außerbetriebnahme erforderlich werden.

Abbildung 6.35 fasst diese Schnittstellen zusammen.

6.5.3. Ausgewählte Security-Framework-Managementschnittstellen zu CobiT

Wie in Abschnitt 6.1 skizziert wurde, behandelt CobiT die Thematik IT-Governance in der Breite. Die 34 von CobiT spezifizierten Prozesse sind – vergleichbar mit dem am Lebenszyklus von IT-Diensten orientierten Vorgehen von ITIL v3 – in die vier Kategorien *Plan and Organize (PO)*, *Acquire and Implement (AI)*, *Deliver and Support (DS)* und *Monitor and Evaluate (ME)* untergliedert. Mit Bezug auf das Management von Security-Frameworks sind vorrangig die folgenden drei Prozesse zu betrachten:

- Der CobiT-Prozess *DS5: Ensure Systems Security* fasst den Begriff *Systems Security* sehr breit auf, d. h. es wird nicht die Systemsicherheit gemäß Abschnitt 6.2, sondern das gesamte operative Sicherheitsmanagement darunter verstanden. CobiT DS5 fordert beispielsweise explizit die Definition von Rollen und Zuständigkeiten, die Berücksichtigung verschiedenster Interessenvertreter, Monitoring, proaktives Testen, das Minimieren der Auswirkungen von Sicherheitsvorfällen und das Buchführen über erkannte Verstöße gegen Richtlinien und im Szenario bekannte, aber noch nicht erfüllte Sicherheitsanforderungen. Die für Security-Frameworks relevanten Schnittstellen sind dabei durch ISO/IEC 27001 A.6, A.10 und A.13 sowie durch ITIL v3 Demand Management, Service Level Management, Service Validation and Testing und die generelle Ausrichtung an einem kontinuierlichen Verbesserungsprozess bereits abgedeckt.
- Mit dem CobiT-Prozess *ME2: Monitor and Evaluate Internal Control* werden u. a. für den ganzen Bereich des Sicherheitsmanagements die Ziele verfolgt, zu dokumentieren, wann sich welche technischen und organisatorischen Maßnahmen als unzureichend erwiesen haben, die Ursachen und Hintergründe dafür zu ermitteln, neben *Self Assessments* auch Audits durch externe Dritte durchführen zu lassen und daraus abgeleitete Verbesserungsmaßnahmen nachweislich zu planen und umzusetzen. Unter Orientierung an der Norm ISO/IEC 27001 ist zu beachten, dass diese ebenfalls organisationsinterne Auditprogramme und von Dritten durchgeführte Zertifizierungsaudits vorsieht, explizites Managementengagement durch Sicherheitsinitiativen fordert und die Behandlung von Sicherheitsvorfällen durch den Maßnahmenblock A.13 regelt; wird ferner das ITIL v3 Problem Management hinzugezogen, so ergeben sich auch für diesen Prozess keine zusätzlichen Schnittstellen im Rahmen des Managements von Security-Frameworks.
- Im Unterschied zu ISO/IEC 27001 und ITIL v3 postuliert CobiT mit dem Prozess *AI1: Identify Automated Solutions* explizit, dass bei der Anschaffung bzw. Implementierung von Managementprozessen und -werkzeugen auf eine möglichst weitreichende Automatisierung zu achten ist. CobiT AI1 verfolgt die drei Teilziele, zunächst den Bedarf an Automatisierung, die zur Umsetzung zuverlässiger und kostensparender Lösungen dienen soll, zu identifizieren; darauf aufbauend sind eine Priorisierung vorzunehmen und die Umsetzbarkeit zu klären. Schließlich sind auch Risiken zu betrachten, die sich genau daraus ergeben können, dass in bestimmten Bereichen noch keine Automatisierung umgesetzt werden konnte.

  Für den Einsatz von Security-Frameworks ergibt sich daraus das explizite Ziel, die Sicherheitsfunktionalität und die administrativen Schnittstellen möglichst weitgehend automatisierbar zu gestalten. Die resultierenden technischen Schnittstellen müssen deshalb bereits beim Customizing und bei der Implementierung von Security-Frameworks berücksichtigt und genutzt werden. Im Gegenzug tragen Security-Frameworks im lau-

fenden Betrieb zur Erfüllung dieser Maßgabe bei.

Die Analyse der Prozesse und Teilaspekte von ISO/IEC 27001, ITIL v3 und CobiT zeigt somit, dass über alle Lebenszyklusphasen hinweg zahlreiche Schnittstellen zu den Security-Frameworks zu betrachten sind, die sich nicht nur auf die szenarienspezifischen Ausprägungen von Security-Frameworks, sondern auch den Umfang und die Inhalte der entsprechenden Leitlinien und Policies auswirken können und müssen. Dies verdeutlicht erneut die Relevanz der über die technischen Inhalte hinausgehenden Betrachtung organisatorischer Aspekte und prozessualen Schnittstellen bereits in den Frameworkkonzepten.

Abschließend ist zu ergänzen, dass in den Standards und Best Practices die von den sie anwendenden Organisationen zu erstellende Dokumentation von Prozessinstanzen eine wesentliche Rolle spielt; sie kann sowohl in Form von Aufzeichnungen (engl. *Records*) als auch expliziten Berichten (engl. *Reports*) vorliegen. Als essentielle Managementaufgabe im Kontext von Security-Frameworks und als Schnittstelle zu diversen anderen Prozessen wird der Umgang mit für Security-Frameworks spezifischen Messungen, Indikatoren und Berichten im nächsten Abschnitt vertieft.

6.6. IT-Sicherheitskennzahlen im Kontext von Security-Frameworks: Messungen, Indikatoren und Berichtswesen

Die Sicherheit von IT-Systemen ist eine Eigenschaft, für die es bislang keine universellen, standardisierten Mess- und Vergleichsverfahren gibt: Entsprechende Maßeinheiten wie bei physikalischen Größen fehlen beim derzeitigen Stand der Technik schlichtweg. Somit können selbst einfach erscheinende Fragen wie beispielsweise

- Welche von n möglichen Konfigurationen eines Systems ist die sicherste?
- Lohnt sich die Investition in Security-Framework z?
- Ist das Sicherheitsniveau von Organisation x höher als das von Organisation y?

im Allgemeinen nicht einheitlich auf Basis einer objektiven Methodik beantwortet werden. Dies zeigt sich auch bei den in Kapitel 4 untersuchten Security-Frameworks darin, dass sie bei der Untersuchung verschiedener Lösungsalternativen für einzelne Module jeweils eigene Vergleichskriterien definieren und heranziehen (vgl. Abschnitt 4.3.1).

Der Bedarf, belastbare quantitative Aussagen zur Informationssicherheit zu treffen, hat seinen Ursprung nicht ausschließlich in der Wissenschaft, sondern vorrangig in der Praxis, insbesondere im Zusammenspiel mit dem Risikomanagement und der IT-Budgetierung [GHJ03]. Dadurch motiviert, dass durch ein zunächst pragmatisches, empirisches Vorgehen keine Metriken gefunden werden konnten, die sich als de-facto Standard durchgesetzt haben, hat das INFOSEC Research Council, das sich aus zahlreichen US-amerikanischen Behörden und Partnern in Kanada und Europa zusammensetzt, im Jahr 2005 den Themenbereich *Enterprise-level Security Metrics* in seine *Hard Problems List* [IHPL05] aufgenommen. Da allerdings auch die intensivere wissenschaftliche Auseinandersetzung mit so genannten Sicherheitsmetriken in den Folgejahren nur wenige konkrete Resultate geliefert hat, hat das NIST in seinen *Directions in Security Metrics Research* 2009 zusammengetragen, welche Meilensteine im Hinblick auf

eine bessere Messbarkeit von Sicherheitseigenschaften erreicht werden müssen [Jan09]. Dabei werden insbesondere praktisch effizient anwendbare Messmethoden und intrinsisch messbare Sicherheitskomponenten gefordert, worauf in diesem Abschnitt spezifisch für Security-Frameworks eingegangen wird.

Die Aussagekraft jeder einzelnen IT-Sicherheitskennzahl ist allerdings meist sehr beschränkt; in der Regel müssen mehrere zusammenhängende Kennzahlen bzw. Messergebnisse analysiert werden, um daraus Schlüsse ziehen zu können. Unter Sicherheitsberichten (engl. *security reports*) werden Dokumente verstanden, die mehrere IT-Sicherheitskennzahlen – in geeigneter Form aufbereitet – enthalten, dadurch den zu einem definierten Zeitpunkt aktuellen Stand wiedergeben und eine Interpretation der Angaben sowie eine Gegenüberstellungen mit früheren Berichten erlauben. Sicherheitsberichte können sich bezüglich ihres Umfangs und Inhalts sowie der Darstellungsform der einzelnen Ergebnisse je nach Zielgruppe unterscheiden; die Ausprägungsform muss dem jeweiligen Bedarf angepasst werden, der hier ebenfalls näher untersucht wird.

In Abschnitt 6.6.1 werden zunächst auf Basis einer Literaturrecherche die mit dem Einsatz von IT-Sicherheitskennzahlen verbundenen Ziele und Herausforderungen zusammengestellt und anschließend in den Kontext von Security-Frameworks eingeordnet. Darauf aufbauend wird in Abschnitt 6.6.2 konzipiert, wie das Messen IT-sicherheitsspezifischer Kennzahlen von Security-Frameworks und deren Auswertung in Anlehnung an das von ISO/IEC 27004 spezifizierte *Measurement Programme* in einer prozessorientierten Form durchgeführt werden kann, die wiederum auf eine kontinuierliche Verbesserung im Laufe des praktischen Einsatzes abzielt.

Die im Rahmen dieser Arbeit konzipierten Methoden zur Spezifikation, Kategorisierung und Dokumentation der entsprechenden Messverfahren und Kennzahlen für Security-Frameworks sind Gegenstand von Abschnitt 6.6.3. In Abschnitt 6.6.4 werden schließlich die Aufbereitung der Kennzahlen zu Berichten und die Auswertung dieser Berichte durch verschiedene Zielgruppen spezifiziert; als Anwendungsbeispiel wird das bekannte Sicherheitsinvestitionsmodell von Gordon und Loeb herangezogen, dessen Übertragbarkeit auf Security-Frameworks gezeigt wird.

6.6.1. Zielsetzung und Herausforderungen beim Einsatz von IT-Sicherheitskennzahlen

IT-Sicherheitskennzahlen und ihre Zusammenstellung zu Sicherheitsberichten dienen allgemein betrachtet den folgenden Zielen:

- *Festhalten und fachliches Beurteilen des Status Quo*: Kennzahlen und Berichte unterstützen die grundlegende Aufgabe des Sicherheitsmanagements, den aktuell erreichten Stand der IT-Sicherheit zu dokumentieren und zu interpretieren. Ein Gegenüberstellen der jeweiligen Werte derselben Kennzahlen, die zu verschiedenen Zeitpunkten ermittelt wurden, ermöglicht einerseits Trendanalysen, die dem Ableiten proaktiver Verbesserungsmaßnahmen dienen, und andererseits die Beurteilung der Auswirkungen sicherheitsrelevanter Ereignisse, beispielsweise der Einführung neuer Sicherheitsmechanismen: Ohne objektive Messungen könnte der Erfolg entsprechender Maßnahmen nicht präzise beurteilt werden.
- *Propagieren IT-sicherheitstechnischer Informationen*: Über Sicherheitsberichte werden die entsprechenden Informationen auch an relevante Dritte weitergegeben. Dies kann

neben dem allgemeinen Berichtswesen und der Eskalation sicherheitsbezogener Vorfälle u. a. auch dazu dienen, Kunden über den Grad des Erreichens der in SLAs vereinbarten Dienstgüte zu informieren oder organisationsintern das IT-Sicherheitsbudget zu rechtfertigen. Ausgewählte Kennzahlen und Berichte dienen auch als Eingabeparameter für andere Prozesse; beispielsweise kann das Risikomanagement die Einschätzungen von Eintrittswahrscheinlichkeiten und Auswirkungen von Schadereignissen auf Basis entsprechender Berichte korrigieren, das Policy Management auf wiederholt erkennbare Verstöße gegen Richtlinien reagieren und das Knowledge Management die diesbezüglich gesammelten Betriebserfahrungen dokumentieren.

- *Bereitstellen IT-sicherheitstechnischer Informationen*: Komplementär zum aktiven Propagieren müssen IT-Sicherheitskennzahlen auch als Kontrollmöglichkeit im Rahmen der IT-Compliance bereitgestellt werden; neben dem Nachweis, dass relevante externe Vorgaben eingehalten werden, ist die Prüfung des Kosten-/Nutzenverhältnisses eine zentrale Aufgabe.

Betrachtet man den Zeitpunkt, an dem sie ausgewertet werden, dienen Kennzahlen somit entweder als Grundlage für strategische Entscheidungen, die zu nachfolgenden Änderungen an der Umgebung führen, als Beitrag zur Qualitätskontrolle und -sicherung nach solchen Änderungen oder der Übersicht zu Stichtagen, z. B. im Kontext eines Audits (vgl. [Jan09]). Die Gesamtheit aller Kennzahlen stellt als pragmatisches Hilfsmittel eine Annäherung an die Bestimmung des Gesamtsicherheitsniveaus dar, das praktisch nicht direkt gemessen werden kann (vgl. [Bohm10]).

Zwei grundlegende Probleme zeigen sich symptomatisch bei der Vorgehensweise zur Beurteilung von Sicherheitseigenschaften und der unscharfen Verwendung von Begriffen wie Messungen und Metriken im Kontext der IT-Sicherheit: Zum einen sind viele IT-sicherheitsspezifische Eigenschaften wesentlich einfacher qualitativ zu beurteilen als quantitativ zu erfassen; mit einer qualitativen Beurteilung sind jedoch gerade im Umfeld der IT-Sicherheit häufig subjektive Schwankungen verbunden [Wan05]. Zum anderen wird der in der Literatur oft vorzufindende Begriff Sicherheitsmetriken (engl. *security metrics*) bislang häufig unpräzise verwendet. Unter Bezug auf die Definition einer Metrik m als Abbildung $m : X \times X \to \mathbb{R}$ mit $x, y, z \in X$ und den vier Bedingungen

1. $m(x, x) = 0$, d. h. jeder Punkt hat zu sich selbst den Abstand 0,
2. $m(x, y) = 0 \Rightarrow x = y$, d. h. Punkte mit Abstand 0 sind identisch,
3. $m(x, y) = m(y, x)$ (Symmetrie) und
4. $m(x, z) \leq m(x, y) + m(y, z)$,

fällt auf, dass viele in der Praxis verwendete „Sicherheitsmetriken“ die Dreiecksungleichung (4.) nicht erfüllen. Vor diesem Hintergrund werden unter dem Begriff Sicherheitsmetriken überwiegend empirische Funktionen, auf deren Zielmenge die Identität sowie eine Größer- oder Kleinerrelation definiert sind, betrachtet [KMY10]. Diesen Status Quo vergleicht Jansen in [Jan09] treffend mit dem früheren Stand in der Entwicklung der Physik, in dem zwar bei Paaren von Gegenständen entschieden werden konnte, welcher davon wärmer bzw. kälter war, aber noch keine Metriken für die Temperatur definiert worden sind. Nach [Jan09] und [Hen02] sollte deshalb statt *Sicherheitsmetriken* besser der Ausdruck *Quantifizierung und Ordnung von Sicherheitsattributen* verwendet werden; insbesondere in der englischen Literatur hat sich der

Begriff *security metrics* jedoch schon durchgesetzt. In dieser Arbeit wird bevorzugt der Begriff *IT-Sicherheitskennzahl* verwendet, um zu verdeutlichen, dass es sich um Zahlenwerte handelt, denen Vorschriften zur quantitativen Messung zugrunde liegen und die mit Maßeinheiten versehen werden können – beispielsweise *Angriffe pro Stunde* oder *Euro*.

Allerdings ist auch die Gewinnung und Auswertung von gegenüber Metriken vereinfachten, sicherheitsspezifischen Kennzahlen mit mehreren Herausforderungen verbunden: Messwerte sind nur begrenzt gültig, da sich beispielsweise Angriffe weiterentwickeln und bislang unbekannte Schwachstellen entdeckt werden können – ein momentan als sicher eingestuftes System kann im nächsten Augenblick als unsicher gelten (vgl. [Wan05]). Durch die laufende Verbesserung der Sicherheitsmechanismen ist im Gegenzug zu beachten, dass sich Sicherheitsberichte eventuell nicht mehr auf den aktuellen Stand der Infrastruktur beziehen, sondern inzwischen z. B. schon Softwareaktualisierung eingespielt wurden (vgl. [Jan09]). Nach [PC10] muss darüber hinaus einerseits berücksichtigt werden, dass sich viele sicherheitsspezifischen Attribute gegenseitig beeinflussen, und andererseits, dass Angreifer die Umgebung auch dahingehend beeinflussen können, dass manipulierte Messwerte geliefert werden.

Dadurch, dass Messungen auf technischer Ebene in der Granularität einzelner Sicherheitsattribute (vgl. Attribute im Informationsmodell in Abschnitt 6.4.3) durchgeführt werden müssen, ergeben sich für Security-Frameworks zwei grundsätzliche Anforderungen bezüglich der Unterstützung von IT-Sicherheitskennzahlen: Zum einen muss eine entsprechend große Menge einzelner Kennzahlen definiert werden, die eine Vielzahl praktisch relevanter Sicherheitsaspekte über alle Frameworkkomponenten hinweg adäquat abdeckt. Dabei muss auch berücksichtigt werden, dass pro Frameworkkomponente bzw. Modul unterschiedliche Realisierungsvarianten zur Auswahl stehen können, die diese Kennzahlen messbar machen müssen. Zum anderen muss vorgegeben werden, wie Kennzahlen aggregiert und zusammengefasst werden können, um Indikatoren auf höherem Abstraktionsgrad zu erhalten, die Aufschluss über das durch das gesamte Security-Framework erreichte Sicherheitsniveau geben, so dass nicht lediglich alle Frameworkkomponenten voneinander isoliert betrachtet werden. Mindestens für diese Kennzahlen ist mittelfristig eine Vereinheitlichung anzustreben, um objektive Vergleiche zwischen der Leistungsfähigkeit von Security-Frameworks zu ermöglichen und die Managementschnittstellen weiter zu vereinheitlichen. Abbildung 6.36 stellt dar, dass Security-Frameworks IT-Sicherheitskennzahlen sowohl in der Breite als auch in der Tiefe definieren müssen: Durch seinen modularen Aufbau besteht jede Frameworkinstanz i. A. aus mehreren Security-Framework-Komponenten (SFK1–SFK7), die ihrerseits technischen Komponenten bzw. Ressourcen entsprechen. Die Sicherheitseigenschaften jeder Ressource müssen quantifiziert werden können, wobei direkte Messungen der Ressourcen i. A. zunächst in techniknahen Kennzahlen (K1–Kd) resultieren. Durch die – oftmals auch komponentenübergreifende – Kombination dieser Kennzahlen lassen sich abgeleitete Kennzahlen mit einem entsprechend höheren Abstraktionsniveau spezifizieren (AK1–AK10). Im Idealfall liefert bereits das Frameworkkonzept Kennzahlen auf verschiedenen Abstraktionsebenen.

Das Durchführen der entsprechenden Messungen und die Auswertung der ermittelten Kennzahlen folgen dabei einem periodisch oder bedarfsorientiert instanziierten Prozess, der im nächsten Abschnitt beschrieben wird.

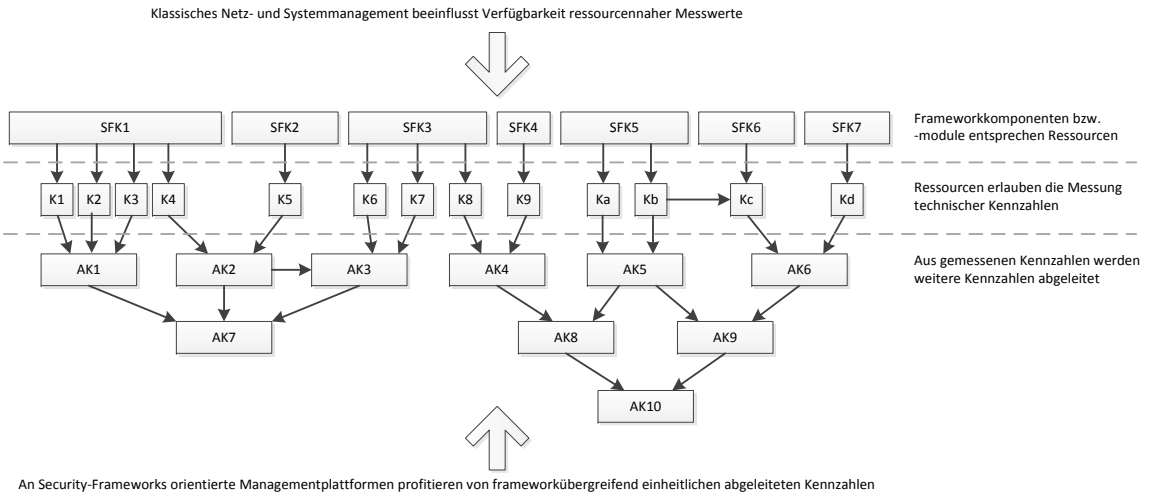


Abbildung 6.36.: Flächendeckende Erfassung von IT-Sicherheitskennzahlen bei Security-Frameworks

6.6.2. Prozessorientiertes Messen, Auswerten und Berichten

Bei der Festlegung, welche Kennzahlen ermittelt und berichtet werden sollen, muss im Allgemeinen ein Kompromiss aus Top-down- und Bottom-up-Vorgehensweise gefunden werden: Aus einer strikten Top-down-Orientierung resultieren, wie eingangs in Abschnitt 6.6 exemplifiziert, beim aktuellen Stand der Technik oftmals Fragestellungen, die mit den verfügbaren Messmethoden nicht ausreichend beantwortet werden können, da eine Zerlegung in einzelne ressourcennahe Messwerte nicht praktikabel ist. Neben konzeptionell unklaren Messverfahren kann die Messbarkeit beispielsweise auch eingeschränkt sein, falls jeder Messvorgang unverhältnismäßig aufwendig bzw. die Implementierung des Messverfahrens zu teuer ist oder falls bestimmte Messgrößen aufgrund vertraglicher oder gesetzlicher Auflagen (z. B. Datenschutz) in einem Szenario nicht erfasst werden dürfen. Wird hingegen bottom-up-orientiert zunächst nur eruiert, welche Messwerte ohne nennenswerten Aufwand geliefert werden könnten, so bleiben die IT-Sicherheitskennzahlen sehr system- und ressourcennah, ohne zielgerichtet festlegen zu können, welche Auswertungen auf höherem Abstraktionsniveau sinnvoll und notwendig für die Beurteilung des Gesamtsicherheitsniveaus sind.

In der Literatur und Praxis hat sich deshalb ein hypothesenbasiertes Vorgehen durchgesetzt, bei dem zunächst eine Reihe von zu verifizierenden bzw. falsifizierenden Annahmen auf mittlerem Abstraktionsgrad formuliert werden, beispielsweise: „*Security-Framework S reduziert die Eintrittswahrscheinlichkeit des Risikos R um mindestens 20%*“. Dabei findet häufig eine explizite Orientierung an bekannten Risiken oder Angreifermodellen statt (vgl. [And07] und [Lan06b]). Von den so formulierten Hypothesen ausgehend müssen anschließend zunächst *konkretisierend* durch Dekomposition

- optional mehrere Subhypothesen definiert werden, die der Diagnose des zu untersuchenden Sachverhalts dienen und nach Möglichkeit bereits eine Zuordnung zu einzelnen Systemen bzw. Komponenten ermöglichen, beispielsweise:

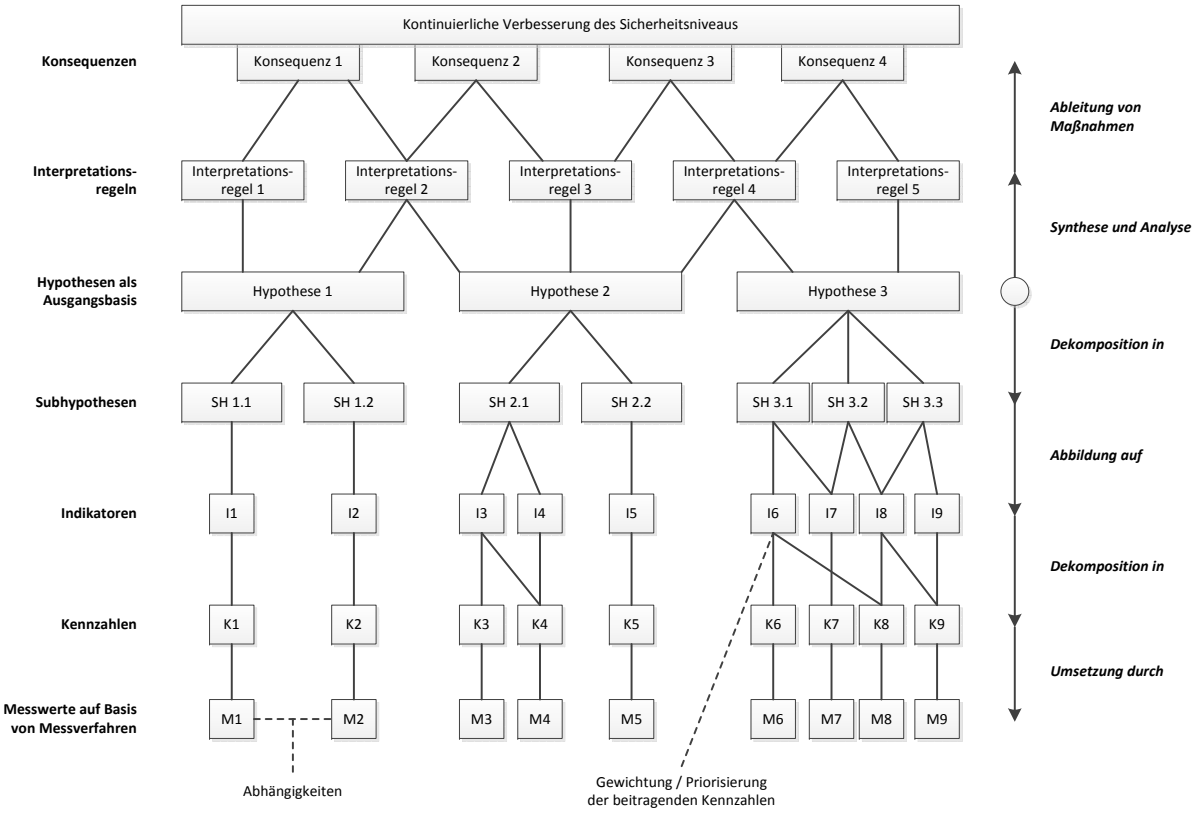


Abbildung 6.37.: Hypothesen als Ausgangsbasis für die Erfassung und Verarbeitung von IT-Sicherheitskennzahlen

  - „*Die Anzahl der im Incident-Management-System erfassten Vorfälle, die auf das Risiko R zurückgehen, fällt um mindestens 20%.*“
  - „*Die Frameworkkomponenten S_1 und S_2 registrieren alle und verhindern mindestens 20% der dem Risiko R zugrundeliegenden Schadereignisse.*“
- durch Messverfahren ermittelbare Indikatoren und Kennzahlen definiert werden, die diese (Sub-) Hypothesen objektiv bestätigen oder widerlegen können, beispielsweise indem die Anzahl entsprechender Datensätze gezählt oder die entsprechenden MO-Attribute ausgelesen werden.

Dabei müssen funktionale Abhängigkeiten zwischen den Messwerten berücksichtigt und Auswertungsregeln unter Anwendung von Gewichten bzw. Priorisierungen formuliert werden (vgl. [WW97] und [CK09]). Komplementär dazu muss *abstrahierend* spezifiziert werden, welche Schlüsse aus der Bestätigung oder Falsifikation einzelner Hypothesen zu ziehen sind, beispielsweise indem diese Ergebnisse in Relation zu den Ergebnissen anderer Hypothesenprüfungen gesetzt werden (vgl. Abbildung 6.37).

Motiviert durch die Vielzahl an Hypothesen, Subhypothesen und Kennzahlen, die zur Beurteilung des Gesamtsicherheitsniveaus herangezogen werden müssen, werden entsprechende Managementwerkzeuge zur Verwaltung benötigt (vgl. Kapitel 7) und ein Prozess erforderlich,

der sicherstellt, dass die jeweiligen Messwerte in der erforderlichen Regelmäßigkeit ermittelt und den definierten Auswertungsverfahren unterzogen werden. In Anlehnung an [ME01], [And07] und ISO/IEC 27004 [I27004] dient der als *Measurement Programme* bezeichnete Prozess folgenden Zielen:

- Es wird festgelegt, welche Arten von **Kennzahlen** zu betrachten sind und welche logische Abfolge von Operationen notwendig ist, um die jeweils konkreten Messwerte zu ermitteln. Typischerweise werden wie in ISO/IEC 27004 folgende Kennzahltypen unterschieden:
  - Basiskennzahlen (engl. *Base Measures*) sind unabhängig von anderen Kennzahlen und entsprechen im Allgemeinen direkt messbaren Werten, beispielsweise MO-Attributen, die optional skaliert werden müssen.
  - Abgeleitete Kennzahlen (engl. *Derived Measures*) ergeben sich aus Funktionen, deren Eingabe mindestens zwei Basiskennzahlen oder andere abgeleitete Kennzahlen umfasst.
  - Indikatoren (engl. *Indicators*) sind Kennzahlen, die als Belege für das Erfüllen bzw. Nichterfüllen einer Hypothese verwendet werden können. Indikatoren können nicht nur aus aktuellen Basiskennzahlen bzw. abgeleiteten Kennzahlen gewonnen werden, sondern auch aus der Gegenüberstellung mit zu früheren Zeitpunkten ermittelten Kennzahlen. Ausgewählte Indikatoren können wie bereits diskutiert als so genannte Schlüsselindikatoren (engl. *Key Performance Indicators*) z. B. in SLAs verwendet werden.

  Die Spezifikation einzelner Kennzahlen wird in Abschnitt 6.6.3 vertieft.
- Die **Verarbeitungskette** von der Erfassung einzelner Messwerte über deren Aggregation und Aufbereitung bis hin zur Auswertung entsprechender Sicherheitsberichte wird festgelegt und analog zu den anderen in diesem Kapitel diskutierten Prozessen u. a. mit der Definition von Rollen, Verantwortlichkeiten, Aufgaben und Eskalationswegen untermauert. Zudem werden die Schnittstellen zu anderen Prozessen, beispielsweise zum Risikomanagement und zu Genehmigungsprozessen, dokumentiert. Die Auswertung und Interpretation von Kennzahlen sowie das Ableiten von Verbesserungsmaßnahmen sind Gegenstand von Abschnitt 6.6.4.
- Analog zum gesamten Sicherheitsmanagementprozess wird über Leitlinien, die Einführung von standardisierten Vorgehensweisen, Schulungen und den Einbezug der Unternehmensleitung sichergestellt, dass brauchbare **Randbedingungen** geschaffen werden, um das Sicherheitsberichtswesen zuverlässig durchzuführen und die von ihm erarbeiteten Ergebnisse und Vorschläge geeignet umzusetzen.

Auch dieser Prozess muss einer **kontinuierlichen Verbesserung** unterliegen, so dass aufgrund von Änderungen an den Anforderungen oder der Infrastruktur neu benötigte Kennzahlen berücksichtigt, nicht mehr benötigte Messverfahren außer Betrieb genommen und identifizierte Schwierigkeiten in der gesamten Verarbeitungskette behoben werden können.

Security-Frameworks bringen sich in den gesamten Prozess insbesondere dadurch ein, dass sie die von ihren Komponenten bereitgestellten Messwerte und dafür anzuwendenden Messverfahren dokumentieren; im Idealfall definieren sie auch Metriken bzw. Kennzahlen auf höherem Abstraktionsgrad, die am Bedarf verschiedener Zielgruppen von Sicherheitsberichten

orientiert sind, und geben vor, wie auf Abweichungen vom Soll-Zustand zu reagieren ist. Die frameworkspezifischen Kennzahlen sind dabei nicht nur auf die Frameworkkomponenten abgestimmt, sondern ermöglichen auch die Beurteilung der Sicherheitseigenschaften der vom Security-Framework geschützten Assets.

6.6.3. Spezifikation, Kategorisierung und Dokumentation von IT-Sicherheitskennzahlen

Die bisherigen Ausführungen haben dargelegt, dass die Definition aussagekräftiger IT-Sicherheitskennzahlen eine durchaus schwierige Aufgabe ist. In diesem Abschnitt wird untersucht, welche Anforderungen IT-Sicherheitskennzahlen erfüllen sollten, wie sie zur Unterstützung ihres Managements strukturiert und gruppiert bzw. kategorisiert werden können und in welcher Form sie dokumentiert werden sollten, um alle Phasen des oben beschriebenen Measurement-Prozesses zu unterstützen.

An IT-Sicherheitskennzahlen bzw. die Messvorgänge zu ihrer Ermittlung können die folgenden Qualitätsansprüche gestellt werden, die aus [And07], [Pay07] und [Jan09] zusammengetragen wurden:

- Die Ermittlung der IT-Sicherheitskennzahl muss **einfach und kostengünstig** erfolgen können. Mögliche Datenquellen sind u. a. dedizierte Messwerkzeuge, Infrastruktur- bzw. Security-Framework-Komponenten, Managementsysteme, ITSM-Artefakte wie Incident Records und die manuelle Erfassung. Aufgrund der Vielzahl möglicher Basiskennzahlen muss bei der Implementierung im Allgemeinen ausgewählt und priorisiert werden; beispielsweise können Basiskennzahlen, die in mehrere abgeleitete Kennzahlen und Indikatoren einfließen, höher priorisiert werden.
- Die Messung der IT-Sicherheitskennzahl muss **wiederholbar** sein und **reproduzierbare Ergebnisse** liefern (engl. *repeatable* und *reproducible measures*). Zwei unabhängig voneinander durchgeführte Messungen desselben Zustands eines Messobjekts müssen also dasselbe Ergebnis liefern, auch wenn die Messung von verschiedenen Personen durchgeführt wird.
- Die Bestimmung der IT-Sicherheitskennzahl muss **objektiv** erfolgen, darf also beispielsweise nicht von der subjektiven Meinung eines Befragten abhängen. Zudem muss in Erwägung gezogen werden, Schutzmaßnahmen gegen absichtliche Manipulationen im Rahmen des Messverfahrens vorzusehen.
- Die IT-Sicherheitskennzahl muss **spezifisch und aussagekräftig** für mindestens eine der untersuchten Hypothesen sein. Ein Erfassen und Berichten beliebiger anderer verfügbarer Kennzahlen wäre nicht zielführend.
- Eventuell vorhandene **Messungenauigkeiten** müssen bekannt sein und berücksichtigt werden. Ebenso sollten **Verifikations- und Validierungsverfahren** festgelegt werden, um Messfehler erkennen zu können.
- Die Messergebnisse müssen zeitabhängig, dürfen also **nicht konstant** sein. Dabei sollte das Messverfahren eine möglichst **geringe Latenz** aufweisen, um zeitnah auf Abweichungen vom Soll-Bereich reagieren zu können.
- Eine IT-Sicherheitskennzahl, die als Indikator fungiert, also im Rahmen des Berichtswesens an Dritte übermittelt wird, sollte **organisationsweit verständlich** und auch

organisationsübergreifend konsistent anwendbar sein. Hilfreich ist dabei, wenn mindestens eine Maßeinheit zum Einsatz kommt, die einfach auf Zeitangaben oder Geldwerte abgebildet werden kann [And07].

Insgesamt sind also wenige, sorgfältig konzipierte IT-Sicherheitskennzahlen einer unkoordinierten Auswertung möglichst vieler beliebiger Messwerte vorzuziehen. Bei einem Basissatz an Kennzahlen, wie er auch in den Konzepten von Security-Frameworks zu definieren ist, sollte zudem auf eine ausgewogene Abdeckung verschiedener Arten von Kennzahlen geachtet werden. Auf Basis einer Literaturrecherche, die aktuelle Arbeiten zu *Security Metrics* umfasst, die Beispielkennzahlen enthalten, lässt sich folgende Kategorisierung vornehmen (vgl. [Ber08], [Hin08], [fIS09] und Anhang B von ISO/IEC 27004):

- Grundlegend ist zwischen **technischen** und **prozessualen** Kennzahlen zu unterscheiden. Technische Basiskennzahlen werden im Allgemeinen von mit Monitoringsystemen vergleichbaren Messwerkzeugen ermittelt, d. h. sie lesen einzelne sicherheitsrelevante Attribute technischer Systeme aus. Prozessuale Kennzahlen dienen der Bewertung von Prozessen wie dem Security Incident Management oder dem Risikomanagement; ihre Basiskennzahlen gehen überwiegend aus den von Prozessrahmenwerken geforderten Verlaufsdokumentationen (*records*) hervor, beispielsweise aus Datenfeldern von Incident Records.
- Über die Dauer eines Messvorgangs für Basiskennzahlen hinausgehend ist das **Timing** von Indikatoren zu berücksichtigen: Sie können entweder zur Frühwarnung eingesetzt werden (engl. *leading indicators*), Aufschlüsse über den Sicherheitszustand genau zum Zeitpunkt der Messung geben (engl. *coincident indicators*) oder die Entwicklungen mit einer zeitlichen Verzögerung widerspiegeln (engl. *lagging indicators*). Die Ausprägung dieses Charakteristikums muss bei der Planung von Kompensationsmaßnahmen und der Erwartungshaltung bezüglich dadurch zeitnah veränderter Kennzahlen berücksichtigt werden.
- Es ist zu unterscheiden, ob eine Kennzahl **system- bzw. servicespezifisch** ist, sich also beispielsweise auf genau einen Dienst bzw. ein zu seinem Erbringen unmittelbar relevantes Asset oder auf eine dedizierte Schutzkomponente abstützt, oder ob sie sich auf **systemübergreifende Sicherheitsbereiche** (die durch so genannte *perimeter defenses* vorgegeben werden) bezieht.
- Schließlich kann anhand der **Hypothesenzielsetzung** differenziert werden, ob beispielsweise die Verfügbarkeit bzw. Zuverlässigkeit oder der Abdeckungsgrad bestimmter Maßnahmen oder Policies geprüft werden soll.

Sowohl zur Verwaltung als auch zur Implementierung ihrer Messverfahren, Weiterverarbeitung und Aggregation zu Sicherheitsberichten müssen die konzipierten Kennzahlen dokumentiert werden. Hierfür existiert bislang kein standardisiertes oder weit verbreitetes Format, da auch ISO/IEC 27004 in seinem nicht normativen Anhang A lediglich unverbindliche Empfehlungen ausspricht. Abgeleitet von [I27004], [And07], [Ert08] und [Hub10] wurde unter Ergänzung einiger Attribute im Rahmen dieser Arbeit die folgende Struktur zur Dokumentation von IT-Sicherheitskennzahlen konzipiert, die auch als Basis für die Dokumentation im Rahmen von Security-Frameworks genutzt werden sollte (vgl. Abbildung 6.38):

- Ein szenarienweit eindeutiger *Identifikator* dient als Schlüsselattribut; es kann sich um einen inkrementellen Zahlenwert oder eine einprägsame Kurzbezeichnung handeln.

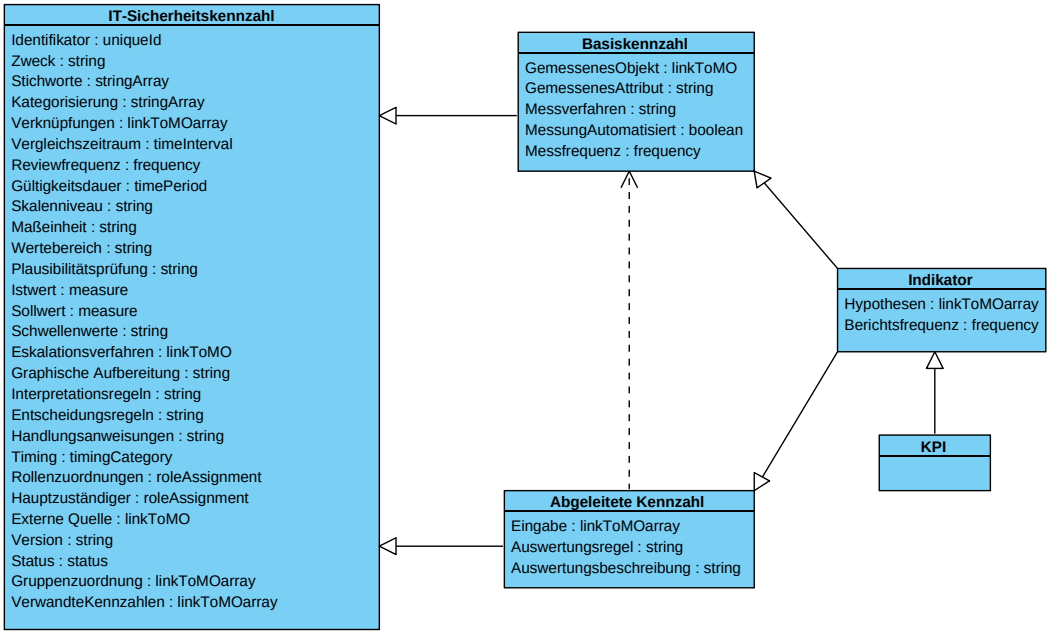


Abbildung 6.38.: Modellierung von IT-Sicherheitskennzahlen

- Der mit der Kennzahl verfolgte *Zweck* wird in natürlicher Sprache festgehalten.
- Über mehrere optionale, frei wählbare *Stichworte* können Vorschläge dokumentiert werden, für welche Arten von Systemen oder Berichten die Kennzahl sinnvoll verwendet werden kann; dabei wird das pragmatische Ziel verfolgt, eine einfache Suche nach passenden Kennzahlen z. B. für neue Berichte zu unterstützen, ohne Anspruch auf Vollständigkeit zu erheben.
- Über eine *Kategorisierung* wird die Kennzahl mindestens einer der oben diskutierten Kategorien zugeordnet.
- Mittels *Verknüpfungen* wird die Kennzahl optional weiteren verwalteten Objekten zugeordnet, beispielsweise Sicherheitsmaßnahmen, technischen Komponenten, Prozessen, Angreifermodellen oder Risiken.
- Bei Basiskennzahlen wird das *Messverfahren* spezifiziert, indem das zu messende *Objekt* und dessen für die Basiskennzahl relevantes *Attribut* benannt werden; die Durchführung eines *Messvorgangs* ist in natürlicher Sprache zu beschreiben, wobei auch angegeben werden sollte, wodurch das Messergebnis eventuell verfälscht werden kann. Zudem ist festzuhalten, ob die Messung *automatisiert* oder manuell erfolgt.
- Bei abgeleiteten Kennzahlen werden die als *Eingabe* verwendeten anderen Kennzahlen spezifiziert und eine *Auswertungsregel* angegeben, für deren Formulierung z. B. eine kennzahlenübergreifend einheitlich verwendete Programmiersprache angewandt werden kann, wobei auch die Möglichkeit einer Kommentierung bzw. natürlichsprachlichen *Beschreibung* genutzt werden sollte.
- Für Indikatoren sind Querverweise auf die *Hypothesen*, zu deren Verifikation oder Falsifikation sie beitragen sollen, zu speichern. Ein Indikator ist gleichzeitig eine Basiskennzahl

oder eine abgeleitete Kennzahl.

- Bei allen Kennzahlen sollte eine *Designbegründung* hinterlegt werden, die über die Beschreibung des Zwecks sowie der Mess- bzw. Auswertungsverfahren hinausgehend dokumentiert, warum die Kennzahl genau so gewählt wurde bzw. welche Alternativen denkbar wären, aber zurückgestellt wurden.
- Für jede Kennzahl sind *Frequenzen* und *Gültigkeitsbereiche* festzulegen:
  - Die *Messfrequenz* gibt bei Basiskennzahlen an, wie häufig die definierten Messvorgänge durchgeführt werden. Analog dazu gibt die *Auswertungsfrequenz* bei abgeleiteten Kennzahlen an, in welchen Abständen die Auswertungsregeln durchlaufen werden.
  - Die *Berichtsfrequenz* entspricht bei Indikatoren einer Empfehlung, wie oft über die Kennzahl berichtet werden soll; beispielsweise kann die Messfrequenz einer für monatliche Berichte konzipierten Kennzahl wesentlich höher sein als die Berichtsfrequenz, um Messausfälle durch vorübergehende Nichtverfügbarkeit von Ressourcen zu vermeiden.
  - Über die optionale Definition eines *Vergleichszeitraums* kann beispielsweise empfohlen werden, dass der aktuelle Wert einer Kennzahl mit dem vor einem Monat, aber nicht mit dem vor mehreren Jahren ermittelten verglichen wird.
  - Die *Reviewfrequenz* legt fest, in welchen Maximalabständen die Spezifikation der Kennzahl einer Analyse und ggf. Überarbeitung unterzogen werden muss.
  - Die *Gültigkeitsdauer* gibt optional vor, zu welchem Termin die Nutzung der Kennzahl begonnen bzw. eingestellt werden soll, beispielsweise weil die gemessenen Objekte noch nicht implementiert sind bzw. wieder außer Betrieb genommen werden.
- Für alle Kennzahlen sind die *Skalenniveaus* und *Maßeinheiten* anzugeben; sie geben Aufschluss über die mögliche Weiterverarbeitung:
  - Basiskennzahlen und unmittelbar daraus abgeleitete Kennzahlen sollten nach Möglichkeit auf einer Kardinalskala basieren, um Zustandsunterschiede exakt quantifizieren zu können. Ordinalskalen werden primär bei manuell zu ermittelnden Kennzahlen, beispielsweise im Rahmen des CVSS2-Verfahrens, eingesetzt (vgl. Abschnitt 6.3.2.3). Nominalskalen sind aufgrund der mit ihnen verbundenen eingeschränkten Aussagekraft im Allgemeinen nur für als Indikatoren verwendete Kennzahlen sinnvoll, bei denen eine automatische Reaktion auf Abweichungen vom Sollwert erfolgt.
  - Die Maßeinheiten der Basiskennzahlen ergeben sich unmittelbar aus der Einheit der Messgröße. Bei Indikatoren, die im Rahmen von Sicherheitsberichten an Dritte kommuniziert werden, ist eine Überführung in für diese gut verständliche Maßeinheiten anzustreben; beispielsweise lassen sich auf Basis der Anzahl von Sicherheitsvorfällen pro Monat unter Berücksichtigung der durchschnittlichen Bearbeitungsdauer und Gehälter die mit den Sicherheitsvorfällen verbundenen Personalkosten in Euro ausdrücken.
- Die automatische Überprüfung, Überwachung und Weiterverarbeitung wird durch eine Reihe zusätzlicher Angaben pro Kennzahl unterstützt:

  - Auf Basis der Spezifikation des möglichen bzw. erwarteten *Wertebereichs* bei Kardinalskalen bzw. der Wertemenge können optional genauer beschriebene *Plausibilitätsprüfungen* implementiert werden, anhand derer größere Messfehler identifiziert werden können.
  - Über die Definition eines *Sollwerts* und optionaler *Schwellenwerte* können Abweichungen des Ist-Zustands vom Soll-Zustand erkannt und beispielsweise *Alarmierungs- oder Eskalationsverfahren* angestoßen werden.

  Diese Angaben können auch bei der graphischen Aufbereitung der Kennzahlen herangezogen werden: Bei der Darstellung der Entwicklung einer Kennzahl über die Zeit in einem kartesischen Koordinatensystem können der Wertebereich zur Einteilung der Ordinatenachse genutzt und die Soll- und Schwellenwerte als Hilfslinien zur intuitiven Interpretation eingezeichnet werden. Weiterführende *Vorschläge zur graphischen Aufbereitung* sollten in natürlicher Sprache spezifiziert werden; beispielsweise können die Verwendung von Balken- oder Tortendiagrammen, der Einsatz unterschiedlicher Farben für verschiedene Wertebereiche und Texte für Legenden angeregt werden, worauf bei der Spezifikation der verschiedenen Berichtsarten zurückgegriffen werden kann.

- Für jede Kennzahl sind *Interpretationsregeln* in natürlicher Sprache zu spezifizieren, durch die verhindert werden soll, dass die Ergebnisse falsch gedeutet werden; beispielsweise muss geregelt werden, wie ein Über- bzw. Unterschreiten des vorgegebenen Sollwerts zu bewerten ist. Bei Indikatoren können zusätzlich *Entscheidungsregeln*, z. B. mit Bezug auf das Erfüllen bzw. Widerlegen von Hypothesen, und zielgruppenspezifische *Handlungsanweisungen* vorgegeben werden, um den subjektiven Ermessensspielraum bzw. mögliche Unklarheiten bei der Auswertung von Sicherheitsberichten zu minimieren. In diesem Kontext ist insbesondere auch die *Timingkategorie* der Kennzahl zu berücksichtigen.
- Darüber hinaus sind pro Kennzahl die folgenden *Metadaten* festzuhalten:
  - Über *Rollenzuweisungen* werden die mit der Kennzahl verbundenen Aufgaben den jeweiligen Personen bzw. Gruppen zugeordnet. Rollen umfassen dabei beispielsweise die für die Messung, die Prüfung bzw. Genehmigung, die Aufbereitung bzw. Visualisierung, die Auswertung und die Weitergabe der Ergebnisse Zuständigen sowie die Zielgruppen von Berichten, für die die jeweilige Kennzahl relevant ist.
  - Neben einem *Hauptzuständigen* für die Kennzahl (Autor bzw. Owner) ist eine ggf. verwendete *externe Quelle* (z. B. Compliance-Vorgabe, SLA, Best-Practice-Dokumentation) festzuhalten.
  - *Versionsinformationen* inklusive des Datums der letzten Überarbeitung und eine *Statusangabe* – beispielsweise „noch nicht implementiert“, „in Benutzung“, „in Überarbeitung“ und „außer Betrieb“ – regeln die Verwendung der Kennzahl in Sicherheitsberichten und unterstützen ihre kontinuierliche Verbesserung.
  - Über die Verknüpfung mit Messobjekten bzw. als Eingabe verwendeten Kennzahlen hinausgehend sind *Zuordnungen zu Gruppen*, beispielsweise aller im Kontext eines Security-Frameworks definierten Kennzahlen, und Verknüpfungen mit *verwandten Kennzahlen*, die beispielsweise neben der aktuell betrachteten Kennzahl ebenfalls in Sicherheitsberichten berücksichtigt werden sollten, vorzunehmen.

Basiskennzahl	
Identifikator	*BK-0001*
Zweck	*Ermittlung der Anzahl automatischer Reparametrisierungen bei Angriffen*
Stichworte	*Security-Framework S, Angriffe, Reparametrisierung*
Kategorisierung	*technisch; dienstspezifisch*
Verknüpfungen	*Security-Framework S*
Vergleichszeitraum	*6 Monate*
Reviewfrequenz	*einmal pro Jahr*
Gültigkeitsdauer	*unbegrenzt*
Skalenniveau	*kardinal*
Maßeinheit	*(Anzahl) Änderungen*
Wertebereich	*positive, ganze Zahlen*
Plausibilitätsprüfung	*Messwert nimmt kontinuierlich zu*
Istwert	---
Sollwert	---
Schwellenwerte	*Differenz zur letzten Messung > 10*
Eskalationsverfahren	*Benachrichtung des Administrators*
Graphische Aufbereitung	*Liniendiagramm des Messwerts im Verlauf der Zeit*
Interpretationsregeln	*Die Kennzahl gibt die Anzahl der automatisch durch…*
Entscheidungsregeln	*Liegt die Anzahl der Reparametrisierungen bei über …*
Handlungsanweisungen	*Rekonfiguration der Schwellenwerte im Security-Fra…*
Timing	*coincident*
Externe Quelle	---
Version	*1.0*
Status	*in Benutzung*
Gruppenzuordnung	*Security-Framework S, ChangeCounterKennzahlen*
VerwandteKennzahlen	*BK-0002; AK-0001; I-0001*
GemessenesObjekt	*Steuerkomponente des Security-Frameworks S*
GemessenesAttribut	*AnzahlAutomatischerReparametrisierungen*
Messverfahren	*Auslesen über Web-Service-API*
MessungAutomatisiert	*Ja*
Messfrequenz	*einmal pro Minute*

Abbildung 6.39.: Beispiel für die Dokumentation einer Basiskennzahl

Abbildung 6.39 veranschaulicht die erarbeitete Struktur am Beispiel einer Basiskennzahl, bei der von einer Schutzkomponente eines Security-Frameworks für Webapplikationen die Anzahl der durch Automatismen bei erkannten Angriffen veranlassten dynamischen Reparametrisierungen ausgelesen wird. Sie kann im Rahmen abgeleiteter Kennzahlen bzw. Indikatoren beispielsweise in Relation zur Anzahl notwendig gewordener manueller Anpassungen gesetzt werden, um den Grad der praktisch erzielten Automatisierung zu bestimmen.

Dadurch, dass die konsequente Spezifikation und Anwendung von IT-Sicherheitskennzahlen generell erst im Entstehen ist, fehlen praktische Erfahrungswerte, die zur Beurteilung der Praxisrelevanz einzelner oder Gruppen von Kennzahlen herangezogen werden können. Der hier vorgestellte Ansatz zur Abdeckung der durch Security-Frameworks induzierten Gruppen von zusammenhängenden Sicherheitsmechanismen und -maßnahmen mit Kennzahlen in der Breite und auf verschiedenen Abstraktionsebenen ist deshalb als komplementär zur Arbeit

von Heyman et al. [HSHJ08] zu betrachten, die *Security Metrics* auf Basis funktionaler Zusammenhänge zu *Security Patterns* zusammenstellt. Beide Ansätze verfolgen die Ziele, den szenarienspezifischen Aufwand, der durch die Konzeption und Implementierung von Kennzahlen entsteht, zu reduzieren und eine system- und dienstübergreifend einheitliche Bewertung zu ermöglichen.

Die Konzepte von Security-Frameworks können über die Vorgabe von IT-Sicherheitskennzahlen hinausgehend weitere Informationen liefern, die zur Interpretation der szenarienspezifischen Messwerte eingesetzt werden können. Beispielsweise können sie Vergleichswerte aus anderen Szenarien enthalten oder typische Verläufe der Entwicklung von Kennzahlen, z. B. vom Zeitpunkt kurz nach der Einführung des Security-Frameworks bis hin zum stabilen Dauerbetrieb, skizzieren.

Die erforderliche Auswertung der ermittelten Kennzahlen erfolgt jedoch, beispielsweise wenn es sich um in SLAs vereinbarte KPIs handelt, häufig durch Personen, die keinen Zugang zu den Mess- und Aggregationswerkzeugen haben bzw. sich damit auseinandersetzen möchten. Stattdessen werden ausgewählte Kennzahlen wie im nächsten Abschritt beschrieben zu Sicherheitsberichten aufbereitet, die zur Information der relevanten Interessenvertreter verwendet werden.

6.6.4. Aufbereitung von IT-Sicherheitskennzahlen zu Berichten und deren Auswertung

Da einzelne IT-Sicherheitskennzahlen eine beschränkte Aussagekraft haben und unterschiedlichen Mess- und Verarbeitungsfrequenzen unterliegen, dienen Sicherheitsberichte der strukturierten Aggregation und Kommunikation thematisch zusammenhängender Kennzahlen zu definierten Zeitpunkten. Im Folgenden werden auf Security-Frameworks basierte Sicherheitsberichte und Datenstrukturen zu ihrer Verwaltung konzipiert; trotz der offensichtlichen Relevanz von Sicherheitsberichten existieren hierfür keine produktunabhängigen, sicherheitsspezifischen Vorarbeiten, die über die Visualisierung einzelner Kennzahlen hinausgehen; aus diesem Grund findet eine grobe Orientierung an Werkzeugen für das SLA-Reporting statt, für das bereits ausgereiftere Konzepte existieren.

Die Auswertung von Sicherheitsberichten beeinflusst unter anderem Entscheidungen über zukünftige Sicherheitsinvestitionen. Als Beispiel für die Anwendbarkeit diesbezüglich existierender Konzepte auf Security-Frameworks wird abschließend das bekannte Gordon-Loeb-Modell diskutiert.

Ausschlaggebend für die Ausprägung der Charakteristika eines Sicherheitsberichts ist seine *Zielgruppe*; diese entscheidet über

- den *Inhalt* und damit auch den Umfang und technischen Tiefgang der Berichte.
- das *Format*, in dem der Bericht vorzulegen ist. Dabei ist grundsätzlich zu unterscheiden, ob der Sicherheitsbericht maschinell weiterverarbeitet werden soll oder beispielsweise mit Diagrammen für Leser aufbereitet werden soll.
- die *Frequenz*, mit der der Sicherheitsbericht zu erstellen und zu kommunizieren ist, beispielsweise monatlich, quartalsweise oder jährlich.

- die *Kommunikationswege*, über die der Bericht zu verteilen ist. Hierzu gehören einerseits beispielsweise die Spezifikation des Ablageortes (Pull-Modell) oder z. B. eines E-Mail-Verteilerkreises (Push-Modell); andererseits muss geregelt werden, ob der Erhalt des Sicherheitsberichts von der Zielgruppe bestätigt bzw. auch sein Inhalt explizit genehmigt werden muss.
- die *Rollenzuweisung*, in der analog zur Spezifikation einzelner Kennzahlen festgehalten werden muss, wer die eigentlichen Zielgruppen, die optionalen Gutachter bzw. Genehmigungsverantwortlichen, die Eigentümer (Owner), die Ersteller und die für die Bereitstellung Verantwortlichen des Sicherheitsberichts sind.

Bezügliche der Formate, in denen Sicherheitsberichte erstellt werden können, ist festzuhalten, dass bislang keine Standardisierungsbemühungen für maschinenverarbeitbare Formate unternommen wurden. Die Anwendung gängiger statistischer Verfahren auf und die graphische Aufbereitung von einzelnen IT-Sicherheitskennzahlen mit unterschiedlichen Diagrammtypen werden ausführlich in [And07] diskutiert und hier deshalb nicht näher betrachtet. Auch für die inhaltliche Strukturierung von IT-Sicherheitsberichten, deren Zielgruppe Personen und nicht IT-Systeme sind, existieren bislang keine Konzepte und Best Practices, die sich organisationsübergreifend durchgesetzt haben. Da Security-Frameworks die Möglichkeit schaffen, zueinander komplementäre, dienstspezifische Kennzahlen zu ermitteln, kann von den bislang in der Praxis häufig zu beobachtenden, an Monitoringsystemen orientierten Darstellungen, bei denen lediglich zu einzelnen Systemen die entsprechenden Messwerte aufgeführt werden, abgekommen werden. Stattdessen bietet sich eine iterativ verfeinernde Strukturierung von Sicherheitsberichten an:

- Zunächst informiert der Sicherheitsbericht über das Gesamtsicherheitsniveau, indem die Hypothesen und Indikatoren herangezogen werden, die einen dienstübergreifenden Abdeckungsbereich aufweisen.
- Die weiteren Berichtsteile sind nach Diensten strukturiert. Dabei wird zunächst allgemein auf die vom Security-Framework definierten Indikatoren zurückgegriffen.
- Je nach Zielgruppe können weitere spezifische Indikatoren für den jeweiligen Dienst integriert werden. Bei kundenspezifischen und anderweitig extern vorgegebenen Kennzahlen sind die damit zu prüfenden Hypothesen nicht zwingend bekannt.
- Als höchster Detaillierungsgrad können die maschinen- bzw. komponentenspezifischen Indikatoren bis hin zu einzelnen Basiskennzahlen verwendet werden.

In den Sicherheitsberichten sollten darüber hinaus Hinweise auf im Berichtszeitraum durchgeführte Änderungen an den Sicherheitsmaßnahmen sowie für die Zukunft bereits geplante Änderungen erwähnt werden, um zu vermeiden, dass notwendige Maßnahmen aufgrund von Latenzen (vgl. Timingkategorie *lagging* oben) unnötig wiederholt durchgeführt werden und dadurch eventuell zu einer Überkompensation und Mehrkosten führen.

Abbildung 6.40 zeigt ein im Rahmen dieser Arbeit konzipiertes partielles Informationsmodell für die Spezifikation von an Security-Frameworks orientierten Sicherheitsberichten, das beispielsweise als Grundlage für ein Reporting-Werkzeug verwendet werden kann. Die in der linken Bildhälfte dargestellten MOs basieren auf den oben genannten Charakteristika; die Untergliederung in externe und interne Berichte, die den angegebenen Einflüssen unterliegen, geht auf die von Schaaf in [Sch08, Kap. 5] vorgestellten SLA-Reporting-Konzepte zurück.

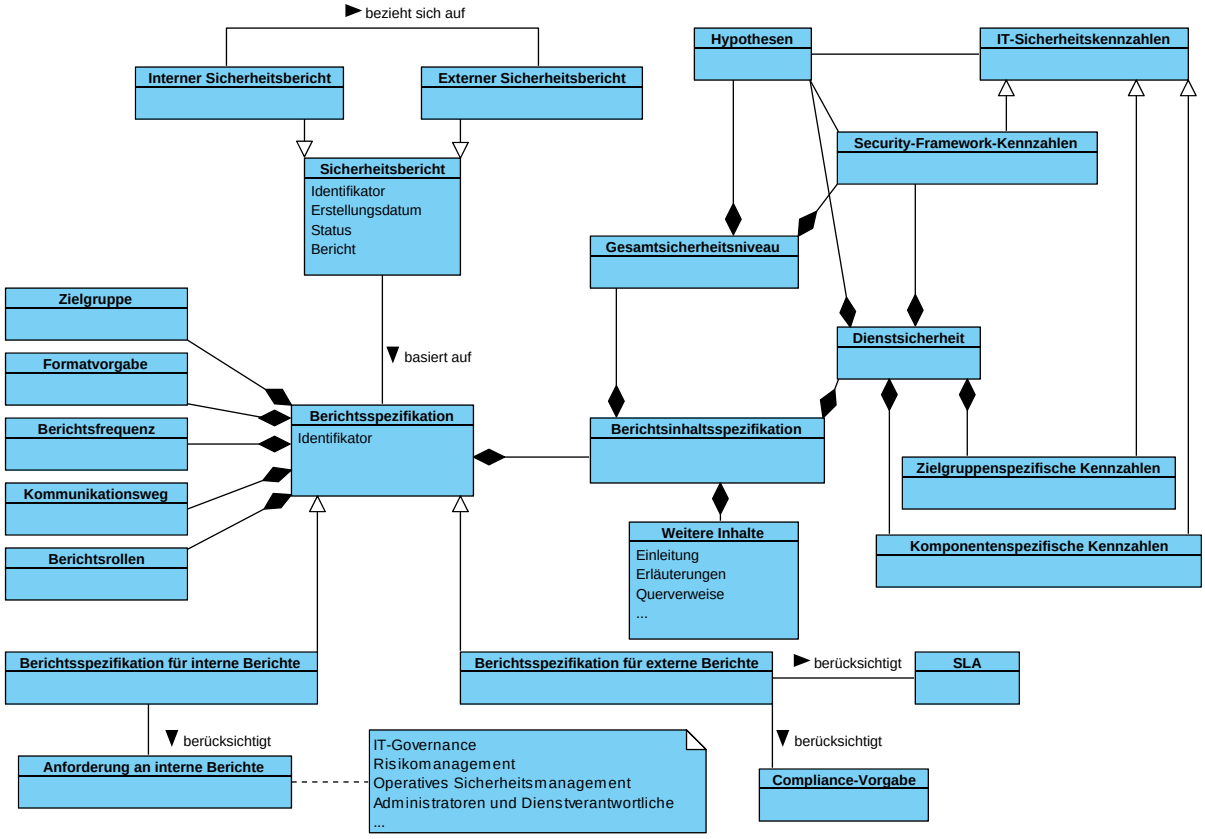


Abbildung 6.40.: Partielles Informationsmodell für Sicherheitsberichte

Die MOs in der rechten Bildhälfte sind direkt von den in den Abschnitten 6.6.1 bis 6.6.3 dargelegten Konzepten abgeleitet.

Auf Basis des in Abschnitt 6.4.4.1 diskutierten Rollenmodells können die folgenden typischen Zielgruppen unterschieden werden:

- *Administratoren* und *Dienstverantwortliche*: Für diese Rollen ist charakteristisch, dass sie für ihre eigenen Dienste jeweils sehr detaillierte, techniknahe Informationen benötigen; hingegen reicht ein ergänzender, allgemeiner Überblick über den Sicherheitszustand der Gesamtinfrastruktur sowie von Diensten, zu denen enge Abhängigkeiten bestehen, meist aus.
- *Auditoren* und *Management*: Zur Überprüfung der Einhaltung von Compliance-Vorgaben sowie als Gesamtüberblick benötigen sowohl Auditoren als auch die Organisationsleitung im Allgemeinen Kennzahlen, die weniger auf einzelne technische Komponenten oder Details von Angriffen eingehen, sondern Aufschluss über das für die einzelnen Dienste und die Gesamtinfrastruktur erreichte Sicherheitsniveau und den dafür erforderlichen Ressourceneinsatz geben. Im Bedarfsfall, beispielsweise falls ein massiver Sicherheitsvorfall eskaliert werden musste, können weitere Kennzahlen ergänzt werden.
- Sicherheitsberichte für *Kunden* umfassen im Allgemeinen die in SLAs vereinbarten

Kennzahlen und ggf. weitere, aus Sicht des Dienstleisters nicht geheimzuhaltende Informationen zum Stand der Sicherheit. Die Kunden sollen damit selbst prüfen können, ob die vertraglich zugesicherten Dienstqualitätseigenschaften eingehalten wurden, und einen Überblick über die Bemühungen des Dienstleisters um eine kontinuierliche Verbesserung erhalten.

- Berichte für das *operative Sicherheitsmanagement* können inhaltlich im Allgemeinen als Obermenge aller anderen Sicherheitsberichte aufgefasst werden, da die Security Engineers nicht nur einen Überblick, sondern detaillierte Informationen über alle Dienste und Infrastrukturteile hinweg benötigen, um den Bedarf für weitere Verbesserungen identifizieren und priorisieren zu können. Um eine übersichtliche Darstellung zu erzielen, können beispielsweise detaillierte Informationen zu Diensten, deren KPIs ihrem Sollwert entsprechen, ausgeblendet bzw. nur bei Bedarf verfügbar gemacht werden.
- Berichte für das *Risikomanagement* haben analog zu den Äquivalenten für die Unternehmensleitung und das operative Sicherheitsmanagement einen szenarienweiten Abdeckungsbereich. Dabei werden einerseits techniknahe bzw. eng an Sicherheitsfunktionalitäten orientierte Kennzahlen benötigt, um beispielsweise neue Bedrohungen, neue Schwachstellen und veränderte Eintrittswahrscheinlichkeiten identifizieren zu können. Um andererseits auch Auswirkungsabschätzungen präzisieren und dem *Finanzwesen* zuarbeiten zu können, sind jedoch zusätzlich die auf die Erfassung des Ressourceneinsatzes spezialisierten Indikatoren zu betrachten.

Die bei den einzelnen Kennzahlen angegebenen Interpretations- und Entscheidungsregeln sowie Handlungsvorgaben, die in geeigneter Form auch in den Sicherheitsberichten wiedergegeben werden, steuern die von den einzelnen Zielgruppen in ihrem Bereich zu ergreifenden Konsequenzen. Neben Reparametrisierungen, die von Administratoren und dem operativen Sicherheitsmanagement vorgenommen werden können, kann sich dabei auch der Bedarf an zusätzlichen Sicherheitsmechanismen und -maßnahmen abzeichnen.

Eine zentrale Fragestellung ist folglich, unter welchen Randbedingungen eine über die laufenden Betriebskosten hinausgehende Investition – im hier betrachteten Fall in die Erweiterung bzw. Ergänzung eines Security-Frameworks – gerechtfertigt ist. Wie bereits im Kontext des Risikomanagements diskutiert wurde, unterscheiden sich Investitionen in Sicherheitsmaßnahmen von klassischen betriebswirtschaftlichen Modellen dadurch, dass keine unmittelbaren Anlagerendite (*Return on Invest*) zu erwarten sind, sondern lediglich eventuell eintretende Schäden verhindert bzw. reduziert werden können. Gordon und Loeb haben mit [GL02] ein inzwischen weit verbreitetes, IT-sicherheitsspezifisches Investitionsmodell vorgelegt, das eine Kosten-/Nutzenabwägung ex ante ermöglicht. Es wurde im Rahmen empirischer Studien erfolgreich angewandt und dient als Basis für andere Modelle, die den Zusammenhang zwischen Kosten, erreichtem Sicherheitsniveau und verhinderten Sicherheitsvorfällen aufzeigen (vgl. [GL06] und [Bohm10]).

Im Rahmen des Finanzwesens muss die Budgetvergabe ans Sicherheitsmanagement im Allgemeinen dreistufig erfolgen (vgl. [Bohm10]); dabei ist zu klären,

1. wie hoch das Gesamtbudget für den Bereich IT-Sicherheit zu veranschlagen ist,
2. wie dieses Budget auf die einzelnen Dienste und Prozesse verteilt werden soll und
3. in welcher Kostenhöhe Einzelmaßnahmen genehmigt werden sollen.

Das Gordon-Loeb-Modell betrachtet hiervon die dritte Fragestellung, indem es die Investitionskosten für eine Sicherheitsmaßnahme den durch ein Risiko zu erwartenden finanziellen Schäden gegenüberstellt. Es trifft dabei folgende Vereinfachungen:

- Es werden nur Investitions-, aber nicht laufende Betriebskosten betrachtet. Diese können ggf. unter Annahme einer begrenzten Nutzungszeit zu den Investitionskosten addiert werden. Zudem wird nicht näher betrachtet, ob die Investition mit einem Wiederverkaufswert verbunden ist oder nicht (z. B. Hardwareanschaffung und -verkauf im Unterschied zu Mitarbeiterschulungen).
- Der z. B. von allgemeiner Inflation beeinflusste Wert des zu investierenden Geldbetrags wird nicht zu verschiedenen Zeitpunkten betrachtet, d. h. das Modell kann nur als Entscheidungsgrundlage dafür herangezogen werden, ob eine Investition sinnvoll erscheint, legt aber nicht den bestmöglichen Zeitpunkt dafür fest.
- Es wird nur eine Bedrohung pro Asset betrachtet, um das Modell möglichst einfach gestalten zu können.

Das Gordon-Loeb-Modell basiert auf drei Parametern: λ ist ein konstanter Wert, der den mit der betrachteten Bedrohung verbundenen finanziellen Schaden widerspiegelt. $t \in [0,1]$ repräsentiert die Wahrscheinlichkeit, dass die Bedrohung eintritt. $v \in [0,1]$ entspricht der Verwundbarkeit, d. h. der Wahrscheinlichkeit, dass der Schaden entsteht, wenn die Bedrohung eintritt. Mit der Bedingung $\lambda < M$ wird sichergestellt, dass der betrachtete potentielle Schaden unterhalb einer Grenze M für katastrophal hohe Verluste liegt, da es bei entsprechend hohen Risiken im Allgemeinen keine realistische Option ist, den mit Investitionsmodellen verbundenen potentiellen Verzicht auf Schutzmaßnahmen in Erwägung zu ziehen.

Die Single Loss Expectancy (vgl. Abschnitt 6.3.2.3) liegt somit bei $L_E = \lambda t v$. Unter der Annahme, dass v szenarienspezifisch beeinflusst werden kann, t hingegen nicht, ist der potentielle Verlust $L = \lambda t$ konstant. Die zentrale Fragestellung des Gordon-Loeb-Modells ist, bis zu welcher Obergrenze eine Investition in eine Sicherheitsmaßnahme, die mit den Kosten z verbunden ist, getätigt werden sollte: Offensichtlich ist die Maßnahme auf jeden Fall nur dann ökonomisch gerechtfertigt, wenn $z < L$. Zielsetzung ist jedoch eine maximale Ersparnis, d. h. z soll so klein wie möglich, muss jedoch unter Berücksichtigung der Auswirkung der Investition auf das verbleibende Risiko optimiert gewählt werden.

Das Gordon-Loeb-Modell sieht deshalb für die Analyse eine Funktion $S(z, v_{alt})$ vor, deren Wert der Verwundbarkeit v_{neu} entspricht, die verbleibt, wenn die mit den Kosten z verbundene Investition getätigt wurde. Dabei wird von den folgenden Annahmen ausgegangen:

- $\forall z : S(z,0) = 0$, d. h. unverwundbare Systeme bleiben unverwundbar.
- $\forall v : S(0,v) = v$, d. h. ohne Investitionen verändert sich die Verwundbarkeit nicht. Dies ist wiederum eine Vereinfachung gegenüber der Realität, in der z. B. durch kostenneutrale Änderungen wie automatisierte Softwareaktualisierungen eine Reduzierung der Verwundbarkeit erfolgen kann.
- $\forall v \in [0,1]$ und $\forall z$ gilt: (Erste partielle Ableitung nach z) $S_z(z,v) < 0$ und (zweite partielle Ableitung nach z) $S_{zz}(z,v) > 0$

Durch die dritte Annahme wird vorgegeben, dass die Funktion S zweimal stetig differenzierbar sein muss; dies ist Voraussetzung dafür, dass das unten beschriebene Optimierungsproblem

gelöst werden kann. Jeder zu betrachtenden konkreten Ausprägung der Funktion $S(z, v)$ liegt die Idee zugrunde, dass sich die Sicherheit zwar umso mehr erhöht bzw. die Verwundbarkeit kontinuierlich abnimmt, je mehr das Investitionsvolumen zunimmt; die erreichbare Reduktion der Verwundbarkeit nimmt dabei jedoch immer stärker ab. Unter der Prämisse, dass perfekte Sicherheit nicht erreicht werden kann, d. h. $\lim_{z\to\infty} S(z, v) = 0$, resultiert, dass die Wahrscheinlichkeit für einen erfolgreichen Angriff mit entsprechenden Investitionen beliebig nah an 0 angenähert werden kann. Die Forderung von Gordon und Loeb nach zweimaliger stetiger Differenzierbarkeit deckt sich allerdings nicht mit der gängigen Praxis diskreter Investitionen in Sicherheitsmaßnahmen, ist für die Lösung des Optimierungsproblems mit gängigen Methoden jedoch unerlässlich, so dass vereinfachend angenommen werden muss, dass Investitionen glatt approximiert werden können.

Für den Fall, dass das Schadereignis eintritt, beträgt die Ersparnis nach Tätigen der Investition $E(z) = (v - S(z, v))L$ bzw. unter Abzug der Investitionskosten netto $E_n(z) = (v - S(z, v))L - z$. Für den Fall, dass es sich um kein unverwundbares System handelt, also $0 < v < 1$ gilt, müssen somit die optimalen Investitionskosten $z^*(v)$ gefunden werden. Aufgrund der dritten obigen Annahme ist $S(z, v)$ bezüglich z strikt konvex und somit $E_n(Z)$ strikt konkav; somit kann das Problem mit Hilfe der konvexen Optimierung gelöst werden: Aus der Zielsetzung

$$\frac{z}{\partial z}\left[(v - S(z, v))L - z\right] = 0$$

ergibt sich die Bedingung an $z^* = Z^*(v)$:

$$-\frac{\partial}{\partial z}S(z^*, v)L = 1.$$

Gordon und Loeb betrachten verschiedene als praktisch relevant erachtete Funktionen $S(z, v)$ und kommen zum Schluss, dass die Obergrenze für z^* in jedem Fall gegen $\frac{1}{e}$ konvergiert, d. h. dass die Investitionskosten rund 37 Prozent der SLE nie übersteigen sollten. Dieses Ergebnis wurde von Willemson zwar durch einfache Gegenbeispiele widerlegt [Wil06]. Baryshnikov weist die Gültigkeit der $\frac{1}{e}$-Grenze in [Bar07] aber für logarithmisch-konvexe Funktionen $S(z, v)$ nach, die dann vorliegen, wenn Einzelinvestitionen in einer Reihenfolge getätigt werden, so dass als nächstes jeweils in diejenige Maßnahme im Rahmen des Budgets investiert wird, die das Restrisiko am stärksten absenkt.

Übertragen auf den Einsatz von Security-Frameworks ist deshalb zu differenzieren, ob die Frameworkkonzepte oder andere bereits vorliegende Erfahrungen mit den von ihnen vorgesehenen Schutzmaßnahmen ausreichen, um eine spezifische Funktion $S(z, v)$ zu definieren, auf deren Basis die mit Bezug auf das Modell optimalen Investitionskosten berechnet werden können. Alternativ kann das Budget anhand der $\frac{1}{e}$-Grenze vorgegeben werden; bezüglich der dabei zu realisierenden Frameworkmodule muss zwischen zwingend notwendigen und optionalen Frameworkkomponenten unterschieden werden. Sofern bereits die Kosten für die zwingend notwendigen Komponenten das Budget übersteigen, müssen Alternativlösungen untersucht werden. Das für optionale Frameworkkomponenten verbleibende Budget sollte jedoch – nicht nur unter sicherheitstechnischen, sondern auch ökonomischen – Gesichtspunkten anschließend für diejenigen Module verwendet werden, die das jeweils noch verbleibende Risiko am stärksten reduzieren. Dies muss jedoch spezifisch für das jeweilige Security-Framework analysiert

werden; es lässt sich somit nicht pauschal entscheiden, ob eher möglichst viele, mit relativ niedrigen Kosten verbundene Frameworkmodule implementiert werden sollten oder nur wenige, bei denen auf jeweils hochwertige Realisierungsvarianten zurückgegriffen wird.

Für den Fall, dass im Rahmen der Auswertung von Sicherheitsberichten entschieden wurde, weitere Investitionen in Sicherheitsmaßnahmen zu tätigen, muss auch geklärt werden, wann dies am besten erfolgen sollte. Während konkrete Sicherheitsvorfälle in der Regel zeitnahe Maßnahmen zur Konsequenz haben, liegen bislang zu wenige empirische Daten vor, um eine klare Strategie empfehlen zu können [GL06]. Aus ökonomischer Sicht ist bei vielen IT-Risiken eine Abwartehaltung (engl. *wait-and-see*) gerechtfertigt (vgl. [GLL03]), so dass Maßnahmen erst dann ergriffen werden, wenn der Bedrohungsfall schon einmal eingetreten ist; durch organisationsübergreifenden Informationsaustausch kann auch bereits dann agiert werden, wenn andere Unternehmen bereits reagieren müssen. Weiterentwicklungen des Gordon-Loeb-Modells berücksichtigen darüber hinaus z. B. die Kapitalverzinsung, die sich aus einer verzögerten Investition ergibt (vgl. [Kro10] und [FPW07]).

6.7. Zusammenfassung

In diesem Kapitel wurde zunächst auf Basis einer Literaturrecherche aufgezeigt, dass sich Security-Frameworks nahtlos in die sich kontinuierlich weiterentwickelnden Konzepte und prozessorientierten Architekturen zum Sicherheitsmanagement integrieren lassen. In der Praxis spielen dabei einerseits Standards und Best Practices zum Sicherheitsmanagement und andererseits gesetzliche und branchenspezifische Auflagen eine nicht zu vernachlässigende Rolle. Hieraus wurde zum einen der Nutzen einer Orientierung des Managements von Security-Frameworks an ISO/IEC 27001 abgeleitet; zum anderen wurde die Relevanz der Teilbereiche Risikomanagement, Datenschutz und Berichtswesen herausgearbeitet.

Zur gesamtheitlichen Betrachtung des Managements von Security-Frameworks und aufgrund deren häufig stark technischer Ausrichtung wurde anschließend das operative Sicherheitsmanagement mit seinen für Security-Frameworks relevanten Schnittstellen analysiert. Hierfür wurden zunächst eine Begriffsbildung vorgenommen und die einzelnen Aufgabenbereiche zusammengetragen und klassifiziert. Die Schwerpunkte liegen dabei auf technischen Maßnahmen zur System- und Netzsicherheit, zur Zugriffsverwaltung, Sicherstellung der hohen Verfügbarkeit von Diensten und Daten sowie auf der Anwendung kryptographischer Mechanismen. Die Vielzahl präventiv ausgerichteter Maßnahmen wird durch Monitoring und die zumindest teilautomatisierte Bearbeitung von sicherheitsrelevanten Vorfällen ergänzt. Wie bereits die Untersuchung aktueller Security-Frameworks in Kapitel 4 gezeigt hatte, liegen hier klar die Schwerpunkte dessen, wozu Security-Frameworks ohne die Notwendigkeit umfassender szenarienspezifischer Ergänzungen eingesetzt werden können.

Die Auswahl konkreter organisatorischer und technischer Maßnahmen zur weiteren Verbesserung des Sicherheitsniveaus ist eines der Teilziele des Risikomanagements, das in allen Standards und Best Practices ein essentieller Bestandteil des Sicherheitsmanagements ist. Mit dem Einsatz von Security-Frameworks ergeben sich mehrere wichtige Vereinfachungen, die sich von der effizienteren Identifizierung der in einem Durchlauf des Risikomanagements zu betrachtenden Assets, Bedrohungen und Schwachstellen über die fundiertere Beurteilung der Eintrittswahrscheinlichkeit und Auswirkungen von Schadereignissen bis hin zu der Auswahl

von Gegenmaßnahmen und der Einstufung des Restrisikos erstrecken. Anhand einer Einordnung in die von NIST SP 800-30 vorgegebene Struktur wurden die Beiträge und der Einsatz von Security-Frameworks analysiert, spezifische Ergänzungen vorgenommen und weitere Risikomanagementmethoden einander gegenübergestellt sowie auf ihre Kombinierbarkeit im Kontext von Security-Frameworks hin untersucht.

Der Betrieb von Security-Frameworks wird durch den Einsatz von integrierten Managementplattformen unterstützt, die auf Basis einer Managementarchitektur die für das Management relevanten Eigenschaften in Form von Managed Objects abbilden und einheitliche Schnittstellen und Basisfunktionen für Managementwerkzeuge bereitstellen. Nach einer Motivation der Notwendigkeit eines integrierten Sicherheitsmanagements für Security-Frameworks und einem Vergleich mit ähnlichen Aufgabenstellungen sowohl im Netz- und Systemmanagement als auch im ITSM Configuration Management wurde als Schwerpunkt ein Informationsmodell spezifiziert, über das sowohl Security-Frameworks als Ganzes als auch ihre Einzelkomponenten und deren Umgebung erfasst und abgebildet werden können. Daran anschließend wurden das grundlegende Organisationsmodell mit seinen Domänen und Rollen und ein auf verschiedenen Nachrichtentypen basierendes Kommunikationsmodell konzipiert. Die Betrachtung von Managementarchitekturen abschließend wurde eine Systematik für die Untergliederung der Funktionsbereiche anhand einer Orientierung an Prozesskategorien, Prozessen und Anwendungsfällen erarbeitet und am Beispiel ausgewählter Bereiche des Risikomanagements exemplarisch umgesetzt.

Neben dieser Einbindung ins operative Sicherheitsmanagement wurde auch das Zusammenspiel mit Managementprozessen analysiert. Hierzu wurden ISO/IEC 27001, ITIL v3 und CobiT analysiert, um jeweils die für Security-Frameworks relevanten Ziele der einzelnen Prozesse, die Einflüsse von und auf Security-Frameworks und schließlich die im Lebenszyklus von Frameworkinstanzen deshalb zu berücksichtigenden Schnittstellen herauszuarbeiten. Dabei wurde gezeigt, dass Security-Frameworks zu allen elf Maßnahmenkategorien der ISO/IEC 27001 wichtige Beiträge liefern und mit ihrer Sicherheitsfunktionalität insbesondere den Bereich der Betriebs- und Kommunikationssicherheit (A.10) abdecken. Am Beispiel eines fiktiven Sicherheitsvorfalls wurde gezeigt, wie von Security-Framework emittierte Sicherheitsmeldungen über SIEM-Systeme geprüft und klassifiziert werden können, um im Rahmen eines Security-Incident-Response-Prozesses, der eine Spezialisierung des ITIL v3 Incident Management darstellt, effizient bearbeitet werden zu können. Es wurde gezeigt, dass durch die Kombination von ISO/IEC 27001 und ITIL v3 kann ein nahezu vollständige Abdeckung der im Kontext von Security-Frameworks relevanten Managementprozesse erreicht werden kann; beispielsweise zeigte sich bei der Untersuchung der CobiT-Prozesse, dass gegenüber der Betrachtung der anderen beiden Referenzen lediglich der Aspekt der Automatisierung noch stärker zu betonen ist. Über Prozessabbildungen können die Ergebnisse zudem auf andere Standards und Best Practices übertragen werden.

Zur Erfassung und Bewertung des erreichten IT-Sicherheitsniveaus und der von Security-Frameworks dazu geleisteten Beiträge werden Kennzahlen benötigt; insbesondere sollen nicht nur qualitative Einschätzungen, sondern quantitative Beurteilungen ermöglicht werden. Da ein direktes Messen der IT-Sicherheit von Systemen und Infrastrukturen nicht möglich ist, muss über die Kombination verschiedener IT-Sicherheitskennzahlen eine Näherung erzielt werden, die für die in der Praxis anzutreffenden Aufgaben wie das Nachweisen der Einhaltung von SLA-Sicherheitsparametern und das Ableiten sinnvoller Verbesserungsmaßnahmen ausreichen. Auf Basis einer Literaturrecherche wurden zunächst der aktuelle Stand der Technik

bezüglich IT-Sicherheitskennzahlen zusammengefasst und seine Defizite aufgezeigt. Spezifisch für Security-Frameworks wurde anschließend in Anlehnung an ISO/IEC 27004 erarbeitet, aus welchen Bestandteilen ein hypothesenbasiertes, prozessorientiertes Vorgehen bei der Spezifikation zusammenhängender Kennzahlen und der Umsetzung der entsprechenden Messverfahren bestehen muss. Auf Basis verwandter Arbeiten wurden anschließend qualitative Anforderungen an IT-Sicherheitskennzahlen zusammengetragen, eine Kategorisierung vorgenommen und eine Struktur für die Dokumentation und Verwaltung von IT-Sicherheitskennzahlen erarbeitet, die im Kontext von Security-Frameworks eingesetzt werden soll. Schließlich wurde konzipiert, wie die durch Security-Frameworks in Zusammenhang gebrachten Kennzahlen zu Sicherheitsberichten aufbereitet werden und wie diese auszuwerten sind, um beispielsweise über die Investition in weitere Sicherheitsmaßnahmen, z. B. zusätzliche Frameworkmodule, zu entscheiden. Hierzu wurde die Übertragbarkeit des Sicherheitsinvestitionsmodells nach Gordon und Loeb auf Security-Frameworks dargelegt.

Sowohl in etablierten Prozessen wie dem Risikomanagement, in das durch den Einsatz von Security-Frameworks primär systemübergreifend beschriebene Teilergebnisse eingebracht werden, die konzeptionelle Anpassungen erfordern, als auch in jüngeren Aufgabenbereichen wie dem Einsatz von Kennzahlen im Rahmen des Sicherheitsmanagements ergibt sich der Bedarf, für das Management von Security-Frameworks relevante Aspekte mit dedizierten Werkzeugen zu unterstützen. Im nächsten Kapitel werden dieser Bedarf analysiert und entsprechende Werkzeugkonzepte erarbeitet.

Kapitel 7.

Werkzeuge für das Management von Security-Frameworks

Inhalt dieses Kapitels

Die nachhaltige Realisierung eines effizienten Managements von Security-Frameworks setzt aus den in Abschnitt 6.4 erörterten Gründen adäquate technische Werkzeuge voraus, die jeweils Teile der Managementabläufe abbilden und Aufgaben entweder **automatisiert erledigen** oder den Ausführenden dabei **gezielt unterstützen**. Aus dem bereits wiederholt

betrachteten Charakteristikum von Security-Frameworks, Sicherheitsmaßnahmen und entsprechende Sicherheitsmechanismen zu bündeln, folgt zunächst, dass die für jede Einzelkomponente geeigneten Werkzeuge auch im Kontext eines Security-Frameworks als Ganzes relevant, für dieses Kompositum aber möglicherweise nicht mehr optimal geeignet sind. Dennoch wäre es nicht zielführend, auf bestehende Sicherheitswerkzeuge schlichtweg zu verzichten und für Security-Frameworks spezifische Varianten von Grund auf neu zu entwickeln. Durch die Diskussion der Stärken und Schwächen aktueller Security-Frameworks in Kapitel 4 und die Analyse der erforderlichen Einbettung in die diversen Managementprozesse in Kapitel 6 wurde vielmehr evident, dass über den gesamten in Kapitel 5 spezifizierten Lebenszyklus hinweg **additive und komplementäre Konzepte** auf technischer und organisatorischer Ebene erforderlich sind, die gezielt auf die beim Einsatz von Security-Frameworks gegenüber einer herkömmlichen Betrachtung ihrer Einzelteile entstehenden Anforderungen und Schnittstellen eingehen.

In Abschnitt 7.1 wird deshalb zunächst der spezifische **Bedarf an Werkzeugen für das Management von Security-Frameworks** analysiert. Diese Bedarfsanalyse erfolgt top-down auf Basis der bereits diskutierten Eigenschaften von Security-Frameworks und den spezifizierten Prozessen und Abläufen. Der Hintergrund dafür ist, dass von einer Bottom-up-Einzelbetrachtung der Werkzeugdefizite ausgewählter Security-Frameworks keine unmittelbar von deren konkreten Anwendungsgebieten losgelösten Erkenntnisse erwartet werden kann. Eine nachfolgende umfassende Behandlung aller identifizierten Werkzeuge würde den Rahmen dieser Arbeit sprengen; deshalb wurden zwei Themenbereiche für eine **vertiefende Analyse und Werkzeugspezifikation** wie folgt ausgewählt:

1. In Abschnitt 7.2 wird ein Werkzeug konzipiert, das als Managementkomponente eines dynamischen Intrusion Detection Systems **automatische Reparametrisierungen der in Security-Frameworks enthaltenen Detektionssensorik** vornimmt, um die IDS-Erkennungsleistung in Relation zum Ressourcenaufwand und den zu behandelnden False-Positive-Fehlalarmen zu optimieren. Es verbindet somit die drei funktionalen Security-Framework-Ziele *Adaptivität*, *Automatisierung* und *Auditing* mit der Managementanforderung zur *Event*-Erzeugung und -Verarbeitung. Damit wird eine Lösung für einige wesentliche der in Abschnitt 4.5 dargelegten Defizite bisheriger Security-Frameworks am Beispiel der Verbesserung der Angriffserkennung vorgelegt. Sie bewegt sich schwerpunktmäßig im *funktionalen* Bereich (Kategorie SF-FUNK) von Security-Frameworks mit Schnittstellen zum *Management* (Kategorie SF-MGMT).
2. Komplementär dazu wird in Abschnitt 7.3 ein **Werkzeug zur an Security-Frameworks orientierten Erfassung und Aufbereitung von Sicherheitskennzahlen** konzipiert und diskutiert. Es setzt die in Abschnitt 6.6 vorgestellten Abläufe unter enger Orientierung an den bislang ebenfalls deutlich unterdurchschnittlich erfüllten Managementanforderungen *Metriken*, *KPIs*, *Berichtsdetails* und *ITSM-Schnittstellen* um (vgl. wiederum Abschnitt 4.5). Sein Schwerpunkt liegt somit im Bereich *Management*, wobei auch die technisch-funktionale Basis, die zur Bereitstellung grundlegender Messwerte erforderlich ist, betrachtet wird.

