Modellierung betrieblicher Informationssicherheit:

Entwicklung einer geschäftsprozessgetriebenen Modellierungsmethodik unter Nutzung eines Referenzmodells

Dissertation

zur Erlangung des akademischen Grades

Dr. rer. pol.

vorgelegt an der

Fakultät Wirtschaftsinformatik und Angewandte Informatik

der

Otto-Friedrich-Universität Bamberg

von

Thomas Reeg

Bamberg, Januar 2011

Gutachter:

Prof. Dr. Otto K. Ferstl

Prof. Dr. Elmar J. Sinz

Tag der Disputation:

16. November 2011

Meinen Eltern

Inhaltsverzeichnis

Abbildungsverzeichnis

Quelltextverzeichnis

Abkürzungsverzeichnis

AAI	Authentication and Authorization Infrastructure
ABAC	Attribute-based Access Control
ACL	Access Control List
AktG	Aktiengesetz
ANSI/INCITS	American National Standards Institute / International Committee for Information Technology Standards
API	Application Programming Interface
AWS	Anwendungssystem
BDSG	Bundesdatenschutzgesetz
bIS	Betriebliches Informationssystem
BPMN	Business Process Modeling Notation
BSI	Bundesamt für Sicherheit in der Informationsverarbeitung
CA	Certification Authorities
CC	Common Criteria
CLASP	Comprehensive Lightweight Application Security Process
COBIT	Control Objectives for Information and Related Technology
CRL	Certificate Revocation List
DAC	Discretionary Access Control
DBMS	Datenbankmanagementsystem
DFN-CERT	Deutsches Forschungsnetz - Computer Emergency Response Team
DGSA	Department of Defense Goal Security Architecture
DMZ	Demilitarized Zone
EBM	Einheitlicher Bewertungsmaßstab
EOD	Evidence of Delivery
EOO	Evidence of Origin
EOR	Evidence of Receipt
EOS	Evidence of Submission
GmbHG	GmbH-Gesetz
HGB	Handelsgesetzbuch
HTTP	Hypertext Transfer Protocol
HW	Hardware

IAS	Interaktionsschema
IdM	Identity Management
IDS	Intrusion Detection System
INSAG	International Nuclear Safety Group
ISMS	Information Security Management Systems
ITSEC	Information Technology Security Evaluation
ITIL	IT Infrastructure Library
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KOS	Konzeptuelles Objektschema
KOT	Konzeptueller Objekttyp
KV	Kassenärztliche Vereinigung
LOT	Leistungsspezifischer Objekttyp
MAC	Message Authentication Codes
MAC	Mandatory Access Control
MaRisk	Mindestanforderungen an das Risikomanagement
MD5	Message-Digest Algorithm 5
MDSD	model driven software development
MLS	Multilevel Security
MTF	Mean Time To Failure
MTTR	Mean Time To Repair
MVZ	Medizinisches Versorgungszentrum
NRD	Non-repudiation of Delivery
NRO	Non-repudiation of Origin
NRR	Non-repudiation of Receipt
NRS	Non-repudiation of Submission
OCL	Object Constraint Language
OECD	Organisation for Economic Cooperation and Development
OEP	oose Engineering Process
ooAM	objektorientiertes Architekturmodell
OTP	One-Time-Passwords
PAM	Pluggable Authentication Modules
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcment Point

PGP	Pretty Good Privacy
PIP	Policy Information Point
PKI	Public Key Infrastructure
RA	Registration Authority
RBAC	Role-based Access Control
ROI	Return on Investment
ROSI	Return on Security Investment
RPC	Remote Procedure Call
S/MIME	Secure / Multipurpose Internet Mail Extensions
SERM	Strukturiertes Entity-Relationship-Modell
SGF	Sicherheitsgrundfunktion
SHA-1	Secure Hash Algorithm 1
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen
SigV	Verordnung zur elektronischen Signatur
SK	Sicherheitskontext
SLA	Service Level Agreement
SO	Sicherheitsobjekt
SOD	Separation of Duty
SOM	Semantisches Objektmodell
SOS	Sicherheitsobjektschema
SOT	Sicherheitsobjekttyp
SOX	Sarbanes Oxley Act
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
T-SOT	Technischer Sicherheitsobjekttyp
TCSEC	Trusted Computer System Evaluation Criteria
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TMG	Telemediengesetz
TOS	Technisches Objektschema
TTP	Trusted third party
UML	Unified Modeling Language
VES	Vorgangs-Ereignis-Schema
VOS	Vorgangsobjektschema

VOT	Vorgangsobjekttyp
WPO	Wirtschaftsprüferordnung
XACML	eXtensible Access Control Markup Language

1. Einleitung

Das Themengebiet der betrieblichen Informationssicherheit ist eine vergleichsweise junge Forschungsdisziplin im Bereich der Wirtschaftsinformatik. Ihre Anfänge sind in erster Linie im technischen Sektor der Informationsverarbeitung zu finden, mit einem Forschungsschwerpunkt, der sich primär auf die Identifikation von Sicherheitsrisiken von Anwendungssystemen und Hardware sowie der Entwicklung entsprechender Gegenmaßnahmen bezog. In diesem Zusammenhang wurden auch verschiedene Vorgehensmodelle und Kriterienwerke durch offizielle Gremien und Organisationen erstellt, einhergehend mit einer zunehmenden Einflussnahme der Legislative durch Gesetze und Verordnungen. Inhaltlich beschäftigen sich diese Publikationen vornehmlich mit technisch orientierten Fragestellungen im Bereich der Absicherung und der sicherheitsorientierten Evaluation betrieblicher Anwendungssysteme (Common Criteria, CC) sowie der entsprechenden IT-Infrastruktur (Bundesamt für Sicherheit in der Informationsverarbeitung, BSI-Grundschutzkataloge). Auf dem rechtlichen Sektor sind primär Aspekte des Datenschutzes (Bundesdatenschutzgesetz, BDSG) und der Risikoprävention in Unternehmen (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, KonTraG) Kernthemen der Regularien.

Im betrieblichen Umfeld greift dieser Ansatz jedoch zu kurz. Betriebliche Informationssicherheit darf nicht nur auf die technische Ebene beschränkt werden, sondern muss über alle Lenkungs- und Leistungsebenen eines Unternehmens hinweg betrachtet werden. Aktuelle Forschungsaktivitäten greifen diese Anforderung zunehmend auf. Es zeigen sich Tendenzen, dass Themen des Managements der Informationssicherheit in dem Betrachtungsfeld Berücksichtigung finden. Das BSI zum Beispiel trägt dieser Entwicklung Rechnung und entwickelt in dem BSI-Standard 100-1 explizit Grundlagen für den Einsatz von Managementsystemen der Informationssicherheit (engl. *information security management systems*, ISMS).

Vor diesem Hintergrund will die vorliegende Arbeit mit einem methodisch fundierten Vorgehen sowohl die strukturelle als auch die prozessorientierte Integration von Aspekten der Informationssicherheit in betrieblichen Systemen unterstützen.

1.1. Problemstellung und Motivation

Die dargestellte Ausgangssituation ist in der aktuellen Form, auch bedingt durch die historisch gewachsene Entwicklung des Themenbereichs, mit unterschiedlichen Problemstellungen behaftet.

Uneinheitliches Begriffssystem

Auf Grund des naturgemäß unterschiedlichen, oder nur teilweise identischen, Begriffsverständnisses von betrieblicher Informationssicherheit, welches den jeweiligen Publikationen zu Grunde liegt, entstehen inkompatible Ansätze, die ohne großen (Lern-) Aufwand nicht effizient in Kombination eingesetzt werden können. Dies muss zum aktuellen Zeitpunkt jedoch notwendigerweise erfolgen, da keine holistischen Ansätze der Betrachtung von betrieblicher Informationssicherheit zur Verfügung stehen.

Semantische Lücke zwischen betrieblicher Lenkungs- und Leistungsebene

Sowohl die technisch orientierte Betrachtung der Informationssicherheit auf Leistungsebene als auch das Management der Informationssicherheit auf Lenkungsebene erfolgen vornehmlich isoliert. Abhängigkeits- und Ableitungsbeziehungen werden in der Regel nicht explizit berücksichtigt. Hieraus resultieren im betrieblichen Umfeld zum Beispiel Disziplinen wie das Security Engineering im Bereich der Softwareentwicklung (Leistungsebene) oder Ansätze der Corporate Governance (Lenkungsebene), deren Interdependenzen nicht durch geeignete Konzepte abgebildet werden. Es entsteht eine semantische Lücke.

Unzureichende Unterstützung bei der Abbildung von Sicherheitsaspekten

Sicherheitsaspekte werden im Bereich der Softwareentwicklung oftmals nur nachgelagert in der späten Realisierungsphase des Softwareentwicklungsprozesses berücksichtigt. Hierdurch wird jedoch die Verantwortung der inhaltlichen Ausgestaltung von software-technischen Sicherheitsmechanismen auf die Rolle des Anwendungsentwicklers abgegeben, der nicht notwendigerweise ebenfalls als Sicherheitsexperte über entsprechendes Domänenwissen verfügt. Die Ursache hierfür liegt mit in der mangelnden Verfügbarkeit von durchgängigen Modellierungsansätzen, die eine möglichst frühe Integration von Sicherheitsaspekten in den Entwicklungsprozess von Anwendungssystemen unterstützen.

Die semantische Lücke zwischen Lenkungs- und Leistungsebene ist nur zu überbrücken, wenn ein einheitliches und strukturiertes Begriffsverständnis der betrieblichen Informationssicherheit gegeben ist. Basierend auf dieser Struktur können dann Konzepte und Vorgehen definiert werden, um den Transfer der Zielvorgaben des Managements auf konkrete Aufgaben bzw. Aufgabenträger des Leistungssystems zu realisieren. Einen zentralen Aspekt stellt in diesem Zusammenhang die Verfügbarkeit einer Modellierungsmethodik für betriebliche Informationssicherheit dar, die rollenbezogen eine möglichst frühe und auch durchgängige Berücksichtigung von Sicherheitsaspekten im betrieblichen Kontext ermöglicht.

1.2. Zielsetzung und Lösungsansatz

Der Forschungsbeitrag der Dissertation besteht in einem ersten Schritt darin, durch eine strukturierte Modellbildung ein generisches Begriffsverständnis der betrieblichen Informationssicherheit zu entwickeln. In einem zweiten Schritt können darauf aufbauend individuelle Maßnahmen zur Überbrückung der semantischen Lücke zwischen Lenkungs- und Leistungssystem identifiziert und realisiert werden können. Als ein diesbezügliches Lösungsverfahren wird ein Modellierungsansatz für betriebliche Informationssicherheit entwickelt, der im Kontext der geschäftsprozessgetriebenen Anwendungssystementwicklung eine durchgängige Berücksichtigung von Sicherheitsaspekten von der Geschäftsprozessebene bis hin zur technischen Spezifikation eines Systems ermöglicht.

Terminologie betrieblicher Informationssicherheit

Als Ausgangspunkt der Betrachtungen muss eine valide Terminologie der Informationssicherheit definiert werden. Hierzu wird der realweltliche Sicherheitsbegriff ontologiebasiert analysiert und das Begriffssystem der Informationssicherheit durch einen Wechsel des Betrachtungsobjektes auf betriebliche Informationssysteme abgeleitet und abgegrenzt.

Referenzmodell betrieblicher Informationssicherheit

Basierend auf diesem abstrakten Begriffsverständnis wird ein generisches **Referenzmodell betrieblicher Informationssicherheit** entwickelt. Die Modellbildung als induktiver Schritt folgt dabei einem Modellierungsansatz, dem als globale Metapher die Interpretation der Informationssicherheit nach dem Konzept der betrieblichen Aufgabe zu Grunde liegt. Auf der Basis eines entsprechenden Meta-Modells der betrieblichen Informationssicherheit werden

die sicherheitsrelevanten Modellelemente sowie deren Beziehungen anhand der Unternehmensarchitektur der SOM-Methodik dargestellt. Das resultierende Referenzmodell wird abschließend durch Anwendung auf ein bestehendes Vorgehensmodell des BSI exemplarisch validiert.

Im weiteren Verlauf dient das Referenzmodell als Grundlage für die deduktive Ableitung relevanter Ansatzpunkte, die zur Überbrückung der semantischen Lücke zwischen Lenkungs- und Leistungssystem Verwendung finden können. Als wichtigster Bereich ist hierbei die Berücksichtigung von **Sicherheitsaspekten auf Geschäftsprozessebene** zu benennen. Dieses Gebiet ist zwar zum aktuellen Zeitpunkt noch nicht im Fokus des allgemeinen Forschungsbereichs anzusiedeln, gleichwohl wird durch diese Zwischenschicht eine durchgängige Betrachtung von Sicherheitsaspekten in betrieblichen Systemen erst ermöglicht. Im Kontext der geschäftsprozessgetriebenen Anwendungsentwicklung kann eine Integration betrieblicher Informationssicherheit in die Modellbildung auf Geschäftsprozessebene somit als Lösungsverfahren zur Vermeidung der diskutierten semantischen Lücke identifiziert werden.

Betriebliche Sicherheitsmodellierung

Im Anschluss wird dieses Lösungsverfahren konkretisiert, indem eine Modellierungsmethodik auf Basis der SOM-Ansatzes entwickelt wird, die in Form eines globalen Vorgehensmodells und ebenenspezifischer Modellierungsansätze eine ganzheitliche Betrachtung von Sicherheitsaspekten ermöglicht. Ausgangspunkt der Betrachtung bildet die Ebene der Geschäftsprozesse, für deren Modelle eine Erweiterung des Modellierungsansatzes durch die Einbindung von Schutzzielen vorgenommen wird. Über das Konzept der Sicherheitsgrundfunktionen können diese Schutzziele sodann in Sicherheitsobjekttypen im Rahmen der fachlichen Modellierung betrieblicher Anwendungssysteme transformiert werden. Das Vorgehen wird abgeschlossen durch die Möglichkeit der Ableitung konkreter, maßnahmen- und implementierungsspezifischer Parameter, die für den Betrieb eines Anwendungssystems benötigt werden.

In der Gesamtheit ergibt sich ein **geschäftsprozessgetriebener Modellierungsansatz für betriebliche Informationssicherheit**, dessen Ausgangspunkt die sicherheitserweiterte Modellierung in Form von Schutzzielen auf Geschäftsprozessebene darstellt. Top-Down betrachtet dient diese Modellbildung zum einen als Basis der Spezifikation von Sicherheitsaspekten im Rahmen der Softwareentwicklung, in Bezug auf die Ebene des Unternehmensplans ermög-

licht sie zum anderen die Steuerung und Kontrolle der Einhaltung regulatorischer Vorschriften (engl. *compliance*) im Rahmen der Corporate Governance.

1.3. Gang der Arbeit

Die vorliegende Arbeit gliedert sich in drei Teile, die im Gesamten aus zehn weiteren Kapiteln bestehen.

Teil I der Arbeit adressiert grundlegende Aspekte der Begriffsbildung und führt methodisch in die Terminologie der betrieblichen Informationssicherheit ein. Kapitel 2 beschreibt die allgemeinen Grundlagen der sicherheitsrelevanten Terminologie anhand eines semantischen Netzes, grenzt bestehende Teildisziplinen gegeneinander ab und transformiert die gewonnenen Erkenntnisse auf das Sicherheitsverständnis in der Informationsverarbeitung. Kapitel 3 baut auf diesem Begriffssystem auf und konkretisiert es vor dem Hintergrund betrieblicher Systeme. Darauf aufbauend wird die Interpretation der Informationssicherheit als betriebliche Aufgabe als grundlegende Metapher der weiteren Arbeit erläutert.

Teil II widmet sich der Strukturmodellbildung der Informationssicherheit in betrieblichen Systemen. Kapitel 4 beschreibt die allgemeinen Grundlagen der Modellbildung und spezifiziert mit einem Meta-Modell der Informationssicherheit die Basis für die Erarbeitung eines konkreten Modellierungsansatzes. Dieser wird im Detail in Kapitel 5 anhand der Konzepte Bezugsobjekt, Sicherheitsartefakt sowie Sicherheitsziel definiert. Kapitel 6 beschließt den zweiten Teil der Arbeit mit der Spezifikation eines strukturellen Referenzmodells betrieblicher Informationssicherheit.

In **Teil III** der Arbeit wird auf der Grundlage des Referenzmodells die geschäftsprozessgetriebene Modellierungsmethodik für betriebliche Informationssicherheit, SOMsec, vorgestellt. Kapitel 7 gibt hierzu eine Einführung und stellt die grundlegende Zielsetzungen sowie das Vorgehensmodell vor. In Kapitel 8 wird als erste Stufe von SOMsec der Modellierungsansatz von Schutzzielen in Geschäftsprozessen erläutert. Darauf aufbauend wird als zweite Stufe die Integration von Sicherheitsanforderungen in die fachliche Anwendungssystemspezifikation in Kapitel 9 dargestellt. In Kapitel 10 wird schließlich der letzte Schritt der Methodik in Form der technischen Sicherheitsspezifikation erläutert.