Abbildung 7.1 fasst diese Einordnung zusammen. Es ist anzumerken, dass die Zusammenstellung der in diesem Kapitel angesprochenen Werkzeuge keinen Anspruch auf Vollständigkeit erhebt. Beispielsweise müssten auch Werkzeuge, die primär anderen Prozessen – beispielsweise im Umfeld des ITSM – zuzuordnen sind, erweitert bzw. an die Spezifika von Security-

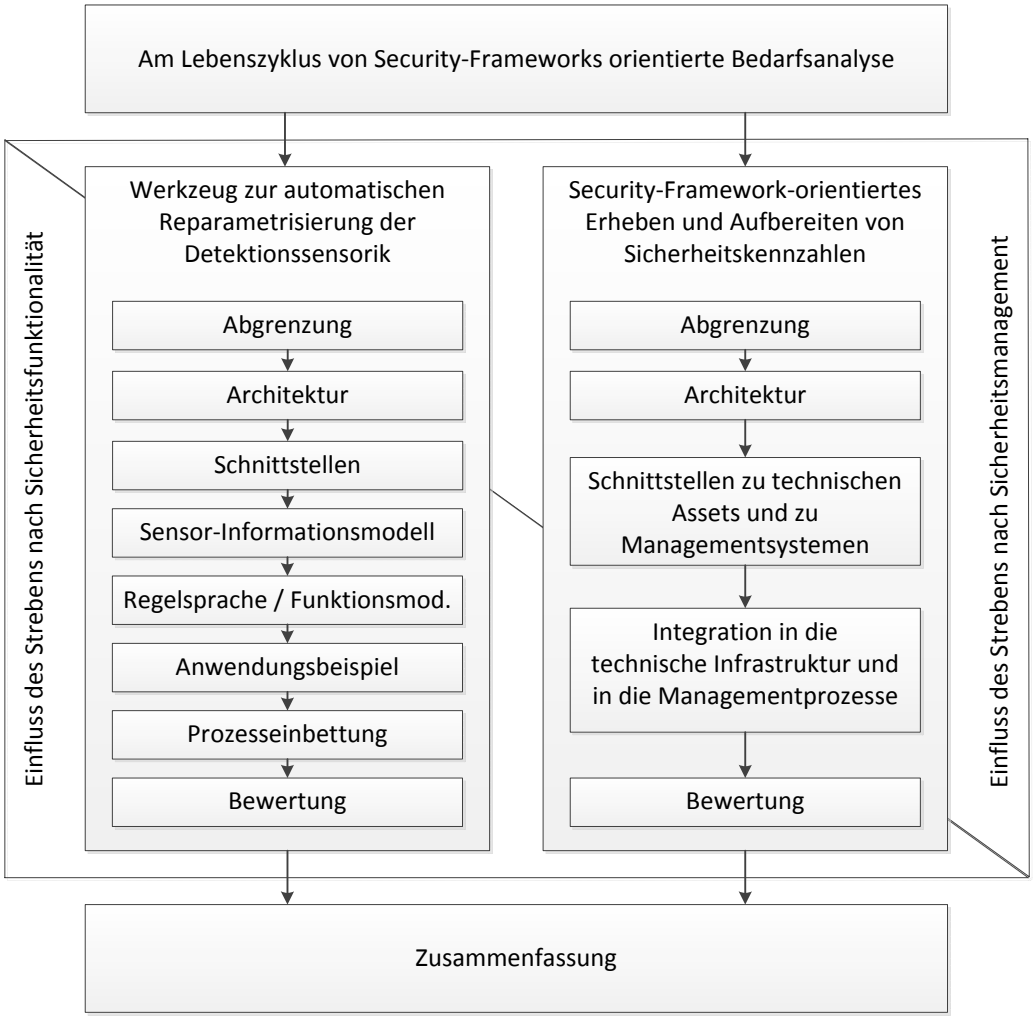


Abbildung 7.1.: Vorgehensmodell in diesem Kapitel

Frameworks angepasst werden. Entsprechende ergänzende Untersuchungen sind z. B. dann durchzuführen, wenn in Anlehnung an die Ausführungen in Abschnitt 6.4 eine vollständige Managementplattform für Security-Frameworks entwickelt werden soll.

7.1. Analyse des Bedarfs an neuen Werkzeugen für das Management von Security-Frameworks

Der Bedarf an einer gezielten Unterstützung der Managementabläufe durch für Security-Frameworks spezifische Werkzeuge ergibt sich überall dort, wo durch die technischen Eigenschaften von Security-Frameworks ein von auf Einzelkomponenten ausgelegten Werkzeugen nicht ausreichend abgedeckter Bedarf entsteht oder wo prozessuale Schnittstellen berücksichtigt werden müssen, die erst durch die Instanziierung eines Frameworkkonzepts entstehen. Im

Folgenden wird dementsprechend primär der Bedarf an *neuen* Werkzeugen betrachtet; dass bestehende Werkzeugkonzepte, beispielsweise für Monitoringsysteme oder das Change Management, geeignet an Spezifika von Security-Frameworks angepasst werden müssen, wurde bereits in Abschnitt 6.4.5 im Kontext von Managementplattformen erläutert.

Die nachfolgenden Ausführungen beschränken sich zudem auf Werkzeuge, die für die meisten der in Kapitel 4 betrachteten Security-Frameworks eingesetzt werden können. Eine erneute Betrachtung einzelner Security-Frameworks zum Ziel der Identifikation der jeweils individuell fehlenden Werkzeuge wird somit nicht in dieser Arbeit durchgeführt, sondern sollte Bestandteil der Weiterentwicklung der jeweiligen Frameworkkonzepte sein. Für die Analyse des Werkzeugbedarfs wurden deshalb die folgenden drei Zwischenergebnisse ausgewertet:

- In Abschnitt 4.5 wurden die Ergebnisse der Bewertungen aller in Kapitel 4 analysierten Security-Frameworks zusammengefasst. Die über alle Security-Frameworks hinweg unterdurchschnittlich erfüllten Anforderungen repräsentieren Aufgabenbereiche, die möglicherweise durch zusätzliche framework-externe bzw. -übergreifende Werkzeuge besser abgedeckt werden können.
- In Kapitel 5 wurden die einzelnen Lebenszyklusphasen von Frameworkkonzepten und Frameworkinstanzen sowie ihre wesentlichen Schnittstellen analysiert. Da sich das Management von Security-Frameworks über den reinen Betrieb hinaus über sämtliche Lebenszyklusphasen erstreckt, spielt die Werkzeugunterstützung in jeder einzelnen Phase eine wichtige Rolle.
- In Kapitel 6 wurden die Schnittstellen von Security-Frameworks u. a. zum operativen Sicherheitsmanagement, zum Risikomanagement, zum Sicherheitsmanagementprozess nach ISO/IEC 27001 und zum IT Service Management nach ITIL v3 erarbeitet. Durch die zum Teil an Prozessen vorgenommenen, durch Security-Frameworks erforderlich werdenden Erweiterungen ergibt sich der Bedarf, die dabei anfallenden zusätzlichen, spezifischen Tätigkeiten ebenfalls mittels Werkzeugen zu unterstützen.

Beschränkt auf einige exemplarische, komplexere Werkzeuge lässt sich anhand der Lebenszyklusphasen strukturiert und über die beiden nachfolgend im Detail konzipierten Werkzeuge hinausgehend somit der folgende neue Werkzeugbedarf festhalten:

- Für die Auswahl von Security-Frameworks und ihren Modulen sowie ihre Initialparametrisierung werden **Planungs- und Simulationswerkzeuge** benötigt. Neben der reinen Berücksichtigung von Security-Frameworks als konzeptionelle Abstraktionsebene muss dabei zwingend eine Reihe neuer Funktionen bereitgestellt werden, die auch losgelöst von Security-Frameworks in herkömmlichen IT-Sicherheitsplanungswerkzeugen noch nicht adäquat umgesetzt wurden. Dies umfasst insbesondere Maßnahmen zur Vermeidung redundanter Komponenten, beispielsweise falls mehrere Security-Frameworks dieselbe Funktionalität benötigen. Dabei muss jedoch die möglichst weitgehende Reduzierung neuer Komponenten in Einklang mit dem im Rahmen des Paradigmas *defense-in-depth* geforderten partiellen funktionalen Überlappung gebracht und somit die Ermittlung einer szenarienspezifisch optimalen Gesamtarchitektur unterstützt werden. Die bei Security-Frameworks identifizierten Defizite zeigen, dass ein solches Planungswerkzeug insbesondere auch zur Verwaltung szenarienspezifischer Anforderungen bzw. Prioritäten und zur Analyse des Kosten-Nutzen-Verhältnisses eingesetzt werden können muss und dass Schnittstellen vorhanden sein müssen, die eine Übernahme der geplanten

Konfiguration in die vom Configuration Management verwalteten Datensätze ermöglichen.

- Für das an Security-Framework angepasste **Risikomanagement** werden Werkzeuge benötigt, die eine zusammenhängende Betrachtung nicht nur der Assets und ihrer Schwachstellen, sondern auch der diesen Assets zugeordneten Security-Frameworks und deren Schutzmechanismen ermöglichen, um die szenarienspezifische Brisanz neu bekannt werdender Schwachstellen besser bewerten zu können. Neben einzelnen Bedrohungen und Schwachstellen sollten Bedrohungsszenarien (vgl. Abschnitt 6.3.5) als Ganzes verwaltet und mit den entsprechenden Beispielen aus den Frameworkkonzepten initialisiert werden können.
- Für alle in einem Szenario eingesetzten Security-Frameworks, die über keine eigenen Management- und Steuerkomponenten verfügen, werden Werkzeuge benötigt, die pro Security-Framework die **komponentenübergreifend konsistente Umsetzung von Managementoperationen** implementieren. Sie bieten dadurch beispielsweise auch eine einheitliche Schnittstelle für andere in Managementplattformen integrierte Werkzeuge. Die dabei für jedes Security-Framework bereitzustellende Funktionalität entspricht jeweils einer Teilmenge der in Abschnitt 6.4.4.3 klassifizierten Funktionen. Die konkrete Ausprägung eines solchen Werkzeugs wird hier nicht näher betrachtet, da sie vom Autor der vorliegenden Arbeit bereits in [GH10] für ein komplementäres Szenario konzipiert wurde: Am Beispiel der Zielsetzung eines organisationsübergreifenden Austausches von Sicherheitsmetadaten wie beispielsweise Zertifikaten und gruppenbasierten Autorisierungsregeln wurde ein Konzept erarbeitet, das auf den von serviceorientierten Architekturen her bekannten Service-Bus-Architekturen als Kommunikationsinfrastruktur basiert. Somit könnte eine vergleichbare, alle Komponenten der in einem Szenario eingesetzten Security-Frameworks umfassende dynamische Busstruktur konzipiert werden, die den sicheren und zuverlässigen Austausch von Steueroperationen und Nachrichten ermöglicht, die Implementierung notwendiger Datenkonvertierungen durch Adapter vereinfacht und die zentrale Kontrolle der Einhaltung szenarienweiter Policies ermöglicht.
- Die sich durch Security-Frameworks zwischen deren vormals isoliert betrachteten Einzelkomponenten ergebenden Zusammenhänge ermöglichen in mehreren Bereichen verbesserte Werkzeuge: Beispielsweise können von dem z. B. in einer Managementplattform hinterlegten Wissen über die gegenseitigen Abhängigkeiten und Auswirkungen der Komponenten von Security-Frameworks auch **Werkzeuge für aktive Sicherheits- bzw. Penetrationstests** profitieren, deren Funktionalität sich bislang auf so genannte Black-Box-Tests beschränkt. Hierbei müssen insbesondere das Zusammenspiel mit den in Managementsystemen zentral gespeicherten Informationen über die einzelnen Komponenten und deren funktionale Abhängigkeiten betrachtet werden, um beispielsweise die Auswirkungen von Angriffen, die aus mehreren Schritten bestehen und sich gegen verschiedene Komponenten wenden, ermitteln zu können.

In Abschnitt 7.2 wird ein Werkzeug zur automatischen Reparametrisierung der in Security-Frameworks und geschützten Assets eingesetzten Angriffsdetektoren spezifiziert. Die vorgestellten Mechanismen vertiefen exemplarisch anhand von Intrusion-Detection-Komponenten, wie eine Kombination der vielen Security-Frameworks zu bescheinigenden Defizite auf technischer und managementspezifischer Ebene durch den Einsatz framework-übergreifender Managementwerkzeuge in den entsprechenden Teilbereichen kompensiert werden kann.

Demgegenüber geht das in Abschnitt 7.3 konzipierte Werkzeug für das Security-Framework-orientierte Erheben und Aufbereiten von Sicherheitskennzahlen auf die praktische Umsetzung der in Abschnitt 6.6 erarbeiteten Mess- und Berichtskonzepte ein, für die – wie ibidem bereits diskutiert – bislang noch keine adäquate und ganzheitliche technische Unterstützung existierte.

7.2. Werkzeug zur automatischen Reparametrisierung der Detektionssensorik in Security-Frameworks

Wie die Kategorisierung der Aufgaben des operativen Sicherheitsmanagements in Abschnitt 6.2 gezeigt hat, dient der größte Teil der üblicherweise eingesetzten technischen Sicherheitsmechanismen der *Prävention* von Sicherheitsvorfällen. Die *Detektion* wird überwiegend durch die automatisierte Auswertung und Korrelation der Meldungen der schon vorhandenen Dienste, Systeme und Präventionsmechanismen durchgeführt und in meist geringerem Umfang durch spezialisierte Sensoren wie Honeypots und Intrusion Detection Systeme (IDS) ergänzt. Für die automatische *Reaktion* auf erkannte oder vermutete Sicherheitsvorfälle existieren bislang nur wenige universelle Konzepte; im Allgemeinen werden im Rahmen der Angriffserkennung Triggermechanismen vorgesehen, die beispielsweise eine E-Mail-Benachrichtigung oder das Anstoßen szenarienspezifisch implementierter Programme und Skripte ermöglichen, die kontinuierlich von den Administratoren an die lokalen Erforderlichkeiten angepasst werden. Durch die so bereitgestellten Automatismen können beispielsweise vorhandene Präventionsmechanismen wie Firewalls dynamisch umkonfiguriert werden, um akute Angriffe einzudämmen (vgl. das Beispielszenario zum Incident Management in Abschnitt 6.5.2.4).

Präventionsmechanismen sind im Allgemeinen durch ihre lokale Autarkie gekennzeichnet, so dass die Anforderungen an ihre Performanz und Skalierbarkeit durch das reguläre Nutzungsverhalten der von ihnen geschützten Assets determiniert werden: Die Anforderungen an den Durchsatz eines Paketfilterfirewalls ergeben sich beispielsweise primär aus der Bandbreite des geschützten Netzes und gegebenenfalls weiteren QoS-Parametern, z. B. zu garantierenden Maximallatenzen beim Weiterleiten einzelner Datenpakete. Demgegenüber sind IDS, die häufig den Kern aller in einem Szenario eingesetzten Detektionsmechanismen bilden, abhängig von der Anzahl, Platzierung und Erkennungsleistung der an sie angeschlossenen Sensorik, die sicherheitsrelevante Meldungen zur genaueren Analyse an zentrale oder z. B. hierarchisch angeordnete Analysestationen sendet. Der IDS-Einsatz steht folglich vor der Herausforderung, dass die quantitative und qualitative Erkennungsleistung innerhalb noch näher zu betrachtender Grenzen proportional zur Anzahl der eingesetzten Sensoren wächst, sich mit jedem weiteren Sensor jedoch eine Vielzahl zusätzlich zu verarbeitender Ereignismeldungen und individuelle Fehlalarme ergeben, die in der Praxis rasch dazu führen, dass eine einzelne zentrale Analysestation mit der Auswertung der großen Zahl an Ereignismeldungen überfordert wird. Während sich die Skalierbarkeit theoretisch durch den Einsatz weiterer Analysestationen, die hierarchisch oder anderweitig vermascht angeordnet sind, verbessern lässt, müssen beim praktischen Einsatz häufig weitere Randbedingungen berücksichtigt werden:

- Die Einführung und der laufende Betrieb zusätzlicher Analysestationen sind mit Kosten verbunden und erhöhen die Gesamtkomplexität des IDS. Unter geeigneter Berücksichtigung weiterer Aspekte wie ihrer Hochverfügbarkeit ist es deshalb ein im Allgemeinen wesentliches Ziel, die Anzahl der erforderlichen Analysestationen zu minimieren.

- Der laufende Betrieb von Sensoren benötigt Ressourcen, die somit möglicherweise anderen Diensten und Anwendungen nicht zur Verfügung stehen. Wenn beispielsweise auf Serversystemen durch den Einsatz von hostbasierten IDS (siehe Abschnitt 2.4.2) regelmäßig sämtliche zum Betriebssystem gehörenden Dateien auf unautorisierte Modifikationen überprüft werden, reduziert sich die für andere Zwecke verfügbare Systemleistung zu den entsprechenden Zeitpunkten. Kommen derartige Mechanismen und Sensoren ohne weitere Koordination beispielsweise im Kontext der Servervirtualisierung zum Einsatz, so potenzieren sich diese Engpässe entsprechend, beispielsweise wenn alle auf derselben physischen Hardware betriebenen virtuellen Maschinen gleichzeitig nach manipulierten lokalen Systemdateien fahnden. Um derartige Engpässe zu vermeiden, sollten IDS-Sensoren folglich möglichst nur dann aktiv eingesetzt werden, wenn sie zur Erkennung oder genaueren Diagnose eines Angriffs benötigt werden und eine übergreifende Koordination der Abläufe rund um die Angriffserkennung stattfindet.

Das in diesem Abschnitt erarbeitete Konzept zur automatischen, dynamischen Reparametrisierung verschiedenster Angriffserkennungssensoren ist somit wie folgt motiviert:

- Die von Security-Frameworks bereitgestellten technischen Lösungen umfassen häufig eine Reihe von Detektionskomponenten, die Policyverstöße und jeweils spezifische Angriffsvarianten erkennen und behandeln können. Diese Behandlung findet bislang jedoch überwiegend frameworkintern statt; Schnittstellen nach außen sind prinzipiell erwünscht, in bisherigen Security-Frameworks allerdings häufig noch nicht explizit ausgeprägt (vgl. Anforderung *SF-MGMT-Events* und Diskussion in Abschnitt 4.5). Die potentielle szenarienweite Angriffserkennungsleistung wird somit noch nicht ausgeschöpft.
- Viele Security-Frameworks sind bereits auf die dynamische Reparametrisierung zur Laufzeit ausgelegt (vgl. Anforderung *SF-FUNK-Adaptivität* und deren überdurchschnittliche Gesamtbewertung an o. g. Stelle), so dass ein bedarfsorientiertes Zu- und Abschalten sowie Rekonfigurieren prinzipiell möglich ist. Demgegenüber sind die in den betrachteten Security-Frameworks bereits implementierten Auswertungsalgorithmen und Automatisierungskonzepte noch nicht ausreichend ausgeprägt (vgl. Anforderungen *SF-FUNK-Auditing* sowie *SF-FUNK-Automatisierung* und deren Bewertungen).
- Bisherige und in der Praxis verbreitete IDS-Architekturen sind überwiegend statisch oder betrachten nur Teilaspekte der dynamischen Rekonfiguration wie beispielsweise das Hinzufügen weiterer, dauerhaft aktiver Sensoren zum Gesamtsystem. Das volle Potenzial der dynamischen Rekonfiguration und die mit ihm verbundenen Möglichkeiten zur Verbesserung der Ressourcennutzung und zur Optimierung der Erkennungsleistung werden noch nicht genutzt.

Das erarbeitete Werkzeugkonzept trägt somit sowohl zur Weiterentwicklung dynamischer IDS-Architekturen unter dem Blickwinkel der verbesserten und ressourcenoptimierten Erkennungsleistung als auch zur Nutzbarmachung eines Schlüsselkonzepts von Security-Frameworks bei. Hierzu wird im folgenden Abschnitt zunächst eine Abgrenzung gegenüber bisherigen und verwandten Arbeiten vorgenommen; die weiteren Ausführungen setzen diese Lösungsansätze als gegeben und funktionsfähig voraus und konzentrieren sich auf die für die Dynamik und für Security-Frameworks spezifischen Aspekte. In Abschnitt 7.2.2 wird das erarbeitete Architekturkonzept für Sensoren und Auswertestationen vorgestellt. Die Abläufe im Rahmen der Ereignisanalyse und die Vorbereitung automatisierter Reaktionen werden in Abschnitt 7.2.3

spezifiziert. In Abschnitt 7.2.4 wird ein Informationsmodell konzipiert, das insbesondere die durch Security-Frameworks vorgegebene potentielle Vielzahl und den dynamischen Einsatz der einzelnen Sensoren berücksichtigt. Das erarbeitete Funktionsmodell für die Spezifikation von Auswertungs- und Steuerungsregeln wird in Abschnitt 7.2.5 beschrieben. Anschließend wird in Abschnitt 7.2.6 ein diese Konzepte zusammenfassendes und erläuterndes Anwendungsbeispiel gegeben, das neben einer Beschreibung des entsprechenden Szenarios auch eine exemplarische Regelimplementierung und eine simulationsgestützte Analyse und Bewertung des Ablaufs umfasst. In Abschnitt 7.2.7 wird auf die für Security-Frameworks spezifische prozessuale Einbettung des Einsatzes des spezifizierten Werkzeugs eingegangen, bevor in Abschnitt 7.2.8 schließlich eine zusammenfassende Bewertung der erreichten Ziele und noch offenen Punkte vorgenommen wird.

7.2.1. Abgrenzung zu verwandten Arbeiten im Bereich der Intrusion Detection Systeme

Die Angriffserkennung auf Basis netz- und systemspezifischer Sensorik wird erforscht und praktiziert, seit die Möglichkeiten entsprechenden Missbrauchs durch Sicherheitsvorfälle evident wurden. Vigna gibt in [Vig10] einen Überblick über die historische Entwicklung von IDS und ihre Meilensteine; er kommt zu dem Schluss, dass sich die schon in den 1990er Jahren geschaffenen Grundlagen im Kern immer noch unverändert auch in aktuellen IDS-Implementierungen finden.

Intrusion Detection gehört somit zu den Themen der IT-Sicherheit, an denen seit mehr als 20 Jahren kontinuierlich aktiv geforscht wurde, so dass im Rahmen des vorgelegten Werkzeugkonzepts auf umfassende Vorarbeiten zurückgegriffen werden kann. Im Folgenden wird deshalb dargelegt, welche bereits vorhandenen Konzepte als Basis genutzt werden, in welchen Teilbereiche neue Aspekte eingebracht werden und welche Themen im vorliegenden Konzept bewusst *nicht* betrachtet werden, da sie Gegenstand anderer laufender Arbeiten sind.

Ausschlaggebend für die Erkennungsleistung eines IDS sind immer seine Sensoren, die in der Regel durch die Beobachtung der aktuellen Nutzung eines Systems oder Netzes Angriffe erkennen und an eine Analysestation melden. Vereinzelt greifen Sensoren über die rein passive Beobachtung hinausgehend auch aktiv stimulierend ein, um ihre Diagnose präzisieren zu können. In der wissenschaftlichen Literatur wurden diesbezüglich bereits u. a. die folgenden Aspekte behandelt:

- **Erkennungsleistung:** Zur Verbesserung der *quantitativen* Erkennungsleistung wurden verschiedenste Angriffsarten und -varianten in ihre Einzelschritte zerlegt und beispielsweise durch exakte oder bewusst unscharf gehaltene Regelwerke, z. B. für die so genannte Deep Packet Inspection, diagnostiziert. Aktuelle IDS-Implementierungen enthalten Hunderte vorgefertigter Regelsätze zur Detektion bekannter Angriffsarten, die von den Herstellern – vergleichbar mit Updates für Antiviren-Software – zum Teil mehrfach täglich aktualisiert werden. Zur *qualitativen* Verbesserung wurden insbesondere Maßnahmen zur Reduktion von Fehlalarmen (*false positives*) untersucht. Das hier vorgelegte Werkzeugkonzept trägt zur Verbesserung der Erkennungsleistung demgegenüber dadurch bei, dass zusätzliche Sensoren und deren modulare Regelwerke bedarfsorientiert zugeschaltet werden, um u. a. die Diagnose präzisieren und möglichst nah an der Angriffsquelle oder dem Angriffsziel positionierte Sensoren nutzen zu können.

- **Sensorplatzierung:** Die Auswahl und Positionierung einzelner Sensoren verfolgt das Ziel, mit einer zur Optimierung der Gesamtkosten möglichst minimalen Anzahl von Sensoren möglichst viele Angriffe so zuverlässig wie möglich erkennen zu können. In [NJ07] wird gezeigt, dass diese Zielsetzung zum klassischen, NP-vollständigen Mengenüberdeckungsproblem äquivalent ist und in großen, komplexen Netzen deshalb beispielsweise auf Greedy-Algorithmen zur Annäherung an eine optimale Lösung zurückgegriffen werden muss; der Einsatz anderer Verfahren wie beispielsweise Model-Checking skaliert aufgrund des zu betrachtenden, exponentiell wachsenden Zustandsraums nicht ausreichend.

  Im in dieser Arbeit betrachteten Fall werden die Sensoren jedoch nicht frei platziert; vielmehr wird auf die von Security-Frameworks bereits vorgesehenen Sensoren, die üblicherweise ortsunveränderlich betrieben werden, genauso zurückgegriffen wie auf weitere, bereits vorhandene Sensoren, deren Position bereits anderweitig festgelegt wurden.

  Analog zu [SCN+09] wird auch für die nachfolgenden Betrachtungen grob differenziert, ob ein Sensor für ein gesamtes Netz (Backbone-Sensor), einen Teil davon (Subnet-Sensor) oder ein einzelnes Endgerät (Host-Sensor) eingesetzt wird. [RRSM06] geht vertiefend darauf ein, wie Sensoren für topologiespezifische Angriffe – beispielsweise das Fälschen der Absenderadresse von IP-Pakten – konfiguriert werden müssen; diesbezüglich wird nachfolgend davon ausgegangen, dass die in Security-Frameworks integrierten Erkennungsalgorithmen bereits adäquat parametrisiert sind, so dass es ausreicht, einzelne Sensormodule ggf. erst nachzuladen und dann zu aktivieren. Ebenso wird nachfolgend nicht darauf eingegangen, wie aus der Analyse der Differenz zwischen den vom IDS detektierten und den anderweitig erkannten Angriffen auf die Notwendigkeit zusätzlicher Sensoren geschlossen werden kann; diesbezüglich betrachtet [CCS+10] den nach oben hin abnehmenden Zugewinn an Erkennungsleistung pro weiterem Sensor in Relation zur damit ebenfalls zunehmenden Anzahl an Fehlalarmen.

- **Dynamik:** Unter der *dynamischen Rekonfiguration* wird in der bisherigen Literatur vorrangig die Eigenschaft von IDS-Implementierungen verstanden, zusätzliche Sensoren und Auswertungsregeln ohne einen Neustart der Analysestationen integrieren zu können. Damit soll insbesondere vermieden werden, dass Angriffe nicht erkannt werden, weil Sicherheitsmeldungen während des Neustarts verloren gehen und für die weiteren Analysen nicht herangezogen werden können.

  Eine bedarfsorientierte Rekonfiguration von Sensoren wird von Vigna, Kemmerer und Blix in [VKB01] vorgeschlagen. Die dort vorgestellte Lösung mit den Namen MetaSTAT sieht jedoch lediglich einen einzigen Typ eines programmierbaren Sensors vor, in den zur Laufzeit angriffsspezifische Analyseregeln eingespielt werden können. Dadurch wird weder der in dieser Arbeit erzielte hohe Grad an Dynamik erreicht noch können bestehende andere Sensoren integriert werden, so dass MetaSTAT nicht mit Security-Frameworks eingesetzt werden kann, die keine expliziten MetaSTAT-Sensoren vorsehen. Auch bezüglich der Auswahl zu aktivierender MetaSTAT-Module wird nicht die mit der in Abschnitt 7.2.5 spezifizierten Regelsprache erzielte Flexibilität erreicht.

- **Verteilte und kooperative IDS:** Sobald die Anzahl der von einer wachsenden Vielzahl an Sensoren gemeldeten Ereignisse implementierungsspezifische Schwellenwerte übersteigt, können diese nicht mehr von einer einzigen, zentralen Analysestation ausgewertet werden, da diese überlastet wird. *Verteilte* IDS bestehen deshalb aus einem

meist hierarchisch strukturierten Geflecht mehrerer Analysestationen, wobei meist eine 1:n-Zuordnung von Analysestationen zu Sensoren durchgeführt wird und die Ergebnisse der Analysestationen ebenfalls wieder meist hierarchisch aggregiert werden. Durch die damit mögliche dezentrale Vorverarbeitung wird eine auch für komplexe Szenarien ausreichende Skalierbarkeit erzielt, wobei u. a. zusätzliche Komponenten, die ausfallen können, und die sich beispielsweise durch eine Vorfilterung ergebenden Auswirkungen auf die Gesamterkennungsleistung berücksichtigt werden müssen. Im hier erarbeiteten Werkzeugkonzept wird hingegen lediglich *eine* zentrale Auswertestation betrachtet, ohne dass sich daraus Einschränkungen für den Einsatz in einer verteilten IDS-Architektur ergeben: Die explizit betrachteten Schnittstellen zur Meldung von Sicherheitsvorfällen an SIEM-Systeme können sinngemäß auch als Schnittstellen zu anderen Analysestationen oder Ergebnisaggregatoren betrachtet werden.

Kooperative IDS stellen Verbünde autarker IDS dar, durch die im Allgemeinen sowohl die Erkennungsleistung gesteigert als auch der Abdeckungsbereich vergrößert werden können. Gelten dabei alle Kooperationspartner als gleichberechtigt, wird die resultierende Gesamtarchitektur auch als *föderiertes* IDS bezeichnet. Kooperative bzw. föderierte IDS werden primär in organisationsübergreifenden Verbünden eingesetzt, da der parallele Betrieb mehrerer IDS-Architekturen innerhalb *einer* Organisation nur in seltenen Fällen ökonomisch sinnvoll ist, z. B. bei außerordentlich hohen Sicherheitsanforderungen im militärischen Bereich. Beispielsweise wird im Rahmen des Projekts GIDS ein föderiertes IDS für die Ressourcenanbieter und Nutzer von Grids am Beispiel des deutschen D-Grid-Verbunds implementiert (vgl. [HFvE+10, Fel08]).

Aus dem interorganisationalen Charakter ergeben sich bei kooperativen IDS allgemein zahlreiche Fragestellungen, die unter anderem die Informationsweitergabe unter Datenschutzaspekten, die Zuverlässigkeit der von anderen übermittelten Meldungen und die möglicherweise notwendige gemeinsame Nutzung einzelner Sensoren durch mehrere Analyseeinheiten betreffen. Zudem muss die in der Praxis aus dem Einsatz unterschiedlichster IDS-Produkte resultierende Heterogenität berücksichtigt werden, die unter anderem zahlreiche syntaktische und semantische Inkompatibilitäten mit sich bringt. In dieser Arbeit wird auf die speziellen Aspekte kooperativer IDS und die in diesen zu betrachtenden Auswirkungen der hier konzipierten Dynamikeigenschaften nicht eingegangen; Architekturkonzepte und Analysealgorithmen speziell für dynamische, kooperative IDS sind Gegenstand der laufenden Forschungsarbeit von Felix von Eye [vE].

Die beim Einsatz von Security-Frameworks üblicherweise vorliegende Vielzahl an Sensoren wird somit in dieser Arbeit nicht unter Kostengesichtspunkten betrachtet, sondern im Hinblick auf die möglicherweise resultierende Flut an zutreffenden Sicherheitsmeldungen und Fehlalarmen. Insbesondere wird angenommen, dass die Menge der zu verschiedenen Zeitpunkten zur Sicherstellung der Erkennungsleistung benötigten Sensoren in Abhängigkeit von den jeweils aktuellen Angriffen variiert und möglichst klein zu halten ist. Ein selektives Zu- und Abschalten von Sensoren und deren Erkennungsmodulen verbessert deshalb die Effizienz der Ressourcennutzung und reduziert gleichzeitig die Anzahl unnötiger Meldungen, wodurch auch die zentralen Auswertestationen entlastet werden. Implizit wird dadurch auch betrachtet, wie die durch den Einsatz von Security-Frameworks ohne explizite Mehrkosten verfügbare Sensorik in vorhandene IDS-Architekturen integriert und genutzt werden kann. Zudem wird berücksichtigt, dass seitens der Security-Frameworks bereits eine Vorfilterung und Aggrega-

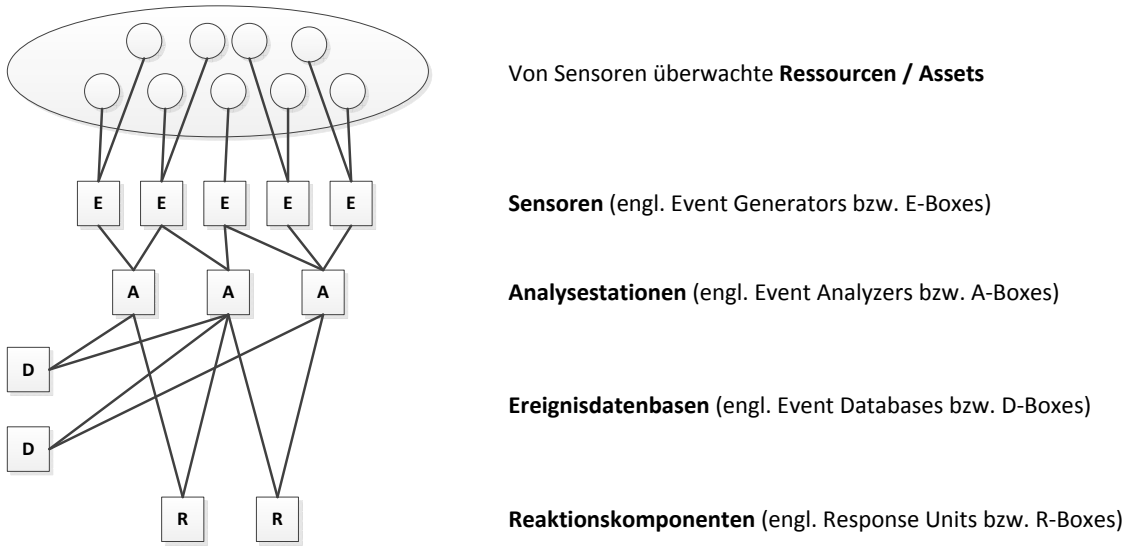


Abbildung 7.2.: Prinzipielle IDS-Gesamtarchitektur auf Basis des Common Intrusion Detection Frameworks

tion bestimmter Sicherheitsereignisse vorgenommen werden kann.

7.2.2. Architekturkonzept für Sensoren und Auswertestationen

Die hier erarbeiteten Neuerungen und Besonderheiten beziehen sich auf die interne Struktur und die internen Abläufe in Sensoren und Auswertestationen, die im Rahmen eines IDS konzertiert eingesetzt werden. Die in Abbildung 7.2 schematisch dargestellte IDS-Gesamtarchitektur deckt sich deshalb mit herkömmlichen IDS-Ansätzen und folgt den etablierten Konzepten der Common Intrusion Detection Framework (CIDF) Architecture [PSSC+99]; dabei sind die folgenden vier Arten von Komponenten zu unterscheiden:

1. **Event generators**, häufig auch als *E-Boxes* bezeichnet, entsprechen der Sensorik und dienen, wie ihr Name bereits impliziert, der Erzeugung von Sicherheitsereignismeldungen, die beispielsweise beim Erkennen von Regelverstößen oder durch heuristische Algorithmen angestoßen wird. Im Folgenden wird der in der deutschen Literatur weiter verbreitete Begriff *Sensor* verwendet.
2. **Event analyzers**, die auch als *A-Boxes* bekannt sind und im Deutschen als Analysestationen bezeichnet werden, verarbeiten die von Sensoren erzeugten Ereignismeldungen. Im Allgemeinen besteht eine *n:m*-Zuordnung von *E-* zu *A-Boxes*, wobei die in der Praxis vorherrschenden Installationen mehrere Sensoren genau einer Analysestation zuordnen. Für den Fall, dass Sensoren nicht direkt mit Analysestationen kommunizieren können, existieren Gateway- und Proxy-basierte Lösungsansätze, die im Folgenden jedoch keine Rolle spielen.
3. **Event databases** oder *D-Boxes* dienen der persistenten Speicherung von Ereignismeldungen. Sie werden im Allgemeinen als Hintergrundspeicher für Analysestationen

genutzt, um ereignisübergreifende Korrelationen auch über längere Zeiträume hinweg vornehmen zu können. In verteilten IDS-Architekturen können diese Datenbasen auch gemeinsam von mehreren Analysestationen und somit zum Informationsaustausch verwendet werden.

4. **Response units**, die oft als *R-Boxes* abgekürzt und im Folgenden als Reaktionskomponenten bezeichnet werden, werden durch die Analysestationen angestoßen und führen vorgegebene, mit den Details des aktuellen Angriffs parametrisierbare Aktionen durch, zu denen beispielsweise das Versenden von E-Mails oder die Rekonfiguration von Sicherheitsmechanismen zählen können. Allgemein kann wiederum von einer *k:m*-Zuordnung von Reaktionskomponenten zu Analysestationen ausgegangen werden.

Mit dieser Arbeit wird darüber hinaus das Konzept der *Auswertestationen* eingeführt: Unter einer Auswertestation wird eine Kombination aus einer Analysestation und einer solchen Reaktionskomponente verstanden, die einer dynamischen Rekonfiguration des IDS selbst oder der push-basierten Weitergabe von Ereignismeldungen an übergeordnete Systeme dient. Soll also beispielsweise als Reaktion auf die Analyse eines Ereignisses ein zusätzlicher Sensor aktiviert werden, so kann der gesamte Vorgang von einer Auswertestation abgewickelt werden, ohne dass separate Analysestationen und Reaktionskomponenten betrachtet werden müssen. Davon losgelöst kann es weiterhin eigenständige Reaktionskomponenten geben, die von einer Auswertestation angestoßen werden. Ebenfalls über die CIDF-Architektur hinausgehend werden Ereignisdatenbasen nicht nur für das Speichern und Auslesen von Informationen durch Auswertestationen genutzt, sondern fungieren auch als Kommunikationsschnittstelle für den pull-basierten Informationsabruf durch andere Komponenten, beispielsweise ITSM-Werkzeuge; dies wird in Abschnitt 7.2.7 vertieft.

Im Folgenden werden die Architektur und die inneren Abläufe sowohl der einzelnen Sensoren als auch der Auswertestationen erarbeitet. Abbildung 7.3 zeigt den generischen Aufbau eines Sensors. Es muss beachtet werden, dass bereits vorhandene Sensoren, die beispielsweise in Komponenten von Security-Frameworks integriert sind, nicht zwingend alle Sensorbestandteile in vollem Umfang ausprägen; auf die damit möglicherweise verbundenen funktionalen Einschränkungen wird im Rahmen der Konzeption der Auswertestationen näher eingegangen. Jeder Sensor dient der Überwachung einer Menge an Ressourcen und besteht aus den folgenden, aufeinander aufbauenden Teilen:

1. **Messdatenakquisition**: Die Überwachung der Ressourcen durch den Sensor erfordert zunächst die Erfassung von Rohdaten, beispielsweise durch die Beobachtung des gesamten Netzverkehrs in einem Subnetz oder die Überwachung einer Systemprotokolldatei auf einem Server. Die erforderlichen Messdaten können in den meisten Fällen rein *passiv* durch Beobachtung der Netz- und Systemaktivitäten gewonnen werden; Sensoren können jedoch auch *aktiv* eingreifen und beispielsweise Messwerte von den überwachten Ressourcen über ein explizites Request-Response-Protokoll abrufen. Das Vorgehen bei der aktiven wie auch bei der passiven Messdatenakquisition kann im Allgemeinen über Parameter gesteuert werden.

   Während primitive Sensoren lediglich eine Art von Ressourcen überwachen können und dabei starren Abläufen folgen, wird im Folgenden von einer Modularität der Sensoren ausgegangen, die sich auch auf die nachfolgend unter 2.–5. beschriebenen Sensorteile auswirkt. Insbesondere sollen einzelne Überwachungsverfahren und Filterregeln dynamisch zu- und abgeschaltet sowie dynamisch parametrisiert werden können. Im Extremfall

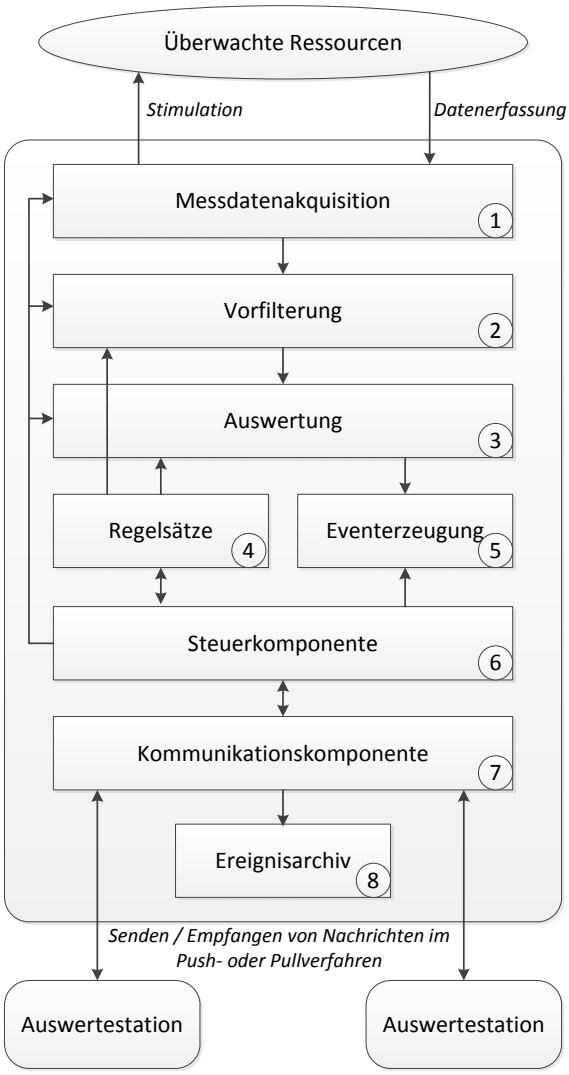


Abbildung 7.3.: Architektur der konzipierten Sensoren

ist der Sensor ähnlich zum oben skizzierten MetaSTAT-Verfahren frei programmierbar und kann zur Laufzeit von einer Auswertestation beliebig modifiziert werden. Im Hinblick auf eine praktische Umsetzbarkeit und Anwendbarkeit wird nachfolgend vereinfacht nur der Fall betrachtet, dass bereits vorgefertigte Module zur Präzisierung der Diagnostik zugeschaltet werden sollen: Überwacht ein Sensor beispielsweise den Netzverkehr zwischen einem Webserver und einem relationalen Datenbankmanagementsystem, so soll der Bedarf abgedeckt werden, die Datenpakete über ein zusätzliches Modul auf SQL-Injection-Angriffe analysieren zu können. Da die hierfür erforderliche Deep Packet Inspection mit einem erhöhten Rechenaufwand verbunden ist, soll das Modul zur SQL-Injection-Analyse in diesem Beispielfall nicht kontinuierlich, sondern nur bedarfsgesteuert aktiv sein.

2. **Vorfilterung**: In allen Szenarien mit gewöhnlichem Schutzbedarf überwiegt die reguläre Nutzung der Infrastruktur deutlich, d. h. Angriffe stellen in Relation dazu seltene Ereignisse dar. Ein Großteil der akquirierten Überwachungsdaten ist somit mit unbedenklicher, erwünschter Nutzung verbunden und kann ohne Auswirkung auf die Angriffserkennungsleistung ignoriert werden. Die von Sensoren durchzuführende Vorfilterung basiert deshalb häufig auf einfachen, effizient implementierten Vergleichsoperationen, so dass z. B. anhand einer Positivliste alle trivial als unkritisch einzustufenden Messdaten verworfen werden können und lediglich alle anderen Informationen nachfolgend näher betrachtet werden müssen. Wie oben bereits angedeutet sind auch die Filterregeln an die aktuell aktivierten Module gekoppelt und können dem aktuellen Bedarf angepasst werden.

3. **Auswertung**: Da jeder Sensor autark Angriffe erkennen und melden können soll, muss er eine Komponente zur Auswertung der erfassten und vorgefilterten Messdaten enthalten. Im einfachsten Fall stellt jedes nicht vorab ausgesiebte Datum ein sicherheitsrelevantes Ereignis dar. Allgemein kommen jedoch komplexere Auswertungsmechanismen zum Einsatz, die auf den jeweiligen Sensortyp und seine Module zugeschnitten sind: Ein Sensormodul zur Auswertung von Systemprotokolldateien wird sich beispielsweise auf die zeilenorientierte Auswertung von Zeichenketten, z. B. unter Anwendung regulärer Ausdrücke, spezialisieren, wohingegen ein Netzsensor beispielsweise Funktionen zur Analyse von TCP- und IP-Headern bereitstellt. Als Ergebnis der Auswertung ist eine Entscheidung zu liefern, ob das analysierte Datum auf einen Angriff hinweist oder ignoriert werden kann.

4. **Regelsätze**: Die Vorfilterung und die Auswertung werden über Regelsätze gesteuert, welche die von den beiden anderen Komponenten bereitgestellten Funktionen nutzen. Bei dieser Sensorkomponente handelt es sich somit um eine in den Sensor integrierte Regeldatenbasis, deren aktuelle Inhalte ebenfalls von den Auswertestationen festgelegt werden können.

5. **Eventerzeugung**: Sobald der Fall eintritt, dass die Auswertung der Messdaten ergeben hat, dass vermutlich ein Angriff vorliegt – oder alternativ explizit Entwarnung gegeben werden kann – hat der Sensor die Aufgabe, die für ihn im jeweiligen Einzelfall relevanten Auswertestationen zu informieren. Die Sensorkomponente zur Eventerzeugung muss somit das ausgewertete Datum durch Datenkonversion und Ergänzung der lokalen Diagnose in ein Sicherheitsereignis umwandeln. Für die Kodierung der Ereignisinhalte wird dabei wiederum auf das bereits mehrfach in dieser Arbeit verwendete IDMEF-Standardformat zurückgegriffen. Im Rahmen der Eventerzeugung muss darüber hinaus die Metainformation festgelegt werden, an welche Auswertestationen das Ereignis kommuniziert werden soll. Die so erstellten Ereignismeldungen werden an die unter Punkt 7. beschriebene Kommunikationskomponente übergeben.

6. **Steuerkomponente**: Die Aktivitäten des Sensors werden zum einen angestoßen, wenn neue zu verarbeitende Messdaten der überwachten Ressourcen akquiriert wurden; zum anderen können von den für den Sensor zuständigen Auswertestationen Anweisungen, beispielsweise zur dynamischen Rekonfiguration, eingehen. Die in den Sensor integrierte Steuerkomponente koordiniert die Umsetzung dieser Steueranweisungen und verwaltet somit die aktuelle Konfiguration und Parametrisierung der anderen Sensorkomponenten. Sie kann darüber hinaus zur Sicherstellung der Autarkie und lokalen Autonomie

des Sensors auf Basis vorgegebener Regelsätze eigene Steueranweisungen generieren und umsetzen. Beispielsweise können autonom zur Schärfung der Diagnostik lokal bereits vorhandene Module aktiviert oder nach einiger Zeit, in der diese keine Angriffe verzeichnen, auch wieder automatisch deaktiviert werden, ohne dass die Auswertestation eine diesbezügliche explizite Anweisung senden muss. Derartige autonome Vorgänge dürfen jedoch nicht dazu führen, dass die Auswertestation in eine zur Realität inkonsistente Sicht auf den aktuellen Betriebsstatus gelangt. Im Regelfall wird die Steuerkomponente deshalb eine Ereignismeldung generieren, mit der die angeschlossenen Analysestationen über die lokal initiierten Veränderungen informiert werden.

Das Informieren der Analysestation über lokal ausgelöste Konfigurationsmodifikationen ist insbesondere auch für die Situation relevant, in der ein Systemadministrator eine regionale Änderung vornimmt, die sich auch auf den Sensor auswirkt – beispielsweise, falls ein Server, auf dem ein Host-IDS-Sensor installiert ist, für Wartungsarbeiten heruntergefahren und somit auch der Sensor geordnet beendet wird. Entsprechende Meldungen können auch Hinweise auf Angriffe, die sich gezielt gegen den Sensor und nicht die von ihm überwachten Ressourcen wenden, liefern.

7. **Kommunikationskomponente**: Die Kommunikationskomponente übernimmt die Kommunikation mit den für den Sensor relevanten Auswertestationen. Erweiterungen, die einen Informationsaustausch zwischen Sensoren ermöglichen, sind denkbar, werden in dieser Arbeit jedoch nicht näher betrachtet. Die Kommunikationskomponente empfängt Steueranweisungen von Auswertestationen, die von dieser in einem Push-Verfahren ausgeliefert werden. Die Übermittlung von Ereignismeldungen an jede Auswertestation kann hingegen entweder auf Push- oder auf Pull-Basis erfolgen:

   - Durch das Senden einer Ereignismeldung vom Sensor an die Auswertestation im Push-Verfahren kann die zeitnahe Weitergabe der Angriffsinformationen erreicht werden; im Allgemeinen ist dies die zu bevorzugende und auch in bisherigen IDS am häufigsten implementierte Variante.
   - Im Pull-Modell macht der Sensor die Ereignismeldungen einer Auswertestation lediglich auf Abruf verfügbar, unternimmt jedoch keine aktiven Zustellversuche. Diese Variante kann überall dort eingesetzt werden, wo beispielsweise aufgrund von Netzzonenkonzepten und Paketfilterfirewalls kein Verbindungsaufbau von außen auf die Auswertestation zugelassen wird oder wo die Auswertestationen, z. B. zur Vermeidung von Überlastsituationen, nur selektiv auf die Daten ausgewählter Sensoren zugreifen möchten. Das Pull-Verfahren ermöglicht zudem eine i. A. ressourcenschonendere Übertragung mehrerer Ereignisse am Stück und kann auch eingesetzt werden, wenn ein beispielsweise mobiler Sensor keine permanente Netzkonnektivität zur Auswertestation hat.

   In beiden Fällen kann die Kommunikationskomponente Ereignismeldungen durch Verwerfen auch bewusst unterdrücken; dies ist beispielsweise dann sinnvoll, wenn eine Vielzahl sehr ähnlicher Meldungen in einem kurzen Zeitraum keinen wesentlichen Erkenntnisgewinn seitens der Auswertestation verspricht: Falls zum Beispiel innerhalb weniger Sekunden Hunderte von IP-Adressen einem Portscan unterzogen werden und somit bereits klar ist, dass ein Angriff vom Typ Portscan vorliegt, könnte beispielsweise gewünscht werden, dass nur noch *eine* diesbezügliche Meldung pro zehn Sekunden an die

Auswertestation kommuniziert wird, um unnötig hohe Netz- und Rechenbelastung zu vermeiden.

8. **Lokales Ereignisarchiv**: An die Auswertestationen zu meldende Ereignisse können optional auch zusätzlich lokal gespeichert werden; neben sicherheitsrelevanten Ereignissen umfasst dies wiederum auch Angaben über autonom getroffene Entscheidungen und den Aktivierungsstatus einzelner Module. Aufgrund der in Sensoren häufig beschränkten lokalen Speicherkapazität kann beispielsweise ein Ringpuffer eingesetzt werden, in dem die letzten n Ereignisse verzeichnet werden. Eine Auswertung dieser Protokollinformationen ist beispielsweise im Rahmen der IT-Forensik relevant, wenn ein Angreifer erfolgreich und möglicherweise gezielt die Kommunikation zwischen Sensor und Auswertestation unterbunden hat, der Vorfall aber anderweitig bemerkt und nachträglich rekonstruiert werden soll.

Die Komponenten 1–5 entsprechen – abgesehen von der dynamischen Zu- und Abschaltung von Modulen und Regelsätzen, die unten noch näher betrachtet werden – herkömmlichen IDS-Sensoren. Aus diesem Grund wird in dieser Arbeit nicht näher darauf eingegangen, welche Regelsprachen zum Einsatz kommen sollen oder welche Funktionalität die Auswerteeinheit zur inhaltlichen Analyse von Meldungen bieten muss. Auf die Aspekte der Dynamik und die damit verbundenen Aufgaben der konzeptionell neuen Komponenten 6–8 wird im Folgenden verstärkt aus der Perspektive der Auswertestationen eingegangen, denen aufgrund des dort verfügbaren Gesamtüberblicks die übergeordnete Koordination aller Sensoren obliegt. Autonom von den in Sensoren integrierten Steuerkomponenten initiierte Vorgänge können sinngemäß als Teilmenge davon aufgefasst werden, werden hier jedoch nicht vertieft, um inhaltliche Redundanzen zu vermeiden. Ebenso wird nicht im Detail betrachtet, dass insbesondere die in Security-Frameworks bereits enthaltene Sensorik oftmals bereits von einer frameworkspezifischen Managementkomponente gesteuert wird: In diesem Fall hat diese Managementkomponente gegenüber der IDS-Auswertestation konzeptionell als Sensor zu fungieren und die Steueranweisungen entsprechend für die einzelnen Komponenten des Security-Frameworks aufzubereiten; diese Situation ist grundsätzlich mit dem Einsatz von Proxies zur Kommunikation in herkömmlichen, CIDF-konformen Architekturen zu vergleichen und kann somit aus IDS-Perspektive als bereits gelöste Problemstellung betrachtet werden.

Abbildung 7.4 gibt einen Überblick über den viergeteilten Aufbau der Auswertestationen:

1. **Sensorkommunikation**: Die Komponente zur Sensorkommunikation übernimmt den Datenaustausch mit allen an die Auswertestation angeschlossenen Sensoren. [GS01] trägt die Anforderungen an die Eigenschaften des Kommunikationswegs zwischen IDS-Sensoren und Analysestationen zusammen: Die Kommunikation muss zuverlässig erfolgen, so dass keine Nachrichten verloren gehen; die grundlegenden Sicherheitseigenschaften Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit sowie ein grundlegender Schutz vor Denial-of-Service-Angriffen müssen gegeben sein; schließlich muss auch die Skalierbarkeit gewährleistet werden, um auch in großen, komplexen Netzstrukturen alle IDS-Nachrichten schnell an die richtigen Analysestationen ausliefern zu können.

   Als Basis für das Kommunikationsprotokoll wird im Folgenden das Intrusion Alert Protocol (IAP, [GBFP01]) verwendet: Es entstand im Umfeld der Arbeiten am CIDF sowie am IDMEF-Standard, sieht mittels Transport Layer Security (TLS) authentifizierte und verschlüsselte Datenverbindungen vor, enthält im Grundumfang den Transport von IDMEF *Alerts* sowie *Heartbeats* und kann um weitere zu übertragende Inhalte erweitert

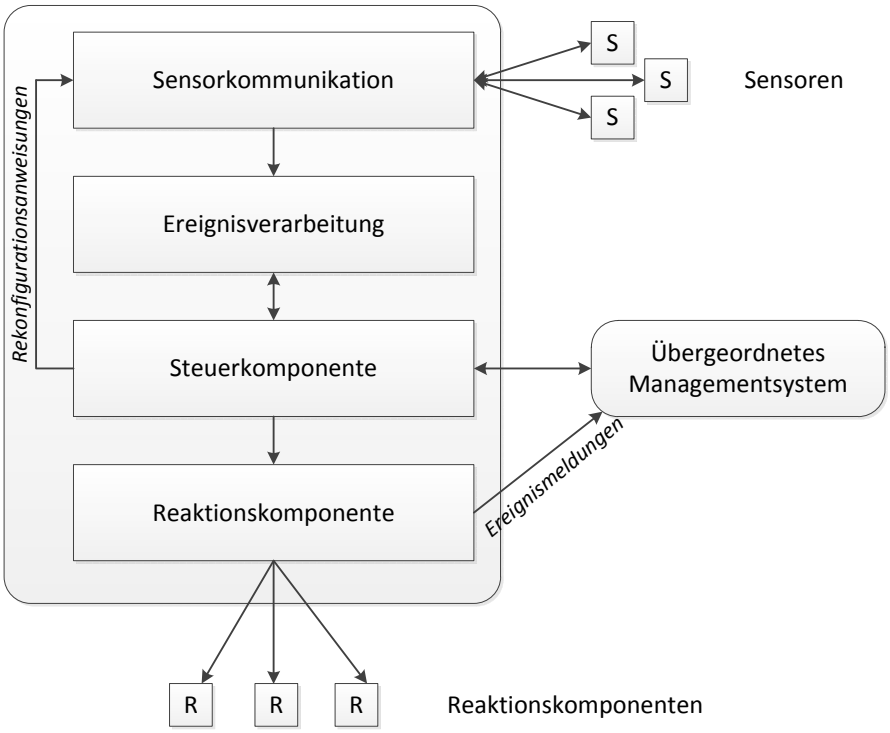


Abbildung 7.4.: Architektur der konzipierten Auswertestation

werden. Über die IDMEF Alerts und Heartbeats wird bereits die Basisfunktionalität zur Übertragung der von Sensoren erzeugten Sicherheitsmeldungen und zur auswertestationsseitigen Überprüfung, ob der Sensor aktuell verfügbar ist, abgedeckt.

Zur Unterstützung der in dieser Arbeit konzipierten Dynamikeigenschaften werden folgende Erweiterungen notwendig, die mit den in Abschnitt 7.2.5 spezifizierten Funktionen korrelieren:

- Übertragen neuer oder modifizierter
  - Module,
  - Regelsätze und
  - Konfigurationsparameter

  von der Auswertestation auf den Sensor. Hierbei müssen sensorseitige Einschränkungen berücksichtigt werden, auf die auch im Rahmen des Informationsmodells in Abschnitt 7.2.4 eingegangen wird.
- Aktivieren bzw. Deaktivieren einzelner Sensormodule und Regeln bzw. Regelsätze durch die Auswertestation.
- Abruf
  - bereitgestellter Ereignismeldungen,
  - der Inhalte des Sensor-Ereignisarchivs und sonstiger Sensorstatistiken,

  - der Liste aktuell installierter bzw. aktivierter Sensormodule sowie deren derzeitige Parametrisierung und der sensorseitig gespeicherten Regelsätze

  vom Sensor durch die Auswertestation (vgl. Pull-Modell der Sensor-Kommunikationskomponente oben).

- Auslesen bzw. Modifizieren der Grundkonfiguration des Sensors, die u. a. steuert, welche Arten von Ereignissen der Sensor für welche Auswertestationen erzeugen soll, durch die Auswertestation.
- Information der Auswertestation über sensorseitig autonom angestoßene Ereignisse wie das Aktivieren bzw. Deaktivieren von Modulen und Regeln, die Änderung von Konfigurationsparametern und erkannte Fehler- bzw. Ausnahmesituationen wie gegen den Sensor selbst gerichtete Angriffe.

Im Hinblick auf spätere Erweiterungen in Richtung eines zusätzlichen Informationsaustausches untereinander zwischen Sensoren und zwischen Auswertestationen muss zudem sichergestellt werden, dass Duplikate erkannt werden können; beispielsweise könnte hierzu jede übertragene Nachricht mit einem eindeutigen Identifikator gekennzeichnet werden.

2. **Eventverarbeitung**: Die Verarbeitung der von den Sensoren gemeldeten Sicherheitsereignissen folgt den in Abschnitt 7.2.3 spezifizierten Abläufen. Die meisten Schritte entsprechen den auch in herkömmlichen IDS im Rahmen der Analysestationen implementierten Vorgängen; als neue Erweiterung dieser existierenden Konzepte wird unten die Schnittstelle zur dynamischen Rekonfiguration spezifiziert.
3. **Steuerkomponente**: Analog zur bei Sensoren beschriebenen Steuerkomponente hat dieser Bestandteil der Auswertestation die Aufgaben, einerseits sämtliche internen Abläufe zu koordinieren und andererseits das Zusammenspiel mit übergeordneten und verwandten Systemen zu arrangieren, beispielsweise also mit Sicherheitsmanagementplattformen und ITSM-Werkzeugen. In Abschnitt 7.2.4 wird dazu zunächst die Verwaltung der an die Auswertestation angeschlossenen Sensoren mit ihren jeweiligen Fähigkeiten konzipiert. Anschließend wird in Abschnitt 7.2.5 der Funktionsumfang einer Regelsprache für die Steuerung der Dynamik unter Berücksichtigung der oben konzipierten Erweiterungen für die Kommunikationsschnittstelle erarbeitet. Auch die Betrachtung des daran anknüpfenden Anwendungsbeispiels geht von den Abläufen in dieser Komponente aus.
4. **Reaktionskomponente**: Die Reaktionskomponente ist für die interne Umsetzung der dynamischen IDS-Rekonfiguration, die sich aus der Eventverarbeitung im Zusammenspiel mit der Steuerkomponente ergibt, zuständig und bildet die technische Schnittstelle zu weiteren, externen Reaktionskomponenten. Sie kann somit beispielsweise vorhandene, dynamisch konfigurierbare Firewalls anweisen, bei einem akuten Angriff zusätzliche IP-Filterregeln aufzunehmen und später wieder zu verwerfen. Zur Auswahl und Ansteuerung dieser externen Werkzeuge greift sie ebenfalls auf die in Abschnitt 7.2.5 konzipierten Funktionen zurück.

Der interne Verarbeitungsablauf beim Eintreffen neuer Sensormeldungen stellt folglich die Ausgangsbasis für alle weiteren Aktionen dar und wird im nachfolgenden Abschnitt spezifiziert.

7.2.3. Ereignisanalyse und Reaktionsautomatisierung

In der vorgestellten Gesamtarchitektur haben die Auswertestationen die Aufgabe, Sensormeldungen zu verarbeiten und geeignet darauf zu reagieren; die hier zu betrachtende Reaktion besteht dabei entweder aus einer dynamischen Rekonfiguration des IDS und seiner Sensoren, durch die im Wesentlichen die Diagnosemöglichkeiten verbessert werden sollen, oder aus dem Anstoßen vorgegebener Abläufe, mit denen akuten oder inzwischen wieder abgeklungenen Angriffen begegnet werden soll. Die Auswertestation hat im Allgemeinen keine eigene, integrierte Sensorik und ist somit auf die Meldungen der externen Sensoren angewiesen. Eine Kernfragestellung bei der Konfiguration und Inbetriebnahme von IDS ist deshalb, welche Sensormeldungen an welche Auswertestationen übermittelt werden sollen. [GS01] beschreibt in diesem Kontext das *Interesse* einer IDS-Analysestation informell als die Menge der Arten von Ereignissen, über die die Analysestation aktuell informiert werden möchte. Dieses Interesse kann ferner wie folgt klassifiziert werden:

- Enthält die IDS-Gesamtarchitektur nur eine einzige Analysestation, so wird deren Interesse als *global* (*enterprise-wide*) eingestuft, da sie prinzipiell Ereignismeldungen von allen eingesetzten Sensoren auswerten wird; in verteilten IDS-Architekturen können zudem Analysestationen mit einem *regionalen* (*domain-specific*) oder rein *lokalen* (*local*) Interesse vorhanden sein.
- Das Interesse der Analysestation kann entweder *permanent* oder nur *temporär* vorhanden sein.
- Das Interesse kann *direkt* von den an die Analysestation angeschlossenen Sensoren abgedeckt werden, oder die entsprechenden Nachrichten müssen z. B. von anderen Analysestationen *propagiert* werden (*propagated interest*).

Herkömmliche IDS-Analysestationen werten lediglich die aktuell in ihrem Interesse liegenden Sensormeldungen aus; alle anderen empfangenen Ereignismeldungen werden nur darauf geprüft, ob sie im Rahmen eines *propagated interest* an andere Analysestationen weitergeleitet werden müssen, aber nicht lokal verarbeitet; eine Vielzahl von Sensormeldungen wird somit schlichtweg verworfen. Die in dieser Arbeit konzipierten Dynamikeigenschaften zielen darüber hinausgehend u. a. darauf ab, dass Sensoren zur Schonung ihrer eigenen Ressourcen und der Transportwege immer nur solche Ereignismeldungen generieren, die im aktuellen Interesse mindestens einer Auswertestation liegen.

Beim Eintreffen einer neuen Sensormeldung, die im Interesse der Auswertestation liegt, wird ihre Auswertung angestoßen. Der Auswertungsprozess entscheidet über die qualitative Erkennungsleistung und folgt auch im Rahmen des hier erarbeiteten Konzepts grundlegend dem Modell, das Kemmerer und Vigna in [KV05] darlegen. Abbildung 7.5 zeigt diese klassische Verarbeitungskette mit den im Rahmen dieser Arbeit vorgenommenen Erweiterungen:

1. Im ersten Schritt wird eine **Normalisierung** der Sensormeldung durchgeführt, um sicherzustellen, dass die von verschiedenen Sensortypen erzeugten Ereignismeldungen nachfolgend einheitlich verarbeitet werden können. Wie oben bereits diskutiert wurde, wird im Folgenden vereinfachend angenommen, dass die Meldungen bereits im IDMEF-Format vorliegen, so dass notwendige Datenkonvertierungen nicht näher betrachtet werden.

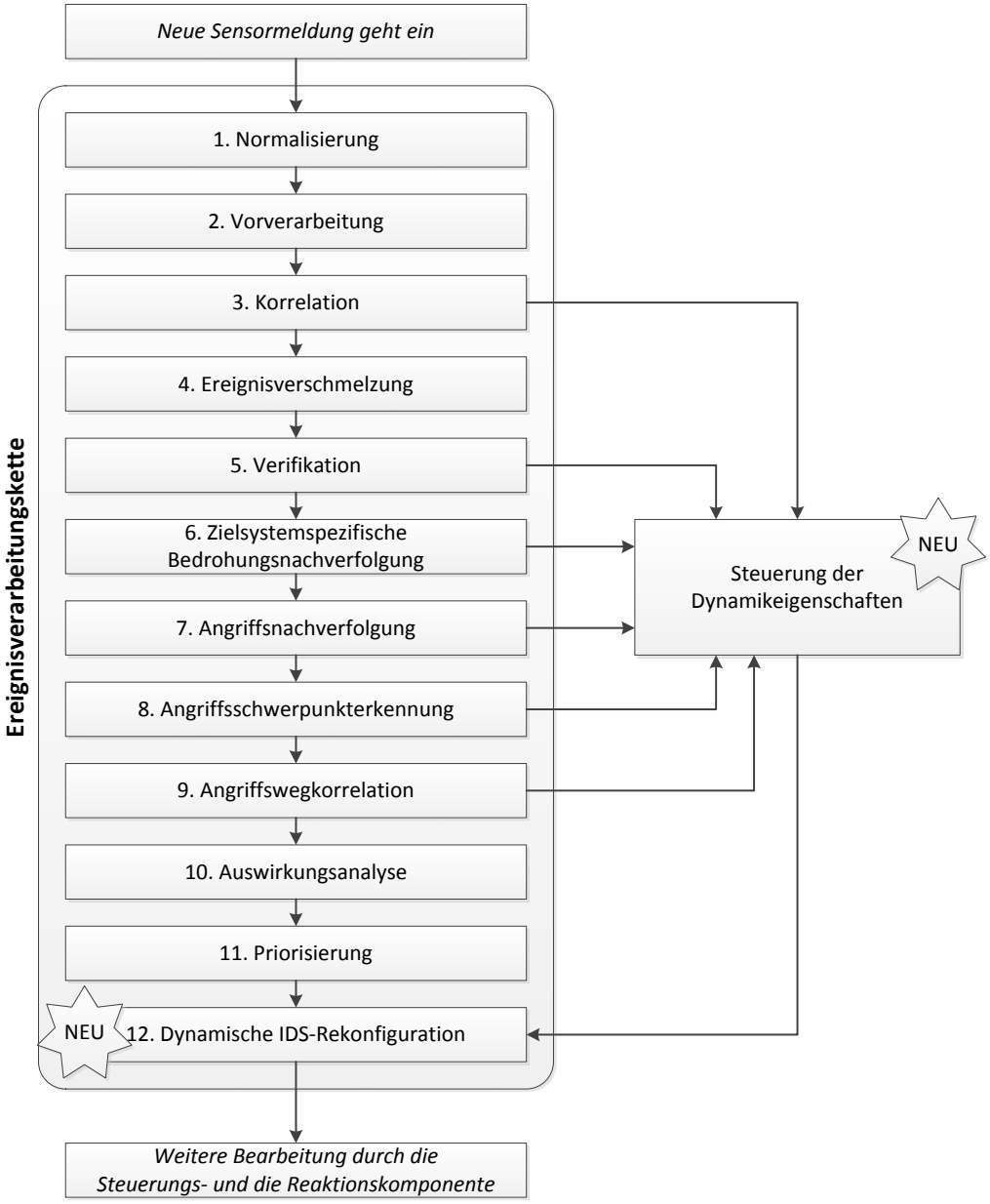


Abbildung 7.5.: Ereignisverarbeitungskette mit spezifischen Erweiterungen für die Dynamiksteuerung

2. Anschließend erfolgt eine **Vorverarbeitung**, die im Wesentlichen Plausibilitätsprüfungen durchführt, mit denen offensichtliche Sensordefekte oder absichtliche Störversuche erkannt werden können.

3. Im Rahmen der **Korrelation**, für die in der Literatur zahlreiche Vorgehensweisen und Algorithmen vorgeschlagen wurden, wird überprüft, ob sich die aktuelle Sensormeldung

zu bereits früher verarbeiteten Ereignissen in eine Beziehung setzen lässt, die auf einen bereits erkannten oder vermuteten Angriff hindeutet. Bei der Korrelation sind folglich sowohl zeitliche Aspekte als auch die topologische Relation des aktuell meldenden Sensors zur Quelle der früheren Ereignisse zu berücksichtigen. Bei diesem Schritt handelt es sich um den ersten in der Verarbeitungskette, der im Rahmen dieser Arbeit um eine Schnittstelle zur Steuerung der Dynamikeigenschaften erweitert wird: Für den Fall, dass das gemeldete Ereignis auf einen Angriff hinweist, der auch von weiteren Sensoren bzw. Sensormodulen zu beobachten sein müsste, die zum betrachteten Zeitpunkt jedoch deaktiviert sind, ergibt sich gegebenenfalls der Bedarf, weitere Sensorik zuzuschalten.

4. Durch die **Ereignisverschmelzung** (*event fusion*) werden mehrere unabhängig voneinander erkannte Ereignisse, die demselben Sicherheitsvorfall zugeordnet werden können, zusammengefasst. Über die von Kemmerer und Vigna vorgeschlagene rein IDS-interne Verwaltung dieser Information hinausgehend wird im Folgenden auch betrachtet, dass die so aktualisierten Aufzeichnungen über Sicherheitsvorfälle an übergeordnete Systeme propagiert werden können (vgl. hierzu die in Abschnitt 6.4.3 beschriebene Verwaltung von Sicherheitsvorfällen über Managementplattformen).

5. Durch einen Schritt zur **Verifikation** wird anschließend überprüft, ob es sich tatsächlich um einen Angriff handelt und ob dieser erfolgreich war. Hierbei spielt einerseits die Zuverlässigkeit des meldenden Sensors eine Rolle, da Fehlalarme (*false positives*) praktisch kaum ausgeschlossen werden können; andererseits sind in den nachfolgenden Schritten erfolglose Angriffe anders zu behandeln als erfolgreiche. Auch in diesem Schritt, der maßgeblich zur qualitativen Erkennungsleistung beiträgt, müssen neue Schnittstellen zur Steuerung der Dynamik vorgesehen werden: Durch das gezielte Zuschalten weiterer geeigneter Sensoren kann zum einen eruiert werden, ob auch diese denselben Angriff melden, so dass die Wahrscheinlichkeit, dass es sich um einen Fehlalarm handelt, gesenkt werden kann. Zum anderen kann häufig nur durch lokal auf dem vermeintlichen Angriffsziel installierte oder in unmittelbarer Nähe platzierte Sensoren entschieden werden, ob ein Angriff erfolgreich war: Beobachtet beispielsweise ein Netz-IDS wiederholte SSH-Loginversuche auf einem Server, kann aufgrund der bei SSH verschlüsselten TCP/IP-Nutzdaten ein auf der Zielmaschine installiertes Host-IDS wesentlich einfacher und zuverlässiger darüber befinden, ob ein Loginversuch erfolgreich war; zusätzliche Informationen, beispielsweise mit welchem Benutzernamen der Angreifer den Loginversuch unternommen hat, stehen sogar nur auf dem Zielsystem zur Verfügung, da nur dieses die Nutzdaten entschlüsseln kann.

6. Die Schritte 6.–9. hängen eng zusammen und dienen einer Verfeinerung der bereits durchgeführten Korrelation mit dem Ziel, über die Betrachtung einzelner Sensormeldungen hinausgehend zu erkennen, welche Ziele der Angreifer mit seinen Aktionen verfolgt. Zunächst wird im Rahmen der **zielsystemspezifischen Bedrohungsnachverfolgung** (*thread reconstruction*) für jedes einzelne Angriffsziel darüber Buch geführt, welche Angriffsschritte derselbe beobachtete Angreifer bereits durchgeführt hat.

7. Komplementär dazu werden bei der **Angriffsnachverfolgung** (*attack session reconstruction*) alle netz- und hostbasierten Ereignismeldungen, die sich auf dasselbe Netzsegment beziehen, miteinander verknüpft.

8. Durch die als **Angriffsschwerpunkterkennung** (*focus recognition*) bezeichnete Auswertung der in den beiden vorherigen Schritten ermittelten Zwischenergebnisse wird

erkannt, ob und auf welche einzelnen Systeme sich der Angriff konzentriert. Sofern der Angreifer damit keine bewusste Täuschung vornimmt, ist es naheliegend und in der Praxis meist die richtige Entscheidung, nachfolgende Reaktionen wie die Verstärkung der Schutzmaßnahmen auf die so identifizierten Angriffsschwerpunkte zu konzentrieren. Im Hinblick auf die hier betrachtete Dynamik des IDS ergibt sich folglich die Zielsetzung, nach Möglichkeit weitere Sensoren und Module zu aktivieren, die die Vorgänge im näheren Umkreis der Angriffsschwerpunkte analysieren können.

9. Die Korrelationsmaßnahmen abschließend wird bei der **Angriffswegkorrelation** (*multistep correlation*) versucht, nachzuvollziehen, aus welchen einzelnen Angriffsschritten bzw. Teilangriffen das beliebig komplexe Gesamtvorhaben des Angreifers besteht; beispielsweise könnte dieser zunächst einen über das Internet erreichbaren Server kompromittieren, um von dort aus nur unternehmensintern erreichbare weitere Maschinen angreifen zu können. Die Erkennungsleistung von IDS ist diesbezüglich nach wie vor noch nicht ausgereift, so dass eine vollständige Rekonstruktion solcher aus mehreren Meilensteinen bestehenden Angriffe, falls überhaupt, häufig nur manuell im Rahmen späterer IT-forensischer Maßnahmen gelingt.
10. Im vorletzten Schritt der klassischen Verarbeitungskette wird die **Auswirkungsanalyse** (*impact analysis*) durchgeführt. Sie stellt den Zusammenhang zwischen den verarbeiteten Ereignismeldungen und den Beeinträchtigungen für den Schutzbedarf der vom beobachteten Angriff betroffenen Assets her.
11. Abschließend wird eine **Priorisierung** durchgeführt, die beim parallelen Vorliegen mehrerer Angriffe sowohl über die Reihenfolge, mit der anschließend automatisierte Reaktionen angestoßen werden, entscheidet als auch als Hilfestellung für die manuelle Bearbeitung im Rahmen des operativen Sicherheitsmanagement fungiert. Für die Bestimmung der Priorität müssen im Allgemeinen Regeln vorgegeben werden, die beispielsweise den Wert der Assets, die Verletzung ihres Schutzbedarfs und die Art des erkannten Angriffs auswerten.
12. Während die Ereignisverarbeitung in herkömmlichen IDS mit dem vorherigen Schritt abgeschlossen und zu nachgeordneten Berichtsabläufen sowie dem Anstoßen externer Reaktionsmechanismen übergegangen wird, ergibt sich in dieser Arbeit als wesentlicher neuer Schritt die Beurteilung der ermittelten Gesamtsicherheitslage mit dem Ziel der **dynamischen IDS-Rekonfiguration**. Dabei soll erreicht werden, dass zunächst über eine zu spezifizierende Regelsprache die aktuelle Sicherheitsmeldung, die ihr zugeordneten Angriffsverläufe und die aktuelle Konfiguration aller IDS-Komponenten ausgewertet werden können. Daran anschließend sollen ebenfalls regelbasiert und unter Nutzung einheitlicher Sensorschnittstellen, die jedoch die individuellen Fähigkeiten der Sensoren berücksichtigen, Maßnahmen wie das Aktivieren und Deaktivieren von Sensoren und deren Modulen durchgeführt werden können.

Externe Eingriffe, die beispielsweise durch Administratoren unter Nutzung einer zentralen Managementplattform durchgeführt werden, können vereinfacht als Einsprung in den neuen Schritt 12 aufgefasst werden; analog dazu sind automatisierte, zeitgesteuerte Umkonfigurationen zu betrachten. Ihre technische Umsetzung bedingt offensichtlich, dass alle für die Auswertestation nutzbaren Sensoren geeignet verwaltet werden und dass eine Basismenge an Funktionen bereitgestellt wird, die für die regelbasierte Auswertung des aktuellen Sicherheitszustands und für die dynamische Rekonfiguration genutzt werden können. Diese beiden

Aspekte werden in den folgenden Abschnitten vertieft.

7.2.4. Informationsmodell für die Sensorverwaltung

Sowohl die in der wissenschaftlichen Literatur veröffentlichten IDS-Architekturen als auch die derzeit marktüblichen IDS-Implementierungen gehen davon aus, dass entweder nur herstellereigene Sensoren an die Analysestationen angeschlossen werden oder Sensoren aus einer fest vorgegebenen, oft nicht besonders umfangreichen Menge von Sensormodellen zum Einsatz kommen. Das hier konzipierte Werkzeug soll hingegen die Möglichkeit bieten, in Security-Frameworks bereits vorhandene Sicherheitsmechanismen und deren Statusmeldungen als Sensorik integrieren zu können. Von den Sensoren wird somit grundlegend lediglich gefordert, dass sie Sicherheitsereignisse an die Auswertestationen melden oder zum Abruf bereitstellen können; zur Vereinfachung wird wie oben bereits diskutiert angenommen, dass die Meldungen im IDMEF-Format vorliegen und mittels IAP-Protokoll übertragen werden. Auf den Einsatz von Konvertern und Protokollumsetzern wird nicht eingegangen.

Um als zentralem Bestandteil der dynamischen Rekonfiguration entscheiden zu können, welche Sensoren und welche Module aktiviert werden sollen bzw. wieder deaktiviert werden können, müssen seitens der Auswertestation Informationen über alle daran angeschlossenen Sensoren vorliegen, die mit der in Abschnitt 7.2.5 spezifizierten Regelsprache bzw. Funktionsbibliothek ausgewertet werden können. Im Folgenden wird deshalb ein Informationsmodell erarbeitet, das Aufschluss über die wichtigsten Attribute von Sensoren und Modulen, die objektorientiert verwaltet werden, gibt.

Ein Aspekt, der bei der Betrachtung der Dynamikeigenschaften nicht im Vordergrund steht, aber für die effektive praktische Anwendung des Modells ausschlaggebend ist, besteht in der Modellierung der Netz- und Systemtopologie, deren Auswertung es ermöglichen muss, u. a. zu entscheiden, ob ein System im Abdeckungsbereich eines Sensors liegt und ob sich ein Sensor bezüglich der Netztopologie in der Nähe eines anderen Sensors befindet. Im Folgenden wird davon ausgegangen, dass Datenstrukturen zur Abbildung der Topologie und darauf basierende Distanzermittlungsverfahren bereits gegeben sind; bei der praktischen Umsetzung kann diese Voraussetzung beispielsweise durch die Orientierung an Netzmanagementsystemen erfüllt werden, mit denen auch ein regelmäßiger Datenabgleich vorgenommen werden sollte.

Abbildung 7.6 zeigt das erarbeitete Informationsmodell als UML-Klassendiagramm; für Sensoren umfasst es die im Folgenden näher erläuterten Attribute:

- *Sensor-Id*: Über einen Identifikator kann der Sensor szenarienweit eindeutig benannt werden.
- *Beschreibung*: Die Beschreibung des Sensors erfolgt in natürlicher Sprache und fasst beispielsweise seine Eigenschaften und seine Platzierung so zusammen, dass das operative Sicherheitsmanagement bei der Implementierung der Regelsätze, die von der Auswertestation verarbeitet werden, unterstützt wird.
- *Sensortyp*: Die Angabe des Sensortyps entspricht einer Grobklassifikation, die durch die beiden nachfolgend beschriebenen Attribute verfeinert wird. Prinzipiell ist zwischen folgenden drei Typen und ihren jeweiligen Subtypen zu differenzieren:
  - *Netzbasierter Sensor*: Der Sensor überwacht den Netzverkehr in seinem Einzugsbereich. Die Subtypisierung umfasst beispielsweise signaturbasierte und auf Basis

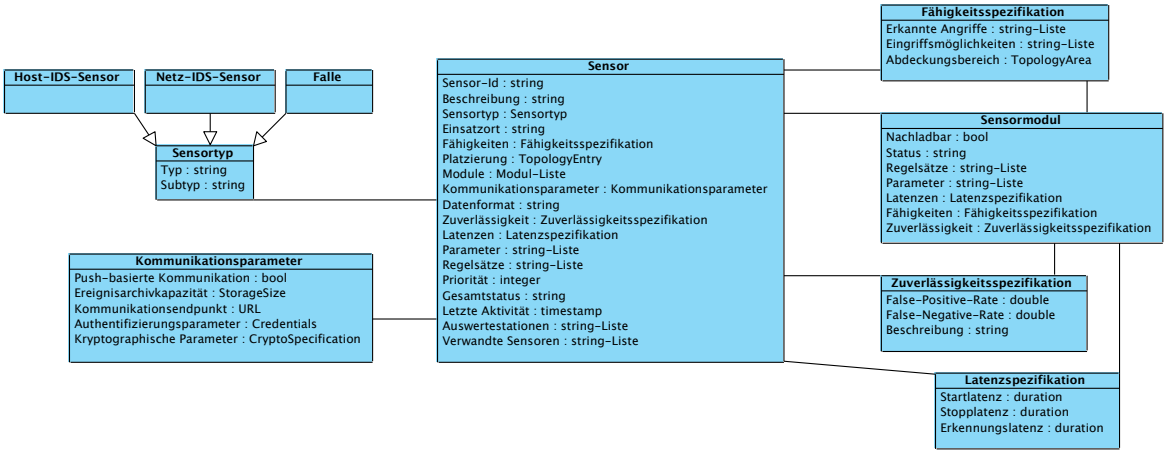


Abbildung 7.6.: Informationsmodell für die Verwaltung der dynamisch reparametrisierbaren Sensoren

von Heuristiken operierende Netz-IDS-Sensoren.

  - *Hostbasierter Sensor*: Host-IDS-Sensoren werden auf Systemen betrieben, deren primärer Zweck ein anderer ist, beispielsweise das Erbringen eines netzbasierten IT-Dienstes. Zu den Subtypen zählen u. a. Virenscanner, Dateiintegritätsprüfer, Rootkit-Detektoren, Protokolldateiüberwachungswerkzeuge und Prozesse, die das Nutzungsverhalten von Anwendern überwachen.
  - *Falle*: Fallen sind dedizierte Systeme, die von regulären Anwendern nicht genutzt werden, sondern ausschließlich dazu dienen, Angreifer anzulocken und Angriffe zu analysieren. Als Subtypen sind beispielsweise Honeypots, die verwundbare Netzdienste vortäuschen, und Malware-Collection-Systeme, die Schadsoftware bewusst ausführen, um ihr Verhalten zu analysieren, zu betrachten.

- *Einsatzort*: Der Einsatzort gibt bei netzbasierten Sensoren an, ob diese *zentral* (Backbone-Sensor) oder *dezentral* (Subnet-Sensor) zu verwenden sind; bei Host-Sensoren und Fallen nimmt das Attribut den Wert *lokal* an.
- *Fähigkeiten*: Die Angabe der Fähigkeiten eines Sensors umfasst
  - eine Aufzählung der Arten von Sicherheitsmeldungen, die der Sensor generieren kann, und somit eine Beschreibung der Angriffstypen, für die der Sensor geeignet ist,
  - eine Angabe der aktiven Eingriffsmöglichkeiten, die der Sensor entweder hat, um beispielsweise mit den überwachten Ressourcen zur Akquisition von Messdaten zu interagieren oder anderweitig stimulierend einzugreifen, oder die sich aus der Kombination von Sensoren mit Reaktionskomponenten ergeben – beispielsweise, falls ein Sensor bestimmte Angriffe nicht nur erkennen, sondern auch unterbinden kann, und
  - die Spezifikation seines Abdeckungsbereichs (*sensor scope*) als Teilmenge der Gesamttopologie.

- *Platzierung*: Ebenfalls auf Basis des vorliegenden Topologiemodells wird der aktuelle Standort des Sensors erfasst; im Regelfall liegt dieser innerhalb oder am Rand des Abdeckungsbereichs.
- *Module*: Für jeden Sensor werden Basisinformationen über die Menge seiner Module geführt. Pro Modul ist dabei zu erfassen, ob es fest integriert ist oder nachgeladen bzw. entfernt werden kann und ob es derzeit aktiviert ist. Darüber hinaus sind modulspezifische Regelsätze und Parameter vorzusehen, deren Ausprägung sensormodellspezifisch variieren kann. Ferner können erwartete Latenzen festgehalten werden, die beim Aktivieren bzw. Deaktivieren des Moduls sowie bei der Erkennung von Angriffen auftreten können. Beispielsweise benötigt ein Modul, das anhand einer Überwachung des Benutzerverhaltens entscheidet, ob es sich statt des regulären Nutzers um einen Angreifer handelt, einen längeren Zeitraum, um mit akzeptabler Zuverlässigkeit entscheiden zu können, dass kein Angriff vorliegt.
- *Kommunikationsparameter*: Die Kommunikationsparameter umfassen die Angabe, ob push- oder pull-basiert mit dem Sensor kommuniziert werden soll, wie viele Einträge maximal im lokalen Ereignisarchiv des Sensors gespeichert werden, welcher Kommunikationsendpunkt (z. B. IP-Adresse und TCP-Portnummer) zu verwenden ist, welche Authentifizierungsparameter (z. B. Shared Secret oder Serverzertifikat) zu verwenden und welche kryptographischen Algorithmen zur Verschlüsselung und Integritätssicherung im Rahmen des IAP-Protokolls einzusetzen sind.
- *Datenformat*: Über dieses Attribut wird das Format benannt, in dem der Sensor seine Ereignismeldungen an die Auswertestation übermittelt; im Regelfall ist IDMEF zu verwenden.
- *Zuverlässigkeit*: Die Zuverlässigkeit gibt an, wie viele Fehler erster und zweiter Art (*false positives* bzw. *false negatives*) beim Sensoreinsatz eintreten. Sofern keine Herstellerangaben oder Untersuchungen durch Dritte vorliegen, muss auf szenarienspezifische Erfahrungen und Schätzwerte zurückgegriffen werden.
- *Latenzen*: Analog zu einzelnen Modulen wird festgehalten, welche Verzögerungen beim Aktivieren bzw. Deaktivieren des gesamten Sensors zu berücksichtigen sind und ob auch bei der Erkennung bzw. Meldung von Sicherheitsereignissen mit Verzug zu rechnen ist.
- *Parameter* und *Regelsätze*: Analog zu den modulspezifischen Parametern und Regelsätzen werden auch sensorweite Parameter und Regelsätze verwaltet.
- *Priorität*: Sofern mehrere Sensoren für die Erkennung bestimmter Angriffe am selben Ort geeignet sind, kann über die Priorität festgelegt werden, in welcher Reihenfolge sie aktiviert werden sollen.
- *Gesamtstatus*: Über den Gesamtstatus wird erfasst, ob der Sensor aktuell aktiviert oder deaktiviert ist bzw. ob eine Fehler- oder Ausnahmesituation vorliegt, in der z. B. kein Kontakt mehr zu ihm möglich ist.
- *Letzte Aktivität*: Ein Zeitstempel gibt an, wann zuletzt eine Aktivität des Sensors registriert wurde; dabei handelt es sich um den Zeitstempel der letzten IDMEF Alert- oder Heartbeat-Nachricht, die von der Auswertestation verarbeitet wurde.
- *Angeschlossene Auswertestationen*: Dieses Attribut gibt in Form einer Liste von Identifikatoren an, an welche Auswertestationen der Sensor aktuell angeschlossen ist. Wie

bereits erläutert wird nachfolgend nur der Fall betrachtet, dass diese Liste genau ein Element enthält. Sind mehrere Auswertestationen berechtigt, beispielsweise Module zu aktivieren, zu parametrisieren und zu deaktivieren, so kann es zu Konflikten kommen, für die im Kontext der *kooperativen* IDS-Architekturen Lösungsmöglichkeiten untersucht werden.

- *Verwandte Sensoren*: Neben verwandten Sensoren, die aufgrund ähnlicher Erkennungsleistungen oder topologischer Nähe ermittelt werden können, können auch manuelle Einträge vorgenommen werden, die als Empfehlungen fungieren, bei bestimmten Angriffen zur Präzisierung der Diagnose auf die angegebenen weiteren Sensoren zurückzugreifen.

Neben den Sensoren muss die Auswertestation noch weitere Informationen verwalten, beispielsweise über die im Rahmen der Ereignisauswertung zu verwendenden Regelsätze, über die bezüglich der erkannten Angriffe zu informierenden übergeordneten Systeme und über die Eigenschaften der externen Reaktionskomponenten. Da diese Aspekte jedoch nicht unmittelbar zur hier betrachteten dynamischen Rekonfiguration der IDS-Komponenten beitragen, werden sie nicht weiter vertieft.

7.2.5. Funktionsmodell für die Spezifikation von Auswertungs- und Steuerungsregeln

Sowohl bei der Auswertung eingegangener Sensormeldungen als auch bei der Vorbereitung und Umsetzung von dynamischen IDS-Rekonfigurationen muss der aktuelle Gesamtzustand, der sich aus dem Zustand der IDS-Komponenten und den verarbeiteten Ereignismeldungen zusammensetzt, ausgewertet werden können. Zur Spezifikation der szenarienspezifisch gewünschten Auswertungen und Reaktionen müssen Regelsätze implementiert werden, wobei die Abarbeitung eines Regelsatzes in den folgenden Situationen angestoßen wird:

- Eine neue Sensormeldung geht über die Sensorkommunikationskomponente der Auswertestation ein und wird nicht bereits bei der Vorfilterung verworfen.
- Ein zeitgesteuertes Ereignis (Timer-Event) tritt ein; beispielsweise kann die Auswertestation das Aktivieren eines zusätzlichen Sensors veranlassen und zeitgesteuert wieder deaktivieren, falls er z. B. innerhalb von 10 Minuten kein relevantes Ereignis meldet.
- In die Konfiguration der Auswertestation wird von außen, z. B. über eine Managementplattform, eingegriffen.

Welche Programmier- oder Policysprache für die Erstellung der Regelsätze zu verwenden ist, kann implementierungsspezifisch festgelegt werden: Da die meisten aktuellen IDS-Produkte u. a. aus Performanzgründen in C implementiert sind, wird im Folgenden ein an die C-Syntax angelehnter Pseudocode verwendet, der die erarbeiteten Konzepte veranschaulichen soll, obwohl auch andere gängige Hochsprachen und bei Systemadministratoren und Security Engineers populäre Skriptsprachen wie Perl oder Python eingesetzt werden könnten. Nachfolgend wird jedoch losgelöst von der Bereitstellung typischer Programmkonstrukte wie Schleifen, Fallunterscheidungen und Vergleichsoperatoren für Zahlen und Zeichenketten auf die Bestandteile einer Funktionsbibliothek eingegangen, die u. a. Zugriff auf die folgenden Informationen und die Ansteuerung anderer Komponenten bieten muss:

- Die Konfiguration der Analysestation inklusive Timer-Events muss gelesen und manipuliert werden können.

- Der Status und die Konfiguration aller angeschlossenen Sensoren und deren Module müssen gelesen und modifiziert werden können.
- Auf die Datenfelder des aktuell bearbeiteten Ereignisses, die Korrelationsergebnisse sowie die Inhalte der angeschlossenen Ereignisdatenbasen muss lesend zugegriffen werden können.
- Programmierschnittstellen externer Komponenten müssen zugänglich gemacht werden. Dies umfasst insbesondere die Kommunikation mit externen Reaktionskomponenten und Managementsystemen, die u. a. Umgebungsinformationen beispielsweise über die aktuelle Netztopologie, Datum und Uhrzeit, etc. liefern sollen.

Generell soll durch die Funktionsbibliothek ein hoher Grad an Flexibilität erreicht werden, so dass implementierte Regelsätze möglichst allgemeingültig gehalten werden können, d. h. dass in ihnen z. B. auf die fest vorgegebene Benennung von Sensoren verzichtet werden kann und diese stattdessen auf Basis ihrer Funktionalität und weiteren Eigenschaften dynamisch ausgewählt werden können. Im Folgenden wird eine Basismenge an Funktionen spezifiziert, auf die auch im Rahmen des nachfolgenden Anwendungsbeispiels zurückgegriffen wird:

- `idmefObject getCurrentEvent()`
  Die Funktion liefert die aktuell verarbeitete Sensormeldung als IDMEF-Objekt, dessen Attribute den einzelnen IDMEF-Datenfeldern wie Quell- und Ziel-IP-Adresse des potentiellen Angriffs entsprechen (vgl. Abschnitt 6.4.3).
- `idmefObject[] getCorrelatedEventSet(idmefObject event)`
  `getCorrelatedEventSet` gibt eine Liste aller Ereignismeldungen zurück, die mit dem als Parameter übergebenen Ereignis korreliert werden konnten.
- `id[] getDatabaseList()`
  liefert eine Liste aller an die Auswertestation angeschlossenen Ereignisdatenbasen.
- `idmefObject[] getEventList(id dbox, timestamp start, timestamp end)`
  ruft alle in der Ereignisdatenbasis `dbox` gespeicherten Sensormeldungen ab, deren Zeitstempel zwischen den angegebenen Start- und Endzeitpunkten liegt.
- `idmefObject[] filterEvents(idmefObject[] events, filterCriteria fc)`
  Die Funktion `filterEvents` gibt aus einer als Parameter übergebenen Liste von Sensormeldungen diejenigen zurück, die die angegebenen Filterkriterien erfüllen; dabei können beispielsweise der Ereignistyp und alle anderen IDMEF-Attribute auf bestimmte Werte oder Wertebereiche eingeschränkt werden.
- `id[] getSensorList()`
  gibt eine Liste aller an die Auswertestation angeschlossenen Sensoren zurück.
- `sensorConfig getSensorConfiguration(id sensor)`
  ruft die aktuelle Konfiguration des als Parameter angegebenen Sensors inklusive seiner aktuellen Regelsätze ab.
- `id[] getModuleList(id sensor)`
  liefert die aktuell auf dem per Parameter spezifizierten Sensor installierten Module als Liste.
- `moduleConfig getModuleConfiguration(id sensor, id module)`
  erlaubt den lesenden Zugriff auf die Modulkonfiguration des angegebenen Moduls des angegebenen Sensors.

- `id[] searchSensor(searchCriteria sc)`
  Die Funktion `searchSensor` gibt eine Liste aller an die Auswertestation angeschlossenen Sensoren zurück, die die als Parameter angegebenen Kriterien erfüllen. Dabei muss anhand des Sensortyps, seines Einsatzortes, seiner Fähigkeiten und der anderen im oben vorgestellten Datenmodell enthaltenen Eigenschaften gefiltert werden können.
- `bool activateSensor(id sensor)` und `bool deactivateSensor(id sensor)`
  dienen zum Aktivieren bzw. Deaktivieren des als Parameter benannten Sensors. Falls die Operation erfolgreich war, wird `true` zurückgeliefert, sonst `false`.
- `bool activateModule(id sensor, id module)` und `bool deactivateModule(id sensor, id module)`
  dienen zum Aktivieren bzw. Deaktivieren des als Parameter benannten Sensors des ebenfalls als Parameter angegebenen Sensors. Falls die Operation erfolgreich war, wird `true` zurückgeliefert, sonst `false`.
- `bool setSensorConfiguration(id sensor, sensorConfig c)`
  spielt die als Parameter übergebene Konfiguration in den angegebenen Sensor ein. Falls dies erfolgreich war, wird `true` zurückgeliefert, sonst `false`.
- `bool checkModuleCompatibility(id sensor, id module)`
  überprüft, ob das angegebene Modul mit dem angegebenen Sensor kompatibel ist. Falls dies der Fall ist, wird `true` zurückgeliefert, sonst `false`.
- `bool uploadModule(id sensor, id module)`
  spielt das angegebene Modul auf dem benannten Sensor ein. Falls die Übertragung erfolgreich oder das Modul bereits eingespielt war, wird `true` zurückgegeben, sonst `false`.
- `bool deleteModule(id sensor, id module)`
  entfernt das angegebene Modul vom benannten Sensor. Falls das Löschen erfolgreich oder das Modul nicht eingespielt war, wird `true` zurückgegeben, sonst `false`.
- `bool setModuleConfiguration(id sensor, id module, moduleConfig c)`
  spielt die als Parameter übergebene Konfiguration in das angegebene Modul des als Parameter angegebenen Sensors ein. Falls dies erfolgreich war, wird `true` zurückgeliefert, sonst `false`.
- `bool fetchBatchEvents(id sensor)`
  stößt das Abrufen der vom angegebenen Sensor lokal vorgehaltenen Meldungen an (Pull-Modell). Die dadurch eingehenden Ereignismeldungen werden regulär im Rahmen der Verarbeitungskette analysiert. Falls das Anstoßen des Vorgangs erfolgreich war, wird `true` zurückgeliefert, sonst `false`.
- `timerId setTimer(callback c, string task, idmefObject e, eventCount n, duration t [, timerId id])`
  Die Funktion `setTimer` konfiguriert ein zeitgesteuertes Ereignis innerhalb der Auswertestation. Wenn der Zeitpunkt des Ereignisses eingetreten ist, wird die Callback-Funktion `c` aufgerufen. Der Ereigniszeitpunkt ist entweder erreicht, sobald die `n`. weitere Sensormeldungen verarbeitet wird, oder nachdem `t` Sekunden vergangen sind. Die Funktion liefert einen eindeutigen Identifikator für den konfigurierten Timer zurück. Dieser kann als optionaler vierter Parameter übergeben werden, um einen schon eingerichteten Timer umzukonfigurieren, beispielsweise um den Zeitpunkt seines

Eintretens zu modifizieren. Der Timer kann gelöscht werden, indem seine Callback-Funktion `c` auf den Wert `NULL` geändert wird. Der angegebenen Callback-Funktion werden die angegebene Zeichenkette `task` und die Sensormeldung `e` als Parameter übergeben, damit diese den Kontext zum Bearbeitungsverlauf wiederherstellen kann; falls dies nicht erforderlich ist, können `task` und `e` ebenfalls jeweils den Wert `NULL` annehmen.

- `bool checkSensorAvailability(id sensor)`
  Liefert `true`, falls der als Parameter angegebene Sensor aktuell angesprochen werden kann, sonst `false`; dies kann intern beispielsweise durch eine IDMEF-Heartbeat-Nachricht überprüft werden.
- `bool checkSensorScope(id sensor, topologyElement target [, eventType e])`
  Die Funktion `checkSensorScope` gibt Aufschluss darüber, ob das angegebene Ziel `target`, bei dem es sich z. B. um einen von einem aktuellen Angriff betroffenen Server handelt, im Abdeckungsbereich (*sensor scope*) des angegebenen Sensors liegt. Optional kann diese Überprüfung anhand eines angegebenen Ereignistyps, der erkannt werden soll, weiter präzisiert werden. Das Ergebnis ist `true`, falls das Ziel im Sensorabdeckungsbereich liegt, sonst `false`.
- `topologyRelation checkTopology(topologyElement a, toplogyElement b)`
  Über `checkTopology` kann ermittelt werden, wie das Infrastrukturelement `a`, z. B. ein Sensor, in Relation zum Infrastrukturelement `b`, z. B. einem Server, platziert ist. Die Ergebniswertemenge umfasst:
  - `localhost`: Beide Infrastrukturelemente werden auf demselben Endgerät betrieben, z. B. ein Host-IDS-Sensor auf einem Webserver.
  - `neighbor`: Beide Infrastrukturelemente sind gleichberechtigt, z. B. zwei Server im selben Subnetz.
  - `uplink`: Infrastrukturelement `a` ist Infrastrukturelement `b` von der Netztopologie her übergeordnet, beispielsweise ein Subnet-IDS-Sensor in Relation zu einem Server in diesem Subnetz.
  - `not related`: Beide Infrastrukturelemente stehen in keinem der anderen Zusammenhänge, z. B. zwei Server in verschiedenen Subnetzen.
- `bool notifySuperior(limit restriction, idmefObject event [, string comment])`
  propagiert eine Sensormeldung oder ein erst bei der Analyse erstelltes IDMEF-Objekt an die der Analysestation übergeordneten Systeme, beispielsweise eine SIEM-Instanz. Es können Einschränkungen vorgegeben werden, beispielsweise dass nur bestimmte andere Systeme informiert werden oder die Anzahl propagierter Nachrichten auf eine Höchstanzahl pro Zeitraum begrenzt wird. Optional kann eine frei wählbare Zeichenkette als Kommentar mitgeschickt werden.
- `id[] getResponseUnitList()`
  liefert eine Liste aller an die Auswertestation angeschlossenen externen Reaktionskomponenten.
- `id[] searchResponseUnit(searchCriteria sc)`
  liefert eine Teilmenge der von `getResponseUnitList` zurückgegebenen Liste externer Reaktionskomponenten, die die angegebenen Suchkriterien erfüllen.

- `responseUnitConfig getResponseUnitConfiguration(id responseunit)`
  ruft die aktuelle Konfiguration und Fähigkeiten der als Parameter angegebenen externen Reaktionskomponente ab.
- `bool callResponseUnitFunction(id responseunit, string functionName, parameterSet p)`
  Über `callResponseUnitFunction` wird die angegebene Funktion der benannten externen Reaktionskomponente mit den ebenfalls übergebenen Parametern aufgerufen. Beispielsweise könnte bei einer Paketfilterfirewall eine Funktion zum Hinzufügen einer neuen Filterregel, die als Parameter übergeben wird, aufgerufen werden.

Die Menge dieser Basisfunktionen ist für die nachfolgenden Betrachtungen ausreichend, aber nicht notwendigerweise vollständig. Bei der Implementierung dieses Werkzeugkonzepts können folglich weitere Funktionen ergänzt werden; insbesondere sollten auch die Anwender des Systems, die szenarienspezifische Regelsätze implementieren müssen, die Möglichkeit erhalten, eigene Funktionen zur Gruppierung häufig benötigter Regelsequenzen definieren zu können.

7.2.6. Anwendungsbeispiel

Die erarbeiteten Konzepte zur dynamischen IDS-Rekonfiguration werden nun anhand eines einfachen, fiktiven Anwendungsbeispiels erläutert. Dazu werden nachfolgend zunächst das Beispielszenario und die exemplarisch betrachteten Angriffe sowie die durch das dynamische IDS umzusetzenden Reaktionen skizziert. Anschließend wird eine Regelimplementierung in Pseudocode erarbeitet, die diese automatischen Reaktionen anstößt. Schließlich wird die Regelabarbeitung anhand einer Simulation analysiert und bewertet.

7.2.6.1. Skizze des Szenarios, der betrachteten Angriffe und der Soll-Reaktionen

Abbildung 7.7 zeigt die relevanten Bestandteile der Netztopologie des betrachteten, fiktiven Szenarios: Ein Unternehmen ist über einen zentralen Uplink mit dem Internet verbunden; das Backbone-Netz wird am Übergang zum Internet-Uplink, der auch einen Paketfilterfirewall umfasst, mithilfe eines Netz-IDS-Sensors überwacht. Das Unternehmensnetz ist in mehrere Subnetze untergliedert, die ein Zonenkonzept widerspiegeln, das Mitarbeiterarbeitsplätze, interne Server und weltweit erreichbare Server voneinander separiert.

Im Folgenden wird eines dieser Subnetze, die so genannte demilitarisierte Zone (DMZ), näher betrachtet: In ihr sind alle Server und netzbasierten Dienste positioniert, die von außen über das Internet erreichbar sein müssen. Dies umfasst neben DNS-, E-Mail- und Webservern auch ein SSH-Gateway, das gleichermaßen für Mitarbeiter und externe Wartungsbeauftragte konzipiert wurde, die sich beispielsweise vom Telearbeitsplatz aus und somit von außerhalb der Büros mit dem Unternehmensnetz verbinden möchten. Für die DMZ ist ein dedizierter Subnet-IDS-Sensor verfügbar, dessen Traffic-Analysefähigkeiten über diejenigen des Backbone-IDS-Sensors hinausgehen. Auf dem SSH-Gateway ist zudem ein Host-IDS-Sensor installiert, der zwei Module umfasst: Einerseits kann die Protokolldatei des SSH-Dienstes überwacht werden, um Aufschluss darauf zu geben, welche Benutzer sich einzuloggen versuchen; zum anderen können die Kommandozeilenbefehle, die erfolgreich angemeldete Benutzer über ihre SSH-Verbindung absetzen, durch eine Heuristik auf Auffälligkeiten untersucht werden, die auf missbräuchliche Verwendung hindeuten. Vereinfachend wird angenommen, dass ausschließlich

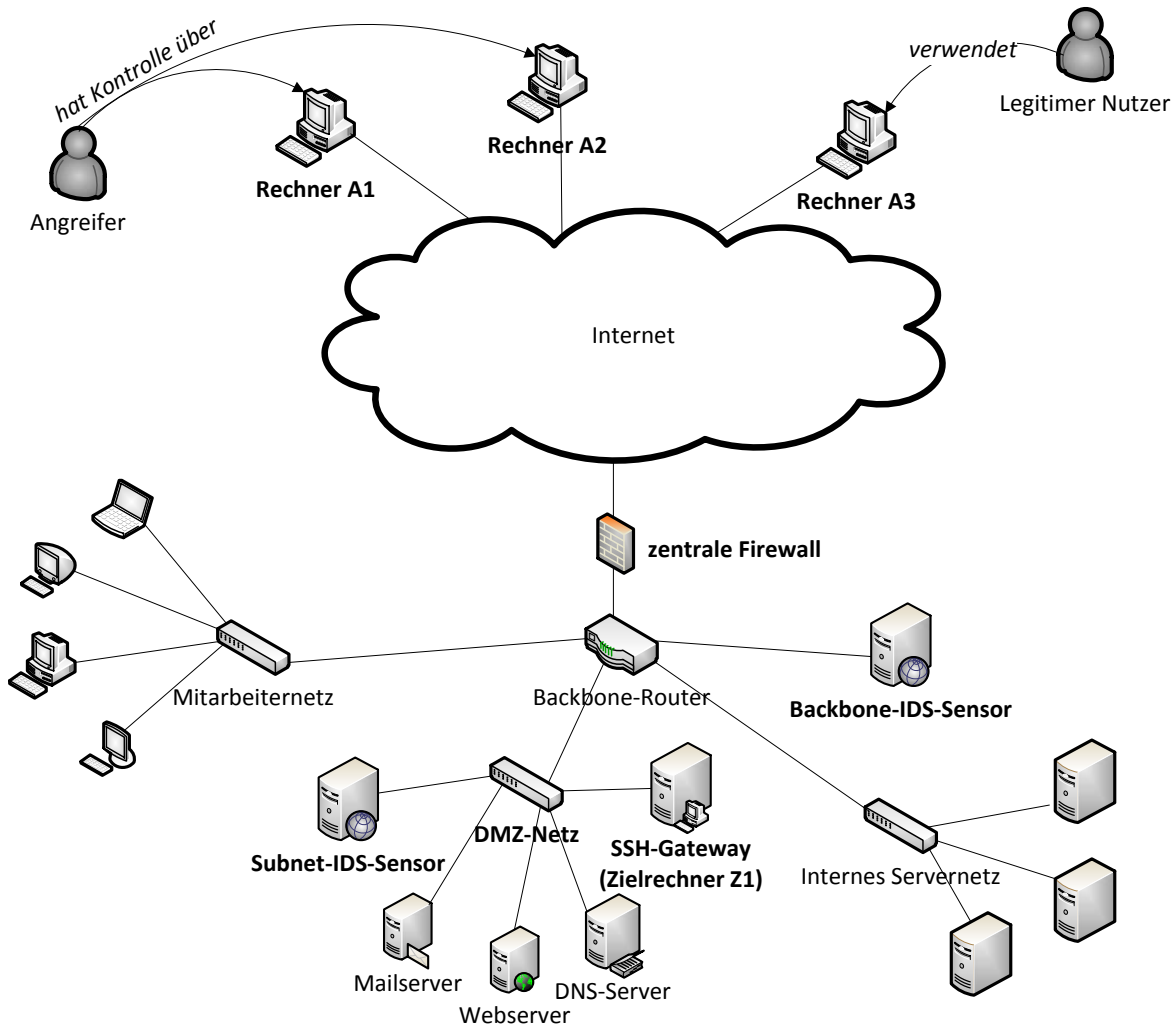


Abbildung 7.7.: Szenario für das Anwendungsbeispiel

IPv4 und darauf basierende Protokolle zum Einsatz kommen, d. h. IPv6-Verbindungen werden nicht betrachtet.

Die betrachteten Angriffe erfolgen in drei aufeinanderfolgenden Phasen, deren Abläufe grob wie folgt charakterisiert werden können:

1. In der ersten Phase wird vom Angreifer über das Internet ein SSH-Portscan der DMZ ausgeführt, d. h. von *einer* externen Quell-IP-Adresse aus werden Verbindungsversuche auf den Ziel-TCP-Port 22 (SSH) aller möglichen Ziel-IP-Adressen durchgeführt. Der Angreifer kann dadurch erkennen, dass auf dem SSH-Gateway-Server ein von außen erreichbarer SSH-Dienst betrieben wird, der zum Ziel der nachfolgenden Angriffsphasen wird.
2. Nach Abschluss des SSH-Portscans und einer kurzen Pause beginnt der Angreifer von derselben Quell-IP-Adresse aus, SSH-Loginversuche auf dem SSH-Gateway durchzufüh-

ren. Er verwendet hierzu gängige Benutzernamen und Passwörter auf Basis eines Wörterbuchangriffs, um eine Kennung mit schwachem Passwort zu kompromittieren und Zugang zum Rechner zu erlangen. Wie nachfolgend erläutert wird, führt dies am Ende der zweiten Phase dazu, dass die Quell-IP-Adresse des Angriffs am Firewall blockiert wird.

3. In der dritten Phase sind SSH-Loginversuche von zwei weiteren externen Quell-IP-Adressen aus zu beobachten. Eine der beiden Quellen ist bei zweiten SSH-Loginversuch erfolgreich, die andere unternimmt lediglich Fehlversuche. Beim erfolgreichen SSH-Login ist zunächst unklar, ob es sich um einen Angreifer, der ein Passwort erraten hat, oder um einen legitimen Benutzer handelt.

Für die nachfolgenden Betrachtungen wird davon ausgegangen, dass die Möglichkeit von SSH-Portscans und gezielten Angriffen auf den SSH-Gateway im Szenario bereits bekannt war und somit bereits a priori ein Soll-Verhalten der verfügbaren IDS-Komponenten definiert wurde, beispielsweise da es sich beim DMZ-Subnetz-IDS und beim SSH-Gateway-Host-IDS um Komponenten eines Security-Frameworks handelt. Im Beispiel soll das folgende Verhalten bezüglich der Sensordynamik, des Überwachungsumfangs und der Reaktionen auf Angriffe erreicht werden:

- Im Regelfall ist ausschließlich der Backbone-IDS-Sensor kontinuierlich in Betrieb. Der Subnet-IDS-Sensor und der Host-IDS-Sensor sollen nur bei Bedarf zugeschaltet und nach angemessenen Betriebszeiten wieder deaktiviert werden.
- Der Backbone-IDS-Sensor wertet lediglich IP- und TCP-Header aus, nimmt aber keine inhaltliche Analyse der Verbindungen vor. Der Subnet-IDS-Sensor kann darüber hinaus per Deep Packet Inspection (DPI) auch die Nutzdaten analysieren, deren Beurteilung bei der z. B. bei SSH-Verbindungen vorliegenden Ende-zu-Ende-Verschlüsselung jedoch Grenzen gesetzt sind.
- Reine (SSH-) Portscans werden als harmlos eingestuft und führen außer zu informativen Meldungen zu keinerlei automatisierten Reaktionen. Wiederholt auftretende erfolglose SSH-Loginversuche sind jedoch durch das Host-IDS näher zu analysieren; falls dabei ein SSH-Dictionary-Angriff oder eine andere Form eines Brute-Force-Angriffs diagnostiziert wird, ist der Angreifer durch Blockieren von Verbindungen seiner Quell-IP-Adresse am Firewall auszusperren.
- Falls ein erfolgreicher SSH-Login zeitlich mit beobachteten Angriffen korreliert, soll das Host-IDS dazu eingesetzt werden, das Benutzerverhalten auf seine Kritikalität hin zu beurteilen.

Der oben beschriebene dreiphasige Angriff führt somit auf Basis des genannten Soll-Verhaltens zu folgendem detaillierteren Soll-Ablauf, der nachfolgend implementiert wird:

- Zu Beginn der ersten Phase ist nur der Backbone-IDS-Sensor aktiv. Er bemerkt eingehende TCP/IP-Verbindungsversuche auf Port 22, die der Reihe nach sämtliche Ziel-IP-Adressen der DMZ durchlaufen, wobei vom Angreifer pro Sekunde zehn Versuche unternommen werden. Bei der zehnten betroffenen Ziel-IP-Adresse meldet der Backbone-IDS-Sensor den Vorfall an die Auswertestation.
- Die Auswertestation aktiviert aufgrund dieser Meldung den Subnet-IDS-Sensor. Dieser beobachtet die Verbindungsversuche auf dem SSH-Port der DMZ-IP-Adressen ebenfalls

und diagnostiziert nach zehn beobachteten Versuchen einen harmlosen SSH-Portscan. Diese Information wird vom Subnet-IDS-Sensor an die Auswertestation gemeldet und von dieser an ein szenarienweit eingesetztes SIEM-System propagiert.

Im Laufe des weiteren SSH-Portscans meldet der Subnet-IDS-Sensor jeden zehnten Versuch wiederum als harmlosen SSH-Portscan an die Analysestation; diese gibt die Information allerdings nur noch einmal pro zehn Sekunden an das SIEM-System weiter. Der Subnet-IDS-Sensor wird 60 Sekunden nach dem letzten Verbindungsversuch wieder deaktiviert.

Zum Abschluss der ersten Phase hat der Angreifer somit erfolgreich die gesamte DMZ auf erreichbare SSH-Server abgesucht; es ist wiederum nur der Backbone-IDS-Sensor aktiv.

- In der zweiten Phase beginnen die gezielten SSH-Loginversuche auf dem SSH-Gateway, wobei ein Versuch pro Sekunde unternommen wird. Der Backbone-IDS-Sensor sendet jedesmal einen IDMEF-Alert an die Auswertestation, die somit nach drei Sekunden zum Schluss kommt, dass von derselben Quell-IP-Adresse aus innerhalb von weniger als zehn Sekunden drei neue Verbindungsversuche auf Ziel-TCP-Port 22 ausgegangen sind.
- Auf das Erreichen dieses Schwellenwertes reagiert die Auswertestation, indem sie den Host-IDS-Sensor auf dem SSH-Gateway aktiviert und das Modul zur Überwachung des SSH-Logfiles startet.
- Der Host-IDS-Sensor meldet auf Basis der Protokolldateianalyse alle fünf Sekunden, dass erfolglose SSH-Loginversuche mit jeweils fünf verschiedenen Benutzernamen durchgeführt wurden. Die erste entsprechende Meldung gibt die Auswertestation einmalig an das SIEM-System weiter, so dass eine entsprechende Monitoringmeldung für das operative Sicherheitsmanagement angezeigt werden kann, aus der sich jedoch kein manueller Handlungsbedarf ergibt.
- Nachdem die wiederholten Meldungen des Host-IDS-Sensors darauf hinweisen, dass die SSH-Loginversuche auf dem SSH-Gateway anhalten, veranlasst die Auswertestation nach 15 Sekunden, dass die auffällig gewordene Quell-IP-Adresse im Firewall gesperrt wird. Das SIEM-System wird von der Auswertestation über die getroffene Maßnahme informiert; die neue Firewallregel hat zunächst eine Betriebsdauer von 120 Sekunden.
- Dadurch, dass die Angriffe nun bereits am Internet-Zugang blockiert werden, beobachtet der Host-IDS-Sensor keine weiteren Loginversuche mehr und wird nach einer Karenzzeit von fünf Sekunden deaktiviert. Zum Ende der zweiten Phase ist somit wiederum nur der Backbone-IDS-Sensor aktiv und es liegen keine Angriffe vor, für die nicht bereits Gegenmaßnahmen eingeleitet wurden.
- Zu Beginn der dritten Phase beobachtet der Backbone-IDS-Sensor den jeweils ersten SSH-Verbindungsversuch von zwei anderen Quell-IP-Adressen. Eine der beiden neuen Quell-IP-Adressen versucht bereits eine Sekunde später, eine weitere SSH-Verbindung zum SSH-Gateway aufzubauen.
- Aufgrund des erst kurz zurückliegenden SSH-Angriffs aktiviert die Auswertestation anders als im vorhergehenden Fall *umgehend* den Host-IDS-Sensor und sein Protokollanalysemodul.
- Der Host-IDS-Sensor meldet nach einem weiteren SSH-Loginversuch der einen neuen Quell-IP-Adresse an die Auswertestation, dass sich ein Benutzer erfolgreich auf dem

SSH-Gateway angemeldet hat. Die Auswertestation gibt diese Information an das SIEM-System weiter, um das operative Sicherheitsmanagement auf dem Laufenden zu halten; sie aktiviert auch das Host-IDS-Sensormodul zur Benutzerverhaltensanalyse.

- Parallel dazu unternimmt die andere neue Quell-IP-Adresse laufend weitere SSH-Loginversuche, über die der Host-IDS-Sensor auf Basis des Protokollanalysemoduls alle fünf Sekunden die Auswertestation informiert. Diese gibt die Information über den SSH-Angriff wie in der zweiten Phase einmalig an das SIEM-System weiter.
- Nachdem der Angriff von der zweiten neuen Quell-IP-Adresse länger als 15 Sekunden anhält, werden von der Auswertestation wiederum eine neue Firewallregel zum Blockieren des Angreifers geschaltet und das SIEM-System über die ergriffene Maßnahme informiert. Der Timer für die Deaktivierung der beiden dynamisch erzeugten Firewallregeln wird dabei erneut auf 120 Sekunden gestellt.
- Das Host-IDS-Sensormodul zur Benutzerverhaltensanalyse kommt nach kurzer Zeit zu dem Schluss, dass es sich beim erfolgreichen SSH-Login um eine legitime Nutzung handelt, beispielsweise weil sich derselbe Nutzer bereits früher von dieser Quell-IP-Adresse aus angemeldet und bislang keine verdächtigen Kommandos ausgeführt hat. Der Host-IDS-Sensor meldet diese Diagnose an die Auswertestation, die sie ans SIEM-System weiterreicht, und deaktiviert das Modul zur Verhaltensanalyse autark.
- Seit der Aktivierung der neuen Firewallregel sind keine neuen SSH-Verbindungsversuche mehr zu beobachten. Somit kann die Auswertestation auch das Host-IDS-Sensormodul zur Protokolldateianalyse und damit den gesamten Sensor wieder deaktivieren.
- Nach Ablauf der 120 Sekunden Betriebszeit werden die dynamisch eingespielten Firewallregeln wieder deaktiviert. Somit ist am Ende der dritten Phase die Ausgangssituation wieder erreicht, in der auch nur der Backbone-IDS-Sensor aktiv ist.

Im nächsten Abschnitt werden die in der IDS-Auswertestation implementierten Regelsätze erarbeitet, mit denen dieses Soll-Verhalten umsetzt werden kann.

7.2.6.2. Exemplarische Regelimplementierung

Der nachfolgende Pseudocode zeigt exemplarisch, wie unter Anwendung der in Abschnitt 7.2.5 spezifizierten Funktionen das in Abschnitt 7.2.6 beschriebene Verhalten implementiert werden kann. Die Implementierung besteht zur Veranschaulichung aus lediglich zwei Funktionen, die als Einsprungpunkte für die Bearbeitung von Timer-Events bzw. von eingehenden Sensormeldungen dienen. In diesen beiden Funktionen wird per Fallunterscheidung differenziert, um welche Art von Ereignis es sich handelt bzw. von welchem Sensor die Meldung stammt, so dass die entsprechenden Reaktionen angestoßen werden können. Anders als bei dieser exemplarischen Darstellung sollte beim praktischen Einsatz – beispielsweise durch die Anwendung grundlegender Refaktorisierungsmethoden – auf einen stärker modularen Aufbau der Regelsätze geachtet werden, um u. a. die Wiederverwendbarkeit zu verbessern. Zudem wird im Beispiel vereinfachend auf die im Realbetrieb essentielle Fehlerbehandlung verzichtet. Dennoch ist die Implementierung so allgemein gehalten, dass sie das Soll-Verhalten auch unabhängig von dem einen beschriebenen Angriffsverlauf umsetzt.

```
[...]

// Funktion zur Behandlung von zeitgesteuerten Ereignissen
void onTimerEvent(string task, idmefObject event) {

  // Handelt es sich um eine zeitgesteuerte Deaktivierung von Firewallregeln?
  // In diesem Fall sind die Reaktionskomponente Firewall zu ermitteln und die
  // dynamisch vom IDS angelegten Filterregeln zu entfernen; letztere koennen
  // auf Basis der Quell-IP-Adressen des betrachteten Ereignisses und der
  // korrelierten Ereignisse ermittelt werden.

  if (task.equals("Remove Firewall Rule")) {
    firewall = searchResponseUnit("description == Backbone-Firewall");
    relevantEvents = getCorrelatedEventSet(event);
    callResponseUnitFunction(firewall, "deleteFilterBySourceIP", relevantEvents);
  }

  // Handelt es sich hingegen um eine zeitgesteuerte Deaktivierung von Sensoren?
  // Dann sind zunaechst alle Module des Sensors und anschliessend dieser selbst
  // zu deaktivieren. Vereinfachend wird nicht geprueft, ob der Sensor nicht
  // bereits deaktiviert ist bzw. ob er aktuell ueberhaupt ansteuerbar ist.

  if (task.equals("Deactivate Sensor") {
    sensor = searchSensor("id == " + event.sensorid);
    modlist = getModuleList(sensor);
    foreach module in modlist {
      modconfig = getModuleConfiguration(sensor, module);
      if (modconfig.status == ACTIVE) {
        deactivateModule(sensor, module);
      }
    }
    deactivateSensor(sensor);
  }

} // Ende der Funktion onTimerEvent

[...]

// Funktion zur Bearbeitung von Sensormeldungen
void onSensorEvent(idmefObject se) {

  // Im Folgenden wird anhand des Sensor-Einsatzortes entschieden, wie das gemeldete
  // Ereignis (Variable se) verarbeitet werden soll.

  sensor = searchSensor("id == " + se.sensorid);

  // Handelt es sich um eine Meldung des Backbone-IDS-Sensors?
  if (sensor.intendedUsage.equals("central")) {

    // Obwohl der Backbone-IDS-Sensor zahlreiche weitere Ereignistypen melden
    // kann, werden nachfolgend nur die fuer das Beispielszenario relevanten
    // Ereignisarten betrachtet.

    // Falls es sich um einen vermuteten SSH-Scan handelt, sollen die
    // passenden Subnet-Sensoren ermittelt und zugeschaltet werden.
    if (se.type == getEventTypeByName("SSH Scan")) {

      foreach s in getSensorList() {

        // Fuer jeden Sensor muss geprueft werden, ob er diese Art von
        // Angriffen fuer die vorliegende Ziel-IP-Adresse erkennen kann
        // und ob er im Uplink-Pfad dieses Ziel liegt (also kein Host-IDS-
        // Sensor ist).
        if ((checkSensorScope(s, se.targetIPaddress, se.type) == true) &&
            (checkTopology(s, se.targetIPaddress) == UPLINK)) {

          // Falls der Sensor aktuell verfuegbar und noch deaktiviert ist,
          // soll er fuer eine bestimmte Zeitdauer aktiviert werden. Falls
          // er bereits aktiv ist, soll die Zeitdauer seiner Aktivierung
          // aufgrund des erneut eingetretenen Ereignisses wieder von vorne
          // beginnen. Vgl. Attribut Gesamtstatus im Informationsmodell.

          if (checkSensorAvailability(s) == true) {

            sc = getSensorConfiguration(s);
            // Zeitgesteuert soll nicht der Backbone-Sensor, sondern der
            // hier aktivierte Sensor deaktiviert werden. Dazu wird eine
            // kuenstliche Ereignismeldung generiert, die als Parameter
            // an die Callback-Funktion uebergeben wird.
            dummyEvent.sensorid = s;

            if (sc.status == DEACTIVATED) {
              // Bislang deaktiviert; deshalb: Sensor aktivieren,
              // Modul fuer SSH Scans aktivieren, automatische Deaktivierung
              // nach 60 Sekunden anstossen.

              activateSensor(s);
              activateModule(s, getModuleIdByName("SSH Scan"));
              subnetSensorTimer = setTimer(onTimerEvent, "Deactivate Sensor", dummyEvent, NULL, 60);
```

```
90              }
91              else {
92                // Sensor ist bereits aktiv; deshalb: Zeitpunkt der automatischen
93                // Deaktivierung neu einrichten.
94                subnetSensorTimer = setTimer(onTimerEvent, "Deactivate Sensor", dummyEvent, NULL, 60,
95                                             subnetSensorTimer);
96              }
97
98            }
99          }
100       }
101     } // Ende der Fallunterscheidung "Ereignistyp == SSH Scan"
102
103     // Falls es sich hingegen um einen gezielten SSH-Brute-Force-Angriff auf
104     // eine einzelne Ziel-IP-Adresse handelt, sollen der passende Host-IDS-Sensor
105     // ermittelt und dort das Modul zur SSH-Protokolldateiueberwachung aktiviert
106     // werden. Der Aktivierungszeitpunkt haengt dabei davon ab, ob es sich um
107     // den ersten solchen Angriff innerhalb einer Zeitspanne handelt, oder ob
108     // vor Kurzem bereits ein anderer SSH-Brute-Force-Angriff beobachtet wurde.
109
110     if (se.type == getEventTypeByName("SSH Brute Force")) {
111
112       // Falls innerhalb der letzten 300 Sekunden bereits ein bestaetigter
113       // SSH-Brute-Force-Angriff vorlag, soll bereits bei der zweiten neu
114       // eingehenden Ereignismeldung reagiert werden, sonst erst bei der
115       // dritten.
116
117       now = time(); // aktueller Zeitstempel
118       recentEventSet = getEventList(getDataBaseList(), (now - 300), now);
119       if (filterEvents(recentEventSet, "type == SSH Brute Force").size() > 0) {
120         threshold = 2;
121       }
122       else {
123         threshold = 3;
124       }
125
126       // Muss auf das aktuell betrachtete Ereignis reagiert werden?
127       reactionRequired = false;
128       relatedEvents = getCorrelatedEventSet(se);
129       if(filterEvents(relatedEvents, "(type == SSH Brute Force) &&
130                       (timeInterval < 10 seconds) &&
131                       (sourceIPaddress.constant == true)").size() >= threshold) {
132         reactionRequired = true;
133       }
134
135       // Falls reagiert werden muss, werden analog zu oben die passenden
136       // Sensoren ausgewaehlt und aktiviert.
137       if (reactionRequired == true) {
138
139         foreach s in getSensorList() {
140
141           if ((checkSensorScope(s, se.targetIPaddress, se.type) == true) &&
142               (checkTopology(s, se.targetIPaddress) == LOCALHOST) &&
143               (checkSensorAvailability(s) == true)) {
144
145             sc = getSensorConfiguration(s);
146             dummyEvent.sensorid = s;
147             if (sc.status == DEACTIVATED) {
148               activateSensor(s);
149               activateModule(s, getModuleIdByName("SSH Logfile Monitoring"));
150               hostSensorTimer = setTimer(onTimerEvent, "Deactivate Sensor", dummyEvent, NULL, 5);
151             }
152             else {
153               // Sensor ist bereits aktiv; deshalb: Zeitpunkt der automatischen
154               // Deaktivierung neu einrichten (Zeitdauer: 5 Sekunden).
155               hostSensorTimer = setTimer(onTimerEvent, "Deactivate Sensor", dummyEvent, NULL, 5,
156                                          hostSensorTimer);
157             }
158         }
159
160       } // Ende der Bedingung "auf Ereignismeldung muss reagiert werden"
161     } // Ende der Fallunterscheidung "Ereignistyp == SSH Brute Force"
162   } // Ende der Fallunterscheidung "meldender Sensor == Backbone-IDS-Sensor"
163
164   // Handelt es sich um eine Meldung des Subnet-IDS-Sensors?
165   if (sensor.intendedUsage.equals("decentralized")) {
166
167     // Falls es sich um einen harmlosen SSH Scan handelt, soll das
168     // uebergeordnete System regelmaessig informiert werden. Andere vom
169     // Subnet-IDS-Sensor detektierbare Angriffe sind im Beispiel
170     // irrelevant.
171
172     if (se.type == getEventTypeByName("SSH Scan")) {
173
174       notifySuperior("once in 10 seconds", se, "Harmloser SSH-Scan");
175
176     } // Ende der Fallunterscheidung "Ereignistyp == SSH Scan"
177   } // Ende der Fallunterscheidung "meldender Sensor == Subnet-IDS-Sensor"
178
179   // Handelt es sich um eine Meldung des Host-IDS-Sensors?
```

```
180   if (sensor.intendedUsage.equals("local")) {
181
182     // Beim Host-IDS-Sensor sind im Beispiel drei Meldungstypen zu
183     // unterscheiden, die darueber Aufschluss geben, ob ein SSH-Brute-Force-Angriff,
184     // ein erfolgreicher SSH-Login oder ein unauffaelliges Nutzerverhalten vorliegt.
185
186     if (se.type == getEventTypeByName("SSH Brute Force")) {
187
188         // Falls bereits fuenf oder mehr Benutzernamen durchprobiert wurden,
189         // soll das uebergeordnete System einmal pro Vorfall informiert werden.
190         if (se.affectedUsers >= 5) {
191           notifySuperior("once per correlated event set", se,
192                          "SSH-Loginversuche mit mind. fuenf Kennungen");
193         }
194
195         // Falls der Angriff mindestens 15 Sekunden anhaelt, soll eine Firewall-
196         // Regel erzeugt und aktiviert werden; darueber ist auch das
197         // uebergeordnete System zu informieren.
198
199         relevantEvents = getCorrelatedEventSet(se);
200         if(filterEvents(relevantEvents, "(type == SSH Brute Force) &&
201                         (timeInterval >= 15 seconds) &&
202                         (sourceIPaddress.constant == true)").size() > 0) {
203
204           firewall = searchResponseUnit("description == Backbone-Firewall");
205           callResponseUnitFunction(firewall, "addFilterBySourceIP", se.sourceIPaddress);
206           firewallTimer = setTimer(onTimerEvent, "Remove Firewall Rule", se, NULL, 120,
207                                    firewallTimer);
208           notifySuperior(NULL, se, "Firewall-Regel erzeugt und aktiviert");
209
210         }
211
212     } // Ende der Fallunterscheidung "Ereignistyp == SSH Brute Force"
213
214     if (se.type == getEventTypeByName("SSH Login")) {
215       // Falls sich ein Benutzer erfolgreich per SSH auf der beobachteten
216       // Maschine eingeloggt hat und der letzte SSH-Brute-Force-Angriff weniger als
217       // fuenf Minuten zurueckliegt, soll das Sensormodul zur
218       // Benutzerverhaltensanalyse aktiviert werden.
219
220       now = time();
221       recentEventSet = getEventList(getDataBaseList(), (now - 300), now);
222       if (filterEvents(recentEventSet, "type == SSH Brute Force").size() > 0) {
223
224         activateModule(sensor, getModuleIdByName("SSH Behavioral Analysis"));
225         // Da der Sensor das Modul autark deaktiviert, sobald es zu einer Entscheidung
226         // darueber gekommen ist, ob das Nutzungsverhalten legitim ist, muss
227         // kein Timer konfiguriert werden.
228         notifySuperior(NULL, se, "Verdaechtiger SSH-Login wird genauer analysiert");
229
230       }
231
232     } // Ende der Fallunterscheidung "Ereignistyp == SSH Login"
233
234     if (se.type == getEventTypeByName("Legitimate Behavior")) {
235       // Falls das Sensormodul zur Verhaltensanalyse zum Schluss kommt, dass das
236       // Nutzungsverhalten legitim ist, soll das uebergeordnete System darueber
237       // informiert werden. Im anderen, hier nicht betrachteten Fall, koennte
238       // eine Reaktionskomponente angestossen werden, die z.B. die Benutzerkennung
239       // sperrt.
240
241       notifySuperior(NULL, se, "Nutzungsverhalten ist legitim");
242
243     } // Ende der Fallunterscheidung "Ereignistyp == Legitimate Behavior"
244   } // Ende der Fallunterscheidung "meldender Sensor == Host-IDS-Sensor"
245 } // Ende der Funktion onSensorEvent
246
247 [...]
```

Im nächsten Abschnitt werden die Eckdaten und Ergebnisse einer Simulation der Anwendung dieser Regelsätze vorgestellt, analysiert und bewertet.

7.2.6.3. Simulation, Analyse und Bewertung des Ablaufs

Bevor in Abschnitt 7.2.8 eine Bewertung des konzipierten Werkzeugs durchgeführt wird, soll im Folgenden eine grundlegende Analyse und Bewertung der Dynamikeigenschaften, die im Beispielszenario erzielt wurden, erarbeitet werden. Zu diesem Zweck wurde im Rahmen der vorliegenden Arbeit eine einfache Simulation implementiert, die neben der Abarbeitung der

obigen Regelsätze in der Auswertestation auch die beschriebenen Angriffsversuche nachstellt, die Erkennungsleistung der Sensoren nachahmt und die Auswirkungen der dynamisch erzeugten, temporären Firewallregeln berücksichtigt. Die Simulation nimmt eine Reihe von Vereinfachungen gegenüber realen Implementierungen vor, die auch der Veranschaulichung und Nachvollziehbarkeit dienen:

- Die kleinste betrachtete Zeiteinheit ist eine Sekunde. Innerhalb einer Sekunde können beliebig viele Nachrichten über das simulierte Netz verschickt werden, deren Reihenfolge nicht verändert wird und deren Empfang sichergestellt ist, sofern keine entsprechende Firewallfilterregel vorliegt. Netzüberlastsituationen und somit Paketverluste sowie ähnliche Fehlersituationen werden folglich nicht betrachtet. Werden innerhalb einer Sekunde zehn Pakete verschickt, so erhalten diese unabhängig von der Berücksichtigung ihrer Reihenfolge alle denselben Zeitstempel, d. h. es werden keine Sekundenbruchteile erfasst.
- Sensormeldungen und Steueranweisungen der Auswertestation werden latenzfrei zugestellt und instantan ausgewertet, d. h. es werden weder Zeitverzögerungen beim Aktivieren bzw. Deaktivieren von Sensoren und Modulen betrachtet noch wird berücksichtigt, dass die Auswertestation möglicherweise nicht alle Sensormeldungen in Echtzeit abarbeiten kann.

  Diese Eigenschaft führt zu einem unrealistischen Verhalten der Simulation in dem Punkt, dass ein Datenpaket, das vom Backbone-IDS-Sensor als Angriffsbestandteil an die Auswertestation gemeldet wird und dort dazu führt, dass ein anderer Sensor (Subnet-IDS-Sensor bzw. Host-IDS-Sensor) zugeschaltet wird, auch bereits vom gerade erst aktivierten Sensor ausgewertet werden kann. Um ein solches Verhalten in der Praxis zu erzielen, müsste z. B. das auslösende Datenpaket im Rahmen der Aktivierungsnachricht mit an den zuzuschaltenden Sensor übermittelt werden; diese unkonventionelle Maßnahme würde jedoch von keiner derzeit bekannten Sensorimplementierung unterstützt werden. Für die Simulationsergebnisse hat dies keine Auswirkung, außer dass jede neue Angriffsphase bereits eine Zeiteinheit früher erkannt wird als dies im Realbetrieb mit herkömmlichen Sensoren vermutlich möglich wäre. Auf entsprechende Einschränkungen der Erkennungsleistung wird in Abschnitt 7.2.8 näher eingegangen.
- Der Angreifer scannt in der betrachteten demilitarisierten Zone des Szenarios 250 Ziel-IP-Adressen mit einer konstanten Geschwindigkeit von 10 Ziel-IP-Adressen pro Sekunde. Insbesondere werden keine Maßnahmen des Angreifers betrachtet, um sich den vorhandenen Sensoren zu entziehen oder diese gezielt anzugreifen.

In Abschnitt 7.2.6.1 wurde bereits der Ablauf der Angriffe in drei Phasen vorgestellt und beschrieben, wie szenarienweit darauf reagiert werden soll. Als Präzisierung dieser Abläufe und Simulationsergebnis der Anwendung der in Abschnitt 7.2.6.2 dargestellten Regelsätze lassen sich die folgenden Schlüsselereignisse und -zeitpunkte festhalten:

- Die Simulation beginnt zum Zeitpunkt $T = 1$. Der Angreifer mit konstanter Quell-IP-Adresse A_1 beginnt seinen SSH-Portscan mit der Geschwindigkeit von 10 Ziel-IP-Adressen pro Sekunde. Beim 10. SSH-Verbindungsversuch meldet der Backbone-IDS-Sensor den SSH-Portscan an die Auswertestation, was dazu führt, dass ebenfalls noch zum Zeitpunkt $T = 1$ der Subnet-IDS-Sensor aktiviert wird; dieser wertet den 10. Verbindungsversuch als erstes vom ihm betrachtetes Ereignis aus. Bei seiner Aktivierung

wird ein 60-Sekunden-Zeitgeber eingerichtet, der zum Zeitpunkt $T = 61$ den Subnet-IDS-Sensor wieder deaktivieren würde.

- Zum Zeitpunkt $T = 2$ erstellt der Subnet-IDS-Sensor nach 10 von ihm analysierten SSH-Verbindungsversuchen die Diagnose, dass ein harmloser SSH-Portscan vorliegt. Er meldet dies an die Auswertestation, die ebenfalls bei $T = 2$ das übergeordnete SIEM-System informiert.

- Von $T = 3$ bis $T = 25$ werden die restlichen der 250 betrachteten Ziel-IP-Adressen gescannt. Der Subnet-IDS-Sensor meldet jeden 10. Versuch, d. h. einmal pro Sekunde, an die Auswertestation. Diese gibt die Meldungen jedoch nur alle 10 Sekunden an das SIEM-System weiter, also zu den Zeitpunkten $T = 2, 12, 22$.

  Mit jeder Meldung des Subnet-IDS-Sensors an die Auswertestation und somit jede Sekunde wird der Zeitgeber für die Sensordeaktivierung neu gestellt. Da die letzte Meldung zum Zeitpunkt $T = 25$ erfolgt, wird der Subnet-IDS-Sensor bei $T = 85$ wieder deaktiviert.

  Die erste der drei Angriffsphasen endet zum Zeitpunkt $T = 99$, wobei ab dem Zeitpunkt $T = 26$ keine Datenpakete mehr vom Angreifer geschickt werden.

- Bei $T = 100$ beginnt die zweite Angriffsphase mit den gezielten Angriffen von der bereits bekannten Quell-IP-Adresse A_1 auf die feste Ziel-IP-Adresse Z_1 des SSH-Gateways, wobei 1 Loginversuch pro Sekunde unternommen wird.

- Zum Zeitpunkt $T = 102$ meldet der Backbone-IDS-Sensor beim dritten Loginversuch innerhalb von 10 Sekunden den Angriffsverdacht an die Auswertestation, die daraufhin den Host-IDS-Sensor mit dem Modul zur Protokolldateianalyse aktiviert. Der Backbone-IDS-Sensor meldet weiterhin jeden dritten Loginversuch an die Auswertestation, d. h. bei $T = 102, 105, 108, 111, 114$. Für das Deaktivieren des Host-IDS-Sensors wird ein 5-Sekunden-Zeitgeber eingerichtet.

- Der Host-IDS-Sensor meldet die Loginversuche immer dann an die Auswertestation, wenn der Angreifer 5 verschiedene Benutzernamen ausprobiert hat, also zu den Zeitpunkten $T = 106, 111, 116$. Die erste Meldung bei $T = 106$ wird auch ans übergeordnete SIEM-System propagiert. Mit jeder Meldung des Host-IDS-Sensors wird der Zeitgeber zu seiner Deaktivierung neu gestellt.

- Die Host-IDS-Sensormeldung zum Zeitpunkt $T = 116$ wird bei der Auswertung der Regelsätze in der Analysestation zum Indikator dafür, dass der Angriff bereits länger als 15 Sekunden anhält. Als Folge davon wird eine neue Firewallfilterregel scharfgeschaltet, über die auch das übergeordnete SIEM-System informiert wird. Zudem wird ein 120-Sekunden-Zeitgeber eingerichtet, der zum hier betrachteten Zeitpunkt dafür sorgen würde, dass die Firewallregel bei $T = 236$ wieder deaktiviert wird.

- Aufgrund der neuen Firewallregel werden die vom Angreifer im Zeitraum $T = 117$ bis $T = 179$ durchgeführten Loginversuche verworfen. Da der Host-IDS-Sensor somit keine Angriffe mehr verzeichnet, wird er 5 Sekunden nach seiner letzten Meldung zum Zeitpunkt $T = 121$ von der Analysestation deaktiviert.

  Die zweite Angriffsphase endet zum Zeitpunkt $T = 199$, wobei ab dem Zeitpunkt $T = 180$ keine Angreiferaktivitäten mehr vorliegen. Zum Ende dieser zweiten Phase

ist bezüglich der Detektionsmechanismen wiederum nur der Backbone-IDS-Sensor aktiv, wobei im Unterschied zur Ausgangssituation bei $T = 0$ eine Firewallregel aktiv ist, die bis $T = 236$ gültig sein soll.

- Die dritte Angriffsphase beginnt bei $T = 200$ mit zwei parallelen SSH-Loginversuchen auf der bekannten Zielmaschine Z_1, die von den neuen Quell-IP-Adressen A_2 und A_3 ausgehen. Auch in diesem Fall wird wieder 1 Loginversuch pro Sekunde unternommen.
- Zum Zeitpunkt $T = 201$ erfolgt der zweite SSH-Loginversuch von A_2 auf Z_1. Aufgrund des weniger als 5 Minuten zurückliegenden SSH-Brute-Force-Angriffs, der durch die neue Firewallregel zum Erliegen gebracht wurde, reicht bereits ein Schwellenwert von 2 Verbindungsversuchen dazu aus, dass die Analysestation den Host-IDS-Sensor mit dem Modul zur Protokolldateiüberwachung aktiviert ($T = 201$). Für den Sensor wird ein 5-Sekunden-Zeitgeber zur Deaktivierung gestartet, der bei jeder der nachfolgend eintreffenden Meldungen umkonfiguriert, d. h. wieder auf 5 Sekunden gesetzt wird.

  Der Host-IDS-Sensor ist somit bereits aktiv, wenn ebenfalls zum Zeitpunkt $T = 201$ der zweite und diesmal erfolgreiche SSH-Verbindungsversuch von A_3 auf Z_1 durchgeführt wird. Der Host-IDS-Sensor meldet dieses Ereignis an die Auswertestation, die es im Kontext der in den letzten 5 Minuten eingegangenen Meldungen als suspekt bewertet, so dass auch das Host-IDS-Sensormodul zur heuristischen Benutzerverhaltensanalyse aktiviert wird. Über dieses Modulzuschalten wird auch das SIEM-System informiert.
- Die SSH-Loginversuche von A_2 auf Z_1 gehen unabhängig davon weiter. Die Auswertungen der entsprechenden Meldungen des Backbone-IDS-Sensors finden zu den Zeitpunkten $T = 201, 203, 205, 207, 209, 211, 213, 215, 217, 219$ statt. Der Host-IDS-Sensor meldet parallel dazu bei $T = 205, 210, 215, 220$ die Loginversuche mit jeweils 5 verschiedenen Benutzernamen. Bei der ersten Meldung zum Zeitpunkt $T = 205$ wird auch das SIEM-System informiert.
- Zum Zeitpunkt $T = 207$ entscheidet der Host-IDS-Sensor auf Basis der Verhaltensanalyse, dass die Nutzung der von A_3 ausgehenden SSH-Verbindung legitim ist und deaktiviert das entsprechende Modul autark. Die Auswertestation gibt die Entwarnung an das SIEM-System weiter.
- Die zum Zeitpunkt $T = 220$ eingehende Meldung des Host-IDS-Sensors über die anhaltenden SSH-Loginversuche von Quell-IP-Adresse A_2 weist unter Bezug auf die entsprechende Meldung bei $T = 205$ wiederum darauf hin, dass der Angriff länger als 15 Sekunden anhält. Entsprechend wird analog zum Ablauf in der zweiten Angriffsphase eine neue Firewallregel aktiviert, über die auch das SIEM-System informiert wird. Der Zeitpunkt für die geplante Deaktivierung der dynamisch angelegten Firewallregeln verschiebt sich dadurch von $T = 236$ auf $T = 340$ (aktueller Zeitpunkt plus 120 Sekunden).
- Durch die neu angelegte Firewallregel werden die weiteren Loginversuche des Angreifers, die von der IP-Adresse A_2 ausgehen, im Zeitraum $T = 221$ bis $T = 229$ blockiert. Ab $T = 230$ unternimmt der Angreifer keine weiteren Aktivitäten mehr.
- Zum Zeitpunkt $T = 225$ wird der Host-IDS-Sensor mit seinem bis dahin noch aktiven Modul zur SSH-Protokolldateianalyse deaktiviert, da er 5 Sekunden lang keine neuen Meldungen liefert. Zum Zeitpunkt $T = 229$ endet auch die legitime Benutzeraktivität. Bei $T = 340$ werden die dynamisch angelegten Firewallregeln termingerecht wieder gelöscht; eine Benachrichtigung darüber wird ans SIEM-System geschickt.

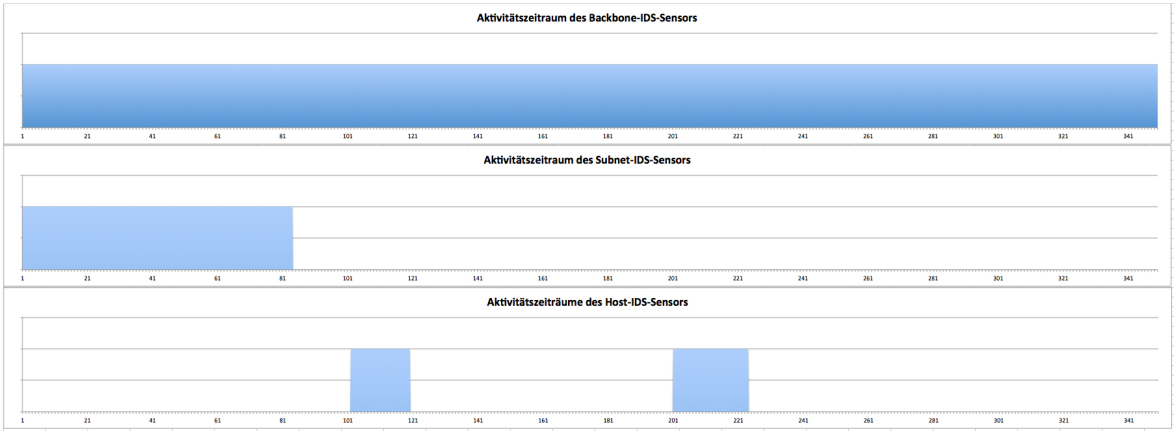


Abbildung 7.8.: Gegenüberstellung der Sensoraktivitätszeiträume im Anwendungsbeispiel (T=1 bis T=350)

- Die Simulation endet zum Zeitpunkt $T = 350$, zu dem sich das Gesamtsystem wieder im selben Zustand befindet wie am Anfang bei $T = 0$.

Diese Simulationseckdaten zeigen zunächst grundlegend, dass die für das Beispielszenario postulierten Reaktionen mit dem konzipierten Werkzeug umgesetzt werden können: Alle Angriffe werden erkannt und korrekt behandelt; auch die legitime Nutzung einer SSH-Verbindung wird korrekt beurteilt und führt nicht etwa zu einem False-Positive-Fehler. Im Szenario wird somit dieselbe Erkennungsleistung erzielt, wie sie auch von herkömmlichen IDS-Implementierungen verlangt werden würde.

Zur Bewertung der spezifizierten und im Beispiel genutzten Dynamikeigenschaften muss deshalb untersucht werden, welche Ressourceneinsparungen gegenüber einem herkömmlichen IDS-Einsatz, bei dem alle Sensoren durchgehend aktiv sind, erzielt werden konnten; diese Einsparungen sind dem u. a. durch die zu erzeugenden, transportierenden und verarbeitenden Steueranweisungen für das Aktivieren und Deaktivieren einzelner Sensoren und Module anfallenden Aufwand gegenüberzustellen. Nicht näher betrachtet wird hingegen der Implementierungsaufwand für die Ansteuerung der Dynamikeigenschaften in den Regelsätzen der Auswertestation. Im Wesentlichen handelt es sich dabei um Ergänzungen der unabhängig von der Dynamik benötigten Regeln zur Weitergabe von Informationen an das SIEM-System sowie zum Anstoßen der Reaktionskomponenten; über geeignete Werkzeuge zum Management dieser Regelsätze könnte der manuelle Zusatzaufwand minimiert werden.

Abbildung 7.8 fasst die Zeiträume zusammen, in denen die drei betrachteten Sensoren aktiv sind. Lediglich der Backbone-IDS-Sensor, dessen Ereignismeldungen die Schlüssel für die Aktivierung weiterer Sensoren und Module darstellen, ist wie im herkömmlichen Fall durchgängig aktiv. Demgegenüber sind über die Gesamtsimulationszeit von 350 Sekunden, die auch einige praxisnahe Ruhephasen ohne akute Angriffe aufweist, der Subnet-IDS-Sensor insgesamt nur 84 und der Host-IDS-Sensor lediglich 43 Sekunden lang aktiv, so dass gegenüber dem herkömmlichen Fall von den beiden Sensoren nur rund ein Viertel bzw. ein Achtel der Gesamtsimulationszeit lang die zur Überwachung benötigten Ressourcen belegt werden.

Betrachtet man anstelle der Aktivierungszeiträume die zu verarbeiteten Datenpakete, so gehen insgesamt 390 Nachrichten von außen ein, von denen jedoch 72 vom Firewall gefiltert werden, so dass der Backbone-IDS-Sensor 318 Nachrichten analysiert. Der Subnet-IDS-Sensor analysiert bereits in den ersten 25 Sekunden der Simulation alle 241 von ihm zu bearbeitenden Datenpakete; dabei handelt es sich um den 250 Nachrichten umfassenden SSH-Portscan in der ersten Angriffsphase, zu dem er ab dem zehnten Datenpaket zugeschaltet wird. Der Host-IDS-Sensor verarbeitet insgesamt 60 Nachrichten. Gegenüber dem herkömmlichen Fall werden somit nur beim Subnet-IDS-Sensor nennenswerte Ressourceneinsparungen gegenüber der Analyse von 318 Nachrichten, also etwas weniger als ein Viertel, erzielt. Der Host-IDS-Sensor wird hingegen zur Präzisierung der Diagnose immer sehr schnell zugeschaltet, so dass er fast alle Datenpakete analysiert, die ihm auch im Dauerbetrieb vorliegen würden. Weitere Ressourceneinsparungen wären durch ein langsameres Zuschalten oder nach Erstdiagnose rascheres Abschalten möglich, könnten jedoch zu Lasten der Erkennungsleistung gehen.

Im Simulationszeitraum werden insgesamt zehn Nachrichten an das SIEM-System generiert und es sind 224 Sekunden lang dynamisch erzeugte Firewallregeln aktiv, was dem herkömmlichen Betriebsfall entspricht. Von der Auswertestation werden 49 Sensormeldungen verarbeitet; 16 davon stammen vom Backbone-IDS-Sensor, 24 vom Subnet-IDS-Sensor und neun vom Host-IDS-Sensor. Die Auswertestation generiert insgesamt zehn Steueranweisungen, von denen drei die Firewall, zwei den Subnet-IDS-Sensor und fünf den Host-IDS-Sensor betreffen; der Host-IDS-Sensor generiert und verarbeitet autark eine sechste Steueranweisung zur Deaktivierung des Moduls zur Benutzerverhaltensanalyse. Insgesamt treten vier zeitgesteuerte Ereignisse in der Auswertestation ein.

Abbildung 7.9 stellt diesen Aufwand dem herkömmlichen, statischen Betriebsmodell gegenüber, in dem zwar mehr Nachrichten verarbeitet werden müssen, aber abgesehen vom Anstoßen der Reaktionskomponenten keine Steueranweisungen erzeugt und verarbeitet werden müssen. Um den Gesamtaufwand abschätzen zu können, wird folgende Gewichtung vorgenommen:

- Der Ressourcenaufwand eines laufenden Sensors, der in einer Zeiteinheit keine Nachricht zu verarbeiten hat, wird mit 0,5 Punkten gewertet.
- Das Verarbeiten einer Nachricht durch einen aktiven Sensor fließt mit 1 Punkt ein.
- Das Erzeugen einer Ereignismeldung (von einem Sensor an die Auswertestation bzw. von der Auswertestation an das SIEM-System) fließt ebenfalls mit 1 Punkt ein.
- Das Auswerten einer Sensormeldung durch die Auswertestation fließt mit 2 Punkten ein.
- Ebenso wird das Erzeugen einer Steueranweisung durch die Auswertestation und die Umsetzung dieser Steueranweisung durch den Sensor bzw. die Reaktionskomponente mit 2 Punkten gewichtet.

Durch diese Gewichtung wird abgebildet, dass einerseits ein aktiver, aber eigentlich nicht benötigter Sensor nur einen Teil seiner Ressourcen verbraucht, und dass andererseits die komplexeren Regelsätze für die Auswertestation und die zu erzeugenden und zu verarbeitenden Steueranweisungen mit einem höheren Aufwand verbunden sind als der herkömmliche Betrieb. Unter diesen Annahmen zeigt sich in der abgebildeten Gesamtauswertung, dass mit dem hier erarbeiteten, dynamischen Ansatz rund 24% des Gesamtaufwands eingespart werden können (992 vs. 1306 Gesamtpunkte). Die Gesamtpunktezahl wird dabei jeweils durch die

		Dynamisches IDS		Herkömmliches IDS	
Art des Aufwands	**Faktor**	**Anzahl**	**Punktezahl**	**Anzahl**	**Punktezahl**
Zeiteinheit mit aktivem Backbone-IDS-Sensor ohne Input	0,5	278	139	278	139
Vom Backbone-IDS-Sensor verarbeiter Input	1	318	318	318	318
Zeiteinheit mit aktivem Subnet-IDS-Sensor ohne Input	0,5	60	30	278	139
Vom Subnet-IDS-Sensor verarbeiteter Input	1	241	241	318	318
Zeiteinheit mit aktivem Host-IDS-Sensor ohne Input	0,5	10	5	302	151
Vom Host-IDS-Sensor verarbeiteter Input	1	60	60	69	69
Vom Backbone-IDS-Sensor erzeugte Meldung	1	16	16	16	16
Vom Subnet-IDS-Sensor erzeugte Meldung	1	24	24	25	25
Vom Host-IDS-Sensor erzeugte Meldung	1	9	9	9	9
Von der Auswertestation erzeugte Meldung	1	10	10	10	10
Von Auswertestation bearbeitete Sensormeldung	2	49	98	50	100
Von Auswertestation generierter Steuerbefehl	2	10	20	3	6
Vom Firewall ausgeführter Steuerbefehl	2	3	6	3	6
Vom Subnet-IDS-Sensor ausgeführter Steuerbefehl	2	2	4	0	0
Vom Host-IDS-Sensor ausgeführter Steuerbefehl	2	6	12	0	0
Aufsummierte Punktezahl			**992**		**1306**

Anmerkungen zum dynamischen IDS:
Der Host-IDS-Sensor wird 2x nach 5 Sekunden Idle-Zeit deaktiviert.
Der Subnet-IDS-Sensor wird 60 Sekunden nach seiner letzten Meldung deaktiviert.

Anmerkungen zum herkömmlichen IDS:
Backbone-IDS-Sensor und Subnet-IDS-Sensor sehen im Szenario dieselben Datenpakate und haben entsprechend die selben Aktivitäts- und Idle-Zeiten.
Anzahl der Zeiteinheiten mit Input für Host-IDS-Sensor:
1 während der ersten Angriffsphase, wenn der SSH-Gateway gerade gescannt wird.
17 während der zweiten Angriffsphase, bis zum Aktivwerden der Firewallregel.
30 während der dritten Angriffsphase, bis zum Ende der Nutzeraktivität.
Somit verbleiben 302 Zeiteinheiten, in denen der Host-IDS-Sensor keinen Input erhält.
Anzahl der Datenpakete, die vom Host-IDS-Sensor verarbeitet werden:
1 während der ersten Angriffsphase.
17 während der zweiten Angriffsphase.
51 während der dritten Angriffsphase.
Somit insgesamt 69 vom Host-IDS-Sensor verarbeitete Datenpakete.

Abbildung 7.9.: Gegenüberstellung des Ressourcenaufwands bei Anwendung der Dynamikkonzepte und bei herkömmlichem IDS-Betrieb

Anzahl an Nachrichten, die der Backbone-IDS-Sensor und der Subnet-IDS-Sensor analysieren müssen, und den durchgängigen Betrieb des Backbone-IDS-Sensors dominiert. Betrachtet man ausschließlich den Host-IDS-Sensor, so ergeben sich mit den Teilpunktezahlen 86 vs. 229 Einsparungen von mehr als 62%, obwohl im Szenario gezielte Angriffe auf die Maschine, auf der dieser Host-IDS-Sensor installiert ist, betrachtet werden.

Das praktisch zu erzielende Einsparpotenzial muss jedoch für jedes Szenario im Einzelnen untersucht werden und hängt unter anderem von der Häufigkeit von Angriffen und der Implementierungsstrategie ab, insbesondere ob beispielsweise verfügbare Sensoren nur stufenweise zugeschaltet oder ob beim Vorliegen eines ersten Verdachtsmoments sofort alle aufgrund ihrer technischen Fähigkeiten in Frage kommenden Sensoren auf einmal aktiviert werden. Es ist offensichtlich, dass umso höhere Einsparungen in der Praxis erzielt werden können, je mehr dezentrale Subnet-IDS-Sensoren und Host-IDS-Sensoren eingesetzt werden sollen, die nur bei Bedarf zugeschaltet werden; davon losgelöst bleibt der Grundsatz erhalten, dass die Anzahl

der IDS-Sensoren unter Berücksichtigung der erforderlichen Erkennungsleistung minimal gehalten werden sollte.

7.2.7. Prozessuale Einbettung im Kontext von Security-Frameworks

Über das beschriebene technische Zusammenspiel zwischen Auswertestation, Sensoren und SIEM-Systemen hinaus soll nun auch knapp die Einbettung der dynamischen IDS-Sensorik in die Managementprozesse und die Gesamtsicherheitsstrategie betrachtet werden. Ausschlaggebend ist dabei, dass die Sensorik den Ausgangspunkt für alle *automatisierten* Detektionsmechanismen darstellt, von denen die Maßnahmen zur Prävention von Sicherheitsvorfällen komplementiert und die vorhandenen Mechanismen zur Reaktion auf Sicherheitsvorfälle angestoßen werden, die darauf abzielen, den Schaden noch vor seinem Eintreten zu verhindern oder zumindest zu minimieren. Demgegenüber werden *manuell* häufig nicht die Angriffe selbst, sondern nur die Symptome ihrer Folgen erkannt, so dass lediglich Folgeangriffe verhindert und IT-forensische Maßnahmen eingeleitet werden können.

Die Regelsätze, nach denen die Auswertestation und die Sensoren intern arbeiten, dienen entsprechend dazu, Policies umzusetzen bzw. deren Einhaltung zu kontrollieren; sie setzen deshalb voraus, dass jeweils das gewünschte vom unerwünschten System- und Nutzungsverhalten mit hinreichender Schärfe differenziert werden kann. Somit können jedoch weder Policies noch Regelsätze statisch sein, sondern müssen regelmäßig auf ihre Effektivität und ggf. auch Effizienz hin überprüft und entsprechend kontinuierlich verbessert bzw. an die sich wandelnde Umgebung angepasst werden. Insbesondere können beispielsweise neue Angriffsarten, Prioritätsveränderungen im Risikomanagement, die Verfügbarkeit neuer Sensoren und Module, die Einführung neuer Reaktionskomponenten, neu eingeführte Assets und Dienste, Modifikationen an der Netztopologie und viele weitere Änderungen, die dem Change Management unterliegen, zur Notwendigkeit einer Überarbeitung der Regelsätze führen.

Für die Integration in die in Kapitel 6 beschriebenen Managementabläufe sind darüber hinaus die folgenden weiteren Schnittstellen zu berücksichtigen:

- Die Anbindung an das **Incident Management** und den **Security-Incident-Response-Prozess** erfolgt einerseits durch den Abgleich der Regelsätze, die beispielsweise die Priorisierung von Sicherheitsmeldungen implementieren (vgl. Schritt 11 in der in Abschnitt 7.2.3 spezifizierten Verarbeitungskette), und andererseits durch das Weiterreichen von Sicherheitsalarmen an das SIEM-System sowie ggf. weitere Managementsystem (vgl. Abschnitt 6.5.2.4).
- Die **Entwicklungs- und Testphasen** sowie periodisch durchgeführte **Sicherheitsüberprüfungen** können dadurch gezielt unterstützt werden, dass die in den Regelsätzen verwendeten Triggermechanismen modifiziert werden; dadurch können Probealarme auch ohne Vorliegen eines tatsächlichen Angriffs ausgelöst und die dafür programmierten Reaktionen analysiert werden. Je nachdem, wie aktiv die Reaktionskomponenten in die Infrastruktur eingreifen, muss im Gegenzug jedoch auch sichergestellt werden, dass von einem Angreifer möglicherweise erfolgreich durchgeführte Modifikationen von Sensoren und Auswertestationen keine unkontrollierbaren Auswirkungen nach sich ziehen. Durch die Einführung von Detektions- und automatisierten Reaktionsmechanismen können sich folglich neue Schwachstellen ergeben, die im Rahmen des Risikomanagements zu betrachten sind.

- Insbesondere beim Einsatz mehrerer Auswertestationen und Sensoren müssen einerseits deren konsistente, aufeinander abgestimmte Konfiguration und Parametrisierung sichergestellt werden. Andererseits muss auch die Verfügbarkeit und Betriebsfähigkeit aller eingesetzten IDS-Komponenten überwacht und ggf. wiederhergestellt werden. Zu diesem Zweck kann beispielsweise über die in diesem Kapitel beschriebene Kopplung zwischen Auswertestationen und den an sie angeschlossenen Systemen hinausgehend eine Integration in **Monitoringsysteme und Managementplattformen** erfolgen.

Über das Propagieren von Sicherheitsmeldungen z. B. an das SIEM-System hinaus können die dynamischen IDS-Komponenten auch sicherheitsrelevante Kennzahlen liefern, beispielsweise wie viele Angriffe erkannt wurden, wie viele und welche Reaktionsmechanismen automatisch angestoßen wurden, wie oft dynamische Reparametrisierungen vorgenommen wurden und welches Ausmaß Angriffe vor ihrer Eindämmung annehmen konnten.

Im Kontext von Security-Frameworks müssen ferner folgende Spezifika berücksichtigt werden:

- Die für Auswertestationen spezifizierte Vorgehensweise und Funktionalität kann in die Steuerkomponenten von Security-Frameworks integriert werden, insbesondere wenn diese eine Reihe von Detektionssensoren und ins Framework integrierte Reaktionskomponenten vorsehen. Die Frameworksteuerkomponente kann in diesem Fall entweder als gleichberechtigte Analysestation in der IDS-Gesamtarchitektur fungieren oder gegenüber einer frameworkexternen Analysestation als entsprechend flexibler Sensor mit einer Reihe von Modulen sowie als Aggregat von Reaktionskomponenten fungieren.
- Für den Fall, dass das Security-Framework ein entsprechendes Zusammenspiel mit externen Analysestationen nicht vorsieht, muss auf die Konsistenz der IDS-Regelsätze mit dem im Rahmen des Security-Frameworks implementierten Reaktionsmechanismen geachtet werden. Durch ein Überlappen der Überwachungsbereiche von Security-Frameworks und IDS-Sensoren kann in diesem Fall eine gegenseitige Zuverlässigkeitskontrolle erfolgen und somit ein Teilaspekt des Defense-in-depth-Paradigmas umgesetzt werden.
- Beispielsweise falls das Security-Framework nicht den für die hier vorgestellten Konzepte verwendeten IDMEF-Standard unterstützt, kann für eine Integration der Frameworkkomponenten der Einsatz dedizierter Datenkonverter bzw. Gateways erforderlich werden, deren Bereitstellung – neben der Auswahl und Zusammenstellung von Detektionskomponenten – im Rahmen des Customizing-Prozesses von Security-Frameworks berücksichtigt werden muss.

Schließlich muss auch bedacht werden, dass die Konzepte von Security-Frameworks neben technischen Reaktionen auch organisatorische Handlungsanweisungen umfassen, so dass die nahtlose Integration nicht nur die hier vorrangig betrachteten technischen Infrastrukturkomponenten umfasst.

7.2.8. Bewertung des konzipierten Werkzeugs

Die Werkzeugkonzeption abschließend werden die Stärken und Schwächen des erarbeiteten Ansatzes herausgestellt und einige offene Punkte, die vertiefende Untersuchungen in Folgearbeiten motivieren, skizziert. Positiv sind zunächst folgende Aspekte festzuhalten:

- Durch das dynamische Zu- und Abschalten sowie das Reparametrisieren der Detektionssensorik kann der Ressourcenverbrauch signifikant verringert werden. Neben den von den Sensoren zur Detektion benötigten Ressourcen betrifft dies insbesondere auch die Auswertestation, die insgesamt weniger Sensormeldungen zu verarbeiten hat und sich auf die für die akut vorliegenden Angriffe relevanten Meldungen fokussieren kann.
- Die dynamikspezifischen Steuerungs- und Automatisierungsmöglichkeiten können nahtlos in die bei IDS-Systemen bereits vorhandene Verarbeitungskette und die Regelsätze zur Bearbeitung von Sensor- und Timermeldungen integriert werden, so dass keine völlig neuen oder parallelen Management- und Implementierungsarbeiten erforderlich werden.
- Die Erkennungsleistung der IDS-Gesamtarchitektur kann dem jeweils aktuellen Bedarf dynamisch angepasst werden und ist trotz der Ressourceneinsparungen im Allgemeinen (mindestens) deckungsgleich mit der Leistung herkömmlicher IDS-Systeme (vgl. latenzbedingte Einschränkungen unten).
- Durch die konfigurierbare, selektive Weitergabe von Sicherheitsmeldungen an externe Komponenten, beispielsweise SIEM-Systeme, kann eine nahtlose Integration in den Security-Incident-Response-Prozesse und ähnliche Managementabläufe erreicht werden.
- Bereits vorhandene Sensorik, die beispielsweise von Security-Frameworks mitgeliefert wird, kann integriert werden; durch die Verwaltung der Sensor- und Moduleigenschaften können auch Beschränkungen, beispielsweise dass Module nicht deaktiviert werden können, berücksichtigt werden.
- Komplexe Sensoren, die autarke Steuerungsentscheidungen treffen können, wurden ebenso berücksichtigt wie mobile oder temporär isolierte Sensoren, die Ereignismeldungen lokal speichern und zum späteren Abruf zur Verfügung stellen.
- Sowohl die Sensoren als auch die Auswertestationen ermöglichen eine von außen durchgeführte Konfiguration und unterstützen somit die Integration in zentrale Managementplattformen.

[MHL+03] und [Jah02] stellen Beurteilungskriterien für IDS-Systeme zusammen, mit denen die Qualität von Sensoren und Analysestationen bewertet werden kann. Betrachtet man davon lediglich diejenigen Aspekte, an denen sich im Rahmen dieser Arbeit gegenüber herkömmlichen IDS-Architekturen Änderungen ergeben haben, so resultiert die oben bereits genannten Punkte ergänzend folgendes Bild:

- Die Skalierbarkeit der IDS-Architektur verbessert sich, da die Anzahl der im selben Zeitraum von der Auswertestation zu verarbeitenden Sensormeldungen von der direkt steuerbaren Anzahl der *aktiven* Sensoren und nicht lediglich von der Anzahl der installierten Sensoren abhängt (vgl. [MHL+03, Abschn. 3.5]).
- Die Diagnose von Angriffen kann im erarbeiteten Ansatz durch das gezielte Zuschalten weiterer Sensoren präzisiert werden (vgl. [MHL+03, Abschn. 3.8]).
- Durch das bedarfsorientierte Zuschalten von Host-IDS-Sensorik wird die Performance derart überwachter Systeme minimal gehalten (vgl. [Jah02, Anf. R4]).
- Die Ansteuerung der Sensoren und Reaktionskomponenten erfolgt modular und ist damit für verschiedene Anwendungen innerhalb eines Szenarios oder ggf. darüber hinaus wiederverwendbar (vgl. [Jah02, Anf. R14]).

Mit dem konzipierten Werkzeug ergeben sich jedoch auch die folgenden neuen Herausforderungen:

- Der Einsatz des konzipierten Werkzeugs setzt einen regulären Schutzbedarf voraus, bei dem die legitime Infrastrukturnutzung gegenüber dem Vorliegen akuter Angriffe im Vordergrund steht. Falls hingegen fast durchgängig Angriffsversuche unternommen werden oder lediglich Sensoren eingesetzt werden, die alle durchgängig betrieben werden müssen, um erste Hinweise auf Angriffe zu erhalten, ist das Ressourceneinsparpotenzial minimal und rechtfertigt die zusätzliche Implementierungskomplexität nicht.
- Durch die Automatisierung von Reaktionsmaßnahmen muss verstärkt darauf geachtet werden, dass die IDS-Architektur nicht selbst zum Ziel oder Verstärker von Angriffen wird. Beispielsweise könnte ein Angreifer, der die automatischen Reaktionen a priori kennt oder durch Versuche ermittelt hat, durch primitive, aber gezielte Angriffe Denial-of-Service-Situationen provozieren.
- Durch das als rein reaktive Maßnahme betrachtete Zuschalten weiterer Sensoren ergeben sich Latenzen bei der Angriffserkennung, die im Worst Case dazu führen, dass erfolgreiche Angriffe nicht erkannt werden, da kein entsprechender Sensor betriebsbereit ist. Abhilfe kann nur geschaffen werden, indem ausgewählte Sensoren, die eine Basisabdeckung ermöglichen, kontinuierlich aktiv bleiben, und indem Möglichkeiten implementiert werden, verdächtige Datenpakete zu speichern und nach Abschluss des Sensorstartvorgangs zu analysieren.

Neben Lösungsansätzen für die genannten potentiellen Defizite sollte in weiteren Arbeiten auch untersucht werden, wie die bislang manuelle Implementierung der Dynamiksteuerung im Rahmen der Regelsätze erleichtert werden kann, beispielsweise indem auf Basis der vorhandenen Sensorverwaltungsinformationen automatisierte Regeln generiert werden, die abhängig von den verarbeiteten Sensormeldungen weitere Sensoren und Module zu- bzw. abschalten. In diesem Kontext sollte auch untersucht werden, wie Skalierbarkeit, Erkennungsleistung und Angreifbarkeit des IDS-System beeinflusst werden, wenn aus einer Menge zueinander ähnlicher Sensoren nicht wie vorgeschlagen prioritätsbasiert, sondern beispielsweise randomisiert ausgewählt wird.

Ferner sollten auch Erweiterungen zu verteilten und kooperativen IDS-Architekturen betrachtet werden, deren Regelsätze die gemeinsame Sensornutzung durch mehrere Auswertestationen sowie die selektive, ggf. teilanonymisierte Weitergabe von Sicherheitsmeldungen an hierarchische oder anders vermaschte Netze von Auswertestationen vorsehen muss. Aus Perspektive des Managements von Sicherheitskomponenten sind schließlich Hilfsmittel erforderlich, die dazu dienen, zu erkennen, wann welche IDS-Regelsätze überarbeitet werden müssen, beispielsweise da sich durch Infrastrukturerweiterungen neue Bereiche ergeben haben, die von der vorhandenen Detektionssensorik noch nicht ausreichend abgedeckt werden.

7.3. Werkzeug für das Security-Framework-orientierte Erheben und Aufbereiten von Sicherheitskennzahlen

In Kapitel 6 wurde bereits eingehend dargestellt, dass es sich bei der Erfassung, Auswertung und Präsentation IT-sicherheitsspezifischer Kennzahlen um einen Aufgabenbereich des

Sicherheitsmanagements handelt, für den bislang noch keine technischen Standards und darauf abgestimmte technische Werkzeuge existieren. Jaquith kommt in [And07, S. 224ff.] zu dem Schluss, dass in Organisationen bislang – falls überhaupt – lediglich Ad-hoc-Lösungen zum Einsatz kommen, bei denen Sicherheitsberichte auf Basis von Tabellenkalkulationssoftware oder durch die „Zweckentfremdung“ von SIEM-Systemen bzw. anderen bereits vorhandenen Managementwerkzeugen erzeugt werden. Im Folgenden wird ein Werkzeug konzipiert, das dediziert zur allgemeinen Akquisition, Verwertung und Präsentation von IT-Sicherheitskennzahlen genutzt werden kann und im Speziellen auf die Besonderheiten von und Schnittstellen zu Security-Frameworks eingeht.

Das Erfassen und Darstellen von Messwerten und Kennzahlen im Umfeld der IT-Sicherheit hat offensichtliche Analogien zum Einsatz von Monitoringsystemen, die der kontinuierlichen Überwachung im Rahmen des Netz- und Systemmanagements dienen. In Abschnitt 7.3.1 wird deshalb zunächst eine Abgrenzung gegenüber Monitoringwerkzeugen und in diesem Kontext verwandten Arbeiten vorgenommen. Nachdem in Abschnitt 6.6 bereits die mit IT-Sicherheitskennzahlen und dem damit verbundenen Berichtswesen einhergehenden Ziele und der prinzipielle, prozessorientierte Erfassungs- und Aufbereitungsablauf dargestellt wurden, werden in Abschnitt 7.3.2 zunächst die daraus resultierenden technischen Anforderungen an das Werkzeug abgeleitet und seine Gesamtarchitektur spezifiziert; dabei werden die sich durch die Zerlegung des gesamten Werkzeugs in seine Einzelbestandteile ergebenden Komponenten jeweils bezüglich ihrer Aufgaben und ihres durch Schnittstellen realisierten Zusammenspiels mit den anderen Komponenten konzipiert.

Der erfolgreiche Einsatz des so erarbeiteten Werkzeugs hängt jedoch auch maßgeblich von seinen nach außen gerichteten Schnittstellen und Interaktionsmöglichkeiten zu anderen technischen Systemen und zu den prozessorientierten organisatorischen Abläufen ab. In Abschnitt 7.3.3 werden deshalb vertiefend die technischen Schnittstellen zu den potentiellen Datenquellen für Messwerte und Basiskennzahlen spezifiziert; neben den Steuerkomponenten von Security-Frameworks gehören hierzu auch andere technische Assets sowie weitere vorhandene Managementsysteme und -werkzeuge, die zur effizienten Gewinnung von Kennzahlen benötigt werden. In Abschnitt 7.3.4 werden dazu komplementär die Ausgabeschnittstellen spezifiziert und die Nutzung des Werkzeugs im Rahmen des Sicherheitsmanagementprozesses skizziert.

Abschnitt 7.3.5 fasst die mit dem konzipierten Werkzeug erreichten Ergebnisse abschließend zusammen, bewertet sie und stellt sie einer Reihe noch offener Punkte und möglicher Weiterentwicklungen gegenüber.

7.3.1. Abgrenzung zu Monitoringsystemen und verwandten Arbeiten

Die aus dem Netz- und Systemmanagement bekannten Monitoringsysteme erfassen verschiedene Charakteristika der Komponenten und Systeme einer IT-Infrastruktur – beispielsweise die aktuelle CPU-Auslastung von Servern und den Datendurchsatz in Netzkomponenten – und bereiten diese Informationen für das Betriebspersonal geeignet auf: Neben häufig interaktiv auswertbaren Visualisierungen sind auch Alarmierungsschnittstellen, beispielsweise per E-Mail oder SMS, vorgesehen. De facto werden Monitoringsysteme zur Verbesserung der Störungserkennung und -beseitigung in allen Organisationen benötigt, die mehr Dienste, Systeme bzw. Komponenten einsetzen als das vorhandene Administrationspersonal ständig direkt im

Blick halten und bezüglich der Einhaltung der QoS-Ziele zuverlässig beurteilen kann.

Neben zahlreichen kommerziellen Softwarepaketen und Open-Source-Implementierungen existiert auch eine größere Zahl an Forschungsprojekten und -arbeiten, die die sich im Laufe der Zeit wandelnden Anforderungen an Monitoringsysteme – insbesondere auch ihren Abdeckungsbereich und ihre Skalierbarkeit – gut widerspiegeln. Gerade aufgrund der Analogien zwischen Monitoringsystemen und dem hier thematisierten Werkzeug für das Management von IT-Sicherheitskennzahlen, die sich in der prinzipiellen Ähnlichkeit der Verarbeitungskette – Erfassen, Aufbereiten und Bereitstellen gemessener Eigenschaften – zeigen, müssen die Unterschiede herausgearbeitet und die Notwendigkeit eines neuen Ansatzes begründet werden. Im Folgenden wird deshalb erläutert, warum herkömmliche Monitoringsysteme zwar nicht zur Verwendung als Werkzeug für IT-Sicherheitskennzahlen geeignet sind, aber dennoch Synergien aus einer grundlegenden Assimilation der Systemarchitektur gewonnen werden können.

Betrachtet man SIEM-Systeme im vorliegenden Kontext als sicherheitsspezifische Monitoringsysteme, so benennt bereits Jaquith in [And07, S. 226] eine Reihe grundlegender Unterschiede stichpunktartig, die nachfolgend etwas näher erläutert werden:

- **Fokus auf Echtzeitauswertung**: Monitoringsysteme dienen der Erfassung und Darstellung des jeweils aktuellen Zustands der überwachten Ressourcen. Im Vordergrund steht die Frage, welche Systeme gerade jetzt z. B. überlastet oder nicht verfügbar sind; zeitnahe Reaktionen sind immer dann nötig, wenn Messwerte eine signifikante Verschlechterung des Betriebszustands andeuten.

  Demgegenüber werden in Sicherheitsberichten die Entwicklungen über längere Zeiträume – beispielsweise Wochen oder Monate – betrachtet, so dass neben dem gerade aktuellen Zustand auch Referenzzeitpunkte berücksichtigt werden. Die Zielsetzung ist nicht, unmittelbar mit Eingriffen auf technischer Ebene zu reagieren, sondern langfristig wirksame Verbesserungsmaßnahmen zu konzipieren.

- **Einzelmesswerte**: Monitoringsysteme stellen überwiegend die bei den Ressourcen gemessenen Werte – beispielsweise Lüfterdrehzahlen, Speicherbelegung und Auslastung – direkt dar. Aggregationen und Korrelationen werden primär für die Root-Cause-Analyse verwendet, d. h. um beispielsweise das Fehlen endgerätespezifischer Messwerte mit dem Ausfall einer zentralen Netzkomponente begründen zu können. Monitoringsysteme können somit als Werkzeuge für die Bereitstellung von Messdaten unter Berücksichtigung der Netztopologie betrachtet werden.

  Für Sicherheitsberichte müssen die Messwerte darüber hinaus miteinander in Zusammenhang gebracht werden; folglich stehen die abgeleiteten Kennzahlen und die Indikatoren gegenüber den rohen Messdaten im Vordergrund.

- **Technische Anomalieerkennung**: Durch Monitoringsysteme werden ausgewählte technische Eigenschaften der angeschlossenen Systeme überwacht; durch Visualisierung und Alarmierung wird auf Abweichungen vom Soll-Zustand aufmerksam gemacht. In der Praxis finden sich häufig Monitoringsysteme, die ausschließlich die technische Infrastruktur überwachen, so dass beispielsweise bei überwachten Servern weitere Systeme hinzugezogen werden müssen, um zu ermitteln, welche Dienste darauf betrieben werden.

  Neben diesen praktischen Unzulänglichkeiten wurden Monitoringsysteme jedoch im Allgemeinen generell nicht für die Abbildung von der Technik losgelöster Geschäftsprozesse konzipiert. Ein herkömmliches Monitoringsystem würde beispielsweise keine Auskunft

darüber geben können, wie viele und welche Mitarbeiter der Organisation im aktuellen Kalenderjahr bereits an einer IT-sicherheitstechnischen Unterweisung teilgenommen haben. Für den Umgang mit IT-Sicherheitskennzahlen müssen jedoch auch entsprechende Systeme und Datenbestände erschlossen werden, die nicht rein technischer Natur sind.

- **Ausrichtung auf das operative Management**: Administratoren, Operateure und Wartungspersonal stellen die primäre Anwendergruppe von Monitoringsystemen dar. Eine unmittelbare Nutzung beispielsweise durch Risikomanager, Finanzplaner und Entscheidungsträger wäre ungewöhnlich – auch die Bedienkonzepte orientieren sich meist an den Anforderungen von Systemadministratoren.

  Ursächlich hierfür sind neben der Verarbeitung reiner Basiskennzahlen die in Monitoringsystemen oft nur beschränkt ausgeprägten Berichtsmöglichkeiten. Als Zielgruppen können zwar häufig verschiedene Administratoren, die für unterschiedliche Systeme zuständig sind, differenziert werden, um ihnen jeweils nur Informationen über die für sie relevanten Ressourcen zukommen zu lassen. Es wird jedoch nicht zwischen verschiedenen Aufgaben bei der Auswertung der Berichte unterschieden, die z. B. eine zielgruppenspezifische Auswahl und Präsentation von Kennzahlen erforderlich machen.

Darüber hinaus beherrschen herkömmliche Monitoringsysteme offensichtlich zahlreiche der in Abschnitt 6.6 betrachteten Teilaufgaben des Management von IT-Sicherheitskennzahlen nicht oder nur unzureichend; hierzu gehören unter anderem:

- Das Verwalten von Hypothesen, Subhypothesen, Interpretationsregeln, etc. mit einer Unterstützung eines kontinuierlichen Verbesserungsprozesses, bei dem beispielsweise die Erforderlichkeit und Aussagekraft einzelner Kennzahlen regelmäßig geprüft werden.
- Die manuelle Erfassung von Kennzahlen, für die eine automatisierte Messung entweder technisch nicht möglich oder ökonomisch nicht sinnvoll ist.
- Die Orientierung an bzw. Integration von sicherheitsspezifischen KPIs und entsprechenden QoS-Parametern beispielsweise aus Service Level Agreements.
- Ausgabeschnittstellen, die über die im Monitoringsystem integrierten Visualisierungsmöglichkeiten und Alarmierungswege hinaus gehen, beispielsweise um Genehmigungs- und Bestätigungsabläufe für Sicherheitsberichte abbilden und eine Integration z. B. mit webbasierten Content-Management-Systemen erreichen zu können.
- Eine prozessuale Integration, beispielsweise in das Risikomanagement und die Investitionskostenrechnung, so dass die Nutzung des Werkzeugs ein nahtloser Bestandteil von Sicherheitsmanagement- und ITSM-Prozessen wird.