Kapitel 11 beschließt die vorliegende Arbeit mit einem Überblick zum aktuellen Stand der Forschung sowie einer zusammenfassenden Bewertung der vorgestellten Inhalte. Den Abschluss bildet ein kurzer Ausblick auf zukünftig mögliche Forschungsaktivitäten im Rahmen des vorgestellten Themengebiets.

1.4. Konventionen

Zentrale Begriffe für die vorliegende Arbeit sowie Definitionen werden im Text **fett** formatiert. Hervorhebungen und Betonungen von Textstellen sind unterstrichen dargestellt. Eine *kursive* Formatierung wird für Fremdwörter, Fachbegriffe oder Abkürzungen verwendet. Verweise auf Modellelemente oder Quellcode werden in der Schriftart `Consolas` formatiert.

Wird im Text eine weibliche bzw. männliche Personenbezeichnung verwendet, so schließt diese die jeweils andere mit ein.

Teil I

Das Begriffssystem der Informationssicherheit

Das Untersuchungsobjekt des ersten Teils der vorliegenden Arbeit stellt das Begriffsverständnis des Themengebiets der Sicherheit dar. Das Ziel besteht in der systematischen Erarbeitung und Abgrenzung des Begriffs der betrieblichen Informationssicherheit als Grundlage für die weiteren Teile dieser Arbeit.

Kapitel 2 beschreibt in diesem Zusammenhang die grundlegende realweltliche Sicherheitsterminologie anhand bestimmter Definitionsmerkmale und grenzt verschiedene Sichten und Teildisziplinen der Sicherheit ab. Diese Ergebnisse werden im Anschluss auf den Bereich der Informationsverarbeitung übertragen. Kapitel 3 widmet sich darauf aufbauend der Definition und dem Begriffsverständnis der betrieblichen Informationssicherheit. Deren Interpretation als betriebliche Aufgabe sowie die ableitbaren Dimensionen der betrieblichen Informationssicherheit dienen im weiteren Verlauf als begriffliche Grundlage und zentrale Metapher dieser Arbeit.

2. Sicherheitsterminologie

Der Sicherheitsbegriff sowie dessen implizites Verständnis findet in unterschiedlichen Bereichen des täglichen Lebens Verwendung. Seine Definition und Interpretation im Hinblick auf die betriebliche Informationsverarbeitung ist demnach ebenfalls von unterschiedlichen, zum Teil auch subjektiv geprägten, Einschätzungen entsprechender Entscheidungsträger geprägt.

Die folgenden Abschnitte beschäftigen sich systematisch mit diesem Sachverhalt, beginnend mit einer einführenden Analyse des allgemeinen Sicherheitsbegriffs in Kapitel 2.1. Kapitel 2.2 behandelt darauf aufbauend relevante Sichtweisen bevor in Kapitel 2.3 Teildisziplinen des Themenkomplexes vorgestellt werden. Das Ziel dieser Abschnitte ist die Erarbeitung der charakterisierenden Faktoren, die auf das zentrale Begriffsverständnis der Sicherheit Einfluss nehmen. Auf der Grundlage dieser Faktoren und des resultierenden Sicherheitsverständnisses wird abschließend in Kapitel 2.4 der in dieser Arbeit genutzte Sicherheitsbegriff in der Informationsverarbeitung definiert.

2.1. Der allgemeine Sicherheitsbegriff

Der Begriff Sicherheit ist im allgemeinen Sprachgebrauch in hohem Maße kontextabhängig zu interpretieren. Insbesondere in der Wissenschaft ergeben sich je nach Disziplin stark unterschiedliche Schwerpunkte bzw. Perspektiven, die das Begriffsverständnis bestimmen [Heit07, 11]. GLAEßNER spricht in diesem Zusammenhang auch von einer „normativen Überlastung“ des Sicherheitsbegriffs [Glae02, 3].

Um die angestrebte methodische Systematisierung und Interpretation des Begriffsverständnisses für den Bereich der Informationsverarbeitung zu erreichen, ist somit eine möglichst allgemeingültige Definition des Sicherheitsbegriffs als Ausgangsbasis zu wählen. Anhand dieser Definition werden charakterisierende Merkmale identifiziert, deren Ausprägungen eine Adaption des allgemeinen Sicherheitsbegriffs auf unterschiedliche Domänen ermöglichen.

2.1.1. Definition und Merkmale

Als Grundlage der folgenden Ausführungen findet eine Definition Verwendung, die die Kernaspekte des Begriffs Sicherheit im Sinne der vorliegenden Arbeit verdeutlicht.

> Sicherheit beschreibt eine Situation, in der sich ein Bezugsobjekt befindet, die als frei von Gefahren bezeichnet werden kann.

Diese Interpretation ist angelehnt an eine allgemeine enzyklopädische Darstellung[1], die Sicherheit als Zustand des Unbedrohtseins charakterisiert, der sich unter anderem im Fehlen von Gefahrenquellen darstellt. Als domänenunabhängige Definition bildet dieser Ansatz in verschiedenen wissenschaftlichen Disziplinen die definitorische Grundlage, so zum Beispiel auch in [Glae02] im Rahmen der sozialwissenschaftlichen Betrachtung oder in [Brom10] im Kontext der Wahrscheinlichkeitstheorie. Als charakterisierende Definitionsmerkmale können die im Text unterstrichenen Begriffe Situation, Bezugsobjekt und Gefahr identifiziert werden. Sie werden als **Definitionsmerkmale des allgemeinen Sicherheitsbegriffs** in den folgenden Abschnitten im Detail dargestellt.

Merkmal Bezugsobjekt

Objekte, für die Sicherheitscharakteristika spezifiziert sind, werden allgemein als **Bezugsobjekte** bezeichnet. Sie besitzen in der Regel **schützenswerte Eigenschaften** (engl. *assets*), die einen subjektiven Wert für das Bezugsobjekt selbst oder dessen Eigentümer, bzw. allgemeiner gefasst, für dessen Stakeholder haben. Ein Bezugsobjekt ist dabei nicht auf einen bestimmten Typ festgelegt. Es kann sich um realweltliche Gegenstände, Menschen oder auch Organisationen handeln, für welche die Sicherheit betrachtet wird. Im Kontext der Wirtschaftsinformatik kann zum Beispiel ein betriebliches System ein Bezugsobjekt darstellen, das im Rahmen einer Sicherheitsbetrachtung analysiert wird.

Merkmal Situation

Die Situation wird durch den **Zustand** eines Bezugsobjektes in Kombination mit dem **Kontext**, in dem es sich befindet, charakterisiert. Der Zustand bezieht sich dabei auf die sicherheitsrelevanten Eigenschaften des Bezugsobjektes selbst, während der Kontext auf die sicherheitsrelevanten Eigenschaften der Umgebung des Bezugsobjektes abzielt. Die Ausprägung von Zustand und Kontext zu einem bestimmten Zeitpunkt bestimmen somit die Gesamtheit aller sicherheitsrelevanten Attribute eines Bezugsobjektes.

---

[1] Vgl. zum Beispiel [Schu02, 8].

Merkmal Gefahr

Gefahren beschreiben die grundsätzliche Möglichkeit eines Fehler- oder Schadensereignisses [HoPr03, 28]. Hat dieses Ereignis Auswirkungen auf das Bezugsobjekt und sind diese Auswirkungen nachteilig in dem Sinn, dass sie die Werte des Bezugsobjektes mindern, so spricht man von einem **Schaden**. Im Rahmen des hier verwendeten Begriffssystems stellt ein Schaden somit einen unerwünschten Zustand eines Bezugsobjektes dar, der den Wert der Assets des Bezugsobjektes mindert. Schäden müssen dabei nicht zwangsläufig materielle Nachteile nach sich ziehen, sie können auch immaterieller oder ideeller Natur sein. Im betriebswirtschaftlichen Kontext sind jedoch auch die letztgenannten Schadenskategorien durch Quantifizierung zu operationalisieren, so dass in der vorliegenden Arbeit als Dimension von Schaden grundsätzlich die Einheit Währung Verwendung findet [GeKo08, 124].

Merkmal Risiko

Aus dem dargestellten Verständnis der Begriffe Gefahr und Schaden ist als vierter Aspekt der Begriff des **Risikos** ableitbar. Allgemein definiert setzt sich dieser zusammen als die berechnete Wahrscheinlichkeit für das Eintreten eines negativen Ereignisses. Im betriebswirtschaftlichen Rahmen wird diese Betrachtung erweitert um den Faktor des finanziellen Nachteils (Schaden), der aus dem Eintreten des negativen Ereignisses resultiert [BSI09, 53]. Diese allgemeine Begriffsdefinition nimmt Bezug auf Ingenieurdisziplinen im technischen Bereich. Hier wird das Risiko etwa nach der DIN/VDE-Norm 31000-2[2] definiert als Produkt der zu erwartenden Häufigkeit eines gefährdenden Ereignisses sowie dem beim Ereigniseintritt zu erwartenden Schadensausmaß [Stel94, 186]. Im Rahmen der Diskussion der Sicherheitsterminologie findet diese grundlegende Interpretation von Risiko in der vorliegenden Arbeit ebenfalls Verwendung.

Die vier dargestellten Merkmale zeigen auf, dass eine Interpretation des Sicherheitsbegriffs in Bezug auf eine Domäne und das damit verbundene Verständnis von Sicherheit beeinflussbar sind. In der vorliegenden Arbeit wird diese Möglichkeit genutzt, um das Begriffsverständnis in Bezug auf das Zielsystem der Wirtschaftsinformatik anzupassen. Die diesbezüglich relevanten Beziehungen der Definitionsmerkmale werden in dem folgenden Abschnitt anhand eines semantischen Netzes weiter detailliert.

---

[2] Normtitel: Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse, vgl. hierzu [DIN87].

2.1.2. Semantisches Netz des allgemeinen Sicherheitsbegriffs

Je nach Perspektive können die Merkmale des allgemeinen Sicherheitsbegriffs unterschiedlich ausgestaltet werden. Die Basis hierfür bildet die Beziehungsstruktur zwischen den Merkmalen, durch die die grundlegende Semantik des Begriffssystems definiert wird. Die folgende Abbildung stellt diese Zusammenhänge grafisch dar[3].

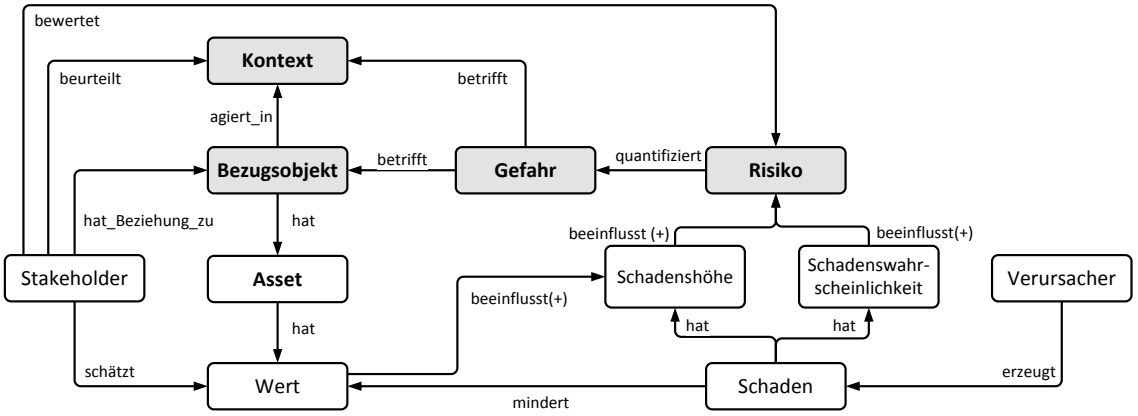

Abbildung 1: Semantisches Netz des allgemeinen Sicherheitsbegriffs

Das semantische Netz stellt als zentrale Elemente die vier Definitionsmerkmale des Sicherheitsbegriffs dar, in der Abbildung fett hervorgehoben. Das Merkmal Situation wird dabei durch das Element Kontext sowie das Element Asset, als Repräsentation des Zustandes des Bezugsobjektes, abgebildet. Erweitert wird das Modell um die im Rahmen der Merkmalsdiskussion bereits eingeführten abhängigen Attribute Schaden und Risiko. Die Verbindung zwischen diesen wird über die Elemente Schadenshöhe und Schadenswahrscheinlichkeit abgebildet. Zur Vervollständigung des Modells findet weiterhin das Konzept des Stakeholders als subjektiv agierende Instanz zur Beurteilung der Sicherheitssituation Berücksichtigung. In ähnlicher Weise fungiert der Verursacher als abstraktes Konzept zur Verdeutlichung der Schadensentstehung. Sowohl Stakeholder als auch Verursacher sind als zielgesteuerte Akteure zu verstehen, in Bezug auf den Wert der betrachteten Assets sind deren Intentionen als konfliktär einzustufen.

[3] Die Art der Beziehung wird unter Nutzung der Notationsform aus dem Bereich System Dynamics dargestellt. Ein Plus-Zeichnen bedeutet, dass sich bei Veränderung der Größe zu Beginn des Pfeils die Größe am Ende des Pfeils in die gleiche Richtung ändert. Ein Minus-Zeichen hingegen wird zur Darstellung von gegenläufigem Änderungsverhalten genutzt. Für einen Überblick zu System Dynamics sei etwa auf [Coyl08] verwiesen.

Die relevante Beziehung für die Bewertung durch einen Stakeholder besteht zwischen den subjektiven Werten der Assets und dem Risiko für das Bezugsobjekt. Der Wert eines Assets beeinflusst direkt die mögliche Schadenshöhe, diese wiederum steigert oder senkt das Risiko. Transitiv besteht somit ein Zusammenhang zwischen dem einem Objekt zugemessenem Wert und dem damit verbundenen Risiko. Für einen Entscheider definiert dieser Risikowert, als Quantifizierung einer möglichen Gefahr, eine Größe, anhand derer die Tragbarkeit der Situation evaluiert werden kann.

Auf der Grundlage des semantischen Netzes können die ausschlaggebenden Faktoren für die Bildung eines Begriffsverständnisses der Sicherheit erläutert werden[4].

2.1.3. Sicherheitsverständnis

Unter dem Begriff Sicherheitsverständnis wird in der vorliegenden Arbeit die grundlegende Auffassung verstanden, die für die Auseinandersetzung mit dem Themenkomplexes der Sicherheit in unterschiedlichen Domänen ausschlaggebend ist. Diese Auffassung ist relevant dafür, wie der Sicherheitsbegriff in Bezug auf eine konkrete Domäne zu interpretieren und zu verwenden ist.

Die Grundlage des Sicherheitsverständnisses bildet das vorgestellte semantische Netz. Darauf aufbauend sind zwei zentrale Einflussfaktoren als bestimmend für das Verständnis anzusehen. Zum einen ist dies die **Auswahl des Bezugsobjektes**, durch die implizit die zu beachtenden sicherheitsrelevanten Aspekte spezifiziert und die Diskurswelt der Sicherheitsbetrachtung abgegrenzt werden. Durch die zusätzliche **Bestimmung einer Sichtweise** wird das Sicherheitsverständnis weiter konkretisiert. Im Ergebnis wird durch diese Kombination das domänenspezifische Verständnis der Sicherheit präzisiert und eine Teilbereichsbildung im Rahmen der Sicherheitsbetrachtung ermöglicht. Die Wahl eines Bezugsobjektes und einer Sichtweise werden als **Einflussfaktoren des Sicherheitsverständnisses** bezeichnet.

[4] Das dargestellte semantische Netz fungiert an dieser Stelle als Visualisierung der grundlegenden Zusammenhänge im Rahmen der Sicherheitsterminologie. Eine der Domäne der Wirtschaftsinformatik entsprechende Erweiterung im Hinblick auf den Bereich der betrieblichen Informationssicherheit wird in Kapitel 3.1.3 vorgestellt.