Die Abbildung dieser und weiterer Funktionalitäten auf das hier erarbeitete Werkzeug wird in Abschnitt 7.3.2 vertieft. Trotz der genannten Defizite und des bisherigen Mangels an dedizierten Werkzeugen zum Management von IT-Sicherheitskennzahlen stellen Monitoringsysteme bzw. die ihnen zugrunde liegenden Architekturen eine gute konzeptionelle Ausgangsbasis für die Entwicklung des hier erarbeiteten Werkzeugs dar. Im Folgenden werden deshalb stellvertretend für zahlreiche weitere wissenschaftliche Arbeiten in diesem Bereich drei signifikante Ansätze aufgegriffen, die das unten spezifizierte Architekturkonzept grundlegend beeinflusst haben:

- Panopticon [CRK+10] ist eine moderne, an der Universität Kapstadt konzipierte und implementierte Monitoringarchitektur. Sie betont die Skalierbarkeit sowohl bezüglich

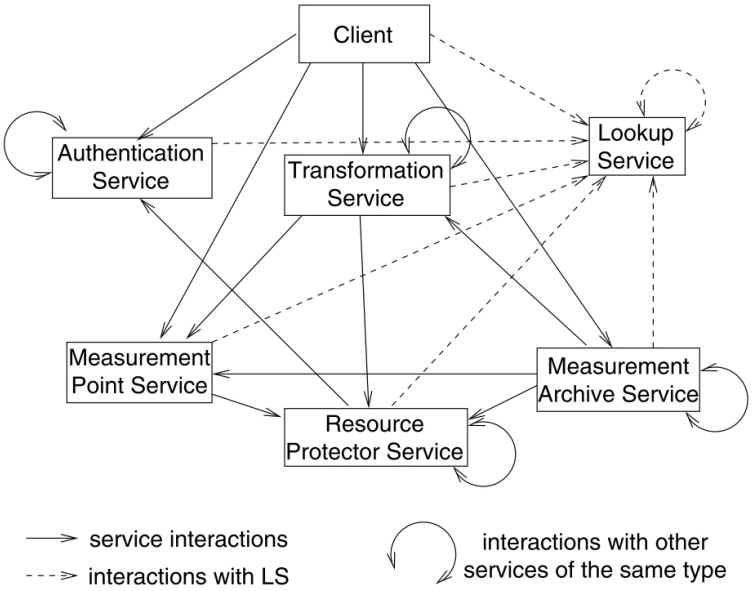


Abbildung 7.10.: Architektur des Netzmonitoringsystems PerfSONAR (Quelle: [HBB+05])

der angeschlossenen Datenquellen, d. h. der überwachten Systeme, als auch im Hinblick auf die in das Monitoringsystem integrierten Visualisierungsmöglichkeiten, die einen Gesamtüberblick über sehr viele überwachte Ressourcen ermöglichen. Der Ansatz realisiert die für heutige Monitoringsysteme übliche Dreiteilung der Architektur:

1. Datensammlungsebene: Die Komponenten der Datensammlungsebene bilden die Schnittstelle zu den überwachten Ressourcen und Systemen. Sie ermöglichen beispielsweise den Abruf aktueller Messwerte über Protokolle wie SNMP. Zur Sicherstellung der Skalierbarkeit und Effizienz des Monitoringsystems müssen Messfrequenzen festgelegt und ein möglichst hoher Parallelisierungsgrad erreicht werden.
2. Steuer- und Speicherebene: Die mittlere Schicht der Panopticon-Architektur übernimmt die Ansteuerung der Datensammlungsebene, beispielsweise indem Messvorgänge regelmäßig angestoßen werden, und die persistente Speicherung der Messergebnisse. Panopticon nutzt hierfür ein klassisches relationales Datenbankmanagementsystem; viele andere Implementierungen setzen auf für das Monitoring spezialisierte Speicherstrukturen wie die Round Robin Databases (RRD, [Oet09]), aus denen alte Einzelmesswerte zwar herausaltern, in denen aber ausgewählte aggregierte Informationen, z. B. Monatsmittel, beibehalten werden.
3. Visualisierungsebene: Die Visualisierungebene bildet die interaktive Schnittstelle zu den Benutzern. Sie stellt sowohl Übersichten als auch die Möglichkeit, einzelne Systeme und deren Messwerte im Detail zu betrachten, bereit.

Diese Einteilung fungiert als Ausgangsbasis für die in Abschnitt 7.3.2 vorgestellte Gesamtarchitektur des hier erarbeiteten Werkzeugs.

- PerfSONAR [HBB+05] ist eine im Rahmen des GN2-Projekts durch die europäischen nationalen Forschungsnetze in enger Zusammenarbeit mit dem US-amerikanischen In-

ternet2 entstandene, auf serviceorientierten Architekturen (SOA) basierende, multidomain-fähige Netzmonitoringarchitektur. Durch das Ziel eines organisations- und länderübergreifenden Einsatzes ist sie insbesondere auf den Umgang mit heterogenen Ressourcen in verschiedenen administrativen Zuständigkeitsbereichen ausgelegt. Ihre in Abbildung 7.10 dargestellte Architektur enthält insbesondere die folgenden, konzeptionell auch für diese Arbeit relevanten Komponenten:

  - Transformation Service: Der PerfSONAR-Datentransformationsdienst bietet neben der reinen Formatkonvertierung von Einzelmessungen auch Funktionen zur Aggregation, Korrelation und Filterung. Er stellt zudem die Ausgangsbasis für Alarmierungen dar, d. h. Messungen, die vorgegebene Schwellenwerte über- oder unterschreiten, können auch in Benachrichtigungen umgewandelt werden.

  - Authentication Service: Der Authentifizierungsdienst ist der zentrale Bestandteil des Benutzer- und Berechtigungsverwaltungskonzepts von PerfSONAR; er unterstützt ein Rollenmodell und basiert auf ausgewählten Abläufen des föderierten Identitätsmanagements (FIM).

  - Lookup Service: Der PerfSONAR-Lookup-Service fungiert als Registrierungsdienst, der eine dynamische Verwaltung von Informationen darüber ermöglicht, welche Messstationen (engl. *measurement points*) verfügbar sind und welche Messdaten diese liefern können.

  Auf die Ausprägung der entsprechenden Komponenten des erarbeiteten Werkzeugkonzepts und ihre technischen Schnittstellen zu den angeschlossenen Datenquellen wird vertiefend in Abschnitt 7.3.3 eingegangen.

- SMONA [DS05, DFS07, Sai07] ist eine von Sailer und Danciu entwickelte Monitoringarchitektur, die herkömmliche, systemnahe Messdaten auswertet und u. a. durch Aggregation und Komposition dieser Daten auch höherwertige, dienstorientierte Managementinformationen bereitstellt.

  Aggregationsvorschriften für Dienstinformationen werden dabei in SISL, einer in [Lan06a] formalisierten Sprache für Regelsätze, formuliert. Neben dem Konzept für die Verarbeitung somit angereicherter Monitoringinformationen (sog. *rich events*) unterstützt SMONA auch die zentral gesteuerte Konfiguration der Adapterkomponenten, von denen wie in Abbildung 7.11 dargestellt die plattformspezifischen Messwerte entgegengenommen werden.

  Die damit vergleichbaren, in dieser Arbeit konzipierten Steuermöglichkeiten werden in Abschnitt 7.3.4 in den Gesamtablauf der Nutzung des erarbeiteten Werkzeugs eingebettet.

Zahlreiche weitere Systemeigenschaften von Monitoringsystemen – beispielsweise die zeitgesteuerte Durchführung von Messungen und die Protokollierung des Verlaufs sowie entsprechende Fehlerbehandlungsmaßnahmen – gehören zum Standardrepertoire aktueller Ansätze und werden im Rahmen des hier erarbeiteten Architekturkonzepts aufgegriffen, ohne sie jeweils einzelnen verwandten Arbeiten zuzuordnen.

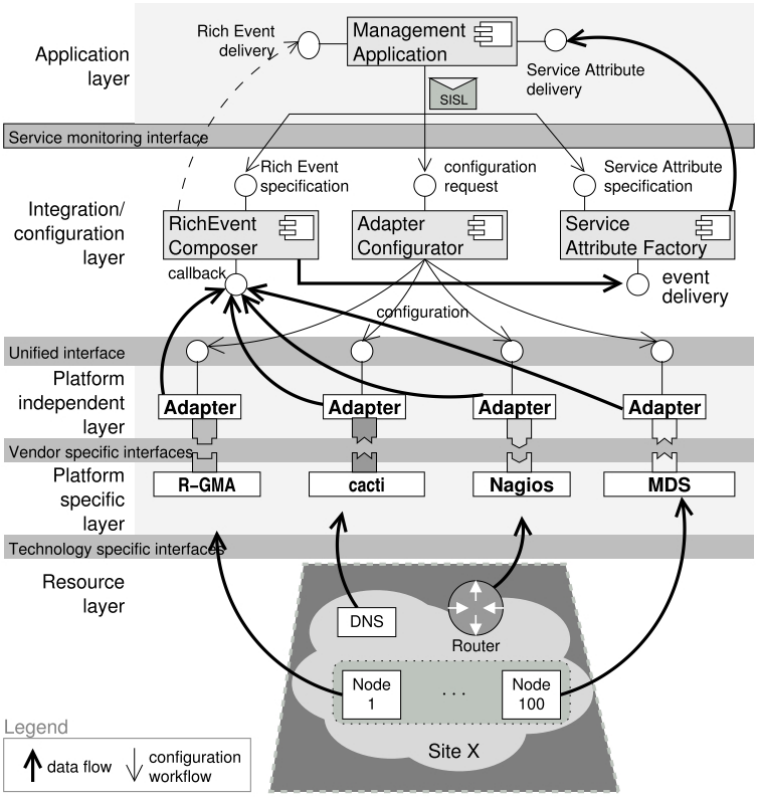


Abbildung 7.11.: Überblick über die Monitoringarchitektur SMONA (Quelle: [DFS07])

7.3.2. Anforderungen an das Werkzeug und resultierende Gesamtarchitektur

In Abschnitt 6.6 wurden die Abläufe bei der Erfassung, Aufbereitung und Präsentation von IT-Sicherheitskennzahlen bereits aus einer prozessorientierten Perspektive beschrieben; neben den Anforderungen an die Eigenschaften einzelner Kennzahlen wurden auch ein Informationsmodell für ihre Verwaltung spezifiziert, ihre Zusammenstellung zu Sicherheitsberichten konzipiert und ihre Auswertung im Rahmen der Investitionskostenrechnung exemplifiziert. Dabei wurde allerdings nicht auf die gezielte Unterstützung aller dieser Abläufe durch ein entsprechendes Werkzeug eingegangen. Aus den konzipierten Vorgehensweisen lassen sich jedoch die folgenden technischen Anforderungen an die Funktionalität des zu erarbeitenden Werkzeugs ableiten, durch die die konkrete Ausprägung der unten spezifizierten Architektur motiviert wird:

- Die Basiszielsetzungen für das Werkzeug sind das Festhalten, Beurteilen, Propagieren und Bereitstellen IT-sicherheitsrelevanter Informationen. Entsprechende Daten müssen folglich akquiriert, aufbereitet, gespeichert bzw. archiviert, visualisiert, propagiert und über technische Schnittstellen abrufbar gemacht werden.
- Verschiedene Datenquellen wie Security-Frameworks, technische Systeme und Assets, Managementsysteme und -werkzeuge müssen ebenso wie eine manuelle Datenerfassung integriert werden. Durch die Heterogenität der Datenquellen muss zwingend mit unter-

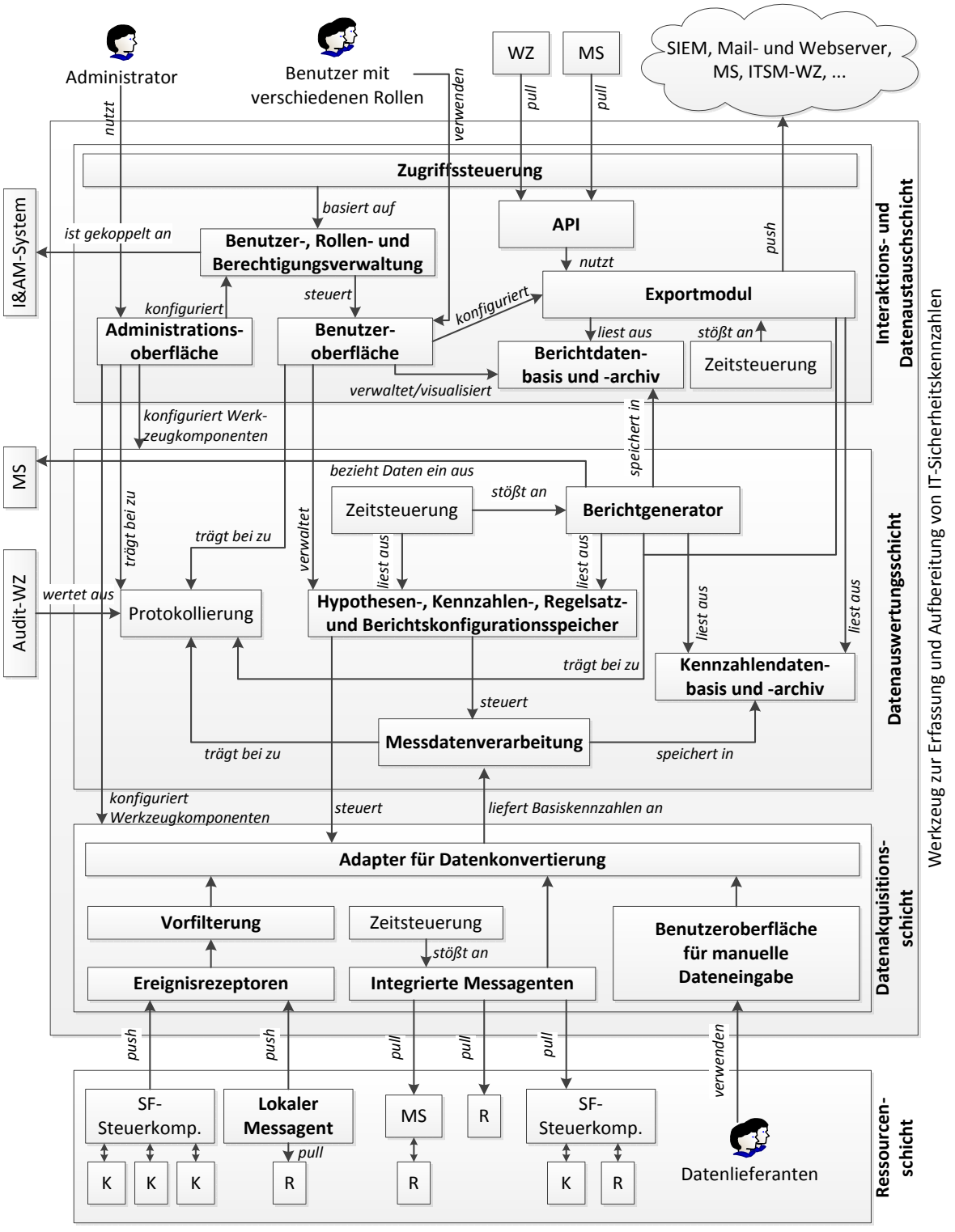
schiedlichen Datenformaten umgegangen werden können.

- Diejenigen Komponenten des Werkzeugs, die Schnittstellen zu den Datenquellen und anderen anzuschließenden Systemen bilden, müssen neben Konfigurationsmöglichkeiten zur Anpassung an Spezifika des Einsatzszenarios auch möglichst einfach in die vorhandene Infrastruktur zu integrieren sein; beispielsweise sollte vermieden werden, zur Erfassung von Messwerten in jedem Fall zusätzliche komplexe Software auf den zu überwachenden Systemen installieren zu müssen.
- Die Aufbereitung und Auswertung der Messdaten muss ein hypothesengetriebenes Vorgehen unterstützen. Das Werkzeug muss somit die Verwaltung von Hypothesen, Subhypothesen und den entsprechenden Interpretationsregeln ebenso verwalten können wie die Kompositionsregeln für abgeleitete Sicherheitskennzahlen, Indikatoren und KPIs. Insofern muss das Werkzeug eine mit Entwicklungsumgebungen vergleichbare Benutzeroberfläche bieten, mit deren Hilfe eine Verwaltung von Kennzahlen über ihren gesamten Lebenszyklus möglich ist (vgl. hierzu [And07, S. 227]).
- Neben den Messdaten und Kennzahlen muss das Werkzeug eine Reihe weiterer Informationen verwalten können, z. B. die relevanten Benutzer, Zielgruppen und Adressaten von Sicherheitsberichten, ihre jeweiligen Rollen und Zugriffsberechtigungen sowie Zeitpläne für die automatisierte Durchführung von Messungen und die Erstellung von Berichten. Darüber hinaus müssen externe Informationsquellen, die z. B. Schwellenwerte für in SLAs definierte QoS-Parameter mit IT-Sicherheitsbezug bereitstellen, angebunden werden können.
- Die Arbeitsabläufe bei der Auswertung von Sicherheitsberichten – von der Bereitstellung bzw. Auslieferung bis hin zum kontinuierlichen Verbesserungsprozess – müssen vom Werkzeug unterstützt werden. Dabei müssen manuelle Eingriffe möglich bleiben, um z. B. automatisch generierte Sicherheitsberichte manuell annotieren zu können, um u. a. auf identifizierte Besonderheiten explizit hinzuweisen, beispielsweise wenn erkennbare Bezüge zu nicht automatisch ausgewerteten Veränderungen in den Geschäftsprozessen existieren (vgl. auch hierzu [And07, S. 227]).

Abbildung 7.12 zeigt die Architektur des hier erarbeiteten Werkzeugs zur Erfassung und Aufbereitung von IT-Sicherheitskennzahlen im Gesamtüberblick. Sie folgt der klassischen Dreiteilung in eine **Datenakquisitionsschicht**, in deren Kontext auch die externen Datenquellen zu betrachten sind, eine **Datenauswertungsschicht**, die den wesentlichen Teil der Automatisierung der Vorgänge übernimmt, und eine **Interaktions- und Datenaustauschschicht**, die sowohl den Bedarf an manueller Analyse der Kennzahlen als auch deren Übernahme in weitere Systeme abdeckt. Im Folgenden werden die einzelnen Komponenten des Werkzeugs mit ihren jeweiligen Aufgaben und Schnittstellen näher beschrieben; auf die Abbildung und die Verarbeitung einzelner Messwerte bezogen wird dabei von unten nach oben vorgegangen.

Die **Datenakquisitionsschicht** dient der Erfassung von Basiskennzahlen. Sie unterscheidet zwischen Messdaten, die von den überwachten Systemen per Push-Kommunikation geliefert werden, von den Datenquellen abzurufenden Messwerten und manuell eingegebenen Kennzahlen. Hierzu kommen folgende Komponenten zum Einsatz:

- Für die Entgegennahme der von den Ressourcen emittierten Messdaten werden *Ereignisrezeptoren* bereitgestellt. Dabei handelt es sich um Kommunikationsendpunkte, die



Legende:
K = Frameworkkomponente, R = Ressource bzw. Asset,
WZ = externes Managementwerkzeug, MS = externes Managementsystem

Abbildung 7.12.: Architektur des konzipierten Managementwerkzeugs für IT-Sicherheitskennzahlen

das von der jeweiligen Ressource genutzte Übertragungsprotokoll unterstützen – beispielsweise durch die Annahme von SNMP-Traps oder den Betrieb eines Web Services.

Als Datenquellen, die eine push-basierte Messwertlieferung unterstützen, kommen beispielsweise die Steuerkomponenten von Security-Frameworks in Frage, die über ähnliche Mechanismen auch an Managementplattformen angebunden werden können (vgl. Abschnitt 6.4.3). Diese haben insbesondere die Eigenschaft, Messdaten aller Frameworkkomponenten aggregieren und kollektiv ausliefern zu können, so dass die Situation berücksichtigt werden muss, dass ein Messagent verschiedenste Messdaten liefern kann. Neben solchen Systemen, die bereits nativ den push-basierten Export von Messdaten unterstützen, sind auch Ressourcen zu betrachten, auf denen ein *lokaler Messagent* nachgerüstet werden muss. Dieser liest die Messwerte pull-basiert aus der betrachteten Ressource aus und übermittelt sie im Push-Verfahren an seinen Ereignisrezeptor. Lokale Messagenten sind überall dort erforderlich, wo ein Auslesen der Messwerte vom hier erarbeiteten Werkzeug aus nicht möglich ist, beispielsweise weil die Ressource keine direkt über das Netz erreichbaren Messpunkte aufweist; damit verbundene Implikationen werden in Abschnitt 7.3.3 näher betrachtet.

- Die von den Ereignisrezeptoren empfangenen Messdaten werden einer *Vorfilterung* unterzogen. Diese dient im Wesentlichen dazu, die Anzahl der in der weiteren Verarbeitungskette aufzubereitenden Messwerte zu beschränken und Überlastsituationen zu vermeiden: Im Unterschied zu Monitoringsystemen benötigt das Werkzeug für IT-Sicherheitskennzahlen relativ selten aktuelle Messwerte – je nach Spezifikation der Kennzahlen reicht ggf. sogar eine Messung pro Berichtszeitraum aus. Kommen seitens der Datenquelle jedoch dieselben push-basierten Meldemechanismen zum Einsatz, die auch zum Anschluss an Monitoringsysteme und Managementplattformen genutzt werden, und liegen somit ggf. mehrere Messungen pro Minute vor, so kann ein großer Teil der gemeldeten Messwerte ohne negative Konsequenzen für die Sicherheitsberichte verworfen werden. Die Filterkomponente hat somit die Aufgabe, die Anzahl der von Messagenten und anderen Datenquellen gelieferten Messwerte geeignet einzuschränken.
- Für den in der Praxis überwiegenden Fall, dass Messwerte von externen Datenquellen im Pull-Verfahren abgerufen werden müssen, kommen ins Werkzeug *integrierte Messagenten* zum Einsatz. Sie nehmen über Managementprotokolle wie SNMP oder in der Rolle eines Web-Service-Clients über das Netz Kontakt mit den Ressourcen auf und rufen dabei die relevanten Messwerte ab. Über dieses Verfahren kann direkt auf einzelne Ressourcen, auf Messwertaggregatoren bzw. Primi inter pares wie Frameworksteuerkomponenten oder weitere Managementsysteme bzw. externe Werkzeuge zugegriffen werden.

  Die Durchführung pull-basierter Messungen wird von einer *Zeitsteuerung* angestoßen, die im Allgemeinen eine periodische Wiederholung in Abhängigkeit von der für jede Basiskennzahl zu definierenden Messfrequenz vorsieht. Auf Aspekte wie die Fehlerbehandlung und den Umgang mit Ausfällen des Werkzeugs selbst wird in Abschnitt 7.3.3 eingegangen.
- Als dritter Datenimportkanal wird eine *Benutzeroberfläche für manuelle Dateneingaben* bereitgestellt. Sie wird von einer als Datenlieferanten bezeichneten Personengruppe verwendet. Die rechtzeitige und zuverlässige Datenlieferung über diese Schnittstelle muss über zusätzliche Maßnahmen, beispielsweise Erinnerungen per E-Mail oder die Inte-

gration in Workflowmanagementwerkzeuge, sichergestellt werden, die hier nicht näher betrachtet werden.

- Eine Reihe von *Adaptern für die Datenkonvertierung* bildet das Bindeglied zwischen der Messwerterfassung und der Verarbeitung der so ermittelten Basiskennzahlen. Die Adapter haben primär die Aufgabe, ressourcen- bzw. plattformspezifische Messdaten in plattformunabhängige Messwerte zu überführen, die anschließend einheitlich in der Datenauswertungsschicht verarbeitet werden können. Neben einer reinen Formatkonvertierung kann dabei auch eine Ergänzung der Daten erforderlich werden, beispielsweise falls die Messagenten nur Zahlen liefern, deren implizit bekannte Maßeinheiten hinzugefügt werden müssen.

Nach der Datenkonvertierung werden die Basiskennzahlen an die **Datenauswertungsschicht** übergeben:

- Die mit dem Vorliegen eines aktuellen Messwerts angestoßene Verarbeitungskette wird in einer Komponente zur *Messdatenverarbeitung* implementiert. Die Verarbeitung umfasst dabei mindestens eine Plausibilitätsprüfung, durch die offensichtliche Fehler bei der Erfassung des Messwerts identifiziert werden können (vgl. Abschnitt 6.6.3), beispielsweise indem der Messwert mit dem pro Basiskennzahl erfassten Bereich gültiger Werte verglichen wird, und die Speicherung der Basiskennzahl in der *Kennzahlendatenbasis*.

  Die Verfügbarkeit einer aktualisierten Basiskennzahl führt kaskadierend auch dazu, dass alle abgeleiteten Kennzahlen, die von ihr Gebrauch machen, neu berechnet und ebenfalls wiederum gespeichert werden können. Die unmittelbare Neuberechnung abgeleiteter Kennzahlen vermeidet einerseits temporäre Inkonsistenzen im gesamten Kennzahlenbestand, die die Benutzer des Werkzeugs irritieren könnten. Andererseits vervielfacht sich der Berechnungsaufwand, wenn Basiskennzahlen sehr häufig erfasst und zu einer größeren Anzahl abgeleiteter Kennzahlen verarbeitet werden müssen; im letzteren Fall ist alternativ eine regelmäßige Aktualisierung der abgeleiteten Kennzahlen, die zeitgesteuert angestoßen wird, in Erwägung zu ziehen.

- Die Kennzahlendatenbasis hält die jeweils aktuellen Werte der gemessenen bzw. deduzierten Kennzahlen vor; ein geeignetes Schema für relationale Datenbankmanagementsysteme kann beispielsweise aus Abbildung 6.38 auf Seite 442 abgeleitet werden. Beim Eintreffen neuer sind die alten Messwerte nicht primitiv zu überschreiben, sondern im Sinne eines *Kennzahlenarchivs* geeignet aufzubewahren. Die Mindestaufbewahrungsdauer hängt dabei maßgeblich von dem für die jeweilige Kennzahl definierten Vergleichszeitraum (siehe gleichnamiges Attribut im Informationsmodell) und eventuell gegebenen Compliance-Randbedingungen ab. Bei einer längeren Speicherdauer ist der kontinuierlich wachsende Speicherbedarf zu berücksichtigen; gegebenenfalls ist eine Priorisierung vorzunehmen, so dass beispielsweise ausgewählte abgeleitete Kennzahlen länger vorgehalten werden als Basiskennzahlen, die nicht als Indikatoren fungieren. Die Archivierung von Basiskennzahlen kann sich jedoch auch positiv auf die nachträgliche Definition neuer abgeleiteter Kennzahlen auswirken, da eine unmittelbare retrospektive Auswertung möglich ist, wenn alle für die Ableitung benötigten Eingabekennzahlen bereits vorliegen.

- Die Verarbeitung der Messdaten wird ebenso wie die nachfolgend beschriebene Erzeugung von Sicherheitsberichten maßgeblich von einer zentralen *Konfigurationsdatenbasis* gesteuert, in der alle Hypothesen, Subhypothesen, Interpretationsregeln, Kennzahlen,

Indikatoren, KPIs, Kompositionsregelsätze und Berichtsspezifikationen gespeichert werden. Die dafür benötigten Datenstrukturen wurden im Rahmen der in den Abschnitten 6.6.3 und 6.6.4 vorgestellten Informationsmodelle spezifiziert. Aus ihnen gehen insbesondere die Abhängigkeiten zwischen Basiskennzahlen und abgeleiteten Kennzahlen, Instruktionen für die Visualisierung bei interaktiver Nutzung und im Rahmen von Sicherheitsberichten sowie die den jeweiligen Zielgruppen mitzuliefernden Interpretationsregeln und Entscheidungshilfen hervor.

- Der *Berichtsgenerator* wertet die in der zentralen Konfigurationskomponente hinterlegten Spezifikationen für zu erstellende Sicherheitsberichte aus und erzeugt diese auf Basis der in der Kennzahlendatenbasis und im Archiv verfügbaren Kennzahlen. Er erzeugt somit eine Zusammenstellung ausgewählter Kennzahlen, die den zum Zeitpunkt der Berichterstellung aktuellen Stand reflektieren. Die Berichte werden zunächst in einem internen Datenformat in der *Berichtsdatenbasis* gespeichert, die der Datenaustauschschicht zugeordnet ist; ihr Schema ergibt sich aus dem in Abschnitt 6.6.4 vorgestellten Informationsmodell.

  Die Erzeugung von Berichten wird wiederum von einer *Zeitsteuerung* angestoßen, die sich hierfür an der Berichtsfrequenz (siehe gleichnamiges Attribut im Informationsmodell) orientiert. Da die Sicherheitsberichte eine Top-down-Sicht auf die bislang bottom-up verarbeiteten Kennzahlen darstellen, spielt die Fehlerbehandlung bezüglich Konsistenz und Aktualität eine zentrale Rolle: Zum einen dürfen für Sicherheitsberichte nur Kennzahlen verwendet werden, die auch verfügbar sind; dies muss von der *Benutzeroberfläche* bei der Konfiguration von Kennzahlen und Berichten sichergestellt werden. Zum anderen muss berücksichtigt werden, dass z. B. aufgrund von Störungen bei der Erfassung von Messdaten lediglich veraltete Informationen vorliegen; hierauf muss z. B. durch entsprechende Protokolleinträge und Annotationen der entsprechenden Abschnitte des Sicherheitsberichts hingewiesen werden.

  Der Berichtsgenerator kann eigene Schnittstellen zu externen Managementsystemen und -werkzeugen enthalten, über die dynamisch für Berichtsinhalte relevante Daten eingebunden werden können, die weder aus der meist statischen Berichtsspezifikation noch aus der Kennzahlendatenbasis hervorgehen, so dass beispielsweise aktuelle IT-sicherheitsspezifische SLA-Parameter aus einem Service-Level-Management-ITSM-Werkzeug importiert werden können.

- Schließlich ist eine Komponente zur *Protokollierung* der Datenauswertungsschicht zugeordnet, obwohl auch die Komponenten der beiden anderen Schichten von ihr Gebrauch machen können. Sie hält den Verlauf der automatisierten Abläufe und der interaktiven Nutzung des Werkzeugs fest und dient damit einerseits der Analyse von Fehlersituationen und fungiert andererseits als Schnittstelle zu externen Auditierungswerkzeugen, die beispielsweise das korrekte Zustandekommen der vorgelegten Sicherheitsberichte prüfen sollen.

Die **Interaktions- und Datenaustauschschicht** umfasst alle Komponenten und Schnittstellen zur Bereitstellung und Weitergabe der aufbereiteten IT-Sicherheitskennzahlen und Berichte:

- Jegliche Formen der Werkzeugnutzung und der Datenauswertung unterliegen zunächst einer *Zugriffssteuerung*. Diese stellt bei jedem Zugriffsversuch über die graphischen

Oberflächen und bei jeder Nutzung der ebenfalls unten beschriebenen Programmierschnittstellen sicher, dass nur solche Daten ausgelesen und nur solche Aktionen durchgeführt werden können, für die der jeweilige Benutzer bzw. das entsprechende externe System autorisiert ist.

Die Zugriffssteuerung fungiert somit als Policy Enforcement Point (PEP) auf Basis einer *Benutzer-, Rollen- und Berechtigungsverwaltung*, die das RBAC-Konzept umsetzt: Die Nutzung der in Abschnitt 7.3.4 näher beschriebenen Funktionalitäten ist an das Innehaben einer entsprechenden Berechtigung gebunden. Sowohl Mengen solcher Berechtigungen als auch Gruppen von Benutzern werden Rollen zugewiesen. Über die Rollen kann somit beispielsweise differenziert werden, wer einzelne Kennzahlen anlegen und pflegen soll, die Inhalte von Sicherheitsberichten festlegen kann oder einen Sicherheitsbericht vor seiner Veröffentlichung genehmigen muss.

Teile dieser Sicherheitsfunktionalität – beispielsweise die Authentifizierung und die Zuordnung von Benutzern zu Rollen – können optional durch die Anbindung an ein zentrales Identity & Access-Managementsystem delegiert werden, wodurch der werkzeugspezifische Administrationsaufwand reduziert werden kann.

- Für die Werkzeugsystemverwalter steht eine dedizierte *Administrationsoberfläche* zur Verfügung. Sie erlaubt komplementär zur Oberfläche für reguläre Nutzer die Durchführung tiefer eingreifender Modifikationen. Hierzu gehören insbesondere die Konfiguration der Komponenten in den beiden anderen Schichten, beispielsweise das Hinzufügen und Entfernen von Messagenten und die Anpassung der Benutzeroberflächen für manuelle Dateneingaben, die Konfiguration von Rollen und Berechtigungen sowie die Auswertung der Werkzeugprotokolle zur Analyse und Beseitigung aufgetretener Fehler.
- Die Werkzeuganwender nutzen die *Benutzeroberfläche* für alle in Abschnitt 7.3.4 erläuterten Aufgaben, zu denen je nach Rolle des Benutzers beispielsweise die Kenntnisnahme von Sicherheitsberichten, das Zusammenstellen neuer Berichte oder das Konzipieren und Implementieren neuer Hypothesen und Indikatoren gehören. Über die Protokollierung von Arbeitsschritten, zu denen der Benutzer explizit aufgefordert wird – beispielsweise die Bestätigung des Erhalts eines Sicherheitsberichts – können Compliance-Anforderungen in Bezug auf die Nichtabstreitbarkeit erfüllt werden.
- Ein *Exportmodul* dient zunächst der Aufbereitung der vom Berichtgenerator erstellten Sicherheitsberichte durch Konvertierung des intern verwendeten Formats in ein zielgruppen- bzw. zielsystemspezifisches Datenformat. Dabei kann es sich sowohl um visuell lesbare (engl. *human readable*) Dokumentenformate wie PDF oder HTML als auch um maschineninterpretierbare Datensätze, z. B. in Form von CSV- oder XML-Dateien, handeln.

  Für den Fall, dass das Exportmodul über die *Zeitsteuerung* oder von einem Anwender über die Benutzeroberfläche angestoßen wurde, gibt es den aufbereiteten Sicherheitsbericht mittels Push-Kommunikation an ein externes System weiter; diese Weiterverarbeitungsmöglichkeiten sind szenarienspezifisch zu konfigurieren und umfassen beispielsweise den Versand per E-Mail, das Hinterlegen auf einem Webserver oder einem Fileserver, den Import in ein SIEM-System und die weitere Bearbeitung z. B. durch ein Dokumentenmanagementsystem, andere Managementsysteme oder ITSM-spezifische Werkzeuge.

  Alternativ dazu kann der Datenbestand von externen Systemen und Werkzeugen auch

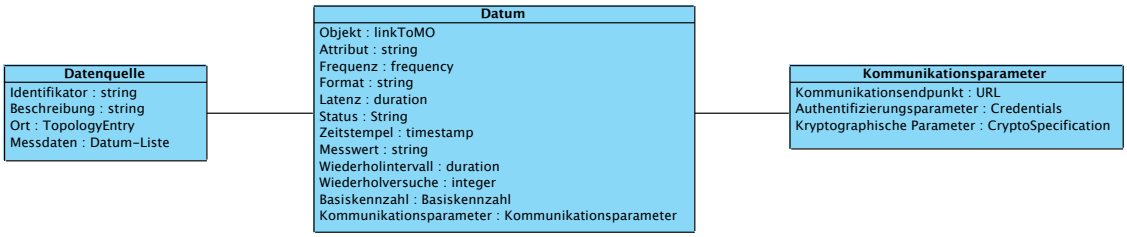


Abbildung 7.13.: Informationsmodell für die Verwaltung angeschlossener Datenquellen

über ein *API* abgerufen werden. Auch diese Schnittstelle nutzt die Konvertierungsfunktionalität des Exportmoduls, ermöglicht über den push-basierten Export jedoch zusätzlich das Auslesen von Kennzahlendatenbasis und -archiv im Rahmen der jeweiligen Berechtigungen. Das API erschließt damit die unten skizzierten Anwendungsfälle, in denen auch weitere Managementsysteme auf die Messdaten bzw. Kennzahlen zugreifen sollen.

- Analog zur Kennzahlendatenbasis wird auch die Berichtsdatenbasis von einem Archiv ergänzt, in dem die Sicherheitsberichte zu Referenzzwecken aufbewahrt werden können. In Abhängigkeit von der Anzahl der Sicherheitsberichte und ihrer Erstellungshäufigkeit ist auch hierfür eine Strategie festzulegen, welche archivierten Berichte – falls überhaupt – wann gelöscht werden sollen.

In den folgenden beiden Abschnitten werden die Schnittstellen zu den Datenquellen und die prozessorientierten Interaktionsmöglichkeiten mit dem Werkzeug näher betrachtet.

7.3.3. Schnittstellen zu Security-Frameworks, Assets und Managementsystemen

Das Be- oder Widerlegen von Hypothesen und damit die Aussagekraft und Qualität der mit dem Werkzeug erstellten Sicherheitsberichte stehen und fallen mit der zuverlässigen Verfügbarkeit der Messdaten, die in Basiskennzahlen münden. Aus diesem Grund werden im Folgenden ausgewählte Aspekte der technischen Schnittstellen zu den Datenquellen näher beleuchtet.

Für die automatisierte Erfassung von Messdaten sieht das oben vorgestellte Architekturkonzept Ereignisrezeptoren mit Filtern sowie Messagenten vor. Ähnlich zur Verwaltung von IDS-Sensoren in Abschnitt 7.2.4 muss das hier konzipierte Werkzeug folglich seine Datenquellen und Erfassungsschnittstellen verwalten; in Abhängigkeit von der Komplexität des Szenarios und der angestrebten Berichtsinhalte werden Dutzende oder Hunderte von Indikatoren und eine dazu im Allgemeinen proportionale Anzahl an Basiskennzahlen benötigt. Für das Management der Datenquellen wurde das in Abbildung 7.13 dargestellte Informationsmodell konzipiert. Jeder Datenquelle werden folgende Attribute zugeordnet:

- Ein *Identifikator* dient der eindeutigen technischen Benennung der Datenquelle.
- Eine in natürlicher Sprache verfasste *Beschreibung* charakterisiert die Datenquelle und erleichtert damit die manuelle Implementierung einer Abbildung von Hypothesen auf die benötigten Messdaten.

- Im Attribut *Ort* wird die Betriebsstätte der Datenquelle angegeben, aus der insbesondere hervorgeht, ob es sich um einen integrierten Messagenten oder ein entferntes System handelt.
- Eine Liste der von der Datenquelle lieferbaren *Messdaten* unterstützt die bereits skizzierte Situation, dass angeschlossene Datenquellen Messwerte mehrerer Komponenten aggregieren und kollektiv ausliefern können.

Abgeleitet vom Informationsmodell für Sicherheitskennzahlen und um für den Erfassungsvorgang notwendige Kommunikationsinformationen ergänzt werden für jedes von der Datenquelle unterstützte *Datum* die folgenden Attribute festgehalten:

- Das gemessene *Objekt* und dessen *Attribut* werden spezifiziert. Diese Angaben dienen beispielsweise auch bei Audits und Reviews der Werkzeugkonfiguration der Prüfung, ob die zur Beschreibung passenden Messdaten akquiriert werden.
- Die *Frequenz* gibt an, wie häufig das Datum erfasst werden soll. Bei pull-basierter Datenakquisition deckt sich diese Frequenz mit derjenigen der zugeordneten Basiskennzahl. Bei von Ereignisrezeptoren empfangenen Messdaten kann auf Grundlage dieser Angabe die Vorfilterung konfiguriert werden.
- Das *Format* beschreibt die grundlegenden Interpretationsregeln für die Messwerte; auf dieser Basis kann beispielsweise ein geeigneter Ereignisrezeptor ausgewählt werden.
- Aus der *Latenz* wird das Alter des Messwerts beim Eintreffen im Werkzeug abgeleitet; es dient der Korrektur der Zeitstempel von Messungen, falls diese dem Datum nicht explizit beigefügt sind. Während technisch durch den Messvorgang und die netzbasierte Datenübertragung resultierende Latenzen im Kontext von IT-Sicherheitskennzahlen häufig vernachlässigt werden können, ist die Berücksichtigung von Verzögerungen oftmals dann sinnvoll, wenn beispielsweise Managementsysteme oder Sicherheitsberichte von Zulieferern als Datenquellen eingebunden werden, die keine Echtzeit-Sicht auf die Messwerte ermöglichen.
- Der *Status* gibt Aufschluss darüber, ob der letzte Versuch zur Akquisition des Datums erfolgreich war oder ob ein Fehler aufgetreten ist. Über einen *Zeitstempel* wird der Zeitpunkt der letzten erfolgreichen Messdatenerfassung festgehalten. Der *Messwert* puffert den zu diesem Zeitpunkt erfassten Wert.
- Zur Fehlerbehandlung werden ein *Wiederholintervall* und eine Maximalanzahl an *Wiederholversuchen* festgelegt. So kann beispielsweise für Messdaten, die nur einmal pro Monat erfasst werden sollen, vorgegeben werden, dass zehn Versuche im Abstand von jeweils einer Stunde unternommen werden sollen, wenn die Datenakquisition zum ursprünglich geplanten Zeitpunkt fehlgeschlagen ist.
- Über das Attribut *Basiskennzahl* wird eine Verknüpfung des Datums mit der Spezifikation seiner Basiskennzahl hergestellt; sie regelt beispielsweise das Vorgehen bei der Plausibilitätsprüfung im Rahmen der Messdatenverarbeitung.
- Die *Kommunikationsparameter* definieren schließlich die technische Schnittstelle zum Messen des angegebenen Attributs des entsprechenden Objekts. In Form eines URLs wird der entsprechende *Kommunikationsendpunkt*, aus dem auch das zu verwendende Protokoll hervorgeht, angegeben. Neben Managementprotokollen wie SNMP und HTTPS-basierter Web-Service-Kommunikation können beispielsweise auch Dateien

oder auszuführende Skripte, deren Ausgabe zu verwenden ist, angegeben werden. *Authentifizierungsparameter* stellen die Authentizität des Messwerts sicher, beispielsweise indem ein gemeinsames Passwort (engl. *shared secret*) oder Zertifikate zum Einsatz kommen. *Kryptographische Parameter* regeln optional weitere Einstellungen wie die Verschlüsselung des Messwerts, durch die Manipulationen verhindert werden können.

Die so beschriebenen Schnittstellen ermöglichen eine nahtlose Integration der Steuerkomponenten von Security-Frameworks, wie sie bereits in Abschnitt 6.4.3 für die Anbindung an Managementplattformen beschrieben wurde. Alternativ dazu können die Komponenten von Security-Frameworks ebenso wie andere Ressourcen direkt an das Werkzeug angebunden werden, wodurch jedoch ein entsprechend redundanter Konfigurationsaufwand notwendig werden würde.

Die Installation lokaler Messagenten auf oder in netztopologischer Nähe zu den Datenquellen kann wie bereits skizziert erforderlich werden, wenn keine push-basierte Messdatenübertragung möglich ist und auch ein pull-basiertes Abrufen der Messdaten nicht gewünscht oder unterstützt wird. Ein typisches Beispiel sind Personalverwaltungssysteme, die als Datenquelle z. B. für die Anzahl sicherheitsgeschulter Mitarbeiter dienen und häufig abgeschottet betrieben werden, so dass kein Zugriff über das Netz von außen möglich ist. Dabei muss jedoch beachtet werden, dass der Betrieb lokaler Messagenten mit zusätzlichem Aufwand verbunden ist und in der Praxis häufig auf Akzeptanzschwierigkeiten sowohl bei den Systemverantwortlichen als auch bei den für den Messagenten zuständigen Administratoren stößt. Als pragmatisches Vorgehen ist in solchen Fällen die manuelle Datenerfassung in Erwägung zu ziehen, die trotz des regelmäßig anfallenden Aufwands mittelfristig nicht notwendigerweise eine unökonomische Lösung darstellt.

Gegenüber der Anbindung automatisierter Datenakquisitionsmechanismen gestaltet sich die Konfiguration der Benutzeroberfläche für manuelle Dateneingaben einfacher; der Werkzeugadministrator muss im Wesentlichen Datenfelder vorgeben, die von den Datenlieferanten auszufüllen sind. Die manuelle Dateneingabe bietet zudem die Möglichkeit, Plausibilitätsprüfungen vorzuziehen und den Benutzer sofort auf vermutete Fehleingaben hinzuweisen. Bei umfangreichen Eingabemasken kann es in Abhängigkeit von den zu erfassenden Angaben sinnvoll sein, die Werte der letzten Eintragung als Vorgabe zu übernehmen oder als Anhaltspunkt anzuzeigen.

Die Erfassung eines Datums kann optional protokolliert werden; hierzu sind beispielsweise der Zeitstempel, der Identifikator, der Messwert und ggf. der Fehlerstatus des Vorgangs festzuhalten.

7.3.4. Integration des Werkzeugs in Managementprozesse

Das konzipierte Werkzeug unterstützt das organisationsweite Berichtswesen zur IT-Sicherheit durchgängig über den gesamten Lebenszyklus der sicherheitsspezifischen Kennzahlen. Neben der oben diskutierten Erfassung der Messdaten sind in diesem Kontext auch die Schnittstellen zu den verschiedenen Benutzergruppen und anderen Managementsystemen, die aufbereitete Sicherheitskennzahlen und -berichte verarbeiten, vertiefend zu betrachten.

Eine zentrale Rolle kommt dabei der Benutzeroberfläche zu, deren Funktionen drei aufeinander aufbauenden Kategorien zugeordnet werden können:

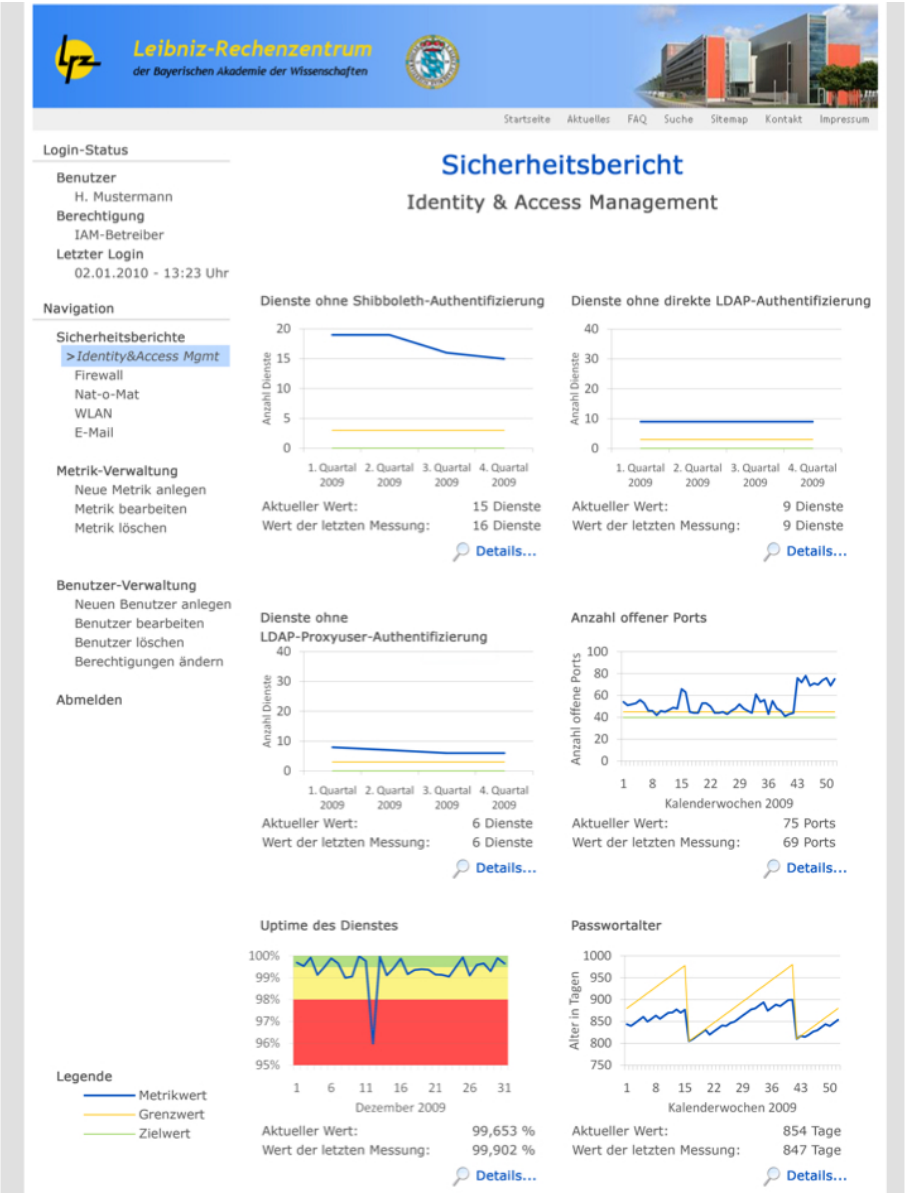


Abbildung 7.14.: Beispiel für die Visualisierung eines Sicherheitsberichts (Quelle: [Hub10])

1. **Lifecycle-Management für IT-Sicherheitskennzahlen**: Die grundlegenden Funktionen für das Verwalten der Kennzahlen bestehen im Anlegen neuer und Modifizieren bestehender Hypothesen, Subhypothesen, Basiskennzahlen, abgeleiteter Kennzahlen und Interpretationsregeln. Kennzahlen können als Indikatoren bzw. KPIs ausgezeichnet und mit SLAs bzw. anderen externen Dokumenten, z. B. Policies, verknüpft werden. Eine bis auf die Behandlung von Fehlersituationen vollständige Automatisierung wird durch die Hinterlegung von Berechnungsvorschriften für abgeleitete Kennzahlen erreicht. Darüber hinaus werden auf Basis der Benutzer- und Rollenverwaltung Zuständigkeiten erfasst, so dass regelmäßige Überprüfungen der konfigurierten Kennzahlen angestoßen

werden können, durch die eine kontinuierliche Verbesserung und die Außerbetriebnahme alter, nicht mehr benötigter Kennzahlen erwirkt werden kann.

2. **Erstellen von Sicherheitsberichten**: Das Werkzeug unterstützt die Erstellung aller für eine Organisation relevanten kennzahlbasierten IT-Sicherheitsberichte, indem deren Inhalte zusammengestellt, Formate, Berichtsfrequenzen und Kommunikationswege festgelegt und die entsprechenden Zielgruppen verwaltet werden können. Die automatisch erzeugten Berichtsteile, die z. B. in Form von Diagrammen aufbereitete Kennzahlen enthalten, können durch die Einbindung eigener Abschnitte – beispielsweise Einleitungen oder Verweise auf relevante andere Dokumente – und Annotationen der Kennzahlvisualisierungen ergänzt werden.
3. **Workflow-orientiertes Präsentieren von Sicherheitsberichten**: Neben dem Export statischer Sicherheitsberichte ermöglicht die Benutzeroberfläche auch ein interaktiven Abrufen der Kennzahlvisualisierungen. Abbildung 7.14 zeigt eine mögliche Ausprägung am Beispiel von Sicherheitskennzahlen für das Identitätsmanagement am LRZ, die in der Diplomarbeit von Florian Huber [Hub10] vertieft wurden. Die zu jeder Kennzahl erfassten Angaben wie Sollwerte und gültige Wertebereiche werden ebenfalls dargestellt und unterstützen als Orientierungshilfe die Interpretation der Diagramme; das Konzept sieht vor, dass bei Bedarf nähere Erläuterungen und Visualisierungen der Kennzahlen in anderen als den per Voreinstellung gezeigten Zeiträumen eingeblendet werden können. Wie unten erläutert wird, erfordert die Einbettung der Werkzeugnutzung in die Sicherheitsmanagement- und ITSM-Prozesse, dass Sicherheitsberichte von verschiedenen Personen in verschiedenen Rollen zur Kenntnis genommen, genehmigt und weiterverarbeitet werden. Diese mit Informationsaustausch verbundenen Vorgänge können von der Benutzeroberfläche beispielsweise durch Funktionen zur Annotation und Festhalten des jeweiligen Genehmigungs- bzw. Kenntnisnahmestatus gezielt unterstützt werden.

Durch die Neuartigkeit des Werkzeugs und seine nicht unerhebliche Komplexität bedingt liegt es nahe, es zunächst als eigenständige Software zu implementieren. Durch die parallel zur Benutzeroberfläche verfügbaren push- und pull-basierten Exportmöglichkeiten wird eine Isolation der Kennzahlendatenbestände jedoch von Anfang an vermieden. Das Exportmodul, das einzelne Kennzahlen und ganze Sicherheitsberichte zur Verfügung stellt, ermöglicht eine selektive, bedarfsorientiert detaillierte Datenübernahme in externe Managementsysteme und unterstützende Werkzeuge. Dadurch kann einerseits eine automatisierte, kontinuierliche Überwachung erreicht werden; andererseits fungiert das Werkzeug als zentraler Zugriffspunkt auf die Messagenten, so dass strukturierte Datenflüsse ermöglicht und redundante Messdatenerfassungen vermieden werden können.

Über die rein konzeptionelle Verfügbarkeit von Sicherheitskennzahlen hinausgehend beeinflussen sich die Abläufe in den Sicherheitsmanagement- bzw. ITSM-Prozessen und die Werkzeugnutzung gegenseitig gewinnbringend. Unter Bezug auf die in Kapitel 6 spezifizierten Prozesse lassen sich exemplarisch die folgenden Schnittstellen festhalten:

- **Risikomanagement**: Das Werkzeug unterstützt das Risikomanagement gezielt durch die kontinuierliche Überwachung bekannter Risiken und kann dabei insbesondere zur Beurteilung und Präzisierung der Eintrittswahrscheinlichkeiten von Schadereignissen beitragen. Im Gegenzug liefert das Risikomanagement neue und verbesserte Hypothesen und damit verbunden einen konkreten Erfassungs- und Auswertungsbedarf.

- **Change Management**: Für das Change Management bietet sich – in diesem Kontext ähnlich zum Financial Management – die Möglichkeit, die Auswirkungen von Infrastrukturänderungen bzw. Investitionen im Bezug auf die IT-Sicherheit zu überprüfen; Kennzahlenverläufe können die Grundlage für die Genehmigung und Priorisierung von Veränderungen bilden, insbesondere wenn sich eine anhaltende Verschlechterung abzeichnet. Der Bedarf an zur Vorbereitung entsprechender Entscheidungen erforderlicher Überwachungs- und Berichtsmaßnahmen beeinflusst wiederum die erfassten und ausgewerteten Sicherheitskennzahlen.
- **Compliance Management**: Sicherheitsberichte bilden die Grundlage für interne und externe Audits bezüglich der Einhaltung von Sicherheitsrichtlinien. Anhand der exportierten Sicherheitsberichte erkannte potentielle Abweichungen können durch die interaktive Nutzung des Werkzeugs bei Bedarf näher analysiert werden. Abweichungen vom Soll-Zustand und in Audits attestierte Mängel, die anderweitig festgestellt wurden und einen Bezug zur IT-Sicherheit aufweisen, können ebenfalls zur Implementierung neuer Kennzahlen führen; diese können im Rahmen von Folgeaudits als Nachweis für durchgeführte Verbesserungsmaßnahmen angeführt werden.
- **Security Incident Management**: Sicherheitsberichte stellen einzelne Sicherheitsvorfälle und deren Auswirkungen in einem größeren Kontext dar; sie ergänzen damit auch beispielsweise die Erstellung von Statistiken über Security-Incident-Records, die einzelne Vorfälle dokumentieren. Im Zusammenspiel mit dem Change Management können die Auswirkungen von aufgrund von Sicherheitsvorfällen getroffenen Verbesserungsmaßnahmen nachverfolgt werden. Über die treibende Rolle des Risikomanagements hinausgehend motiviert das Security Incident Management dabei nicht nur die Spezifikation von Kennzahlen, sondern fungiert mit seinen Werkzeugen und Managementsystemen auch als Datenquelle für das Kennzahlenmanagementsystem.
- **Service Level Management** und **Supplier Management**: Durch die Zielgruppenorientierung der Sicherheitsberichte und die Unterstützung verschiedener Rollen für Benutzer des konzipierten Werkzeugs erfolgt ein wichtiger Schritt in Richtung eines umfassenden *Customer Security Management*, indem Kunden bzw. den von ihnen benannten sicherheitstechnischen Ansprechpartnern direkter Zugriff auf die Sicht des Dienstanbieters auf die Sicherheitseigenschaften der angebotenen Dienste gewährt wird. Anhand der Sicherheitsberichte können die Kunden selbst vermeintliche Verstöße gegen in SLAs vereinbarte, sicherheitsspezifische Dienstgüteparameter prüfen. Über die Benutzeroberfläche des Werkzeugs können sie ggf. auch eigene, für die eigenen Bedürfnisse maßgeschneiderte Sicherheitsberichte zusammenstellen und für sie geeignete Exportformate wählen.

  Komplementär dazu kann das Werkzeug eingesetzt werden, um die von Zulieferern bzw. von der Organisation genutzten externen IT-Dienstleistern erreichten Sicherheitseigenschaften zu überwachen. Sofern die Gegenseite ebenfalls ein vergleichbares Werkzeug einsetzt bzw. kundenspezifische Sicherheitsberichte bereitstellt, können diese als Datenquellen angebunden und für Soll-Ist-Vergleiche sowie zur Überprüfung auf Abweichungen von lokalen Messdaten herangezogen werden. Ein entsprechender Abgleich von Sicherheitsberichten ist somit eine der tragenden Säulen einer organisationsübergreifenden Integration der IT-sicherheitsbezogenen Prozesse.
- **Availability Management**: Wie bereits in Abschnitt 6.5.2.2 diskutiert wurde, fallen

die Verfügbarkeit von Diensten als Basisziel der IT-Sicherheit und der kundenseitige Bedarf an auch losgelöst von der IT-Sicherheit möglichst störungsfrei betriebenen Diensten zusammen. Sicherheitsberichte belegen somit einerseits den Einfluss von Sicherheitsvorfällen auf die Verfügbarkeit; andererseits liefern das Availability Management und die SLAs Zielvorgaben für die Verfügbarkeit, die vom Kennzahlenmanagementsystem berücksichtigt werden müssen – insbesondere auch dann, wenn bislang generell noch keine anderen sicherheitsbezogenen Parameter im Rahmen von SLAs vorgesehen sind.

- **Configuration Management**: Die Configuration Management Database stellt eine der umfangreichsten Datenquellen für das Kennzahlenmanagementsystem dar, da die darin gespeicherten Configuration Items sowohl alle Assets mit diversen auch aus Sicherheitsperspektive relevanten Attributen als auch deren gegenseitige Beziehungen erfassen. Die CMDB liefert bei der Spezifikation neuer Hypothesen auch erste Anhaltspunkte, welche Dienste und Systeme geeignete Messdaten bereitstellen können. Das Kennzahlenmanagementsystem und seine Messagenten stellen zudem selbst CIs dar, die vom Configuration Management zu verwalten sind.

- **Continual Service Improvement**: Mit den Prozessen *Measuring* und *Service Reporting* bettet das Continual Service Improvement nach ITIL v3 das hier konzipierte Werkzeug in das gesamte ITSM-Berichtswesen ein. Dadurch wird zum einen sichergestellt, dass die Sicherheitsberichte den relevanten Zielgruppen vorgelegt werden; zum anderen wird eine Abstimmung der Inhalte von Sicherheitsberichten mit anderen ITSM-Berichten erwirkt, so dass eine prozessübergreifend konsistente Sicht erreicht wird.

- **Operatives Sicherheitsmanagement**: Das operative Sicherheitsmanagement profitiert am unmittelbarsten von der regelmäßigen Bereitstellung von Sicherheitskennzahlen. Aus den Dokumenten, die im Rahmen der in Abschnitt 6.5.1 beschriebenen Prozesse erstellt werden, beispielsweise der allgemeinen Sicherheitsleitlinie und der Spezifikation regulärer Assetnutzung, gehen unmittelbar Hypothesen und zu überwachende Sicherheitseigenschaften hervor; das Kennzahlenmanagementsystem trägt somit dazu bei, Verstöße gegen diese Richtlinien zu identifizieren und ihre Häufigkeit im Laufe der Zeit zu verfolgen. Durch die Anbindung von Datenquellen wie Personalverwaltungssystemen können Sicherheitseigenschaften, die sich nicht aus technischen Systemen auslesen lassen, berücksichtigt werden. Schließlich kann das Kennzahlenmanagementsystem auch zur längerfristigen Auswertung von sonst überwiegend auf den akuten Bedarf ausgerichteten Werkzeugen beitragen; beispielsweise können die von SIEM-Systemen aggregierten Ereignismeldungen und die sich im Laufe der Zeit durch neuartige Angriffe verändernde Erkennungsleistung von Intrusion-Detection-Systemen analysiert und beispielsweise mit den Datenbeständen des Vulnerability Management korreliert werden.

Die dadurch erreichte Integration des Werkzeugs in die Managementabläufe deckt sich auch mit Anforderung an Security-Frameworks, Kennzahlen für verschiedene Zielgruppen bereitzustellen, ohne jedoch eine umfassende eigene, für das jeweilige Framework spezifische und darauf beschränkte Berichterstattung anbieten zu müssen (vgl. Anforderungen *SF-MGMT-Berichtsdetails* und *SF-MGMT-Metriken*).

7.3.5. Bewertung des konzipierten Werkzeugs und mögliche Weiterentwicklungen

Das konzipierte Werkzeug trägt direkt zum Erreichen aller drei mit IT-Sicherheitskennzahlen und Sicherheitsberichten verfolgten Ziele bei: Es erlaubt das Festhalten und Bewerten der jeweils szenarienspezifischen Sicherheitseigenschaften, propagiert die ermittelten Ergebnisse aktiv an verschiedene Zielgruppen und stellt die Kennzahlen und Berichte zur Integration mit anderen Managementsystemen zum Abruf bereit. Es unterstützt dabei den hypothesengetriebenen Ansatz für Sicherheitsberichte, d. h. es werden nicht bei jeder Modifikation der IT-Infrastruktur bottom-up so viele zusätzliche Messdaten wie möglich bereitgestellt, indem neue Messagenten konfiguriert werden; vielmehr unterstützt das Werkzeug die Konzeption der gezielten Überwachung ausgewählter Sicherheitseigenschaften und deren Abbildung auf zusammenhängende Messwerte. Hypothesen, ihre Bestandteile und zur Beurteilung der Ergebnisse erforderliche Interpretationsregeln können mit dem Werkzeug nicht nur dokumentiert, sondern direkt implementiert und ausgewertet werden. Über push- oder pull-orientierte Messagenten können die Erfassung von Messdaten und das selektive Importieren von Datenbeständen anderer Managementsysteme automatisiert werden; parallel dazu ist eine manuelle Datenerfassung für solche Kennzahlen vorgesehen, deren automatisierte Akquisition nicht praktikabel ist. Durch integrierte Workflowunterstützungsfunktionalität kann ein kontinuierlicher Verbesserungsprozess, der unter anderem auf regelmäßigen Reviews der implementierten Kennzahlen beruht, vorangetrieben werden. Die Inhalte der Sicherheitsberichte werden sowohl in Form statischer Dokumente als auch über eine Benutzeroberfläche zugänglich gemacht; diese unterstützt neben vertiefenden interaktiven Recherchen auch die Arbeitsabläufe und den Informationsaustausch, beispielsweise durch die Möglichkeit zur Annotation von Berichtsteilen und die Abbildung von Genehmigungs- und Reviewprozessen.

Das vorgelegte Architekturkonzept beschränkt sich auf die Kernfunktionalitäten zur Unterstützung der in Abschnitt 6.6 spezifizierten Prozessabläufe; somit sind zusätzliche Funktionen und Erweiterungen der Architektur denkbar: Die in diesem Kapitel vorgestellte Verarbeitungskette für Messdaten mündet ausschließlich in Sicherheitsberichten; die im Informationsmodell für Sicherheitskennzahlen vorgesehenen Schwellwerte und Verknüpfungen mit **Eskalationsverfahren** könnten darüber hinaus für automatisierte Alarmierungen genutzt werden. Neben einer Anbindung der Komponente zur Messdatenverarbeitung beispielsweise an SIEM-Systeme könnten auch **benutzerspezifische Benachrichtigungen** vorgesehen werden, um Alternativen zu einer rein manuellen Interpretation der periodisch erstellten Sicherheitsberichte bieten zu können. Die Werkzeugarchitektur ist zudem unter dem Aspekt der **Ausfallsicherheit** zu überdenken; neben einer Vermeidung von Single Points of Failure, zu der beispielsweise die Replikation der Datenbasen beitragen kann, sind auch komponentenspezifische Self-Recovery-Verfahren vorzusehen, z. B. falls die Zeitsteuerung für die Messdatenerfassung gestört sein sollte. In diesem Zusammenhang kann auch die von Monitoringsystemen bekannte Berücksichtigung geplanter Wartungsarbeiten, die zu einer Verschiebung der Messzeitpunkte führen muss, betrachtet werden. Schließlich sollten zur Vervollständigung der Integrationsmöglichkeiten auch alle über den Abruf von Sicherheitsberichten und Kennzahlen hinausgehenden Funktionen der Benutzeroberfläche über eine **Programmierschnittstelle** zugänglich gemacht werden. Für die Nachhaltigkeit einer praktischen Umsetzung sind dazu jedoch noch konzeptionelle Vorarbeiten erforderlich; beispielsweise existieren bislang keine standardisierten Formate für den Austausch von Kennzahlenspezifikationen.

7.4. Zusammenfassung

Viele der in Kapitel 4 ermittelten Defizite bisheriger Security-Frameworks stehen der effizienten Umsetzung der in Kapitel 6 konzipierten Managementprozesse noch im Weg. In diesem Kapitel wurde deshalb zunächst unter Orientierung am Lebenszyklus von Security-Frameworks, der in Kapitel 5 spezifiziert wurde, analysiert, in welchen Bereichen ein besonders starker Bedarf an zusätzlichen Managementwerkzeugen besteht, die den praktischen Einsatz von Security-Frameworks gezielt unterstützen. Zwei dieser Werkzeuge wurden anschließend im Detail konzipiert und auf exemplarische Szenarien angewendet; ihre Auswahl und Spezifikation veranschaulicht die Kombination, die aus einer stark technisch-funktionalen Orientierung der Werkzeuge und den zu erzielenden Managementeigenschaften erreicht werden muss.

Das erste Werkzeug dient der automatischen Reparametrisierung der Detektionssensorik in Security-Frameworks und stellt eine konsequente Weiterentwicklung bestehender Konzepte zu dynamischen Intrusion Detection Systemen unter Berücksichtigung der Möglichkeiten und Zielsetzungen von Security-Frameworks dar. Nach einer Abgrenzung zu verwandten Arbeiten wurden die Architekturkonzepte und internen Arbeitsabläufe der Sensoren zur Erkennung IT-sicherheitsrelevanter Ereignisse und der zentralen Auswertestationen, die für die Dynamiksteuerung verantwortlich sind, spezifiziert. Die Verwaltung modular aufgebauter, dynamischer und optional autarker Sensoren erforderte die Erarbeitung eines Informationsmodells zur Sensorverwaltung und die Konzeption einer Funktionsbibliothek für die Auswertung der Sensormeldungen und die Ansteuerung der Dynamikeigenschaften. Im Rahmen eines Anwendungsbeispiels, für das ein vollständiger Auswertungs- und Steuerregelsatz implementiert und einer Simulation unterzogen wurde, wurden die durch die Dynamikeigenschaften erzielten Ressourceneinsparungen analysiert und beurteilt. Abschließend wurden die Einbettung des Werkzeugs in die Managementabläufe konzipiert und weitere Fragestellung, die eine Weiterentwicklung des Konzepts motivieren, herausgearbeitet.

Das zweite im Detail konzipierte Werkzeug dient der Erfassung und Aufbereitung von IT-Sicherheitskennzahlen, deren Prinzipien bereits in Abschnitt 6.6 diskutiert wurden. Es unterstützt Security-Frameworks als messdatenaggregierende Agenten, ist darüber hinaus jedoch auch für andere Datenquellen geeignet. Die Motivation für diese generische Ausrichtung des Werkzeugs ist der generelle Mangel an Möglichkeiten zur quantitativen Auswertung von Sicherheitseigenschaften, der nicht nur Security-Frameworks zu attestieren ist, aber eine nahtlose Verknüpfung des Sicherheitsmanagements mit anderen ITSM-Prozessen erheblich erschwert. Nach einer Abgrenzung gegenüber Monitoringsystemen, die einen ähnlichen Aufbau, aber andere Zielsetzungen und Schwerpunkte haben, wurden die Architektur des Kennzahlenmanagementsystems konzipiert und die Komponenten der Datenerfassungs-, Datenverarbeitungs- und Datenaustauschschicht spezifiziert. Im Anschluss wurden die technischen Schnittstellen zu den Datenquellen und das Vorgehen bei deren Verwaltung näher betrachtet. Schließlich wurden die Schnittstellen zwischen der Werkzeugnutzung und den Teilprozessen des Sicherheitsmanagements und des IT Service Management exemplifiziert, die erreichten Ziele rekapituliert und zukünftige Weiterentwicklungsmöglichkeiten vorgestellt.

Die praktische Relevanz der konzipierten Werkzeuge wird auch im Rahmen des Anwendungsbeispiels im nächsten Kapitel gezeigt.

Kapitel 8.

Beispiel für den Einsatz und das Management von Security-Frameworks

Inhalt dieses Kapitels

Ziel dieses Kapitels ist die vertiefende Veranschaulichung und Bewertung der in den vorhergehenden Kapiteln erarbeiteten Konzepte und Methoden anhand eines praxisnahen Anwendungsbeispiels. Hierzu soll ein komplexer IT-Dienst betrachtet werden, der unter nicht unerheblichem Zeit- und Budgetdruck implementiert werden muss, zahlreiche Abhängigkeiten von anderen IT-Diensten aufweist und nahtlos in die schon vorhandene Infrastruktur eines IT-Dienstleisters integriert werden soll. Durch diese Randbedingungen wird ein in der

Praxis häufig anzutreffendes Umfeld umrissen, das bereits ohne die explizite umfassende Berücksichtigung von IT-Sicherheitseigenschaften eine nicht unerhebliche Herausforderung für die Betreiber von IT-Diensten darstellt. Die Komplexität des Beispielszenarios wird ferner dadurch gesteigert, dass ein heterogener Reifegrad bezüglich der eingesetzten Sicherheitsmechanismen, IT-Service-Management- und Sicherheitsmanagementprozesse angenommen wird. In einer solchen typischen „gewachsenen Umgebung“ sollen nun sowohl mehrere Security-Frameworks zum Schutz des neuen IT-Dienstes parallel als auch die in dieser Arbeit konzipierten Managementwerkzeuge eingesetzt werden, um das Sicherheitsniveau zu steigern.

Als konkretes Anwendungsbeispiel, auf das die so charakterisierte Ausgangssituation zutrifft, fungiert das Projekt zum Aufbau des Petascale-Höchstleistungsrechners SuperMUC, der 2012 am Leibniz-Rechenzentrum (LRZ) der Bayerischen Akademie der Wissenschaften in Betrieb genommen wird und einen Meilenstein bei der Entwicklung des LRZ zum Europäischen Zentrum für Supercomputing darstellt. Dieses Szenario bietet für die weiteren Betrachtungen aus der Perspektive des Managements von Security-Frameworks drei Vorteile: Erstens betreibt das LRZ seit mehr als vier Jahrzehnten Großrechenanlagen bzw. Höchstleistungsrechner und kann somit auf umfassende Erfahrungen und Kenntnisse u. a. der relevanten Anforderungen und Sicherheitsmechanismen zurückgreifen, setzte dabei aber überwiegend auf szenarienspezifische Sicherheitskonzepte und somit keine Security-Frameworks ein. Zweitens sind mit SuperMUC mehrere Rollout-Phasen verbunden, die der sukzessiven Steigerung der Rechen- und Speicherkapazitäten dienen und somit auch mehrere Rollout-Phasen für die Security-Frameworks motivieren. Drittens kommen durch die Rolle des LRZ beispielsweise im Gauss Centre for Supercomputing e. V. (GCS), der Partnership for Advanced Computing in Europe (PRACE) und der European Grid Infrastructure (EGI) organisationsübergreifende Aspekte zum Tragen, die sich unmittelbar auf die Nutzung des Dienstes SuperMUC und somit auch die Ausprägung und das Management der eingesetzten Security-Frameworks auswirken.

Dieses Kapitel ist wie folgt und in Abbildung 8.1 dargestellt strukturiert: In Abschnitt 8.1 wird das SuperMUC-Szenario zunächst näher beschrieben, indem die Einführung eines neuen Höchstleistungsrechners mit ihren **Anforderungen** an die Integration in die vorhandene Infrastruktur und den LRZ-Dienstleistungskatalog skizziert wird; zudem werden sowohl die technische als auch die organisatorische Ausgangssituation erläutert. Daran anknüpfend werden in Abschnitt 8.2 die im hier exemplarisch betrachteten Implementierungsprojekt verfolgten **Ziele** definiert: Neben den zu erreichenden Sicherheitszielen und den Eckdaten der Infrastrukturintegration werden auch die gewünschten Managementeigenschaften und der Umfang der Anwendung von Security-Frameworks spezifiziert.

Die weiteren Abschnitte thematisieren die organisatorischen und technischen Aspekte des Einsatzes von Security-Frameworks und gehen dabei anhand des in Kapitel 5 konzipierten Lebenszyklus vor: In Abschnitt 8.3 wird zunächst die **Projektorganisation** vorgestellt, indem die für alle Security-Framework-bezogenen Themen relevanten Rollen und Zuständigkeiten sowie die für den Projektverlauf benötigten Akzeptanzkriterien definiert werden. Anschließend werden in Abschnitt 8.4 die für das Anwendungsbeispiel relevanten Teile der **SuperMUC-Gesamtarchitektur** mit einigen grundlegenden Sicherheitsmechanismen vorgestellt, die im weiteren Verlauf durch die Module und Komponenten von Security-Frameworks ergänzt werden. Auf dieser Basis wird in Abschnitt 8.5 demonstriert, wie drei zueinander überwiegend komplementäre und in ausgewählten Bereichen bewusst überlappende **Security-Frameworks** an das SuperMUC-Szenario angepasst werden können. Neben den Resultaten der Modul- und Mechanismenauswahl werden auch die Infrastrukturintegration und der resul-

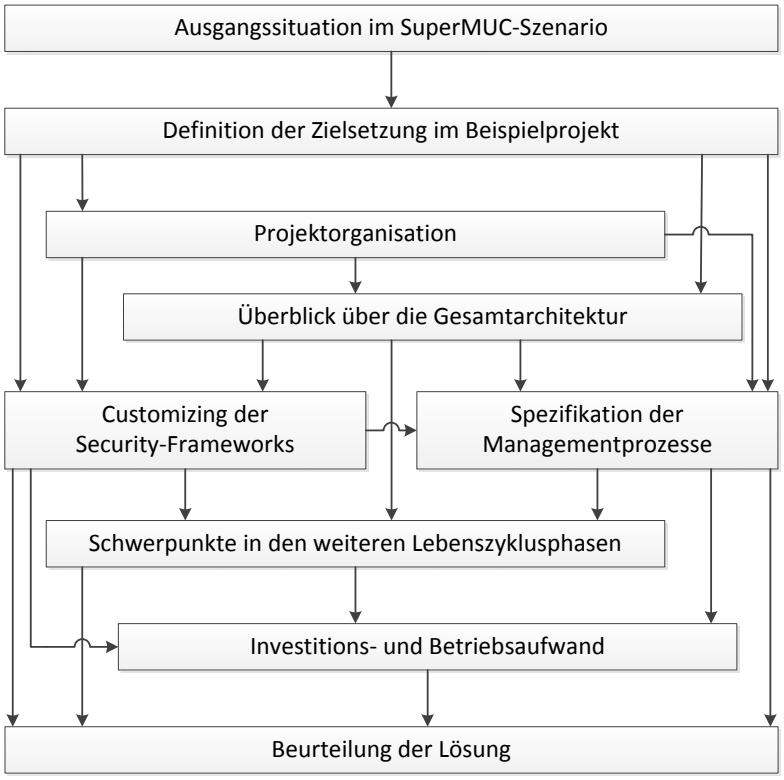


Abbildung 8.1.: Vorgehensmodell in diesem Kapitel

tierende Mehrwert vorgestellt. Diese technischen Ausführungen werden in Abschnitt 8.6 durch die **Spezifikation der Managementprozesse** und prozessualen Schnittstellen ergänzt, wobei neben den ITSM-Prozessen und Sicherheitsmanagementabläufen auch der Einsatz der in dieser Arbeit konzipierten Werkzeuge behandelt wird. Im Anschluss geht Abschnitt 8.7 auf ausgewählte **Schwerpunkte der weiteren Lebenszyklusphasen** ein: Neben den für Security-Frameworks relevanten Implementierungsaspekten und der Vorgehensweise bei der Inbetriebnahme wird ein Ausblick auf mögliche Überarbeitungsphasen und letztlich auch die Vorbereitungen für die Außerbetriebnahme bzw. Ablösung durch Nachfolgesysteme gegeben.

In Abschnitt 8.8 wird anschließend der **Investitions- und Betriebsaufwand** betrachtet, wobei sich die Ausführungen auf die organisatorischen und technischen Sicherheitsmaßnahmen beschränken und nicht der Dienst als Ganzes betrachtet wird. Schließlich wird in Abschnitt 8.9 eine **Bewertung der vorgestellten Lösung** vorgenommen; neben den erreichten Zielen werden dabei auch offene Punkte und mögliche weitere Schritte diskutiert. Das Kapitel endet mit einer Zusammenfassung in Abschnitt 8.10.

Für alle weiteren Ausführungen ist zu berücksichtigen, dass der Dienst SuperMUC sowie seine interorganisationale Einbettung und die daraus resultierenden Sicherheitsanforderungen zwar den realen Gegebenheiten entsprechen, im Rahmen dieses Anwendungsbeispiels aber auch fiktive, wenngleich realitätsnahe Ergänzungen vorgenommen wurden, um den Fokus auf das Management von Security-Frameworks zu lenken: Beispielsweise stehen von den in dieser Arbeit konzipierten Managementwerkzeugen noch keine hinreichend universell einsetzbaren,

stabilen Implementierungen zur Verfügung, so dass die Beschreibungen ihres Einsatzes im SuperMUC-Szenario zwar einen möglichen Soll-, aber nicht den kurzfristig erreichbaren Ist-Zustand widerspiegeln.

8.1. Beschreibung der Ausgangssituation im SuperMUC-Szenario

Der Betrieb von Höchstleistungsrechnern, die Spitzenplätze in der internationalen Top-500-Liste einnehmen, ist nicht nur mit hohen Investitionskosten für das Design und die Anschaffung der Hardware sowie die Bereitstellung einer Stellfläche von mehreren hundert Quadratmetern verbunden; auch die Betriebskosten, insbesondere für den Stromverbrauch des Höchstleistungsrechners an sich und seiner klimatechnischen Infrastruktur, sind enorm. Der Betrieb ist deshalb ökonomisch nur sinnvoll, so lange – unter geeigneter Berücksichtigung der Investitionskosten – das Verhältnis aus Rechenleistung zu Betriebskosten in Anbetracht der kontinuierlichen Weiterentwicklung der Technik stimmig bleibt. Hieraus resultieren am LRZ im Regelfall **Betriebsdauern von fünf bis sechs Jahren** pro Höchstleistungsrechner, gegen deren Ende der Übergang auf ein Nachfolgesystem geplant wird.

Im Folgenden wird deshalb das Projekt zur Ablösung des nationalen Höchstleistungsrechners HLRB II, der 2006 in Betrieb genommen wurde, durch das Petascale-System SuperMUC betrachtet. Damit verbunden ist, dass im Szenario sowohl Betriebs- als auch Sicherheitskonzepte und die damit verbundenen Betriebserfahrungen für mehrere Vorgängersysteme bereits vorhanden sind, so dass entsprechende Arbeiten nicht von Grund auf neu angegangen werden müssen. Vielmehr handelt es sich bei dem neu aufzubauenden um einen mit den bislang angebotenen Services vergleichbaren Dienst, der jedoch auf Basis anderer Hardware, anderer Software und im Zusammenspiel mit anderen Herstellern bzw. Zulieferern realisiert werden muss. Im Zuge seiner Einführung werden zudem die LRZ-internen system- bzw. dienstspezifischen Abläufe und Prozesse weiterentwickelt; ferner müssen **organisatorische und technische Weiterentwicklungen** im Umfeld des LRZ, wie es unten noch näher beschrieben wird, berücksichtigt werden.

Für den Höchstleistungsrechner SuperMUC sind dabei **drei Meilensteine** bezüglich seiner Hardwarekonfiguration geplant: Zunächst wird ein so genanntes Migrationssystem in Betrieb genommen, das auch als SuperMIG bzw. aufgrund der üppigen Ausstattung der einzelnen Knoten mit in Form von Shared Memory nutzbarem RAM auch als *Fat Node Island* (FNI) bezeichnet wird. Es bietet mit 8.200 Intel-Westmere-EX-CPU-Kernen mehr Rechenleistung als das Vorgängersystem HLRB II, verbraucht aufgrund der technischen Weiterentwicklungen aber nur einen Bruchteil an Strom und Stellfläche. Der Zeitraum, in dem nur dieses Migrationssystem produktiv betrieben wird, während parallel dazu an der Installation der weiteren Hardware gearbeitet wird, wird als **Phase 0** bezeichnet. Der Übergang zur **Phase 1**, der den zweiten Projektmeilenstein darstellt, erfolgt mit der Inbetriebnahme der 18 *Thin Node Islands* (TNIs); dort kommen Intel Sandy-Bridge-EP-Prozessoren mit 16 CPU-Kernen pro Knoten zum Einsatz, wobei pro TNI ebenfalls mehr als 8.000 CPU-Kerne erreicht werden. In der Phase 1 besteht SuperMUC somit als einem FNI, 18 TNIs sowie den als *Service-Nodes* bezeichneten, assoziierten Systemen wie z. B. den Login-Nodes, auf denen sich die Benutzer interaktiv einloggen können, und weiteren dedizierten Systemen, z. B. für Festplatten-Speicherplatz; auf diese wird unten näher aus Sicherheitsperspektive eingegangen. Der dritte Meilenstein, der die **Phase 2** einläutet, ist mit einer weiteren Vergrößerung insbesondere der

Rechenkapazität verbunden, deren genauer Zeitpunkt und Umfang erst im Projektverlauf festgelegt wird, wenn u. a. die Produktreife der dann aktuellen CPU-Entwicklungen beurteilt werden kann. Anders als beim Vorgängersystem HLRB II soll dabei aber voraussichtlich keine Leistungssteigerung durch Hardwareaustausch in situ erfolgen, sondern zusätzliche Hardware in Betrieb genommen und ins Gesamtsystem integriert werden.

Von der Anlieferung der ersten Hardware bis zum Erreichen des Benutzerbetriebs in Phase 1 vergeht rund ein Kalenderjahr. Unter Berücksichtigung vorhergehender Planungen zur Auswahl des Systems stehen somit rund 18 Monate zwischen der Vertragsunterzeichnung mit dem Systemhersteller und dem Eintritt in Phase 1 zur Verfügung, in denen neben dem Dienst auch die Sicherheitsmaßnahmen geplant, implementiert, getestet und in Betrieb genommen werden müssen. Die Bewältigung der damit verbundenen Aufgaben in der verfügbaren Zeit erfordert eine sowohl hersteller- als auch LRZ-seitige Parallelisierung, auf die unter dem Aspekt der Rollenverteilung in Abschnitt 8.3 eingegangen wird. Da für das Vorgängersystem HLRB II keine Security-Frameworks zum Einsatz kamen, wird auf dessen während der SuperMUC-Phase 0 anfallende Außerbetriebnahme nicht näher eingegangen.

Neben dem Aufbau und der Inbetriebnahme des neuen Dienstes muss seine **Integration** insbesondere in den folgenden vier Bereichen betrachtet werden, von denen die meisten direkte Auswirkungen auf den Einsatz von Security-Frameworks haben:

- Das Zusammenspiel des SuperMUC mit anderen LRZ-Dienstleistungen, z. B. dem Visualisierungszentrum, dem landesweit genutzten LRZ-Linux-Cluster, den angebotenen Grid-Diensten sowie dem Backup- und Archivierungsdienst muss konzipiert werden.
- Der Dienst SuperMUC baut auf zahlreiche andere, LRZ-intern bereits vorhandene Dienste auf; er soll beispielsweise den auf Basis von Firewalls geschützten Zugang zum Wissenschaftsnetz und Internet, die Service-Load-Balancer-Infrastruktur und das LRZ-weite Identity Management nutzen.
- Im Rahmen organisationsübergreifender Verbünde wie den oben bereits genannten GCS, PRACE und EGI werden neben strategischen und organisatorischen auch technische Vorgaben entwickelt, die bei der Umsetzung des Dienstes und im weiteren Betrieb berücksichtigt werden müssen. Darüber hinaus sind bei SuperMUC neben kunden- bzw. nutzerseitigen Bedarfsmeldungen auch die Weisungen eines Lenkungsausschusses umzusetzen.
- Am LRZ laufen Parallelprojekte zur stärkeren Ausrichtung des IT Service Management an ISO/IEC 20000-1 sowie des Sicherheitsmanagements an ISO/IEC 27001. Entsprechend sollen z. B. auch SuperMUC-spezifische Meldungen über Betriebsstörungen oder Sicherheitsvorfälle über die am LRZ etablierten Prozesse abgewickelt werden, die zum Teil wiederum Schnittstellen zu organisationsübergreifenden Abläufen aufweisen; beispielsweise existiert für die Meldung von Sicherheitsvorfällen ein GCS-Alarmierungsverfahren und Vorfälle, die mehrere High-Performance-Computing-Dienstleister betreffen, werden zusammen mit dem DFN- bzw. EGI-CERT bearbeitet.

Unter Bezugnahme auf die in Abschnitt 5.1.1 spezifizierten, im Vorfeld des Einsatzes von Security-Frameworks zu klärenden Voraussetzungen stellt sich die **Ausgangssituation** somit wie folgt dar:

- Die Hauptmotivation für die Auseinandersetzung mit neuen oder verbesserten Sicherheitsmechanismen ist die Einführung eines neuen IT-Dienstes; andere, reaktiv orientierte

Motivationslagen wie beispielsweise in Audits festgestellte Mängel liegen nicht vor.

- Angesichts des Investitionsvolumens für den neuen Dienst und die mit ihm verbundene internationale Reputation seines Betreibers liegt für alle am Projekt Beteiligten – vom Hersteller über das Management bis hin zu den Systemadministratoren – nahe, dass die IT-Sicherheit im Gesamtprojekt von Anfang an mit berücksichtigt werden soll.
- Die terminlichen Randbedingungen werden von der Bereitstellung und möglichst raschen Inbetriebnahme des Dienstes diktiert. Eine Projektverzögerung, die sich aus Engpässen bei der Umsetzung von Sicherheitsmaßnahmen ergibt, wäre nicht akzeptabel; da somit nicht darauf gewartet werden kann, dass eine „nahezu perfekte“ Sicherheitslösung aufgebaut wird, steigt die Bedeutung einer kontinuierlichen Verbesserung im Rahmen des Sicherheitsmanagements.
- Das Projekt findet zu einem Zeitpunkt statt, zu dem sich möglicherweise auch die im Szenario zu betrachtenden Angreifermodelle nachhaltig wandeln. Zum einen werden HPC-Systeme generell zu attraktiveren Angriffszielen, da sie zunehmend auf x86-Prozessor- bzw. Linux-Betriebssystembasis realisiert werden und somit oftmals dieselben Verwundbarkeiten aufweisen wie herkömmliche Linux-Server. Zum anderen ergeben sich beispielsweise durch die virtuelle Währung *BitCoin*, bei der Rechenleistung in Geldwerte umgewandelt wird, Angriffsarten, bei denen die hohe Rechenleistung von HPC-Systemen ein wichtiges Differenzierungsmerkmal potentieller Angriffsziele ausmacht. Kompromittierte HPC-Systeme werden somit nicht mehr nur überwiegend als Sprungbrett für weitere Angriffe oder aufgrund der typischerweise hohen verfügbaren Netzbandbreite z. B. zum Massenversand von Spam-E-Mails missbraucht, sondern vom Angreifer explizit aufgrund ihrer spezifischen Rechenkapazität ausgewählt.
- Im betrachteten Szenario stellt die Benutzerfreundlichkeit ein nicht zu vernachlässigendes Kriterium dar. Anders als beispielsweise bei einigen Installationen im militärischen Bereich, bei denen die HPC-Systeme intern von einer kleinen Nutzergruppe verwendet werden, soll der Dienst SuperMUC internationalen Spitzenwissenschaftlern verschiedenster Disziplinen den einfachen Zugang zu Rechen- und Speicherressourcen ermöglichen. Alleine schon durch die geographische Verteilung dieser Nutzerschaft bedingt ist keine lokale Abschottung des Systems möglich. Auch mit hohem logistischen Aufwand verbundene Sicherheitslösungen wie beispielsweise eine Authentifizierung über Smartcards könnten im Szenario nicht realisiert werden.
- Durch die im Projekt sehr enge Zusammenarbeit des Dienstbetreibers mit dem Hersteller des Systems ist das erforderliche Hintergrundwissen sowohl über die LRZ-Infrastruktur und die LRZ-Prozesse als auch die Hard- und Softwareeigenschaften des neuen Dienstes vorhanden.
- Die Security-Frameworks sollen im Beispiel parallel zum neuen Dienst eingeführt werden, wobei berücksichtigt werden muss, dass auch vorher bereits zahlreiche Sicherheitsmechanismen im Einsatz waren. Die Wiederverwendbarkeit vorhandener Schutzmaßnahmen und die nahtlose Integration in die am LRZ vorhandene Infrastruktur sind deshalb ebenso wichtig wie das reibungslose Zusammenspiel der resultierenden Sicherheitskonzepte mit dem neuen Dienst.

Zudem sollen in diesem Anwendungsbeispiel mehrere Security-Frameworks parallel implementiert werden; dies dient jedoch nicht nur der Veranschaulichung der erarbeiteten Konzepte,

sondern bietet sich auch aufgrund der komplementären Sicherheitsfunktionalität der in Frage kommenden Security-Frameworks an.

8.2. Definition der Zielsetzung für das SuperMUC-Beispielprojekt

Unter Berücksichtigung der in Abschnitt 5.2.2 erarbeiteten Konzepte muss zu Beginn eines Projekts zur Instanziierung von Security-Frameworks zunächst eine Einbettung des Vorhabens in die Servicestrategie (vgl. Dienstleistungslebenszyklus nach ITIL v3) vorgenommen werden. Hierzu werden nachfolgend die wesentlichen Ziele für das Anwendungsbeispiel definiert. Unter Vernachlässigung der nicht für Security-Frameworks spezifischen Zielsetzungen, beispielsweise der Realisierung des Projekts unter Einhaltung der Zeit- und Budgetvorgaben, sind dabei die sicherheitsfunktionalen Eigenschaften, die Integration in die bestehende Infrastruktur und die für die Security-Frameworks spezifischen Managementeigenschaften zu betrachten.

Hierbei zeichnen sich die folgenden Schwerpunkte ab:

- Bezüglich der Sicherheitsfunktionalität werden vorrangig die vom LRZ zu erbringenden Aspekte, also beispielsweise die technische Umsetzung von Benutzerauthentifizierung und -autorisierung sowie die Einbindung in die organisationsübergreifenden Verbünde und in die lokale Infrastruktur betrachtet. Die reine Systemsicherheit wird auf Basis des SuperMUC-Betriebskonzepts in weiten Teilen an den Hersteller delegiert; lokale Härtungsmaßnahmen werden deshalb im Folgenden nur soweit vertieft, wie es für das Zusammenspiel mit den Security-Frameworks erforderlich ist. Die zu erreichenden **Sicherheitsziele** können deshalb vereinfacht wie folgt zusammengefasst werden:
  - Es muss sichergestellt werden, dass nur bekannte, zuverlässig authentifizierte und autorisierte Personen Zugang zum SuperMUC-System und seinen Ressourcen erhalten.
  - Es müssen geeignete Maßnahmen zur Sicherstellung der Vertraulichkeit von Anwenderdaten und somit insbesondere eine zuverlässige gegenseitige Abschottung der Benutzer bzw. Benutzergruppen untereinander erzielt werden. Auch einem Missbrauch der verarbeiteten Daten durch den Betreiber des Systems ist vorzubeugen.
  - Es muss eine hohe Systemverfügbarkeit erreicht werden; das heißt, dass auch beim Eintreten von Sicherheitsvorfällen die Priorität auf eine möglichst rasche Rückkehr zum Soll-Zustand gelegt werden soll.
  - Neben präventiven Maßnahmen muss es explizit auch Überwachungs- und Monitoringmechanismen geben, die eine rasche Erkennung von Sicherheitsvorfällen erlauben.
  - Für typische Sicherheitsvorfälle, beispielsweise dass das Passwort eines Benutzers kompromittiert wurde, sind a priori Reaktionswege festzulegen, die eine effiziente Bearbeitung ermöglich. Auch für alle anderen IT-sicherheitsspezifischen Schadensfälle sind die Zuständigkeiten und Verantwortlichkeiten vorab zu regeln.
  - Es ist ein Sicherheitsberichtswesen zu etablieren, das den kontinuierlichen Verbesserungsprozess unterstützt und zur frühzeitigen Erkennung des Bedarfs an zusätzlichen oder verbesserten Sicherheitsmaßnahmen beiträgt.