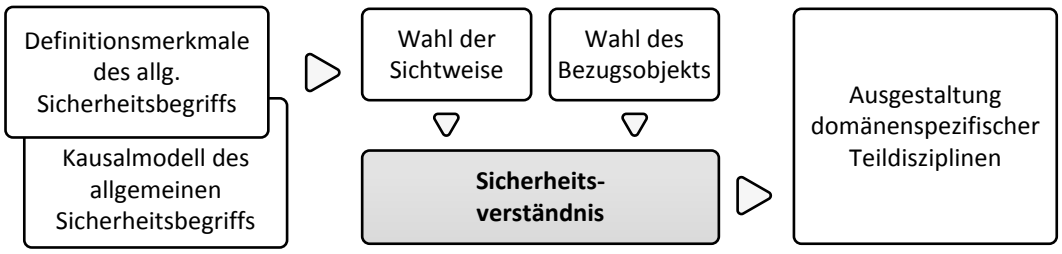

Abbildung 2: Beziehungsstruktur des Sicherheitsverständnisses

Ein gegebenes Sicherheitsverständnis bildet die Grundlage für die Bestimmung und vor allem Ausgestaltung von Teildisziplinen der Sicherheit im Rahmen der jeweiligen Domäne[5]. Dies bedeutet, dass auch Teildisziplinen durch die Wahl von Bezugsobjekt und Sichtweise beschreibbar und somit kategorisierbar sind. Die beiden Aktivitäten der Auswahl sind dabei als orthogonal zu betrachten, da sie untereinander keine Abhängigkeiten aufweisen.

Die Zielsetzung der Darstellung dieser Zusammenhänge besteht in der Schaffung einer Systematisierungshilfe, anhand derer die Teildisziplinen der Sicherheit in verschiedenen Domänen analysiert werden können. Zu diesem Zweck werden im folgenden Kapitel mögliche Sichtweisen auf den Sicherheitsbegriff vorgestellt, die dann in Verbindung mit verschiedenen Bezugsobjekten zur Darstellung von Teildisziplinen der Sicherheit herangezogen werden können. Auf der Grundlage dieser Konzepte ist es dann möglich, die entsprechenden Sicherheitsdisziplinen des Zielsystems der Wirtschaftsinformatik aus dem allgemeinen Sicherheitsbegriff abzuleiten.

2.2. Sichten auf den allgemeinen Sicherheitsbegriff

Eine Sicht oder Sichtweise auf den allgemeinen Sicherheitsbegriff konkretisiert dessen Verständnis in Bezug auf eine bestimmte Domäne. Der Begriff „Sicht“ wird in diesem Zusammenhang analog zu seiner Nutzung im Bereich der Informationssystemarchitekturen verwendet. Hier stehen Sichten für Projektionen auf das Meta-Modell einer Modellebene, die jeweils nur einen Teilausschnitt dieser Ebene unter einem bestimmten Blickwinkel erfassen und zur Komplexitätsreduktion bei der Modellbildung eingesetzt werden [Sinz99a, 1037]. Analog hierzu erfassen Sichten auf den allgemeinen Sicherheitsbegriff bestimmte Blickwinkel auf das Begriffsverständnis, indem die Elemente des semantischen Netzes bei der Betrachtung unter-

[5] Allgemein anerkannte Teildisziplinen stellen zum Beispiel die Bereiche Security und Safety dar, die in Kapitel 2.3 und 2.4.1 im Detail beschrieben werden.

schiedlich gewichtet oder ausgestaltet werden. Projektionen sind hierbei möglich, jedoch nicht zwingend notwendig, eine Sicht kann auch alle Merkmale erfassen und durch deren individuelle Ausprägungen spezifiziert werden. Anhand der vorgestellten Merkmale können die verschiedenen realweltlichen Sichten auf den Sicherheitsbegriff identifiziert und kategorisiert werden.

2.2.1. Objektzentrierte Sicht

Den Ausgangspunkt für die Sicherheitsbetrachtung stellt das Bezugsobjekt selbst sowie dessen Assets dar. Diese Sichtweise kann demzufolge in zwei Teilsichten differenziert werden.

Typorientierte Sicht

Der Sicherheitsbegriff wird umfassend für eine bestimmte Klasse von Bezugsobjekten verwendet, ohne auf konkrete, instanzbezogene sicherheitsrelevante Eigenschaften einzugehen. Als Beispiele dieser Sichtweise gelten abstrakte Sicherheitsbegriffe wie Fahrzeugsicherheit oder Datenbanksicherheit.

Attributorientierte Sicht

Im objektorientierten Sinn stellen Assets Attribute von Bezugsobjekten dar, denen besonderer Wert zugemessen wird. Im Rahmen der attributorientierten Sicht werden diese Attribute als zentrale sicherheitsrelevante Größen der Betrachtung angesehen. Als Eigenschaften können sowohl struktur- als auch verhaltensbezogene Assets Verwendung finden. Ein Beispiel für diese Sichtweise ist die allgemeine Bezeichnung Informationssicherheit, die sich auf das Asset Information eines Bezugsobjektes, zum Beispiel eines Anwendungssystems, bezieht. Weitere Beispiele sind Prozesssicherheit, Funktionssicherheit oder Betriebssicherheit.

2.2.2. Situationszentrierte Sicht

Den Fokus der Sicherheitsbetrachtung stellt nicht das Bezugsobjekt selbst dar, sondern der Kontext, in dem sich das Objekt befindet. Analog zu der vorgestellten Definition des Merkmals Situation kann dieser Kontext wiederum durch die Ausprägung bestimmter Eigenschaften zu einem bestimmten Zeitpunkt repräsentiert werden. Sie stellen in diesem Zusammenhang den Fokus der situationszentrierten Sichtweise dar. Als Beispiel kann die Betrachtung der allgemeinen rechtlichen Sicherheit dienen, die bei einem Markteintritt für ein ausländisches Unternehmen relevant ist. Der Markt wird hierbei als Bezugsobjekt der Betrachtung

ausgewählt, die rechtliche Sicherheit des Landes ist als kontextbezogenen Eigenschaft zu interpretieren.

Es wird deutlich, dass die Ausgestaltung der situationszentrierten Sicht in hohem Maße abhängig ist von der Abgrenzung und Wahl des Bezugsobjektes. Würde im obigen Beispiel das Land selbst als Bezugsobjekt definiert werden, so entspräche die Betrachtung der rechtlichen Sicherheit einer attributorientierte Sichtweise.

2.2.3. Gefahrenzentrierte Sicht

Ausgangspunkt dieser Sichtweise stellen Gefahren dar, welche den Zustand der Sicherheit eines Bezugsobjektes beeinträchtigen. Analog zum vorgestellten semantischen Netz wird durch diese Betrachtung auch das vierte Merkmal des Risikos mit abgedeckt, da beide Aspekte die Eintrittswahrscheinlichkeit eines negativen Ereignisses mit einbeziehen. Beispiele der gefahrenzentrierten Sichtweise sind etwa Einbruchssicherheit oder Ausfallsicherheit.

Durch die Wahl einer bestimmten Sichtweise auf den allgemeinen Sicherheitsbegriff wird die grundlegende Einstellung eines Stakeholders dem Themenkomplex gegenüber verdeutlicht. In Verbindung mit der Auswahl eines Bezugsobjektes, als Charakteristikum für die zu betrachtende Domäne, lassen sich somit die entsprechenden Teildisziplinen der Sicherheit beschreiben.

2.3. Allgemeine Sicherheitsdisziplinen

Das Themengebiet der Sicherheit wird in der Praxis oftmals in weitere Teilbereiche untergliedert. Eine im englischsprachigen Raum weit verbreitete Differenzierung ist die Unterteilung in die Disziplinen **Security** und **Safety**. Während der Begriff Safety primär aus dem Ingenieurbereich kommt, wird der Ursprung der Bezeichnung Security hingegen der Informationsverarbeitung zugeschrieben [Schi99, 30]. Anhand der oben dargestellten Kriterien aus Sichten, Bezugsobjekten und Assets, können diese Teilbereiche im Folgenden systematisch erläutert werden.

Die inhaltliche Ausrichtung der Teildisziplinen wird primär über die zu Grunde liegende Sichtweise charakterisiert. Um die entsprechenden Unterschiede aufzuzeigen, werden beide Disziplinen anhand des gleichen, abstrakten Bezugsobjektes vorgestellt. Als gemeinsames

Bezugsobjekt dient hierbei ein generisches System, das gemäß der allgemeinen Systemtheorie[6], als Menge von Elementen sowie deren Beziehungen untereinander verstanden wird. Aus typorientierter Sichtweise[7] betrachtet, bildet somit das Verständnis einer allgemeinen Systemsicherheit die Grundlage für die folgenden Ausführungen.

2.3.1. Safety

Der Begriff Safety wird in diversen Bereichen der Forschung und der Praxis stark unterschiedlich interpretiert. Hinsichtlich des Bezugsobjektes System kann er vergleichsweise allgemein definiert werden als Schutz eines Systems vor unerwünschtem Verhalten des Systems selbst [Shir07, 257]. Aus Innensicht betrachtet, bezeichnet Safety somit die **Funktionssicherheit** eines Systems. Es wird gefordert, dass die realisierte Ist-Funktionalität mit der definierten Soll-Funktionalität übereinstimmt. Aus systemtheoretischer Sicht bedeutet dies, dass ein funktionssicheres System keine funktional unzulässigen Zustände annimmt, es also unter allen (definierten) Betriebsbedingungen funktioniert [Ecke06, 5].

Zentraler Aspekt dieser Disziplin ist dabei, dass es sich grundlegend um die Sicherheit vor **nichtintentionaler Beeinträchtigung** handelt [Dier04, 344]. Der Begriff impliziert somit Sicherheit vor zufällig oder fahrlässig entstehenden Gefahren, die aus Sicht des Systems durch interne Fehler entstehen, zum Beispiel Bauteilversagen. Safety behandelt demzufolge Fragestellungen, die die Zuverlässigkeit eines Systems betreffen, somit dessen Ablauf- und Ausfallsicherheit [Oppl97, 3].

Verfahren und Maßnahmen der Disziplin Safety werden oftmals als Techniken der **Fehlertoleranz** bezeichnet. Relevante Kenngrößen hierbei sind Zuverlässigkeit (engl. *mean time to failure*, MTTF), Wiederherstellbarkeit (engl. *mean time to repair*, MTTR) und Verfügbarkeit, als Wahrscheinlichkeit, dass ein System zu einem bestimmten Zeitpunkt funktionsfähig ist [BoHe99, 418].

Hinsichtlich der Sichtweise bezieht sich Safety auf die Funktionalität als Eigenschaft eines Systems. Dieser Disziplin liegt somit eine **attributorientierte Sichtweise** zu Grunde. Sie kann durch die folgenden Ausprägungen der vorgestellten Kriterien charakterisiert werden.

---

[6] Die Systemtheorie als wissenschaftliche Disziplin stellt für viele Forschungsbereiche einen Bezugsrahmen dar. Der zentrale Systembegriff wird zum Beispiel in [Fers79] näher beleuchtet.

[7] Vgl. hierzu Kapitel 2.2.1.

- Bezugsobjekt - allgemeines System
- Asset - Funktion
- Sicht - objektzentriert, attributorientiert

Zusammenfassend kann Safety durch den Ausdruck „Spiel gegen den Zufall“ beschrieben werden.

2.3.2. Security

Der Bereich Security adressiert weniger die Innensicht eines Systems, wie im Bereich der Safety, sondern vielmehr dessen Außensicht. Er bezieht sich dabei auf den Schutz vor unerwünschtem Verhalten der Umgebung in Bezug auf das System selbst [Pohl04, 678f].

Security bezieht sich dabei auf die Sicherheit vor **intentionaler Beeinträchtigung** [Dier04, 344], somit auf den Schutz vor absichtlich herbeigeführten Gefahren, die ein System aus Außensicht bedrohen, wie etwa Kriminalität oder Terrorismus.

Die Disziplin Security stellt weniger auf konkrete Attribute eines Systems ab, wie etwa die Funktionsweise, sondern vielmehr auf eine generelle Absicherung vor externen Gefahren. Letztere bilden somit die Grundlage für die **gefahrenzentrierte Sichtweise**, die diesem Teilbereich zu Grunde liegt. Es ergeben sich die folgenden Ausprägungen der Kriterien.

- Bezugsobjekt - allgemeines System
- Asset - nicht spezifiziert
- Sicht - gefahrenzentriert

Charakterisiert werden kann der Bereich Security durch den Ausdruck „Spiel gegen Absicht“.

Die vorgestellten Teildisziplinen der allgemeinen Systemsicherheit finden ihre Entsprechung ebenfalls in spezialisierten Themengebieten, wie zum Beispiel dem Maschinenbau. Die Unterschiede ergeben sich hierbei hauptsächlich durch die Abgrenzung des Bezugsobjektes und die entsprechende Anpassung der Sichtweise. Der Sicherheitsbegriff hinsichtlich des für die vorliegende Arbeit relevanten Forschungsgebietes der Informationsverarbeitung wird in den folgenden Abschnitten näher betrachtet.

2.4. Sicherheitsdisziplinen in der Informationsverarbeitung

Der Sicherheitsbegriff in der Informationsverarbeitung ist, analog zum allgemeinen Begriffssystem, durch verschiedene Sichtweisen und Bezugsobjekte geprägt. Bis heute hat sich demzufolge in diesem Feld kein grundlegendes und allgemein anerkanntes Begriffssystem herausgebildet [Pohl04, 678].

Um eine einheitliche und konsistente Terminologie für die vorliegende Arbeit zu spezifizieren, wird der allgemeine Sicherheitsbegriff auf den Bereich der Informationsverarbeitung transformiert. Dieser deduktive Schritt bildet den Ausgangspunkt für die Erörterungen im Hinblick auf den Bereich der betrieblichen Informationssicherheit in Kapitel 3.

2.4.1. Safety und Security

Die Transformation des Begriffssystems erfolgt in einem ersten Schritt durch die Anpassung des Bezugsobjektes an die Domäne der Informationsverarbeitung. Hierzu wird das bisher verwendete Konzept des allgemeinen Systems zu einem **informationsverarbeitenden System** spezialisiert. Ein solches wird als Menge von Elementen verstanden, die intern und über ihre Beziehungen zueinander den Objekttyp Information verarbeiten bzw. austauschen. Im Rahmen der Darstellung der Sicherheitsdisziplinen sind informationsverarbeitende Systeme aufgabenträgerorientiert zu interpretieren und können beispielhaft als Anwendungssysteme oder Hardwaresysteme verstanden werden.

Auf Basis dieses Bezugsobjektes sind nun die bereits allgemein spezifizierten Teildisziplinen Safety und Security für den Bereich der Informationsverarbeitung erneut zu betrachten.

Safety in der Informationsverarbeitung

Die Interpretation von Safety in Bezug auf informationsverarbeitende Systeme erfolgt analog zu der allgemeinen Interpretation. Auch hier wird von Funktionssicherheit im Sinne von erlaubten und nicht erlaubten Zuständen gesprochen, die ein System einnehmen sollte bzw. könnte. Weiterhin findet sich in der Literatur auch der Begriff der Ordnungsmäßigkeit eines informationsverarbeitenden Systems, die durch Safety sicherzustellen ist [Kers95, 72f]. Ordnungsmäßigkeit wird hierbei als verfahrensbezogene Eigenschaft des informationsverarbeitenden Systems gesehen, die durch Konformitätsprüfungen zu validieren ist.

Fragen der Safety werden in diesem Bereich häufig bei Applikationen bzw. Hardwarekomponenten diskutiert, die zum Beispiel in direktem Zusammenhang mit der Sicherung von Menschenleben stehen, etwa Flugkontrollsysteme. SOMMERVILLE beschreibt dies durch die Forderung, dass ein ordnungsgemäßes bzw. funktionssicheres System bei Fehlfunktion niemals Menschen oder Systemumgebungen schädigen darf [Somm07, 55].

Security in der Informationsverarbeitung

Security wird in der Informationsverarbeitung als Bereich angesehen, der den Schutz eines Hard- oder Softwaresystems vor externen Angriffen behandelt [Somm07, 55]. In welcher Weise diese Angriffe wirken bzw. auf was sie abzielen, wird hierbei jedoch nicht konkretisiert. Insbesondere spezielle Assets von informationsverarbeitenden Systemen werden in dieser Auffassung nicht explizit beachtet. Aus praktischer Perspektive umfasst Security somit sowohl den Schutz vor unautorisierten Zugriffen auf eine Datenbank wie auch vor einem unberechtigten Betätigen des Ausschalters an einem Server.

Sowohl bei Safety als auch bei Security bleiben somit die grundlegenden attributorientierten bzw. gefahrenzentrierten Sichtweisen konstant. Im Bereich Security sind jedoch auch stärkere Eingrenzungen im Hinblick auf die Berücksichtigung der Informationen als schützenswerte Güter von informationsverarbeitenden Systemen vorstellbar [Ecke06, 3]. So wird in enger gefassten Definitionen von Security explizit der Schutz der in einem System verarbeiteten Daten vor unberechtigter Manipulation als Zielsetzung der Disziplin angeführt [Kers95, 73f]. Es erfolgt somit eine Verschiebung der zu Grunde liegenden Sichtweise in Richtung einer objektzentrierten Sicht, die auf den Schutz der jeweiligen Informationen des Systems abzielt.