- Bei der **Integration** des neuen Dienstes und seiner Sicherheitsmaßnahmen in die Infrastruktur müssen die folgenden Teilziele im Projekt berücksichtigt werden:
  - Obwohl das SuperMUC-System zu den wichtigsten Diensten im gesamten Portfolio des LRZ gehört, dürfen weder alle bereits etablierten Schutzmechanismen und organisatorischen Maßnahmen komplett umgestaltet werden noch darf der neue Dienst die Einführung von komplexen, zu den bisherigen Konzepten parallelen und redundanten Sicherheitsinfrastrukturen erforderlich machen.
  - Die geschaffene Lösung muss flexibel sein, so dass die kontinuierliche, organisationsübergreifend vorangetriebene Weiterentwicklung – beispielsweise bezüglich der Standardisierung von Zugangsverfahren im GCS- bzw. Grid-Umfeld – berücksichtigt werden kann.
  - Es muss ein Kompromiss erreicht werden, bei dem sowohl die mit dem Betrieb der Vorgängermaschinen gewonnenen Erfahrungen und die damit verbundenen eingespielten Abläufe berücksichtigt als auch die mit dem Projekt verbundenen Möglichkeiten zur Weiterentwicklung und Verbesserung genutzt werden können.
- In Anlehnung an die Definition von IT-Services nach ITIL v3 geht das organisationsweite Management in der Regel nicht rein technikgetrieben vor, sondern berücksichtigt immer auch die involvierten Personen und Abläufe („people, processes, and technology“). Dadurch ergeben sich für die **Managementeigenschaften** die folgenden Teilziele:
  - Bezüglich des Personaleinsatzes müssen die Organisationsstruktur und die Kompetenzprofile berücksichtigt werden. Wie in Abschnitt 8.3 vertieft wird, muss beispielsweise beachtet werden, dass die zuständigen Systemadministratoren nur zum Teil auf die IT-Sicherheit spezialisiert sind und dass der abteilungsübergreifende Arbeitskreis zum Thema IT-Sicherheit keine direkte Weisungsbefugnis für das Projektteam hat; somit müssen also auch Gruppen- und Abteilungsleiter geeignet in die Projektkommunikation eingebunden und die langfristigen Verantwortlichkeiten im Rahmen eines Betriebskonzepts spezifiziert werden. Alle LRZ-seitig Projektbeteiligten sind im IT Service Management nach ISO/IEC 20000 geschult, einige auch im Sicherheitsmanagement nach ISO/IEC 27000. Folglich soll einerseits das Personal im Rahmen der bereits vorhandenen Fachkenntnisse in das Projekt und in den Betrieb eingebunden und andererseits der zusätzliche Schulungsbedarf, der sich u. a. aus dem Einsatz von Security-Frameworks ergeben kann, identifiziert werden.
  - Im Hinblick auf die Managementprozesse sind einerseits die organisationsweit bereits etablierten Verfahren zu nutzen; es wäre offensichtlich kontraproduktiv, ein separates Verfahren für die Erfassung und Bearbeitung von Störungsmeldungen aufzubauen, wenn für alle anderen Dienste bereits ein einheitliches Incident Management realisiert wurde. Andererseits existieren dienstspezifische Abläufe unter anderem bezüglich der technischen Administration und der Benutzerbetreuung von HPC-Systemen, die weitestgehend von den Vorgängersystemen übernommen werden können und im Weiteren nicht im Detail, sondern nur bezüglich ihrer Schnittstellen zum Sicherheitsmanagement betrachtet werden.
  - Vorhandene Managementsysteme und die damit verbundenen Arbeitsabläufe müssen so weit wie möglich beibehalten werden; mit der Einführung des neuen Dienstes sollte beispielsweise nicht die Notwendigkeit größerer Umstellungen im LRZ-

weiten Netz- und Systemmanagement aufkommen. Demgegenüber ist die Einführung zusätzlicher, für den Dienst oder seine Sicherheitsmechanismen spezifischer Werkzeuge, wie sie beispielsweise für das Management von Security-Frameworks benötigt werden, tragbar. Dabei sind am LRZ parallel zur Inbetriebnahme des SuperMUC laufende Arbeiten zu berücksichtigen; beispielsweise werden im Rahmen des in Abschnitt 7.2.1 bereits kurz dargestellten Projekts GIDS Angriffserkennungsmechanismen speziell für Grid-Ressourcen implementiert, die zwar kein Security-Framework darstellen, in der Gesamtarchitektur aber dennoch geeignet berücksichtigt werden müssen.

Für die Exemplifizierung der in dieser Arbeit spezifizierten Konzepte und Methoden wird zusätzlich postuliert, dass die auszuwählenden Security-Frameworks von verschiedenen Autoren bzw. Herstellern stammen und partiell überlappende Anwendungsbereiche ausweisen; damit kann sowohl die Auswahl der jeweils am Besten geeigneten Maßnahmen als auch die bewusste Schaffung von Redundanz im Sinne des *Defense-in-depth*-Paradigmas demonstriert werden.

8.3. Organisation des SuperMUC-Beispielprojekts

Die Anwendung der in dieser Arbeit konzipierten Methoden ist an eine Rollenverteilung gebunden, die in Abschnitt 2.2.1 eingeführt und im gesamten Kapitel 5 konsequent umgesetzt wurde. In diesem Abschnitt werden die entsprechenden Rollenzuordnungen im Beispielszenario vorgestellt, da sich hieraus die in den weiteren Abschnitten relevante Aufgabenverteilung und die Möglichkeit zur Anwendung der einheitlichen Nomenklatur ergeben.

Zunächst ist festzuhalten, dass es sich beim Aufbau und bei der Inbetriebnahme des SuperMUC trotz der im Vorfeld bei der Dienstplanung durchgeführten Einbettung des Vorhabens in die deutschen und europäischen Supercomputing-Strategien um ein allein vom LRZ organisiertes Projekt handelt. An der Implementierung wirken deshalb LRZ-Mitarbeiter sowie der Systemhersteller und von diesem – beispielsweise für die Durchführung von Schulungen – beauftragte Subunternehmer mit; es wird jedoch kein weiteres Personal z. B. aus dem GCS- oder PRACE-Umfeld mit Implementierungsaufgaben betraut. Somit liegt auch die **Verantwortung** für die Umsetzung der Vorgaben, die im Rahmen der organisationsübergreifenden Verbünde entstanden sind, beim LRZ.

Für die **Durchführung** des Projekts wird sowohl LRZ- als auch herstellerseitig Personal zur Verfügung gestellt, wobei wie in Abbildung 8.2 dargestellt fachspezifische Teams u. a. für die Bereiche Softwarekonfiguration, Monitoring, Batch-Schnittstellen, Backup und Archivierung, Security und Dokumentation eingeführt werden. Die Mitglieder der einzelnen Teams treffen sich zu Besprechungen überwiegend bedarfsorientiert; regelmäßige Gesamtprojekttreffen und die gemeinsame Nutzung einer zentralen Groupware-Lösung für die Ablage von Dokumenten, das Verwalten aktueller Aufgaben und das Verfolgen identifizierter Schwierigkeiten unterstützen den erforderlichen Informationsfluss. Der spätere Betrieb des Dienstes soll von einer Teilmenge des Projektpersonals, d. h. mit reduzierten Teamstärken, übernommen werden können.

Für das Projekt kann die folgende Zuordnung von Rollen zu beteiligten Personen durchgeführt werden:

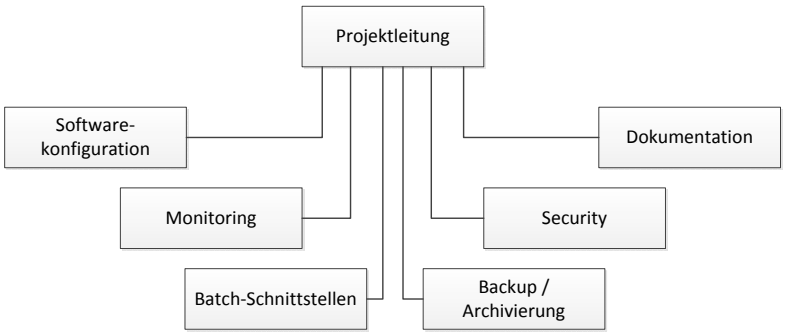


Abbildung 8.2.: Fachspezifische Teams im SuperMUC-Einführungsprojekt

- *Administrator*: Als Administratoren fungieren primär Mitarbeiter der LRZ-Abteilung Hochleistungssysteme; wie bereits bei früheren HPC-Systemen werden sie von einigen vom Hersteller für die Betriebsdauer abgeordneten Mitarbeitern unterstützt. Die jeweiligen Zuständigkeiten werden im Betriebskonzept festgelegt.
- *Anwender*: In der Gesamtnutzerschaft des Vorgängersystems finden sich einige als *friendly users* bezeichnete, repräsentative Anwendergruppen, die bereit sind, das neue HPC-System auch bereits vor der Aufnahme des allgemeinen Benutzerbetriebs unter Inkaufnahme damit möglicherweise verbundener Instabilitäten zu verwenden. Auf Basis ihrer Rückmeldungen können zusätzliche Anforderungen aus Sicht der Anwender frühzeitig erfasst und umgesetzt werden.
- *Auditor*: Da das SuperMUC-System keinem von außen durchgeführten Audit unterzogen wird und für HPC-Dienste bislang auch keine LRZ-internen Audits durchgeführt werden, handelt es sich beim Auditor um eine Rolle, die keiner Einzelperson fest zugeordnet werden kann; vielmehr handelt es sich um eine dynamische Rolle, die je nach Projektphase und Themenbereich von unterschiedlichen Personen wahrgenommen werden kann, beispielsweise wenn die fachlichen Voraussetzungen für die Abnahme eines Teilsystems bzw. für das Erreichen eines Projektmeilensteins geprüft werden müssen.
- *CISO*: Der Chief Information Security Officer ist eine vom Projekt unabhängige, organisationsweite Rolle, die von einem Mitglied der LRZ-Leitung wahrgenommen wird.
- *Designer*: Im Kontext des Managements von Security-Frameworks sind die Designer für die Detailspezifikation einzelner Sicherheitsmechanismen zuständig, d. h. es wird nachfolgend nicht die technische Gestaltung des gesamten Höchstleistungsrechners betrachtet. Im Anwendungsbeispiel gibt es kein dediziertes Personal, das diese Rolle wahrnimmt; stattdessen sind sowohl Administratoren als auch Security Engineers partiell auch in dieser Rolle aktiv.
- *Entwickler*: Die Entwickler realisieren im Umfeld von Security-Frameworks die Instanzierung des szenarienspezifischen angepassten Frameworkkonzepts. Ähnlich zur Rolle des Designers muss diese Aufgabe im Beispielprojekt von den Administratoren und Security Engineers übernommen werden.
- *Projektleiter*: Mit der Gesamtprojektleitung wird ein Mitarbeiter des Systemherstellers beauftragt, um den LRZ-seitig anfallenden Koordinationsaufwand zu reduzieren und

die Gesamtverantwortung sowohl für die Bereitstellung des HPC-Systems als auch den Erfolg des Projekts bei einer Organisation zu bündeln.

- *Prozesseigner*: Der Leiter der LRZ-Abteilung Hochleistungssysteme fungiert als Prozesseigner für alle mit dem Dienst SuperMUC zusammenhängenden Geschäftsprozesse.
- *Security Engineer*: Die Security Engineers des LRZ sind in Form eines abteilungsübergreifenden Arbeitskreises organisiert und unterstützen die Einführung und Verbesserung von Sicherheitsmaßnahmen sowohl konzeptionell als auch in der Implementierungsphase. Einige der Security Engineers sind auch für die Administration und den Betrieb einzelner Sicherheitsmechanismen verantwortlich.
- *Systemarchitekt*: Bei dieser Rolle muss zwischen dem Systemarchitekten für das gesamte HPC-System und dem Architekten für die Sicherheitsmaßnahmen unterschieden werden; beide Rolleninhaber müssen sich offensichtlich eng untereinander abstimmen. Die HPC-Systemarchitektur wird auf Basis der vom LRZ definierten Anforderungen vom Hersteller konzipiert; für die Sicherheitsarchitektur müssen analog zum Design und zur Entwicklung wiederum die LRZ-seitigen Security Engineers und die Administratoren zusammenarbeiten.
- *Technologieexperte*: Auch diese Rolle ist im betrachteten Projekt nicht dediziert besetzt und wird deshalb von den Security Engineers mit übernommen.

Darüber hinaus wird eine Gesamtprojektplanung vorgenommen, die neben den Terminen und Meilensteinen auch die einzelnen Aufgaben, deren gegenseitige Abhängigkeiten und absehbare Risiken – beispielsweise Lieferengpässe bei bestimmten Hardwarekomponenten – spezifiziert. Für jeden Themenbereich werden auf Basis der definierten Rollen die Zuständigkeiten zugewiesen und Hauptansprechpartner festgelegt. Für das Gesamtsystem werden Abnahmekriterien definiert, von denen die sicherheitsspezifischen Ziele eine Teilmenge darstellen (vgl. Abschnitt 8.2).

8.4. Überblick über die SuperMUC-Gesamtarchitektur

Bevor in den weiteren Abschnitten auf die Details der Anpassung von Security-Frameworks an das SuperMUC-Szenario und die damit einhergehenden Managementprozesse eingegangen wird, wird im Folgenden die SuperMUC-Architektur beschrieben, um die spätere Zuordnung von Schutzkomponenten zu Assets verdeutlichen zu können. Abbildung 8.3 ist der Benutzerdokumentation entnommen und zeigt die Systemarchitektur schematisch und mit dem Ziel der allgemeinen Verständlichkeit vereinfacht. Im Fokus dieser Darstellung stehen einerseits die **CPU- und RAM-Ressourcen**, die wie bereits diskutiert aus einem FNI und 18 TNIs bestehen, und andererseits die **Hintergrundspeicher**, wobei zwischen Ablagebereichen für Benutzerverzeichnisse (*home directories*), hochperformanten parallelen Filesystemen für temporäre Dateien und Ausgabedateien (*scratch*- und *work*-Bereiche) sowie den Backup- und Archivierungsmöglichkeiten unterschieden wird.

Abbildung 8.4 stellt die SuperMUC-Gesamtarchitektur mit ihren für die weiteren Ausführungen erforderlichen einzelnen Komponenten dar und ordnet auch bereits erste Sicherheitskomponenten schematisch in die grundlegenden Datenflüsse ein. Auch diese Abbildung ist zugunsten der Übersichtlichkeit gegenüber der Realität stark vereinfacht und betont die sicherheitsrelevanten Schnittstellen, ohne auf die jeweils interne Realisierung der Funktionalität

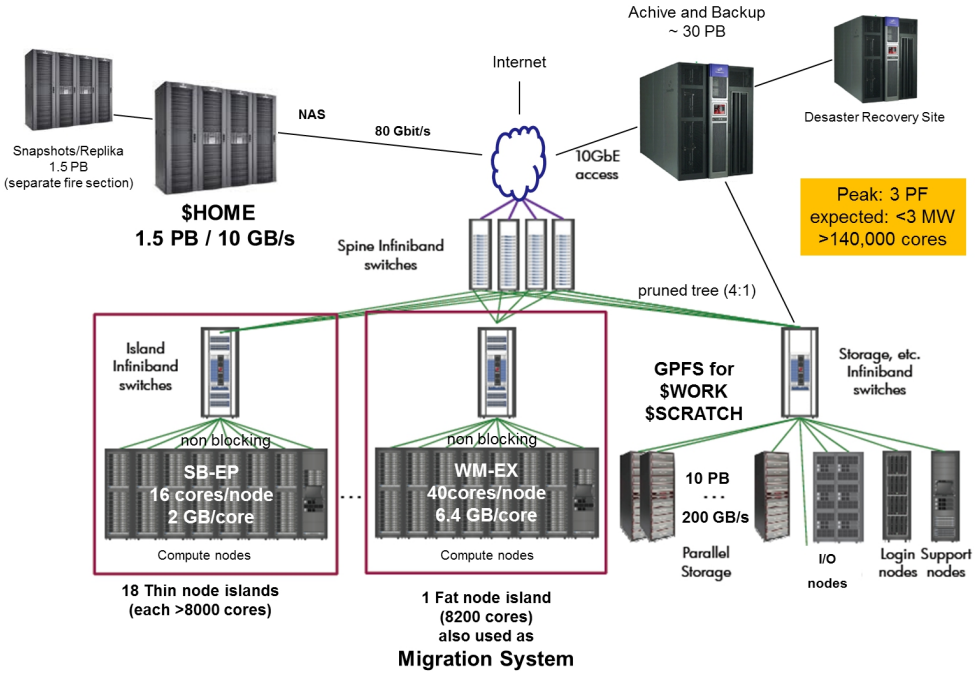


Abbildung 8.3.: Darstellung der SuperMUC-Architektur für Anwender (Bildquelle: `http://www.lrz.de/services/compute/supermuc/systemdescription`)

einzugehen. Insbesondere wurde auf die Darstellung der Hardwareredundanz, die zur Lastverteilung und Erhöhung der Ausfallsicherheit dient, beispielsweise indem den Benutzern mehrere Login-Knoten zur Verfügung gestellt werden, verzichtet. Zudem wurden die verschiedenen Dateiablagebereiche vereinfachend zu einem System zusammengefasst, da sie hinsichtlich ihrer Sicherheitseigenschaften ähnlich behandelt werden können. Zur Erläuterung der Architektur werden die Abläufe nachfolgend aus Benutzerperspektive, in der Abbildung also von oben nach unten und primär an den mit Fettschrift hervorgehobenen Elementen orientiert, erläutert:

- Jeder **Benutzer** kann den Dienst SuperMUC von seinem **Arbeitsplatzrechner** oder einer anderweitig lokal zur Verfügung gestellten Infrastruktur nutzen, sofern er dafür berechtigt ist. Diese Autorisierung erhält er entweder, indem er als LRZ-Benutzer erfasst wird und somit vom LRZ eine Kennung zugewiesen bekommt, oder indem er zu einer Einrichtung gehört, die z. B. im Rahmen des Grid-Computing einen eigenen so genannten **Identity-Provider** betreibt, der vom LRZ als Datenquelle akzeptiert wird.
- Zur Nutzung der Rechen- und Speicherressourcen verbindet sich der Benutzer per SSH bzw. GridSSH mit einem **Login-Node**. Die Login-Nodes können sowohl interaktiv per SSH-Kommandozeile oder für den Transfer von Dateien eingesetzt werden, die dann auf einem der **Fileserver** abgelegt werden. Der Zugriff auf die Login-Nodes wird zum einen über eine **Firewall** gesteuert, d. h. Benutzer können den SuperMUC-Dienst nur von vorab bekanntgemachten Quellnetzen bzw. einzelnen Maschinen aus verwenden; Verbindungsversuche von allen anderen Quellen aus werden unterbunden, wodurch be-

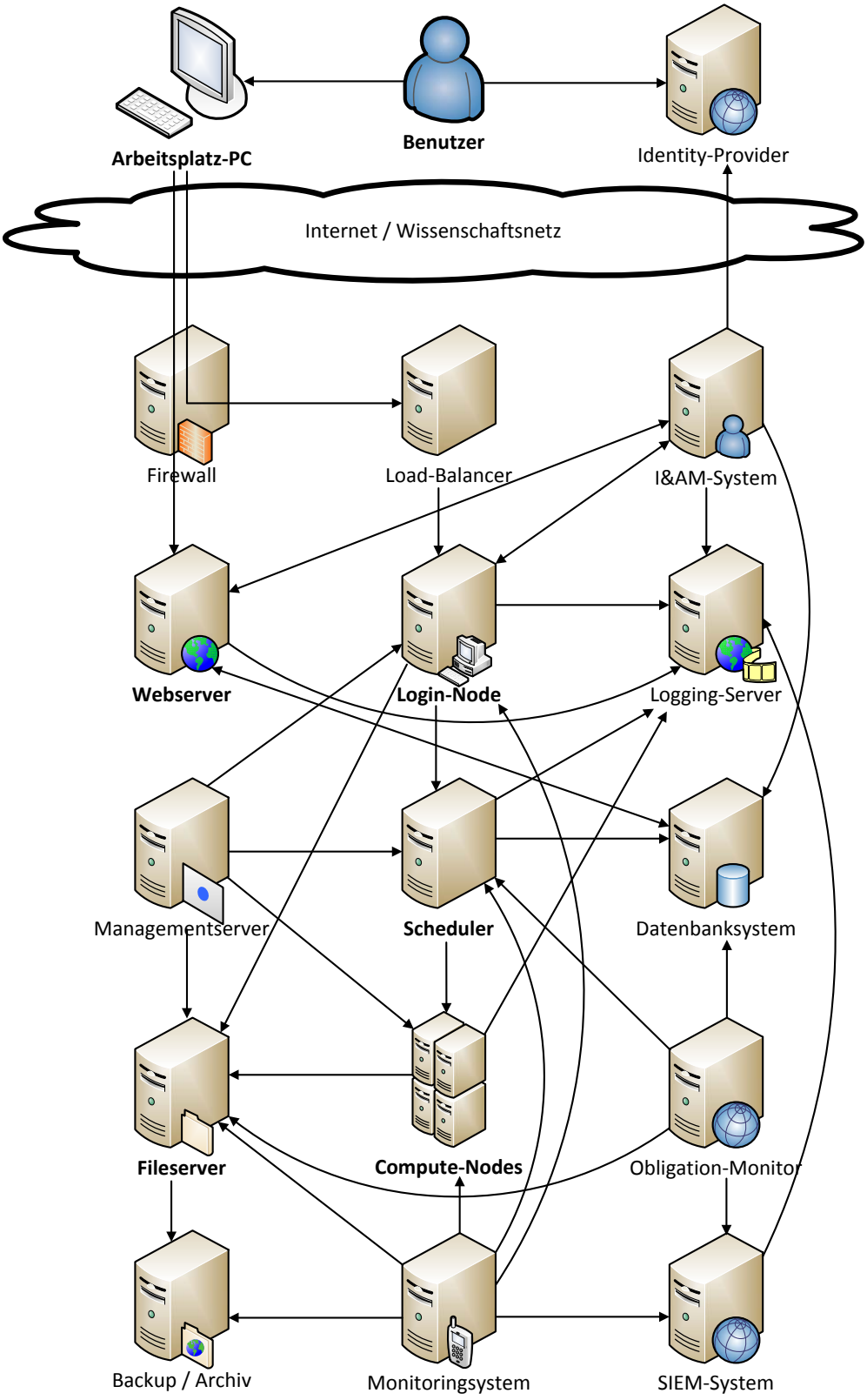


Abbildung 8.4.: SuperMUC-Architektur mit ausgewählten zentralen Diensten und Sicherheitskomponenten

reits ein großer Teil der Angriffsversuche im Keim erstickt werden kann. Zum anderen übernimmt ein vorgeschalteter Service-**Load-Balancer** die Verteilung der eingehenden Verbindungen auf die verfügbaren Login-Nodes, die dadurch möglichst gleich ausgelastet werden sollen.

- Alternativ meldet sich der Benutzer per Browser auf einem SuperMUC-spezifischen **Webserver** an. Über diesen erhält er Zugriff auf nicht allgemein verfügbare Systemdokumentationen, kann Statistiken über seine HPC-Nutzung abrufen und wird über den Bearbeitungsstatus von ihm gemeldeter Störungen informiert.
- Die Login-Nodes und der SuperMUC-Webserver sind an das LRZ-weite **Identity & Access Management System** gekoppelt. Dadurch wird sichergestellt, dass nur bekannte, authentifizierte und autorisierte Benutzer Zugang zu den Login-Nodes erhalten. Das I&AM-System deckt dabei sowohl vom LRZ selbst erfasste Benutzer als auch den Abruf von Benutzerinformationen über den jeweils zuständigen Identity-Provider ab.
- Als weiterer zentraler Dienst wird ein **Logging-Server** genutzt, der Protokolleinträge von allen an der SuperMUC-Gesamtarchitektur beteiligten Komponenten entgegennimmt und deren zentrale Auswertung und Korrelation unterstützt; über seine Schnittstellen zu den einzelnen Komponenten lässt er nur die Meldung neuer Protokolleinträge zu, die somit vom Quellsystem nicht gelöscht werden können. Ein Angreifer, der eine solche Quellmaschine kompromittiert, könnte somit zwar lokale Protokolldateien manipulieren, hat aber keine Möglichkeit, die bereits an den zentralen Logging-Server gemeldeten Protokolleinträge zu modifizieren, ohne zunächst auch diese Maschine zu kompromittieren.
- Über die Login-Nodes bzw. mit Hilfe der darauf auch installierten Middleware bringen die Benutzer ihre als Jobs bezeichneten rechen- und speicherintensiven Programme ein, die auf den **Compute-Nodes** ausgeführt werden sollen. Die Verwaltung entsprechender Warteschlangen und die Zuordnung von Jobs zu Compute-Nodes übernimmt ein zentraler **Scheduler**. Er berücksichtigt dabei einerseits den Status der Compute-Nodes, beispielsweise bezüglich ihrer aktuellen Last und geplanter Wartungsarbeiten, für die die Compute-Nodes freigehalten werden sollen, und führt andererseits als Grundlage für das Accounting Buch darüber, welcher Benutzer bzw. welche Benutzergruppe wann welche Programme wie lange auf welchen Compute-Nodes ausgeführt hat; da jedem Benutzerprojekt nur eine begrenzte CPU- bzw. Speicherkapazität zugestanden wird, übernimmt der Scheduler auch die Rolle eines Policy Enforcement Points (PEP), der die Ausführung bestimmter Programme unterbindet – beispielsweise, wenn die zugewiesenen Kontingente bereits überschritten wurden oder aktuell keine geeigneten Compute-Nodes zur Verfügung stehen.
- Die vom Scheduler erzeugen Accountingdaten und weitere Informationen über Benutzer und Jobs werden in einem **Datenbanksystem** abgelegt, das auch als zentrale Informationsquelle für den SuperMUC-Webserver dient.
- Die Login-Nodes, Compute-Nodes und der Scheduler werden von einem zentralen **Managementserver** aus verwaltet; als Managementplattform kommt dabei die Open-Source-Softwaresuite xCAT (*Extreme Cloud Administration Toolkit*) zum Einsatz, die auf das effiziente Management einer Vielzahl zueinander recht ähnlicher Maschinen, wie sie insbesondere die Compute-Nodes darstellen, ausgelegt ist. Dazu werden auf dem Fileserver Systemabbilder (*system images*) vorgehalten, die von den Compute-Nodes, die

ohne eigene Festplatten auskommen, über das Netz gebooted und dabei zur Laufzeit einer geeigneten Konfigurationsanpassung unterzogen werden.

- Benutzerdaten, d. h. die zu den Jobs gehörenden Programme, Eingabedaten und Ausgabedaten, werden automatisch auf Bandlaufwerken gesichert (**Backup**); darüber hinaus können Benutzer bei Bedarf auch eine Langzeitarchivierung anstoßen.
- Ein **Monitoringsystem** überwacht die Verfügbarkeit und Dienstgüte der SuperMUC-Komponenten. Es kann ausgewählte oder aggregierte Meldungen an andere, organisationsweit genutzte Systeme weitergeben und eine Alarmierung der SuperMUC-Administratoren beim Überschreiten vorgegebener Schwellenwerte durchführen.
- Der **Obligation-Monitor** ist als zentraler Bestandteil eines der ausgewählten Security-Frameworks bereits in die Abbildung eingezeichnet, um seine Schnittstellen zu den anderen Komponenten zu verdeutlichen. Er hat die Aufgabe, benutzerspezifizierte Aktionen wie das Löschen nach Ende der Bearbeitung eines Jobs nicht mehr benötigter Eingabedateien automatisch umzusetzen.
- Ein LRZ-weit eingesetztes **SIEM-System** auf Basis der Open-Source-Software OSSIM aggregiert sicherheitsrelevante Meldungen, die entweder vom Monitoringsystem weitergeleitet, vom Obligation-Monitor erzeugt oder durch Auswertung der Einträge im Logging-Server erhalten wurden.

Alle SuperMUC-spezifischen Komponenten sind zudem in eigenen VLANs und IP-Subnetzen gekapselt, um die am LRZ übliche dienstspezifische Netzsegmentierung umzusetzen.

Beim Netzzugang mit Firewallschutz, dem Load-Balancer, dem I&AM-System, dem Datenbanksystem, dem Logging-Server, dem Monitoringsystem, der Backup- und Archivierungslösung sowie dem SIEM-System handelt es sich um Dienste und Sicherheitskomponenten, die nicht spezifisch für den SuperMUC sind, so dass sich Synergien aus der Nutzung des LRZ-Dienstportfolios ergeben können. Zum Teil müssen an diesen Diensten jedoch Anpassungen bzw. Ergänzungen vorgenommen werden; beispielsweise muss sichergestellt werden, dass die für alle GCS-Sites einheitlich vorgesehenen Authentifizierungsverfahren vom I&AM-System unterstützt werden. Darüber hinaus sind – auch mit Bezug auf die IT-Sicherheit und die Konfiguration der Komponenten von Security-Frameworks – weitere zentrale Dienste wie die Public-Key-Infrastruktur des DFN-Vereins (DFN-PKI) und das Grid-spezifische Intrusion Detection System GIDS zu nutzen. Auf die damit verbundenen Schnittstellen und Designentscheidungen wird an den entsprechenden Stellen in den nächsten beiden Abschnitten eingegangen.

8.5. Customizing der Security-Frameworks für den Dienst SuperMUC

Die folgenden Ausführungen bis einschließlich Abschnitt 8.7 orientieren sich bezüglich der beschriebenen Vorgehensweise an dem in Kapitel 5 spezifizierten Lebenszyklus von Frameworkinstanzen. Da die Anwendung des in Kapitel 3 erarbeiteten Kriterienkatalogs zur Bewertung und Auswahl von Security-Frameworks bereits umfassend in Kapitel 4 exemplifiziert wurde, werden nachfolgend in Abschnitt 8.5.1 nur knapp die für das Beispielszenario wichtigsten Anforderungen zusammengetragen, um in Abschnitt 8.5.2 auf die Schwerpunkte und Ergebnisse

der Anpassungen der auf dieser Basis ausgewählten drei Security-Frameworks eingehen zu können.

8.5.1. Szenarienspezifische Anforderungen an Security-Frameworks

Insbesondere durch die hybride Nutzung des SuperMUC-Dienstes einerseits durch vom LRZ verwaltete Benutzer und andererseits im Rahmen diverser Grid-Verbünde treffen für einige der in Abschnitt 3.1.1 beschriebenen Charakteristika von Szenarien, in denen Security-Frameworks eingesetzt werden können, jeweils mehrere Ausprägungen zu: Mindestens die *Anzahl der beteiligten Organisationen*, die *Szenariendynamik* und der *Benutzerkreis* müssen je nach Anwendungsgebiet differenziert betrachtet und die Ergebnisse miteinander kombiniert werden. Darüber hinaus ergeben sich durch die Komplexität und die spezifischen Eigenschaften des SuperMUC-Dienstes einige Anforderungen, die zu einer Schwerpunktbildung bezüglich der von Security-Frameworks zur Verfügung zu stellenden Merkmale führen; diese gehen mit einer gegenüber der in Abschnitt 3.7.3 zusammengefassten szenarienübergreifend allgemeinen Gewichtung verstärkt mit *wichtigen* und *essentiellen* Anforderungen einher.

Im Folgenden werden deshalb die für das SuperMUC-Szenario charakteristischen Aspekte der vier in dieser Arbeit durchgängig verwendeten Anforderungskategorien zusammengetragen:

1. Bezüglich der sicherheitsfunktionalen Eigenschaften (**SF-FUNK**) ergeben sich die folgenden Anforderungsschwerpunkte:

   - Für die *Abschottung* des Dienstes SuperMUC ist es wichtig, Konzepte umzusetzen, durch welche die trotz der Einbindung des Dienstes in organisationsübergreifende Verbünde gegebene lokale Autarkie nicht gefährdet wird. Da die organisationsübergreifende Zusammenarbeit beispielsweise im Rahmen von GCS auf strategischer Ebene erfolgt und derzeit z. B. keine Bildung gemeinsamer Gruppen von Systemadministratoren auf technischer Ebene vorsieht, muss ein uneingeschränkter Zugriff von Partnereinrichtungen auf die LRZ-Ressourcen unterbunden werden.
   - Eine wichtige Rolle kommt der *Adaptivität* der eingesetzten Sicherheitskomponenten zu. Durch die Größe und Komplexität des SuperMUC-Systems bedingt muss beispielsweise zwingend vermieden werden, dass Konfigurationsanpassungen einen Neustart des Dienstes nach sich ziehen; auch andere Formen der mit einer Anpassung der Sicherheitsmechanismen verbundenen Dienstausfälle sind weitgehend auszuschließen. Die Schutzmaßnahmen müssen folglich Angriffe im Rahmen a priori abgesteckter Grenzen ohne manuelle Eingriffe in ihre Konfiguration abdecken können.
   - Bezüglich der von den Security-Frameworks bzw. Sicherheitsmechanismen berücksichtigen *Angriffe* ist es im Szenario essentiell, dass auf HPC- und Grid-Spezifika eingegangen wird.
   - Auch die *Automatisierung* ist im SuperMUC-Szenario essentiell, da das System trotz seiner physischen Größe und hardware- wie auch softwareseitigen Komplexität von einem in Relation dazu kleinen Team von Administratoren gepflegt werden muss. Auch im Hinblick auf die Nutzung bereits vorhandener Infrastrukturkomponenten und Schutzmechanismen muss berücksichtigt werden, dass der SuperMUC-Dienst aus deren Perspektive nur einen von zum Teil vielen angebundenen Diens-

ten darstellt, so dass abteilungsübergreifend nicht beliebig viele Ressourcen für im Dauerbetrieb manuell durchzuführende Tätigkeiten gebunden werden dürfen.

2. Bezüglich der Integrationseigenschaften (**SF-INT**) sind primär die folgenden Anforderungen zu berücksichtigen:

   - Da die Bereitstellung des SuperMUC-Dienstes in mehreren Phasen erfolgt, sollten auch die Security-Frameworks entsprechende *Ausbauphasen* unterstützen, die sich terminlich mit den SuperMUC-Meilensteinen in Einklang bringen lassen.
   - Durch den Bedarf an organisationsübergreifend einheitlichen Lösungen – beispielsweise bezüglich der in einem Grid-Verbund bereitzustellenden Authentifizierungsverfahren – und dem Bedarf an einer kontinuierlichen Weiterentwicklung der eingesetzten technischen Schutzmaßnahmen gilt auch die *Erweiterbarkeit* des Security-Frameworks als sehr wichtig.
   - Aufgrund der gemeinsamen Nutzung zentraler Sicherheitsdienste wie dem I&AM-System sowie den Firewalls an den Netzzonenübergängen kommt dem *Parallelbetrieb* auch im SuperMUC-Szenario eine essentielle Bedeutung zu.

     Demgegenüber spielt beispielsweise die *Polyinstanziierbarkeit* der einzusetzenden Security-Frameworks eine nur untergeordnete Rolle, da im Beispielszenario nur die einmalige Installation am LRZ betrachtet wird; die HPC-Systeme der Partnereinrichtungen müssen nicht notwendigerweise mit denselben Security-Frameworks bzw. einer gemeinsam erarbeiteten Frameworkkonfiguration ausgestattet werden.
   - Der *Skalierbarkeit* der Security-Frameworks kommt eine offensichtlich essentielle Rolle zu, da neben der Größe des Dienstes mit seiner sechsstelligen Anzahl an CPU-Kernen auch die Benutzeranzahl und das Volumen der zu transportieren Ein- und Ausgabedaten stetig zunehmen.
   - Die *Usability* der Sicherheitsmechanismen ist sowohl aus Benutzer- als auch aus Administratorenperspektive wichtig; insbesondere darf der Zugang zum neuen HPC-Dienst für die Benutzer nicht unnötig erschwert werden, um zu vermeiden, dass das System dadurch an Attraktivität bei den Nutzerzielgruppen verliert.
   - Schließlich ist auch die *Wiederverwendbarkeit* ein wichtiger Faktor bei den Arbeiten an und mit den Security-Frameworks. Neben der bereits thematisierten Nutzung am LRZ bereits vorhandener Sicherheitsmechanismen ist dabei auch darauf zu achten, dass neu eingeführte Maßnahmen nach Möglichkeit auf zukünftige Nachfolgesysteme übertragen werden können, ohne für diese von Grund auf neu aufgebaut werden zu müssen.

3. Die Schwerpunkte der Managementeigenschaften (**SF-MGMT**) korrelieren im SuperMUC-Szenario mit den folgenden Anforderungen:

   - Das Erzeugen von Sicherheitsmeldungen und geeignete Schnittstellen für Sicherheitsmanagementwerkzeuge zum Zugriff auf sicherheitspezifische *Events* sind wichtig, um zeitnahe Reaktionen auf vermutete bzw. entdeckte Sicherheitsvorfälle erzielen zu können.
   - Die mit den Security-Frameworks sowohl bezüglich ihrer Bereitstellung als auch im laufenden Betrieb verbundenen *Kosten* müssen sich im Gesamtrahmen des

Projekts bewegen; dabei müssen insbesondere die laufenden Betriebskosten und -aufwendungen adäquat gestaltet werden können.

- Die *Mandantenfähigkeit* ist einerseits im Hinblick auf die vom LRZ selbst verwalteten Projekte und andererseits bezüglich der verschiedenen Grid-Verbünde, an denen das LRZ beteiligt ist, wichtig. Insbesondere dürfen sich durch die jeweiligen Spezifika dieser Nutzungskategorien keine negativen gegenseitigen Einflüsse ergeben.
- Die *Performanz* ist aus offensichtlichen Gründen essentiell; da die Qualität und der Mehrwert eines HPC-Systems maßgeblich von der hohen Performanz bei der Übertragung und Verarbeitung von Daten abhängen, dürfen durch die Security-Frameworks keine neuen Engpässe in die Gesamtarchitektur eingebracht werden.
- Auch dem *Support* für die Security-Frameworks bzw. ihre Komponenten kommt im Szenario eine wichtige Rolle zu, da analog zu Störfällen bei anderen SuperMUC-Komponenten eine rasche Störungsbeseitigung bei den Sicherheitsmaßnahmen zur Dienstqualität beiträgt. Die bedarfsorientierte zeitnahe Verfügbarkeit entsprechenden Expertenwissens zu den einzelnen Security-Frameworks ist deshalb mit der regionalen Lagerung von Hardwareersatzteilen vergleichbar.

4. Bezüglich der Dokumentationseigenschaften (**SF-DOKU**) ist schließlich festzuhalten, dass analog zur sicherheitsfunktionalen Anforderung an die Erkennung spezifischer Angriffe auch die für das hier betrachtete Anwendungsumfeld relevante *Angreifermodelle* berücksichtigt werden müssen, die z. B. gezielt HPC- oder Grid-Ressourcen angreifen.

Diese Anforderungsschwerpunkte beeinflussen aus offensichtlichen Gründen nicht nur die Auswahl, sondern auch die Anpassung der Security-Frameworks an das SuperMUC-Szenario. Hierauf wird im folgenden Abschnitt eingegangen.

8.5.2. Schwerpunkte und Ergebnisse der Anpassungen der Security-Frameworks

Bei SuperMUC handelt es sich um einen stark spezialisierten Dienst, der in seiner spezifischen Form als organisationsübergreifend genutzte HPC-Plattform für wissenschaftlichen Einrichtungen nur von relativ wenigen IT-Dienstleistern angeboten wird. Entsprechend ist zum einen die Menge der für diesen Dienst prinzipiell geeigneten Security-Frameworks gut überschaubar; zum anderen bietet sich im SuperMUC-Szenario die Möglichkeit, auf lokal entstandene Frameworkkonzepte zurückzugreifen, für die auch entsprechendes unterstützendes Fachwissen verfügbar ist. Im weiteren Verlauf des Anwendungsbeispiels wird die Umsetzung der folgenden drei Security-Frameworks für SuperMUC betrachtet:

1. Das *Framework für föderiertes Sicherheitsmanagement* von Helmut Reiser wurde bereits in Abschnitt 4.3.1 detailliert betrachtet. Es ist insbesondere für die Nutzung des SuperMUC im Rahmen der Grid-Projekte und weiteren organisationsübergreifenden Verbünde relevant und behandelt dabei die meisten der o. g. sicherheitsfunktionalen Zielsetzungen.
2. Mit dem *policy-based security framework for privacy-enhancing data access and usage control in Grids* [Homm11] hat der Autor der vorliegenden Arbeit ein Frameworkkonzept spezifiziert, das auf Basis seiner Vorarbeiten in [Hom08a] und [Homm09] die technischen

und organisatorischen Voraussetzungen für die datenschutzgesetzkonforme Verarbeitung personenbezogener Daten in Grids und anderen HPC-Verbünden ermöglicht. Es bindet aktuelle Konzepte aus dem organisationsübergreifenden Identity Management mit ein und komplementiert das Frameworkkonzept von Helmut Reiser somit spezifisch im Bereich Datenschutz (*privacy management*).

3. Das Linux-Kernel-spezifische Security-Framework von Wright et al. wurde auf Seite 192 vorgestellt. Im SuperMUC-Szenario wird es zum einen zur betriebssystemseitigen Härtung (*system hardening*) eingesetzt und bildet zum anderen die systemspezifische Schnittstelle für die Zugriffskontrolle im Rahmen des Datenschutz-Security-Frameworks.

Alle drei ausgewählten Security-Frameworks weisen die Eigenschaft auf, dass sie die am LRZ bereits vorhandenen Sicherheitsmaßnahmen sowohl um sicherheitsfunktionale Mechanismen als auch organisatorische bzw. rechtliche Aspekte ergänzen. Ihrer nahtlosen Integration in die bereits vorhandene Infrastruktur kommt deshalb eine wichtige Bedeutung zu, deren Umsetzung in diesem Anwendungsbeispiel verdeutlicht werden soll. Aufgrund dieser Zielsetzung und den durch die langjährige und zum Teil in mehreren Iterationen durchgeführte Entwicklung der Security-Frameworks erzielten Reifegrad steht im Folgenden die Konzeption der praktischen Anwendung im Vordergrund, wohingegen auf die in Kapitel 5 für jede Lebenszyklus geforderten Rückkanäle zu den Frameworkautoren nicht vertiefend eingegangen wird.

Nachfolgend werden die Schwerpunkte und Ergebnisse der Anpassungsphase für jedes der drei Security-Frameworks zusammengestellt. Dabei wurden die folgenden Einschränkungen getroffen:

- Das Customizing wird vereinfachend nur für die ersten beiden Rollout-Phasen, d. h. die SuperMUC-Betriebsphasen 0 und 1, durchgeführt. Für spätere Erweiterungen, die z. B. mit dem Übergang zur SuperMUC-Betriebsphase 2 eingeführt werden könnten, sollten die ersten mit dem praktischen Einsatz der Security-Frameworks gewonnenen Erfahrungen berücksichtigt werden, so dass hierfür nur grob die Richtung vorgegeben wird.

- Auf Basis der in Kapitel 5 spezifizierten Vorgehensweise müssten im Rahmen der Customizingphase einige Konzepte vorgelegt werden, die beispielsweise auf die Einbettung in Managementarchitekturen und das Schaffen von Schnittstellen zu den ITSM-Prozessen abzielen. Auf diese Aspekte wird im Folgenden jedoch nicht beim Customizing, sondern separat an den entsprechenden Stellen in Abschnitt 8.6, in dem die Managementprozesse beschrieben werden, eingegangen.

- Auf eine fachliche, organisatorische und fiskalische Prüfung der Anpassungsergebnisse wird verzichtet, da es sich um ein fiktives Anwendungsbeispiel handelt. Auf ausgewählte fiskalische Aspekte wird stattdessen im Rahmen der Aufwandsbetrachtung in Abschnitt 8.8 eingegangen.

In einem realen Projekt würde das Customizing wie in Abschnitt 5.5 beschrieben überwiegend von den Designern und Systemarchitekten sowie den Security Engineers durchgeführt werden; die hier vorgestellten Ergebnisse gehen hingegen aus offensichtlichen Gründen auf Überlegungen des Autors dieser Arbeit zurück.

8.5.2.1. Customizing-Ergebnisse des Frameworks für föderiertes Sicherheitsmanagement

Das Security-Framework von Helmut Reiser wurde explizit u. a. im Rahmen der auch für das LRZ relevanten Grid-Projekte entwickelt, so dass die darin genannten Beurteilungskriterien für zur Auswahl stehende Sicherheitskomponenten direkt auf das SuperMUC-Szenario angewendet werden können. Zudem setzt das Security-Framework an genau den Stellen an, die für das Zusammenspiel der lokalen Autarkie und der erforderlichen organisationsübergreifenden Abstimmung relevant sind.

Wie in Abbildung 4.3 auf Seite 150 dargestellt setzt sich das Security-Framework aus acht Sicherheitsdienstklassen zusammen, die alle für das SuperMUC-Szenario relevant sind; im Bereich der Sicherheitsdienstklasse *Privacy-Dienste* ergeben sich Überlappungen mit bzw. Schnittstellen zum unten beschriebenen Datenschutz-Security-Framework. Die Anpassung der rund 20 Sicherheitsdienste in diesen acht Klassen resultiert in der folgenden Zielsetzung für die Implementierung:

1. Die **Datensicherheitsdienste** umfassen die technischen Maßnahmen zur Sicherstellung der drei grundlegenden IT-Sicherheitsziele Integrität, Verbindlichkeit und Vertraulichkeit:

   - Die *Integrität* der *Kommunikation* wird analog zur Vertraulichkeit wie unten beschrieben mit Standardwerkzeugen zur sicheren Kommunikation erreicht. Die Integrität der *gespeicherten Daten* wird durch das Backup- und Archivierungskonzept unterstützt; darüber hinausgehende Maßnahmen zur Erkennung böswilliger Modifikationen an Benutzerdaten können aufwandsbedingt jedoch noch nicht angeboten werden, u. a. da es für die Benutzer im Einzelfall nicht zumutbar wäre, den jeweiligen Soll-Zustand explizit zu definieren. Das Frameworkkonzept weist auch explizit darauf hin, dass heutige Middleware-Implementierungen noch keine entsprechenden Mechanismen dafür bereitstellen.
   - Der Forderung nach *Verbindlichkeit* wird durch die LRZ-seitige Protokollierung, beispielsweise der submittierten HPC-Jobs, nachgekommen. Durch die Verwendung des zentralen Logging-Servers kann eine Manipulation durch externe Angreifer weitgehend ausgeschlossen werden. Reiser weist jedoch explizit darauf hin, dass beim aktuellen Stand der Technik weitere Mechanismen fehlen, um die Verbindlichkeit dieser Protokolldaten garantieren zu können, d. h. dass eine absichtliche Manipulation durch den Dienstbetreiber bislang nicht zuverlässig verhindert werden kann.
   - Die *Vertraulichkeit* der Daten wird über Verschlüsselung erreicht. Interaktive Verbindungen, die der Benutzer zu den Login-Nodes bzw. zum SuperMUC-spezifischen Webserver aufbaut, werden durch das SSL-Protokoll geschützt (im Rahmen von SSH bzw. HTTPS). Bei der Übertragung großer Dateien (Bulk File Transfer) über die Grid-Middleware kann jeder Benutzer zur Performanzsteigerung optional auf die Verschlüsselung verzichten. Beim Zugriff auf den SuperMUC-Dienst über Grid-Middleware wird neben der client-server-orientierten Nachrichtenverschlüsselung im Rahmen einzelner TCP/IP-Verbindungen auch eine Ende-zu-Ende-Verschlüsselung erreicht. Es muss jedoch berücksichtigt werden, dass die Vertraulichkeit der in den SuperMUC-Dateisystemen gespeicherten Dateien durch diese Mechanismen nicht garantiert werden kann, wenn sie vom Benutzer nicht

bereits in verschlüsselter Form abgespeichert werden; lediglich die per Backup gesicherten und archivierten Dateien können nach Konfiguration durch den Benutzer verschlüsselt werden.

2. Im Rahmen der **AAI-Dienste** werden die fünf zentralen Aspekte des Identity Management betrachtet:
   - Die zuverlässige *Identifikation* erfolgt entweder im Rahmen der am LRZ etablierten Benutzerverwaltungsprozesse oder auf Basis entsprechender Vertrauensbeziehungen zu Partnereinrichtungen in Grid-Verbünden. Um beide Quellen für Benutzerdaten miteinander verbinden und dadurch die mit Datenredundanz und potentiellen Inkonsistenzen verbundene Mehrfacherfassung von Personen zu vermeiden, muss die LRZ-Benutzerverwaltung dahingehend erweitert werden, dass neben den LRZ-intern verwendeten Benutzeridentifikatoren auch die aus Grid-User-Zertifikaten entnommenen DN-Einträge (*distinguished name* des Zertifikatsinhabers) zugeordnet werden können.
   - Die *Authentifizierung* wird analog zu früheren Höchstleistungsrechnern und nach Abstimmung mit den Partnereinrichtungen über Passwort, SSH-Schlüsselpaare oder Grid-User-Zertifikate abgewickelt. Diese Verfahren werden von der SSH-Server- bzw. GridSSH-Software, die auf den Login-Nodes zum Einsatz kommen, unterstützt. Neben mehrere Jahre gültigen Grid-User-Zertifikaten, die über ausgewählte Registration Authorities beantragt werden, können auch kurzlebige, d. h. nur einige Stunden oder wenige Tage gültige Zertifikate beispielsweise des vom DFN betriebenen Short Lived Credential Services (SLCS) genutzt werden; die Voraussetzungen hierfür wird durch die Einbindung des LRZ Identity-Providers in die deutsche Hochschulföderation DFN-AAI erreicht.
   - Die *Autorisierung* ergibt sich aus der Zuordnung einzelner Kennungen zu Projekten bzw. Gruppen im Rahmen der LRZ-Benutzerverwaltung. Neben der grundlegenden Berechtigung zum Login auf dem SuperMUC können beispielsweise auch Kontingente für den Plattenplatz verwaltet werden.
   - Die Umsetzung der *Zugriffskontrolle* im Sinne eines PEP obliegt primär dem auf dem SuperMUC eingesetzten Betriebssystem im Zusammenspiel mit dem Autorisierungsmanagement; dieses muss beispielsweise die gegenseitige Abschottung von Benutzerprojekten bzw. einzelnen Benutzern realisieren. Für Grid-Benutzer muss die Zugriffskontrolle ferner von der eingesetzten Middleware umgesetzt werden. Für den Zugriff auf Benutzerdaten, der vom LRZ beispielsweise zur Erstellung von Backups angestoßen wird, muss ferner das Zusammenspiel mit dem unten erläuterten Datenschutz-Security-Framework berücksichtigt werden.
   - Ein *Single Sign-On*, d. h. die Nutzung mehrerer Dienste nach einmaliger Passworteingabe, wird implizit bei der Verwendung von SSH-Schlüsselpaaren oder Grid-User-Zertifikaten bzw. Short Lived Credentials unterstützt, so dass hierfür keine zusätzlichen Komponenten erforderlich sind.
3. An **Basisdiensten** werden das Trust-Level-Management und das Policy-Management betrachtet:
   - Über das *Trust-Level-Management* werden Vertrauensbeziehungen und davon ableitbare Autorisierungsentscheidungen verwaltet. Obwohl beispielsweise

mit [Bou09] hochgradig dynamische Konzepte für die Realisierung und Anwendung von Trust-Levels vorgestellt wurden, setzen die aktuellen Grid-Anwendungen noch überwiegend auf statische Konfigurationen. Dabei werden die erforderlichen Vertrauensbeziehungen vertraglich vereinbart und die damit implizierten Berechtigungen manuell und pauschal für alle davon abgedeckten Benutzergruppen konfiguriert. Die Zuordnung einzelner Benutzer zu diesen Berechtigungsklassen wird technisch durch die Überprüfung der Grid-User-Zertifikate umgesetzt. Hierdurch verlagert sich ein Teil der Problematik des Trust-Level-Managements zu den Registration Authorities, die Grid-User-Zertifikate ausstellen; beispielsweise ergeben sich Restriktionen, wenn Zertifikate für Benutzer angefordert werden, deren Nationalität einem Land zugeordnet ist, für das die Exportkontrolle für Supercomputer anzuwenden ist (vgl. [BMBF11]).

- Bezüglich des *Policy-Management* ergeben sich für das SuperMUC-Szenario keine Besonderheiten gegenüber früheren bzw. den anderen HPC-Diensten am LRZ. Dies ist insbesondere darauf zurückzuführen, dass die Regelungen, die z. B. im Rahmen von GCS, D-Grid und PRACE getroffen wurden, bereits manuell in Einklang mit den LRZ-lokalen Richtlinien gebracht wurden. Aufgrund der bislang relativ geringen Dynamik ist dabei auch der Bedarf an einer weitergehenden bzw. vollständigen Automatisierung des Policy-Mappings gering und wird hier nicht vertieft. Auch in der Gegenrichtung hat die Inbetriebnahme des SuperMUC keine Auswirkungen auf die vorhandenen PKIs und Grid-spezifischen Acceptable Use Policies (AUPs).

4. Die **Privacy-Dienste** umfassen die Aspekte Anonymisierung und Datenschutz:

   - Bezüglich der *Anonymisierung* ist das Zusammenspiel mit dem im Rahmen des D-Grid entstandenen Grid Intrusion Detection System zu betrachten: Über ein technisches Betriebskonzept wird sichergestellt, dass für die Grid-weite Angriffserkennung nur pseudonymisierte bzw. ausreichend anonymisierte Alarmmeldungen u. a. mit dem DFN-CERT ausgetauscht werden. Von Benutzern auf dem SuperMUC gespeicherte Dateien liegen davon unabhängig jedoch im Verantwortungsbereich der jeweiligen Benutzer; dies wird in den LRZ-Benutzungsrichtlinien geregelt, ist ebenfalls Gegenstand des Datenschutz-Security-Frameworks und wird hier deshalb nicht näher betrachtet.

   - Der *Datenschutz* wird bislang primär über entsprechende vertragliche Rahmenwerke der Grid-Verbünde geregelt, die auch die Ausgangsbasis für die technische Umsetzung durch das Datenschutz-Security-Framework bilden. Für LRZ-seitig lokal erfasste Benutzer gelten die entsprechenden Punkte der LRZ-Benutzungsrichtlinien. In beiden Fällen wird sichergestellt, dass Benutzer der Weitergabe ihrer personenbezogenen Daten im für den Dienstbetrieb erforderlichen Umfang explizit zustimmen müssen.

5. Im Rahmen der Sicherheitsdienstklasse **VO-Management** werden die folgenden Dienste betrachtet:

   - Die Verwaltung von Informationen über *Virtuelle Organisationen* (*virtual organizations*, VOs) spielt im Kontext des SuperMUC-Szenarios keine Rolle, da im Rahmen des Dienstes keine spezifischen VOs existieren.

- Das *Gruppenmanagement* korreliert am LRZ mit der benutzergruppen- bzw. projektspezifischen Autorisierungsverwaltung, die im Rahmen der AAI-Dienste implementiert wird. Dabei ist ein regelmäßiger Abgleich der Informationen über Projektstrukturen in den Grid-Umgebungen und in der LRZ-Benutzerverwaltung erforderlich, der jedoch bereits für frühere HPC-Dienste im Rahmen des Identity Management implementiert wurde und unverändert übernommen werden kann.

6. Die **Sicherheitsmanagement-Basisdienste** umfassen das Auditing, das Logging sowie die Behandlung von Sicherheitsalarmen:

   - Unter *Auditing* wird im Frameworkkonzept ein Prozess, der z. B. im Rahmen einer Zertifizierung von Externen durchgeführt wird, verstanden. Im SuperMUC-Szenario findet zwar eine Abstimmung der Sicherheitskonzepte – sowohl LRZ-intern im Rahmen des Sicherheitsarbeitskreises als auch z. B. GCS-weit – statt, eine Zertifizierung, z. B. durch den TÜV-Süd nach ISO/IEC 27001, ist derzeit jedoch nicht geplant. Der Aufwand für eine entsprechende Zertifizierung erscheint einerseits durch die Notwendigkeit zur Rezertifizierung bei Änderungen bzw. Weiterentwicklungen am Dienst bzw. im gesamten LRZ in Relation zur Betriebszeit des SuperMUC-Dienstes von 5–6 Jahren zu hoch; andererseits kann es als praktisch ausreichend gelten, die im wissenschaftlichen HPC-Umfeld bekannten Sicherheitsanforderungen überdurchschnittlich umzusetzen.
   - Für das *Logging* wird ein zentraler, von allen SuperMUC-Komponenten genutzter Logging-Server vorgesehen. Zudem ist am LRZ ein vom Sicherheitsarbeitskreis angestoßenes Parallelprojekt in Arbeit, das sich mit der LRZ-weiten Vereinheitlichung von Protokollierung und Protokollauswertung befasst. Eine Integration in die hausweite Lösung kann auf Basis einer hierarchischen Struktur, bei der dienstspezifische Logging-Server ausgewählte Informationen an eine zentrale Stelle propagieren, umgesetzt werden.
   - Auch bezüglich der *Sicherheitsalarme* kann auf bereits vorhandene zentrale Lösungen zurückgegriffen werden. Dabei müssen die von der Grid-Middleware und den SuperMUC-Komponenten erzeugten Alarmmeldungen an das zentrale SIEM-System weitergeleitet werden.

7. Im Rahmen von **Sandboxing und Virtualisierung** wird angestrebt, eine möglichst weitreichende Abschottung der von Benutzern in Form von HPC-Jobs gestarteten Programme gegenüber dem Betriebssystem und den Prozessen und Dateien der anderen Anwender zu erzielen, wobei die Sicherheitsfunktionalität der dafür eingesetzten Mechanismen über die vom Betriebssystem regulär angebotenen Mechanismen hinausgeht. Im Frameworkkonzept wird jedoch dokumentiert, dass die dafür derzeit zur Verfügung stehenden technischen Lösungen einerseits die erreichbare Performanz deutlich beeinträchtigen und andererseits den manuellen Administrationsaufwand aufgrund mangelnder Automatisierung erhöhen. Aus diesen Gründen wird beim SuperMUC auf zusätzliche Sandboxing- und Virtualisierungsmaßnahmen verzichtet.

   Es ist anzumerken, dass für Teilaspekte dieser Problematik inzwischen Lösungen, die in die Grid-Middleware integriert sind, geschaffen wurden; diese richten beispielsweise abgeschottete Umgebungen für dynamisch angelegte Grid-Kennungen ein, die zu Testzwecken über Self-Service-Web-Frontends an Grid-interessierte, nicht zuverlässig iden-

tifizierte und authentifizierte Benutzer vergeben werden. Da dieser Anwendungsfall auf den SuperMUC-Dienst nicht zutrifft und für andere Grid-Benutzer die o. g. Einschränkungen gelten, wird dieser Lösungsansatz im Rahmen des Anwendungsbeispiels nicht weiter verfolgt.

8. Schließlich befasst sich die Dienstklasse **Gefahrenabwehr** mit dem *Firewall-Traversal*: Über eine Kopplung der LRZ-Benutzerverwaltung mit den Firewallkomponenten, die auch den Zugriff auf die SuperMUC-Login-Nodes regeln, wird erreicht, dass Benutzer die IP-Adressen bzw. Subnetze, von denen aus sie sich auf dem SuperMUC einloggen möchten, registrieren müssen. Durch den Einsatz der Grid-Middleware Globus bedingt ist zudem nur eine statische Firewall-Konfiguration erforderlich, so dass auf aufwendigere Verfahren zum dynamischen Freischalten von TCP- bzw. UDP-Ports verzichtet werden kann. Somit kann eine relativ einfache Lösung auf Basis der bereits vorhandenen Komponenten geschaffen werden, die im Szenario keine signifikanten Nachteile gegenüber dynamischen Verfahren wie dem Hole-Punching und dem Cooperative On-Demand Opening hat.

Mit Ausnahme der Sicherheitsdienstklasse *Sandboxing und Virtualisierung*, die im Beispielszenario nicht umgesetzt werden kann, können somit alle vom Security-Framework vorgesehenen Sicherheitsdienste durch Anpassungen und Ergänzungen von Komponenten, die am LRZ bereits u. a. für frühere HPC-Dienste eingesetzt wurden, realisiert werden.

8.5.2.2. Customizing-Ergebnisse des security framework for privacy-enhancing data access and usage control

Datenschutzklauseln, die regeln, welche personenbezogenen Daten ein Benutzer einem IT-Dienstleister zu welchen Zwecken zur Verfügung stellen muss, um einen IT-Dienst im gewünschten Umfang nutzen zu können, sind derzeit meist Passagen von allgemeinen Geschäftsbedingungen bzw. Benutzungsrichtlinien oder anderweitig verbindlicher Vertragsbestandteil. Der Dienstleister legt die entsprechenden Inhalte somit nach eigenem Ermessen fest und dem Anwender steht es frei, den Dienst unter diesen Randbedingungen zu nutzen oder darauf zu verzichten. Einer der zentralen Aspekte der europäischen Datenschutzgesetzgebung ist die Zweckbindung, die besagt, dass personenbezogene Daten ausschließlich zu denjenigen Zwecken genutzt werden dürfen, für die sie ursprünglich erfasst wurden; die Erfassung selbst setzt das Einverständnis des Betroffenen oder eine anderweitige gesetzliche Grundlage voraus.

Herkömmliche Zugriffskontrollkonzepte, wie sie auch von Betriebssystemen für Dateisysteme umgesetzt werden, unterscheiden zwar Subjekte (Benutzer), Objekte (Dateien) und die Art des Zugriffs (z. B. lesend bzw. schreibend), berücksichtigen aber den Zweck des Zugriffs nicht. Somit fehlen technische Mechanismen, um die Zweckbindung sicherzustellen bzw. den Missbrauch personenbezogener Daten zuverlässig und nachweisbar zu verhindern. Mit der Einführung von Privacy-Managementsystemen, die beispielsweise die von IBM entwickelte und beim W3C eingereichte Enterprise Privacy Authorization Language (EPAL, [EPALW3]) implementieren, wird die Zugriffskontrollschicht in Anwendungen und Betriebssystemen dahingehend erweitert, dass auch der Zugriffszweck bei versuchtem Lesen bzw. Schreiben von personenbezogenen Daten erfasst, ausgewertet und der Vorgang ggf. unterbunden wird. Damit kann beispielsweise erreicht werden, dass die E-Mail-Adresse eines Benutzers für die elektronische Übermittlung einer Rechnung genutzt wird, gleichzeitig aber nicht für den Versand

von Newslettern bzw. Werbung verwendet werden kann, sofern der Betroffene dem nicht explizit zugestimmt hat. Die von derartigen Lösungen vorgesehenen Abläufe sind jedoch rein dienstleisterintern, so dass der Benutzer höchstens indirekt darauf Einfluss nehmen kann.

Das *security framework for privacy-enhancing data access and usage control*, das im Folgenden vereinfachend als Datenschutz-Security-Framework bezeichnet wird, erweitert speziell im HPC- und Grid-Umfeld vorhandene Access-Control-Konzepte und bietet dabei die folgende, in ihrer Gesamtheit neue Sicherheitsfunktionalität:

- Benutzer können die Zweckbindung der über sie erfassten Daten in der Granularität einzelner Datenfelder (z. B. E-Mail-Adresse) über ein Self-Service-Webportal selbst steuern.
- Benutzerspezifizierte Policies zur Zweckbindung können mit betreiberseitigen Vorgaben und z. B. Grid-weiten Regelungen kombiniert werden; für zueinander widersprüchliche Policies sind verschiedene Ansätze zur Konfliktbeseitigung vorgesehen.
- Neben Einstellungen für die personenbezogenen Daten des Benutzers selbst können auch entsprechende Zugriffsregeln für die von ihm eingebrachten HPC- bzw. Grid-Jobs konfiguriert werden. Dabei wird in beliebiger Granularität vorgegangen, d. h. es wird im Allgemeinen nach Programmcode, Eingabedaten und Ausgabedaten differenziert, mehrere zusammenhängende Jobs können zu Projekten zusammengefasst werden usw.; darüber kann beispielsweise geregelt werden, dass der Dienstleister keine Backups der Eingabedateien von HPC-Jobs erstellen darf, beispielsweise wenn es sich um medizinische Forschungsdaten mit Patienteninformationen handelt.
- Dienstleisterseitig werden so genannte Obligationen unterstützt; dabei handelt es sich um einen flexiblen Mechanismus, der bestimmte Aktionen anstößt, wenn entsprechende Ereignisse eintreten. Beispielsweise können die Eingabedaten für einen HPC-Job unmittelbar nach seiner Fertigstellung gelöscht werden.
- Benutzer haben die Möglichkeit zur Selbstauskunft, d. h. sich mittels eines Webportals über die dienstleisterseitigen Zugriffe auf ihre Daten zu informieren.

Eine ausführliche Darstellung der vollständigen Sicherheitsfunktionalität und ihrer jeweiligen Motivation findet sich in [Homm11].

Das Datenschutz-Security-Framework umfasst in mehreren Stufen ausbaubare Referenzarchitekturen sowohl für die Dienstleister (Service-Provider) als auch für die Heimatorganisationen der Benutzer (Identity-Provider), die insbesondere bei Grid-Projekten die Rolle vertrauenswürdiger Datenquellen für Benutzerinformationen darstellen. Das Security-Framework differenziert dabei zwischen den beiden Phasen der Datenübertragung und der Datennutzung: In der Datenübertragungsphase (*initial data access phase*) wird der Benutzer bei der Auswahl von Service-Providern unterstützt, welche die von ihm gewünschten Randbedingungen bezüglich der Daten-Zweckbindung akzeptieren. Die nachfolgende Nutzungssteuerungsphase (*data usage control phase*) stellt die Zweckbindung bei Service-Provider-internen Datenzugriffen sicher und gewährt dem Benutzer Einblick in entsprechende Protokolldateien.

Für das LRZ sind prinzipiell beide Referenzarchitekturen relevant, da es sowohl als HPC- bzw. Grid-Service-Provider auftritt als auch die Rolle des Identity-Providers für Wissenschaftler aus dem Münchner Raum, die HPC-Ressourcen bei anderen Anbietern nutzen wollen, einnimmt. Für das SuperMUC-Szenario wird nachfolgend jedoch nur Service-Provider-Teil des Security-Frameworks betrachtet. Abbildung 8.5 zeigt die entsprechende Referenzarchitektur;

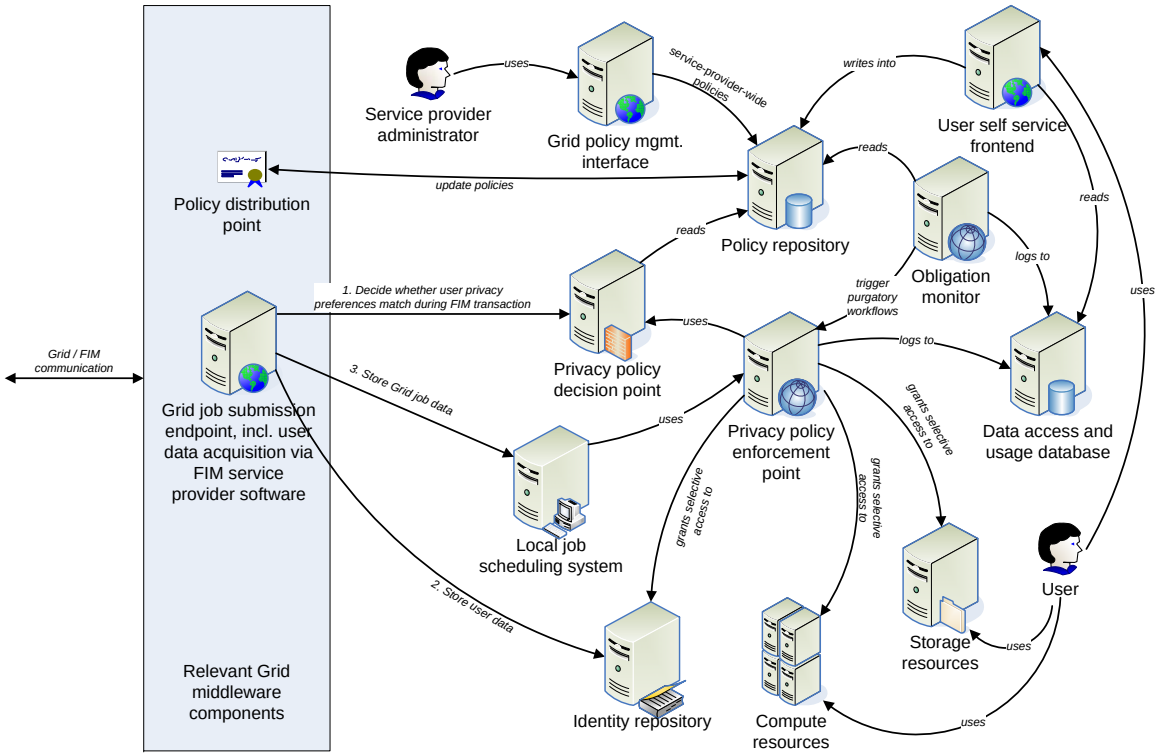


Abbildung 8.5.: Referenzarchitektur des Datenschutz-Security-Frameworks für Service-Provider

sie besteht aus den folgenden Komponenten, die wie jeweils angegeben in das Anwendungsbeispiel zu integrieren sind:

- Grundlegende Informationen über einen Benutzer, die zum Anlegen einer lokalen Kennung erforderlich sind, werden per Federated Identity Management (FIM) vom Identity-Provider des Benutzers zur *FIM Service Provider Software* übertragen. Über FIM-Protokolle wird dabei sichergestellt, dass der Benutzer mit der Weitergabe seiner personenbezogenen Daten zu diesem Zweck einverstanden ist (vgl. [Homm07]). Die übertragenen Daten werden dienstleisterseitig im *Identity Repository* gespeichert. Im SuperMUC-Szenario sind diese beiden Komponenten bereits vorhanden: Das Identity-Repository ist Bestandteil des I&AM-Systems und der FIM-Service-Provider wird auf Basis der Open-Source-Software Shibboleth betrieben, die auch zusammen mit der genutzten Grid-Middleware verwendet werden kann.
- Bei jedem organisationsinternen Zugriff auf Daten, für die eine Zweckbindung vereinbart wurde, kommt ein Privacy-PEP zum Einsatz, der komplementär zur herkömmlichen Autorisierung auf Basis der Lese- und Schreibberechtigungen des Zugreifenden auch den Zweck des Zugriffs auswertet und den Vorgang bei einem Verstoß gegen die Zweckbindung abbrechen kann. Die PEP-Rolle muss von einem System übernommen werden, das der Zugreifende nicht umgehen kann, d. h. die entsprechende Funktionalität muss entweder in jeder Anwendung, mit der auf die Daten zugegriffen werden kann, oder z. B. vom

Betriebssystem oder Fileserver unterstützt bzw. in Form eines zwingend zu nutzenden Gateways realisiert werden. Im SuperMUC-Szenario muss beispielsweise sichergestellt werden, dass auch die Zugriffe des Job-Scheduling-Systems und der Backup-Prozesse kontrolliert werden. Zur technischen Umsetzung kommt dabei wie in Abschnitt 8.5.2.3 beschrieben das dritte hier betrachtete Security-Framework zum Einsatz.

- Der PEP trifft die Entscheidung über die Zulässigkeit des Datenzugriffs nicht selbst, sondern wendet sich dafür an einen dedizierten *Privacy Policy Decision Point* (PDP). Dieser wertet zum einen die in einem Policy-Repository gespeicherten Zweckbindungen aus, die dem Frameworkkonzept gemäß in der Policysprache XACML formuliert werden. Policies können dabei über weitere vom Security-Framework konzipierte Komponenten entweder von den lokalen Administratoren eingetragen, von Benutzern selbst spezifiziert und mittels FIM-Protokollen übertragen oder beispielsweise von einem Grid-verbundweiten Policy-Distribution-Point übernommen werden. Zum anderen wird jeder Zugriffsversuch zusammen mit der vom PDP getroffenen Entscheidung in einer *Data Access and Usage Database* protokolliert. Im SuperMUC-Szenario wird somit ein XACML PDP als neue Komponente benötigt, wohingegen für das Policy-Repository der schon vorhandene Datenbankdienst und für das Datenzugriffsprotokoll der Logging-Server genutzt werden.

- Über den *Data Usage Control Self Service* kann jeder Benutzer im Sinne einer Selbstauskunft lesend auf die ihn betreffenden Einträge aus dem Datenzugriffsprotokoll zugreifen. Diese Funktionalität soll für das Anwendungsbeispiel vereinfachend in den SuperMUC-spezifischen Webserver integriert werden; falls das Datenschutz-Security-Framework später auch für weitere Dienste eingesetzt werden soll, wird eine Verlagerung der Funktionalität z. B. in ein dediziertes Webfrontend erforderlich.

- Schließlich prüft der *Obligation Monitor* (OM) regelmäßig oder durch den Dienst – im Anwendungsbeispiel u. a. durch den Job-Scheduler – angestoßen, ob zur Erfüllung spezifizierter Obligationen Aktionen wie das Löschen von Dateien durchgeführt werden müssen. Die Umsetzung entsprechender Obligationen wird vom OM ebenfalls protokolliert, damit sich der Benutzer darüber informieren kann. Für die OM-Implementierung sind szenarienspezifische Anpassungen erforderlich, damit zum einen der OM genau die im Szenario relevanten Obligationen unterstützt und zum anderen die von ihm angestoßenen Aktionen von den SuperMUC-Komponenten zuverlässig erledigt werden.

Das Konzept des Security-Frameworks sieht vor, dass nicht alle Komponenten gleichzeitig in Betrieb genommen werden müssen. Somit bietet es sich an, zunächst das Policy-Repository sowie den PDP und den PEP zu implementieren, um damit die Grundfunktionalität zur Verfügung zu stellen, mit der die bislang bereits in Richtlinien in natürlicher Sprache formulierten Zweckbindungen technisch umgesetzt werden können. Dies soll im Anwendungsbeispiel bereits für die SuperMUC-Betriebsphase 0 erreicht werden. Im nächsten Schritt sollen für die Betriebsphase 1 die Selbstauskunft und der OM realisiert werden. Erst später, beispielsweise mit dem Eintritt in die SuperMUC-Betriebsphase 2, soll auch der automatisierte Policyaustausch mit anderen Service- und Identity-Providern unterstützt werden, da die Partnereinrichtungen für diesen Zweck ebenfalls erst noch entsprechende Komponenten bereitstellen müssen.

8.5.2.3. Customizing-Ergebnisse des Linux-Kernel-Security-Frameworks

Das Security-Framework für den Kernel des Betriebssystem Linux wurde bereits auf Seite 192 vorgestellt und mit Bezug auf den Anforderungskatalog analysiert. Es bietet die Möglichkeit, die vom Kernel den einzelnen Funktionsbibliotheken bzw. Programmen im User-Space zur Verfügung gestellten Betriebssystemfunktionen über versionsübergreifend stabile Schnittstellen (Hooks) modular zu erweitern und deckt dabei die Bereiche Prozessmanagement, Programmausführung, Interprozesskommunikation, Dateisysteme und Netzzugriffe ab.

Das Security-Framework bietet somit die Möglichkeit, szenarienspezifische Systemhärtungskonzepte direkt in den Betriebssystemkern integrieren zu können. Da Maßnahmen zur Härtung des SuperMUC-Systems wie in Abschnitt 8.2 beschrieben zu den vom LRZ an den Systemhersteller delegierten Aufgaben gehören und im Anwendungsbeispiel nicht im Detail betrachtet werden, wird die Beschreibung der Anwendung des Security-Frameworks im Folgenden auf den Aspekt Filesystem-Hooks (vgl. [WCS+02, Abs. 4.5]) beschränkt. Über diese Schnittstelle können lesende und schreibende Zugriffe auf Verzeichnisse und Dateien abgefangen, geprüft und ggf. unterbunden werden.

Diese Sicherheitsfunktionalität wird im SuperMUC-Szenario im Zusammenspiel mit dem Datenschutz-Security-Framework benötigt, um die Zweckbindung der von Benutzern auf dem SuperMUC bzw. seinen Dateisystemen gespeicherten Daten zu überprüfen. Im Speziellen soll dabei als Einstieg in die Nutzung der vom Datenschutz-Security-Framework ermöglichten Funktionalität sichergestellt werden, dass sowohl der Systemprozess zur Erstellung von Backups als auch SSH-basierte Zugriffe von LRZ-Administratoren auf Benutzerdateien nur dann zugelassen werden, wenn diese von den Benutzern explizit genehmigt wurden, d. h. eine entsprechende benutzerindividuelle Policy vorhanden ist. Damit soll ein wesentlicher Beitrag zur Sicherstellung der Vertraulichkeit von Benutzerdaten (vgl. Abschnitt 8.5.2.1) geleistet werden, bei dem jedoch berücksichtigt werden muss, dass er bei Weitem nicht alle Angriffsvarianten abdecken kann; trotz eines solchen im Betriebssystem verankerten Schutzes könnten die LRZ-Administratoren beispielsweise physisch auf die Festplatten zugreifen oder ihre Privilegien missbrauchen, um diesen Schutz wieder zu entfernen. Zur Erkennung eines solchen Missbrauchs sind somit weitere Maßnahmen erforderlich, die vereinfachend darauf reduziert werden, dass der Ausbau von Festplatten und das Entfernen von Kernelmodulen mit Sicherheitsalarmen verbunden wird, die vom LRZ-Sicherheitsteam und nicht von den SuperMUC-Administratoren auszuwerten sind.

Die technische Umsetzung der Zweckbindungsprüfung wird dadurch erschwert, dass das für den SuperMUC verwendete Dateisystem wie unter Linux- und UNIX-Systemen allgemein üblich zwar dateieigentümer- und gruppenbasierte Zugriffssteuerungskonzepte unterstützt, bei Lese- und Schreibvorgängen jedoch den Zweck des Zugriffs nicht betrachtet. Eine Erweiterung der vom Betriebssystem gebotenen Dateioperationen um die Angabe eines Zugriffszwecks wäre nicht praktikabel, da neben dem Betriebssystemkern selbst auch alle Anwendungen dahingehend erweitert werden müssten, dass sie den Zweck kennen und an den Kernel durchreichen; da unter anderem für das Backupsystem proprietäre Software zum Einsatz kommt, an der keine entsprechenden Änderungen vorgenommen werden können, muss eine pragmatische Alternative implementiert werden. Das Security-Framework soll deshalb wie folgt vereinfacht ab der SuperMUC-Betriebsphase 1 eingesetzt werden:

- Über einen Filesystem-Hook werden alle lesenden und schreibenden Zugriffe abgefangen,

aber nur diejenigen näher betrachtet, die sich auf benutzerspezifische Dateien und nicht beispielsweise auf Systemdateien beziehen; diese können anhand der Dateisystempfade für die Home-Directories bzw. Projektarbeitsverzeichnisse der Benutzer einfach identifiziert werden.

- Sofern der Zugriff vom Prozess der Backup-Software ausgeht, wird vereinfachend angenommen, dass der Zweck eines lesenden Zugriffs die Erstellung des Backups und der Zweck eines schreibenden Zugriffs die Wiederherstellung gesicherter Dateien ist.

- Sofern der Zugriff unter einer administrativen Benutzerkennung erfolgt und es sich dabei um einen Prozess handelt, der in der systemweiten Prozesshierarchie unterhalb des (Grid)SSH-Serverprozesses angesiedelt ist, wird als Verwendungszweck die Benutzerunterstützung durch LRZ-Administratoren angenommen.

- Falls einer dieser beiden Zugriffszwecke identifiziert wurde, fungiert das hier beschriebene Kernelmodul als PEP für das Datenschutz-Security-Framework und wendet sich wie in Abschnitt 8.5.2.2 beschrieben an den Privacy-PDP. Falls dieser die Entscheidung liefert, dass der Zugriff nicht zugelassen werden soll, bricht das Kernelmodul den Zugriff auf das Dateisystem ab.

Es muss berücksichtigt werden, dass diese pauschale Annahme von Zugriffszwecken Risiken birgt, die damit vergleichbar sind, dass ein Benutzer, der den Zugriffszweck manuell eintragen muss, absichtlich falsche Angaben macht. Den präventiven Eigenschaften des Linux-Security-Frameworks sind somit technische Grenzen gesetzt, die wiederum durch Detektionsmechanismen, die auf der Protokollierung der Zugriffsentscheidungen durch den PDP des Datenschutz-Security-Frameworks aufbauen, unterstützt werden. Letztlich muss jedoch eine Kontrollinstanz entscheiden, ob die technisch zugelassenen Zugriffe in der Tat legitim waren; dies kann entweder manuell erfolgen oder durch den Abgleich der Zugriffszeitpunkte z. B. mit den Zeiträumen, in denen Anfragen bzw. Störungsmeldungen des betroffenen Benutzers bearbeitet wurden, zumindest partiell automatisiert werden.

Abbildung 8.6 zeigt die insgesamt resultierende SuperMUC-Gesamtarchitektur unter Berücksichtigung der aufgrund der drei szenarienspezifisch angepassten Security-Frameworks zusätzlich erforderlichen Komponenten. Für jede Komponente ist zudem eingezeichnet, im Abdeckungsbereich welchen Security-Frameworks sie sich befindet und zu welcher SuperMUC-Betriebsphase die beschriebene Sicherheitsfunktionalität erreicht werden soll. Dabei verweist der Buchstabe A auf das Framework für föderiertes Sicherheitsmanagement, B auf das Datenschutz-Security-Framework und C auf das Linux-Kernel-Security-Framework. Die Ziffern 0, 1 und 2 beziehen sich auf die in Abschnitt 8.1 erläuterten SuperMUC-Betriebsphasen. Nicht explizit von Security-Frameworks abgedeckte LRZ-Systeme wie die Load-Balancer und Managementserver unterliegen den dafür üblichen anderen am LRZ eingesetzten Sicherheitsmaßnahmen, die hier nicht näher betrachtet werden.

Nach dieser Betrachtung der technischen Aspekte des Einsatzes der Security-Frameworks in der Customizingphase werden nachfolgend die prozessualen Auswirkungen erarbeitet; die für die Implementierung und die weiteren Lebenszyklusphasen relevanten Aspekte sind daran anschließend Gegenstand von Abschnitt 8.6.

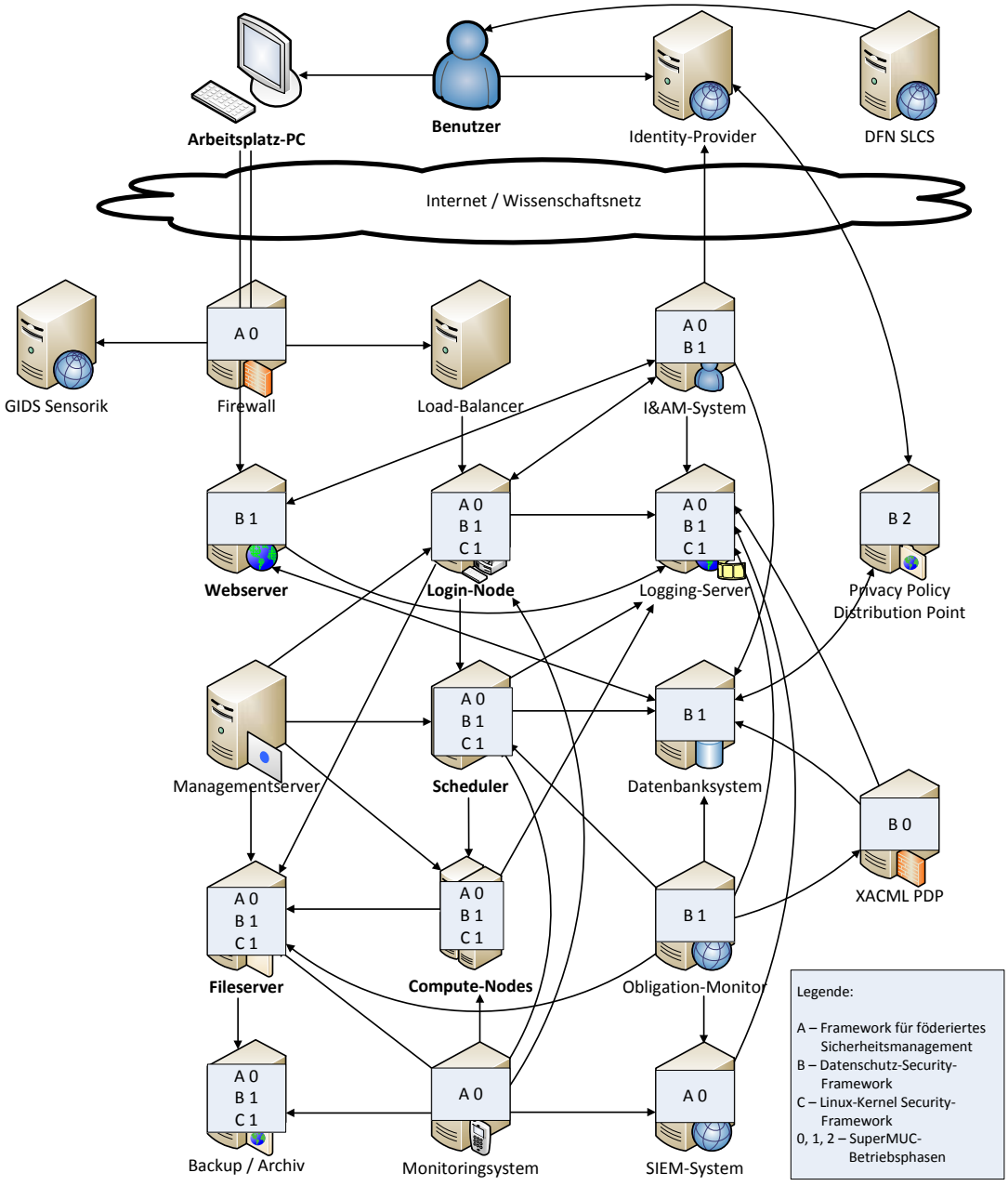


Abbildung 8.6.: SuperMUC- und Security-Framework-Komponenten nach dem Customizing

8.6. Spezifikation der Managementprozesse im SuperMUC-Szenario

Wie bereits einleitend in Abschnitt 8.1 dargelegt wurde, laufen am LRZ parallel zur SuperMUC-Einführung mehrjährige Projekte zur Verbesserung des IT Service Management auf Basis der Referenzprozesse nach ISO/IEC 20000 sowie zur Ausrichtung des Sicherheits-

managements an ISO/IEC 27001. In beiden Bereichen werden die jeweiligen Prozesse und Abläufe im Rahmen entsprechender Teilprojekte zeitversetzt eingeführt, woraus sich auch unterschiedliche Prozessreifegrade ergeben, die im Zusammenspiel mit vorhandenen und neu im Aufbau befindlichen Diensten berücksichtigt werden müssen.

Eine vollständige und detaillierte Betrachtung aller LRZ-Prozesse wäre für das Anwendungsbeispiel nicht zielführend und würde den Rahmen dieser Arbeit sprengen. Aus diesem Grund wird nachfolgend nach ITSM- und Sicherheitsmanagementprozessen getrennt nur auf die für den Einsatz von Security-Frameworks im SuperMUC-Szenario wichtigsten Auswirkungen eingegangen. Zudem werden im Rahmen der entsprechenden Prozesse auch die Möglichkeiten zum Einsatz der beiden Werkzeuge zur dynamischen Reparametrisierung von Detektionssensorik und zur Erfassung bzw. Aufbereitung von Sicherheitskennzahlen erläutert.

8.6.1. IT-Service-Management-Prozesse im SuperMUC-Szenario

Die LRZ-seitigen Arbeiten an der Einführung standardorientierter ITSM-Prozesse sollen in einer Organisationszertifizierung nach ISO/IEC 20000 münden. Durch ITIL v2 als gemeinsame Basis für ISO/IEC 20000 und ITIL v3 lassen sich die in dieser Arbeit, auf ITIL v3 basierenden Konzepte jedoch einfach auf die Prozesslandschaft am LRZ übertragen.

Nachfolgend werden ausschließlich die für den laufenden Betrieb relevanten ITSM-Prozesse betrachtet; somit wird beispielsweise auf die Einbettung von HPC-Dienstleistungen in die Servicestrategie bzw. das Dienstportfolio des LRZ nicht weiter eingegangen.

8.6.1.1. Incident Management im SuperMUC-Szenario

Das Incident Management, bei dem neben der Beseitigung erkannter bzw. gemeldeter Störungen für HPC-Dienste das Request Fulfillment, also beispielsweise die Bereitstellung der von Benutzern benötigten Software und Programmierbibliotheken, im Vordergrund steht, gehört zu den im Rahmen des ISO/IEC 20000-Projekts als erstes eingeführten Prozessen. Es wurde bereits für das SuperMUC-Vorgängersystem erfolgreich praktiziert, erfordert jedoch einige Anpassungen an den neuen Dienst, die parallel laufende Weiterentwicklung der Sicherheitsmanagementprozesse und den Einsatz von Security-Frameworks.

Zunächst ist festzuhalten, dass der SuperMUC aus Perspektive des Incident Management nur einen von vielen Diensten im LRZ-Portfolio darstellt. Trotz einer dienstspezifischen Parametrisierung, die beispielsweise die Eskalation von Störungsmeldungen bzw. Incident Tickets an den SuperMUC-Hersteller oder weitere externe Dienstleister realisiert, bleiben die prinzipiellen Abläufe unverändert erhalten: Neben den eingesetzten Monitoringsystemen und Managementplattformen, auf die bei den anderen Prozessen noch näher eingegangen wird, können Störungsmeldungen und Anfragen von Benutzern über einen webbasierten Self-Service, telephonisch oder per E-Mail eingehen. Alle Incidents werden über ein zentrales, prozessübergreifend eingesetztes ITSM-Werkzeug, bei dem es sich um ein aufwendig an die LRZ-Bedürfnisse angepasstes kommerzielles Softwarepaket handelt, verwaltet. Bei HPC-Diensten gehen erfahrungsgemäß überwiegend Benutzeranfragen ein, deren Bearbeitung spezifisches Fachwissen erfordert, so dass die Erstlösungsrate, d. h. der Prozentsatz der vom Service-Desk-Personal, das den First-Level-Support übernimmt, geringer als bei anderen Diensten ist. Die meisten

Incident Tickets werden vom so genannten Dispatcher deshalb einem zur Anfrage passenden Mitarbeiter im Second-Level-Support, oftmals also einem der LRZ-seitigen SuperMUC-Administratoren, zugewiesen. Dieser ist für die gegebenenfalls erforderliche Eskalation des Incidents an Dritte wie den SuperMUC-Hersteller verantwortlich.

Bezogen auf den Schwerpunkt dieses Anwendungsbeispiels ist das Incident Management am LRZ primär unter folgenden Aspekten relevant:

- Das Incident Management ist eng mit dem in Abschnitt 8.6.2.7 vertieften Security-Incident-Response-Prozess (SIR-Prozess) verzahnt. Insbesondere muss bei der manuellen Auswertung von Benutzermeldungen geprüft werden, ob ein vom SIR-Prozess zu bearbeitender Vorfall vorliegt.
- Von Monitoringsystemen automatisiert eingebrachte Incidents umfassen auch Störungen von Security-Framework-Komponenten bzw. weiteren Sicherheitsmechanismen; falls beispielsweise ein IDS-Sensor ausfällt oder eine sicherheitsspezifische Kennzahl über einen längeren Zeitraum hinweg nicht erfasst werden kann, muss dieser Sachverhalt im Rahmen des Incident Management näher untersucht werden.
- Störungen müssen zum Teil organisationsübergreifend bearbeitet werden, beispielsweise wenn Benutzer Schwierigkeiten mit der Einrichtung von Grid-Jobs berichten oder dedizierte Netzverbindungen zwischen HPC-Sites Hardwaredefekte aufweisen.

Am LRZ wurde bislang noch kein Problem-Management-Prozess explizit eingeführt, so dass dessen Teilaspekte wie die Pflege einer Known-Error-Database ebenfalls zu den Aufgaben des Incident Management gehört.