Um die Trennschärfe zwischen den Disziplinen zu erhalten, wird die angesprochene objektzentrierte Sicht in der vorliegenden Arbeit als eine eigene Disziplin der Informationssicherheit eingeführt.

2.4.2. Informationssicherheit

Informationssicherheit als Disziplin basiert auf den grundlegenden Ansätzen des Bereichs Security im Sinne des Schutzes vor externen Einflüssen. Sie konkretisiert im Kontext der Informationsverarbeitung jedoch die Sichtweise hin zu einer objektzentrierten, attributorientierten Sicht, die Informationen als schützenswerte Güter von Anwendungs- und Hardwaresystemen in den Mittelpunkt stellt.

Informationssicherheit kann somit als Teildisziplin angesehen werden, deren Ziel es ist sicherzustellen, dass ein System nur solche Zustände annimmt, die zu keiner unautorisierten Informationsgewinnung oder -änderung durch externe Entitäten führen [Ecke06, 5]. Die entsprechenden Charakteristika dieses Bereichs lassen sich wie folgt zusammenfassen.

- Bezugsobjekt - informationsverarbeitendes System
- Asset - Information
- Sicht - attributorientiert

Informationssicherheit bildet somit eine Spezialisierung der Disziplin Security in Bezug auf die Domäne der Informationsverarbeitung und bildet die Grundlage für die Ausführungen dieser Arbeit.

2.4.3. Bildung von Teildisziplinen im Vergleich

Die vorgestellten Teildisziplinen des Themenkomplexes Sicherheit in der Informationsverarbeitung werden trotz des Vorhandenseins größtenteils gleicher Bezugsobjekte oftmals sehr unterschiedlich behandelt und zueinander in Beziehung gesetzt. Dieses Phänomen beginnt im Grunde mit der Benennung der jeweiligen Bereiche. Im deutschsprachigen Raum wird der Begriff Sicherheit sehr unscharf und allgemein verwendet, eine initiale Unterscheidung von Safety und Security wie im Englischen findet nicht statt [Stra91, 38]. Umgekehrt wird dem Begriff Security im Englischen ein durchaus weitreichender Bedeutungsumfang zugeschrieben, im Deutschen hingegen wird der Sicherheitsbegriff durch Präpositionen wie Daten-Sicherheit oder IT-Sicherheit präzisiert.

Analog zu dieser Betrachtung finden sich auch unterschiedliche Verständnisse dahingehend, was die Sicherheitsbereiche eigentlich ausdrücken. Manche Autoren sehen sie als Eigenschaften des Bezugsobjektes [Fire05], andere stellen den Aufgabencharakter in den Vordergrund [FePf00]. Auch hier scheint eine Abgrenzung notwendig.

In der vorliegenden Arbeit bildet die allgemeine Unterteilung in die Bereiche Security und Safety die Grundlage. Sie wird jedoch erweitert um den spezialisierten Bereich der Informationssicherheit, um den Fokus auf die Information als Asset der Betrachtung zu richten. Weiterhin wird ein aufgabenorientierter Ansatz gewählt, der die Sicherheitsbereiche als Disziplinen mit bestimmten Zielsetzungen charakterisiert. Um diese Sichtweise zu präzisieren und gegen Bezeichnungen wie IT-Sicherheit oder Computer Sicherheit abzugrenzen, werden ausgewählte Begriffssysteme in den folgenden Abschnitten vergleichend vorgestellt.

Begriffssystem des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Informationssicherheit hat im Sinne des BSI den Schutz von Informationen zum Ziel, unabhängig davon welches Bezugsobjekt referenziert wird [BSI09, 49]. Der Begriff IT-Sicherheit wird als diesbezügliche Spezialisierung verstanden, der sich konkret auf die Sicherheit von elektronisch gespeicherter Information bezieht. Obwohl der Begriff Informationssicherheit als umfassender gilt, verwendet das BSI in ihren Publikationen generell den Begriff IT-Sicherheit als Synonym, wie es den Anschein hat hauptsächlich aus Gründen der Kontinuität.

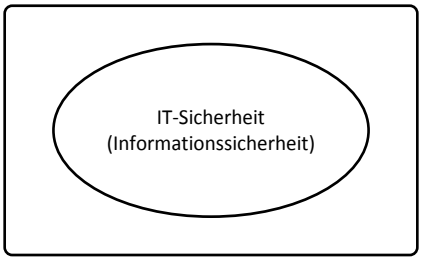

Abbildung 3: Begriffsabgrenzung des BSI

Eine definitorische Abgrenzung verschiedener Teildisziplinen konnte in den Standards des BSI nicht identifiziert werden. Die sukzessive Einführung des Begriffs der Informationssicherheit scheint jedoch angedacht [BSI08b, 12].

Begriffssystem nach Opplinger

OPPLINGER unterscheidet grundlegend in die Teilbereiche Computersicherheit (Compusec) und Kommunikationssicherheit (Comsec). Informationssicherheit wird als echte Obermenge dieser Teilbereiche angesehen, während der Begriff IT-Sicherheit als Vereinigungsmenge von Compusec und Comsec definiert wird.

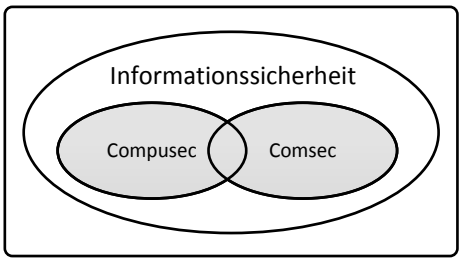

Abbildung 4: Begriffsabgrenzung nach OPPLINGER

IT-Sicherheit wird dabei als Fachgebiet definiert, das sich mit der sicheren Speicherung, Verarbeitung und Übertragung von Daten befasst [Oppl97, 4f].

Begriffssystem nach Pohl

Informationssicherheit wird durch POHL mit dem Begriff Security gleichgesetzt. Eine Teilmenge von ihr bildet neben weiteren Bereichen, wie etwa der Betriebssicherheit, die IT-Sicherheit, oder auch Computer Security. Informationssicherheit zielt dabei auf die Vertrauenswürdigkeit eines Systems ab, die durch die Vermeidung unberechtigter Nutzung, Verfügbarkeit von Daten sowie einer verbindlichen Verarbeitung dieser Daten gekennzeichnet ist [Pohl04, 679].

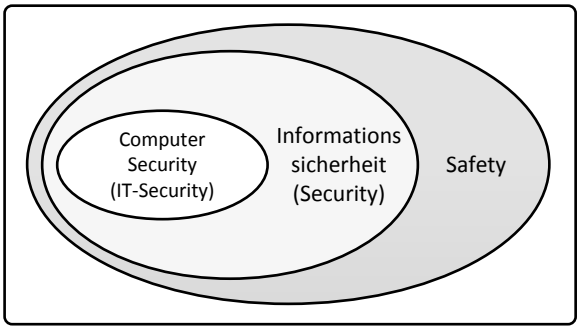

Abbildung 5: Begriffsabgrenzung nach POHL

Neben diesen Aspekten greift POHL auch Safety als Teilbereich auf und charakterisiert diesen als übergreifendes Konstrukt, das neben IT-Systemen auch die Umwelt dieser Systeme beinhaltet [Pohl04, 678].

Begriffssystem nach Eckert

Informationssicherheit entspricht in diesem Fall ebenfalls dem Bereich Security, mit dem Ziel des Schutzes der durch ein System verarbeiteten Informationen. ECKERT differenziert hiervon den Begriff der Datensicherheit (engl. *protection*), die rein auf den Schutz der Daten als Repräsentation von Information abzielt [Ecke06, 5].

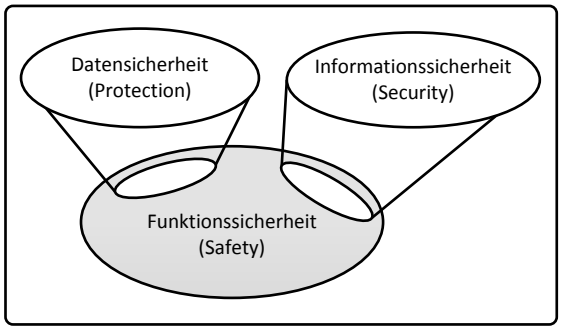

Abbildung 6: Begriffsabgrenzung nach ECKERT

Informationssicherheit und Datensicherheit werden dabei als Prozess charakterisiert, der über den Lebenszyklus eines Systems kontinuierlich zu verfolgen ist. Die Grundlage bzw. Voraussetzung für Informationssicherheit ist laut ECKERT die Funktionssicherheit, die mit dem Begriff Safety gleichsetzt wird [Ecke06, 4f].

Begriffssystem der vorliegenden Arbeit

Im Rahmen der vorliegenden Arbeit werden die beiden Disziplinen Security und Safety als disjunkt angesehen. Der Hauptgrund hierfür liegt primär in der inhaltlichen Unterscheidung, ob es sich um unzulässige intentionale externe Beeinflussung handelt (Security) bzw. um unzulässige nicht-intentionale Beeinträchtigungen, die systemintern auftreten (Safety). Wichtig bei dieser Argumentation ist, dass das betrachtete Bezugsobjekt als konstant anzusehen ist, somit Security und Safety hinsichtlich des gleichen Bezugsobjektes differenziert werden[8].

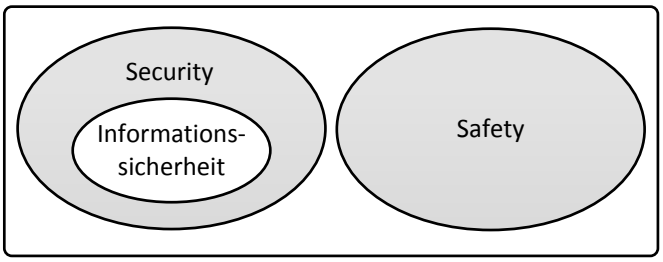

Abbildung 7: Begriffsabgrenzung Informationssicherheit

Basierend auf dieser Differenzierung wird **Informationssicherheit** dann als Spezialisierung von Security angesehen, die attributorientiert auf das Asset Information ausgerichtet ist.

Bei dem vorgestellten Verständnis von Informationssicherheit ist in der Folge zu prüfen, in welchem Kontext diese Abgrenzung anwendbar ist. Bisher wurde sie im Rahmen informationsverarbeitender System auf Aufgabenträgerebene im Sinne von Hard- oder Softwaresystemen vorgenommen. Gegenstandsbereich der Wirtschaftinformatik sind in diesem Zusammenhang jedoch betriebliche Systeme, durch die realweltliche Unternehmen oder Organisationen repräsentiert werden. Eine dahingehende Erweiterung zu dem Konzept der **betrieblichen Informationssicherheit** wird in dem folgenden Kapitel vorgestellt.

[8] Gerade dieser Aspekt wird in der Literatur oftmals nicht berücksichtigt, wenn argumentiert wird, dass eine Differenzierung in Security und Safety im Kontext der IT nicht zielführend ist. Vgl. hierzu etwa [Dier04].

3. Betriebliche Informationssicherheit

Auf Grundlage der Ausführungen zur allgemeinen Sicherheit bzw. Informationssicherheit wird der Begriff der betrieblichen Informationssicherheit als Kernthema der vorliegenden Arbeit eingeführt. Dieser orientiert sich an der Definition des betrieblichen Informationssystems nach FERSTL und SINZ [FeSi08, 2] und wird somit als Sicherheit des informationsverarbeitenden Teilsystems eines Gegenstandsbereichs, wie etwa einer Unternehmung, angesehen.

Kapitel 3.1 geht auf die grundlegende Definition betrieblicher Informationssicherheit ein und analysiert diese aus Innen- sowie aus Außensicht. Das Ergebnis dieser Analyse bildet die Grundlage für die Betrachtung der betrieblichen Informationssicherheit unter der Metapher der betrieblichen Aufgabe in Kapitel 3.2. Abschließend werden in Kapitel 3.3 die aus dieser Metapher resultierenden Dimensionen der betrieblichen Informationssicherheit abgeleitet, die im weiteren Verlauf der Arbeit als Strukturierung der Erläuterungen fungieren.

3.1. Sicherheit in betrieblichen Systemen

Durch die Merkmale Bezugsobjekt, Asset und Sicht sind die Teildisziplinen der Sicherheit differenzierbar. Ein Wechsel der bisherigen Betrachtungsweise in den Gegenstandsbereich der Wirtschaftsinformatik erfolgt somit durch die Neubelegung der entsprechenden Merkmale.

3.1.1. Grundlagen und Definition

Als Bezugsobjekt findet das Konzept des betrieblichen Objektsystems Verwendung, das die Diskurswelttobjekte des betrachteten Ausschnittes der betrieblichen Realität, die zugehörigen Umwelttobjekte sowie die Beziehungen zwischen diesen Objekten abbildet [FeSi08, 5]. Ein betriebliches Objektsystem beschreibt somit konkrete Unternehmen oder Organisationen, die im Rahmen der Wirtschaftsinformatik betrachtet werden. Relevante Assets dieses Systems, stellen im vorliegenden Kontext die Informationen dar, die in diesem System erzeugt oder verarbeitet werden. Die folgende Abbildung stellt eine mögliche Systemabgrenzung anhand unterschiedlicher Kriterien dar.

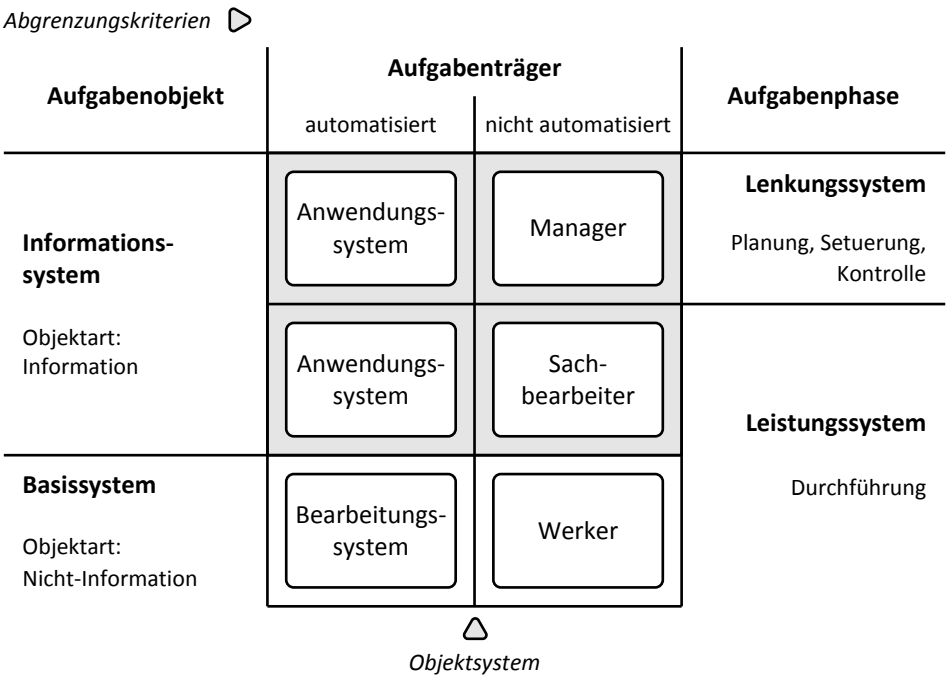

Abbildung 8: Teilsysteme des Objektsystems (nach [FeSi08, 5])

Die Festlegung der Objektart Information als Asset der Betrachtung führt zu einer inhaltlichen Deckungsgleichheit des Bezugsobjektes mit dem Teilsystem des Informationssystems, das durch die Anwendung des Objektprinzips zur Systemabgrenzung entsteht[9]. Der spezifische Begriff des betrieblichen Informationssystems (bIS) bezeichnet dann das gesamte informationsverarbeitende Teilsystem eines betrieblichen Objektsystems [FeSi08, 2]. Aufgaben dieses Teilsystems bestehen in der Lenkung betrieblicher Prozesse sowie der Erzeugung von Dienstleistungen, sofern diese auf der Objektart Information beruhen [FeSi08, 11]. In der Abbildung ist das bIS grau hinterlegt dargestellt.

Für die Definition des Begriffs der betrieblichen Informationssicherheit wird das Konzept des bIS als zentrales Bezugsobjekt genutzt. **Betriebliche Informationssicherheit** bezeichnet somit die Sicherheit des betrieblichen Informationssystems vor Einflüssen, die zu unautorisierter Informationsgewinnung oder –manipulation führen.

Die in der Definition verwendete attributorientierte Sichtweise wird anhand der Assetbestimmung und der resultierenden Teilsystemabgrenzung deutlich. Gleichwohl wird durch die explizite Berücksichtigung der Einflüsse, egal ob exogen oder endogen, Bezug genommen auf die gefahrenzentrierte Sichtweise, die der „Elterndisziplin“ Security zu Grunde

[9] Eine detailliert Darstellung der Abgrenzungskriterien ist in [FeSi08, 6] zu finden.

liegt. Analog zu den bisherigen Differenzierungen kann der Bereich der betrieblichen Informationssicherheit somit wie folgt charakterisiert werden:

- Bezugsobjekt - betriebliches Informationssystem
- Asset - Information
- Sicht - attributorientiert

Das betriebliche Informationssystem bildet das zentrale Bezugsobjekt der Sicherheitsbetrachtungen in der vorliegenden Arbeit. Analog dazu fungiert die betriebliche Informationssicherheit als entsprechender aufgabenorientierter Teilbereich der Security. Die folgenden Abschnitte betrachten diese Disziplin nun eingehender aus unterschiedlichen Blickwinkeln.

3.1.2. Außensicht betrieblicher Informationssicherheit

Erfolgt die Betrachtung eines Systems aus Außensicht, so wird einerseits sein äußeres Verhalten gegenüber der Umwelt erkennbar, andererseits die Schnittstellen, mit denen es diesbezüglich interagiert [FeSi08, 21]. Überträgt man diese Sichtweise auf das Themengebiet der betrieblichen Informationssicherheit, so werden letztgenannte Schnittstellen, und somit die Außensicht, im Wesentlichen durch deren Teilbereiche beschrieben.

Die Bildung von Teilbereichen der betrieblichen Informationssicherheit erfolgt durch die weitere Detaillierung des betrieblichen Informationssystems als Bezugsobjekt. Gemäß der Teilsystemdefinition in Abbildung 8 werden anhand der Phasen- und Automatisierungsdifferenzierung weitere Komponenten erkennbar. Im Wesentlichen wird dadurch deutlich, dass sich betriebliche Informationssicherheit einerseits sowohl auf personelle wie auch auf maschinelle Aufgabenträger bezieht, auf der anderen Seite Aufgaben des Lenkungssystems ebenso betrifft wie die des Leistungssystems. Aus dieser Differenzierung kann somit eine ebenenorientierte Strukturierung der betrieblichen Informationssicherheit abgeleitet werden.

Die **Aufgabenebene** beinhaltet eine Menge von Informationsverarbeitungsaufgaben, die durch Informationsbeziehungen miteinander verknüpft sind und die sowohl dem Lenkungssystem als auch dem Leistungssystem zugeordnet werden können. Die **Aufgabenträgerebene** wird durch die Menge aller maschinellen und personellen Aufgabenträger des betrieblichen Informationssystems gebildet, die durch Kommunikationsbeziehungen miteinander verbunden sind [FeSi08, 3f].

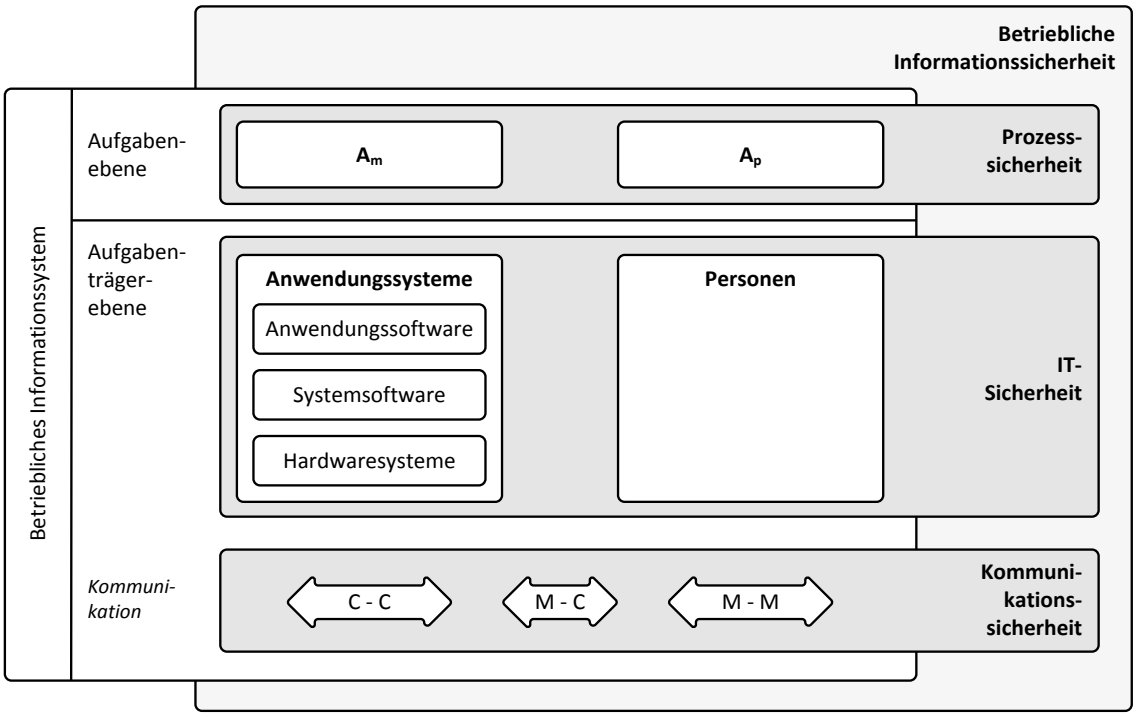

Abbildung 9: Teilbereiche betrieblicher Informationssicherheit

Betriebliche Informationssicherheit kann anhand der vorgestellten Struktur des Bezugsobjektes aus Außensicht in die drei Teilbereiche **Prozesssicherheit**, **IT-Sicherheit** und **Kommunikationssicherheit** unterteilt werden. Differenzierendes Merkmal ist jeweils das Teil-Bezugsobjekt des betrieblichen Informationssystems, auf das sich die jeweilige Disziplin bezieht.

Die **Prozesssicherheit** adressiert die Aufgabenebene des betrieblichen Informationssystems. Ziel ist die Sicherheit der Aufgabendurchführungen sowie der Informationsbeziehungen zwischen den Aufgaben. Prozesse, als Abfolge von Aufgabendurchführungen, sollen somit in der vorgesehenen Art und Weise durchführbar sein, ohne das Informationen durch unautorisierte Parteien eingesehen oder modifiziert werden können.

IT-Sicherheit bezieht sich auf die Aufgabenträgerebene des betrieblichen Informationssystems. Entgegen der Auffassung, dass sich diese Teildisziplin nur auf maschinelle Aufgabenträger bezieht, werden personelle Aufgabenträger explizit als Bezugsobjekte der IT-Sicherheit berücksichtigt. Dieser Ansatz trägt der Meinung Rechnung, dass der Mensch immer den schwächsten Faktor in einer, auch computergestützten, Sicherheitskette bildet[10] [MiSi06, 20]

[10] Aus angriffsorientierter Perspektive betrachtet wird dieser Teilbereich als „Social Engineering“ bezeichnet, vgl. hierzu [ScSh04] oder [Proc+09].

[Nohl09]. IT-Sicherheit bezieht sich somit auf die Sicherheit von Anwendungssystemen vor unautorisierter Informationsgewinnung bzw. -manipulation sowie auf den Schutz von Nutzern im Umgang mit den bereitgestellten und verarbeiteten Informationen.

Kommunikationssicherheit bezieht sich auf die Kommunikationssysteme der Aufgabenträgerebene, durch die die Kommunikationskanäle zur Realisierung der Informationsbeziehungen auf Aufgabenebene bereitgestellt werden. Kommunikationssysteme fungieren als Basismaschine, auf der Anwendungssysteme und Personen als Nutzermaschine operieren[11]. Die Sicherheit der Übertragung von Informationen in diesen Systemen ist Gegenstand dieser Teildisziplin.

Die Aufgabenträgerebene eines betrieblichen Informationssystems als Menge von Anwendungssystemen, Personen und Kommunikationssystemen [FeSi08, 4f] wird durch die Teilbereiche IT-Sicherheit und Kommunikationssicherheit vollständig abgedeckt. Zusammen mit der Prozesssicherheit auf Aufgabenebene wird die Disziplin der betrieblichen Informationssicherheit aus Außensicht somit vollständig beschrieben. Sie umfasst dabei prinzipiell auch nicht-elektronisch gespeicherte Informationen des betrieblichen Umfelds, aus der Perspektive der Wirtschaftsinformatik betrachtet wird dieser Aspekt in der vorliegenden Arbeit jedoch nicht weiter berücksichtigt.

3.1.3. Innensicht betrieblicher Informationssicherheit

Die Innensicht eines Systems beleuchtet die interne Struktur und das Verhalten der jeweiligen Komponenten und Teilsysteme [FeSi08, 22]. In Bezug auf die betriebliche Informationssicherheit wird diese Sichtweise durch die Beziehungsstruktur der inhaltlichen Bestandteile dieser Sicherheitsdisziplin repräsentiert. Gemäß dem Aufbau der Arbeit lassen sich diese Komponenten als Erweiterung des allgemeinen Sicherheitsbegriffs interpretieren und können analog dazu als semantisches Netz der Innensicht betrieblicher Informationssicherheit dargestellt werden.

[11] Zum Konzept der Nutzer- und Basismaschine vgl. [FeSi84, 74ff].

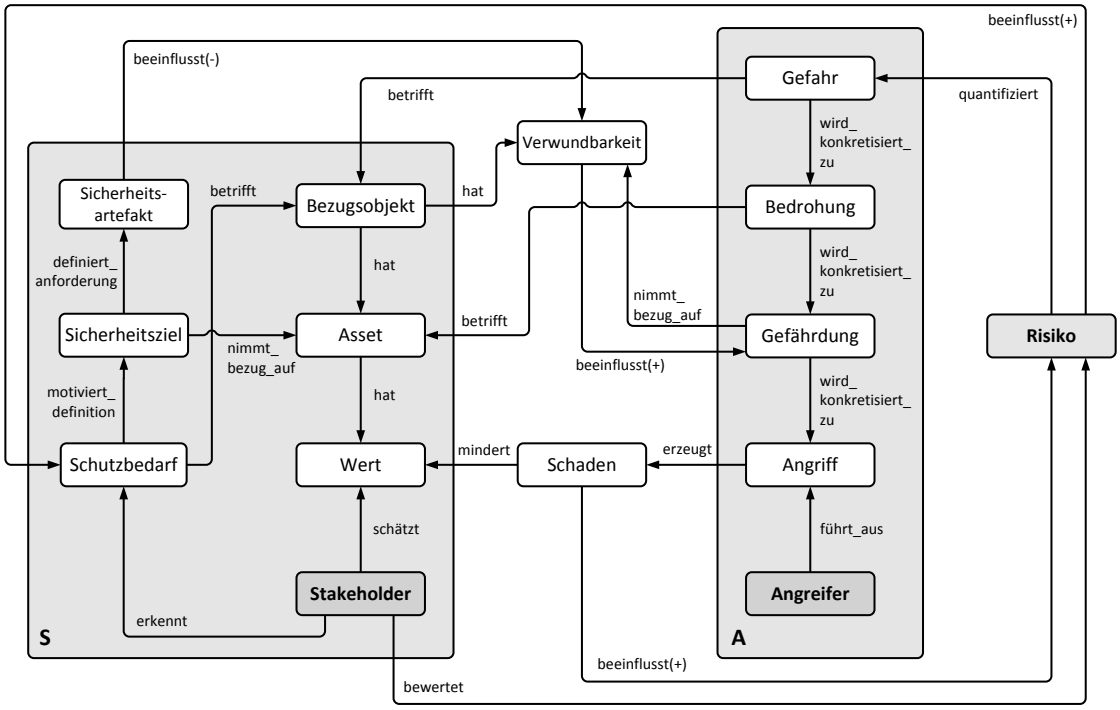

Abbildung 10: Innensicht betrieblicher Informationssicherheit[12]

Im Vergleich zu Abbildung 1 erfolgt bei der Betrachtung der Innensicht eine weitergehende Differenzierung des allgemeinen Sicherheitsmerkmals Gefahr in die Begriffe **Verwundbarkeit**, **Bedrohung**, **Gefährdung** und **Angriff** sowie damit einhergehend die Einführung von Gegenmaßnahmen in Form von **Sicherheitszielen** und **Sicherheitsartefakten**. Systematisiert werden die Begriffe dabei in die inhaltliche Perspektive S des Stakeholders sowie die Perspektive A eines Angreifers[13]. Die folgenden Erläuterungen orientieren sich an dieser Einteilung, die durch die Darstellung des Risikobegriffs als verbindendes Element ergänzt werden.

3.1.3.1. Perspektive des Angreifers

Aus der Sicht des Angreifers erfolgt durch die Abstufungen des Gefahrenbegriffs eine zunehmende Präzisierung der Situation. Gefahren beziehen sich allgemein auf Typen von bestimmten Bezugsobjekten, Bedrohungen hingegen fokussieren auf bestimmte Assets dieser

[12] In Anlehnung an [Fire04, 62] und [Ecke06, 30]. Die Darstellung ist konzipiert als Erweiterung von Abbildung 1, bestimmte Elemente wie zum Beispiel der Begriff Kontext wurden jedoch aus Darstellungsgründen entfernt.

[13] Es ist anzumerken, dass die in Abbildung 10 definierten Beziehungen zwischen den Elementen keinen Anspruch auf Vollständigkeit erheben. Es ist offensichtlich, dass, je nach Blickwinkel, unterschiedliche Interpretationen zulässig sind. Die gewählte Darstellungsform ist abgestimmt auf das Verständnis der vorliegenden Arbeit und hat das Ziel, diese Zusammenhänge als Grundlage für die Ausführungen zu visualisieren.

Objekte. Gefährdungen schließlich stellen auf konkrete Instanzen der Bezugsobjekte mit entsprechenden Verwundbarkeiten ab.

Gefahr

Gefahren beschreiben, wie in Kapitel 2.1.2 eingeführt, die Möglichkeit eines Fehler- oder Schadensereignisses. Im Kontext der betrieblichen Informationssicherheit als Teildisziplin der Security beziehen sich Gefahren auf die intentionale Verursachung von Schaden und werden daher explizit in der konzeptuellen Domäne A eines Angreifers als Spezialisierung des Verursacherprinzips aus Abbildung 1 aufgenommen. Gefahren sind in diesem Zusammenhang als abstraktes Konzept zu verstehen, das in Bezug auf das Asset Information weiter konkretisiert wird.

Bedrohung

Eine Bedrohung (engl. *threat*) bezeichnet in der Literatur einen Zustand oder ein Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert eines Assets eines Bezugsobjektes [BSI09, 46]. Im Vergleich zu dem Begriff Gefahr erfolgt somit eine assetorientierte Präzisierung des Begriffsverständnisses, die in der Abbildung durch die Verbindung zwischen Bedrohung und Asset symbolisiert wird. Im Kontext der betrieblichen Informationssicherheit kann somit zum Beispiel von einer Bedrohung der Vertraulichkeit des Assets Information gesprochen werden.

Verwundbarkeit

Eine Verwundbarkeit (engl. *vulnerability*), oder auch Schwachstelle, ist ein sicherheitsrelevanter Fehler eines Bezugsobjektes. Ursachen können in der Konzeption, Implementierung, Konfiguration oder der Organisation des Bezugsobjektes liegen [BSI09, 54]. Die Existenz einer Verwundbarkeit ist die Voraussetzung dafür, dass eine Gefährdung durch einen Angriff realisiert werden kann und in der Konsequenz Schaden an dem Bezugsobjekt verursacht wird.

Gefährdung

Eine Gefährdung (engl. *applied threat*) ist eine Bedrohung, die auf eine Verwundbarkeit eines Bezugsobjektes einwirkt. Das parallele Vorhandensein einer solchen Schwachstelle und einer Bedrohung ist somit die Voraussetzung für eine konkrete Gefährdung, die in der Literatur auch als räumlich, zeitlich und nach ihrer Art konkretisierte Gefahr definiert wird [BSI09,

48f]. Existiert im Umkehrschluss betrachtet keine Verwundbarkeit des Bezugsobjektes, so kommt es auch zu keiner Gefährdung.

Beispiel

Anhand des Szenarios „Surfen im Internet“ kann das Verständnis der Zusammenhänge zwischen den bisher vorgestellten Begriffen verdeutlicht werden.