8.6.1.2. Configuration Management im SuperMUC-Szenario

Durch seine große Zahl an Einzelkomponenten, die insbesondere durch die Compute-Nodes zustande kommt, stellt SuperMUC einen für heutige Verhältnisse äußerst komplexen Dienst mit einer Vielzahl von Abhängigkeiten dar, die andere LRZ-Dienste bei Weitem übertrifft. Eine zur Handhabung der anderen LRZ-Server analoge Aufnahme aller SuperMUC-Nodes als Configuration Items (CIs) in eine zentrale CMDB würde die bereits vorhandenen ITSM-Werkzeuge überfrachten, so dass zwangsweise ein für SuperMUC spezifisches Configuration Management ausgeprägt werden muss, das geeignete Schnittstellen zum organisationsweiten Prozess aufweist.

Um die zentralen Configuration-Management-Werkzeuge auch für den SuperMUC-Dienst nutzen zu können, werden die SuperMUC-Komponenten dort nur in aggregierter Form, d. h. nach Compute-Islands und Storage-Komponenten getrennt, verwaltet. Dadurch bleiben die Anzahl der CIs überschaubar und der Detaillierungsgrad ausreichend, um beispielsweise Störungsmeldungen grob zuordnen zu können. Für die Verwaltung der einzelnen Nodes und ihrer Hardwarekomponenten bis hin zu Netzteilen und Lüftern werden hingegen SuperMUC-spezifische Managementsysteme eingesetzt; diese bieten den z. B. für die logische wie auch physische Lokalisierung auszutauschender defekter Hardwarekomponenten erforderlichen Informationsdetailgrad und werden z. B. vom Second-Level-Support bei der Bearbeitung von Störungsmeldungen genutzt. Zwischen diesen beiden allgemein für ITSM genutzten bzw. SuperMUC-spezifischen Systemen muss ein regelmäßiger Datenabgleich stattfinden; da sich die Hardwareausstattung des Systems nur bei den Betriebsphasenübergängen ändert, sind bei

der Datensynchronisation vorrangig der Betriebsstatus und Informationen über den aktuellen Softwarestand zu betrachten.

Im Unterschied zu den SuperMUC-Hardwarekomponenten sind die eingesetzten Security-Framework-Komponenten überschaubar, so dass sie wie andere Sicherheitsmechanismen auch regulär über das Configuration Management verwaltet werden. Das für CIs am LRZ verwendete Datenmodell sieht die Speicherung des Soll-Zustands vor, so dass der Einsatz von Prüfwerkzeugen möglich ist, um auf Basis dieses Datenbestands einen Soll-Ist-Abgleich durchführen zu können. Aufgrund der dem Anwendungsszenario zugrunde liegenden Autarkie jeder an den betrachteten Verbünden beteiligten Organisation ergibt sich der Vorteil, dass nur vor größeren Konfigurationsänderungen, die direkte Auswirkungen auf die Partnerorganisationen bzw. deren Benutzer haben, Absprachen erforderlich werden. In den meisten Fällen handelt es sich dabei um Routineänderungen wie den Austausch von Serverzertifikaten und das Freischalten einzelner Maschinen und Subnetze in den eingesetzten Firewalls, die zuvor den nachfolgend beschriebenen Change-Management-Prozess durchlaufen haben.

8.6.1.3. Change Management im SuperMUC-Szenario

Durch die Verteilung der Betriebsverantwortung auf LRZ-internes und vom Systemhersteller abgeordnetes Personal ergeben sich Unterschiede im Change Management des SuperMUC gegenüber anderen LRZ-Diensten, die jedoch auf die Kernkonfiguration des SuperMUC-Dienstes beschränkt sind und sich nicht auf die anderen Infrastrukturkomponenten wie beispielsweise den Netzzugang und die netzbasierten Sicherheitsmechanismen wie Firewalls auswirken.

Das SuperMUC-spezifische Change Management behandelt im Allgemeinen viele kleine Änderungen an der Dienstkonfiguration wie das Einspielen aktualisierter Softwarepakete, auf die separat unten im Rahmen des Release und Deployment Management eingegangen wird. Vorrangig zu betrachten sind hier deshalb größere und komplexere Änderungen, die entweder vom SuperMUC-Dienst oder seiner Einbettung in organisationsübergreifende Verbünde ausgehen oder sich unmittelbar auf diese auswirken. Hierzu kann es beispielsweise kommen, wenn sich an den anzubietenden Authentifizierungsverfahren größere Änderungen ergeben; u. a. ist absehbar, dass bis zur SuperMUC-Betriebsphase 2 auch eine X.509v3-zertifikatsbasierte SSH-Authentifizierung unterstützt werden muss. Ferner müssen u. a. auch bezüglich ihrer IT-Sicherheitsimplikationen Parallelprojekte wie die flächendeckende Einführung des IPv6-Protokolls im Münchner Wissenschaftsnetz, die damit verbundene Umstellung auf andere Security-Monitoringwerkzeuge und die Aufrüstung der Netz-Backbone-Infrastruktur auf 40 bzw. 100 Gbit/s-Verbindungen berücksichtigt werden.

Da sich das Change Management am LRZ derzeit generell noch im Aufbau befindet, werden viele Abläufe rund um die Planung, Genehmigung und Durchführung von Änderungen bislang noch abteilungsintern gehandhabt. Für größere, abteilungsübergreifend relevante Änderungen fungiert ein mit den Abteilungsleitern besetztes Gremium als Change Advisory Board; von diesem genehmigte Änderungsanträge werden anschließend wiederum in abteilungsspezifische Prozesse eingebracht, von denen die Planung, die Vorbereitung, das Testen, das Terminieren, das Ankündigen und die Durchführung verantwortet werden.

8.6.1.4. Release und Deployment Management im SuperMUC-Szenario

Da es sich bei den Hardwareerweiterungen an den Übergängen der Betriebsphasen um dedizierte Projekte handelt, sind im Rahmen des Release und Deployment Management hauptsächlich Softwareaktualisierungen zu betrachten. Aufgrund der pro Island dreistelligen Anzahl an Knoten müssen Softwarepakete auf so vielen Maschinen eingespielt werden, dass die herkömmlichen, am LRZ eingesetzten Softwarekonfigurationskonzepte nicht mehr angewandt werden können und somit dedizierte Lösungen erforderlich werden.

Änderungen an der Softwarekonfiguration ergeben sich vorrangig in folgenden Fällen:

- Der Hersteller der eingesetzten Linux-Distribution bietet Softwareaktualisierungen an. Dabei ist einerseits zu unterscheiden, ob nur einzelne Softwarepakete, z. B. auf Basis von Security-Patches, aktualisiert werden müssen, oder ob im Rahmen mehr oder weniger regelmäßig erscheinender Servicepacks sehr viele Softwarekomponenten auf einmal ausgetauscht werden. Andererseits muss auch berücksichtigt werden, ob der Betriebssystemkern oder die anderen Softwarepakete aktualisiert werden. Neue Versionen des Betriebssystemkerns erfordern zum einen ein erneutes Einbringen der szenarienspezifischen Anpassungen des Linux-Kernel-Security-Frameworks und sind zum anderen typischerweise mit einem Neustart des aktualisierten Systems verbunden, so dass es zu temporären Dienstausfällen kommen kann.
- Benutzer beantragen die Bereitstellung zusätzlicher Software bzw. Programmierbibliotheken, die für die Ausführung ihrer Projekte auf dem SuperMUC erforderlich sind.
- Aktualisierte Softwareversionen werden von Dritten bereitgestellt. Neben den im voranstehenden Punkt genannten Softwarepaketen kann es sich dabei beispielsweise auch um neue Versionen der Grid-Middleware handeln, die von anderen Gruppen im LRZ bereitgestellt werden.

Aufgrund zum Teil sehr aufwendiger Anpassungen von Softwarepaketen an die HPC-Umgebung hat sich bereits mit den SuperMUC-Vorgängersystemen das zeitnahe Einspielen von Security-Updates als große Herausforderung erwiesen. Wie unten noch näher erläutert wird, sind Sicherheitskennzahlen bezüglich der Verzögerung beim Einspielen von Softwareaktualisierungen jedoch ein wesentliches Kriterium zur Beurteilung des erreichten Gesamtsicherheitsniveaus.

Im Rahmen des Deployment-Prozesses müssen die technischen Besonderheiten des SuperMUC-Dienstes berücksichtigt werden: Hierzu muss zwischen mit herkömmlichen Linux-Servern vergleichbaren, mit lokalen Festplatten ausgestatteten Komponenten wie den Login-Nodes und so genannten *diskless* Nodes, zu denen alle Compute-Nodes gehören, unterschieden werden. Alle mit Festplatten ausgestatteten Systeme können in der Regel im laufenden Betrieb aktualisiert werden und müssen nur neu gestartet werden, wenn auch der Linux-Kernel einem Update unterzogen wurde. Demgegenüber wird für die festplattenlosen Systeme auf dem SuperMUC-Managementserver ein zentrales Abbild des einzusetzenden Betriebssystems gepflegt, das die Compute-Nodes im Rahmen des Systemstarts über das SuperMUC-interne Netz beziehen und geeignet parametrisieren. Damit verbunden ist jedoch die Einschränkung, dass selbst kleinere Änderungen auf den Compute-Nodes erst dann aktiv werden, wenn sie neu gestartet werden. Ein Neustart darf jedoch im Allgemeinen nur dann erfolgen, wenn auf dem Knoten gerade keine HPC-Jobs ausgeführt werden, um die zum Teil sehr lange und

im Allgemeinen knotenübergreifend ausgeführten Benutzerprojekte nicht zu beeinträchtigen. Zum Deployment gehört somit auch die Planung, welche Knoten z. B. nach Abschluss welcher noch laufenden HPC-Jobs neu gestartet werden sollen, wobei es durch dieses Vorgehen wiederum zu relativ großen Verzögerungen kommen kann, bis Sicherheitsaktualisierungen restlos auf allen Knoten aktiv geworden sind.

8.6.1.5. Availability und Capacity Management im SuperMUC-Szenario

Für die Sicherstellung der möglichst hohen Verfügbarkeit des SuperMUC-Dienstes werden mit anderen LRZ-Diensten vergleichbare Maßnahmen ergriffen. Zum einen ermöglicht es die SuperMUC-Architektur, beispielsweise bei Störungen nur ausgewählte Teile außer Betrieb zu nehmen, ohne dass der Betrieb des Gesamtdienstes darunter in einer für die Anwender erkennbaren Form leidet. Zum anderen werden regelmäßige Wartungsarbeiten eingeplant, die terminlich mit anderen Arbeiten im LRZ abgestimmt werden, so dass die Anzahl an Zeiträumen, in denen der Dienst nicht genutzt werden kann, minimiert wird. Die Hochverfügbarkeit der Sicherheitsmechanismen und Security-Framework-Komponenten wird ebenfalls über Hardwareredundanz gesichert: Alle Sicherheitssysteme, die einen potentiellen Single Point of Failure darstellen, werden von mindestens zwei Maschinen erbracht, für die eine entsprechende Failover-Konfiguration existiert.

Das Kapazitätsmanagement umfasst analog zu den anderen HPC-Diensten des LRZ die folgenden Aspekte:

- Rechenkapazität: Über die zu den Betriebsphasenübergängen vorgesehenen Erweiterungen der CPU-Ressourcen hinausgehend können keine Anpassungen vorgenommen werden; hierzu würde neben dem Budget auch der erforderliche Stellplatz fehlen. Aufgrund der intensiven Nutzung der HPC-Dienste müssen SuperMUC-Anwender folglich mit längeren Wartezeiten rechnen, bevor ihre genehmigten Projekte tatsächlich zur Ausführung kommen. Da die Rechenkapazität nicht erweitert werden kann, wird stattdessen eine bessere Ausnutzung der vorhandenen Kapazität angestrebt, u. a. indem die Anwender bezüglich der Anpassung ihrer Projekte an die SuperMUC-Rechnerarchitektur geschult und unterstützt werden.
- Speicherkapazität: Der für Home-Directories, Backup und Archivierung verfügbare Speicherplatz wird den Bedarfsentwicklungen kontinuierlich angepasst. Zu diesem Zweck wird eine Reihe von Kunden bzw. Anwendervertretern regelmäßig über die aktuelle Platzbelegung informiert und um Rückmeldungen zum in sechs bzw. 18 Monaten erwarteten Bedarf gebeten. Durch Kombination dieser Rückmeldungen mit Erfahrungswerten kann der Umfang der regelmäßig durchgeführten Neubeschaffungen zuverlässig festgelegt werden; bei der Außerbetriebnahme anderer Dienste können bestehende Speicherkapazitäten zudem umgewidmet werden.
- Netzdurchsatz: Die im Rahmen der HPC-Jobs immer mehr und immer aufwendiger zu verarbeitenden Daten müssen zunächst auf den SuperMUC transferiert werden; dafür spielen die Netzanbindung des SuperMUC im Münchner Wissenschaftsnetz und die Integration ins deutsche Forschungsnetz zentrale Rollen. Neben LRZ-internen Maßnahmen, die beispielsweise die hohe Bandbreite beim Zugriff auf die Fileserver und bei der Datenübermittlung an das LRZ-Visualisierungszentrum sicherstellen, wird dabei auch auf dedizierte Netzverbindungen z. B. zu Partnerrechenzentren im Rahmen von PRACE

zurückgegriffen. Da diese dedizierte Netzinfrastruktur nur von als vertrauenswürdig eingestuften Organisationen genutzt wird und beispielsweise kein direkter Zugriff darauf aus dem Internet möglich ist, werden hierfür keine zusätzlichen Sicherheitsmechanismen benötigt.

Auch die Kapazitäten der für den Betrieb sicherheitsrelevanter Systeme erforderlichen Systeme werden kontinuierlich an Änderungen im Anforderungsprofil angepasst. Dadurch kann beispielsweise vermieden werden, dass die Identity-Management-Komponenten durch die wachsende Zahl an Authentifizierungsvorgängen überlastet werden oder IDS-Sensoren nicht mit der Weiterentwicklung bei der Netzbandbreite mithalten können.

8.6.1.6. Service Level und Supplier Management im SuperMUC-Szenario

Mit den LRZ-Kunden und Anwendern des SuperMUC-Dienstes werden wie bei anderen wissenschaftlichen Höchstleistungsrechenzentren auch bislang keine expliziten Service Level Agreements abgeschlossen; vielmehr verpflichtet sich das LRZ im Rahmen seiner Betriebs- und Benutzungsordnung für den SuperMUC selbst, den Dienst bestmöglich zu betreiben und verfolgt somit eine Best-Effort-Strategie. Dabei findet auch keine Bevorzugung z. B. der HPC-Jobs oder Anfragen bestimmter Benutzergruppen statt. Dennoch liegen LRZ-interne Zielsetzungen vor, die zwar nicht Vertragsgegenstand mit den Kunden werden, aber zur Beurteilung des Dienstbetriebs und der Prozessinstanzen herangezogen werden. Beispielsweise sollen Störungsmeldungen, denen eine hohe Priorität zugeordnet wurde, innerhalb von vier Stunden bearbeitet und spätestens nach zwei Arbeitstagen gelöst werden.

Das dem Service Level Management zugeordnete Berichtswesen über die Qualität der erbrachten Dienste erfolgt zweigeteilt: Zum einen haben Benutzer jederzeit über den webbasierten Self-Service Zugriff auf detaillierte Statistiken über ihre eigene SuperMUC-Nutzung. Zum anderen informiert das LRZ u. a. in seinen Jahresberichten über die gesamte Systemnutzung und ggf. eingetretene wichtige Ereignisse.

Weitere Abstimmungen des Dienstangebots auf den Benutzerbedarf werden im Rahmen des SuperMUC-Lenkungsausschusses vorgenommen, zu dessen Aufgaben auch die Genehmigung von Projektanträgen durch potentielle Benutzer gehört. Ihm gehören überwiegend Vertreter von Wissenschaftlern und damit der Zielnutzergruppe an.

Das Supplier Management ist am LRZ noch dezentral organisiert und somit den jeweiligen Abteilungen zugeordnet, die entsprechende Verträge mit Zulieferern und Wartungsfirmen abschließen. Neben dem SuperMUC-Systemhersteller sind dabei auch die vertraglichen Regelungen für Dienste wie das Backup- und Archivsystem sowie die Load-Balancer zu berücksichtigen; diese sehen wiederum feste Obergrenzen für die Reaktion auf und die Bearbeitung von Störungsmeldungen vor, so dass beispielsweise defekte Hardware innerhalb kurzer Zeit ausgetauscht werden kann. In Bezug auf das Sicherheitsmanagement am LRZ stehen dabei zwei Aspekte im Vordergrund:

1. Neu angelieferte und in Betrieb genommene Komponenten müssen bezüglich ihrer Sicherheitseigenschaften optimiert vorkonfiguriert werden (vgl. Paradigma *secure in deployment* in Abschnitt 2.3.2).
2. Für beispielsweise aufgrund von Defekten, Aufrüstungen oder Außerbetriebnahme abgebaute Komponenten, die Speichermedien wie Festplatten oder Bänder enthalten, müssen

datenschutzgesetzkonforme Regelungen zur Vernichtung der darauf gespeicherten Informationen existieren. Dies ist insbesondere bei defekten Speichermedien, die nicht mehr vom LRZ selbst mit üblichen Mitteln überschrieben werden können, und bei größerem logistischem Aufwand, beispielsweise wenn Hunderte von Festplatten einzeln durch Überschreiben gelöscht werden müssten, erforderlich (vgl. auch Abschnitt 8.6.2.3).

Die Einhaltung dieser Vorgaben muss vom LRZ kontinuierlich überwacht werden.

8.6.2. Sicherheitsmanagementprozesse im SuperMUC-Szenario

Die Verantwortung des LRZ für den Betrieb einer vierstelligen Anzahl an eigenen Servern und des gesamten Münchner Wissenschaftsnetzes (MWN) hat dazu geführt, dass viele Aspekte des operativen Sicherheitsmanagements bereits seit Langem stark ausgeprägt sind. Die organisationsweit koordinierte, also gruppen- und abteilungsübergreifende Auseinandersetzung mit Sicherheitsmanagementprozessen ist hingegen analog zur Ausrichtung der ITSM-Prozesse an ISO/IEC 20000 noch vergleichsweise neu. Somit sind die SuperMUC-spezifischen Abläufe nicht nur nahtlos in die bestehenden Prozesse zu integrieren, sondern tragen auch zu deren Überarbeitung und Weiterentwicklung bei.

Im Folgenden werden die Sicherheitsmanagementprozesse im SuperMUC-Szenario nicht wie in Kapitel 6 anhand der Referenzprozesse von ISO/IEC 27001 strukturiert dargestellt, sondern den drei inhaltlichen Schwerpunkten *Prävention*, *Detektion* und *Reaktion* zugeordnet. Für jeden der drei Bereiche werden sowohl die technischen als auch die organisatorischen, SuperMUC-spezifischen Kernideen erläutert. Hierzu gehen wie in Abbildung 8.7 dargestellt die Abschnitte 8.6.2.1 bis 8.6.2.4 zunächst auf die Benutzer- und Berechtigungsverwaltung, das Zutritts- und Zugriffsmanagement für Administratoren, den Themenkomplex Informationsmanagement, weitere ausgewählte Aspekte des operativen Sicherheitsmanagements und damit auf die präventiven Maßnahmen ein. Die Abschnitte 8.6.2.5 und 8.6.2.6 behandeln anschließend mit der Netz- und Systemüberwachung sowie dem Einsatz von dynamischer IDS-Sensorik die Detektionsmechanismen im SuperMUC-Szenario. Die geplante Reaktion auf Sicherheitsvorfälle und die Möglichkeiten zur IT-forensischen Analyse im SuperMUC-Szenario sind Gegenstand der Abschnitte 8.6.2.7 und 8.6.2.8. Schließlich gehen die beiden Abschnitte 8.6.2.9 und 8.6.2.10 auf das Risikomanagement und den Einsatz von Sicherheitskennzahlen im SuperMUC-Szenario und somit auf die kontinuierliche Unterstützung aller anderen Prozesse und Abläufe ein.

8.6.2.1. Identity & Access Management im SuperMUC-Szenario

Der Betrieb von HPC-Diensten, die von Hunderten externer und oftmals nicht persönlich bekannter Benutzer verwendet werden, um beliebigen eigenen Code auf dem HPC-System ausführen zu können, ist mit offensichtlichen IT-Sicherheitsrisiken verbunden. Eine essentielle Maßnahme ist deshalb, die Systemnutzung zumindest auf diesen Personenkreis und den jeweils benötigten Umfang zuverlässig einzuschränken. Das LRZ betreibt zu diesem Zweck seit 2008 ein modernes, LDAP-basiertes Identity-Management-System, in dem alle Benutzer und deren Berechtigungen verwaltet werden. Alle SuperMUC-Authentifizierungen und Autorisierungsvorgänge werden auf entsprechende LDAP-Queries abgebildet. Die SuperMUC-spezifische Komplexität ergibt sich dabei daraus, dass neben Benutzern, die manuell vom

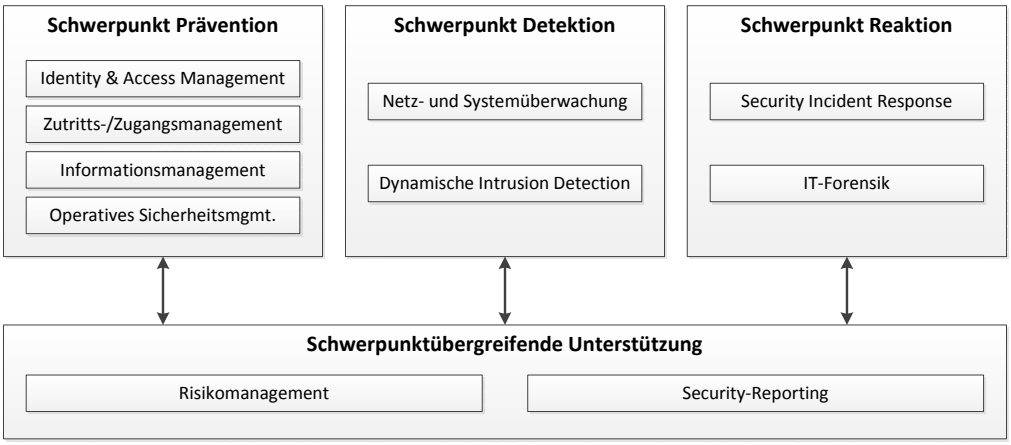


Abbildung 8.7.: Einordnung der Prozesse im SuperMUC-Szenario nach Schwerpunkten

LRZ eingetragen und berechtigt werden, über in [Homm07] beschriebene Mechanismen auch Grid-Benutzer mit bestimmten Berechtigungen automatisiert übernommen und föderationsspezifische Authentifizierungs- und Autorisierungsabläufe unterstützt werden. Sofern in Einzelfällen qualitätssichernde Maßnahmen in diesen automatisierten, organisationsübergreifenden Abläufen scheitern, muss entsprechend manuell eingegriffen werden.

Für das SuperMUC-spezifische Identitätsmanagement spielen insbesondere die folgenden beiden Aspekte eine zentrale Rolle:

1. **Deprovisioning**: Alle Forschungsprojekte, die auf dem SuperMUC durchgeführt werden, und alle dafür eingesetzten Benutzerkennungen haben eine begrenzte Laufzeit, die bedarfsorientiert verlängert werden kann. Durch automatisches Deaktivieren und Löschen von Kennungen wird sichergestellt, dass Benutzer nicht länger Zugriff auf HPC-Ressourcen erhalten als dies für ihre wissenschaftlichen Aufgaben erforderlich ist. Bei Bedarf können ausgewählte Berechtigungen auch zu einem späteren Zeitpunkt wiederhergestellt werden, beispielsweise falls Zugriff auf archivierte Dateien benötigt wird.
2. **Datenqualität**: Unter anderem die Umsetzung von Rollenkonzepten und CPU- sowie Speicherkontingentierung erfordert, dass dieselbe Person nicht mehrfach erfasst wird; hierzu sind in [Homm07] beschriebene, ausgereifte Korrelationsmechanismen erforderlich, die mit der Vielzahl von Identitätsdatenquellen und deren Einschränkungen – beispielsweise dem Fehlen eines gemeinsamen technischen Identifikators für Personen – umgehen können. Zudem bilden die im Identity-Management-System gespeicherten Kontaktinformationen die Grundlage für die Kommunikation im Rahmen der ITSM-Prozesse, beispielsweise bei der Bearbeitung von Störungsmeldungen, und müssen zur Vermeidung unnötiger Verzögerungen durch Recherchen nach aktuellen Daten auch langfristig qualitativ hochwertig sein.

Der Umfang des LRZ-internen Dienstes Identity & Access Management wird unmittelbar vom SuperMUC-Dienst beeinflusst: Beispielsweise wird das Identity-Management-System bis zur Betriebsphase 1 um die Verwaltung von SuperMUC-Plattenplatzkontingenten erweitert; auch neuartige Authentifizierungsverfahren wie SSH-Logins mit X.509v3-Zertifikaten

werden zunächst exklusiv für den SuperMUC-Dienst eingeführt. Zudem wird spezifisch für den SuperMUC-Dienst eine Reihe von Sicherheitskennzahlen bereitgestellt, auf die in Abschnitt 8.6.2.10 eingegangen wird.

8.6.2.2. Zutritts- und Zugangsmanagement für Administratoren im SuperMUC-Szenario

Neben regulären Benutzern, deren Zugangsberechtigungen wie oben beschrieben im Identity-Management-System verwaltet werden und die keine physische Zutrittsberechtigungen zu den Rechnerräumen haben, sind im Kontext des *Privileged Account Management* Administratoren und anderes Wartungspersonal zu betrachten.

Das LRZ regelt den physischen Zutritt und damit die Möglichkeit, hardwarenahe Arbeiten und Manipulationen vornehmen zu können, über ein zentral verwaltetes Schließsystem; dauerhaften Zugang zu den Rechnergebäuden und den einzelnen Rechnerräumen erhalten dabei nur ausgewählte Administratoren, zu deren Aufgaben Hardwarearbeiten an den Systemen gehören, und Mitarbeiter des Gebäudemanagements, das beispielsweise die Klimatechnik betreut. Für externes Wartungspersonal gelten gesonderte Anmeldungs- und Beaufsichtigungsregelungen, die jedoch nicht SuperMUC-spezifisch sind und hier nicht näher betrachtet werden.

Einschränkungen des Zutrittskontrollkonzepts ergeben sich aus der starken räumlichen Verteilung der SuperMUC-Komponenten, die sich über zwei Gebäude und vier Rechnerräume erstreckt; sie resultiert aus dem funktionsorientierten Raumkonzept, das unterschiedliche Aufstellorte für Rechen- und Speichersysteme vorsieht, und dem zeitlichen Verlauf des Systemaufbaus, da das SuperMUC-Migrationssystem bereits aufgebaut und in Betrieb genommen wurde, als sich das für die weiteren SuperMUC-Komponenten vorgesehene Rechnergebäude noch im Bau befand. Personen, die aufgrund ihrer Tätigkeiten Zutritt zu einem der Rechnerräume benötigen, in dem sich auch SuperMUC-Komponenten befinden, haben somit auch zu diesen unmittelbaren Zutritt. Die damit verbundenen Risiken werden jedoch als akzeptabel eingestuft, so dass auf kostspielige zusätzliche Schutzmechanismen – beispielsweise absperrbare Racks mit hochwertigen Schließsystemen – bewusst verzichtet wird.

Als weitere Besonderheit bezüglich des physischen Zutritts muss der Charakter des LRZ als öffentliche Forschungseinrichtung berücksichtigt werden. Interessierte Externe, die sich beispielsweise über den Aufbau moderner Rechenzentrumsinfrastrukturen informieren möchten, werden in Einzelfällen durch die Rechnergebäude geführt; dabei gelten ähnlich zur Anwesenheit externer Wartungsbeauftragter Regelungen zur kontinuierlichen Beaufsichtigung der Gäste.

Der softwareseitige Zugang zu den SuperMUC-Komponenten ist für alle Administratoren im SuperMUC-Betriebskonzept und damit für die gesamte Betriebsdauer des Systems a priori geregelt. Sowohl beim Zugang über die Hardware-Konsolen in den Rechnerräumen als auch beim entfernten Zugang über SSH kommen ausschließlich personalisierte Kennungen zum Einsatz, d. h. es wird nicht nur eine *root*-Kennung verwendet, deren Passwort allen Administratoren bekannt ist, sondern jeder Systemverwalter verwendet einen individuellen administrativen Zugang, so dass im Zusammenspiel mit dem zentralen Logfile-Server zumindest nachvollzogen werden kann, welche Person zu welchem Zeitpunkt auf welchen Systemen tätig war.

Eine detaillierte, vor Manipulationen geschützte Aufzeichnung aller Administratortätigkeiten erfolgt *nicht*, da beispielsweise eine lückenlose Aufzeichnung aller Tastatur- und Mauseingaben inklusive Zeitstempeln, wie sie von einigen Herstellern von Sicherheitsprodukten vor-

gesehen ist, als Arbeitsüberwachung und der Arbeitsatmosphäre abträglich eingestuft wird. Eine vom Autor dieser Arbeit mitverfasste Abhandlung über die technischen und organisatorischen Möglichkeiten zur Prävention und Detektion potentieller Innentäter in Hochschulrechenzentren findet sich in [vEMH12]. Die dort vorgestellten Konzepte und ihre Grenzen gelten unverändert für den SuperMUC-Dienst und werden hier nicht vertieft; als Ergebnis muss jedoch berücksichtigt werden, dass es technisch in der Praxis kaum zu verhindern ist, dass ein böswilliger Administrator Hintertüren ins System einbaut und diese auch langfristig gut verbergen kann. Dies ist insbesondere dann problematisch, wenn einzelne Administratoren vorzeitig vor Ende des SuperMUC-Dienstbetriebs ausscheiden; die in diesem Fall üblichen Automatismen zum Entzug der Berechtigungen umfassen nur diejenigen, die im zentralen Identity-Management-System verwaltet werden. Hat ein Administrator seine Systemverwaltungsberechtigung dazu missbraucht, sich am Identity-Management-System vorbei weitere Zugänge zum System einzurichten, bleiben diese auch über sein offizielles Ausscheiden hinaus erhalten; diese Situation erfordert kontinuierliche Kontrollen durch die offiziellen Administratoren (vgl. hierzu Abschnitt 8.6.2.5).

8.6.2.3. Informationsmanagement im SuperMUC-Szenario

Anders als beispielsweise im militärischen Bereich und in den Verwaltungsrechenzentren von Bund und Ländern wird am LRZ keine durchgängige **Datenklassifizierung** forciert, d. h., dass die Autoren bzw. Quellen von Informationen oder deren Eigentümer nicht zwangsweise detailliert festlegen müssen, wer in welchem Umfang auf die entsprechenden Daten zugreifen darf. Dennoch besteht auch im SuperMUC-Kontext der Bedarf nach einer einfachen, stufenweisen Regelung, so dass alle verarbeiteten Daten einer der folgenden vier Kategorien zugeordnet werden können:

1. *Öffentlich zugängliche Informationen*, beispielsweise Hinweise, wie Projekte und Kennungen für den SuperMUC-Dienst beantragt werden können, werden ohne Zugriffsbeschränkung auf der LRZ-Webseite veröffentlicht oder z. B. auf E-Mail-Anfrage hin zur Verfügung gestellt.
2. *Informationen und Dokumentationen für die Nutzer des Dienstes* werden auf dem SuperMUC-spezifischen Webserver bereitgestellt bzw. sind über den SuperMUC selbst zugänglich. Der Zugriff ist somit nur authentifizierten und zum entsprechenden Zeitpunkt autorisierten Benutzern möglich. Dabei handelt es sich überwiegend um Dokumentationen zur Nutzung des Dienstes, die für die Allgemeinheit nicht relevante Informationen enthalten. Eine Weitergabe der entsprechenden Dokumente an Dritte ist durch die Benutzungsrichtlinien untersagt, wird jedoch nicht technisch kontrolliert.
3. *Benutzerspezifische Daten* werden grundsätzlich analog zu anderen LRZ-Diensten behandelt. Sie werden insbesondere nicht veröffentlicht und eine Einsichtnahme durch LRZ-Personal erfolgt nur in Abstimmung mit den jeweiligen Benutzern, beispielsweise im Rahmen der Programmierberatung zur Anpassung von Programmcode an die Rechnerarchitektur. Über das Datenschutz-Security-Framework können Benutzer individuell Verfeinerungen dieser Regeln vornehmen und dem LRZ-Personal beispielsweise Einsicht in den Programmcode, nicht aber die Ein- und Ausgabedateien der entsprechenden HPC-Jobs gewähren. Weitere Differenzierungen sind u. a. nach Projekten, Benutzern und Datenverarbeitungszwecken möglich.

4. *LRZ-interne Informationen* umfassen beispielsweise Daten zur Konfiguration der SuperMUC-Komponenten. Sie werden weder öffentlich noch den Benutzern zugänglich gemacht; auch LRZ-intern werden sie nur an Personal mit entsprechenden Aufgaben kommuniziert.

Eine darüber hinausgehende organisationsübergreifende Datenklassifizierung findet bislang nicht statt. Mit der zunehmenden industriellen Nutzung von HPC- und Grid-Ressourcen sind jedoch Änderungen und Verfeinerungen der Schutzklassen, die sich noch im SuperMUC-Betriebszeitraum auswirken, denkbar.

Die Existenz vertraulicher und zu schützender Informationen hat Auswirkungen auf die **Entsorgung von Datenträgern**. Insbesondere die in den Speicher-, Backup- und Archivsystemen eingesetzten Festplatten und Magnetbänder unterliegen entsprechenden Auflagen:

- Bei hardwareseitigen Defekten können Dateien nicht mehr vom LRZ selbst gelöscht bzw. überschrieben werden. Die zuverlässige Datenvernichtung muss deshalb Bestandteil der Verträge mit den Firmen, die z. B. den Austausch in der Garantiezeit vornehmen, sein.
- Analog dazu liegt beim Rückbau des Dienstes zum Ende seiner Betriebszeit ein Mengenproblem vor, das vom LRZ nicht alleine bewältigt werden kann. Sofern Speichermedien nicht für andere LRZ-Dienste weiterhin genutzt, sondern abgebaut werden sollen, muss die Datenvernichtung Bestandteil des Vertrags über die Rücknahme der Hardwarekomponenten sein.
- Sofern eine Weitergabe von Speichermedien an Nachnutzer erfolgt, beispielsweise wenn alte Speicher- und Archivsysteme anderen Hochschulen überlassen werden, muss der Nachnutzer ebenfalls zur datenschutzgesetzkonformen Vernichtung der zusammen mit den Speichermedien übergebenen Informationen verpflichtet werden.

Darüber hinaus stehen Aktenvernichter für Papier und Shredder für optische Speichermedien wie CDs und DVDs zur Verfügung. Die Nutzung dieser Werkzeuge wird jedoch nicht in Sinne einer *Data Leakage Prevention* kontrolliert; über die Regelung der Zweckbindung elektronisch verarbeiteter Informationen auf Basis des Datenschutz-Security-Frameworks hinausgehend wäre es aufwandsbedingt nicht praktikabel, beispielsweise das Photographieren von Bildschirminhalten oder das Kopieren von Dateien auf USB-Speichermedien zu verhindern.

Bei der IT-sicherheitsspezifischen **Informationsakquisition** muss zwischen allgemeinen und SuperMUC-spezifischen Informationskanälen differenziert werden. Allgemeine Informationen über neu bekannt gewordene Sicherheitslücken, Software-Updates etc. erreichen das LRZ beispielsweise über Mailinglisten der eingesetzten Linux-Distribution, Warnmeldungen vom DFN- bzw. EGI-CERT und weitere sicherheitsspezifische Diskussionsmedien wie Bugtraq. Zudem werden entsprechende Beobachtungen aus eigenen Forschungsprojekten und Forschungskooperationen mit Lehrstühlen der Münchner Universitäten sowie auf Basis der in Abschnitt 8.6.2.6 beschriebenen Sensormeldungen gemacht. Auch Angriffe auf andere LRZ-Systeme dienen als Indikatoren möglicher Sicherheitslücken und aufkommender SuperMUC-Angriffsversuche. Daneben fungieren die vom Hersteller abgeordneten SuperMUC-Administratoren auch als Schnittstelle zur Weitergabe herstellerintern bekannt werdender Sicherheitsinformationen; sie sind auch dafür verantwortlich, Sicherheitsmeldungen über SuperMUC-Komponenten, die von Drittherstellern stammen, zu aggregieren und propagieren.

Ein Großteil der **Dokumentation** der sicherheitsspezifischen Eigenschaften des SuperMUC-Systems entsteht während des Einführungsprojekts; hierbei stellen beispielsweise die Betriebs- und Sicherheitskonzepte Deliverables der einzelnen Lebenszyklusphasen der Frameworkinstanzen dar. Ferner werden Protokolle zu Projektbesprechungen und einzelnen Projektaktivitäten erstellt, die auch in die formale Abnahme des Gesamtsystems einfließen. Im laufenden Betrieb werden auch Arbeiten mit Werkzeugen, die zur Unterstützung der ITSM- und Sicherheitsmanagementprozesse eingesetzt werden, dokumentiert. Durch das Festhalten von Motivation, Begründung für den Einsatz, Durchführungsverlauf und Ergebnissen wird nicht nur eine Rekonstruktion der einzelnen Tätigkeiten in der erforderlichen Tiefe ermöglicht, sondern es können auch entsprechende Auswertungen, z. B. zur Planung von Verbesserungen, vorgenommen werden können.

8.6.2.4. Ausgewählte Aspekte des operativen Sicherheitsmanagements im SuperMUC-Szenario

Neben den oben bereits genannten umfasst das operative Sicherheitsmanagement im SuperMUC-Szenario die im Folgenden skizzierten weiteren präventiven Maßnahmen. Diese weisen jedoch entweder keine Besonderheiten gegenüber anderen LRZ-Diensten auf oder sind aus dem SuperMUC-Systemadministrationskonzept hervorgegangen und wurden somit nicht primär unter IT-Sicherheitsaspekten konzipiert:

- Software-Update-Management und template-basiertes Hardening: Wie in Abschnitt 8.6.1.4 dargelegt wurde, bestehen die SuperMUC-Compute-Nodes aus festplattenlosen Systemen, die beim Einschalten ein Betriebssystemabbild von einem zentralen xCAT-Managementsystem beziehen. Als Vorteil daraus ergibt sich, dass Software-Updates nur in die wenigen eingesetzten Betriebssystemabbilder eingespielt werden müssen und auch nur diese z. B. mit dem Linux-Kernel-Security-Framework ausgestattet werden müssen, um dennoch eine flächendeckende Abdeckung zu erreichen. Zur Härtung der Systeme wird analog zu anderen LRZ-Diensten der Minimalitätsgrundsatz angewendet, d. h. es werden nur diejenigen Systemsoftwarepakete und Dienste installiert, die für die Bereitstellung und Nutzung des SuperMUC-Dienstes zwingend erforderlich sind.
- Netzsegmentierung: Alle SuperMUC-Komponenten sind in dedizierten IP-Subnetzen platziert, deren Datenverkehr auch über virtuelle LANs (VLANs) von anderen Diensten und Servern des LRZ abgeschottet wird; hierdurch kann ein unberechtigtes Mitschneiden oder Manipulieren des SuperMUC-internen Netzverkehrs zuverlässig verhindert werden. Für die externe IP-basierte Kommunikation müssen hingegen andere Mechanismen zur Sicherstellung der Vertraulichkeit und Integrität eingesetzt werden, beispielsweise die bereits erläuterten verschlüsselten interaktiven SSH-Verbindungen und Dateiübertragungen.
- Penetrationstests: Über das Internet und damit im Allgemeinen trotz der Firewallregeln weltweit erreichbare LRZ-Systeme werden auf Basis des vom DFN-CERT bereitgestellten Dienstes *Netzwerkprüfer* regelmäßig auf Veränderungen getestet. Der Dienst führt im Wesentlichen einen Portscan durch, der Aufschluss darüber gibt, auf welchen TCP/IP-Ports von außen ansprechbare Dienste aktiv sind. Kommen unerwartet neue „offene“ Ports hinzu, so liegt ein Anzeichen für Fehlkonfigurationen oder von Angrei-

fern erfolgreich eingerichtete Hintertüren vor; auch bei bekannten Ports ist regelmäßig zu überprüfen, ob die dahinterstehende Software mit Bezug auf aktuell bekannte Schwachstellen auf einem aktuellen Stand und adäquat konfiguriert ist.

Vertiefende präventive Maßnahmen wie beispielsweise über Portscans hinausgehende Penetrationstests, bei denen ein Security Engineer in der Rolle eines Angreifers detaillierter nach potentiellen Schwachstellen sucht, werden nicht regelmäßig durchgeführt. Ähnlich zu den in Abschnitt 8.6.2.8 beschriebenen IT-forensischen Maßnahmen besteht dabei die Schwierigkeit, dass LRZ-intern kein dediziertes Personal vorhanden ist, das sich bezüglich Schwachstellenanalysen und den dafür erforderlichen komplexen und äußerst umfangreichen Werkzeugen kontinuierlich auf dem aktuellsten Stand halten kann. Bei akuten Verdachtsmomenten oder sich beispielsweise aus der Zusammenarbeit mit Partnereinrichtungen ergebendem Bedarf können jedoch analog zu einigen anderen LRZ-Diensten externe Sicherheitsdienstleister mit der Durchführung tiefgehender Penetrationstests beauftragt werden.

8.6.2.5. Netz- und Systemüberwachung im SuperMUC-Szenario

Alle im Produktivbetrieb eingesetzten LRZ-Server und alle für Kunden zugänglichen Dienste werden netz- und systemseitig kontinuierlich überwacht. Die Verwaltung der SuperMUC-Komponenten über Managementplattformen und Monitoringsysteme liefert dabei allgemeine Informationen über potentielle Störungen, die ihrerseits wiederum mit potentiellen Sicherheitsvorfällen in Verbindung stehen können. Netzseitig kommen dabei folgende detektierende Maßnahmen zum Einsatz:

- Alle für den SuperMUC relevanten aktiven Netzkomponenten, d. h. Router und Switches, werden über eine MWN-weit eingesetzte Netzmanagementplattform überwacht, die über das Managementprotokoll SNMP sowohl die geräteinternen Selbsttests überwacht, um frühzeitig defekte Komponenten wie Lüfter zu identifizieren, als auch die aktuelle Auslastung der einzelnen Netzverbindungen prüft. Ungewöhnlich hoher Datenverkehr kann dabei ein Indikator für Angriffsversuche sein.
- Der gesamte Netzverkehr wird am Übergang zum deutschen Wissenschaftsnetz X-WiN auf Auffälligkeiten untersucht; dabei kann beispielsweise die charakteristische Botnetz-Kommunikation, die Rückschlüsse auf einzelne kompromittierte Maschinen zulässt, erkannt werden. Hierfür sind Regelsätze und Schwellenwerte definiert, durch die auch automatisierte Meldungen an das zentrale SIEM-System OSSIM vorgenommen werden (vgl. Abschnitt 8.6.2.6).
- Alle Netzkomponenten, die präventive Mechanismen bereitstellen, berichten Verstöße gegen ihre Regelsätze ebenfalls über das zentralisierte Logging und können somit über das SIEM-System ausgewertet werden; hierzu zählen insbesondere die Firewalls, die konfigurierten Router-ACLs und Beschränkungen der Dienstnutzung, die auf den Load-Balancern konfiguriert werden.

Zudem werden Netzverkehrscharakteristika wie IP-Verbindungsendpunkte und übertragene Datenvolumina samt Zeitstempeln auf Basis von Accounting- und so genannten NetFlow-Daten für einen Zeitraum von sieben Tagen gespeichert. Neben automatisierten regelmäßigen Auswertungen, die in einem zur SuperMUC-Einführung parallelen Projekt implementiert wer-

Abbildung 8.8.: Beispiel für die Integration von SuperMUC-Komponenten in die Monitoringwerkzeuge

den, spielen diese Informationen bei der Rekonstruktion von Sicherheitsvorfällen eine zentrale Rolle.

Bezüglich der Systemüberwachung wird analog zum Configuration Management zwischen der überschaubaren Zahl u. a. an Login-Nodes und Managementservern auf der einen Seite und der großen Menge der Compute-Nodes auf der anderen Seite differenziert. Die mit den herkömmlichen LRZ-Servern vergleichbaren SuperMUC-Komponenten werden wie in Abbildung 8.8 dargestellt in das reguläre LRZ-Systemmonitoring integriert, das neben einem Buchführen über die Versionen der eingesetzten Software u. a. auch die CPU- und Speicherplatzüberwachung durchführt. Analog zum Netzverkehr kann ungewöhnlich hohe CPU-Last dabei beispielsweise wiederum ein Indikator für von Angreifern gestartete Prozesse sein. Die Compute-Nodes werden hingegen über eine dediziert für den SuperMUC-Dienst eingesetzte Monitoringsoftware überwacht, die neben dem Status der Hardware auch die HPC-Jobs einbezieht und somit auch die Schnittstelle zum Performance-Management bildet. Eine automatisierte Angriffserkennung ist auf dieser Ebene nicht möglich, da keine semantische Interpretation des von den Benutzern eingebrachten und ausgeführten Codes möglich ist.

8.6.2.6. Einsatz dynamischer Angriffserkennungssensorik im SuperMUC-Szenario

Durch das Netz- und Systemmonitoring, die für das SuperMUC-Anwendungsbeispiel eingesetzten Security-Frameworks und weitere laufende Sicherheitsprojekte ist am LRZ ein breites Spektrum an Detektionssensorik vorhanden. Die meisten Sensoren können mehrere verschiedene Angriffsarten erkennen und melden; umso wichtiger werden dadurch die Korrelation von Meldungen und die konzertierte Auswertung, um bei Sicherheitsvorfällen geordnet reagieren zu können. Im Folgenden wird deshalb als Anwendungsbeispiel für das in Abschnitt 7.2 spezifizierte Managementwerkzeug knapp zusammengestellt, welche Sensoren zu berücksichtigen sind, wie diese an eine zentrale Auswertestation angebunden werden können und welche Zielsetzungen bei der dynamischen Sensorrekonfiguration und der Auswertung im SuperMUC-Szenario zu verfolgen sind.

Sicherheitsereignisse und Sicherheitsalarme werden von den folgenden Sensoren erzeugt, die wie in Abbildung 8.9 dargestellt integriert werden:

- Wie in Abschnitt 8.6.2.5 beschrieben liefern die Netzkomponenten und Netzüberwachungssysteme Sicherheitsmeldungen. Dies umfasst insbesondere Verstöße gegen

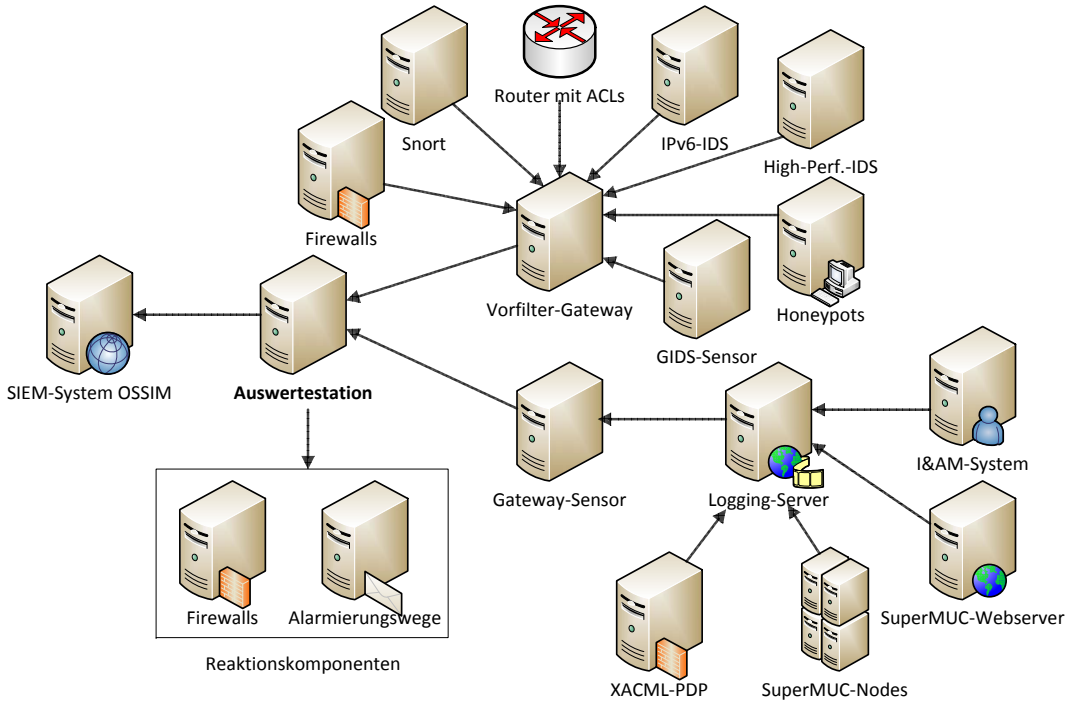


Abbildung 8.9.: Anbindung der Detektionssensorik im SuperMUC-Szenario und primäre Meldedatenflüsse

Firewall-Regeln und Alarme des LRZ-weit eingesetzten Intrusion Detection Systems Snort. Bislang werden Snort-Sensoren nur am zentralen X-WiN-Übergang eingesetzt, zusätzliche Snort-Instanzen in serverspezifischen Subnetzen befinden sich jedoch in einem Parallelprojekt in Vorbereitung, um auch MWN-interne Angriffe besser erkennen zu können.

- In Forschungsprojekten und -kooperationen werden zusammen mit anderen Institutionen Sicherheitssensoren im Pilotbetrieb und zum Teil produktiv betrieben:
  - Im Rahmen des in Abschnitt 7.2.1 skizzierten GIDS-Projekts werden Grid-spezifische Angriffssensoren betrieben, die alle an Grid-Projekten beteiligte LRZ-Ressourcen überwachen; hierzu gehört neben dem SuperMUC- beispielsweise auch der LRZ-Linux-Cluster-Dienst. Ein Mehrwert gegenüber den ausschließlich lokal betriebenen Snort-Instanzen ergibt sich einerseits durch die Grid-weite Korrelation der Sensormeldungen, deren Ergebnisse LRZ-seitig ausgewertet werden können, und andererseits durch die zu Snort komplementäre Softwarebasis Prelude; die Kombination beider IDS-Produkte wirkt sich positiv auf die Erkennungsleistung und die Fehlerrate aus.
  - Zusammen mit dem Fraunhofer AISEC wird ein FPGA-basierter Honeypot am LRZ betrieben, der ganze Subnetze voller vermeintlich schwachstellenbehafteter Server vortäuscht und dadurch Angreifer, die die öffentlichen IP-Netze des LRZ analysieren, anzieht. Wie für Honeypots üblich werden keine regulären Dienste

erbracht, so dass alle Verbindungen in die Honeypot-Netze als Angriffsversuche klassifiziert werden können.

- Moderne Konzepte für High-Performance-Intrusion-Detection-Systeme, die trotz Bandbreiten von 10 Gbit/s und mehr eine parallele Auswertung mit vielen IDS-Regelsätzen ermöglichen, werden zusammen mit dem Lehrstuhl für Netzarchitekturen und Netzdienste der TU München erprobt.
- Im Rahmen eines in Vorbereitung befindlichen Forschungsprojekts mit einem Hersteller von High-Performance-Firewalls und der Hochschule München soll insbesondere die Erkennungsleistung von IPv6-basierten Angriffen in IPv4-/IPv6-Dual-Stack-Umgebungen verbessert werden.

- Die von den Security-Frameworks abgedeckten Mechanismen fungieren als primäre Datenquellen für SuperMUC-spezifische Angriffsmeldungen:
  - Das Framework für föderiertes Sicherheitsmanagement betrachtet u. a. alle Authentifizierungs- und Autorisierungsvorgänge, so dass ihm beispielsweise Meldungen über fehlgeschlagene Loginversuche von Benutzer- und Administratorkennungen zugeordnet werden können.
  - Das Datenschutz-Security-Framework protokolliert potentielle Datenschutzverstöße, die durch unzulässige betreiberseitige Versuche des Zugriffs auf Benutzerdateien zustande kommen; sein Schwerpunkt liegt deshalb auf der Erkennung von Angriffen durch Innentäter.
  - Das Linux-Kernel-Security-Framework meldet über seine Systemschnittstellen erkannte Policyverstöße und ermöglicht dadurch eine genaue Zuordnung von Angriffsversuchen zu den einzelnen Kennungen, von denen sie ausgehen. Seine Meldungen sind deshalb insbesondere im Kontext des in Abschnitt 8.6.2.7 beschriebenen Vorfallstyp *kompromittierte Benutzerkennung* relevant.

- Auf ausgewählten Servern werden Host-Intrusion-Detection-Systeme eingesetzt, um primär Manipulationen an Systemdateien zu erkennen, die nicht auf reguläre Software-Updates zurückzuführen sind. In einem Parallelprojekt wird das in [vEMH12] beschriebene lernfähige Werkzeug implementiert, das auf den Login-Nodes eingesetzt werden kann und damit Teile der in Abschnitt 7.2.6.1 beschriebenen Verhaltensanalyse umsetzt, indem es beurteilt, ob der Login eines Benutzers von einem bestimmten Quellsystem aus und zu einer bestimmten Uhrzeit als übliches Ereignis oder als verdächtig zu gelten hat.

Zur Anbindung dieser Sensorik an die zentrale Auswertestation müssen sowohl die sensorseitig bereits vorhandenen Schnittstellen als auch deren Einschränkungen bezüglich einer dynamischen Steuerung berücksichtigt werden:

- IDS-Sensoren, wie sie beispielsweise im Rahmen von GIDS betrieben werden, unterstützen sowohl die direkte Weitergabe von Sicherheitsmeldungen an Auswertestationen als auch das im Werkzeugkonzept verwendete IDMEF-Datenformat. Die meisten der im SuperMUC-Szenario vorliegenden Sensoren dieser Art unterstützen jedoch nur eine sehr eingeschränkte zentrale, dynamische Steuerung ihrer Regelsätze. Um eine Überlastung der Auswertestation durch zur Angriffserkennung nicht benötigte Meldungen zu

vermeiden, muss deshalb ein Gateway implementiert werden, der eine dynamisch rekonfigurierbare Filterung der von den Sensoren gemeldeten Ereignissen vornimmt und nur die aktuell für die Auswertestation relevanten Meldungen an diese weiterleitet.

- Die übrigen Sensoren, insbesondere die in Security-Frameworks integrierten Sicherheitsmechanismen, unterstützen größtenteils lediglich die Protokollierung von Ereignissen in einem zentralen Logging-Server. Als Schnittstelle zur Auswertestation wird deshalb ein weiterer Gateway-Sensor benötigt, der die Protokolleinträge auswertet und in Form von IDMEF-Nachrichten an die Auswertestation überträgt. Auch ihm kommt eine besondere Rolle bezüglich der Dynamiksteuerung zu, da eine pauschale Konvertierung aller Protokolleinträge zu viele und größtenteils irrelevante Meldungen produzieren würde. Er trägt somit durch eine steuerbare, selektive Auswertung ausgewählter Protokolleinträge maßgeblich zur Skalierbarkeit des gesamten Detektionsverfahrens bei; wie der Gateway für die Filterung von IDS-Meldungen muss jedoch auch diese Komponente erst implementiert werden.

Zur Optimierung der Erkennungsleistung und Verbesserung der Skalierbarkeit sind somit primär die folgenden Dynamikeigenschaften zu implementieren:

- Die zentrale Snort-IDS-Instanz am X-WiN-Übergang, die eine Schlüsselrolle in der gesamten Angriffserkennung bezüglich der Erkennungsleistung einnimmt, kann aufgrund des hohen Verkehrsvolumens und begrenzter interner Verarbeitungskapazität zu jedem Zeitpunkt nur wenige Regelsätze zur Auswertung der Datenpakete umsetzen. Es müssen deshalb für aktuell zu beobachtende Angriffe passende Regelsätze aktiviert und andere dafür abgeschaltet werden.
- Dem GIDS-Sensor kommt aufgrund der von ihm durchgeführten Abstimmung der Angriffserkennung mit anderen Grid-Sites die Aufgabe zu, automatische Anpassungen der Ausrichtung der LRZ-weiten Erkennungsleistung anzustoßen. Wird beispielsweise von den als vertrauenswürdig eingestuften Partner-Sites ein Angriff bestimmten Typs angezeigt, so muss durch die dynamische Rekonfiguration der Detektionssensorik sichergestellt werden, dass entsprechende Angriffsversuche auch LRZ-seitig zuverlässig erkennt werden können. Der GIDS-Sensor ist darüber hinaus der Auslöser für automatische Reaktionen, für die entsprechende organisationsübergreifende Vereinbarungen getroffen wurden.
- Der Gateway-Sensor zur Auswertung von Protokolleinträgen ist wie bereits oben skizziert mit der Zielsetzung verbunden, nur die für die aktuell zu beobachtenden Angriffe relevanten Protokollinformationen zu propagieren. Dabei kann es sich je nach Angriffstyp beispielsweise um Informationen über fehlgeschlagene Authentifizierungen, die vom Identity-Management-System geliefert wurden, oder um Angaben zu Quell-IP-Adressen, die gegen Firewall-Regelsätze verstoßen haben, handeln.

Als übergeordnetes System für die Auswertestation fungiert das bereits erläuterte zentrale SIEM-System, das im LRZ auch die zentrale Stelle ist, an der automatisierte Reaktionen wie das dynamische Einfügen von Firewallregeln und die Alarmierung des operativen Sicherheitsmanagements implementiert werden. Entsprechende Anpassungen für den SuperMUC-Dienst werden dort analog zu den übrigen LRZ-Diensten vorgenommen. Im Vordergrund steht dabei, möglicherweise schädliche automatisierte Reaktionen, die sich aus Fehlalarmen oder gezielten Angriffen auf den Automatismus ergeben können, zu vermeiden und sowohl für bekannte als

auch möglicherweise neuartige Angriffe auf die Alarmierung des zuständigen Personals zu setzen.

Mittelfristig ist darüber hinaus anzustreben, weitere Informationsquellen in die automatisierte Bewertung potentieller Angriffe einfließen zu lassen; dies betrifft insbesondere den sofortigen Einbezug der o. g. NetFlow-Daten, die bislang lediglich separat bzw. manuell im Rahmen der Bearbeitung von Sicherheitsvorfällen analysiert werden.

8.6.2.7. Security Incident Response im SuperMUC-Szenario

Für den geordneten Umgang mit Sicherheitsvorfällen wurde am LRZ ein dedizierter Security-Incident-Response-Prozess in Kraft gesetzt, der sich zwar am regulären Incident Management orientiert, aber gezielt auf die IT-Sicherheitsspezifika eingeht. Insbesondere existiert mit dem Computer Security Incident Response Team des LRZ (LRZ-CSIRT) eine eigene Bearbeitergruppe, deren Zusammensetzung anders als beim First Level Support bzw. beim LRZ Service Desk primär auf einschlägigen Sicherheitsmanagementkompetenzen beruht.

Für jeden Sicherheitsvorfall wird aus einer rund zehn Personen umfassenden Liste ein Koordinator (*Security Incident Coordinator*, SIC) bestimmt, der für die Bearbeitungsdauer Weisungsbefugnis hat und zunächst ein Bearbeitungsteam zusammenstellt, das neben CSIRT-Mitgliedern beispielsweise auch die zuständigen Systemadministratoren umfasst. Die hohe Effizienz des LRZ-SIR-Prozesses ergibt sich daraus, dass für als Standard Security Incidents (SSIs) bezeichnete Arten von Sicherheitsvorfällen bereits a priori festgelegt wird, wie geordnet darauf reagiert werden soll. Somit kann beim Eintreten eines solchen Vorfalls schnell und einheitlich strukturiert reagiert werden, ohne dass das genaue Vorgehen zunächst umfassend konzipiert und abgestimmt werden muss. Für den SuperMUC können dabei insbesondere die folgenden drei SSIs vorgesehen werden:

1. **Kompromittierte Benutzerkennung**: Da der SuperMUC-Dienst von vielen hundert Benutzern über Forschungsnetze und das Internet von verschiedensten Standorten aus genutzt wird, kann technisch nicht verhindert werden, dass Angreifer über geknackte oder abgehörte Passwörter, ausgespähte Benutzerzertifikate bzw. SSH-Keys oder über kompromittierte Benutzer-Clients bzw. Server an anderen Standorten auf den SuperMUC gelangen können. Die Erkennung kompromittierter Benutzerkennungen ist meist schwierig, da sich die dabei LRZ-seitig zu beobachtenden Abläufe bei Authentifizierung und Autorisierung im Regelfall in keinster Weise von einer legitimen Dienstnutzung unterscheiden. Alle eingesetzten technischen Mechanismen, wie sie auch von den Security-Frameworks bereitgestellt werden, stoßen dabei an ihre Grenzen. Die Erkennung erfolgt deshalb häufig auf Basis externer Meldungen oder der Beobachtung ungewöhnlicher Prozesse, die vom Angreifer auf den SuperMUC-Nodes gestartet wurden, durch die Administratoren. Die Reaktion besteht primär aus der umgehenden Sperrung der kompromittierten Kennung sowie der Kontaktaufnahme mit dem betroffenen Benutzer bzw. seiner Heimateinrichtung und sekundär aus der Analyse, ob die Kennung auf dem SuperMUC als Ausgangsbasis für weitere Angriffe missbraucht wurde.
2. **root-Exploits**: Sicherheitslücken in Betriebssystemkomponenten, für die noch kein Software-Update verfügbar ist oder eingespielt wurde, können von Angreifern – beispielsweise unter Verwendung einer kompromittierten Benutzerkennung – unter Umständen ausgenutzt werden, um systemadministrative Berechtigungen auf einzelnen

SuperMUC-Nodes zu erlangen. Damit geht die Gefahr einher, dass der Angreifer nicht nur auf die Dateien eines einzelnen Benutzers zugreifen kann, sondern dieselben Ge- und Missbrauchsmöglichkeiten erlangt wie die Gruppe der legitimen SuperMUC-Administratoren; zur Erkennung trägt deshalb insbesondere das Datenschutz-Security-Framework bei, das den Zugriff auf Anwenderdateien durch administrative Kennungen überwacht. Neben tiefgreifenden Systemmanipulationen auf den kompromittierten Nodes kann der Angreifer somit auch versuchen, zahlreiche weitere Kennungen von SuperMUC-Benutzern zu kompromittieren, über die anschließend oft auf Zugriff auf HPC-Dienste bei anderen Rechenzentren möglich ist. Die Schwerpunkte bei der Bearbeitung solcher Vorfälle, die zu den „größten anzunehmenden Unfällen“ beim Betrieb von HPC-Systemen zählen, liegen deshalb über die Behandlung der kompromittierten Benutzerkennungen hinausgehend bei der Beseitigung der zugrundeliegenden Sicherheitslücke und der Neuinstallation aller betroffenen Nodes und Systeme.

3. **Denial-of-Service-Angriffe**: Mit steigender Popularität der o. g. BitCoin-Währung, die anonyme und nicht nachverfolgbare Zahlungsvorgänge unterstützt, nimmt auch die Zahl der Erpressungsversuche zu; der Angreifer droht dabei, über Botnetze, die aus mehreren tausend ferngesteuerten Rechnern bestehen, Netz- und Systemüberlastsituationen herbeizuführen, falls eine gewisse BitCoin-Summe nicht rechtzeitig gezahlt wird; es sind mehrere Fälle bekannt, in denen deutsche Internet-Provider und auch bayerische Universitäten bei ausbleibenden Zahlungen tatsächlich angegriffen wurden (siehe auch [Coin11]). Die Auswirkungen von Angriffen dieser Form können durch eine entsprechende Konfiguration der Firewalls und Login-Nodes abgeschwächt werden, gehen jedoch mit Beeinträchtigungen des regulären Benutzerbetriebs einher, so dass im Rahmen der SSI-Bearbeitung primär Vorbereitungen getroffen werden, um zum vorher unbekannten Zeitpunkt des Eintretens der Angriffe schnell reagieren und baldmöglichst wieder zum Regelbetrieb zurückkehren zu können.

In allen Fällen erfolgt eine Zusammenarbeit mit Partnereinrichtungen, beispielsweise durch die Alarmierung der anderen GCS-Sites und durch enge Abstimmung der Bearbeitungsschritte mit den CERTs des DFN-Vereins und der EGI. Damit wird auch das Ziel verfolgt, dass Sicherheitsvorfälle auf dem SuperMUC nicht auf andere HPC-Sites übergreifen, worunter auch die Reputation des LRZ leiden würde.

Die Behandlung von Sicherheitsvorfällen, die keine SSIs darstellen, muss im Einzelfall überlegt und umgesetzt werden. Dem CSIRT kommt in jedem Fall die Rolle zu, über die Behebung eines akuten Vorfalls hinausgehend auch an einer nachfolgend intensiveren Beobachtung der betroffenen SuperMUC-Komponenten mitzuwirken, um beispielsweise zu prüfen, ob die Schwachstellen, die zum Vorfall geführt haben, wirklich gefunden und beseitigt wurden, oder ob ein vergleichbarer Vorfall bereits nach kurzer Zeit erneut auftritt. Alle Vorfälle werden LRZ-intern in Form von Security-Incident-Records dokumentiert und fließen im Rahmen von Post-Incident-Reviews in die Planung der Verbesserung der vorhandenen Sicherheitsmechanismen ein.

8.6.2.8. Möglichkeiten zur IT-Forensik im SuperMUC-Szenario

Fast alle bisher auf LRZ-HPC-Systeme zu beobachtenden Angriffsversuche und erfolgreichen Angriffe zielten darauf ab,

- das jeweilige System zu kompromittieren, um von dort aus Angriffe auf weitere Systeme durchführen zu können,
- Kennungen zu kompromittieren, um auf weitere Systeme Zugriff erlangen zu können, oder
- die Ressourcen für eigene Prozesse des Benutzers – beispielsweise zum Versand von Spam-E-Mails, Generieren von BitCoins oder Durchführen von DoS-Angriffen – zu missbrauchen.

Entsprechende Vorfälle sind trotz des damit verbundenen Arbeitsaufwands als relativ harmlos einzustufen, da sie sich gegen Ressourcen, aber nicht gegen die verarbeiteten Daten richten. Diesbezüglich wesentlich gravierender sind Vorfälle einzustufen, die auf das gezielte Ausspähen z. B. aktuellster Forschungsergebnisse abzielen. Derartige Vorfälle rechtfertigen den Aufwand, der mit einer über den oben beschriebenen SIR-Prozess hinausgehenden IT-forensischen Analyse der kompromittierten Systeme verbunden ist. Dabei sollen im Wesentlichen vorhandene Beweismittel in einer vor Gericht verwertbaren Form gesichert, der genaue Ablauf des gesamten Angriffs rekonstruiert und die eindeutige Identifikation des Angreifers unterstützt werden. Da häufig mehrere HPC-Sites parallel von solchen Angriffen betroffen sind, muss wiederum eine enge Abstimmung mit den Partnern, CERTs und Strafverfolgungsbehörden stattfinden.

Die IT-Forensik ist eine eigene, komplexe und sich technisch ständig weiterentwickelnde Disziplin. Dies führt dazu, dass am LRZ keine IT-Forensikspezialisten verfügbar sind, die sich z. B. bezüglich der Angriffstechniken und Forensikwerkzeuge fachlich immer auf dem aktuellsten Stand halten können; die derzeit relativ geringe Anzahl entsprechender Sicherheitsvorfälle würde entsprechend dediziertes Personal auch nicht rechtfertigen. Die zur Thematik verfügbare Literatur ist inzwischen jedoch so umfangreich, dass eine kurzfristige, bedarfsgesteuerte Einarbeitung durch das zuständige LRZ-CSIRT-Team kaum realisierbar wäre. Aus diesem Grund wurde im Rahmen einer Diplomarbeit ein auf die LRZ-Umgebung zugeschnittener IT-Forensik-Leitfaden entwickelt (siehe [Rom12]). Er gibt abhängig von der Art des Angriffs Anleitungen zum IT-forensischen Vorgehen vor, so dass die wichtigsten Analysen und Beweissicherungsschritte in Form einer Checkliste auch ohne lange Einarbeitungszeit und tiefgehende Forensikfachkenntnisse durchgeführt werden können. Diese Vorgehensweise sichert belastbare Resultate, zumindest solange keine völlig neuartigen Angriffe durchgeführt werden. Für die IT-forensische Analyse des SuperMUC-Dienstes ist dabei dessen Nähe zu herkömmlichen Linux-Server-Systemen von großem Vorteil, da entsprechende Standardwerkzeuge eingesetzt werden können, mit denen auch auf anderen LRZ-Systemen bereits Erfahrungen gesammelt werden konnten.

Der IT-Forensik-Workflow wird bei entsprechenden Vorfällen aus dem SIR-Prozess angestoßen und liefert seine Ergebnisse an diesen zurück; technische Inhalte sind dabei gesicherte Beweise über den Angriffsverlauf und Protokolleinträge, die Informationen z. B. über aufgespürte ausgetauschte Systemdateien und Zugriffe auf Benutzerdateien enthalten. Dabei wird insbesondere eine Integritätssicherung durchgeführt, um nachweisen zu können, dass Beweismaterial durch die IT-Forensik nicht zerstört oder modifiziert worden ist. Es muss berücksichtigt werden, dass forensische Analysen mit einem gewissen Zeitaufwand verbunden sind, der im Konflikt zum Ziel des SIR-Prozesses steht, betroffene Systeme schnellstmöglich zu säubern und wieder zum Regelbetrieb zurückzukehren. Im schlechtesten Fall kommt es dadurch zu längeren Betriebsunterbrechungen; durch die Partitionierung des gesamten SuperMUC-Systems und die Redundanz z. B. der Login-Nodes können IT-forensisch zu analysierende

Komponenten im Idealfall jedoch analog zur Behandlung von Hardwaredefekten meist so isoliert werden, dass der Dienst schnellstmöglich wieder in Betrieb gehen kann, ohne sich negativ auf die Forensikergebnisse und deren Verwertbarkeit auszuwirken.

8.6.2.9. Risikomanagement im SuperMUC-Szenario

Das Management von IT-Sicherheitsrisiken wird am LRZ bislang überwiegend auf der Ebene einzelner Dienstgruppen durchgeführt; alle HPC-Dienste, zu denen neben SuperMUC beispielsweise das LRZ-Linux-Cluster gehört, bilden eine solche Gruppe. Alle Dienste in der Gruppe haben ähnliche Nutzungscharakteristika und sind damit im Kontext derselben Angreifermodelle zu betrachten. Für die HPC-Dienste ergeben sich spezifische Angreifermodelle beispielsweise aus der Einbindung in organisationsübergreifende Grid-Infrastrukturen und ihrer prinzipiellen Aufgabe, in einer Multi-User-Umgebung autorisierten Benutzern die Möglichkeit zur Ausführung eigener, inhaltlich ungeprüfter Programme zu gewähren.

Nach der Identifikation dienstgruppenspezifischer Risiken, die in der Verantwortung der jeweiligen Abteilung liegt und durch die in Abschnitt 8.6.2.3 beschriebenen Abläufe zur Informationsbeschaffung unterstützt wird, werden ihre Eintrittswahrscheinlichkeit und die mit ihnen verbundenen Auswirkungen sowie mögliche Gegenmaßnahmen in enger Abstimmung mit dem Sicherheitsarbeitskreis und damit unter abteilungsübergreifender Beteiligung evaluiert. Ergebnisse und Planungen werden zur Genehmigung hierarchisch weitergegeben; die anzuschaffenden oder zu verbessernden technischen Sicherheitsmechanismen werden anschließend wiederum abteilungsintern verantwortet.

Anders als beispielsweise beim Betrieb der E-Mail- und Fileserver-Dienste muss beim SuperMUC dessen a priori begrenzte Betriebszeit berücksichtigt werden. Je größer IT-sicherheitsmotivierte Änderungen sind und je später sie vorgeschlagen werden, desto weniger ökonomisch sinnvoll sind sie im Allgemeinen. Für den SuperMUC-Dienst ist insgesamt von vergleichsweise konstanten Assets – der Übergang von Betriebsphase 1 zu Betriebsphase 2 verändert die Sicherheitseigenschaften und -anforderungen nicht – und ebensolchen organisatorischen Randbedingungen auszugehen. Somit ist die vorrangige Zielsetzung für das SuperMUC-Risikomanagement, Beeinträchtigungen für Partnerorganisationen und Benutzer durch präventive Maßnahmen möglichst zuverlässig zu vermeiden, alle sicherheitsmotivierten Änderungen pragmatisch jedoch nur bei konkreten Bedrohungen durchzuführen, um unnötige Investitionskosten und mit der Maßnahme verbundenen Personalaufwand zu vermeiden.

Primär sind somit die folgenden Aspekte und Weiterentwicklungen der Risiken zu betrachten:

- Änderungen an der Motivation für und an der Vorgehensweise bei HPC-spezifischen Angriffen: Wie oben bereits erläutert wurde, stellt beispielsweise der Missbrauch von HPC-Ressourcen zur BitCoin-Generierung auf Basis kompromittierter Benutzerkennungen ein neues Angriffsmuster dar, das von der früher häufig zu beobachtenden Remote-Kompromittierung von Linux-Serverdiensten signifikant abweicht und entsprechend andere Präventions- und Detektionsmaßnahmen motiviert.
- Weiterentwicklung der eingesetzten Software und Sicherheitsmechanismen: Die zum Zugriff auf HPC-Ressourcen erforderliche Software wird kontinuierlich weiterentwickelt; Änderungen an der Grid-Middleware und die Möglichkeit zur SSH-Authentifizierung über X.509v3-Zertifikate sind zwei in diesem Kontext bereits diskutierte Beispiele. Ne-

ben der organisationsübergreifenden Abstimmung einzusetzender Verfahren und Softwareversionen sind analog zu anderen Diensten neu bekannt werdende Sicherheitslücken in der eingesetzten Software zu berücksichtigen.

- Sicherheitsvorfälle bei Partnersites und anderen HPC-Anbietern müssen als zuverlässige Indikatoren für zu erwartende Angriffe bzw. potentiell auch beim SuperMUC-Dienst analog vorhandene Verwundbarkeiten gewertet werden.

Die konkreten Arbeitsinhalte des Risikomanagements werden dabei stark vom nachfolgend vorgestelltem SuperMUC-Sicherheitsberichtswesen beeinflusst.

8.6.2.10. Sicherheitskennzahlen und Security-Reporting im SuperMUC-Szenario

Wie viele andere Organisationen hat das LRZ im Rahmen der Ausrichtung seiner ITSM-Prozesse an Standards und Best Practices damit begonnen, Kennzahlen für die Quantifizierung ausgewählter Eigenschaften zur Beurteilung der eigenen Prozesse zu konzipieren, zu erfassen und auszuwerten. Im Bereich Sicherheitsmanagement stehen diese Bemühungen jedoch noch am Anfang; die Einführung eines neuen Dienstes wie SuperMUC bietet deshalb eine günstige Gelegenheit, Sicherheitskennzahlen von Anfang an einzusetzen und parallel zum Dienst auf Basis der damit gesammelten Erfahrungen kontinuierlich zu erweitern und zu verbessern.

Wie bereits in Abschnitt 6.6 erörtert wurde, kann es weder eine einzige Kennzahl geben, die das Gesamtsicherheitsniveau beschreibt, noch existieren bislang organisationsübergreifend verbreitete Kennzahldefinitionen, die eine naheliegende Grundlage für die Anwendung z. B. im SuperMUC-Szenario darstellen. Neben einer reinen Beurteilung des Status Quo soll auch die langfristige Planung durch Sicherheitsberichte gezielt unterstützt werden. Im Folgenden werden deshalb exemplarisch für den SuperMUC-Dienst Sicherheitskennzahlen entwickelt, indem entsprechende Hypothesen aufgestellt und diese auf technische Systeme und geeignete Messpunkte abgebildet werden. Dabei werden verschiedene Themenbereiche – vom Systemmanagement über Intrusion Detection bis hin zu ITSM-Prozessen – abgedeckt, um die SuperMUC-Sicherheitseigenschaften von verschiedenen Perspektiven aus zu beleuchten. Daran anschließend wird skizziert, für welche Zielgruppen SuperMUC-bezogene Sicherheitsberichte erstellt werden sollten.

Alle nachfolgend formulierten Hypothesen beziehen sich auf die oben bereits diskutierten SuperMUC-Systemeigenschaften und die Einbettung des Dienstes in die am LRZ vorhandene Infrastruktur unter Berücksichtigung der erläuterten Sicherheitsziele. Die jeweils genannten Schwellenwerte sind Zielvorgaben, die im Vorfeld des Dienstbetriebs realistisch erscheinen und im Rahmen der kontinuierlichen Verbesserung auf Basis praktischer Erfahrungen ggf. verschärft oder gelockert werden müssen. Nach Themenbereichen strukturiert werden die folgenden Hypothesen für das SuperMUC-spezifische Security-Reporting vorgeschlagen, deren Zielsetzung und technische Realisierung unten vertieft werden:

- **Systemmanagement**:
  - Hypothese **SYS-1**: Zu jedem Zeitpunkt sind mindestens 98% der SuperMUC-Komponenten (Login-Nodes, Compute-Nodes, SuperMUC-Webserver, ...) auf einem Software-Update-Stand, der nicht älter als sieben Tage ist.

  - Hypothese **SYS-2**: Software-Updates werden nach ihrem Verfügbarwerden innerhalb von durchschnittlich drei Tagen eingespielt.
  - Hypothese **SYS-3**: Mindestens 80% aller verfügbaren Softwareupdates werden innerhalb von sieben Tagen eingespielt.
  - Hypothese **SYS-4**: Alle aktiven Compute-Nodes werden vom Managementsystem überwacht.
  - Hypothese **SYS-5**: Die Verfügbarkeit des Dienstes ist abgesehen von geplanten Wartungszeiträumen mindestens 97%.

- **Netzmanagement**:
  - Hypothese **NET-1**: Von außerhalb des MWN sind nur genau diejenigen TCP/IP-Ports auf SuperMUC-Komponenten erreichbar, die in der Soll-Spezifikation dokumentiert sind.
  - Hypothese **NET-2**: Das im Monatsmittel betrachtete Verhältnis von aus- zu eingehendem Datenverkehr variiert pro Jahr um weniger als 10%.

- **Identity Management**:
  - Hypothese **IDM-1**: Der Anteil von zertifikatsbasierten Authentifizierungen an allen Authentifizierungsvorgängen nimmt kontinuierlich zu.
  - Hypothese **IDM-2**: Der Anteil fehlgeschlagener Authentifizierungs- und Autorisierungsvorgänge liegt unter 2% der Gesamtnutzung.
  - Hypothese **IDM-3**: Die Anzahl der den SuperMUC-Dienst aktiv nutzenden Kennungen variiert im Monatsmittel betrachtet ungeachtet der Projektfluktuation um weniger als 10%.
  - Hypothese **IDM-4**: Die Supercomputer-Exportrestriktionen werden eingehalten, da Benutzer bestimmter Nationalitäten keinen Zugriff erhalten.

- **Intrusion Detection**:
  - Hypothese **IDS-1**: Zur Analyse von potentiellen Angriffen müssen weniger als 1% aller Protokolleinträge ausgewertet werden.
  - Hypothese **IDS-2**: Die Anzahl erkannter Angriffe weist zwischen den Berichtszeiträumen keine starken Schwankungen auf.
  - Hypothese **IDS-3**: Mehr als 99% aller Angriffsversuche folgen einer bekannten Angriffsart und werden entweder automatisiert behandelt oder bewusst ignoriert.
  - Hypothese **IDS-4**: Es gibt keine Verstöße gegen die Zweckbindung beim Zugriff auf Benutzerdaten.
  - Hypothese **IDS-5**: Mehr als 95% der SuperMUC-spezifischen Firewall-Regeländerungen werden automatisiert durchgeführt.

- **Sicherheitsvorfälle**:
  - Hypothese **SIR-1**: Pro Jahr ereignet sich maximal ein Sicherheitsvorfall, bei dem der Anwender root-Rechte erlangt, der manuell bearbeitet werden muss und dessen Bearbeitungsaufwand dabei unter 15 Personentagen liegt.

  - Hypothese **SIR-2**: Mit den lokal vorhandenen Detektionsmechanismen können alle Sicherheitsvorfälle erkannt werden, die auch aus externen Quellen gemeldet werden.

- **IT Service Management**:

  - Hypothese **ITSM-1**: Service-Desk-Anfragen von SuperMUC-Benutzern mit Bezug zur IT-Sicherheit machen weniger als 5% aller SuperMUC-Service-Desk-Anfragen aus.

  - Hypothese **ITSM-2**: Pro Monat müssen weniger als fünf IT-sicherheitsbedingte Changes durchgeführt werden.

Für jede Hypothese werden nun die entsprechenden Basiskennzahlen und abgeleiteten Kennzahlen mit ihren entsprechenden Messpunkten sowie die jeweils verfolgte Motivation erläutert:

- **Systemmanagement**:

  - Die Hypothesen SYS-1 bis SYS-3 betrachten verschiedene Aspekte des Software-Update-Managements unter Berücksichtigung der in der Praxis z. B. aufgrund von Hardware-Wartungsarbeiten unvermeidbar auftretenden Verzögerungen bei einzelnen Nodes. Zum einen können Nodes, die beispielsweise aufgrund von Hardwaredefekten temporär außer Betrieb sind, nicht sofort auf den aktuellen Softwarestand gebracht werden. Zum anderen stellen Software-Updates jedoch eine essentielle, in der Praxis äußerst bewährte Präventionsmaßnahme dar, deren zuverlässige zeitnahe Umsetzung stark betont werden soll. Neue Software-Updates werden zusammen mit dem Zeitpunkt, ab dem sie verfügbar sind, vom Configuration Management erfasst. Die SuperMUC-Systemmanagementwerkzeuge protokollieren, welche Updates zu welchem Zeitpunkt auf welchen Komponenten eingespielt werden. Die erforderlichen Kennzahlen können aus der Differenz der Anzahl der Komponenten, auf denen die Updates eingespielt wurden, zur Gesamtanzahl an Komponenten sowie aus den entsprechenden Zeitstempeln abgeleitet werden.

  - Die Hypothese SYS-4 zielt darauf ab, sicherzustellen, dass Compute-Nodes nicht versehentlich der Überwachung durch das Managementsystem entzogen werden. Die Überwachung einzelner Nodes kann beispielsweise bei bekannten Hardwaredefekten temporär deaktiviert werden, um unnötige Fehlermeldungen zu vermeiden; es darf jedoch nicht vergessen werden, sie nach Wiederinbetriebnahme auch wieder mithilfe des Managementsystems zu überwachen. Als Basiskennzahlen können die Anzahl der aktuell überwachten Compute-Nodes und die Anzahl der Compute-Nodes, für die Wartungsarbeiten geplant sind, ermittelt werden und der bekannten, pro SuperMUC-Betriebsphase konstanten Gesamtzahl an Compute-Nodes gegenübergestellt werden.

  - Die Hypothese SYS-5 fordert eine Beobachtung unerwarteter Nichtverfügbarkeitszeiträume, die beispielsweise durch Sicherheitsvorfälle oder ungeplant erforderlich werdende Wartungsarbeiten eintreten können. Die prozentuale Dienstverfügbarkeit ist eine abgeleitete Kennzahl, die unter Berücksichtigung geplanter Wartungsarbeiten direkt von den eingesetzten Monitoringsystemen bezogen werden kann.

- **Netzmanagement**:

  - Viele Angriffsmöglichkeiten für externe Angreifer bieten sich primär über weltweit erreichbare, IP-basierte Serverdienste. Das zur Systemhärtung eingesetzte Minimalitätsprinzip installierter Serverdienste lässt sich im Rahmen des Netzmanagements prüfen. Über den oben beschriebenen DFN-Service *Netzwerkprüfer* lassen sich offene TCP/IP-Ports automatisiert ermitteln und können ebenso automatisiert mit einer im Rahmen des Betriebskonzepts erarbeiteten Soll-Spezifikation abgeglichen werden. Als abgeleitete Kennzahl zur Überprüfung der Hypothese NET-1 dient die Anzahl der TCP/IP-Ports, die von außen erreichbar sind, obwohl sie nicht in der Soll-Spezifikation aufgeführt sind.
  - Die Netzverkehrsstatistik lässt Rückschlüsse auf möglicherweise missbräuchliche Systemnutzung zu. Die Hypothese NET-2 geht davon aus, dass trotz der unterschiedlichen wissenschaftlichen Projekte, die auf dem SuperMUC rechnen, das Verhältnis von aus- zu eingehendem Datenverkehr in etwa gleich bleibt: Wissenschaftler kopieren ihre Eingabedaten auf den SuperMUC und rufen die Ausgaben ihrer Programmläufe ab. Kippt dieses Verhältnis unerwartet, da beispielsweise in einem Monat erheblich mehr ausgehender Datenverkehr als sonst zu beobachten ist, sind nähere Analysen erforderlich, da beispielsweise ein erfolgreicher Angriff mit nachfolgender Datenausspähung zugrunde liegen könnte. Die zur Bestimmung des Verhältnisses aus ein- und ausgehendem Datenverkehr erforderlichen Daten werden von den Netzmanagementsystemen bereitgestellt. Der Verlauf dieser abgeleiteten Kennzahl muss in einem gleitenden Zeitfenster von jeweils insgesamt zwölf Monaten ausgewertet werden.

- **Identity Management**:
  - Latente Probleme beim Einsatz passwortbasierter Authentifizierung wie vergessene und von Angreifern ausgespähte Passwörter führen dazu, dass die organisationsübergreifenden HPC-Verbünde die Nutzung zertifikatsbasierter Authentifizierung propagieren. Die Hypothese IDM-1 soll die Beobachtung dieser Tendenz anregen, um langfristige Planungen bezüglich der zu unterstützenden Authentifizierungsverfahren zu ermöglichen. Ferner können sprunghafte Änderungen bei den praktisch genutzten Authentifizierungsverfahren ein Hinweis auf eine möglicherweise größere Anzahl kompromittierter Benutzerkennungen sein, die beispielsweise aus einem Sicherheitsvorfall bei anderen HPC-Sites resultiert. Das Identity-Management-System stellt entsprechende Zähler für jede Art von Authentifizierungsverfahren bereit, so dass der Anteil zertifikatsbasierter Authentifizierungen trivial abgeleitet werden kann.
  - Die Hypothese IDM-2 betrachtet fehlgeschlagene Loginversuche auf dem SuperMUC; aufgrund von Tippfehlern bei Passwörtern und anderen technischen Schwierigkeiten stellen im praktischen Betrieb nicht alle Fehlversuche einen Angriff dar. Steigt die Anzahl von Fehlversuchen jedoch überproportional an, muss untersucht werden, ob beispielsweise Brute-Force-Angriffe vorliegen, die durch zusätzliche Maßnahmen abgeschwächt werden sollten. Das Identity-Management-System liefert auch hierfür die entsprechenden Basiskennzahlen über erfolgreiche Logins bzw. Fehlversuche.
  - Aufgrund der konstanten Rechenkapazität wird im Rahmen der Hypothese IDM-3 davon ausgegangen, dass auch die Anzahl der den Dienst aktiv nutzenden Ken-

nungen in etwa konstant bleibt. Das Identity-Management-System kann analog zu den obigen Beschreibungen nicht nur die Anzahl der Logins pro Monat liefern, sondern auch Auskunft darüber erteilen, wie viele verschiedene Kennungen den Dienst im entsprechenden Zeitraum genutzt haben. Ein langfristiger Anstieg des Werts der Kennzahl deutet auf Defizite bei der Deprovisionierung von Kennungen hin, d. h. dass vergebene Berechtigungen möglicherweise nicht wieder zeitnah entzogen werden. Ein kurzfristiger sprunghafter Anstieg kann hingegen wiederum auf kompromittierte Benutzerkennungen hinweisen.

  - Die oben diskutierten, gesetzlich vorgeschriebenen Exportrestriktionen [BMBF11] verbieten Benutzern ausgewählter Nationalitäten den Zugriff auf HPC-Dienste wie SuperMUC. Die Nationalität von HPC-Benutzern wird am LRZ entweder manuell erfasst oder kann – insbesondere bei der automatisierten Übernahme von Grid-Kennungen – mit Einschränkungen aus den im Grid-User-Zertifikat gespeicherten Angaben ausgelesen werden. Als Basiskennzahl für die Hypothese IDM-4 wird die Anzahl der SuperMUC-berechtigten Kennungen verwendet, deren Besitzer einer der in den Exportrestriktionen genannten Nationalitäten angehören.

- **Intrusion Detection**:
  - Die Hypothese IDS-1 dient der Bewertung von Skalierbarkeit und Effizient der eingesetzten dynamischen Intrusion-Detection-Komponenten. Sie geht davon aus, dass nur ein Bruchteil aller Protokolleinträge sicherheitsrelevant ist und zur Erkennung akuter Angriffe ausgewertet werden muss. Die zur Bestimmung des Verhältnisses aus ausgewerteten zu insgesamt vorhandenen Protokolleinträgen wird von dem in Abschnitt 8.6.2.6 beschriebenen Gateway-Sensor zur Verfügung gestellt.
  - Bisherige Erfahrungen mit Angriffen auf HPC-Dienste deuten im monatlichen Mittel auf eine Gleichverteilung über die Zeit hin. Die Hypothese IDS-2 dient entsprechend der Prüfung auf auffällige Häufungen, die Indikatoren für neue oder stark geänderte Angreifermodelle sein können und möglicherweise Korrelationen mit besonderen Ereignissen erlauben, die die Attraktivität des SuperMUC-Dienstes für Angriffe signifikant beeinflusst haben. Die entsprechende Basiskennzahl kann vom zentralen SIEM-System übernommen und dem entsprechenden Wert des vorherigen Berichtszeitraums gegenübergestellt werden.
  - Die Hypothese IDS-3 zielt auf die Bewertung des erreichten Automatisierungsgrads beim Umgang mit Angriffsversuchen ab: Nur ein Bruchteil aller Angriffe soll eine manuelle Analyse und Einleitung von Gegenmaßnahmen erfordern; zudem müssen die IDS-Regelsätze zur Erkennung von Angriffen kontinuierlich auf dem aktuellen Stand gehalten werden. Die erforderliche Basiskennzahl über automatisiert behandelte Angriffsversuche wird vom SIEM-System bereitgestellt; sie muss in Relation zu den manuell behandelten Angriffsversuchen gestellt werden, deren Anzahl bislang ebenfalls nur manuell aus den entsprechenden Dokumentationsdatensätzen des operativen Sicherheitsmanagements entnommen werden kann.
  - Verstöße gegen die Zweckbindung beim Zugriff auf Benutzerdaten deuten auf das Fehlverhalten von Administratoren oder die Fehlkonfiguration z. B. des Backup-Dienstes hin. Ihre im Rahmen der Hypothese IDS-4 benötigte Anzahl kann den vom Datenschutz-Security-Framework vorgenommenen Protokolleinträgen entnommen werden.

  - Analog zu IDS-3 thematisiert die Hypothese IDS-5 den Automatisierungsgrad, in diesem Fall bezüglich der automatisierten Reaktionen auf erkannte Angriffe. Zu häufig erforderliche manuelle Firewall-Regeländerungen wären nicht nur mit entsprechendem Aufwand, sondern auch praktisch unvermeidlichen kleineren Verzögerungen verbunden, während denen die proaktiven Schutzmechanismen nicht adäquat konfiguriert sind. Die erforderlichen Basiskennzahlen können den Protokolleinträgen der dynamischen IDS-Auswertestation, die auch ans SIEM-System gemeldet werden, und den im ITSM-Werkzeug gespeicherten Change Records entnommen werden.

- **Sicherheitsvorfälle**:

  - Trotz aller präventiven Maßnahmen und automatisierten und somit zeitnahen Reaktionen können Sicherheitsvorfälle nicht gänzlich ausgeschlossen werden. Ein akzeptables Sicherheitsniveau gilt gemäß Hypothese SIR-1 als dann erreicht, wenn eine bestimmte Anzahl an Sicherheitsvorfällen pro Zeitraum nicht überschritten wird und dabei keinen Aufwand, der über den genannten Schwellenwert hinausgeht, verursacht. Die erforderlichen Basiskennzahlen können den in Abschnitt 8.6.2.7 vorgestellten Security-Incident-Records entnommen werden. Wird diese Hypothese praktisch widerlegt, so besteht dringender Handlungsbedarf bei der Verbesserung der Sicherheitsmaßnahmen.