Nutzt eine Person das Internet durch einen Webbrowser, so besteht grundlegend eine abstrakte Gefahr der Kompromittierung des verwendeten Computers, da technisch gesehen eine bidirektionale Verbindung zwischen Dritten und dem Computer des Nutzers vorhanden ist. Eine konkretere Bedrohung für die Informationen, die auf dem Computer gespeichert sind, entsteht durch die Existenz einer Webseite, die unautorisiert Schadsoftware auf dem Rechner des Nutzers einzuschleusen versucht. Verwendet der Nutzer eine Browserversion, die solche Operationen zulässt und werden keine Schutzmaßnahmen, wie zum Beispiel Virenscanner, eingesetzt, so besitzt das System in dieser Hinsicht eine Schwachstelle. Das Vorhandensein der Schwachstelle sowie die Existenz der Bedrohung erzeugen somit eine konkrete Gefährdung für die Daten des Nutzers. Die Realisierung der Gefährdung in Form eines konkreten Angriffs erfolgt dann durch den Aufruf einer entsprechend präparierten Webseite. Existiert die Schwachstelle hingegen nicht, da zum Beispiel die Schadsoftware erkennende Virenscanner aktiv sind, so besteht diesbezüglich auch keine Gefährdung und ein entsprechender Angriff kann nicht stattfinden.

Die letztendliche Verbindung zwischen Angreifer und Bezugsobjekt bzw. Asset wird auf Grund der dargestellten Abstufung des Gefahrenbegriffs schrittweise konkretisiert. Aus Sicht des Stakeholders geht dies einher mit einer antizipierten Zunahme der Eintrittswahrscheinlichkeit eines Schadens zum einen und teilweise auch mit einer gesteigerten Identifizierbarkeit möglicher Gruppen von Angreifern[14] zum anderen. Diese Einschätzungen manifestieren sich sodann im Risikobegriff der betrieblichen Informationssicherheit.

3.1.3.2. Risikobegriff betrieblicher Informationssicherheit

Der Risikobegriff bzw. die Risikobewertung durch einen Stakeholder im Rahmen der betrieblichen Informationssicherheit definiert zum Großteil den Grad der Relevanz, der einer be-

[14] Bestimmte Typen von möglichen Angreifern, wie etwa Firmenangehörige oder externe Hacker, sowie deren potentielle Motive werden zum Beispiel in [Kizz05, 136ff] oder [Ecke06, 19ff] klassifiziert. Im Rahmen der Arbeit wird diese Differenzierung nicht weiter betrachtet.

stimmten Gefährdung für eine weitergehende Betrachtung beigemessen wird. In diesem Zusammenhang ist zu definieren, ab welcher Höhe des Risikos eine Situation als unsicher eingestuft wird. Dieser Punkt wird als geheimhin als **Grenzrisiko** bezeichnet und gilt als größtes noch vertretbares Risiko eines bestimmten Vorgangs oder Zustandes [Lip+92, 369].

Sicherheit wird in dieser risikoorientierten Interpretation als Sachlage aufgefasst, bei der ein konkretes Risiko nicht höher eingestuft wird als das zuvor definierte Grenzrisiko. Aus diesem Verständnis ableitbar ist die Tatsache, dass die Begriffe Sicherheit und Gefahr nicht, wie in der Gemeinsprache oftmals angenommen, als Gegensätze definiert sind, sondern sich vielmehr auf einen gemeinsamen Maßstab beziehen, das **Schadensrisiko**. Sicherheit und Gefahr werden dabei durch das Grenzrisiko separiert [GeKo08, 123]. Der Begriff Gefahr ist hierbei als Oberbegriff anzusehen, der, wie beschrieben, in Abhängigkeit von einem Konkretisierungsgrad auch als Bedrohung oder Gefährdung interpretiert werden kann. In Bezug auf den Maßstab des Schadensrisikos würden die letztgenannten Elemente durch subjektiv bestimmbare Punkte auf der Achse repräsentiert werden, wobei generell gilt, dass ein Schadensrisiko bei einer Bedrohung geringer ist als das bei einer Gefährdung.

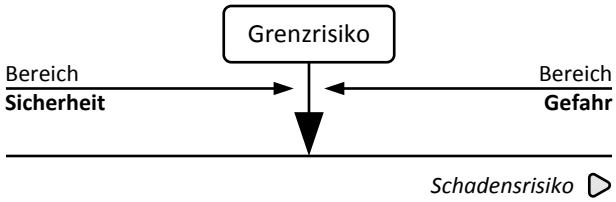

Abbildung 11: Der Begriff des Grenzrisikos (nach [GeKo08, 123])

Der Begriff des Schadensrisikos nimmt Bezug auf die zentrale Rolle, die die Schadenshöhe bei der Beurteilung von Risikowerten einnimmt. In der Praxis erfolgt hierbei oftmals eine funktionale Verknüpfung zwischen Eintrittswahrscheinlichkeit und Schadenshöhe, so dass gilt:

$$\text{Risiko} = f(\text{Eintrittswahrscheinlichkeit}, \text{Schadensausmaß})$$

Dabei ist zu beachten, dass diese Bewertung in der Regel eine rein qualitative Aussage darstellt, da kein definierter funktionaler Zusammenhang zwischen den beiden zentralen Risikomerkmalen Eintrittswahrscheinlichkeit und Schadenshöhe angegeben werden kann. Eine oftmals vorgenommene „einfache“ Multiplikation der beiden Größen gilt als nicht allgemeingültig anerkannt [Petz96, 20].

Im Rahmen der betrieblichen Informationssicherheit wird Risiko[15] in der Regel in der dargestellten Art und Weise interpretiert. Konkret fließen dabei die Merkmale **Gefährdungspotential** und **Schadenspotential** in die Bewertung mit ein [Ecke06, 15f]. Das Gefährdungspotential bezieht sich dabei auf die Abschätzung der Eintrittswahrscheinlichkeit einer Gefährdung. Ausreichendes Wissen über mögliche Bedrohungen sowie existente Schwachstellen sind hierfür die Voraussetzung. Die Bewertung des Schadenspotentials auf der anderen Seite macht eine umfassende Katalogisierung der zu betrachtenden Assets notwendig, sowie die möglichst objektive Quantifizierung der jeweiligen Werte für einen entsprechenden Stakeholder. In betrieblichen Systemen sind für die Erfüllungen der beiden Voraussetzungen hohes Fach- und umfassendes Prozesswissen notwendig, so dass neben dem ohnehin stark subjektiven Charakter der Risikobewertung auch eine möglichst objektive Einschätzung als durchaus schwierig zu charakterisieren ist [Ecke06, 16].

3.1.3.3. Perspektive des Stakeholders

Als Gegenpol zu der getroffenen Konkretisierung der Gefahr sind aus der Sicht S des Stakeholders ebenfalls Präzisierungen vorzunehmen. Diese beziehen sich vornehmlich auf die Spezifikation von Maßnahmen, die den Schutz der Bezugsobjekte bzw. der entsprechenden Assets zum Ziel haben.

Schutz

Unter dem Begriff Schutz werden alle Arten von Maßnahmen subsumiert, die dazu dienen einen gewissen Grad an Sicherheit für ein Bezugsobjekt herzustellen und somit das definierte Grenzrisiko zu unterschreiten. Dies kann gemäß der Definition von Risiko zum einen durch die Reduzierung des Schadensausmaßes erfolgen oder aber durch die Verringerung des Gefährdungspotentials [GeKo08, 128]. Da die subjektive Wertschätzung eines Assets durch den Stakeholder jedoch nicht beliebig beeinflussbar ist, konzentrieren sich beide Aspekte im Prinzip auf die Vermeidung bzw. Reduktion von Verwundbarkeiten, um die Entstehung von Gefährdungen zu verhindern bzw. deren mögliche Schadwirkung zu reduzieren. Erreicht wird dies durch die Einführung von Zieldefinitionen und darauf aufbauend Sicherheitsartefakten, die durch den Stakeholder zu spezifizieren sind. Das in Abbildung 10 diesbezüglich dargestellte Element Schutzbedarf ist dabei als abstrakte Komponente zu verstehen, die das Bedürfnis und den Willen eines Stakeholders zur Herstellung von Sicherheit widerspiegelt und

[15] Schadensrisiko und Risiko werden in der Arbeit synonym verwendet.

somit auch seine Zielorientierung darstellt. Die transitive Beziehung zwischen Schutzbedarf und Verwundbarkeit über die Elemente Sicherheitsziel und Sicherheitsartefakt in der Abbildung machen den dargestellten Zusammenhang deutlich.

Sicherheitsziel

Die Erreichung von Sicherheit stellt kein homogenes Einzelziel dar, sondern umfasst ein Bündel vielfältiger Einflussfaktoren [Lip+92, 369]. Für die Menge aus sicherheitsbezogenen Sach- und Formalzielen wird in der vorliegenden Arbeit der Oberbegriff **Sicherheitsziele** verwendet. Sie beziehen sich auf bestimmte Eigenschaften von Bezugsobjekten bzw. deren Assets, sowie auf die Art und Weise, wie diese unter Sicherheitsgesichtspunkten zu gewährleisten und zu erhalten sind.

Unter sicherheitsorientierten Formalzielen werden in der Regel unternehmensexterne gesetzliche Regelungen oder unternehmensinterne Vorgaben subsumiert, die sich auf die Qualität der Zielerreichung beziehen. Formalziele werden in den Ausführungen der folgenden Abschnitte nur rudimentär betrachtet, da sie für die vorliegende Arbeit im Vergleich zu Sachzielen nur geringe Relevanz aufweisen[16].

Sachziele, auch als **Schutzziele** bezeichnet, beziehen sich in erster Linie auf konkrete Eigenschaften der zu schützenden Assets von Bezugsobjekten. Die **Integrität** eines Datensatzes zum Beispiel stellt solch ein Attribut dar. Wird der Datensatz unberechtigt manipuliert, so führt der einhergehende Verlust der Integrität potentiell zu Schäden für den jeweiligen Stakeholder. Grundlegend besteht somit ein konkretes Schadensrisiko, das auf der subjektiven Wertschätzung der Eigenschaft Integrität des Datensatzes beruht sowie auf der Bewertung der Eintrittswahrscheinlichkeit eines Verlustfalles. Ist dieses subjektiv geschätzte Schadensrisiko kleiner als das definierte Grenzrisiko, so besteht Sicherheit hinsichtlich des Attributs Integrität. Dieser anzustrebende Soll-Zustand spiegelt den Zielcharakter der Schutzziels Integrität wider.

Neben dem Genannten werden in der Literatur die zwei weiteren Ziele **Vertraulichkeit** und **Verfügbarkeit** als klassische Schutzziele geführt [FePf00, 708]. Ihre Zuweisbarkeit ist dabei indirekt abhängig vom Typ des jeweiligen Bezugsobjektes, d.h. bestimmte Schutzziele greifen nicht zwingend für jedes Bezugsobjekt semantisch sinnvoll. So erscheint das Schutzziel

[16] Kapitel 5.4.2 gibt hierzu eine überblicksartige Zusammenfassung.

Integrität zum Beispiel wenig sinnvoll, wenn es auf eine Person als Aufgabenträger bezogen wird.

Aus empirischer Sicht betrachtet sind Schutzziele Momentaufnahmen dichotom nominalskalierter Merkmale. Integrität, Vertraulichkeit oder Verfügbarkeit eines Bezugsobjektes sind zu einem bestimmten Zeitpunkt entweder gegeben oder nicht. Im Hinblick auf den zukünftigen Bestand dieses Zustandes kann jedoch keine Aussage getroffen werden. Hierfür ist wiederum die Einschätzung der Eintrittswahrscheinlichkeit eines, das jeweilige Schutzziel betreffenden, Schadens ausschlaggebend. Im Rahmen der Risikobetrachtung bedeutet dies, dass Schutzziele eben dann erfüllt sind, wenn das tatsächlich antizipierte Schadensrisiko geringer ausfällt als das definierte Grenzrisiko. Es sind somit zwei subjektiv festzulegende Werte ausschlaggebend für die Bestimmung ob ein Schutzziel als erreicht gilt. Eine Angabe hingegen, bis zu welchem Grad es erfüllt ist, kann auf Basis der Risiken nur schwerlich getroffen werden und ist abhängig davon, welche diesbezüglichen Methoden zum Einsatz kommen. Schutzziele als integraler Bestandteil der vorliegenden Arbeit werden in Kapitel 5.4.3 im Detail dargestellt.

Sicherheitsartefakte

Unter dem Begriff Sicherheitsartefakt werden alle Ergebnisse von sicherheitsbezogenen Maßnahmen subsumiert, die im Sinne des Schutzes und der Herstellung von Sicherheit auf Bezugsobjekte bzw. deren Verwundbarkeiten einwirken. Das Begriffsverständnis lehnt sich dabei an die Definition und Semantik des Konzepts der Artefakte im Rahmen der UML (Unified Modeling Language) an. Artefakte werden hier als informationstragende Elemente verstanden, die als Folge von Entwicklungs- bzw. Arbeitsschritten entstehen bzw. für deren Durchführung benötigt werden [Bor+05, 151]. Im Kontext der betrieblichen Informationssicherheit sind Sicherheitsartefakte inhaltlich mit den definierten Schutzzielen für ein Bezugsobjekt verbunden. So kann zum Beispiel eine Zugriffskontrollstrategie als Sicherheitsartefakt verstanden werden, das sich auf die Vertraulichkeit einer Information als Schutzziel bezieht. Ex post mindert oder eliminiert der Einsatz von Sicherheitsartefakten bestimmte Verwundbarkeiten von Bezugsobjekten, ex ante verhindert er deren Ausnutzung und damit indirekt das Auftreten von akuten Gefährdungen. In Kapitel 5.3 werden Sicherheitsartefakte im Detail besprochen und in Bezug auf konkrete Bezugsobjekte dargestellt.

Zusammenfassend betrachtet, werden durch den Stakeholder, ausgehend von der Feststellung des Schutzbedarfs, zielorientiert Maßnahmen in Form von zu erstellenden Sicherheitsartefak-

ten definiert, um mögliche Gefährdungen zu reduzieren. Die Elemente Schutzbedarf und Risiko sind in dieser Interpretation in der subjektiven Wahrnehmung eines Stakeholders eng miteinander verknüpft. Zum einen besteht eine positive Korrelation ausgehend von Risiko zu Schutzbedarf, da ein geschätztes, über dem Grenzrisiko liegendes, Schadensrisiko den gewünschten Schutzbedarf steigert. In der Gegenrichtung kehrt sich dieses Verhältnis ins Gegenteil, da ein realisierter Schutz das Schadensrisiko letztendlich mindert, somit eine negative Korrelation vorliegt[17]. Hierbei wird ebenfalls deutlich, dass auch temporale Aspekte bei der Definition der Beziehungen zu berücksichtigen sind. Während die erste Relation gleichbleibend über die Zeit hinweg Gültigkeit besitzt, so kommt die negative Korrelation zwischen Schutzbedarf und Risiko zum Beispiel erst nach der Reduktion der Gefährdung durch Sicherheitsartefakte zum Tragen.

Neben diesen grundlegenden Bewertungen ist die interne Abstimmung und Gewichtung dieses Verhältnisses zwischen Risiko und Schutzbedarf durch einen Stakeholder elementar für die Initiierung bzw. die Durchführung entsprechender Prozesse zur Herstellung betrieblicher Informationssicherheit. Beeinflusst wird dieser Aspekt zusätzlich durch den Standpunkt, den ein Entscheider durch eine, zum Teil auch unbewusste, Fokussierung auf Schutz- oder auf Risikoaspekte einnimmt. Entsprechende Formen sowie die diesbezügliche Ausrichtung der Arbeit werden im folgenden Abschnitt erläutert.

3.1.4. Interpretationen betrieblicher Informationssicherheit

Informationssicherheit als Thema im betrieblichen Umfeld wird in der Literatur sehr unterschiedlich erschlossen und interpretiert. Grundsätzlich allen Ansätzen gemein sind in der Regel jedoch zwei Punkte. Zum einen gilt Sicherheit nicht als absolute sondern als **relative Größe**. Freiheit vor allen Gefahren, im Sinne der Definition des allgemeinen Sicherheitsbegriffs als absolute Sicherheit zu interpretieren, ist in realen Situationen grundsätzlich nicht realisierbar. Zum zweiten wird Sicherheit als **subjektiver Begriff** verstanden, da er, gemäß der Definition des Grenzrisikos, stark von individuellen Standpunkten und Einschätzungen eines Stakeholders abhängig ist [Lip+92, 369].

Neben diesen grundlegend anerkannten Eigenschaften des Sicherheitsbegriffs hat die Einstellung eines Stakeholders gegenüber der betrieblichen Informationssicherheit große Auswir-

[17] Diese Beziehung ist in Abbildung 10 nur indirekt über die Elemente Sicherheitsziel, Sicherheitsartefakt, Verwundbarkeit, Gefährdung und Risiko dargestellt.

kungen auf die Nutzung entsprechender Methoden und Verfahren. Diese subjektiven Auffassungen und Standpunkte zur Erreichung von Sicherheit können nach LIPPERT[18] in drei Kategorien unterteilt werden, die anhand von Elementen des semantischen Netzes aus Abbildung 10 darstellbar sind.

Ansatzpunkt Sicherheitsartefakte

Es wird versucht, Sicherheit primär durch umfassende Sicherheitsartefakte zu erreichen, die als Reaktion auf das Erkennen einer Verwundbarkeit zu realisieren sind. Dies lenkt die Aufmerksamkeit jedoch zu stark auf die Umsetzungsmöglichkeiten und die Vor- bzw. Nachteile einzelner Verfahren. Eine notwendige Konzeptionsphase wird somit vernachlässigt und zu schnell in die Realisierungsphase übergegangen. Von Vorteil bei diesem Ansatz sind unter Umständen schnell erzielte Lösungen, die jedoch auf der anderen Seite in Bezug auf die Berücksichtigung sicherheitsrelevanter Sach- und Formalziele zu kurz greifen.

Ansatzpunkt Gefährdung

Die Erreichung von Informationssicherheit wird hauptsächlich durch die Reduktion von Gefährdungen bestimmt. Nach dieser Auffassung wird ein System dann als sicher charakterisiert, wenn das Eintreffen bzw. die Konsequenzen von gefährdenden Ereignissen ausgeschlossen werden kann. KERSTEN bezeichnet diesen Ansatz auch als „Sicherheit durch Ausschluss“ [Kers95, 84]. Grundlage dieses Verständnisses muss daher eine umfassende Sachkenntnis über bestehende Gefahren und Gefährdungen sein, deren Kategorisierung sowie ein umfassender Maßnahmenkatalog zur Abwehr dieser Gefahren. Es ist jedoch zu bezweifeln, dass ein vollständiges Wissen über alle Gefährdungen bestehen kann, wodurch diese Sichtweise fast zwangsläufig zu einer unvollständigen oder einseitigen Sicherheitsbetrachtung führen muss.

Ansatzpunkt Risiko

Diese Auffassung von Informationssicherheit basiert auf der risikoorientierten Betrachtung von Sicherheit, bei der ein konkretes Risiko für ein Bezugsobjekt geringer als ein definiertes Grenzrisiko einzustufen ist, um als sicher zu gelten[19]. Durch die reine Festlegung des Grenzrisikos wird somit bestimmt, welcher Zustand eines Bezugsobjektes als sicher gilt und welcher

[18] Vgl. hierzu [Lip+92].

[19] Vgl. Abbildung 11.

nicht. In der Konsequenz bedeutet dies, dass Sicherheit primär durch die Bestimmung und Kontrolle von Risiken überwacht wird [TeSc00, 18]. Diese Risiken sind für jedes Bezugsobjekt individuell zu definieren bzw. auch bei Veränderungen der Umwelt, zum Beispiel durch Fortschritt von Technik oder Gesellschaft, neu zu bewerten und festzulegen [GeKo08, 123]. Die beschriebene risikoorientierte Auffassung ist dabei natürlich nicht vollständig frei von der Berücksichtigung von Gefahren. LIPPERT beschreibt dies durch notwendige Aufgaben, die eben auch die Analyse relevanter Gefahren sowie die Ableitung entsprechender Sicherheitsmaßnahmen behandelt [Lip+92, 369].

Fazit

Der zentrale Aspekt in diesem Zusammenhang besteht in dem Ausmaß, mit dem ein bestimmter Ansatzpunkt bestimmend ist für den betrieblichen Umgang mit dem Thema der Informationssicherheit. In Bezug auf das semantische Netz aus Abbildung 10 würde der Ansatzpunkt Gefährdung einer Fokussierung auf die Perspektive A des Angreifers gleichkommen, wohingegen der Ansatzpunkt Sicherheitsartefakt eine Konzentration auf die Perspektive S des Stakeholders bedeuten würde. Der Ansatzpunkt des Risikos, als gewählte Grundlage dieser Arbeit, verknüpft die beiden erstgenannten Ansätze und ermöglicht somit eine konzeptionell und technisch ausgewogene Betrachtung des Themas. In dem semantischen Netz sind die Grundlagen dieser Interpretation durch die Beziehungen zwischen Schutzbedarf, Sicherheitsziel und Risiko visualisiert.

Die risikoorientierte Grundhaltung hat ebenfalls Auswirkungen auf die Abstimmung der Innen- und Außensicht der betrieblichen Informationssicherheit. Der Teilbereich Prozesssicherheit zum Beispiel bezieht sich auf das Bezugsobjekt der Aufgabenebene eines betrieblichen Informationssystems. Aus risikoorientierter Perspektive wird in diesem Zusammenhang die Perspektive des Angreifers nur in geringem Maße betrachtet. Eine entsprechende Herangehensweise führt somit aus Innensicht dazu, dass nur ein Teilgraph des semantischen Netzes für die Abdeckung der relevanten Elemente ausreichend ist. Basierend auf dieser Betrachtungsweise bildet sich auch die Grundlage für die Spezifikation einer Modellierungsmetapher heraus. In Teil II und III der Arbeit wird dies zum Beispiel daran ersichtlich, dass auf Ebene der Geschäftsprozesse keine Bedrohungen bzw. Gefährdungen modelliert werden.

3.2. Informationssicherheit als betriebliche Aufgabe

Informationssicherheit kann in Bezug auf den Bereich der betrieblichen Informationsverarbeitung als Querschnittsaufgabe interpretiert werden [PoWe93, 16]. Die im Vorfeld bereits angesprochenen Tätigkeiten, wie etwa die Bestimmung eines Schutzziels oder die Bewertung des Schadensrisikos, sind im betrieblichen Kontext somit nicht isoliert, sondern als Teilaufgaben einer globalen Gestaltungsaufgabe anzusehen. Anhand des Konzeptes der betrieblichen Aufgabe ist dieser Sachverhalt zu verdeutlichen.

3.2.1. Das Konzept der betrieblichen Aufgabe

Unter einer betrieblichen Aufgabe kann eine Problemstellung verstanden werden, deren Lösung gegebene Anfangszustände in gewünschte Endzustände zielorientiert überführt [FeSi08, 60]. Im Rahmen der Beschreibung wird zwischen Außen- und Innensicht unterschieden.

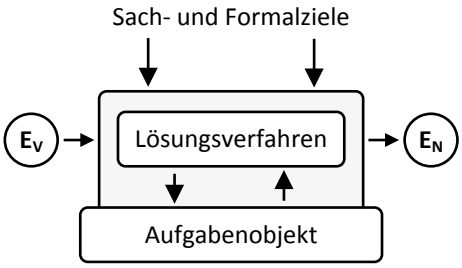

Abbildung 12: Struktur der betrieblichen Aufgabe

Die **Außensicht** einer Aufgabe umfasst die Zielsetzungen der Aufgabe, das Aufgabenobjekt sowie die Vor- und Nachereignisse (E_V, E_N), die eine Aufgabendurchführung auslösen bzw. die aus einer Durchführung resultieren. Sachziele bestimmen dabei den fachlichen Zweck einer Aufgabe, Formalziele die Art und Weise, wie eine Aufgabe durchzuführen ist. Das Aufgabenobjekt schließlich beschreibt den Gegenstandsbereich der Aufgabe [FeSi08, 96].

Aus **Innensicht** einer Aufgabe wird primär das Lösungsverfahren der Aufgabe beschrieben. Es besteht aus einer Menge von Aktionen, die auf das Aufgabenobjekt einwirken oder dessen Zustände erfassen, sowie einer Aktionensteuerung, die geeignete Aktionen zur Verfolgung der Sach- und Formalziele auslöst [Fers92, 6f]. Im Gegensatz zur Außensicht wird dabei Bezug genommen auf Typen von Aufgabenträgern, welche für die Durchführung der Aufgabe vorgesehen sind. Dieser Ansatz ermöglicht die Abstimmung der Beschreibung des Lösungsverfahrens auf personelle oder maschinelle Aufgabenträger [FeSi08, 97].

3.2.2. Aufgabencharakter betrieblicher Informationssicherheit

Die Schaffung von Informationssicherheit ist als komplexe Aufgabe einzustufen [Lip+92, 372], die in erster Näherung als Gesamtaufgabe eines Unternehmens zu verstehen ist und sukzessive in Teilaufgaben und deren Beziehungen untereinander zerlegt werden kann[20]. Den Ausgangspunkt einer solchen Zerlegung und Systematisierung von Teilaufgaben stellt in dieser Arbeit die Abbildung der vorgestellten Begriffssystematik der betrieblichen Informationssicherheit auf das Konzept der betrieblichen Aufgabe dar. Auf diese Weise wird sichergestellt, dass einerseits keine begrifflichen Mehrdeutigkeiten existieren, andererseits kann die resultierende Strukturierung des Begriffssystems als grundlegende Metapher für die weiteren Ausführungen Verwendung finden.

Ausgangspunkt der Verknüpfung bildet die Definition einer abstrakten Aufgabe mit der Zielsetzung „Herstellung und Aufrechterhaltung betrieblicher Informationssicherheit“. Gemäß den Ausführungen in Kapitel 3.1.1 entspricht das Bezugsobjekt somit dem betrieblichen Informationssystem, als organisatorischer Aufgabenträger kann etwa ein Bereich des Informationsmanagements[21] fungieren. Eine Verknüpfung des Begriffssystems betrieblicher Informationssicherheit mit dem Konzept der betrieblichen Aufgabe kann wie folgt durchgeführt werden.

Das Aufgabenobjekt einer betrieblichen Aufgabe wird übertragen auf das Begriffssystem der Sicherheit durch das **Bezugsobjekt** repräsentiert. Im Rahmen der betrieblichen Informationssicherheit wird dies durch die Elemente des betrieblichen Informationssystems dargestellt. Identifiziert werden können somit die informationsverarbeitenden Aufgaben eines betrieblichen Systems sowie die entsprechenden personellen und maschinellen Aufgabenträger.

Die Zielsetzungen der abstrakten Aufgabe werden durch **Sicherheitsziele** vorgegeben. Das globale Sachziel stellt dabei die Sicherheit des Assets Information dar. In Abhängigkeit von der Ausprägung des Bezugsobjektes entsprechen konkrete Sachziele dann den **Schutzzielen** der Informationssicherheit. Als Formalziele gelten neben allgemeinen betriebswirtschaftlichen Anforderungen auch rechtliche Vorgaben, wie sie zum Beispiel im Sarbanes Oxley Act (SOX) oder dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

---

[20] Diese Sichtweise korrespondiert mit der Bestimmung der Leistungsaufgaben eines betrieblichen Informationssystems, die aus einer abstrakten Gesamtaufgabe einer Organisation ableitbar sind [Sinz99b, 1050].

[21] Vgl. hierzu [FeSi08, 433].

definiert sind[22]. Vor allem durch letztere wird aus staatlicher Sicht der anzustrebende Zielerreichungsgrad der Sachziele in Unternehmen spezifiziert. Um die Beziehung zum Thema der Informationssicherheit zu verdeutlichen, werden Formalziele im weiteren Verlauf als **Sicherheitsvorgaben** bezeichnet. Der Begriff des Sicherheitsziels umfasst somit sachzielorientiert in Form von Schutzzielen sowie formalzielorientiert in Form von Sicherheitsvorgaben alle sicherheitsrelevanten Anforderungen im Rahmen einer Aufgabenstellung.

Als **Vorereignisse** für die Aufgabendurchführung kommen im Wesentlichen zwei Aspekte in Frage. Beide basieren auf dem Grad des Schadensrisikos, das, entweder intern oder extern motiviert, als auschlaggebender Faktor für die zielorientierte Durchführung fungiert. Zum einen kann der subjektiv empfundene Grad des Risikos einen bestimmten Schwellenwert erreichen, so dass ein Stakeholder die Notwendigkeit sieht den Schutzbedarf zu erhöhen. Oftmals tritt dieser Fall ein, wenn gravierende Verwundbarkeiten offenkundig und somit entsprechende Handlungen notwendig werden. Der zweite Fall bezieht sich auf die extern motivierte Veranlassung der Aufgabendurchführung, in der Regel angestoßen durch rechtliche Vorgaben. In dieser Interpretation nehmen Gesetze bzw. externe Auflagen somit eine Doppelbedeutung ein: Einerseits fungieren sie als Formalziele, andererseits können sie auch als Vorereignis für die Durchführung angesehen werden.

Ein **Nachereignis** wird in diesem Zusammenhang durch einen Zustand des betrieblichen Informationssystems repräsentiert, der aus risikoorientierter Sichtweise betrachtet ein im Ergebnis geringeres Schadensrisiko aufweist, als das diesbezüglich definierte Grenzrisiko.

Aufgabenobjekt, Zielsetzungen sowie Ereignisse verkörpern die Außensicht der globalen Aufgabe Informationssicherheit. Diese Sichtweise korrespondiert mit der in Kapitel 3.1.2 vorgestellten Abgrenzung von Teildisziplinen, die sich analog zu dieser Metapher anhand der unterschiedlichen Bezugsobjekte ableiten lassen.

Die Durchführung eines **Lösungsverfahrens** der globalen Aufgabe zielt darauf ab, einen gewünschten Zustand gemäß obiger Definition des Nachereignisses zu schaffen. Aus ergebnisorientierter Sicht betrachtet, werden durch die Aktionen eines solchen Vorgangstyps bestimmte Sicherheitsartefakte erzeugt, die auf das jeweilige Bezugsobjekt als Aufgabenobjekt einwirken. Die Realisierung dieser Sicherheitsartefakte bewirkt dann eine Zustandsänderung

[22] Eine Einführung in rechtliche Anforderungen und Regelungen gibt zum Beispiel [Spei07, 327ff].

der Bezugsobjekte, so dass ein Nachereignis entsprechend den Sachzielen der Aufgabendefinition erzeugt wird.

Die Spezifizierung der Aufgabeninnensicht mittels eines Lösungsverfahrens korrespondiert in dieser Sicht mit dem semantischen Netz der betrieblichen Informationssicherheit[23]. Die Ergebnisse des Lösungsverfahrens in Form von Sicherheitsartefakten reduzieren im Endergebnis für einen Stakeholder das konkrete, aufgabenobjektbezogene Risiko und sichern somit die gewünschte Zielerreichung im Hinblick auf die Umsetzung von Sicherheitszielen. Eine direkte Beziehung zwischen Sicherheitszielen und Risiko ist dabei jedoch nicht gegeben, da aus bereits angeführten Gründen ein Zielerreichungsgrad nicht operationalisierbar ist.

3.3. Dimensionen betrieblicher Informationssicherheit

Aus inhaltlicher Perspektive betrachtet, lassen sich Außen- und Innensicht der betrieblichen Informationssicherheit unmittelbar auf das Konzept der betrieblichen Aufgabe übertragen. Ausgehend von dieser Metapher sind verschiedene Perspektiven oder Dimensionen abzuleiten, anhand derer konkrete Inhalte der Informationssicherheit systematisch darstellbar sind[24]. Als Kernelemente können Ziele, Lösungsverfahren und Aufgabenobjekte, im Sinne der Informationssicherheit somit **Sicherheitsziele**, **Sicherheitsartefakte** und **Bezugsobjekte**, identifiziert werden. Jedes dieser Elemente definiert dabei eine Dimension, unter der die inhaltliche Ausgestaltung der Aufgabe Informationssicherheit zu betrachten ist.

[23] Vgl. hierzu Abbildung 10.

[24] Vgl. hierzu [Konr98, 20].