  - Die Hypothese SIR-2 bildet das Ziel ab, die LRZ-seitig durch die verwendeten Detektionsmechanismen erzielte Erkennungsleistung so hoch zu halten, dass alle Sicherheitsvorfälle, die Informationen oder Beschwerden von außen verursachen, bereits bekannt sind. Nur von außen gemeldete Sicherheitsvorfälle sind somit ein Indikator für unzureichende präventive und detektierende Maßnahmen. Die als Basiskennzahl verwendete Anzahl nur extern gemeldeter Vorfälle wird im Rahmen von deren Bearbeitung manuell erfasst.

- **IT Service Management**:

  - Benutzeranfragen an den Service-Desk mit Bezug auf Themen der IT-Sicherheit sind zu einem gewissen Grad nicht unüblich, beispielsweise wenn vergessene Passwörter zurückgesetzt oder der Umgang mit zertifikatsbasierter Authentifizierung erläutert werden soll. Überproportional viele Anfragen zu diesen Themen können jedoch z. B. ein Anzeichen für die möglicherweise unbefriedigende Benutzerfreundlichkeit der eingesetzten Sicherheitsmechanismen sein, auf die mittelfristig geeignet reagiert werden muss. Die für die Hypothese ITSM-1 benötigten Basiskennzahlen können den Incident Records des ITSM-Werkzeugs entnommen werden, die dem Dienst SuperMUC zugeordnet sind und als sicherheitsspezifisch klassifiziert sind.

  - Die Hypothese ITSM-2 betrachtet Teilaspekte von SYS-1 bis SYS-3 und IDS-5 aus der Perspektive des IT Service Management. Eine zu große Anzahl an sicherheitsbedingt erforderlichen Changes ist ein Indikator für die mangelnde Reife und Stabilität der eingesetzten Softwarekomponenten oder deutet auf anhaltende Schwierigkeiten bei der adäquaten Konfiguration der Sicherheitsmechanismen hin. Die entsprechende Basiskennzahl kann den im ITSM-Werkzeug verwalteten Change Records entnommen werden.

Aus den genannten Kennzahlen kann eine Reihe von Key Performance Indicators bestimmt werden, die eine besondere Relevanz für mehrere der u. g. Zielgruppen für Sicherheitsberichte haben:

- **KPI-1**: Die Latenz beim Einspielen von Software-Updates ist ein Qualitätsmerkmal für die Zusammenarbeit mit dem SuperMUC-Systemhersteller, der auch mit dieser Aufgabe betraute Administratoren abordnet.
- **KPI-2**: Die Anzahl der unerwünscht von außen erreichbaren TCP/IP-Ports ist ein Qualitätsmerkmal für die Einhaltung der LRZ-internen Netz- und Sicherheitskonzepte.
- **KPI-3**: Verstöße gegen die Zweckbindung von Benutzerdaten sind ein Indikator für die Einhaltung des Datenschutzes und damit extern vorgegebener Compliance-Auflagen.
- **KPI-4**: Die Anzahl der manuell zu bearbeitenden Sicherheitsvorfälle ist ein Indikator für die Qualität der eingesetzten präventiven Sicherheitsmechanismen.
- **KPI-5**: Der Anteil sicherheitsspezifischer Benutzeranfragen ist ein Indikator für die Benutzerfreundlichkeit der umgesetzten Sicherheitsmaßnahmen.
- **KPI-6**: Der erreichte Automatisierungsgrad beim Umgang mit Angriffsversuchen ist ein Qualitätsmerkmal für die Zusammenstellung und Konfiguration der IDS-Komponenten.

Wie in Abschnitt 6.6.4 beschrieben und von dem in Abschnitt 7.3 spezifizierten Werkzeug unterstützt werden die Sicherheitskennzahlen zu Sicherheitsberichten aufbereitet; hierfür können rudimentär die folgenden Zielgruppen, Berichtsfrequenzen und -inhalte festgelegt werden:

- **SuperMUC-Betriebsgruppe**: Sicherheitsberichte für die SuperMUC-Administratoren sind wöchentlich zu generieren und enthalten alle Kennzahlen im Detail; neben Diagrammen werden entsprechend auch Tabellen mit den genauen Werten vorgelegt. Der Sicherheitsbericht enthält für alle Hypothesen auch deren Interpretationsregeln und die mit vorhergesehenen potentiellen Abweichungen verbundenen Handlungsanweisungen.
- **Abteilungsbesprechungen**: Zur Diskussion in den regelmäßigen Abteilungsbesprechungen sind zweiwöchentlich Sicherheitsberichte vorzulegen, die jedoch auf Hypothesen und Kennzahlen mit vom erwarteten Verhalten abweichenden Ergebnissen beschränkt sind. Ihnen werden wiederum die Interpretationsregeln und Handlungsanweisungen beigefügt.
- **Arbeitskreis Sicherheit**: Der LRZ-Sicherheitsarbeitskreis ist monatlich mit Sicherheitsberichten zu versorgen. Dabei sind jedoch nicht die einzelnen Basiskennzahlen, sondern nur die hypothesenbezogenen abgeleiteten Kennzahlen relevant. Die Aufbereitung erfolgt in Form von Diagrammen, d. h. die einzelnen exakten Werte werden nur auf Nachfrage zur Verfügung gestellt; auch die Interpretationsregeln und Handlungsanweisungen werden beigefügt.
- **LRZ-Leitung**: Der LRZ-Leitung gegenüber ist quartalsweise in einer mündlichen Präsentation zu berichten; Gegenstand des Berichts sind die KPIs, die zu mündlich erläuterten Diagrammen aufbereitet werden, sowie ggf. einzelne Sicherheitsvorfälle, die manuell behandelt werden mussten.
- **LRZ-Jahresbericht**: In den jährlichen LRZ-Bericht, der auch frei zugänglich im Internet veröffentlich wird, fließen ausgewählte KPIs ein, die zu Diagrammen mit manuell erstellten schriftlichen Erläuterungen aufbereitet werden.

- **SuperMUC-Hersteller**: Dem Systemhersteller werden monatliche Sicherheitsberichte vorgelegt, die nur die systemspezifischen Kennzahlen mit exakten Werten, Diagrammen, Interpretationsregeln und Handlungsanweisungen enthalten. Kennzahlen aus anderen Bereichen werden bei Bedarf in geeigneter Form nachgetragen.
- **GCS-Verbund**: Zur Abstimmung im Rahmen organisationsübergreifender Verbünde wie GCS werden die definierten KPIs in quartalsweisen Berichten herangezogen. Abweichungen vom erwarteten Verhalten werden benannt, ohne LRZ-interne Details offenzulegen. Die Ergebnisse werden den Sicherheitsberichten der Partnerorganisationen gegenübergestellt, um erforderliche Anpassungen aufeinander abstimmen zu können.

Durch diese Berichtsstruktur wird sichergestellt, dass die hier ermittelten dienstspezifischen Sicherheitskennzahlen analog zu denen anderen Dienste regelmäßig ausgewertet werden. Bei jeder neu definierten Hypothese ist am Anfang unsicher, ob die vorgegebenen Schwellenwerte praktisch einhaltbar sind und eine auch langfristig hohe Aussagekraft gegeben ist. Sie werden deshalb auf Basis praktischer Erfahrungen im Laufe der Zeit kontinuierlich angepasst, um sicherheitsrelevante Abweichungen fokussiert erkennen zu können. Mittelfristig ist dabei insbesondere eine Ergänzung um weitere Hypothesen und Indikatoren interessant, die auch bei anderen HPC-Anbietern verwendet werden und somit einen organisationsübergreifenden Vergleich und konzertierte Planungen ermöglichen.

8.7. Zentrale Aspekte in den weiteren Lebenszyklusphasen

In den obenstehenden Abschnitten wurden nach einer Schilderung der Ausgangssituation und Ziele die technischen und prozessualen Sicherheitskonzepte auf Basis ausgewählter Security-Frameworks und unter Einsatz der in dieser Arbeit konzipierten Managementwerkzeuge dargelegt, wie sie gemäß dem in Kapitel 5 spezifizierten Lebenszyklus von Frameworkinstanzen als Ergebnis der auf die initiale Auswahl von Security-Frameworks folgenden Customizingphase vorzulegen sind. Im Folgenden werden alle weiteren Lebenszyklusphasen – von der Implementierung über den Betrieb bis hin zur Planung der Außerbetriebnahme – betrachtet. Da es sich um ein fiktives Anwendungsbeispiel handelt, dessen Inhalte nicht in vollem Umfang und erst nach Abschluss der vorliegenden Arbeit für den realen SuperMUC-Dienst am LRZ umgesetzt werden, können keine konkreten realen Erfahrungen retrospektiv analysiert werden. Stattdessen werden a priori ausgewählte zentrale Aspekte und Schwerpunkte jeder Lebenszyklusphase skizziert.

8.7.1. Implementierungs- und Migrationsaspekte im SuperMUC-Szenario

Die Komplexität des Dienstes SuperMUC, dessen Hardwarezusammenstellung eine Sonderanfertigung ist, führt unter anderem dazu, dass die aus dem Software Engineering bekannte, klassische Trennung zwischen weitgehend identischen Entwicklungs-, Test-, Integrations- und Produktivumgebungen nicht realisiert werden kann. Systemnahe Implementierungen, wie sie beispielsweise für das Linux-Kernel-Security-Framework erforderlich sind, müssen deshalb in herkömmlichen Entwicklungsumgebungen erarbeitet und getestet werden; sie können dann im Rahmen der SuperMUC-Betriebsphasenübergänge zusammen mit den anderen Konfigurationsänderungen getestet werden, wobei diese Testumgebung später fließend in die Produktivumgebung übergeht. Dieser Übergang wird dadurch erleichtert, dass Benutzergruppen

stufenweise auf neu hinzukommende bzw. umkonfigurierte Komponenten zugelassen werden, so dass zunächst Rückmeldungen von wohlgesonnenen Benutzern eingeholt und eventuell verbleibende Fehler noch im bereits eingeschränkt laufenden Betrieb ausgemerzt werden können.

Der Mangel an SuperMUC-spezifischen Testumgebungen wirkt sich jedoch auch auf die übrigen Dienste aus, so dass beispielsweise die netzbasierten Schutzmechanismen nicht zunächst in einer Laborumgebung getestet werden können, sondern sofort produktiv konfiguriert werden müssen. Im Allgemeinen ergeben sich hieraus keine Einschränkungen, da die auch für andere Dienste eingesetzten und zum Teil den Kunden im MWN angebotenen Sicherheitsmaßnahmen auf die dynamische Erweiterung ausgelegt sind. Dennoch muss in dieser Konstellation berücksichtigt werden, dass beispielsweise bestimmte Formen von Lasttests zu Einschränkungen des Produktivbetriebs anderer Dienste führen könnten, die durch sorgfältige Planung vermieden oder, sofern sie zwingend z. B. für die Abnahme des gesamten SuperMUC-Systems erforderlich sind, auf geeignete Zeitpunkte gelegt werden müssen.

Durch die von den eingesetzten Security-Frameworks gebotene Funktionalität erweitert sich implizit auch der Umfang der Abnahmekriterien für den gesamten SuperMUC-Dienst; beispielsweise müssen sicherheitsspezifische Testfälle definiert werden, durch die u. a. die verschiedenen Authentifizierungsmethoden systematisch getestet und die Nutzung des Dienstes durch verschiedene Nutzergruppen mit unterschiedlichen Berechtigungen nachgestellt werden.

In der geschilderten Ausprägung fallen folgende Implementierungsarbeiten an, die über eine Konfiguration der am LRZ bereits verfügbaren Sicherheitsmaßnahmen hinausgehen:

- Für die Erfassung der Sicherheitskennzahlen müssen Messagenten implementiert werden, die Basiskennzahlen abrufen und in das in Abschnitt 7.3 spezifizierte Werkzeug übernehmen.
- Für die dynamische Steuerung der IDS-Komponenten werden die in Abschnitt 8.6.2.6 beschriebenen Schnittstellenkomponenten zur Konvertierung von Protokolleinträgen und zur Vorfilterung von IDMEF-Meldungen benötigt.
- Für den Einsatz des Datenschutz-Security-Frameworks werden ein XACML PDP, der Obligation Monitor und der Policy Distribution Point benötigt; dabei können bestehende Implementierungen genutzt werden, deren Schnittstellen jedoch szenarienspezifisch angesteuert werden müssen.
- Für das Linux-Kernel-Security-Framework müssen die benötigten Filesystem-Hooks mit ihrer Anbindung an den XACML PDP implementiert werden.

Für den Betrieb der Komponenten des Datenschutz-Security-Frameworks sowie die IDS-Gateways wird geeignet leistungsfähige Hardware benötigt; zwar können virtuelle Maschinen eingesetzt werden, dennoch sind entsprechende Maßnahmen zur Kapazitätsplanung und ggf. Beschaffung frühzeitig zu berücksichtigen (vgl. auch Abschnitt 8.8). Die Messagenten für Sicherheitskennzahlen und das Linux-Kernel-Security-Framework sind auf bereits vorhandenen Maschinen einzusetzen, verursachen dabei keinen signifikanten Ressourcenaufwand und müssen deshalb bei der in der Implementierungsphase anfallenden Planung der zum späteren Betrieb erforderlichen Hardwareressourcen nicht näher betrachtet werden.

8.7.2. Aspekte der Inbetriebnahme von Security-Frameworks im SuperMUC-Szenario

Dadurch, dass mangels einer separaten Testumgebung die meisten der eingesetzten Sicherheitsmechanismen bereits von Anfang an in der Produktivumgebung konfiguriert und auch entsprechend getestet werden müssen, reduziert sich implizit der in dieser Lebenszyklusphase erforderliche Aufwand zu Lasten stärkerer Abhängigkeiten und höherer Risiken in der vorhergehenden Implementierungsphase.

Zu den in dieser Phase durchzuführenden Initialparametrisierungen gehören insbesondere

- die Formulierung der LRZ-seitig vorgegebenen XACML-Policies für das Datenschutz-Security-Framework, so dass beispielsweise Administratoren nur dann auf Benutzerdateien zugreifen dürfen, wenn diese mit einer expliziten Zweckbindung freigegeben wurden;
- die Konfiguration der Login-Nodes, so dass die erforderlichen Authentifizierungsverfahren unterstützt und die grundlegende Autorisierung zur Nutzung des SuperMUC-Dienstes im Zusammenspiel mit dem I&AM-System durchgeführt wird;
- die Übernahme von sicherheitsspezifischen Parametern vom SuperMUC-Vorgängersystem und deren Anpassung auf Basis des Betriebskonzepts, beispielsweise die bereits bislang genutzten Firewall-Regelsätze.

Im Rahmen der Abnahme des Systems müssen das Erreichen der oben beschriebenen Ziele und die Funktionalität sowohl der implementierten Sicherheitsmechanismen als auch der an den SuperMUC angepassten, bereits vorhandenen Sicherheitsdienste überprüft werden. Zu diesem Zweck müssen beispielsweise die auch regelmäßig im laufenden Betrieb vorgesehenen, in Abschnitt 8.6.2.4 beschriebenen Maßnahmen wie Penetrationstests angewendet werden. Die weiteren Migrations- und Inbetriebnahmeschritte umfassen den sukzessiven Umzug ausgewählter Benutzer und Projekte vom SuperMUC-Vorgängersystem und die Freigabe des Systems, so dass auch neue Projekte, die auf dem SuperMUC gerechnet werden sollen, beantragt und angelegt werden können.

8.7.3. Betriebs-, Überarbeitungs- und Außerbetriebnahmeaspekte im SuperMUC-Szenario

Die **Betriebsphase** mit ihren vorgesehenen Wartungsintervallen umfasst die kontinuierliche praktische Umsetzung und Verbesserung der in den Abschnitten 8.6.1 und 8.6.2 spezifizierten Managementprozesse. Sie ist durch die regelmäßige Durchführung von proaktiven Maßnahmen wie Penetrationstests und die kontinuierliche Anpassung der Detektionsmechanismen an neue und veränderte Angriffsvarianten geprägt; das für den SuperMUC-Dienst eingeführte Sicherheitsberichtswesen unterstützt zudem das Vorgehen beim Identifizieren und Planen technischer und organisatorischer Verbesserungsmaßnahmen.

Für die **Überarbeitungsphase** können naturgemäß a priori keine konkreten Inhalte geplant werden, die darüber hinausgehen, was in Abschnitt 8.5.2.1 bereits für die späteren SuperMUC-Betriebsphasenübergänge konzipiert wurde, da die in Abschnitt 5.9 zusammengestellten möglichen szenarienspezifischen Auslöser für größere Überarbeitungen – beispielsweise veränderte Randbedingungen oder negative Erfahrungen mit Teilen von Security-Frameworks – noch

nicht vorliegen können. Prinzipiell bietet sich jedoch eine enge Verzahnung größerer Änderungen an Security-Frameworks und den weiteren eingesetzten Schutzmechanismen mit den Übergängen zwischen den SuperMUC-Betriebsphasen an, da hierbei mit hoher Wahrscheinlichkeit Systemrekonfigurationen erforderlich werden, die zu Einschränkungen im Dienstbetrieb führen und somit auch für systemnahe Arbeiten an den Sicherheitsmechanismen genutzt werden können.

Einerseits durch die technologische Weiterentwicklung bei Prozessoren und Speicherkomponenten bedingt und andererseits aufgrund des begrenzten Investitions- und Betriebsbudgets steht von Anfang an fest, dass der Dienst SuperMUC nach einer gewissen Laufzeit wieder außer Betrieb genommen bzw. durch in dann leistungsfähigeres Nachfolgesystem abgelöst werden soll. Bereits im Kontext des SuperMUC-Risikomanagements wurden die daraus resultierenden Auswirkungen auf die Beurteilung sicherheitsspezifischer Änderungen oder Erweiterungen am Gesamtsystem unter Berücksichtigung der Restlaufzeit diskutiert. Im Kontext der Außerbetriebnahme von Security-Frameworks oder deren Anpassung an Nachfolgesysteme ist grundlegend davon auszugehen, dass insbesondere die vom Framework für föderiertes Sicherheitsmanagement vorgesehenen Komponenten beibehalten werden können, da sie auch im Rahmen anderer Dienste genutzt werden und somit auch auf zukünftige HPC-Systeme angewendet werden können. Auch die im Rahmen des Datenschutz-Security-Frameworks implementierten Komponenten können auf weitere Dienste und somit auch auf ein Nachfolgesystem übertragen werden. Eine Besonderheit weist somit lediglich das sehr systemnahe Linux-Kernel-Security-Framework auf; seine Implementierung kann nur dann angepasst werden, wenn das Nachfolgesystem mit ähnlichen Betriebssystem- und Softwarekonfigurationen aufgebaut wird. Falls dies nicht der Fall sein sollte, müssten andere Systemschnittstellen zur Umsetzung der vom Datenschutz-Security-Framework verwalteten Policies geschaffen werden.

Einige sicherheitsrelevante Datenbestände müssen auch über die Außerbetriebnahme des SuperMUC hinaus beibehalten werden; beispielsweise müssen Autorisierungsdaten für den Zugriff auf archivierte Projektdateien aufbewahrt werden, um den Nutzern auch später noch Zugang zu genau ihren eigenen Datenarchiven zu ermöglichen.

8.8. Betrachtung von Investitions- und Betriebsaufwand im SuperMUC-Szenario

Die im Kontext des Risikomanagements in Abschnitt 6.3.3 betrachtete Regel, dass die Kosten für technische und organisatorische Sicherheitsmaßnahmen zur Risikoreduktion die Höhe erwarteter Schäden aus ökonomischer Perspektive auf keinen Fall übersteigen soll, kann auch im SuperMUC-Szenario angewendet werden, da anders als z. B. in militärischen HPC-Anwendungsszenarien ein regulärer Schutzbedarf der verarbeiteten Informationen angenommen werden kann. Im Folgenden werden fokussiert nicht die Gesamtkosten für den SuperMUC-Dienst, sondern nur die Investitions- und Betriebskosten für die im Rahmen der drei ausgewählten Security-Frameworks eingesetzten Sicherheitsmaßnahmen betrachtet. In Relation zu den Anschaffungs- und Betriebskosten für den gesamten SuperMUC-Dienst, zu denen auch die vom LRZ gestellten SuperMUC-Administratoren gezählt werden müssen und die im höheren achtstelligen Euro-Bereich liegen, zeigt sich dabei jedoch, dass die sicherheitsspezifischen Ausgaben nur einen Bruchteil der Gesamtkosten für die Bereitstellung und Pflege des Dienstes ausmachen.

Im Folgenden wird vereinfachend nur zwischen Hard-/Softwarekosten und Personal- bzw. Projektkosten differenziert; zudem wird die Verteilung zwischen Investitions- bzw. Einführungskosten und laufenden Betriebskosten betrachtet. Alle Angaben zum Personalaufwand sind Schätzwerte auf Basis von Betriebserfahrungen mit früheren und ähnlichen Diensten und unterliegen der damit verbundenen Unschärfe. Bei Preisangaben zu bereits existierenden und im Rahmen des Szenarios genutzten LRZ-Sicherheitsdiensten wurden an den LRZ-Dienstleistungskatalog angelehnte Angaben verwendet und aufgerundet, um Preissteigerungen im Betriebszeitraum zu berücksichtigen; in der dabei zugrunde gelegten Vollkostenrechnung sind Personal- und Verbrauchskosten, z. B. für Strom und Wartungsverträge, bereits enthalten und werden nicht separat aufgeführt.

Bezüglich der **Hard- und Softwarekosten** ist zwischen neu anzuschaffender Hardware, dediziert zu betreibenden Systemen, Lizenzgebühren und Implementierungskosten für szenarienspezifische Entwicklungen zu unterscheiden:

- **Hardwareanschaffung**: Zu den Hardwareanschaffungen wird die Bereitstellung von physischen Servern, Appliances und zusätzlichen Ressourcen für den Betrieb virtueller Maschinen gerechnet, wobei im Allgemeinen implizit davon ausgegangen wird, dass sämtliche Komponenten zur Sicherstellung der Ausfallsicherheit doppelt ausgelegt werden. Dabei wird zum einen angenommen, dass am LRZ bereits vorhandene, mandantenfähige Sicherheitsmechanismen wie die Firewalls noch ausreichende Kapazitäten aufweisen; zum anderen werden auch Komponenten wie die Logging-Server, die im Rahmen des SuperMUC-Dienstes ausgebaut, aber nur zu einem kleinen Teil sicherheitsspezifisch genutzt werden, und Maschinen für den Betrieb der dynamischen IDS-Rekonfiguration und der Sicherheitskennzahlenerfassung, die auch im Kontext anderer LRZ-Dienste genutzt werden können, nicht explizit betrachtet.

  Aufgeschlüsselt nach den drei Security-Frameworks ergibt sich der folgende Bedarf:

  - Im Rahmen des Security-Frameworks für föderiertes Sicherheitsmanagement werden wie oben erläutert ausschließlich bereits vorhandene Schutzmechanismen verwendet und lediglich SuperMUC-spezifisch konfiguriert. Damit verbundene Anschaffungen umfassen konkret die folgenden beiden Positionen:
    * Die Nutzung der Firewalls, die den Zugang zum SuperMUC-spezifischen Webserver sowie zu den Login-Nodes absichern, ist mit Einrichtungskosten in Höhe von 250 Euro verbunden.
    * Zur besseren Lastverteilung und weiteren Erhöhung der Ausfallsicherheit wird ein weiteres Replikat des LDAP-basierten Authentifizierungs- und Autorisierungsservers, der Bestandteil des Identity-Management-Systems ist, aufgebaut; wie für andere Replika wird hierfür eine virtuelle Maschine genutzt, deren Einrichtungskosten bei 100 Euro liegen.
  - Für das Datenschutz-Security-Framework werden die folgenden Komponenten benötigt:
    * Der Betrieb des Obligation Monitors, des XACML PDPs und des Privacy Policy Distribution Points werden aus Redundanzgründen zwei virtuelle Maschinen benötigt, deren Einrichtungskosten somit bei 200 Euro liegen.
    * Für die Speicherung der XACML-Policies wird eine Datenbankinstanz benötigt, deren Bereitstellung 50 Euro kostet.

Die Self-Service-Funktionen des Datenschutz-Security-Frameworks werden in den SuperMUC-Webserver integriert und sind somit mit keinen separaten Hardwarekosten verbunden.

– Das Linux-Kernel-Security-Framework kommt auf den SuperMUC-Komponenten zum Einsatz und benötigt somit keine eigene Hardware.

- **Hardwarebetrieb**: Die Betriebskosten sind analog zu den Beschaffungskosten für die o. g. Komponenten zu betrachten:
  - Die jährlichen Betriebskosten für die Firewall betragen 900 Euro.
  - Jede virtuelle Maschine kostet unter der Annahme einer Ausstattung mit den derzeit üblichen Ressourcen (2 CPUs, 4 GB RAM, 30 GB NAS-Speicher, Betriebssystem Linux) jährlich 600 Euro. Für alle drei virtuellen Maschinen fallen somit jährlich 1.800 Euro Betriebskosten an.
  - Für den Betrieb der Datenbankinstanz sind jährlich 100 Euro zu veranschlagen.
- **Lizenzgebühren**: Im SuperMUC-Szenario fallen keine zusätzlichen Lizenzgebühren für sicherheitsspezifische Hard- und Software an: Die Lizenzkosten z. B. für die Firewall- und Datenbankmanagementwerkzeuge sind bereits in den o. g. Vollkosten für den laufenden Betrieb enthalten; ansonsten kommen ausschließlich Open-Source-Softwarepakete und Eigenentwicklungen zum Einsatz, für die keine Lizenzkosten anfallen.
- **Softwareimplementierung**: Da die Entwicklung der entsprechenden Teile der Security-Frameworks und Schnittstellenkomponenten vom LRZ selbst auf Basis von Open-Source-Softwarepaketen durchgeführt wird, fallen keine Kosten für Softwareentwicklung durch Dritte oder für verwendete Entwicklungsumgebungen und Funktionsbibliotheken an. Der damit verbundene Personalaufwand wird unten betrachtet.

Somit sind für die Hardwareanschaffung insgesamt 600 Euro zu veranschlagen; hinzu kommen jährliche Betriebskosten in Höhe von 2.800 Euro. Die Gesamtkosten liegen bei einer angenommenen Betriebsdauer von sechs Jahren somit bei 17.400 Euro.

Wie bei den hard- und softwarebezogenen Aufwendungen muss auch bezüglich des **Personalaufwands** zwischen einmaligen und laufenden Kosten differenziert werden. An **einmaligen Aufwendungen** sind zu betrachten:

- **Softwareimplementierung**: Im Rahmen der Instanziierung des Datenschutz-Security-Frameworks und des Linux-Kernel-Security-Frameworks fallen Softwareentwicklungsarbeiten an, die auf Basis ihrer Schnittstellen auch aufeinander abgestimmt werden müssen:
  - Für das Linux-Kernel-Security-Framework müssen die Filesystem-Hooks mit ihrer Schnittstelle zum XACML PDP implementiert und getestet werden. Hierfür wird ein Aufwand von 20 Personentagen veranschlagt.
  - Für die initiale Formulierung der Datenschutz-Policies in XACML wird ein Aufwand von 5 Personentagen angenommen, der bereits den Einarbeitungsaufwand in die Konzepte und den Umgang mit XACML-Policyeditoren beinhaltet.

  - Zur Integration der Datenschutz-Self-Service-Funktionalität in den SuperMUC-Webserver, über den sich Benutzer über die Einhaltung ihrer Datenschutzanforderungen informieren können, werden weitere 5 Personentage Implementierungsaufwand berücksichtigt.
  - Zur szenarienspezifischen Umsetzung von XACML-Obligations durch die entsprechende Monitoringkomponente, die im Wesentlichen aus dem zeitgesteuerten Entfernen von Dateien und Protokolleinträgen besteht, werden ebenfalls 5 Personentage veranschlagt.

  Explizit nicht betrachtet wird der Implementierungsaufwand für die Auswertestation mit der Funktion zur dynamischen IDS-Rekonfiguration und für das Werkzeug zur Erfassung und Aufbereitung von Sicherheitskennzahlen als Ganzes, da diese nicht nur für den SuperMUC-Dienst entwickelt und eingesetzt werden. Ebenso wird davon ausgegangen, dass Security-Framework-Komponenten wie der Obligation Monitor verfügbar sind und lediglich mit geringem Konfigurationsaufwand wie unten beschrieben eingesetzt werden können. Es fallen jedoch die folgenden SuperMUC-spezifischen Implementierungsaufgaben an:

  - Für die dynamische IDS-Rekonfiguration sind die folgenden einmaligen Arbeiten durchzuführen:
    * Die beiden Sensor-Gateways zur Auswertung der Protokolleinträge und zur Vorfilterung von IDMEF-Nachrichten müssen implementiert und getestet werden. Hierfür werden jeweils 10 Personentage, insgesamt also 20 Personentage veranschlagt.
    * Es muss ein initialer Regelsatz für die Steuerung der Dynamikeigenschaften, der auf die im SuperMUC-Szenario vorhandenen Sensoren und Reaktionskomponenten eingeht, erstellt und getestet werden. Hierfür werden 5 Personentage angesetzt.
  - Analog dazu fallen im Kontext der Erhebung und Auswertung der Sicherheitskennzahlen die folgenden einmaligen Aufwendungen an:
    * Die Erfassung der Basiskennzahlen muss durch die Adaption vorhandener, generischer Messagenten implementiert werden, so dass die entsprechenden Quellsysteme wie das Identity-Management-System ausgelesen werden können. Dafür werden 5 Personentage veranschlagt.
    * Die in Abschnitt 8.6.2.10 definierten Hypothesen und ihre Abbildungen auf abgeleitete Kennzahlen und Basiskennzahlen müssen in das Kennzahlenmanagementwerkzeug eingepflegt werden. Hierfür wird ein Aufwand von 2,5 Personentagen geschätzt.
    * Ebenso müssen die regelmäßig automatisiert zu erstellenden Sicherheitsberichte für die definierten Zielgruppen konfiguriert werden; dies wird mit weiteren 2,5 Personentagen angesetzt.

- **Anpassung existierender Sicherheitsmechanismen**: Neben den oben genannten Implementierungsarbeiten, die in neuen Systemen bzw. neuen Modulen für existierende Systeme münden, müssen auch Konfigurationsanpassungen an bereits existierenden

Sicherheitsmechanismen vorgenommen werden. Entsprechende Arbeiten an Sicherheitsmechanismen, die im LRZ-Dienstleistungskatalog verzeichnet sind, beispielsweise an den Firewalls, sind bereits durch die Vollkostenrechnung bei der Bereitstellung abgedeckt. Somit verbleiben die folgenden Positionen:

- Das Identity-Management-System muss erweitert werden, so dass einerseits SuperMUC-Zugangsberechtigungen und weitere Autorisierungsinformationen wie CPU- und Speicherkontingente zentral verwaltet werden können und andererseits die zusätzlich benötigten Authentifizierungsverfahren wie X.509v3-Zertifikate für SSH-Verbindungen unterstützt werden. Der Aufwand hierfür wird mit 20 Personentagen veranschlagt.
- Die im Rahmen des GIDS-Projekts entwickelte Angriffserkennungssensorik muss rekonfiguriert werden, so dass einerseits die am SuperMUC-Dienst beteiligten Ressourcen mit überwacht werden und andererseits entsprechende Sicherheitsmeldungen an die Auswertestation propagiert werden. Dabei ist von einem Aufwand von 2 Personentagen auszugehen.

Laufender Personalaufwand fällt hingegen anteilig in allen von den ITSM- und Sicherheitsmanagement abgedeckten Prozessen an; hervorzuhebende Schwerpunkte sind dabei:

- **Bearbeitung von Sicherheitsvorfällen**: Wie bei der Diskussion der Hypothese SIR-1 dargelegt wurde, kann das Eintreten von Sicherheitsvorfällen trotz aller präventiven Maßnahmen und schneller, teilautomatisierter Reaktionen nicht ausgeschlossen werden. Als Zielsetzung wird von einem jährlichen Maximalaufwand von 15 Personentagen ausgegangen, der in die Aufwandsbestimmung einfließt.
- **Monitoring und Verbesserung der technischen Sicherheitskonfiguration**: Neben den technischen Überwachungssystemen müssen auch die Sicherheitsberichte durch die entsprechenden Zielgruppen regelmäßig ausgewertet werden und laufende Anpassungen der Sicherheitsmechanismen durchgeführt werden; hierzu zählen beispielsweise die Spezifikation und Evaluation neuer Angriffserkennungsregeln und ausschließlich sicherheitsspezifische Softwareaktualisierungen. Insgesamt wird ein jährlicher Aufwand von 30 Personentagen angenommen.
- **Konzeption und Dokumentation**: Die bestehenden Sicherheitskonzepte müssen im Einklang mit den o. g. technischen Verbesserungen regelmäßig überarbeitet werden; ebenso sind die SuperMUC-spezifischen sicherheitstechnischen Arbeiten geeignet zu dokumentieren. Hierfür werden weitere 20 Personentage pro Jahr angesetzt.
- **Kontinuierliche Prozessverbesserung**: Neben den technischen Sicherheitskonzepten müssen auch die Managementprozesse und ihre Werkzeugunterstützung fortlaufend weiterentwickelt werden; dieser Position sind beispielsweise auch die Bewertung der bereits eingesetzten Sicherheitskennzahlen, die Spezifikation neuer Hypothesen und die Überarbeitung der Sicherheitsberichte zuzuordnen. Der jährliche Aufwand dafür wird ebenfalls mit 20 Personentagen veranschlagt.

Somit ergeben sich mit 92 Tagen einmaligen Personalaufwands und jährlich zusätzlich anfallenden 85 Personentagen somit über sechs Jahre Betriebsdauer betrachtet geschätzte Aufwendungen in Höhe von 602 Personentagen, denen die üblichen Zuschläge für Urlaub etc. zugerechnet werden müssen; folglich kann davon ausgegangen werden, dass im Projekt- und

Investitionskosten			**Betriebskosten**	
Firewall-Nutzung	250 €		Firewall-Nutzung	900 €
Server (LDAP-Replikat)	100 €		3 Server	1.800 €
2 Server (Datenschutz-SF)	200 €		Datenbankinstanz	100 €
Datenbankinstanz	50 €			
			Summe (pro Jahr)	2.800 €
Summe (Gesamtlaufzeit)	**600 €**		**Summe (Gesamtlaufzeit)**	**16.800 €**
Summe Investitions- und Betriebskosten:		**17.400 €**		

Einmaliger Personalaufwand (in Personentagen)			**Laufender Personalaufwand (in Personentagen)**	
Implementierung Linux-Kernel-SF	20		Bearbeitung von Sicherheitsvorfällen	15
Initiale Formulierung XACML-Policies	5		Monitoring und technische Verbesserungen	30
Implementierung Datenschutz-Self-Services	5		Konzeption und Dokumentation	20
Implementierung XACML-Obligations	5		Kontinuierliche Prozessverbesserung	20
Implementierung Sensor-Gateways	20			
Initiale IDS-Regelsätze	5			
Adaption von Messagenten	5			
Implementierung von Hypothesen und KPIs	2,5			
Implementierung von Sicherheitsberichten	2,5			
Anpassungen Identity-Management-System	20			
Anpassungen GIDS-Sensor	2			
			Summe (pro Jahr)	85
Summe (Gesamtlaufzeit)	**92**		**Summe (Gesamtlaufzeit)**	**510**
Summe Personalaufwand:		**602 Personentage**		

Abbildung 8.10.: Übersicht über Kosten und Personalaufwand im Anwendungsbeispiel

Betriebszeitraum das Äquivalent einer halben Personalstelle für SuperMUC-spezifische Sicherheitsaufgaben bereitgestellt werden muss. Aufgrund der fachlichen Spezialisierung verteilt sich dieser Aufwand jedoch auf mehrere Personen und lässt sich nicht einem einzigen, dafür dedizierten Mitarbeiter zuordnen.

Insgesamt fallen die geschätzten, für das LRZ anfallenden SuperMUC-sicherheitsspezifischen Betriebskosten, die in Abbildung 8.10 zusammengefasst sind, mit unter 20.000 Euro für Hard- bzw. Software und rund 600 Tagen Personalaufwand über einen Zeitraum von sechs Jahren relativ gering aus und sind mit anderen Diensten vergleichbar.

Aus dem Einsatz von Security-Frameworks ergeben sich dabei im Wesentlichen erhebliche Einsparungen beim Personalaufwand für die Erstellung des SuperMUC-Gesamtsicherheitskonzepts; durch die weitgehende, erfolgreiche Integration in die vorhandene Infrastruktur und die damit verbundene Nutzung bereits vorhandener Sicherheitsmaßnahmen fällt zudem nur beim Datenschutz-Security-Framework und der damit verbundenen Schnittstelle zum Linux-Kernel-Security-Framework Einarbeitungsaufwand in neue Konzepte und Softwarewerkzeuge an.

8.9. Bewertung der vorgestellten Lösung für das SuperMUC-Szenario

Abschließend soll die für den SuperMUC-Dienst konzipierte Lösung nun bewertet werden. Da es sich einerseits um eine sehr spezifische und somit einzigartige Kombination aus Dienst und Umfeld handelt und andererseits keine in ihrer thematischen Breite und bezüglich des Detailgrads vergleichbaren Dokumentationen anderer HPC-Installationen verfügbar sind, kann keine vergleichende Bewertung durchgeführt werden. Vielmehr wird im Folgenden knapp untersucht, inwieweit die gesteckten Ziele mit der vorgestellten Lösung erreicht wurden, welche funktionalen und anderweitigen Aspekte noch offen sind, welchen Mehrwert der Einsatz von Security-Frameworks gegenüber einer herkömmlichen Erarbeitung von Sicherheitskonzepten bietet und wie der mit dem Lösungsweg verbundene Aufwand beurteilt werden kann.

In Abschnitt 8.2 wurden die zu erreichenden Ziele definiert. Mit dem erarbeiteten, auf Security-Frameworks basierenden Architekturkonzept konnten alle **sicherheitsfunktionalen Ziele** erreicht werden:

- Die Authentifizierungs- und Autorisierungsvorgänge werden wie im Framework für föderiertes Sicherheitsmanagement vorgesehen über die Anbindung des am LRZ vorhandenen Identity-Management-Systems abgewickelt, das zu diesem Zweck sowohl funktional als auch durch zusätzliche Hardware zur Verbesserung von Lastverteilung und Ausfallsicherheit erweitert wird.
- Die Vertraulichkeit wird über verschlüsselte Datenübertragung, verschlüsselte Backups und eine vom Betriebssystem erzwungene gegenseitige Abschottung der Benutzer und Projekte erreicht. Mittels der vom Datenschutz-Security-Framework bereitgestellten Funktionalität können auch Missbrauchsversuche durch den Betreiber verhindert werden.
- Die Hochverfügbarkeit des Dienstes wird durch Redundanz bei der Implementierung von Sicherheitsmechanismen nicht eingeschränkt; auch beim Eintreten von Sicherheitsvorfällen wird durch das Zusammenspiel des Security-Incident-Response-Prozesses mit den IT-forensischen Maßnahmen das Ziel verfolgt, den Dienstbetrieb schnellstmöglich wieder aufnehmen zu können.
- Die umfassenden präventiven Maßnahmen werden durch Detektionsmechanismen ergänzt; neben dedizierten IDS-Regelsätzen werden dabei auch Maßnahmen aus dem Netz- und Systemmanagement sowie weitere bereits vorhandene Sicherheitswerkzeuge integriert.
- Für typische Sicherheitsvorfälle wie einzelne kompromittierte Benutzerkennungen werden vorab entsprechende Reaktionswege festgelegt.
- Das Sicherheitsberichtswesen wird durch SuperMUC-spezifische Hypothesen und KPIs, die für alle identifizierten Zielgruppen geeignet aufbereitet werden, unterstützt.

Auch die **Integrationsziele** werden vollständig erreicht: Für die Absicherung des SuperMUC-Dienstes werden am LRZ bereits vorhandene Sicherheitsmechanismen eingesetzt und zum Teil an spezifische Anforderungen angepasst; bezüglich der von Security-Frameworks benötigten Basisdienste wie Datenbanken und Webserver wird ebenfalls auf Dienste aus dem LRZ-Dienstleistungskatalog bzw. im SuperMUC-Kontext bereitgestellte Systeme zurückgegriffen.

Sowohl bei den zum Einsatz kommenden technischen Verfahren als auch bei den dafür relevanten ITSM- und Sicherheitsmanagementprozessen sind Schnittstellen zur organisationsübergreifenden Koordination vorgesehen.

Schließlich werden die **organisatorischen Ziele** ebenfalls erreicht: Durch das Zusammenspiel beispielsweise der SuperMUC-Administratorengruppe mit dem LRZ-Sicherheitsarbeitskreis können bestehende Strukturen und Kompetenzen genutzt und gezielt eingebunden werden. Einarbeitungszeiten und Schulungsbedarf fallen lediglich im Kontext des Datenschutz-Security-Frameworks an, da bislang insbesondere keine XACML-Policies zum Einsatz kamen. Bezüglich aller ITSM- und Sicherheitsmanagementprozesse wird eine vollständige Integration in bestehende Abläufe erreicht; laufende Entwicklungen in Parallelprojekten mit Sicherheitsbezug werden ebenso berücksichtigt wie die Nutzung bereits vorhandener Managementplattformen und -werkzeuge.

Obwohl somit alle diskutierten Anforderungen erfüllt sind, muss berücksichtigt werden, dass die Arbeiten an der Sicherheitslösung für den SuperMUC-Dienst nicht nach deren initialer Bereitstellung abgeschlossen werden können: In Abschnitt 8.5.2.1 wurden beispielsweise noch vorhandene Defizite der eingesetzten Middleware bezüglich der Integrität und Verbindlichkeit erläutert, die vom Framework für föderiertes Sicherheitsmanagement identifiziert wurden und entsprechende technische Weiterentwicklungen erforderlich machen. Auch der Einsatz des Datenschutz-Security-Frameworks und die damit verbundene Formulierung von Policies stehen erst am Anfang und müssen weiter ausgebaut werden. Ferner bleibt prima facie unklar, ob die vorgesehenen Automatismen ausreichen oder ob sich im Betrieb neue, häufig wiederholende Abläufe ergeben, die zusätzliche Schnittstellen und Werkzeuge zur effizienten Bearbeitung erforderlich machen. Schließlich muss auch berücksichtigt werden, dass die Weiterentwicklungen im Bereich der ITSM- und Sicherheitsmanagementprozesse sowie in den parallel laufenden Sicherheitsprojekten neue Ergebnisse liefern werden, die in den Betrieb des SuperMUC-Dienstes geeignet einfließen müssen.

Aufgrund der Erfahrungen, die LRZ-seitig bereits mit dem Betrieb und der Absicherung von HPC-Diensten vorliegen, wäre der Einsatz von Security-Frameworks offensichtlich nicht zwingend erforderlich gewesen, da bestehende Konzepte verwendet und angepasst werden könnten. Dennoch ergibt sich aus ihrer Anwendung ein unmittelbarer und erheblicher Mehrwert: Zunächst spannt das Security-Framework für föderiertes Sicherheitsmanagement einen thematischen Rahmen auf, in den bestehende Konzepte und Sicherheitsmechanismen eingeordnet und bezüglich der Eignung für den SuperMUC-Dienst bewertet werden können. Im Rahmen seiner SuperMUC-spezifischen Anpassungen konnte bestätigt werden, dass keine wesentlichen sicherheitsspezifischen Teilfragestellungen übersehen wurden und dass Teilbereiche, in denen neue und überarbeitete Maßnahmen und Mechanismen erforderlich sind, identifiziert werden konnten. Es liefert somit auch grundlegende Informationen für ein nachhaltiges Risikomanagement und die kontinuierliche Verbesserung der resultierenden SuperMUC-Sicherheitsarchitektur. Das Datenschutz-Security-Framework und das Linux-Kernel-Security-Framework lösen im Zusammenspiel die bislang offenen Fragestellungen rund um die Datenzweckbindung und die Verhinderung betreiberseitigen Datenmissbrauchs. Sie ergänzen das Framework für föderiertes Sicherheitsmanagement funktional und stellen auf Basis von Standardkomponenten gebrauchsfertige Lösungen bereit, die lediglich eine SuperMUC-spezifische Konfiguration erfordern, im laufenden Betrieb keinen signifikanten Mehraufwand verursachen und auch aus Benutzerperspektive zusätzliche Sicherheitsfunktionalität bieten. Auch die konzipierten Managementwerkzeuge zur dynamischen IDS-Reparametrisierung und zur Er-

stellung von Sicherheitsberichten konnten unmittelbar angewandt werden und nutzen dabei neben bereits vorhandenen Sicherheitsmechanismen die von den Security-Frameworks bereitgestellten Komponenten und Schnittstellen.

Durch die von den Security-Frameworks vorgegebenen Lösungswege und deren Variationen verringert sich somit unmittelbar der zur Konzeption einer SuperMUC-Sicherheitsarchitektur erforderliche Aufwand. Auch der Implementierungs- und Betriebsaufwand liegt, wie in Abschnitt 8.8 dargelegt wurde, in einem angemessenen Bereich, so dass aus dem Schutzbedarf weder initiale noch laufende Kosten entstehen, durch die die IT-Sicherheit gegenüber den anderen Aspekten des Dienstes zu einem kritischen Faktor würde. Insbesondere deckt sich der zunächst zur Bereitstellung hohe und im laufenden Betrieb deutlich niedrigere Personalaufwand mit dem Verlauf des SuperMUC-Gesamtprojekts; somit erweist sich auch die enge Verzahnung der Security-Framework-Lebenszyklus und Rolloutphasen mit denjenigen des SuperMUC-Dienstes als praktikabler Ansatz, so dass aus den im Kontext des Gesamtprojekts gegebenen engen Terminen keine Nachteile für das erreichte Sicherheitsniveau entstehen.

8.10. Zusammenfassung

In diesem Kapitel wurde ein umfassendes Beispiel für die Anwendung und das Management von Security-Frameworks auf Basis der in den vorhergehenden Kapiteln erarbeiteten Methoden und Konzepte gegeben. Mit SuperMUC wurde ein komplexer IT-Dienst gewählt, bei dem neben umfangreichen technischen und organisatorischen Integrationsaufgaben auch eine Kombination aus intra- und interorganisationalen Managementaspekten und ein mehrstufiger Deployment-Ablauf zu betrachten sind.

Zunächst wurden die Eckdaten des Dienstes und der Umgebung, in die er integriert werden muss, vorgestellt; dabei wurden sowohl technische als auch organisatorische Schnittstellen festgelegt, die im weiteren Verlauf durchgängig berücksichtigt wurden. Nach einer Schilderung der Motivation für den Einsatz von Security-Frameworks wurden die für diese Arbeit wesentlichen Ziele, die das SuperMUC-Einführungsprojekt verfolgt, definiert. Hierbei wurde in Anlehnung an die strukturierte Bewertung von Security-Frameworks zwischen sicherheitsfunktionalen, integrationsspezifischen und managementbezogenen Zielen differenziert. Zur Abbildung dieser Ziele auf Konzeptions-, Entwicklungs- und Betriebsaufgaben wurde anschließend die Organisation des SuperMUC-Beispielprojekts konzipiert, indem entsprechende Rollen und Zuständigkeiten unter Berücksichtigung der vorhandenen Organisationsstruktur spezifiziert wurden.

Um die Einordnung der sicherheitstechnischen Lösungskomponenten vorzubereiten, wurde im Folgenden ein Überblick über die SuperMUC-Gesamtarchitektur gegeben, der Abhängigkeiten und Datenflüsse sowohl aus Benutzersicht als auch aus LRZ-interner Perspektive aufgezeigt hat. Auf dieser technischen Basis wurden zunächst die Anforderungen an Security-Frameworks SuperMUC-spezifisch priorisiert und die Auswahl konkreter Security-Frameworks erläutert. Für das Framework für föderiertes Sicherheitsmanagement, das Datenschutz-Security-Framework und das Linux-Kernel-Security-Framework wurden darauf aufbauend die Schwerpunkte in der Customizingphase und deren Ergebnisse erarbeitet und diese in die Gesamtsystemarchitektur integriert.

Im Anschluss an diese technischen Betrachtungen wurden die im SuperMUC-Szenario relevanten Managementprozesse spezifiziert, wobei wie in den vorangehenden Teilen der Arbeit

zwischen IT-Service-Management- und Sicherheitsmanagementprozessen untergliedert wurde. Neben dem LRZ-internen Zusammenspiel dieser Prozesse wurden dabei auch die entsprechenden Schnittstellen zur organisationsübergreifenden Prozessen betrachtet. Zudem wurde aufgezeigt, wie die in dieser Arbeit konzipierten Managementwerkzeuge zur dynamischen Reparametrisierung von IDS-Komponenten und zur Erfassung und Aufbereitung von Sicherheitskennzahlen SuperMUC-spezifisch eingesetzt werden können.

Daran anschließend wurden ausgewählte Aspekte in den weiteren Lebenszyklusphasen der Frameworkinstanzen bis hin zu deren Außerbetriebnahme bzw. Übernahme auf ein mögliches SuperMUC-Nachfolgesystem diskutiert. Auf Basis dieser Betrachtung des gesamten Lebenszyklus wurden anschließend die Investitions- und Betriebskosten nach Aufwendungen für Hard-/Software, Softwareentwicklung und Personal getrennt analysiert. Schließlich wurde eine Bewertung der vorgestellten Lösung vorgenommen, die auf die Zielerreichung, offene Aspekte, den Mehrwert durch den Einsatz von Security-Frameworks und den mit ihnen verbundenen Aufwand eingeht.

Kapitel 9.

Zusammenfassung und Ausblick

Inhalt dieses Kapitels

Security-Frameworks stellen nicht nur einzelne Bausteine, sondern komplexe und für ausgewählte IT-Sicherheitsfragestellungen oftmals umfassende Baukästen aus organisatorischen und technischen Sicherheitsmaßnahmen dar; sie können je nach ihrer Ausprägung entweder auf einzelne, durchaus komplexe IT-Dienste bzw. auf ganze IT-Architekturen oder im Rahmen der Softwareentwicklung angewendet werden. Ihr Einsatz bietet insbesondere dort einen attraktiven Mehrwert, wo entweder der szenarienspezifische Aufwand für die Erstellung ganzheitlicher Sicherheitskonzepte zu reduzieren ist oder organisationsübergreifend vergleichbare, bewährte Sicherheitslösungen etabliert werden sollen.

Die in der Praxis implementierten Security-Frameworks müssen wie andere Sicherheitskomponenten auch betrieben, gewartet und kontinuierlich verbessert werden, um ihrem sicherheitsfunktionalen Anspruch nachhaltig gerecht zu werden. Das somit erforderliche Management von Security-Frameworks stand zu Beginn dieser Arbeit unter anderem vor der Herausforderung, dass die Konzepte von Security-Frameworks bislang meist sehr stark technikorientiert dokumentiert sind und als Seiteneffekt davon oft auf Managementaspekte, falls überhaupt, nur punktuell eingehen. Im Rahmen dieser Arbeit wurden deshalb **Konzepte und Methoden** erarbeitet, die ein **integriertes Management von Security-Frameworks** ermöglichen: Dabei werden neben technischen Herausforderungen wie dem harmonischen parallelen Einsatz mehrerer Security-Frameworks im selben Szenario auch die Schnittstellen u. a. zum IT Service Management und zu den Teilprozessen des Sicherheitsmanagements, beispielsweise zum Risikomanagement, betrachtet.

Diese Arbeit abschließend werden nachfolgend zunächst die **inhaltlichen Schwerpunkte und wichtigsten Ergebnisse** der einzelnen Kapitel **zusammengefasst**, in Zusammenhang gebracht und in anschließend mit Bezug auf die ursprünglichen Zielsetzungen **kritisch**

bewertet. Daran anknüpfend wird in Abschnitt 9.2 eine Reihe noch offener Punkte erläutert, die weiterführende und vertiefende **Forschungsarbeiten im Umfeld von Security-Frameworks** motivieren. Schließlich werden in Abschnitt 9.3 **Forschungsfragestellungen in eng verwandten Themenbereichen** aufgezeigt, die im Rahmen weiterer Arbeiten zu betrachten sind und von den hier geleisteten Vorarbeiten profitieren.

9.1. Zusammenfassung der Arbeit und Bewertung der Ergebnisse

Wie einleitend in **Kapitel 1** dargestellt wurde, stehen funktionale Zielsetzungen bei der Entwicklung, bei der Bereitstellung und beim Betrieb von IT-Systemen nach wie vor im Vordergrund. Ein Umdenken, das dazu führt, dass auch IT-Sicherheitsaspekte von Anfang an berücksichtigt werden, findet erst allmählich statt, obwohl es von Security-Engineering-Paradigmen wie *secure-by-design* bereits seit längerer Zeit gefordert wird. Neben ökonomischen Aspekten wie der Produkteinführungszeit (engl. *time to market*) und dem nur indirekten Einfluss von Sicherheitseigenschaften auf Umsatz und Gewinn besteht in der Praxis häufig das Problem, dass nicht alle Beteiligten parallel zu ihren Kernaufgaben auch Sicherheitsexperten sein können, die ihr diesbezügliches Wissen kontinuierlich auf dem aktuellsten Stand halten.

Als Kern einer Lösung dieser Problematik bietet sich der **Einsatz von Security-Frameworks** an: Diese stecken einen für das jeweilige Anwendungsgebiet spezifischen Rahmen aus Sicherheitsperspektive ab und bieten **aufeinander abgestimmte technische und organisatorische Lösungsbausteine**, die **szenarienspezifisch** ausgewählt, **angepasst** und bei Bedarf ergänzt werden können. Gegenüber einer von Grund auf neu durchgeführten Sicherheitskonzeption ergeben sich Vorteile wie ein verringerter Aufwand und eine breite konzeptionelle und praktisch bewährte Ausgangsbasis, über die eine möglichst vollständige Lösung einfacher erreicht werden kann.

Im Kontext einer sehr breiten IT-Dienstpalette, wie sie in Rechenzentren und IT-Abteilungen trotz anhaltender Tendenzen zur Auslagerung einzelner Dienste vorzufinden ist, stellt jedes Security-Framework jedoch wiederum nur einen punktuellen Lösungsansatz dar, der in ein **übergreifendes Sicherheitskonzept** eingebettet werden muss. Das Gesamtziel der vorliegenden Arbeit ist deshalb das **integrierte Management von Security-Frameworks**; die Integration zielt dabei sowohl auf den aufeinander abgestimmten, **parallelen Einsatz mehrerer Security-Frameworks** als auch die **prozessuale Verflechtung**, unter anderem mit IT-Service-Management-Prozessen, ab. Die beiden zentralen **Herausforderungen** sind dabei die Vielfalt bzw. Heterogenität der existierenden Security-Frameworks und deren voneinander isolierte Entstehung, aufgrund derer viele Aspekte ihres Zusammenspiels und ihres kombinierten Einsatzes zunächst ungeklärt waren.

Unter Berücksichtigung dieser Herausforderungen wurde die **Zielsetzung der Arbeit** in vier Teilziele zerlegt:

1. Entwicklung einer adaptierbaren **Methodik für die szenariengetriebene Analyse, Bewertung und Gegenüberstellung von Security-Frameworks**. Dies ermöglicht die Entscheidung, ob und welche Security-Frameworks in einem konkreten Szenario eingesetzt werden, aus der Perspektive der Organisation, die als Frameworkanwender fungiert.

2. Entwicklung eines modularen **Leitfadens für die Entwicklung von Security-Frameworks** aus der Sicht ihres Managements. Hierdurch wird sichergestellt, dass neue Security-Frameworks von Anfang an die von ihnen gewünschten Managementeigenschaften berücksichtigen und bestehende Security-Frameworks gezielt verbessert werden können.
3. **Spezifikation des vollständigen Security-Framework-Lebenszyklus**. Da viele Security-Frameworks lediglich ihre technischen und organisatorischen Bausteine und zum Teil noch deren szenarienspezifische Anpassung beschreiben, wird durch die präzise Spezifikation weiterer Lebenszyklusphasen wie Implementierung, Betrieb und Überarbeitung die Grundlage für den praktischen Einsatz und die Verwaltung mit Managementplattformen analog zu den von den Security-Frameworks geschützten IT-Diensten geschaffen.
4. **Spezifikation von Security-Framework-Managementprozessen** und ausgewählten Aspekten ihrer **Werkzeugunterstützung**. Neben für Security-Frameworks spezifischen Abläufen sind dabei auch Schnittstellen, unter anderem zu den ITSM-Prozessen, und die technische Unterstützung und Automatisierung zu berücksichtigen.

Zur Strukturierung der Lösungswege, die zu den einzelnen Teilzielen führen, wurden in der Einleitung zwölf ausgewählte Dimensionen des Managements von Security-Frameworks vorgestellt und zahlreiche offene wissenschaftliche Einzelfragestellungen abgeleitet, die in den weiteren Kapiteln im Detail untersucht und beantwortet wurden. Aus ihrer thematischen Gruppierung ergab sich die **Grundstruktur der Arbeit**, die vereinfacht wie folgt zusammengefasst werden kann:

- Die Kapitel 2 bis 4 erarbeiten die **Grundlagen**, indem zunächst eine **Begriffsbildung** und Einordnung vorgenommen wird, **Anforderungen** auf Basis von Szenarien definiert und priorisiert sowie **existierende Security-Frameworks analysiert** und bewertet werden.
- In den Kapiteln 5 bis 7 werden **neue Methoden und Konzepte** erarbeitet, um den gesamten **Lebenszyklus von Security-Frameworks** abzudecken, die **prozessualen Schnittstellen** und den **Einsatz von Managementplattformen und Sicherheitskennzahlen** zu definieren und ausgewählte Aufgaben gezielt mit dedizierten **Managementwerkzeugen** zu unterstützen.
- Kapitel 8 gibt schließlich ein umfassendes **Anwendungsbeispiel**, das die erarbeiteten Konzepte und Methoden exemplifiziert und die Ergebnisse qualitativ und quantitativ beurteilt.

Anhand dieser Struktur werden die erarbeiteten Ergebnisse in den nachfolgenden Abschnitten 9.1.1 bis 9.1.3 zusammengefasst und in Abschnitt 9.1.4 bewertet.

9.1.1. Kapitel 2–4: Basiskonzepte, Anforderungen und Status Quo

In **Kapitel 2** wurden zunächst die Grundlagen für die Diskussion der Eigenschaften von Security-Frameworks gelegt: Im ersten Schritt wurde eine Abgrenzung der technischen und organisatorischen Aspekte des Sicherheitsmanagements vorgenommen und es wurden die dafür notwendigen Schnittstellen analysiert. Analog dazu wurde die Beziehung zwischen dem

Sicherheitsmanagement und dem IT Service Management herausgearbeitet. Unter Berücksichtigung der so aufbereiteten Zusammenhänge und gegenseitigen Abhängigkeiten wurde anschließend eine Einordnung von Begriffen, Methoden und Prozessen in den Kontext von Security-Frameworks vorgenommen. Als treibende Kraft für das Sicherheitsmanagement wurde dabei in Anlehnung an die Normenreihe ISO/IEC 27000 ein **risikogetriebenes Vorgehen** bei der Priorisierung von Maßnahmen und bei der Implementierung technischer Sicherheitsmechanismen identifiziert.

Da technische und organisatorische Sicherheitsmaßnahmen Hand in Hand gehen müssen, wurden anschließend die Aufgaben beteiligter Individuen und Gruppen betrachtet: Dabei wurden einerseits 15 organisatorische **Rollen**, die Personen im Umfeld von Security-Frameworks und deren Management in Einrichtungen annehmen können, definiert; diese wurden in den nachfolgenden Kapitel konsequent einheitlich angewandt. Andererseits wurden unter Berücksichtigung der **Methoden des Security-Engineering** wichtige Teilaspekte wie die Benutzerfreundlichkeit von Sicherheitsmechanismen und der Bedarf an Schulungen zur Sensibilisierung aller Involvierten analysiert. Auf der technischen Seite wurden die Paradigmen *secure-by-design*, *secure-by-default* und *secure-in-deployment* sowie die beim parallelen Einsatz mehrerer Sicherheitskomponenten gegeneinander abzuwägenden Aspekte Redundanzfreiheit und bewusste Überlappungen (*defense-in-depth*) betrachtet.

Da sich die weiteren Kapitel aufgrund der Zielsetzung der gesamten Arbeit auf die Managementaspekte von Security-Frameworks konzentrierten, eine Betrachtung der mit ihrem Einsatz erzielten Sicherheitsfunktionalität aber ebenfalls von grundlegender Bedeutung ist, wurde in Kapitel 2 anschließend eine Analyse und **Kategorisierung** der in Security-Frameworks häufig berücksichtigten **Angriffe** und typischerweise eingesetzten **Sicherheitsmechanismen** durchgeführt. Schwerpunkte waren dabei gezielte Angriffe auf einzelne Softwarekomponenten, beispielsweise durch Code-Injection-Versuche, Manipulationen des netzbasierten Nachrichtenaustausches, beispielsweise durch einen Man-in-the-Middle, und die von Angreifern geschickt durchgeführte Kombination verschiedener Angriffsvarianten. Viele eingesetzte Sicherheitsmechanismen basieren auf ebenfalls vorgestellten kryptographischen Verfahren, nutzen bestehende Authentifizierungs- und Autorisierungsinfrastrukturen und integrieren Standardkomponenten wie Firewalls und Intrusion Detection Systeme in die Security-Framework-Gesamtarchitektur.

Komplementär zu dieser empirischen Analyse wurde anschließend der **Begriff Security-Framework** definiert; dies war insbesondere auch durch die uneinheitliche Verwendung des Begriffs in bisheriger Literatur erforderlich. Der historischen Entwicklung wurde dadurch Rechnung getragen, dass der Begriff dual sowohl für **Frameworkkonzepte** als auch für **Frameworkinstanzen** verwendet werden kann, wodurch eine entsprechende Differenzierung bei der Betrachtung des gesamten Lebenszyklus erforderlich wird. Die Begriffsbildung sieht eine zwingende Einbettung in einen **kontinuierlichen Verbesserungsprozess** vor, so dass die Einführung eines Security-Frameworks keine einmalige punktuelle Maßnahme sein darf. Zudem wird explizit von einer Aufteilung sowohl in technische als auch in organisatorische Maßnahmen ausgegangen, die szenarienspezifisch adaptiert und kombiniert werden können.

Kapitel 2 schloss mit einer **Einordnung von Security-Frameworks in Informationssicherheitsmanagementsysteme und Sicherheitsarchitekturen**, anhand deren organisations- bzw. szenarienweitem Anwendungsbereich die nahtlose Einbettung von Security-Frameworks in Gesamtsicherheitskonzepte erläutert wurde.

Kapitel 3 zielte daran anknüpfend auf die **Ermittlung von Anforderungen** an Security-Frameworks aus Managementperspektive, die Kategorisierung und Gewichtung dieser Anforderungen sowie die **Methodik zur Anwendung des entsprechenden Kriterienkatalogs** ab. Das breite Spektrum potentieller Einsatzszenarien erschwerte die Ermittlung von Anforderungen insbesondere unter dem Blickwinkel der Vollständigkeit. Deshalb wurde der Lösungsweg eingeschlagen, in Frage kommende Szenarien zunächst anhand von zehn zueinander komplementären Charakteristika zu kategorisieren; dabei kommt beispielsweise zum Tragen, ob Security-Frameworks nur organisationsintern oder in organisationsübergreifenden Verbünden eingesetzt werden sollen, ob im Szenario personenbezogene Daten verarbeitet werden und wie viele Security-Frameworks parallel eingesetzt werden sollen.

Im Anschluss wurden **vier Szenarien** ausgewählt, die eine breite Streuung dieser Charakteristika aufweisen, so dass eine möglichst breite Abdeckung erreicht wurde:

- Das Leibniz-Rechenzentrum fungiert im ersten Szenario als Beispiel für IT-Dienstleister, die eine Vielzahl unterschiedlichster Dienste anbieten und komplexe Infrastrukturen betreiben. Neben einer großen Anzahl an Anwendern stehen dabei die Infrastrukturkomplexität und damit verbunden die Integrationsanforderungen im Vordergrund.
- Das zweite Szenario beschreibt den Einsatz von Security-Frameworks bei einem webbasierten Micropayment-Anbieter. Es stellt organisationsübergreifende Aspekte, z. B. im Zusammenspiel mit Scoring-Agenturen und E-Commerce-Anbietern, und die Einhaltung rechtlicher Rahmenbedingungen ebenso wie den hohen Bedarf an durchgängiger Verfügbarkeit in den Vordergrund. Zugleich veranschaulicht es, dass sich aus Sicherheitsmaßnahmen in der Praxis häufig keine erheblichen Einschränkungen der Benutzbarkeit ergeben dürfen.
- Das dritte Szenario geht mit dem Grid-Computing auf die organisationsübergreifende Nutzung von Rechen- und Speicherressourcen im wissenschaftlichen Umfeld ein. Ihm liegt eine nur lose Kopplung der beteiligten Organisationen zugrunde, deren Infrastrukturen eine zum Teil hohe Heterogenität aufweisen. Im Vordergrund steht hier einerseits, dass die zu schützenden Ressourcen im Allgemeinen zusätzlich parallel in anderer Form, z. B. für lokales oder regionales High Performance Computing, eingesetzt werden. Andererseits wird Nutzern die Ausführung fast beliebigen eigenen Codes ermöglicht, so dass spezielle, systemnahe Sicherheitsmechanismen benötigt werden, um missbräuchlicher Verwendung vorzubeugen. Durch die Dynamik realer Grid-Verbünde und virtueller Organisationen motiviert wurden in diesem Szenario auch Vorgehensweisen betrachtet, wie Security-Frameworks parallel zu den von ihnen geschützten Assets in Betrieb genommen und nicht erst später nachgerüstet werden können.
- Mit Learning Management Systemen wurden im vierten Szenario schließlich Dienste untersucht, die sich an vielen Firmen- und Hochschulstandorten evolutionär entwickeln und sich dabei von kleinen Testinstallationen hin zu organisationsweiten, komplexen verteilten Systemen wandeln. Neben einer sukzessiven Öffnung für weitere Nutzergruppen wird dabei betrachtet, dass der Betrieb sicherer Systeme in der Praxis oft nicht von Anfang an durch IT-Abteilungen oder Rechenzentren erfolgt, sondern durch die ersten Anwender – im Szenario die Dozenten – des Systems selbst erfolgt; zudem müssen auch Angriffe durch Innentäter – im Szenario zur Systemnutzung berechtigte Lernende – berücksichtigt werden.

Szenarienspezifische Prioritäten und die szenarienübergreifende Mehrfachnennung von Anforderungen bilden dabei die Basis für deren spätere Gewichtung. Die aus den Szenarien ermittelten Anforderungen wurden auf Basis einer Literaturrecherche ergänzt; dabei wurden auch Anforderungen, die sich aus den Methoden des Security-Engineering und aus Standards für das Informationssicherheitsmanagement ergeben, eingebracht.

Die **55 ermittelten Anforderungen** wurden jeweils einer von **vier Kategorien** zugeordnet, die als Strukturierungsmittel spezifiziert wurden:

- Funktionale Anforderungen decken die technischen und sicherheitsspezifischen Aspekte ab und nehmen Bezug auf die in Kapitel 2 vorgestellten Ziele der IT-Sicherheit und des Sicherheitsmanagements.
- Integrations- und Betriebsanforderungen umfassen die szenarienspezifische Adaption von Security-Frameworks und die Einbettung in vorhandene Infrastrukturen.
- Managementanforderungen beschreiben die Schnittstellen zur Steuerung und Kontrolle von Security-Frameworks sowohl auf technischer Ebene, die beispielsweise von Managementplattformen realisiert wird, als auch aus Perspektive der Führungsebene von Organisationen und deren Informationsbedarf.
- Dokumentationsanforderungen thematisieren sowohl den Inhalt als auch die Form von Frameworkkonzepten, um eine effiziente praktische Anwendbarkeit zu gewährleisten.

Im Anschluss wurde eine Methodik zur szenarienspezifischen Ergänzung möglicher weiterer Anforderungen, zur hierarchischen Gewichtung aller Anforderungen und zur konkreten Evaluation und Bewertung von Security-Frameworks konzipiert. Nach einer Darstellung der Zusammenhänge und gegenseitigen Abhängigkeiten aller ermittelten Anforderungen wurde diese Methodik angewandt, um den in der Arbeit durchgängig eingesetzten **Anforderungskatalog** zu erstellen, dessen einzelne Gewichtungen individuell begründet wurden.

Diese Diskussion der Anforderungen an Security-Frameworks abschließend wurde der Anforderungskatalog zu einem **Leitfaden für die Autoren von Frameworkkonzepten** aufbereitet. Durch die Orientierung daran kann bei der Dokumentation von Security-Frameworks sichergestellt werden, dass keine wesentlichen managementrelevanten Themenbereiche übersehen werden; zudem kann er als Strukturierungshilfe herangezogen werden.

In **Kapitel 4** wurden aktuelle Security-Frameworks analysiert und anhand des Kriterienkatalogs beurteilt; auf Basis des konzipierten Leitfadens wurden zudem Vorschläge für die weitere Verbesserung der untersuchten Frameworkdokumentationen erarbeitet. Die grundlegende Zielsetzung bestand dabei nicht in der vergleichenden Beurteilung von Security-Frameworks, wie sie beispielsweise für die Auswahl konkreter Frameworkkonzepte für die oben genannten Szenarien erforderliche wäre. Vielmehr sollten **generelle Stärken und Schwächen** ermittelt werden, um auf dieser Basis die Zielsetzungen der weiteren Kapitel dieser Arbeit zu schärfen.

Die Analyse vorbereitend wurde zunächst eine **Kategorisierung von Security-Frameworks** vorgenommen. Für die drei Security-Framework-Kategorien Software Engineering, IT-Dienste und IT-Architekturen wurden die jeweils typischen inhaltlichen Schwerpunkte und primären Zielgruppen diskutiert. Im Anschluss wurde den Auflagen eines Systematic-Review-Prozesses gemäß die angewandte Vorgehensweise bei der Literaturrecherche nach Security-Frameworks dargelegt; dabei wurde insbesondere eine Einschränkung auf Arbeiten,

die die Kriterien der Definition von Security-Frameworks in Kapitel 2 erfüllen und deren letzte Aktualisierung zum Zeitpunkt der Analyse nicht länger zehn Jahre zurück lag, vorgenommen.

Daran anschließend wurden die bei Security-Frameworks vorherrschenden **Designkonzepte** empirisch ermittelt: Obwohl bislang keine allgemeinen Designrichtlinien oder anderen konkreten Vorgaben existierten, zeichneten sich typische Strukturen von Frameworkkonzepten ab. Hierzu gehören unter anderem eine Orientierung an konkreten Szenarien, ein architektureller Gesamtüberblick, eine Diskussion und Bewertung zur Auswahl stehender alternativer Lösungsmodule und häufig auch die Spezifikation neuer, von den Frameworkautoren selbst eingebrachten Lösungs- bzw. Schnittstellenkomponenten. Bereits bei dieser Strukturanalyse wurde deutlich, dass bislang nur vereinzelt auch auf das Customizing und die praktische Anwendung von Security-Frameworks im Detail eingegangen wird.

Den Schwerpunkt des Kapitels bildete die **Einzelanalyse von über 75 Security-Frameworks**. Zwei Analysen wurden zur Veranschaulichung der Anwendung des in Kapitel 3 erarbeiteten Kriterienkatalogs im Detail vorgestellt; für die Darstellung der Ergebnisse der weiteren Analysen, die über einen Zeitraum von über einem Jahr angefertigt wurden, wurde eine kompakte Form gewählt.

Auf Basis dieser Resultate wurden die derzeit typischen Stärken und Schwächen von Security-Frameworks herausgearbeitet und diskutiert. Es zeigte sich, dass insbesondere die **Managementanforderungen nur deutlich unterdurchschnittlich erfüllt** wurden. Elf dieser Anforderungen wurden sogar von 60 oder mehr der untersuchten Security-Frameworks überhaupt nicht berücksichtigt; so fehlten insbesondere Schnittstellen zum IT Service Management und Maßnahmen zur Quantifizierung der erreichten Sicherheitseigenschaften und damit die Einbettung in das Sicherheitsberichtswesen. Positiv zu vermerken war jedoch, dass die sicherheitsfunktionalen Anforderungen durchwegs gut erfüllt werden. Bezüglich der Integrationsanforderungen wurden insbesondere das Customizing, die praktische Einführung und ein stufenweises Vorgehen beim Deployment nicht ausreichend methodisch unterstützt, was ein großes Hindernis für den praktischen Einsatz darstellt.

Schließlich wurden daraus Konsequenzen für den praktischen Einsatz abgeleitet und die Schwerpunkte der vorliegenden Arbeit motiviert und präzisiert. Hierzu gehören die Betrachtung des gesamten Lebenszyklus von Security-Frameworks, die Spezifikation von Managementprozessen und prozessualen Schnittstellen samt einer Einbettung in einen kontinuierlichen Verbesserungsprozess und die gezielte Unterstützung des Managements von Security-Frameworks durch dedizierte Werkzeuge. An diesem Bedarf orientiert sich die Kapitelstruktur des nachfolgend zusammengefassten zweiten Teils der Arbeit.

9.1.2. Kapitel 5–7: Lebenszyklus, Managementprozesse und -werkzeuge

Kapitel 5 spezifiziert den vollständigen **Lebenszyklus** von Security-Frameworks im Detail; im Unterschied beispielsweise zum Leitfaden für Frameworkautoren in Kapitel 3 wurde dabei ein Wechsel in die Perspektive von Frameworkanwendern vollzogen.

Die duale Verwendung des Begriffs Security-Framework erforderte die differenzierte Betrachtung von Frameworkkonzepten und Frameworkinstanzen, woraus sich in der Folge ein Bedarf an der engen **Verzahnung der beiden Lebenszyklen** unter zusätzlicher Berücksichtigung der Einbettung in szenarienspezifische Projekte, beispielsweise zur parallelen Einführung von

durch Security-Frameworks geschützten Ressourcen, und Prozesse ergab. Alle Betrachtungen gehen zudem durchgängig von der Möglichkeit aus, dass mehrere Security-Frameworks parallel eingesetzt werden können und dabei grundlegend komplementär zueinander agieren, sich hinsichtlich ihres Abdeckungsbereichs aber im Sinne der *defense-in-depth* auch bewusst partiell überlappen können.

In einem ersten Schritt wurden die Voraussetzungen und Anforderungen analysiert, die nicht von den Security-Frameworks, sondern von den Szenarien erfüllt werden müssen, um diese effizient einführen und einsetzen zu können. Im zweiten Schritt wurde der Lebenszyklus von Frameworkkonzepten in Anlehnung an den Systems Development Life Cycle (SDLC) spezifiziert. Er umfasst die Phasen Planung, Anforderungsanalyse, Design, Referenzimplementierung, Dokumentation, Begutachtung und Freigabe sowie den praktischen Einsatz. Neben der Beschreibung jeder Phase wurden deren **Schnittstellen** untereinander, zu den Frameworkinstanzen sowie zu den sich kontinuierlich weiterentwickelnden Zielen, Assets, Angriffen und Schwachstellen spezifiziert.

Den Schwerpunkt bildete anschließend die detaillierte und einheitlich strukturierte Beschreibung aller Lebenszyklusphasen von Frameworkinstanzen. Mit den sieben Phasen *Auswahl*, *Customizing*, *Instanziierung*, *Test und Inbetriebnahme*, *Betrieb und Wartung*, *Überarbeitung* sowie *Außerbetriebnahme* wurde eine an Service-Management-Standards orientierte Granularität gewählt. Neben der jeweiligen **Zielsetzung**, den Voraussetzungen, **Tätigkeitsschwerpunkten** und beteiligten Rollen bzw. **Verantwortlichkeiten** in Form von RASCI-Matrizen wurden für jede Phase die Schnittstellen spezifiziert, besonders relevante Anforderungen herausgearbeitet und der phaseninterne **Ablauf mit seinen Einzelaktivitäten** und dafür geeigneten Methoden dargelegt; hierfür wurden aktuelle Methoden auf Basis des Security-Engineering aufgegriffen und integriert, beispielsweise die modellbasierte Sicherheitstestautomatisierung und das bedrohungsmodellgetriebene Sicherheitstesten. Eine **Erfolgskontrolle** wird dabei jeweils durch Angaben zu Deliverables, zu Abnahmekriterien und zum Berichtswesen ermöglicht. Insgesamt werden damit insbesondere auch diejenigen Bereiche abgedeckt, auf die Frameworkkonzepte bislang sehr häufig zu wenig oder gar nicht eingehen. Diese vertiefende Betrachtung der Lebenszyklusphasen von Frameworkinstanzen schloss mit einer Diskussion der Ergebnisse und deren Auswirkungen sowohl auf die Konzeption von Security-Frameworks als auch auf ihr Management.

Kapitel 6 spezifiziert die für das Management von Security-Frameworks erforderlichen **Managementprozesse** und die **technischen** sowie **organisatorischen prozessualen Schnittstellen**; durch seine Breite und Tiefe bildet es den Kern der managementspezifischen Betrachtungen von Security-Frameworks in dieser Arbeit. Als vorrangiges Ziel wird dabei konsequent die Integration betrachtet: Alle erarbeiteten Abläufe zielen darauf ab, die frameworkübergreifende, skalierbare Anwendung einheitlicher Managementmethoden und die nahtlose Einbettung aller Security-Frameworks in die bereits vorhandene IT-Infrastruktur ermöglichen, unterstützen, bewerten und kontinuierlich verbessern zu können.

Zu diesem Zweck wurde zunächst eine Differenzierung der beim praktischen Einsatz von Security-Frameworks relevanten Tätigkeiten einerseits im Rahmen des **Informationssicherheitsmanagements als Prozess** und andererseits im Kontext des **operativen Sicherheitsmanagements** vorgenommen. Dabei wurde die Entstehung des aktuellen Status Quo des Sicherheitsmanagements berücksichtigt und eine **Kategorisierung von Aufgaben**, die im Rahmen des operativen Sicherheitsmanagements anfallen, vorgenommen. Auf dieser Ba-

sis wurde die Entscheidung getroffen, die weiteren Analysen und Spezifikationen analog zu existierenden, aktuellen Standards und Best Practices zu strukturieren; als erste Konsequenz daraus ergab sich wiederum, dass das dort vorherrschende risikoorientierte Vorgehen auf das Management von Security-Frameworks übertragen werden musste. Hierzu wurde erarbeitet, welche Beiträge Security-Frameworks und die aus ihrem Betrieb resultierenden Sicherheitseigenschaften in die einzelnen Phasen des **Risikomanagements** – von der Identifikation von Bedrohungen bis hin zur Auswahl geeigneter Sicherheitsmaßnahmen – leisten können und gezeigt, dass Security-Frameworks maßgeblich zur Vereinfachung und effizienten Umsetzung ausgewählter Kernaktivitäten im Risikomanagement beitragen können. In ausgewählten Phasen des Risikomanagementprozesses wurden zudem Schnittstellen zu technikspezifischen Vorgehensweisen geschaffen; beispielsweise wurde aufgezeigt, wie sich praxisbewährte Verfahren wie CVSS2 zur Bewertung von Verwundbarkeiten im Kontext von Security-Frameworks nahtlos ins Risikomanagement einbetten lassen. Ausgehend von der spezifizierten Verzahnung des Managements von Security-Frameworks mit dem Risikomanagement nach NIST SP 800-30 wurde auch die **Übertragbarkeit auf weit verbreitete andere Risikomanagementmethoden**, z. B. nach ISO/IEC 27005, OCTAVE und dem ISACA Risk IT Framework, aufgezeigt.

Im Anschluss wurde eine **integrierte Managementarchitektur für Security-Frameworks** konzipiert. Nach einer motivierenden Betrachtung von Analogien, unter anderem zum Netz- und Systemmanagement, wurde der Schwerpunkt auf das **Informationsmodell** gelegt; es beschreibt die über die Komponenten von Security-Frameworks und die geschützten Assets sowie andere eingesetzte Sicherheitsmechanismen und Sicherheitswerkzeuge zu verwaltenden Informationen. Ergänzend wurden die Eckpunkte für die **Organisations-, Kommunikations- und Funktionsmodelle** abgesteckt und eine Vorgehensweise für die Umsetzung in Form von Managementplattformen spezifiziert. Ebenso wurden die Möglichkeiten zur konzeptionellen und technischen Integration bereits vorhandener Sicherheitswerkzeuge in diese Managementplattformen analysiert.

An diese Managementkonzepte anknüpfend wurden die prozessrelevanten Schnittstellen erarbeitet. Zum einen wurde **ISO/IEC 27001** analysiert, um die beim Einsatz von Security-Frameworks vertiefend zu betrachtenden Maßnahmen abzuleiten und zu konkretisieren. Zum anderen wurde das Zusammenspiel mit IT-Service-Management-Prozessen am Beispiel von **ITIL v3** spezifiziert, wobei insbesondere auf die Zusammenhänge zueinander komplementärer Prozesse – beispielsweise zur Integration des Security Incident Managements in das reguläre Incident Management – herausgearbeitet wurden. Alle erarbeiteten Konzepte wurden ferner in den Kontext der jeweiligen Lebenszyklusphasen und hinsichtlich der von Security-Frameworks jeweils konkret gelieferten Inhalte eingeordnet. Ergänzend wurden Prozesse und Aktivitäten aus dem Bereich IT-Governance und Compliance Management untersucht und bezüglich ihrer Auswirkungen auf das Management von Security-Frameworks bewertet.

Abschließend wurde in Kapitel 6 die Vorgehensweise bei der Konzeption, Akquisition und Aufbereitung von **Sicherheitskennzahlen beim Einsatz von Security-Frameworks** spezifiziert. Nach einer Betrachtung des Status Quo, die gezeigt hat, dass die Quantifizierung von Sicherheitseigenschaften unter anderem zu den *Hard Problems*, die vom INFOSEC Research Council gepflegt wird, zählt und bislang höchstens szenarienspezifisch, aber nicht organisationsübergreifend einheitlich ausgeprägt ist, wurde das **hypothesenorientierte Vorgehen** bei der Definition von Sicherheitskennzahlen vorgestellt und auf Security-Frameworks übertragen. Neben einem Informationsmodell für das **Management von Sicherheitskennzahlen und**

Sicherheitsberichten wurde eine Vorgehensweise für die **Erstellung zielgruppenspezifischer Sicherheitsberichte** konzipiert; die inhaltliche Strukturierung dieser Berichte ist dabei eng an den Abdeckungsgrad und die konzeptionellen Inhalte von Security-Frameworks angelehnt. Im Kontext der Auswertung dieser Sicherheitsberichte wurde schließlich gezeigt, wie das **Sicherheitsinvestitionskostenmodell** von Gordon und Loeb auf den Einsatz und das stufenweise Deployment von Security-Frameworks übertragen werden kann.

Kapitel 7 widmete sich der **Konzeption von Werkzeugen**, die Teile des Managements von Security-Frameworks automatisieren bzw. gezielt unterstützen. Die Analyse des Bedarfs an entsprechenden Werkzeugen orientierte sich wiederum konsequent am gesamten Lebenszyklus von Security-Frameworks, so dass unter anderem die Notwendigkeit von Planungs- und Simulationswerkzeugen, an für Security-Frameworks angepassten Risikomanagementwerkzeugen und Managementwerkzeugen für die frameworkübergreifend konsistente Umsetzung von Managementoperationen dargelegt wurde. Daran anschließend wurden zwei Werkzeuge vertiefend spezifiziert, die neben ihren sicherheitsfunktionalen Eigenschaften jeweils auch die erforderlichen Managementeigenschaften bereitstellen.

Als erstes detailliert betrachtetes Werkzeug wurde eine **Auswertestation für Intrusion Detection Systeme** konzipiert, mit der die u. a. **in Security-Frameworks enthaltenen Angriffserkennungssensoren dynamisch reparametrisiert** werden können, um auf Basis der erforderlichen Erkennungsleistung Betriebsressourcen einsparen und somit die partiell überlappenden Abdeckungsbereiche optimal ausnutzen zu können. Zunächst wurden dazu relevante Arbeiten aus dem Umfeld von Intrusion Detection Systemen analysiert und eine Abgrenzung der eigenen Beiträge vorgenommen. Als Grundlage wurde anschließend ein **Architekturkonzept für Sensoren und Auswertestationen** erstellt, das neben einem Gesamtüberblick auch detailliert auf die internen Abläufe in jedem Sensor, die Kommunikation mit einer zentralen Auswertestation und die in ihr verankerten Korrelations- und Steuerungsmechanismen eingeht. Zur Automatisierung der dynamischen Rekonfiguration wurde darauf aufbauend zunächst ein **Informationsmodell zur Sensorverwaltung** erarbeitet, das eine einheitliche Sicht auf die typischerweise sehr heterogenen Sensoren und deren individuelle Erkennungsfähigkeiten ermöglicht. Auf dieser Basis wurde ein **Funktionsmodell** spezifiziert, dessen Kern aus einer umfassenden Funktionsbibliothek besteht, die im Rahmen von Programmier- bzw. Policysprachen von der Auswertestation verwendet werden kann, um u. a. einzelne Sensoren bzw. deren Module zur Laufzeit zu- und abschalten bzw. umkonfigurieren zu können, um die jeweils aktuell benötigte Erkennungsleistung sicherzustellen. Im Rahmen eines umfassenden Anwendungsbeispiels wurde aufgezeigt, wie entsprechende Regelsätze zur Erkennung typischer SSH-Scan- und Brute-Force-Angriffe eingesetzt werden können. Die Ergebnisse einer **Simulation** dieses Anwendungsbeispiels wurden genutzt, um die bei gleichbleibender **Erkennungsleistung** erheblichen **Ressourceneinsparungen** zu analysieren und zu bewerten. Nach einer Spezifikation der prozessualen Einbettung des Werkzeugs wurde eine Reihe möglicher Weiterentwicklungen aufgezeigt, die u. a. den Informationsverlust bei verspäteter Zuschaltung einzelner Sensormodule kompensieren und auch den Einsatz in Szenarien mit erhöhtem Schutzbedarf der Assets ermöglichen.

Als zweites Werkzeug wurde ein **Managementsystem für IT-Sicherheitskennzahlen** spezifiziert, das alle Bereiche von der technischen Erfassung von Messwerten über deren Aufbereitung zu Indikatoren bis hin zur automatischen regelmäßigen Erstellung zielgruppenspezifischer Sicherheitsberichte abdeckt. Hierzu wurden zunächst Analogien und Unterschiede zu herkömmlichen Netz- und Systemmonitoringwerkzeugen aufgezeigt und die im Kontext

von Security-Frameworks spezifischen Anforderungen ermittelt. Darauf aufbauend wurde eine aus vier Schichten bestehende **Werkzeugarchitektur** spezifiziert, die neben einer manuellen Werkzeugnutzung mit rollenspezifischen Berechtigungen auch Schnittstellen zum automatisierten Datenaustausch mit anderen Managementwerkzeugen und somit u. a. eine **nahtlose Integration in ITSM-Reporting-Werkzeuge** ermöglicht. Neben den technischen Schnittstellen, mit denen z. B. die Sicherheitsbasiskennzahlen aus den Managementkomponenten von Security-Frameworks ausgelesen werden können, wurden auch die Prozesse, beispielsweise für das Lifecycle-Management von IT-Sicherheitskennzahlen, und die Workflows, z. B. für die Erstellung und Genehmigung von Sicherheitsberichten, sowie die Nutzung der erstellten Sicherheitsberichte im Kontext ausgewählter ITSM-Prozesse konzipiert. Nach einer Bewertung der erreichten Funktionalität wurden wiederum Möglichkeiten zur Weiterentwicklung skizziert, die u. a. eine stärkere Integration mit Echtzeitanalysen durch SIEM-Systeme ermöglichen würden.

9.1.3. Kapitel 8: Anwendungsbeispiel

Kapitel 8 verfolgte das Ziel, ein umfassendes Anwendungsbeispiel zu geben, das einen Großteil der erarbeiteten Konzepte, Methoden und Werkzeuge anhand eines realistischen Szenarios demonstriert. Mit **SuperMUC** wurde dabei ein komplexer, organisationsübergreifend genutzter High-Performance-Computing- und Grid-Computing-Dienst gewählt, der viele Abhängigkeiten von anderen Diensten in der bereits vorhandenen Infrastruktur aufweist und unter den in der Praxis üblichen terminlichen und finanziellen Randbedingungen bereitgestellt werden muss.

Nach einer Diskussion der szenarienspezifischen Ziele und der daraus resultierenden Priorisierung der Anforderungen an Security-Frameworks wurde zunächst die **Gesamtarchitektur des Systems** mit einigen grundlegenden Sicherheitsmechanismen, die sich durch die Einbettung des SuperMUC in die IT-Infrastruktur am LRZ ergeben, vorgestellt. Darauf aufbauend wurde das SuperMUC-spezifische **Customizing von drei Security-Frameworks** vorgestellt, die einen prinzipiell komplementären Charakter haben, sich in ausgewählten Bereichen jedoch bewusst überlappen.

Auf Basis der resultierenden technischen Sicherheitsarchitektur wurden die erforderlichen Anpassungen an den ITSM- und Sicherheitsmanagementprozessen im LRZ vorgestellt. Zur Verdeutlichung der Flexibilität der erarbeiteten Konzepte wurde dabei eine Strukturierung des Sicherheitsmanagements anhand präventiver, detektierender und reagierender Aktivitäten vorgenommen, statt die Beschreibungen wie in den vorangehenden Kapiteln anhand der Referenzprozesse in Normen wie ISO/IEC 27001 zu gliedern. In diesem Kontext wurde auch der **Einsatz der beiden Werkzeuge** zur dynamischen Reparametrisierung der Detektionssensorik und zur Erfassung und Auswertung von IT-Sicherheitskennzahlen demonstriert. Hierzu wurden u. a. rund 20 Hypothesen zur Einschätzung des erreichten Sicherheitsniveaus definiert und auf Kennzahlen, die von den eingesetzten Frameworkkomponenten geliefert werden können, abgebildet.

Anschließend wurden die Schwerpunkte in den weiteren Lebenszyklusphasen – von der Implementierung und Inbetriebnahme bis hin zur möglichen Übertragung auf Nachfolgesysteme – konzipiert. Die praktische Umsetzung dieser Konzepte ist mit einem **Investitions- und Betriebsaufwand** verbunden, der – gegliedert nach Personalaufwand bzw. Hard- und

Softwarekosten – im Anschluss analysiert wurde. Dabei hat sich gezeigt, dass er nur einen Bruchteil der Gesamtkosten für den Dienst beträgt und dass gegenüber einer herkömmlichen Vorgehensweise, bei der Sicherheitsmaßnahmen von Grund auf szenarienspezifisch konzipiert werden, erhebliche Einsparungen mit sich bringt.

Abschließend wurden die erreichten sicherheitsfunktionalen Eigenschaften in Relation zu den mit den Maßnahmen verbundenen Kosten bewertet und mögliche szenarienspezifische Weiterentwicklungen aufgezeigt.

9.1.4. Bewertung der Ergebnisse

Im Folgenden werden die wichtigsten Ergebnisse und wissenschaftlichen Beiträge dieser Arbeit eingeordnet, bewertet und auch hinsichtlich ihrer Verwertbarkeit durch Frameworkautoren und Frameworkanwender analysiert.

Die vorliegende Arbeit hat zunächst eine in ihrer Breite und Tiefe neue, **systematische Zerlegung** und Betrachtung von Fragestellungen rund um den Einsatz und die Verbesserung von Security-Frameworks vorgenommen und dabei insbesondere die Querbeziehungen zwischen dem Sicherheitsmanagement, dem konkreten Einsatz technischer Sicherheitsmechanismen und dem IT Service Management hergestellt. Bereits die auf Basis einer strukturierten Aufbereitung verschiedenster Einsatzszenarien ermittelten Anforderungen an Security-Frameworks gehen dabei weit über die in bisheriger Literatur behandelten Analysen hinaus. Entsprechende Recherchen und systematischen Zusammenstellungen wurden jedoch auch bei Teilaspekten vorgenommen: Die zur Anwendung auf Security-Frameworks erforderlichen Zusammenstellungen aktueller Methoden und Inhalte u. a.

- zur Untergliederung des Sicherheitsmanagementprozesses,
- zum operativen Sicherheitsmanagement,
- zum Risikomanagement und
- zu IT-Sicherheitskennzahlen

verfolgten denselben ganzheitlichen, strukturierenden Ansatz und lieferten zahlreiche neue, in bisheriger Literatur noch nicht erreichte Ergebnisse. Neben umfassenden Literaturrecherchen wurden jedoch auch empirische Methoden, beispielsweise zur Ermittlung der typischen Struktur von Frameworkkonzepten, erfolgreich angewandt.

Als wesentlicher Teilaspekt dieser strukturierten Zusammenstellungen wurde eine Reihe von **Klassifikationen und Kategorisierungen** vorgenommen, für die in der vorliegenden Vollständigkeit und thematischen Breite ebenfalls nicht auf umfassende Vorarbeiten zurückgegriffen werden konnte. Neben der Kategorisierung von Security-Frameworks per se betraf dies u. a. die von diesen häufig betrachteten Angriffe und die zur Auswahl angebotenen Gegenmaßnahmen sowie die Charakterisierung von Szenarien, in denen Security-Frameworks und andere IT-Sicherheitskonzepte eine wichtige Rolle spielen. Analog dazu wurde eine Reihe von **Definitionen und Spezifikationen** vorgenommen; dies umfasste beispielsweise Definition des Begriffs *Security-Framework* an sich mit der Differenzierung zwischen Konzepten und Instanzen, die Spezifikation von deren Lebenszyklen samt ihrer Zusammenhänge und Schnittstellen sowie die detaillierte Festlegung von Abläufen sowie von Rollen und Zuständigkeiten im Rahmen aller Lebenszyklusphasen und Managementprozesse.

Über den gesamten Themenbereich Security-Frameworks verteilt wurden zudem **neue Konzepte und Methoden** geschaffen:

- Aufgrund der konsequenten Betrachtung von Security-Frameworks als Abstraktionsebene aus Managementperspektive konnte eine **IT-sicherheitsspezifische Managementarchitektur** erarbeitet werden, die bisherige punktuelle, einzelwerkzeugorientierte Ansätze ablösen und für die parallele Verwaltung mehrerer Security-Frameworks und anderer Sicherheitsmechanismen effizient eingesetzt werden kann.
- Es wurden innovative, ergänzende **Werkzeugkonzepte** und ihre nahtlose Einbettung in die Managementabläufe spezifiziert. Beispielsweise wurde mit dem Werkzeug zum weitgehend automatisierten Management von Sicherheitskennzahlen und Sicherheitsberichten, das auch auf die Spezifika von Security-Frameworks eingeht, ein wichtiger Beitrag zum aktuellen und auf massives industrielles Interesse stoßende Thema *security metrics* geliefert. Er liefert zudem eine bislang in fast allen Frameworkkonzepten fehlende Möglichkeit zur quantitativen Bewertung des Einsatzes und praktischen Betriebs von Security-Frameworks.
- Zudem wurden explizite **Schnittstellen-, Abhängigkeits- und Auswirkungsdefinitionen** zwischen Security-Frameworks und den ITSM- und Sicherheitsmanagementprozessen vorgenommen, deren Umfang und Detaillierungs- sowie Konkretisierungsgrad erheblich über die Spezifikationen der Referenzprozesse z. B. in ITIL v3 und ISO/IEC 27001 hinausgeht; auch die Spezifikation der konkreten Einbettung von Managementwerkzeugen in die für Security-Frameworks spezifischen Managementprozesse betrat konzeptionelles Neuland gegenüber den vormals in sich abgeschlossenen Frameworkkonzepten.

Ferner bleibt bemerkenswert, dass auch von bisherigen Arbeiten nicht näher berücksichtigte Aspekte vertiefend bearbeitet wurden. Beispielsweise wurden nicht nur Anforderungen *an Security-Frameworks*, sondern auch *an Szenarien*, in denen Security-Frameworks eingesetzt werden sollen, und sämtliche Lebenszyklusphasen bis hin zur Außerbetriebnahme von Security-Frameworks spezifiziert.

Die erarbeiteten Konzepte tragen auch zu einer Reihe konkreter methodischer **Verbesserungen** bei. So wurde zunächst in Form einer einfach zu nutzenden Checkliste spezifiziert, wie die Dokumentation von Frameworkkonzepten besser strukturiert und vervollständigt werden kann. Anschließend wurden Referenzprozesse für das IT Service Management und das Sicherheitsmanagement durch die bislang fehlende, explizite Spezifikation der zu betrachtenden Schnittstellen angereichert. Die effiziente Anwendung von Risikomanagementmethoden wurde im Kontext von Security-Frameworks durch die konkrete Benennung der Zusammenhänge in den einzelnen Teilabläufen und die Übertragung der erarbeiteten Konzepte auf mehrere Standards und Best Practices unterstützt. Ferner trug die umfassende Integration dynamischer Steuerungsmöglichkeiten unter Berücksichtigung der Fähigkeiten vorhandener Sensorik zur konsequenten Weiterentwicklung von Intrusion Detection Systemen bei; mit der Erarbeitung eines generischen Informationsmodells zur Sensorverwaltung und der Konzeption eines Bewertungsschemas für den Vergleich des Aufwands bei IDS-Auswertungen wurden weitere bewährte Ansätze aufgegriffen, verallgemeinert und in den größeren Kontext eingebettet.

Ferner wurde eine Reihe von Methoden auf das Management von Security-Frameworks **übertragen bzw. angewandt**. Dies umfasst beispielsweise

- die Untersuchung von Netz- und Systemmanagement- sowie Konfigurationsmanagementkonzepten als konzeptionelles Vorbild für Sicherheitsmanagementarchitekturen,
- die Übertragung von Investitionskostenmodellen auf die Planung des Einsatzes und Ausbaus von Security-Frameworks und
- die Orientierung von Frameworklebenszyklen am SDLC bzw. an den ITSM-Lebenszykluskonzepten.

Zudem wurden ausgewählte Konzepte für organisationsübergreifendes IT Service Management auf den Einsatz von Security-Frameworks in Unternehmensverbünden und in gemischten Umgebungen, in denen Komponenten von Security-Frameworks sowohl organisationsintern als auch im inter-organisatorischen Kontext eingesetzt werden, übertragen. Die zielgerichteten Anwendungen bestehender Konzepte und Verfahren umfassen

- den Einsatz von Security-Engineering-Methoden auf die Entwicklung und Anwendung von Security-Frameworks, insbesondere zur Umsetzung der Paradigmen *secure-by-design*, *secure-by-default*, *secure-in-deployment* und *defense-in-depth*;
- die Spezifikation eines szenarienspezifisch adaptierbaren Bewertungsverfahrens mit hierarchisch strukturierten Kriterien;
- die Verwendung policy-basierter Managementarchitekturen auf die Konfiguration von Security-Frameworks und deren Managementwerkzeuge;
- die Integration von Softwareentwicklungsmodellen in Security-Framework-Einführungsprojekte im Kontext der Implementierung szenarienspezifischer Schnittstellenkomponenten unter Hinzunahme aktueller Ansätze beispielsweise für die modellbasierte Sicherheitstestautomatisierung;
- den Einsatz u. a. von Bewertungsverfahren wie CVSS2 und Bedrohungsmatrizen zur Planung und Charakterisierung des Betriebs von Security-Frameworks.

Schließlich wurden zahlreiche **Einordnungen und Bewertungen** vorgenommen, die ebenfalls Neuerungen gegenüber bisherigen Arbeiten darstellen. Hierzu gehört beispielsweise die strategische Einordnung von Security-Frameworks in Informationssicherheitsmanagementsysteme und die Abläufe u. a. im Risikomanagement, im IT Service Management nach ITIL v3 und im operativen Sicherheitsmanagement. Zudem wurden über 75 aktuelle Security-Frameworks in die ermittelten Kategorien eingeordnet und anhand des Kriterienkatalogs beurteilt, um Verbesserungsvorschläge für die Weiterentwicklung zu identifizieren und Gemeinsamkeiten bzw. Trends zu identifizieren.

Einige dieser Ergebnisse stellen nicht nur wissenschaftliche Beiträge dar, sondern können auch von **Autoren von Security-Framework-Konzepten** wie folgt unmittelbar weiterverwendet werden:

- Die erstellte Checkliste für Frameworkautoren enthält Vorgaben für die Struktur und die wesentlichen Inhalte von Frameworkdokumentationen. Sie kann sowohl für neue Security-Frameworks als auch für neue Versionen bereits existierender Security-Frameworks eingesetzt werden. Neben aus Managementperspektive zu erfüllenden Anforderungen wird dabei auch der gesamte Lebenszyklus des Security-Frameworks betrachtet.

- Im Rahmen der Status-Quo-Analyse wurden konkrete Anregungen für die weitere Verbesserung von über 75 Security-Frameworks erarbeitet.
- Die erstellten Architektur- und Werkzeugkonzepte können als Grundlage für das Management zukünftiger Security-Frameworks verwendet werden.
- Frameworkautoren gewinnen durch die vorliegende Arbeit Hintergrundinformationen zum praktischen Einsatz und Management von Security-Frameworks, die bei der Konzeption berücksichtigt werden können. Durch die Beschreibung der Verzahnung z. B. mit dem Risikomanagement ergeben sich auch Verknüpfungen mit Abläufen außerhalb des rein operativen Security-Framework-Betriebs.
- Das umfassende Anwendungsbeispiel zeigt die Kombination mehrerer Security-Frameworks innerhalb eines Szenarios auf und trägt damit zum Verständnis praktischer Zielsetzungen und Randbedingungen bei.

Auch für die **Anwender von Security-Frameworks**, also Organisationen, die Security-Frameworks einsetzen, betreiben und mit Managementsystemen verwalten möchten, ergeben sich unmittelbare Vorteile:

- Der erarbeitete Kriterienkatalog dient zusammen mit der spezifizierten Anpassungsmethodik als Grundlage für die Bewertung, Gegenüberstellung und Auswahl von Security-Frameworks in eigenen Szenarien. Die zu seiner Ableitung beschriebenen Szenarien und Hintergrundinformationen sowie das umfassende Anwendungsbeispiel dienen zudem zur Heranführung an die Thematik und leisten zusammen mit der Analyse von Anforderungen an Szenarien eine Hilfestellung bei der Vorbereitung der eigenen Umgebung auf den Einsatz von Security-Frameworks.
- Die Status-Quo-Analyse gibt einen Überblick über derzeit aktuelle Ausprägungen von Security-Frameworks und deren typische Stärken und Schwächen.
- Die detaillierte Spezifikation des Lebenszyklus von Frameworkinstanzen kann als Leitfaden für eigene Security-Framework-Einführungsprojekte dienen, da sie u. a. bei der Benennung der jeweils verantwortlichen Rollen sowie der zu erstellenden Dokumente und Deliverables hilft und die jeweiligen Tätigkeitsschwerpunkte pro Lebenszyklusphase vorgibt.
- Die Arbeit gibt einen umfassenden Überblick über die Managementabläufe und die Schnittstellen zum gesamten Spektrum an IT-Service-Management- und Sicherheitsmanagementprozessen. Ferner werden konkrete Methoden, z. B. für das Risikomanagement, den Einsatz sicherheitsspezifischer Managementwerkzeuge, das Sicherheitsberichtswesen, die technische Integration u. a. von Angriffserkennungssensorik, die für Security-Frameworks spezifischen Aufgaben im operativen Sicherheitsmanagement und zum Einsatz von Sicherheitsmanagementplattformen vorgegeben.
- Die neu konzipierten Werkzeuge zur Verbesserung der Ressourcennutzung durch die dynamische Adaption der Sensoraktivität im Umfeld von Intrusion Detection Systemen und zur quantitativen Bewertung des erreichten Sicherheitsniveaus auf Basis zielgruppenspezifischer Sicherheitsberichte können in eigenen Szenarien flexibel eingesetzt werden.

Trotz dieser Ergebnisse und des Umfangs der vorliegenden Arbeit konnten einige Teilaspekte nicht umfassend bearbeitet und einige Teilfragestellungen nicht vollständig gelöst werden. Im

folgenden Abschnitt wird deshalb auf mögliche Anschlussarbeiten und Weiterentwicklungen eingegangen.

9.2. Ausblick auf mögliche Weiterentwicklungen

Weitere Arbeiten, die unmittelbar auf den vorliegenden Ergebnissen aufbauen können, lassen sich grob in die drei Kategorien *konzeptionelle Weiterentwicklungen*, *Implementierung* und *praktische Anwendung* einteilen.

Konzeptionelle Weiterentwicklungen betreffen zunächst nicht nur die in dieser Arbeit spezifizierten Methoden, sondern insbesondere auch die untersuchten Security-Frameworks: Auf Basis der ermittelten Anforderungen wurden bereits individuelle Verbesserungsvorschläge erarbeitet. Unter Anwendung der neuen Konzepte zum gesamten Lebenszyklus, zu den Managementprozessen und zum Einsatz von Werkzeugen können im jeweiligen Security-Framework bislang fehlende Lösungsbestandteile erarbeitet und bisher nur schwach ausgeprägte Aspekte vertieft werden. Zu wünschen ist in diesem Kontext insbesondere eine konsequentere Umsetzung des Prinzips der kontinuierlichen Verbesserung mit kürzeren, beispielsweise jährlichen Releasezyklen; sie beugt nicht nur der sicherheitsfunktionalen bzw. inhaltlichen Veraltung der Frameworkkonzepte vor, sondern ermöglicht auch ein stufenweises Vorgehen bei der Integration der Vielzahl der in dieser Arbeit vorgestellten Managementkonzepte. Als einer der thematischen Schwerpunkte bei der Weiterentwicklung einzelner Frameworkkonzepte ist die Definition von frameworkspezifischen Sicherheitskennzahlen zu sehen, da diese Aufgabe unmittelbar relevant für den praktischen Einsatz der Security-Frameworks und mit hohem konzeptionellen Aufwand verbunden ist.

Im Kontext verbesserter Security-Frameworks, deren Eigenschaften mit Sicherheitskennzahlen beurteilt werden kann, müssen auch verbesserte Methoden zur Bewertung der sicherheitsfunktionalen Eigenschaften konzipiert werden. Während in der vorliegenden Arbeit die Managementeigenschaften im Vordergrund standen, stellt die erzielte technische Schutzwirkung der von einem Security-Framework vorgegebenen Komponenten ein szenarienspezifisches, für die Auswahl und den Einsatz ausschlaggebendes Kriterium dar. Unter Einbezug der bereits hier an Security-Frameworks angepassten Abläufe, beispielsweise im Risikomanagement, sind deshalb Vorgehensweisen beim Vergleich von Sicherheitsmechanismen zu erarbeiten, die nicht nur die Frameworkkonzepte für sich, sondern auch bereits im Anwendungsszenario vorhandene Schutzkomponenten geeignet berücksichtigen.

Weitere Aufgaben im Rahmen der konzeptionellen Weiterentwicklung betreffen die untersuchten Managementprozesse: Zum einen wurden in Kapitel 6 zwar für ein breites Spektrum an ITSM-Prozessen und verschiedenste Teile des Sicherheitsmanagements alle wesentlichen, beim Einsatz von Security-Frameworks zu berücksichtigenden *Schnittstellen* konzipiert; die explizite Spezifikation von *Referenzprozessen*, wie sie als methodischer Ansatz beispielsweise auch von ITIL verfolgt wird, wurde jedoch nur für ausgewählte Teile wie das Risikomanagement vorgenommen. Zur Vertiefung und als Leitfaden für die praktische Umsetzung sind deshalb in ihrer Gesamtheit ausgeführte Prozessbeschreibungen zu erarbeiten, die alle hier konzipierten Schnittstellen umsetzen. Um eine noch breitere praxisrelevante Abdeckung zu erzielen, sind neben ITIL auch weitere prozessbasierte Ansätze, beispielsweise das am Rande betrachtete MOF, zu untersuchen; mit dem in Abschnitt 6.5 vorgestellten Konzept des *process mapping*

wurden bereits die Grundlagen für die Übertragung der im Kontext von ISO/IEC 27001 und ITIL erarbeiteten Ergebnisse gelegt.

Schließlich sind die hier geleisteten konzeptionellen Arbeiten in Bezug auf ihre Anwendungsbereiche und ihre Skalierbarkeit weiter auszubauen: Der Fokus der vorliegenden Arbeit lag auf dem Einsatz von Security-Frameworks in Organisationen und organisationsübergreifenden Verbünden mit einem als regulär einzustufenden IT-Sicherheitsbedarf. In Anschlussarbeiten ist deshalb zum einen die Anwendung und Verbesserung in Umgebungen mit erhöhtem Schutzbedarf, beispielsweise bei militärischen Anwendungen und beim Schutz kritischer Infrastrukturen, zu betrachten. Zum anderen sind für kleinere Umgebungen bis hin zu Heimanwender-Szenarien Vereinfachungen vorzunehmen, wobei insbesondere auch auf die Aufgabenverteilung zwischen den Herstellern, den Betreibern und den eigentlichen Anwendern – beispielsweise beim Einsatz von *Smart Metern* bei der Stromversorgung – eingegangen werden muss. Für alle Anwendungsgebiete ist zudem die Automatisierung der konzipierten Managementabläufe zu vertiefen, der insbesondere bei hochgradig verteilten Systemen eine Schlüsselrolle bezüglich der Skalierbarkeit der eingesetzten Sicherheitsmaßnahmen zukommt.

Ein weiterer Schwerpunkt möglicher Weiterentwicklungen liegt auf der **Implementierung** der in dieser Arbeit vorgestellten Konzepte und Werkzeuge, die bislang nur partiell bzw. in Form von Simulationen vorgenommen wurde. Die Kernkomponente stellt dabei die in Kapitel 6 konzipierte Managementplattform für Security-Frameworks dar. Ihre Realisierung setzt die am Beispiel der Anwendung im Rahmen des Risikomanagements durchgeführte Ermittlung von Anwendungsfällen (*use cases*) für alle betrachteten Prozesse voraus und erfordert die Implementierung technischer Schnittstellen zur Integration der betrachteten Sicherheitsmanagementwerkzeuge.

Ferner sind die detailliert spezifizierten Werkzeugkonzepte umzusetzen: Für die Implementierung der dynamischen Reparametrisierung von Angriffserkennungssensoren bietet sich dabei die Erweiterung weit verbreiteter Open Source Intrusion Detection Systeme wie *Snort*, *bro* oder *Prelude* an, so dass bestehende Implementierungen von Angriffserkennungs- und Korrelationsmechanismen wiederverwendet werden können. Eine von Grund auf neue Implementierung bietet sich hingegen für die konzipierte Security-Reporting-Architektur an, da sie die in Kapitel 7 erörterten Unterschiede zu bereits vorhandenen Managementwerkzeugen, beispielsweise für das Netz- und Systemmonitoring, aufweist und somit eine für die praktische Anwendung passende Basisplattform noch fehlt.

Konzeptionell zu vertiefen und zu implementieren sind schließlich auch die weiteren in Kapitel 7 skizzierten Werkzeuge: Ein hoher praktischer Bedarf besteht einerseits an Planungs- und Simulationswerkzeugen, die unter Berücksichtigung der im Anwendungsszenario bereits vorhandenen Sicherheitsmaßnahmen den Einsatz von Security-Frameworks bzw. deren Einzelkomponenten sowohl aus der Perspektive der Investitionskostenrechnung als auch zur Beurteilung des zu erwartenden sicherheitsspezifischen Mehrwerts bewerten und zugleich als Basis z. B. für die Durchführung proaktiver Penetrationstests dienen. Ebenso werden Werkzeuge benötigt, die über die Grenzen von Security-Frameworks hinweg und somit hersteller- und komponentenübergreifend Konzepte für die Verwaltung und Umsetzung von Sicherheitsparametern ermöglichen: Beispielsweise werden die einzusetzenden Verschlüsselungsalgorithmen für unterschiedliche Dienste wie VPN und Backup praktisch meist unabhängig von verschiedenen IT-Betriebsabteilungen festgelegt und unterschiedliche Werkzeuge für das Ausrollen von PKI-Zertifikaten eingesetzt, ohne dass sich daraus neben dem administrativen Mehr-

aufwand sicherheitsspezifische Vorteile ergeben; für die konsistente Umsetzung der Vorgaben aus Sicherheitsrichtlinien werden entsprechend neuartige Steuerungs- und Kontrollwerkzeuge benötigt.

Als dritter Schwerpunkt der möglichen Weiterentwicklungen ist die **praktische Anwendung** zu betrachten. Sie umfasst zunächst die reale Umsetzung der in dieser Arbeit entwickelten Konzepte und Methoden in konkreten Szenarien und ist, wie bereits die Diskussion des fiktiven SuperMUC-Anwendungsbeispiels in Kapitel 8 gezeigt hat, mit einem proportional angemessenen, aber nicht zu vernachlässigenden Aufwand verbunden. Letztlich können viele der erarbeiteten Ergebnisse erst beim Vorliegen praktischer Erfahrungen gezielt evaluiert und bewertet werden und dadurch wiederum zur weiteren Verbesserung der Konzepte beitragen.

Eine zentrale Voraussetzung für die praktische Beurteilung dieser Verfahren ist der Aufbau eines auf präzise definierten Sicherheitskennzahlen basierenden Sicherheitsberichtswesens. Dieses kann auf Basis des vorgestellten Werkzeugkonzepts nicht nur für Security-Frameworks und deren Managementprozesse etabliert, sondern auch auf bereits vorhandene Sicherheitsmaßnahmen und -mechanismen angewandt werden. Dadurch wird es über die Beurteilung der vorgelegten Konzepte hinausgehend möglich, den praktischen Einsatz der zu einem Szenario passenden Security-Frameworks mit der bislang üblichen, von Grund auf neu durchgeführten szenarienspezifischen Sicherheitskonzeption zu vergleichen und unter Aspekten wie Zeitaufwand und Gesamtbetriebskosten (engl. *total cost of ownership*) zu beurteilen.

Das Vorliegen umfassender praktischer Erfahrungen ist schließlich die Grundlage für weiterführende Schritte zur Aufnahme der neuen Konzepte in Best-Practice-Werke und Standards: Während sich die bislang sehr technische Ausprägung der Konzepte von Security-Frameworks inhibitorisch auf ihre Berücksichtigung in prozessorientierten Werken wie ITIL und ISO/IEC 27001 auswirkte, hat die inhärente Eigenschaft von Security-Frameworks, zusammengehörende Sicherheitsmaßnahmen zu aggregieren, in Kombination mit den nunmehr definierten Managementprozessen und -schnittstellen ein hohes Potential, sofern der resultierende Mehrwert für ein breites Spektrum an Organisationen auch praktisch nachgewiesen werden kann.

9.3. Ausblick auf offene Forschungsaufgaben in verwandten Bereichen

Neben der Weiterentwicklung und Umsetzung der in dieser Arbeit dargelegten Konzepte und Methoden ergibt sich an vielen Stellen der Bedarf an weiterführenden Arbeiten in eng verwandten Bereichen. Im Folgenden werden ausgewählte Themen, die Berührungspunkte zu den vorgelegten Ergebnissen aufweisen, skizziert.

Im Bereich **Sicherheitsmanagement** ergibt sich zunächst der Bedarf an organisationsübergreifenden Prozessen, die noch stärker auf organisatorische Aspekte eingehen: Zwar existieren bereits ausgereifte technische Lösungen, beispielsweise für Trust Level Management und Identity Management bzw. für ausgewählte Verbundformen wie das Grid-Computing, und organisationsübergreifende ITSM-Prozesse wie das Incident Management und das Configuration Management. Für sicherheitsspezifische Prozesse wie das Risikomanagement, die Behandlung von Sicherheitsvorfällen, die Zuweisung von Zuständigkeiten und Verantwortlichkeiten, das

Sicherheitsberichtswesen und die Abstimmung von Sicherheitsparametern kommen organisationsübergreifend bislang jedoch nur szenarienspezifische und oftmals ad hoc gewählte Abläufe zum Einsatz. Die Spezifikation von Referenzprozessen und die Konzeption von Methoden für verschiedene Betriebsmodelle, die von der herkömmlichen Ausgliederung von Betriebsprozessen bis hin zur kooperativen Diensterbringung reichen und die durch Virtualisierung unter dem Stichwort Cloud Computing ermöglichte Dynamik berücksichtigen, sind deshalb condiciones sine quibus non für den sicheren Betrieb zukünftiger verteilter IT-Infrastrukturen.

Für die hier primär im Kontext von Security-Frameworks thematisierten Sicherheitskennzahlen werden Best Practices und Standards benötigt. Neben der organisationsübergreifenden Vergleichbarkeit erreichter Sicherheitsniveaus, die auch außerhalb von Organisationsverbünden – beispielsweise bei der Beurteilung und Auswahl von IT-Dienstleistern – erforderlich ist, sind auch Maßnahmen zur Auditierung und Zertifizierung zu konzipieren, die über die derzeit bereits für IT-Produkte angebotene qualitative Analyse durch neutrale Dritte hinausgehen. Als wesentliche Grundlage müssen hierfür zunächst Programmier- und Kommunikationsschnittstellen zur Sicherstellung der maschinellen Verarbeitbarkeit und als Basis für den organisationsübergreifenden Austausch von Sicherheitskennzahlen spezifiziert werden.

Im Umfeld **technischer Sicherheitsmechanismen** hat sich zum einen gezeigt, dass Intrusion Detection Systeme, obwohl sie bereits seit über zwei Jahrzehnten im Einsatz und bewährt sind, noch weiter ausgebaut werden müssen. Neben IDS-Ansätzen, die nicht nur dynamisch, sondern auch kooperativ agieren, um die Skalierbarkeit und die Erkennungsleistung über den Einzugsbereich einer einzelnen Analysestation hinaus zu verbessern, werden IDS-Architekturen zunehmend nicht nur im Unternehmensumfeld, sondern aufgrund der fortschreitenden Vernetzung der Haustechnik auch in stark dezentralisierten Umgebungen benötigt. Hierfür müssen insbesondere branchenübergreifende Lösungen, an denen unter anderen Energieversorger, Telekommunikationsunternehmen und Elektronikhersteller mitwirken, erarbeitet werden. Zum anderen dient der größte Teil technischer Sicherheitsmaßnahmen dem Schutz vor externen Angreifern oder wird primär zu diesem Zweck eingesetzt; dadurch, dass verteilte Systeme zunehmend komplexer werden und somit zu ihrem Betrieb ein immer größer werdender Personenkreis beitragen muss, steigt jedoch auch der Bedarf an einem Schutz vor Innentätern. Somit werden zukünftig auch verstärkt Konzepte, Mechanismen und Werkzeuge zur Vorbeugung, Erkennung und Behandlung von so genannten *Insider Threats* benötigt.

Auch für das **Security Engineering** ergibt sich der Bedarf an weiteren Methoden und Werkzeugen: Während für die Forschung und Lehre im Bereich der Rechnernetze ausgereifte Simulations- und Testwerkzeuge wie der Network Simulator *ns-3* zur Verfügung stehen, fehlen bislang entsprechende universell anwendbare Hilfsmittel für das Security Engineering, mit denen zu schützende Infrastrukturen und Dienste, technische Sicherheitsmaßnahmen und angreifende Systeme effizient modelliert, variiert, erprobt und analysiert werden können. Die Ergebnisse entsprechender Untersuchungen sollten direkt in den Entwicklungsprozess der analysierten Software und Systeme eingebracht und mit anderen Beurteilungskriterien kombiniert werden können; stellvertretend sei hierfür die Beurteilung der Benutzerfreundlichkeit genannt: Während diese bereits methodisch auf viele Teile der Gestaltung von Benutzeroberflächen und Webanwendungen erfolgreich angewandt wird, fehlen bislang einheitliche Kriterien für die Beurteilung der Anwenderfreundlichkeit komplexerer Sicherheitsmechanismen.

Abschließend ist anzumerken, dass trotz der bereits vorhandenen Vielfalt an Security-Frameworks auch weiterhin zahlreiche, weit verbreitete IT-Dienste und IT-Architekturen exis-

tieren und laufend neu entstehen, für die bislang noch keine ganzheitlichen, szenarienübergreifend anwendbaren Sicherheitslösungen erarbeitet wurden. Auch zukünftig werden deshalb flexibel anpassbare Sicherheitsmaßnahmen und deren Komposition zu innovativen Security-Frameworks dringend benötigt.

Anhang A.

Literaturverzeichnis

[AAAK08] Walid Al-Ahmad und Reem Al-Kaabi: *An extended security framework for e-government.* In: *Proceedings of the 2008 IEEE International Conference on Intelligence and Security Informatics.* IEEE, 2008. (Zitiert auf den Seiten 143 und 220.)

[AB02] C. Adams und S. Boeyen: *UDDI and WSDL extensions for Web service: a security framework.* In: *Proceedings of the 2002 ACM workshop on XML security*, Seiten 30–35. ACM New York, NY, USA, 2002. (Zitiert auf den Seiten 141 und 179.)

[ACRYPT] Bruce Schneier: *Applied Cryptography.* ISBN 0-471-12845-7, John Wiley & Sons Verlag, 1996. (Zitiert auf Seite 145.)

[ADA01] Christopher J. Alberts, Audrey J. Dorofee und Julia H. Allen: *OCTAVE Catalog of Practices, Version 2.0.* `http://www.sei.cmu.edu/library/abstracts/reports/01tr020.cfm`, 2001. (Zitiert auf den Seiten 336 und 357.)

[AFJ08] Aliya Awais, Muddassar Farooq und Muhammad Younus Javed: *Attack analysis & bio-inspired security framework for IP multimedia subsystem.* In: *Proceedings of the 10th annual conference on Genetic and evolutionary computation - GECCO '08*, New York, 2008. ACM Press. (Zitiert auf den Seiten 144 und 224.)

[AH08] Suhair Hafez Amer und John A. Hamilton: *Understanding Security Architecture.* In: *Proceedings of SpringSim 2008*, Seiten 335–342. IEEE, 2008. (Zitiert auf Seite 314.)

[AHP] Thomas Saaty: *Relative Measurement and its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors – The Analytic Hierarchy/Network Process.* Review of the Royal Spanish Academy of Sciences, Series A, Mathematics, 102(2):251–318, Juni 2008. (Zitiert auf Seite 126.)

[AICP10] Auditing Standards Board of the American Institute of Certified Public Accountants: *Statement on Auditing Standards No. 70: Service Organizations (SAS 70), ISO/IEC 27001 NIST SP 800-53 Control Mapping Templates.* `http://www.sas70checklists.com/isoiec-27001-nist-sp-800-53-control-mapping-templates`, 2010. (Zitiert auf Seite 393.)

[AJ03] Joerg Abendroth und Christian D. Jensen: *A Unified Security Framework for Networked Applications.* In: *Proceedings of SAC 2003.* ACM, 2003. (Zitiert auf den Seiten 142, 188 und 189.)

[All04] J.H. Allen: *Building a Practical Framework for Enterprise-Wide Security Management.* In: *Secure IT Conference Networked Systems Survivability.* California State University, 2004. (Zitiert auf den Seiten 144, 225 und 226.)

[Amo94] Edward Amoroso: *Fundamentals of Computer Security Technology.* ISBN 0-13-108929-3, Prentice Hall, 1994. (Zitiert auf Seite 339.)

[ANC+10] Joao Antunes, Nuno Neves, Miguel Correia, Paulo Verissimo und Rui Neves: *Vulnerability Discovery with Attack Injection.* IEEE Transactions on Software Engineering, 36(3):357–370, Mai 2010. (Zitiert auf Seite 286.)

[And07] Andrew Jaquith: *Security Metrics — Replacing Fear, Uncertainty, and Doubt.* Addison-Wesley Longman, Amsterdam, ISBN 978-0321349989, 2007. (Zitiert auf den Seiten 437, 439, 440, 441, 447, 502, 503 und 508.)

[Ande08] Ross Anderson: *Security Engineering, second edition.* ISBN 978-0-470-06852-6, Wiley Publishing, 2008. (Zitiert auf den Seiten 17, 35, 344 und 352.)

[AS03] A. Alkassar und C. Stüble: *Security framework for integrated networks.* In: *Proceedings of MILCOM 2003.* IEEE, 2003. (Zitiert auf den Seiten 144 und 235.)

[ASM06] Ali Abbas, Abdulmotaleb El Saddik und Ali Miri: *Internet Security Approach: Design of an internet's security taxonomy.* In: *Proceedings of 19th IEEE Canadian Conference on Electrical and Computer Engineering.* IEEE, 2006. (Zitiert auf Seite 39.)

[Bar07] Yuliy Baryshnikov: *IT Security Investment and Gordon-Loeb's 1/e rule.* `http://ect.bell-labs.com/who/ymb/pub.html`, 2007. (Zitiert auf Seite 451.)

[Bas91] R. Baskerville: *Risk analysis as a source of professional knowledge.* Computers & Security, 10(9):749–764, 1991. (Zitiert auf Seite 347.)

[BBF03] M. Barni, F. Bartolini und T. Furon: *A general framework for robust watermarking security.* Signal Processing, 83(10):2069–2084, 2003. (Zitiert auf den Seiten 141 und 182.)

[BBH+03] R. Breu, K. Burger, M. Hafner, J. Jürjens, G. Popp, G. Wimmel und V. Lotz: *Key Issues of a Formally Based Process Model for Security Engineering.* In: *ICSSEA 2003 - Sixteenth International Conference Software & Systems Engineering & their Applications*, Paris, 2003. (Zitiert auf Seite 38.)

[BBNC01] M.R. Blackburn, R.D. Busser, A.M. Nauman und R. Chandramouli: *Model-based Approach to Security Test Automation*, 2001. (Zitiert auf Seite 286.)

[BDL06] David Basin, Jürgen Doser und Torsten Lodderstedt: *Model driven security: From UML models to access control infrastructures.* ACM Transactions on Software Engineering and Methodolology, 15(1):39–91, 2006. (Zitiert auf Seite 2.)

[Ber08] Scott Berinato: *A Few Good Information Security Metrics.* `http://www.csoonline.com/article/print/220462`, 2008. (Zitiert auf Seite 441.)

[Bewe01] Robert Adunka: *Infoportal Bewerten der Universität Erlangen.* `http://www.mfk.uni-erlangen.de/~bewerten/`, 2007. (Zitiert auf Seite 108.)

[BGL08] Lawrence Bodin, Lawrence Gordon und Martin Loeb: *Information Security and Risk Management.* Communications of the ACM, 51(4), 2008. (Zitiert auf Seite 347.)

[BGRH09] Aaron Beach, Mike Gartrell, Baishakhi Ray und Richard Han: *Secure SocialAware: A Security Framework for Mobile Social Networking Applications.* Technischer Bericht CU-CS-1054-09, University of Colorado at Boulder, 2009. (Zitiert auf den Seiten 144 und 233.)

[BGS06] Michael Brenner, Markus Garschhammer und Martin Sailer: *CMDB-Yet Another MIB? On Reusing Management Model Concepts in ITIL Configuration Management.* In: *Proceedings of Distributed Systems: Operations and Management (DSOM 2006)*, Seiten 269–280. Springer, 2006. (Zitiert auf Seite 366.)

[BL03] A. Bassi und J. Laganier: *Towards an IPv6-based security framework for distributed storage resources.* In: *Proceedings of CMS 2003, LNCS 2828.* Springer, 2003. (Zitiert auf den Seiten 143 und 205.)

[BMBF11] Referat IT-Systeme im Bundesministerium für Bildung und Forschung (BMBF): *Supercomputer und Exportkontrolle – Hinweise zu internationalen wissenschaftlichen Kooperationen.* `http://www.bmbf.bund.de/pub/supercomputer_und_exportkontrolle.pdf`, 2011. (Zitiert auf den Seiten 544 und 578.)

[Bohm10] Rainer Böhme: *Security Metrics and Security Investment Models.* In: *Proceedings of IWSEC 201, LNCS 6434*, Seiten 10–24. Springer, 2010. (Zitiert auf den Seiten 435 und 449.)

[Bou09] Latifa Boursas: *Trust–Based Access Control in Federated Environments.* Dissertation, Technische Universität München, München, 2009. (Zitiert auf Seite 544.)

[Bre07] Brenner, Michael: *Werkzeugunterstützung für ITIL-orientiertes Dienstmanagement – Ein modellbasierter Ansatz.* ISBN: 3-837-002-012, Books on Demand, 2007. (Zitiert auf Seite 322.)

[BRS06] S.G. Batsell, N.S. Rao und M. Shankar: *Distributed Intrusion Detection and Attack Containment for Organizational Cyber Security.* `http://www.ioc.ornl.gov/projects/documents/containment.pdf`, 2006. (Zitiert auf den Seiten 144 und 227.)

[Bry00] Ciaran Bryce: *A Security Framework for a Mobile Agent System.* In: F. Cuppens (Herausgeber): *Proceedings of ESORICS 2000, LNCS 1895*, Seiten 273–290. Springer, 2000. (Zitiert auf den Seiten 141 und 172.)

[BS00] B. Schneier: *Secrets & Lies – Digital Security in a Networked World.* ISBN 0-471-25311-1, Verlag John Wiley & Sons, 2000. (Zitiert auf Seite 2.)

[BSI08a] BSI: *Managementsysteme für Informationssicherheit (ISMS).* BSI-Standard 100-1, Bundesamt für Sicherheit in der Informationstechnik, 2008. (Zitiert auf Seite 320.)

[BSI08b] BSI: *Risikoanalyse auf der Basis von IT-Grundschutz.* BSI-Standard 100-3, Bundesamt für Sicherheit in der Informationstechnik, 2008. (Zitiert auf den Seiten 319 und 351.)

[BSIGSK] Bundesamt für Sicherheit in der Informationstechnik: *BSI IT-Grundschutz-Kataloge, Stand 9. Ergänzungslieferung.* ISBN 978-3-88784-915-3, Bundesanzeiger-Verlag, 2007. (Zitiert auf den Seiten 1, 17 und 21.)

[BSISMS] Alfred Scheerhorn und Jens Nedon: *Studie zu ISO-Normungsaktivitäten ISO/BPM – Anforderungen an Information Security Management Systeme.* Technischer Bericht ISO-BPM-ISMS 040305, Bundesamt für Sicherheit in der Informationstechnik, 2004. (Zitiert auf Seite 53.)

[BUGTRQ] SecurityFocus: *Bugtraq electronic mailing list.* `http://www.securityfocus.com/archive/1`, 2008. (Zitiert auf Seite 38.)

[Bur05] Mark Burgess: *A Tiny Overview of Cfengine: Convergent Maintenance Agent.* In: *Proceedings of the 1st International Workshop on Multi-Agent and Robotic Systems, MARS/ICINCO.* Springer, 2005. (Zitiert auf Seite 384.)

[C40DT] IT Governance Institute: *CobiT 4.0 – Deutsche Ausgabe.* ISBN 1-933284-37-4, 2005. (Zitiert auf Seite 319.)

[Can07] Catharina Candolin: *A security framework for service oriented architectures.* In: *Proceedings of MILCOM 2007.* IEEE, 2007. (Zitiert auf den Seiten 143 und 217.)

[CCS+10] Hao Chen, John a. Clark, Siraj a. Shaikh, Howard Chivers und Philip Nobles: *Optimising IDS Sensor Placement.* In: *2010 International Conference on Availability, Reliability and Security*, Seiten 315–320. IEEE, Februar 2010. (Zitiert auf Seite 463.)

[CDH05] K. Clark, J. Dawkins und J. Hale: *Security risk metrics: Fusing enterprise objectives and vulnerabilities.* In: *Proceedings of SMC'05*, Seiten 388–393. IEEE, 2005. (Zitiert auf Seite 346.)

[CFZA02] M.J. Covington, P. Fogla, Z. Zhan und M. Ahamad: *A Context-Aware Security Architecture for Emerging Applications.* In: *Proceedings of 18th Annual Computer Security Applications Conference (ACSAC 2002)*, 2002. (Zitiert auf den Seiten 143 und 206.)

[Che07] Tong-sheng Che: *A Policy Language for Adaptive Web Services Security Framework.* In: *Proceedings of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, Seiten 261–266. IEEE, 2007. (Zitiert auf den Seiten 141 und 170.)

[CK09] S. Chandra und R.A. Khan: *Software security metric identification framework (SSM).* In: *Proceedings of the International Conference on Advances in Computing, Communication and Control – ICAC3 '09*, Seiten 725–731. ACM Press, 2009. (Zitiert auf Seite 438.)

[CKPH05] Scott Cantor, John Kemp, Rob Philpott und Eve Maler (Hrsg.): *Security Assertion Markup Language v2.0.* OASIS Security Services Technical Committee Standard, 2005. (Zitiert auf Seite 99.)

[CM05] A. Charfi und M. Mezini: *Using aspects for security engineering of web service compositions.* In: *Proceedings of the 2005 IEEE International Conference on Web Services.* IEEE, 2005. (Zitiert auf den Seiten 141 und 180.)

[CM07] E. Cachia und M. Micallef: *A Multi-Tier, Multi-Role Security Framework for E-Commerce Systems.* In: *Proceedings of the 14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems.* IEEE Computer Society, 2007. (Zitiert auf den Seiten 141 und 169.)

[CNP06] Antonio Capone, Stefano Napoli und Alberto Pollastro: *MobiMESH: An Experimental Platform for Wireless MESH Networks with Mobility Support.* In: *Proceedings of QShine'06.* ACM Press, 2006. (Zitiert auf Seite 229.)

[CobiT4] IT Governance Institute: *CobiT 4.1 – Framework, Control Objectives, Management Guidelines, Maturity Models.* ISBN 1-933284-72-2, 2007. (Zitiert auf den Seiten 21, 24 und 25.)

[Coin11] Stephan Zimprich: *Firmen im Visier der Online-Erpresser.* `http://www.wiwo.de/technik-wissen/firmen-im-visier-der-online-erpresser-482717/2/`, 2011. (Zitiert auf Seite 571.)

[CRK+10] Duncan Clough, Stefano Rivera, Michelle Kuttel, Vincent Geddes und P. Marais: *Panopticon: a scalable monitoring system.* In: *Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists*, Seiten 39–47. ACM, 2010. (Zitiert auf Seite 504.)

[CSF05] V. Cridlig, R. State und O. Festor: *An Integrated Security Framework for XML based Management.* In: *9th IFIP/IEEE International Symposium on Integrated Network Management*, Seiten 587–600. IEEE, 2005. (Zitiert auf den Seiten 142 und 190.)

[CSTT06] A. Cater-Steel, W.G. Tan und M. Toleman: *Challenge of adopting multiple process improvement frameworks.* In: *Proceedings of the 14th European Conference on Information Systems*, Seiten 1–12, 2006. (Zitiert auf Seite 393.)

[CSYW07] Richard A. Caralli, James F. Stevens, Lisa R. Young und William R. Wilson: *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* `http://www.cert.org/octave/allegro.html`, 2007. (Zitiert auf Seite 358.)

[Dad02] Nou Dadoun: *Security Framework for IP Telephony White Paper.* `http://ftp.tiaonline.org/TR-41/TR4144inactive/Public/2002-02-Vancouver/TR41.4.4-02-02-008SecurityFrameworknd.pdf`, 2002. (Zitiert auf den Seiten 142 und 200.)

[Demi86] W. Edwards Deming: *Out of the Crisis.* ISBN 0-911379-01-0, MIT Center for Advanced Engineering Study, 1986. (Zitiert auf Seite 21.)

[DFS07] Vitalian A. Danciu, Nils gentschen Felde und Martin Sailer: *Declarative Specification of Service Management Attributes.* In: *Proceedings of the 10th IFIP/IEEE International Symposium on Integrated Network Management*, Seiten 429–438. IEEE, Mai 2007. (Zitiert auf den Seiten 506 und 507.)

[DGBC04] A. Detsch, L. P. Gaspary, M. P. Barcellos und G. G. H. Cavalheiro: *Towards a flexible security framework for peer-to-peer based grid computing.* In: *Proceedings of the 2nd workshop on Middleware for grid computing.* ACM Press, 2004. (Zitiert auf den Seiten 144 und 240.)

[DKM01] R.J. Detry, S.D. Kleban und P.C. Moore: *The Generalized Security Framework.* Technischer Bericht, Sandia Report SAND2001-8338, 2001. (Zitiert auf den Seiten 141 und 178.)

[DMTF11] DMTF: *Common Information Model v2.28.0.* `http://www.dmtf.org/standards/cim`, 2011. (Zitiert auf Seite 366.)

[DPR06] Kurt Dillard, Jared Pfost und Stephen Ryan: *The Security Risk Management Guide.* `http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c782b6d3-28c5-4dda-a168-3e4422645459`, 2006. (Zitiert auf den Seiten 344 und 355.)

[DS00] Premkumar T. Devanbu und Stuart Stubblebine: *Software engineering for security: a roadmap.* In: *ICSE '00: Proceedings of the Conference on The Future of Software Engineering*, Seiten 227–239, New York, NY, USA, 2000. ACM. (Zitiert auf Seite 37.)

[DS05] Vitalian A. Danciu und Martin Sailer: *A monitoring architecture supporting service management data composition.* In: *Proceedings of the 12th Annual Workshop of HP OpenView University Association.* ISBN 972–9171–48–3, 2005. (Zitiert auf Seite 506.)

[DSG05] M.L. Das, A. Saxena und V.P. Gulati: *A security framework for mobile-to-mobile payment network.* In: *IEEE International Conference on Personal Wireless Communications.* IEEE, 2005. (Zitiert auf den Seiten 142 und 187.)

[DuCo10] Dublin Core Metadata Initiative: *Dublin Core Metadata Element Set, Version 1.1.* `http://dublincore.org/documents/dces/`, 2010. (Zitiert auf Seite 372.)

[Ecke09] Claudia Eckert: *IT-Sicherheit: Konzepte - Verfahren - Protokolle, 6. Auflage.* ISBN 978-3-486-58999-3, Oldenbourg Wissenschaftsverlag, 2009. (Zitiert auf den Seiten 6, 15, 17, 18, 28, 32, 336, 344 und 351.)

[EFN09] Andreas Ekelhart, Stefan Fenz und Thomas Neubauer: *AURUM: A framework for information security risk management.* In: *42nd Hawaii International Conference on System Sciences*, Seiten 1–10. IEEE, 2009. (Zitiert auf Seite 341.)

[Elo03] J.H.P. Eloff: *Information security management: a new paradigm.* In: *Proceedings of SAICSIT 2003*, Seiten 130–136, 2003. (Zitiert auf Seite 313.)

[Eng07] Tom Engel: *Evaluierung und Positionierung biometrischer Authentisierungsverfahren bei der BMW Group.* Diplomarbeit, Ludwig-Maximilians-Universität München, März 2007. (Zitiert auf Seite 106.)

[EPALW3] Calvin Powers und Matthias Schunter: *Enterprise Privacy Authorization Language, W3C member submission.* `http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/`, 2003. (Zitiert auf Seite 546.)

[Ert08] Volkan Ertürk: *A framework based on continuous security monitoring.* Master Thesis, The Middle East Technical University, 2008. (Zitiert auf Seite 441.)

[EvSS06] Christian Eibl, Basie von Solms und Sigrid Schubert: *A Framework for Evaluating the Information Security of E-Learning Systems.* In: *Proceedings of the 2nd Internation Conference on Informatics in Secondary Schools*, Vilnius, Litauen, 2006. Springer. (Zitiert auf Seite 100.)

[Fel08] Nils Otto vor dem gentschen Felde: *Ein föderiertes Intrusion Detection System für Grids.* Doktorarbeit, Ludwig-Maximilians-Universität München, 2008. (Zitiert auf Seite 464.)

[Fen10] Stefan Fenz: *From the Resource to the Business Process Risk Level.* In: *Proceedings of the South African Information Security Multi-Conference*, Seiten 1–9, 2010. (Zitiert auf Seite 346.)

[fIS09] The Center for Internet Security: *The CIS Security Metrics 2009 - Consensus Metric Definitions v1.0.0*, 2009. (Zitiert auf Seite 441.)

[For11] TM Forum: *TM Forum's Information Framework (SID).* `http://www.tmforum.org/InformationFramework/1684/home.html`, 2011. (Zitiert auf Seite 366.)

[FPW07] Ulrich Faisst, Oliver Prokein und Nico Wegmann: *Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen.* Zeitschrift für Betriebswirtschaft, 77(5):511–538, Mai 2007. (Zitiert auf Seite 452.)

[GAB+10] Geri Georg, Kyriakos Anastasakis, Behzad Bordbar, Siv Hilde Houmb, Indrakshi Ray und Manachai Toahchoodee: *Verification and Trade-Off Analysis of Security Properties in UML System Models.* IEEE Transactions on Software Engineering, 36(3):338–356, Mai 2010. (Zitiert auf Seite 281.)

[GBFP01] D. Gupta, T. Buchheim, B. Feinstein und R. Pollock: *IAP: Intrusion Alert Protocol.* `http://tools.ietf.org/html/draft-ietf-idwg-iap-05`, 2001. (Zitiert auf Seite 470.)

[GG03] C.H. Gebotys und R.J. Gebotys: *A framework for security on NoC technologies.* In: *Proc of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI'03).* IEEE, 2003. (Zitiert auf den Seiten 143 und 208.)

[GH10] Stephan Graf und Wolfgang Hommel: *Informationsmanagement in Hochschulen*, Kapitel Organisationsübergreifendes Management von Föderations-Sicherheitsmetadaten auf Basis einer Service-Bus-Architektur, Seiten 233–246. ISBN-13: 978-3642047190, Springer, 2010. (Zitiert auf Seite 459.)

[GHJ03] D. Geer, K.S. Hoo und A. Jaquith: *Information security: why the future belongs to the quants.* IEEE Security & Privacy Magazine, 1(4):24–32, 2003. (Zitiert auf Seite 433.)

[GL02] Lawrence A. Gordon und Martin P. Loeb: *The economics of information security investment.* ACM Transactions on Information and System Security, 5(4):438–457, November 2002. (Zitiert auf Seite 449.)

[GL06] Lawrence a. Gordon und Martin P. Loeb: *Budgeting process for information security expenditures.* Communications of the ACM, 49(1):121–125, Januar 2006. (Zitiert auf den Seiten 449 und 452.)

[GLL03] Lawrence Gordon, Martin P. Loeb und William Lucyshyn: *Information Security Expenditures and Real Options: A Wait-and-See Approach.* Computer Security Journal, XIX(2), 2003. (Zitiert auf Seite 452.)

[GR06] Kapil Kumar Gupta und Kotagiri Ramamohanarao: *Network Security Framework.* Journal of Computer Science and Network Security, 6(7B):151–157, 2006. (Zitiert auf den Seiten 144 und 231.)

[Gra02] Frank Graf: *Providing security for eLearning.* Computers & Graphics, 26(2):355–365, 2002. (Zitiert auf den Seiten 95 und 100.)

[Graf09] Stefan Graf: *Durchgängiges Identity Management und interoperable E-Portfolios zur Unterstützung lebenslangen Lernens.* Doktorarbeit, Technische Universität München, München, 2009. (Zitiert auf Seite 95.)

[GS01] Rajeev Gopalakrishna und E.H. Spafford: *A framework for distributed intrusion detection using interest driven cooperating agents.* In: *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID 2001)*, Seiten 1–23, 2001. (Zitiert auf den Seiten 470 und 473.)

[GT06] V. Gunupudi und S.R. Tate: *SAgent: A Security Framework for JADE.* In: *Proceedings of the fifth international joint conference on Autonomous agents and multiagent systems.* ACM, 2006. (Zitiert auf den Seiten 141 und 177.)

[HAN99] Heinz-Gerd Hegering, Sebastian Abeck und Bernhard Neumair: *Integriertes Management vernetzter Systeme — Konzepte, Architekturen und deren betrieblicher Einsatz.* dpunkt-Verlag, ISBN 3-932588-16-9, Januar 1999. (Zitiert auf den Seiten 3, 53, 289, 361, 363, 364, 365, 366, 379, 380 und 383.)

[Har06] G. Hardy: *Guidance on Aligning COBIT, ITIL and ISO 17799.* Information Systems Control Journal, 1, 2006. (Zitiert auf Seite 393.)

[HBB+05] Andreas Hanemann, J. Boote, E. Boyd, Jérôme Durand, Loukik Kudarimoti, R. Lapacz, D. Swany, Szymon Trocha und Jason Zurawski: *Perfsonar: A service oriented architecture for multi-domain network monitoring.* In: *Proceedings of Service-Oriented Computing (ICSOC 2005)*, Seiten 241–254. Springer, 2005. (Zitiert auf Seite 505.)

[HC04] Angeli Hoekstra und Nicolette Conradie: *CobiT, ITIL and ISO 17799: How to use them in conjunction.* `http://www.cccure.org/Documents/COBIT/COBIT_ITIL_and_BS7799.pdf`, 2004. (Zitiert auf Seite 393.)

[HCCT03] K.S. Hong, Y.P. Chi, L.R. Chao und J.H. Tang: *An integrated system theory of information security management.* Information Management and Computer Security, 11:243–248, 2003. (Zitiert auf Seite 314.)

[Hen02] Ronda Henning: *Workshop on Information Security System Scoring and Ranking.* Applied Computer Security Associates, 2002. (Zitiert auf Seite 435.)

[HFvE+10] Wolfgang Hommel, Nils Otto vor dem gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott: *Architekturkonzept für ein Grid-basiertes IDS.* `http://www.grid-ids.de/documents/GIDS_MS16-1.pdf`, 2010. (Zitiert auf Seite 464.)

[Hin08] Gary Hinson: *7 myths about security metrics.* `http://www.noticebored.com/html/metrics.html`, 2008. (Zitiert auf Seite 441.)

[HK05] W. Heinbockel und M. Kwon: *Phyllo: a peer-to-peer overlay security framework.* In: *1st IEEE ICNP Workshop on Secure Network Protocols (NPSec).* IEEE, 2005. (Zitiert auf den Seiten 144 und 232.)

[HLP+09] Vicente Hernandez, Lourdes Lopez, Oscar Prieto, José-F. Martinez, Ana-B. Garcia und Antonio Da Silva: *Security Framework for DPWS Compliant Devices.* In: *Proceedings of Third International Conference on Emerging Security Information, Systems and Technologies*, Seiten 87–92. IEEE, Juni 2009. (Zitiert auf den Seiten 142 und 199.)

[HO06] F. Hansen und V. Oleshchuk: *Location-based security framework for use of handheld devices in medical information systems.* In: *Proceedings of Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, Pisa, Italy.* IEEE, 2006. (Zitiert auf den Seiten 142 und 193.)

[Hom08a] Wolfgang Hommel: *Using Policy-based Management for Privacy-Enhancing Data Access and Usage Control in Grid Environments.* In: *Proceedings 8th IEEE International Symposium on Cluster Computing and the Grid (CCGrid'08)*, Lyon, France, May 2008. IEEE Press. (Zitiert auf Seite 540.)

[Homm07] Wolfgang Hommel: *Architektur- und Werkzeugkonzepte für föderiertes Identitäts-Management.* Dissertation, Ludwig-Maximilians-Universität, München, 2007. (Zitiert auf den Seiten 90, 99, 548 und 560.)

[Homm09] Wolfgang Hommel: *Using Policy-based Management for Privacy-Enhancing Data Access and Usage Control in Grid Environments.* International Journal of Grid and High Performance Computing, 1(2):15–29, April 2009. (Zitiert auf den Seiten 91 und 540.)

[Homm11] Wolfgang Hommel: *Cloud, Grid and High Performance Computing: Emerging Applications*, Kapitel A policy-based security framework for privacy-enhancing data access and usage control in Grids, Seiten 118–134. ISBN-13: 978-1-60960-603-9, IGI Global, 2011. (Zitiert auf den Seiten 540 und 547.)

[HPVULC] HP Invent: *HP Open Source Middleware Stacks White Paper: Security of Open Source Middleware Stacks.* Technischer Bericht 5991–7435, Hewlett-Packard, 2006. (Zitiert auf Seite 29.)

[HS98] P.C. Hyland und Ravi Sandhu: *Management of Network Security Applications.* In: *NCSC National Information Systems Security*, 1998. (Zitiert auf den Seiten 325 und 366.)

[HSHJ08] T. Heyman, R. Scandariato, C. Huygens und W. Joosen: *Using security patterns to combine security metrics.* In: *Proceedings of the Third International Conference on Availability, Reliability and Security*, Seiten 1158–1165. IEEE Computer Society, 2008. (Zitiert auf Seite 446.)

[Hua05] D. Huang: *Semantic policy-based security framework for business processes.* In: *4th Semantic Web and Policy Workshop*, Seiten 2–7. Springer, 2005. (Zitiert auf den Seiten 144, 236 und 237.)

[Hub10] Florian Huber: *Konzeption und Implementierung von Sicherheitsmetriken und -berichten für das Identity & Access Management im MWN*, 2010. Diplomarbeit

an der Ludwig-Maximilians-Universität München, Institut für Informatik, 2010. (Zitiert auf den Seiten 441, 517 und 518.)

[Hul08] George Hulme: *Balanceakt Compliance – IT-Security oder ein zufriedener Prüfer?* http://www.searchsecurity.de/themenbereiche/sicherheits-management/compliance/articles/111884/, 2008. (Zitiert auf Seite 324.)

[Hum08] E. Humphreys: *Information security management standards: Compliance, governance and risk management.* Information Security, 13(4):247–255, November 2008. (Zitiert auf den Seiten 314 und 394.)

[Hump87] Watts Humphrey: *Characterizing the Software Process: A Maturity Framework.* IEEE Software, 56(2):73–79, März 1987. (Zitiert auf Seite 60.)

[HW03] D. Hutchinson und M. Warren: *Security for Internet banking: a framework.* Logistics Information Management, 16(1):64–73, 2003. (Zitiert auf den Seiten 142 und 198.)

[HW04] J. Hu und A.C. Weaver: *A dynamic, context-aware security infrastructure for distributed healthcare applications.* In: *Proceedings of First Workshop on Pervasive Security, Privacy and Trust (PSPT)*, Seiten 1–8. IEEE, 2004. (Zitiert auf den Seiten 141 und 181.)

[I20k1] ISO/IEC 20000-1:2005: *Information technology – Service management – Part 1: Specification.* International Organization for Standardization and International Electrotechnical Commission, 2005. (Zitiert auf Seite 322.)

[I27001] ISO/IEC 27001:2005: *Information technology – Security techniques – Information security management systems – Requirements.* International Organization for Standardization and International Electrotechnical Commission, 2005. (Zitiert auf den Seiten 17, 28, 53 und 258.)

[I27004] ISO/IEC 27004:2009: *Information technology - Security techniques - Information security management - Measurement.* International Organization for Standardization and International Electrotechnical Commission, 2009. (Zitiert auf den Seiten 439 und 441.)

[I27005] ISO/IEC 27005:2008: *Information technology – Security techniques – Information security risk management.* International Organization for Standardization and International Electrotechnical Commission, 2008. (Zitiert auf Seite 355.)

[I7498] ISO 7498-2:1989: *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.* International Organization for Standardization, 1989. (Zitiert auf Seite 310.)

[IHPL05] INFOSEC Research Council: *INFOSEC Hard Problem List.* http://www.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf, 2005. (Zitiert auf Seite 433.)

[ISA09] ISACA: *The Risk IT Framework.* ISBN 978-1-60420-111-6, 2009. (Zitiert auf den Seiten 355 und 357.)

[ISFSGP] Information Security Forum: *The Standard of Good Practice for Information Security.* http://www.isfstandard.com/, 2007. (Zitiert auf Seite 21.)

[ISO89] ISO/IEC 7498-4:1989: *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management framework.* International Organization for Standardization and International Electrotechnical Commission, 1989. (Zitiert auf Seite 365.)

[ISO27k] ISO/IEC 27000-series:2005: *ISMS Family of Standards on Information technology – Security techniques – Information security management systems.* International Organization for Standardization and International Electrotechnical Commission, 2005. (Zitiert auf den Seiten 1, 17 und 21.)

[ITILv3] Office of Government Commerce (OGC): *IT Infrastructure Library v3: Service Design, 2nd impression.* ISBN 978-0113310470, The Stationery Office (TSO), 2007. (Zitiert auf den Seiten 21 und 34.)

[Jah02] Marko Jahnke: *An open and secure infrastructure for distributed intrusion detection sensors.* In: *Proceedings of the NATO Regional Conference on Communication and Information Systems (RCMCIS'02), Zegrze, Polen*, 2002. (Zitiert auf Seite 500.)

[Jan09] Wayne Jansen: *Directions in Security Metrics Research, NISTIR 7564.* National Institute of Standards and Technology Report, 2009. (Zitiert auf den Seiten 434, 435, 436 und 440.)

[JBHB03] P. Jaferian, D. Botta, K. Hawkey und K. Beznosov: *Design guidelines for IT security management tools.* In: *Proceedings of the SOUPS Workshop on Usable IT Security Management (USM).* ACM Press, 2003. (Zitiert auf Seite 145.)

[Jurj02] Jan Jürjens: *Using UMLsec and goal trees for secure systems development.* In: *SAC '02: Proceedings of the 2002 ACM symposium on Applied computing*, Seiten 1026–1030, New York, 2002. ACM. (Zitiert auf Seite 38.)

[Kar03] Frank Kargl: *Sicherheit in Mobilen Ad hoc Netzwerken.* Dissertation, Fakultät für Informatik, Universität Ulm, 2003. (Zitiert auf den Seiten 144 und 238.)

[KBT06] Pandurang Kamat, Arati Baliga und Wade Trappe: *An Identity-Based Security Framework For VANETs.* In: *Proceedings of VANET 2006.* ACM, 2006. (Zitiert auf den Seiten 143 und 221.)

[KE03] Chris Kaler und Anthony Nadalin (Eds.): *Web Services Federation Language (WS-Federation).* `http://www-106.ibm.com/developerworks/webservices/library/ws-fed/`, 2003. (Zitiert auf Seite 46.)

[Keo05] Sye Loong Keoh: *A Policy-based Security Framework for Ad-hoc Networks.* Ph.D.-Thesis, Imperial College London, 2005. (Zitiert auf den Seiten 143 und 213.)

[KFJ03] L. Kagal, T. Finin und A. Joshi: *A policy based approach to security for the semantic web.* In: *Proceedings of ISWC 2003, LNCS 2870.* Springer, 2003. (Zitiert auf den Seiten 143 und 212.)

[Kir05] Phongsak Kiratiwintakorn: *Energy efficient security framework for wireless local area networks.* Ph.D.-Thesis, University of Pittsburgh, 2005. (Zitiert auf den Seiten 142, 149, 159 und 160.)

[KK08] Heinrich Kersten und Gerhard Klett: *Sicherheitsmanagement – die tägliche Praxis.* In: *Der IT Security Manager.* Vieweg+Teubner, 2008. (Zitiert auf Seite 326.)

[Kla11] Klarl, Heiko: *Zugriffskontrolle in Geschäftsprozessen – Ein modellgetriebener Ansatz.* ISBN 3-834-814-652, Vieweg+Teubner, 2011. (Zitiert auf Seite 314.)

[KLH+07] Geon Woo Kim, Deok Gyu Lee, Jong Wook Han, Sang Choon Kim und Sang Wook Kim: *Security Framework for Home Network: Authentication, Authorization, and Security Policy.* In: *Proceedings of PAKDD 2007, LNAI 4819*, Seiten 621–628. Springer, 2007. (Zitiert auf den Seiten 144 und 234.)

[KMY10] Leanid Krautsevich, Fabio Martinelli und Artsiom Yautsiukhin: *Formal approach to security metrics - What does more secure mean for you?* In: *Proceedings of ECSA 2010.* IEEE, 2010. (Zitiert auf Seite 435.)

[KR09] Hoon Ko und Carlos Ramos: *A Study on Security Framework for Ambient Intelligence Environment.* In: *Proceedings of the 5th International Conference on Wireless and Mobile Communications.* IEEE, 2009. (Zitiert auf den Seiten 144 und 223.)

[Kro10] S. Kronschnabl: *Konzeption eines Modells zur Bestimmung des optimalen Investitionsbeitrags in IT-Sicherheits- bzw. IT-Notfallmaßnahmen unter Berücksichtigung Compliance-bedingter Anforderungen.* In: *Proceedings der Wirtschaftsinformatik 2010.* Univ.-Verl. Göttingen, 2010. (Zitiert auf Seite 452.)

[KV05] R.A. Kemmerer und Giovanni Vigna: *Hi-DRA: Intrusion detection for Internet security.* Proceedings of the IEEE, 93(10):1848–1857, 2005. (Zitiert auf Seite 473.)

[Lab11] NIST Information Technology Laboratory: *The Security Content Automation Protocol (SCAP).* `http://scap.nist.gov/`, 2011. (Zitiert auf Seite 341.)

[Lan06a] Sebastian Lange: *Formalisierung von Aggregationsvorschriften für Dienstinformationen.* Diplomarbeit, Ludwig-Maximilians-Universität München, Institut für Informatik, 2006. (Zitiert auf Seite 506.)

[Lan06b] H. Langweg: *Framework for malware resistance metrics.* In: *Proceedings of the 2nd ACM workshop on Quality of protection.* ACM, 2006. (Zitiert auf Seite 437.)

[LGZ97] Jussipekka Leiwo, Ana Gamage und Yuliang Zheng: *A Framework for the Management of Information Security.* In: *Proceedings of the 1997 Information Security Workshop (ISW'97)*, 1997. (Zitiert auf den Seiten 312 und 313.)

[LSM+98] P.A. Loscocco, S.D. Smalley, P.A. Muckelbauer, R.C. Taylor, S.J. Turner und J.F. Farrell: *The inevitability of failure: The flawed assumption of security in modern computing environments.* In: *Proceedings of the 21st National Information Systems Security Conference.* IEEE, 1998. (Zitiert auf Seite 147.)

[Mao09] Tingting Mao: *Interoperable Internet-Scale Security Framework for RFID Networks.* Ph.D.-Thesis, Massachusetts Insitute of Technology, 2009. (Zitiert auf den Seiten 144 und 230.)

[Mar11] Patricia Marcu: *Architekturkonzepte für interorganisationales Fehlermanagement.* Doktorarbeit, Ludwig-Maximilians-Universität München, 2011. (Zitiert auf Seite 379.)

[MB03] G.K. Mostéfaoui und P. Brezillon: *A generic framework for context-based distributed authorizations.* In: *Proceedings of CONTEXT 2003, LNAI 2680.* Springer, 2003. (Zitiert auf den Seiten 140 und 168.)

[MB06] Mark Merkow und James Breithaupt: *Information Security: Principles and Practices.* ISBN 9780131547292, Prentice Hall, 2006. (Zitiert auf Seite 326.)

[ME01] A. Martins und J.H.P. Eloff: *Measuring Information Security.* Technischer Bericht, Rand Afrikaans University, 2001. (Zitiert auf Seite 439.)

[MHL+03] P. Mell, Vincent Hu, R. Lippmann, Josh Haines und Marc Zissman: *NIST IR 7007: An overview of issues in testing intrusion detection systems.* NIST Internal Report, National Institute of Standards and Technology, 2003. (Zitiert auf Seite 500.)

[MHR11] Stefan Metzger, Wolfgang Hommel und Helmut Reiser: *Integriertes Management von Sicherheitsvorfällen.* In: *Proceedings des 18. DFN-Workshops Sicherheit in vernetzten Systemen*, 2011. (Zitiert auf Seite 328.)

[Mic05] Microsoft: *The STRIDE Threat Model.* `http://msdn.microsoft.com/library/ms954176.aspx`, 2005. (Zitiert auf Seite 339.)

[Mic10] Microsoft: *Security Development Lifecycle Version 5.0.* `http://www.microsoft.com/sdl/`, 2010. (Zitiert auf den Seiten 37 und 281.)

[MIT11a] MITRE: *A Standardized Common Event Expression (CEE) for Event Interoperability.* `http://cee.mitre.org/`, 2011. (Zitiert auf Seite 384.)

[MIT11b] MITRE: *Common Vulnerabilities and Exposures – The Standard for Information Security Vulnerability Names.* `http://cve.mitre.org/`, 2011. (Zitiert auf den Seiten 332 und 348.)

[ML05] C. Marnewick und L. Labuschagne: *A security framework for an ERP system.* Technischer Bericht, Academy for Information Technology, University of Johannesburg, Auckland Park, South Africa, 2005. (Zitiert auf den Seiten 141 und 185.)

[MMD+03] J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla und Anandha Murukan: *Threat Modeling – DREAD.* `http://msdn.microsoft.com/en-us/library/ff648644.aspx`, 2003. (Zitiert auf Seite 348.)

[MP00] R. Molva und A. Pannetrat: *Scalable multicast security with dynamic recipient groups.* ACM Transactions on Information and System Security (TISSEC), 3(3):136–160, 2000. (Zitiert auf den Seiten 142 und 196.)

[MP05] J. Magiera und A. Pawlak: *Security Frameworks for Virtual Organizations*, Kapitel 2.3 in Virtual Organizations: Systems and Practices, Seiten 133–148. Springer, 2005. (Zitiert auf den Seiten 144, 236 und 237.)

[MPTP] Phillip Hallam-Baker: *Micro Payment Transfer Protocol (MPTP).* W3C Working Draft WS-mptp-951122, November 1995. (Zitiert auf Seite 80.)

[MS03] Kevin D. Mitnick und William L. Simon: *The Art of Deception: Controlling the Human Element of Security*. Wiley & Sons, ISBN 978-0764542800, 2003. (Zitiert auf Seite 40.)

[MSR07] Peter Mell, Karen Scarfone und Sasha Romanosky: *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*. `http://www.first.org/cvss/cvss-guide.html`, 2007. (Zitiert auf den Seiten 258, 348 und 350.)

[N80010] Pauline Bowen, Joan Hash und Mark Wilson: *Information Security Handbook: A Guide for Managers*. NIST Special Publication 800-100, Oktober 2006. (Zitiert auf Seite 21.)

[NJ07] Steven Noel und Sushil Jajodia: *Attack graphs for sensor placement, alert prioritization, and attack response*. In: *Proceedings of CyberSpace Research Workshop*, Seiten 3–20. George Mason University, 2007. (Zitiert auf Seite 463.)

[NSA04] NSA: *Guide to Microsoft .NET Framework Security*. `http://www.nsa.gov/ia/_files/app/oldFiles/NET_Framework_Sec1.pdf`, 2004. (Zitiert auf den Seiten 141, 175 und 176.)

[Oet09] Tobias Oetiker: *Round Robin Database Tool RRDtool Documentation*. `http://oss.oetiker.ch/rrdtool/`, 2009. (Zitiert auf Seite 505.)

[OGSDP] Bob Blakley und Craig Heath: *Security Design Patterns*. The Open Group, ISBN: 1-931624-27-5, 2004. (Zitiert auf Seite 38.)

[OLH06] C. Onwubiko, A.P. Lenaghan und L. Hebbes: *An Integrated Security Framework for Assisting in the Defense of Computer Networks*. In: *Proceeding of the Joint IST Workshop on Sensor Networks & Symposium on Trends in Communications, SymptoIC'06, Bratislava*. IEEE, 2006. (Zitiert auf den Seiten 143 und 222.)

[Olo92] Tomas Olovsson: *A structured approach to computer security*. `http://www.cs.plu.edu/courses/netsec/arts/tr122.pdf`, 1992. (Zitiert auf Seite 312.)

[OWASP] OWASP Foundation: *Open Web Application Security Project (OWASP)*. `http://www.owasp.org/index.php/Main_Page`, 2010. (Zitiert auf den Seiten 38 und 338.)

[Pay07] Shirley Payne: *A guide to security metrics*, 2007. (Zitiert auf Seite 440.)

[PC09] Stefano Paris und Antonio Capone: *Implementation of a Security Framework for Wireless Multi-hop Networks*. In: *Proceedings of Q2SWinet'09*. ACM Press, 2009. (Zitiert auf den Seiten 144 und 229.)

[PC10] Shari Lawrence Pfleeger und Robert K. Cunningham: *Why Measuring Security Is Hard*. IEEE Security & Privacy Magazine, 8(4):46–54, Juli 2010. (Zitiert auf Seite 436.)

[Pet07] Gunnar Peterson: *Security Architecture Blueprint*. Arctec Group, LCC Technical Report, `http://www.arctecgroup.net/`, 2007. (Zitiert auf den Seiten 53, 314 und 315.)

[Pet08] Nicolai Munk Petersen: *Security Framework for Mobile Applications*. Technischer Bericht, University of California, Los Angeles, CA, USA, 2008. (Zitiert auf den Seiten 142 und 201.)

[PGSP07] C.E. Pigeot, Y. Gripay, M. Scuturici und J.M. Pierson: *Context-Sensitive Security Framework for Pervasive Environments.* In: *Proceedings of the Fourth European Conference on Universal Multiservice Networks (ECUMN'07).* IEEE, 2007. (Zitiert auf den Seiten 144, 225 und 226.)

[PI01] George Pangalos und Christos Ilioudis: *A Framework for an Institutional High Level Security Policy for the Processing of Medical Data and their Transmission through the Internet.* Journal of Medical Internet Research, 3(2), 2001. (Zitiert auf den Seiten 143 und 207.)

[PIT08] PITMA: *PITMA Security Framework – Policy, Implementation, Training, Maintenance and Auditing.* `http://www.e-cq.net/pitma-overview.html`, 2008. (Zitiert auf den Seiten 142 und 195.)

[Poh04] Hartmut Pohl: *Taxonomie und Modellbildung in der Informationssicherheit.* Datenschutz und Datensicherheit, 28, 2004. (Zitiert auf den Seiten 15 und 16.)

[Poh04b] Hartmut Pohl: *Taxonomie und Modellbildung in der Begriffswelt safety und security, Entwurf Version 3.0.* `http://www-sec.uni-regensburg.de/media/begriffeWSMai2004/pohl_taxonomie_und_modellbildung_safety_security_v3.0.pdf`, 2004. (Zitiert auf den Seiten 15, 16, 18, 19, 20, 39 und 40.)

[PPF+03] S. Pallickara, M. Pierce, G. Fox, Y. Yan und Y. Huang: *A security framework for distributed brokering systems.* Technischer Bericht, Community Grid Computing Labs, Department of Computer Science, Indiana University, 2003. (Zitiert auf den Seiten 143 und 215.)

[PSSC+99] Phil Porras, Dan Schnackberg, Stuart Staniford-Chen, Davis, Maureen Stillman und Felix Wu: *The Common Intrusion Detection Framework Architecture.* `http://gost.isi.edu/cidf/drafts/architecture.txt`, 1999. (Zitiert auf Seite 465.)

[RC2119] S. Bradner: *RFC 2119: Key words for use in RFCs to Indicate Requirement Levels.* Request for Comment RFC 2119, IETF, Network Working Group, 1997. (Zitiert auf Seite 126.)

[RC2196] Barbara Fraser: *RFC 2196: Site Security Handbook.* Request for Comment RFC 2196, IETF, Network Working Group, 1997. (Zitiert auf Seite 311.)

[RC2828] R. Shirey: *RFC 2828: Internet Security Glossary.* Request for Comment RFC 2828, IETF, Network Working Group, 2000. (Zitiert auf Seite 15.)

[RC4120] C. Neuman, T. Yu, S. Hartman und K. Raeburn: *RFC 4120: The Kerberos Network Authentication Service (V5).* Request for Comment RFC 4120, IETF, Network Working Group, 2005. (Zitiert auf Seite 46.)

[RC4765] H. Debar, D. Curry und B. Feinstein: *RFC 4765: The Intrusion Detection Message Exchange Format (IDMEF).* Request for Comment RFC 4765, IETF, Network Working Group, 2007. (Zitiert auf Seite 375.)

[Rei08] Helmut Reiser: *Ein Framework für föderiertes Sicherheitsmanagement.* Habilitationsschrift, Ludwig-Maximilians-Universität München, 2008. (Zitiert auf den Seiten 144, 149, 150 und 151.)

[RH03] Saeed Rajput und Basit Husain: *Application Defense: Next Generation of Unified Enterprise Security.* In: *Proceedings of the International IEEE Workshop on Frontiers of Information*, Pakistan, 2003. IEEE Press. (Zitiert auf Seite 194.)

[Rom12] Anton Romanyuk: *Konzeption eines IT-Forensikleitfadens für das Leibniz-Rechenzentrum.* Diplomarbeit, Ludwig-Maximilians-Universität München, 2012. (Zitiert auf Seite 572.)

[RRSM06] Marco Rolando, Matteo Rossi, Niccolò Sanarico und Dino Mandrioli. In: *Proceedings of the 2006 international workshop on Software engineering for secure systems - SESS '06*, Seiten 65–71, New York, New York, USA, 2006. ACM Press. (Zitiert auf Seite 463.)

[Rub07] Thies Rubarth: *Sicherheitskonzepte in global verteilten Anwendungen.* Masterarbeit, Hochschule für angewandte Wissenschaften Hamburg, 2007. (Zitiert auf den Seiten 142 und 203.)

[Sai07] Martin Sailer: *Konzeption einer Service-MIB: Analyse und Spezifikation dienstorientierter Managementinformation.* Doktorarbeit, Ludwig-Maximilians-Universität München, 2007. (Zitiert auf den Seiten 367, 370 und 506.)

[Sal04] Mathias Sallé: *IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing.* Technischer Bericht HPL-2004-98, Hewlett-Packard, 2004. (Zitiert auf Seite 393.)

[SAM08] Frederick T. Sheldon, Robert K. Abercrombie und Ali Mili: *Evaluating security controls based on key performance indicators and stakeholder mission.* Proceedings of the 4th annual workshop on Cyber security and information intelligence research, 2008. (Zitiert auf Seite 286.)

[Sch99] Bruce Schneier: *Attack Trees: Modeling Security Threats.* Dr. Dobb's Journal, December 1999, 1999. (Zitiert auf den Seiten 339 und 340.)

[Sch08] Thomas Schaaf: *IT-gestütztes Service-Level-Management – Anforderungen und Spezifikation einer Managementarchitektur.* Doktorarbeit, Ludwig-Maximilians-Universität München, 2008. (Zitiert auf den Seiten 378 und 447.)

[SCN+09] S. Shaikh, Howard Chivers, Philip Nobles, J. Clark und Hao Chen: *A deployment value model for intrusion detection sensors.* In: *Proceedings of ISA 2009, LNCS 5576*, Seiten 250–259. Springer, 2009. (Zitiert auf Seite 463.)

[SDLC] US Department of Justice: *Systems Development Life Cycle Guidance Document.* `http://www.justice.gov/jmd/irm/lifecycle/table.htm`, Januar 2003. (Zitiert auf Seite 259.)

[SeTo08] Cigital Inc.: *Security Touchpoints.* `http://www.cigital.com/training/touchpoints/`, 2008. (Zitiert auf Seite 37.)

[SFK00] R. Sandhu, D. Ferraiolo und D. Kuhn: *The NIST Model for Role Based Access Control: Toward a Unified Standard.* In: *Proceedings of the 5th ACM Workshop Role-Based Access Control*, Seiten 47–63. ACM Press, 2000. (Zitiert auf Seite 46.)

[SH03] V. Shah und F. Hill: *An aspect-oriented security framework.* In: *Proceedings of DARPA Information Survivability Conference and Exposition.* IEEE, 2003. (Zitiert auf den Seiten 141 und 174.)

[SH04] V. Shah und F. Hill: *An Aspect-Oriented Security Framework: Lessons Learned.* In: *Proceedings of the AOSD Technology for Application-level Security (AOSDSEC) 2004 Workshop*, Lancaster, 2004. AOSD.NET. (Zitiert auf Seite 174.)

[SHKS01] J.Z. Sun, D. Howie, A. Koivisto und J. Sauvola: *A hierarchical framework model of mobile security.* In: *Personal, Indoor and Mobile Radio Communications – 12th IEEE International Symposium.* IEEE, 2001. (Zitiert auf den Seiten 143 und 209.)

[SKI08] Seonghan Shin, Kazukuni Kobara und Hideki Imai: *A Security Framework for Personal Networks.* In: *Proceedings of COMSWARE 2008.* IEEE, 2008. (Zitiert auf den Seiten 143 und 216.)

[SLJ+07] A. Saxena, M. Lacoste, T. Jarboui, U. Lucking und B. Steinke: *A software framework for autonomic security in pervasive environments.* In: *Proceedings of ICISS 2007, LNCS 4812.* Springer, 2007. (Zitiert auf den Seiten 142, 188 und 189.)

[SO05] Guttorm Sindre und L. Opdahl: *Eliciting security requirements with misuse cases.* Requirements Engineering, 10(1):34–44, January 2005. (Zitiert auf Seite 38.)

[SP8H12] NIST: *An Introduction to Computer Security: The NIST Handbook.* NIST Special Publication SP 800-12, National Institute for Standards and Technology, 1995. (Zitiert auf Seite 320.)

[SP8H14] Mark Wilson, Dorothea de Zafra, Sadie Pitcher, John Tressler und John Ippolito: *Generally Accepted Principles and Practices for Securing Information Technology Systems.* NIST Special Publication SP 800-14, National Institute for Standards and Technology, 1996. (Zitiert auf Seite 320.)

[SP8H30] Gary Stoneburner, Alice Goguen und Alexis Feringa: *Risk Management Guide for Information Technology Systems.* NIST Special Publication SP 800-30, National Institute for Standards and Technology, 2002. (Zitiert auf den Seiten 320 und 351.)

[SSA05] Riaz A. Shaikh, Kashif Sharif und Ejaz Ahmed: *Performance Analysis of Unified Enterprise Application Security Framework.* In: *Proceedings of the Engineering Sciences and Technology, SCONEST 2005.* IEEE, 2005. (Zitiert auf den Seiten 142 und 194.)

[SSA08] Shamsul Sahibudin, Mohammad Sharifi und Masarat Ayat: *Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations.* 2008 Second Asia International Conference on Modelling & Simulation (AMS), Seiten 749–753, Mai 2008. (Zitiert auf Seite 393.)

[SSMT07] R. Sulaiman, D. Sharma, W. Ma und D. Tran: *A multi-agent security framework for e-health services.* In: *Proceedings of KES 2007 WIRN 2007, Part II, LNAI 4693*, Seiten 547–554. Springer, 2007. (Zitiert auf den Seiten 143 und 210.)

[Sta06] Steve Stasiukonis: *Social Engineering, the USB Way.* `http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634`, 2006. (Zitiert auf Seite 40.)

[Stal07] William Stallings: *Standards for Information Security Management.* The Internet Protocol Journal, 10(4), 2007. (Zitiert auf Seite 33.)

[Ste06] J. Steven: *Adopting an enterprise software security framework.* IEEE Security & Privacy, 4(2):84–87, 2006. (Zitiert auf Seite 148.)

[STL+03] Yee Jiun Song, Wendy Tobagus, Der Yao Leong, Brad Johanson und Armando Fox: *iSecurity: A Security Framework for Interactive Workspaces.* Technischer Bericht CSTR 2004-03, Stanford University, 2003. (Zitiert auf den Seiten 142 und 191.)

[Sun05] Sun Microsystems: *Java™ security overview.* `http://java.sun.com/developer/technicalArticles/Security/whitepaper/JS_White_Paper.pdf`, 2005. (Zitiert auf den Seiten 141, 175 und 176.)

[SW09] Mikko Siponen und Robert Willison: *Information security management standards: Problems and solutions.* Information & Management, 46(5):267–270, Juni 2009. (Zitiert auf Seite 322.)

[SYSREV] Barbara Kitchenham: *Procedures for Performing Systematic Reviews.* Keele University Technical Report TR/SE-0401, ISSN:1353-7776, Keele University, Staffs, UK, Juli 2004. (Zitiert auf Seite 138.)

[SZS04] Riaz Shaikh, S. Zaidi und Kashif Sharif: *Modular approach for unified enterprise application security.* In: *Proceedings of US-Pakistan international workshop on High Speed Optical Networks and Enabling Technologies*, Pakistan, 2004. IEEE Press. (Zitiert auf Seite 194.)

[TC03] Bengisu Tulu und Samir Chatterjee: *A new security framework for HIPAA-compliant health information systems.* In: *Proceedings of Ninth Americas Conference on Information Systems*, Seiten 929–938. Association for Information Systems, 2003. (Zitiert auf den Seiten 141 und 183.)

[TM02] J. Thelin und P.J. Murray: *A Public Web Services Security Framework Based on Current and Future Usage Scenarios.* In: *Proceedings Of The International Conference On Internet Computing.* CSREA Press, 2002. (Zitiert auf den Seiten 141 und 171.)

[TN06] T. Thein und T.T. Naing: *Grid Security Framework for Managing the Certificate.* In: *IEEE/WIC/ACM International Conference on Web.* ACM, 2006. (Zitiert auf den Seiten 144 und 228.)

[Tsi02] Yiannis Tsiounis: *A Security Framework for Card-Based Systems.* In: *Proceedings of FC 2001, LNCS 2339*, Seiten 210–231. Springer, 2002. (Zitiert auf den Seiten 143 und 214.)

[Tud01] Tudor, Jan Killmeyer: *Information Security Architecture.* ISBN 978-0849315497, Auerbach Publications, 2001. (Zitiert auf Seite 314.)

[TX07] Lu Tao und Lei Xue: *Study on Security Framework in E-Commerce.* In: *Proceedings of Wireless Communications, Networking and Mobile Computing, 2007.* IEEE, 2007. (Zitiert auf den Seiten 142, 148 und 204.)

[Ueh08] M Uehara: *Security Framework in a Virtual Large-Scale Disk System.* In: *Proceedings of the conference on Distributed Computing Systems*, Seiten 30–35. IEEE, 2008. (Zitiert auf den Seiten 142 und 202.)

[Ush03] Abe Usher: *Towards a Taxonomy of Information Assurance.* `http://www.sharp-ideas.net/ia/information_assurance.htm`, 2003. (Zitiert auf Seite 326.)

[VCS03] M. Ventuneac, T. Coffey und I. Salomie: *A policy-based security framework for Web-enabled applications.* In: *Proceedings of the 1st international symposium on Information and communication technologies.* Trinity College Dublin, 2003. (Zitiert auf den Seiten 141 und 184.)

[vE] Felix von Eye: *D-KIDS: Ein dynamisches, kooperatives Intrusion Detection System (Arbeitstitel).* Promotionsvorhaben, Ludwig-Maximilians-Universität München. (Zitiert auf Seite 464.)

[vEMH12] Felix von Eye, Stefan Metzger und Wolfgang Hommel: *Innentäter in Hochschulrechenzentren – organisatorische und technische Maßnahmen zur Prävention und Detektion.* In: *Proceedings des 19. DFN-Workshop Sicherheit in vernetzten Systemen*, 2012. (Zitiert auf den Seiten 562 und 568.)

[Vig10] Giovanni Vigna: *Network intrusion detection: dead or alive?* In: *Proceedings of the 26th Annual Computer Security Applications Conference*, Seiten 117–126. ACM, 2010. (Zitiert auf Seite 462.)

[VKB01] Giovanni Vigna, R. Kemmerer und Per Blix: *Designing a Web of Highly-Configurable Intrusion Detection Sensors.* In: *Recent Advances in Intrusion Detection*, Seiten 69–84. Springer, 2001. (Zitiert auf Seite 463.)

[vS96] R. von Solms: *Information security management: The second generation.* Computers, 15(4):281–288, 1996. (Zitiert auf Seite 313.)

[vS00] Basie von Solms: *Information security – The third wave.* Computers & Security, 19:615–620, 2000. (Zitiert auf den Seiten 310 und 313.)

[vS04] Basie von Solms: *The 10 deadly sins of information security management.* Computers & Security, 23(1):371–376, 2004. (Zitiert auf Seite 313.)

[vS05] Basie von Solms: *Information Security Governance in ICT Based Educational Systems.* Kolloquium Didaktik der Informatik und E-Learning der Universität Siegen, `http://www.die.informatik.uni-siegen.de/forschung/kolloquium`, 2005. (Zitiert auf Seite 100.)

[Wan05] A.J.A. Wang: *Information security models and metrics.* In: *Proceedings of the 43rd annual Southeast regional conference-Volume 2.* ACM, 2005. (Zitiert auf den Seiten 435 und 436.)

[WCS+02] C. Wright, C. Cowan, S. Smalley, J. Morris und G. Kroah-Hartman: *Linux Security Modules: General Security Support for the Linux Kernel.* In: *Proceedings of the Foundations of Intrusion Tolerant Systems.* IEEE, 2002. (Zitiert auf den Seiten 142, 192 und 550.)

[WhMa09] Michael Whitman und Herbert Mattord: *Principles of information security, third edition.* ISBN 978-1-4239-0177-8, Verlag Thomson Course Technology, 2009. (Zitiert auf den Seiten 17, 32 und 337.)

[Wil06] Jan Willemson: *On the Gordon & Loeb model for information security investment.* In: *Workshop on the Economics of Information Security*, Seiten 1–12. Springer, 2006. (Zitiert auf Seite 451.)

[WM06] K. Wilson und P. Machanick: *SecureTorrent: A Security Framework for File Swarming.* In: *Proceedings of ACSAC 2006, LNCS 4186*, Seiten 538–544. Springer, 2006. (Zitiert auf den Seiten 142 und 197.)

[WM08] Christian Wolter und Michael Menzel: *Modelling security goals in business processes.* In: *Proceedings der Modellierung 2008*, Seiten 197–212, 2008. (Zitiert auf Seite 314.)

[WT03] G. Wilson und U.O. Tharakan: *Unified security framework.* In: *Proceedings of the 1st international symposium on middleware interoperability of enterprise applications.* ACM, 2003. (Zitiert auf den Seiten 145 und 241.)

[WW97] Chenxi Wang und William A. Wulf: *Towards a framework for security measurement*, 1997. (Zitiert auf Seite 438.)

[WWX07] Linzhang Wang, Eric Wong und Dianxiang Xu: *A Threat Model Driven Approach for Security Testing.* In: *Third International Workshop on Software Engineering for Secure Systems (SESS'07: ICSE Workshops 2007).* IEEE, Mai 2007. (Zitiert auf Seite 286.)

[XACML3] Erik Rissanen (Hrsg.): *OASIS eXtensible Access Control Markup Language Version 3.0.* OASIS XACML Technical Committee Specification, 2010. (Zitiert auf Seite 389.)

[XGLQ04] Bing Xie, Xiaolin Gui, Yinan Li und Depei Qian: *A New Grid Security Framework with Dynamic Access Control.* In: *Proceedings of GCC 2004, LNCS 3251.* Springer, 2004. (Zitiert auf den Seiten 143 und 211.)

[XKW+03] Y. Xu, L. Korba, L. Wang, Q. Hao, W. Shen und S. Lang: *A Security Framework for Collaborative Distributed System Control at the Device-Level.* In: *Proceedings of the 1st IEEE International Conference on Industrial Informatics.* IEEE, 2003. (Zitiert auf den Seiten 141 und 186.)

[YHF+03] Yan Yan, Yi Huang, Geoffrey Fox, Ali Kaplan, Shrideep Pallickara und Marlon Pierce: *Implementing a Prototype of the Security Framework for Distributed Brokering Systems.* In: *Proceedings of the International Conference on Security and Management*, Seiten 212–218. CSREA Press, 2003. (Zitiert auf Seite 215.)

[YKL+05] Z. Yao, D. Kim, I. Lee, K. Kim und J. Jang: *A security framework with trust management for sensor networks.* In: *Proceedings of Security and Privacy for Emerging Areas in Communication Networks*, Seiten 190–198. IEEE, 2005. (Zitiert auf den Seiten 143 und 219.)

[YYCZ05] S.S. Yau, Y. Yao, Z. Chen und L. Zhu: *An adaptable security framework for service-based systems.* In: *Proceedings of the 10th IEEE International Workshop on Object-Oriented Real-Time Dependable Systems.* IEEE Computer Society, 2005. (Zitiert auf den Seiten 141 und 173.)

[Zang76] Christof Zangemeister: *Nutzwertanalyse in der Systemtechnik – Eine Methodik zur multidimensionalen Bewertung und Auswahl von Projektalternativen.* Verlag Wittemann, ISBN 3-923264-00-3, 1976. (Zitiert auf Seite 106.)

[ZCS08] Xinwen Zhang, Michael J. Covington und Ravi Sandhu: *Toward a Usage-Based Security Framework for Collaborative Computing Systems.* ACM Transac-

tions on Information and System Security, 11(1):1–36, 2008. (Zitiert auf den Seiten 144 und 239.)

[Zia08] Tanveer Ahmad Zia: *A security framework for wireless sensor networks.* Ph.D.-Thesis, University of Sydney, 2008. (Zitiert auf den Seiten 143 und 218.)