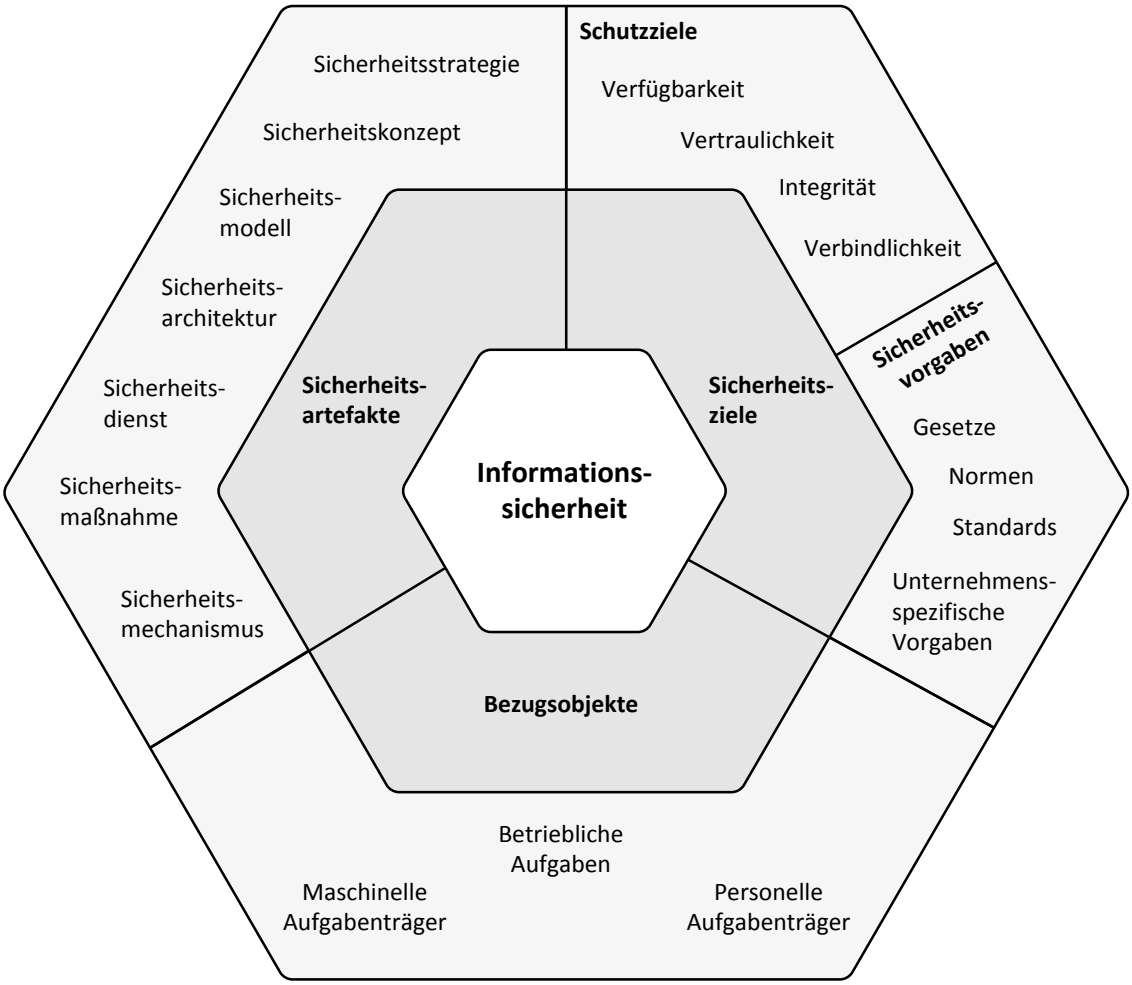

Abbildung 13: Dimensionen betrieblicher Informationssicherheit

Der äußere Bereich der Darstellung führt überblicksartig Elemente zu den drei angegebenen Dimensionen auf. Diese werden in Teil II der Arbeit weiter konkretisiert.

Es wird deutlich, dass der Begriff der betrieblichen Informationssicherheit inhaltlich deutlich weiter gefasst ist, als der in der Praxis häufig synonym verwendete Begriff der IT-Sicherheit. Sichtbar wird dies vor allem in der erweiterten Betrachtung der Sicherheitsziele und –artefakte, die sich nicht ausschließlich auf den technischen Bereich der Informationsverarbeitung beziehen.

Im betrieblichen Kontext kann die abstrakte Aufgabenspezifikation zur „Herstellung und Aufrechterhaltung betrieblicher Informationssicherheit" als **unternehmensweite Meta-Aufgabe** [Fers92, 4] betrachtet werden. Als Gestaltungsaufgabe ist sie im Rahmen organisatorischer Strukturen in der Regel dem Bereich des IT-Sicherheitsmanagements zugeordnet. Je nach unternehmensspezifischer Verankerung bzw. inhaltlicher Ausrichtung dieser Manage-

mentdisziplin sind somit unterschiedliche Teilaufgaben zu identifizieren, die im jeweiligen Kontext sinnvoll erscheinen. Um die Kernelemente der Aufgabe vollständig und vor allem unabhängig darzustellen, werden sie im folgenden Teil II der Arbeit anhand der dargestellten Dimensionen ohne Bezug auf konkrete Managementansätze analysiert. Dieses Vorgehen unterstützt zudem das Ziel der methodischen Erarbeitung eines Struktur- bzw. Referenzmodells der betrieblichen Informationssicherheit, anhand dessen entsprechende Ansätze der Sicherheitsmodellierung darstellbar sind.

Teil II

Struktur betrieblicher Informationssicherheit

Teil II der Arbeit bezieht sich auf die strukturorientierte Modellierung betrieblicher Informationssicherheit. Das Ziel bildet die Erarbeitung eines Modellierungsansatzes, der eine strukturierte und eindeutige Definition des Begriffsverständnisses der Informationssicherheit im Unternehmenskontext ermöglicht.

Kapitel 4 spezifiziert vor diesem Hintergrund die Meta-Ebene des Modellierungsansatzes. Kapitel 5 erläutert aus inhaltlicher Sicht die Schemaebene, indem es mögliche Extensionen der Meta-Objekttypen anhand eines methodischen Rahmens beschreibt. Kapitel 6 integriert die Inhalte der vorangehenden Kapitel durch die Vorstellung eines strukturorientierten Referenzmodells betrieblicher Informationssicherheit, anhand dessen grundlegende Ergebnisse als Grundlage für den dritten Teil der Arbeit erarbeitet werden können.

4. Strukturmodellierung betrieblicher Informationssicherheit

Die abstrakte Meta-Aufgabe zur Herstellung und Aufrechterhaltung betrieblicher Informationssicherheit ist auf Grund ihrer Komplexität für eine detaillierte Analyse in dieser Aggregationsstufe nicht geeignet. Um sicherheitsrelevante Teilaufgaben und deren Beziehungen sowie Anhängigkeiten zwischen Sicherheitszielen, Sicherheitsartefakten und Bezugsobjekten zu identifizieren, ist eine weitere Differenzierung durch eine sukzessive Zerlegung der Gesamtaufgabe durchzuführen. Dieses Vorgehen ermöglicht im Anschluss die Modellbildung betrieblicher Informationssicherheit, mit dem Ziel einer konsistenten und eindeutigen Integration der Meta-Aufgabe in die Strukturen der jeweiligen Organisationsform.

Kapitel 4.1 beschreibt einführend die Notwendigkeit und Inhalte der Modellbildung in Bezug auf die betriebliche Informationssicherheit. Kapitel 4.2 geht im Anschluss auf die Grundlagen zur Erstellung entsprechender Strukturmodelle der Informationssicherheit ein. In Kapitel 4.3 wird schließlich der diesbezügliche Modellierungsansatz der vorliegenden Arbeit vorgestellt.

4.1. Einführung

Die Erstellung von Modellen zur Beschreibung und Systematisierung eines Aufgabengebietes wird im Unternehmenskontext oftmals angewendet, um die Komplexität eines Sachverhaltes zu reduzieren. Im Hinblick auf die Informationssicherheit ist diese grundlegende Modellbildung jedoch stark subjektiven Einschätzungen unterworfen und orientiert sich oftmals an unternehmensintern definierten und gelebten Strukturen. Es entstehen somit unterschiedliche Zusammenhänge und Interpretationen zwischen den Begrifflichkeiten der allgemeinen Modellterminologie sowie, daraus resultierend, auch unterschiedliche Beziehungen zwischen den Teilaufgaben der Informationssicherheit. In Abhängigkeit von der Ausprägung dieses Bezugsrahmens sind somit unterschiedliche Vorgehensweisen und Ansätze realisierbar, die Meta-Aufgabe Informationssicherheit als Gestaltungsaufgabe zu interpretieren. Für eine umfassende Betrachtung der Informationssicherheit ist es daher ausschlaggebend, welches grundlegende Modell der Informationssicherheit Verwendung findet.

Zum Beispiel sieht MÜLLER das Sicherheitsartefakt „Sicherheitsarchitektur“ als „eine Art Baukasten von Sicherheitselementen“, konkret von Sicherheitsanforderungen, prinzipiellen

Bedrohungen und Sicherheitsstrategien sowie –prinzipien [Müll05, 141]. Er bezieht dieses Artefakt auf alle Elemente eines Unternehmens. ECKERT hingegen setzt die Sicherheitsarchitektur gleich mit der Sicherheitsinfrastruktur und sieht sie als den Bestandteil der Systemarchitektur, der die festgelegten Sicherheitseigenschaften durchsetzt und die relevanten Sicherheitsmaßnahmen zur Erbringung der Sicherheitsdienste zur Verfügung stellt [Ecke06, 30]. Sie bezieht dieses Artefakt somit auf konkrete betriebliche Anwendungssysteme. Es wird deutlich, dass mit der unterschiedlichen Begriffsauslegung des Sicherheitsartefakts Sicherheitsarchitektur verschiedene Bezugsobjekte einhergehen und somit auch unterschiedliche Lösungsverfahren zur Bearbeitung der Teilaufgabe „Definition einer Sicherheitsarchitektur“ resultieren.

Modellsystem betrieblicher Informationssicherheit

Um ein möglichst allgemeingültiges Verständnis der Informationssicherheit zu etablieren, wird in der vorliegenden Arbeit die Spezifikation eines grundlegenden Modellsystems der Informationssicherheit angestrebt.

Der grundlegende Ansatz basiert dabei auf der Analyse der aus der Zerlegung der globalen Meta-Aufgabe resultierenden Systematik von Teilaufgaben, die in Bezug auf die Informationssicherheit relevante Charakteristika aufweisen. Bestimmte Sicherheitsartefakte haben demnach ausschließlich auf bestimmte Bezugsobjekte sicherheitsrelevante Auswirkungen, ebenfalls stellen einzelne Sicherheitsziele auch nur für bestimmte Sicherheitsartefakte verwendbare Zielvorgaben dar.

Die Analyse der Meta-Aufgabe besteht dabei primär in der Zerlegung des Aufgabenobjekts und der Aufgabenziele sowie der Identifikation der Kommunikationskanäle zwischen den entstehenden Teilaufgaben [FeSi08, 231]. In Bezug auf die Informationssicherheit entstehen durch diesen Vorgang Tripel, bestehend aus spezifischen Ausprägungen der drei Dimensionen Sicherheitsziel, Sicherheitsartefakt und Bezugsobjekt. Jedes Tripel beschreibt dabei eine Teilaufgabe im gesamtbetrieblichen Kontext der Informationssicherheit, zum Beispiel die Spezifikation einer Sicherheitsarchitektur (Sicherheitsartefakt) für ein betriebliches Anwendungssystem (Bezugsobjekt) zur Sicherstellung der Vertraulichkeit (Schutzziel).

Die Beziehungen zwischen den Teilaufgaben definieren ein Netz aus sicherheitsbezogenen Aufgaben, die maßgeblich durch das entsprechend verwendete Lösungsverfahren zur Erstellung eines Sicherheitsartefakts charakterisiert werden. Es entsteht eine Systematik von (Teil-)

Aufgaben, die als Grundlage für die Betrachtungsweise und Interpretation der Informationssicherheit in Unternehmen und somit auch für entsprechende Vorgehensmodelle zu deren Durchsetzung ausschlaggebend ist. Diese Systematik wird in der vorliegenden Arbeit als **Modellsystem der Informationssicherheit** bezeichnet.

Strukturmodellbildung betrieblicher Informationssicherheit

Die Etablierung des Modellsystems hat zum Ziel, einen konsistenten methodischen Rahmen zu bilden, in dem unterschiedliche Schwerpunkte der Informationssicherheit unternehmensspezifisch abgebildet werden können. In der vorliegenden Arbeit folgt dieser Vorgang einer systemtheoretischen Ausrichtung, anhand derer ein abstraktes Gesamtsystem der betrieblicher Informationssicherheit sowohl aus struktureller als auch aus verhaltensorientierter Sichtweise betrachtet werden kann. Der Schwerpunkt der Ausführungen liegt hierbei auf der strukturellen Sicht, da diese für die notwendige Eindeutigkeit eines einheitlichen Begriffsverständnisses ausschlaggebend ist und somit indirekt die verhaltensorientierten Aspekte beeinflusst. Im Ergebnis wird die Definition eines **generischen Strukturmodells betrieblicher Informationssicherheit** angestrebt, anhand dessen eine unternehmensspezifische Analyse des Themengebiets erfolgen kann.

Ein generisches Strukturmodell der Informationssicherheit stellt ein Modellsystem der Informationssicherheit dar, indem es Bezugsobjekte, Sicherheitsartefakte und Sicherheitsziele anhand bestehender Konzepte systematisiert und in entsprechenden Ausprägungen zueinander in Beziehung setzt. Es bildet somit den angesprochenen methodischen Rahmen, anhand dessen bestimmte Aspekte der betrieblichen Informationssicherheit strukturiert werden können. Durch die resultierende Vergleichbarkeit entsprechender Ansätze wird potentiell erst dann ersichtlich, in welcher Weise Informationssicherheit in der jeweiligen Organisationsform ausgestaltet wird, bzw. noch auszugestalten ist. Die Strukturmodellbildung leistet somit einen grundlegenden Beitrag zur Eindeutigkeit des Verständnisses des Themenkomplexes der Informationssicherheit im unternehmerischen Kontext und bildet somit die Basis für eine wirksame und nachhaltige Durchführung entsprechender Lenkungs- und Leistungsaufgaben.

4.2. Grundlagen der Strukturmodellierung

Ein Strukturmodell der Informationssicherheit setzt die unterschiedlichen Elemente der betrieblichen Sicherheitsbetrachtung zueinander in Beziehung. Die Elemente ergeben sich dabei

aus den konzeptuellen Bestandteilen der Teilaufgaben, die durch die Zerlegung der Meta-Aufgabe der betrieblichen Informationssicherheit entstehen. Gesucht ist somit ein Konzept, das eine Modellierung der Komponenten Sicherheitsziel, Sicherheitsartefakt und Bezugsobjekt sowie deren Beziehungen zueinander ermöglicht.

Aus dieser Perspektive betrachtet, stellt das in Kapitel 4.1 angegebene Tripel aus Sicherheitsarchitektur, Anwendungssystem und Vertraulichkeit als Schutzziel einen Teilbereich eines Strukturmodells dar, der sich auf die Aufgabenträgerebene bezieht. Im Rahmen einer umfassenden Betrachtung der betrieblichen Informationssicherheit ist dieser Bereich zu ergänzen, zum Beispiel um entsprechende Elemente auf Geschäftsprozessebene. Es gilt somit, einen generischen **Modellierungsansatz** zu spezifizieren, anhand dessen spezifische Strukturmodelle der Informationssicherheit erstellt werden können. Der folgende Abschnitt führt in die diesbezüglichen Grundlagen der Modellierung ein.

4.2.1. Modelltheorie

Ein Modell kann allgemein als abstraktes und immaterielles Abbild eines Ausschnittes der Realität für die zweckorientierte Nutzung durch bestimmte Subjekte interpretiert werden [BeVo96, 19]. Unter einem Modell M wird ein 3-Tupel $M = (S_O, S_M, f)$ verstanden, bestehend aus einem Objektsystem S_O, einem Modellsystem S_M und einer Modellabbildung $f: V_O \rightarrow V_M$, die die Systemkomponenten V_O des Objektsystems auf die Systemkomponenten V_M des Modellsystems abbildet [FeSi08, 128].

Die Modellabbildung f kann in Bezug auf das vorliegende Objektsystem der Informationssicherheit nur informal spezifiziert werden, da es sich bei S_O nicht um ein formales System sondern vielmehr um einen Ausschnitt der betrieblichen Realität, die betriebliche Diskurswelt, handelt. Weiterhin unterliegt sie in hohem Maße der subjektiven Wahrnehmung eines Modellierers im Kontext der jeweiligen Organisation. Eine Modellbildung erfolgt vor diesem Hintergrund auf Basis eines konstruktivistischen Modellierungsverständnisses[25].

Um die Verwendung des Modells und dessen Nutzbarkeit trotz des hohen subjektiven Anteils zu gewährleisten, ist es relevant, die subjektiven Einflüsse zu begrenzen bzw. für Dritte sicht-

[25] Der Modellierer steht nach diesem Verständnis in einer Kontextbeziehung zu dem zu modellierenden Objektsystem. In diesem Kontext perzipiert er die Realität, grenzt das Objektsystem somit implizit davon ab und interpretiert es aus subjektiver Sicht. Basierend auf dieser Interpretation und den Modellierungszielen erfolgt dann die Konstruktion des Modellsystems. Vgl. hierzu [Hamm99, 27f] oder [Schl04, 34ff].

bar und nachvollziehbar zu machen. Wichtige konzeptuelle Hilfsmittel sind diesbezüglich Meta-Modelle und Metaphern. Zusammen beschreiben diese Konzepte den zu nutzenden **Modellierungsansatz** als Beschreibungsrahmen, der die Sichtweise des Modellierers auf Objektsystem und Modellsystem sowie das zur Spezifikation verwendete Begriffssystem festlegt [FeSi08, S.130f].

Metapher

Eine Metapher dient in diesem Zusammenhang als sprachlicher Ausdruck zur Beschreibung der Sichtweise, die ein Modellierer bei der Erfassung des Objektsystems zu Grunde legt und auf die Spezifikation des Modellsystems überträgt.

Meta-Modell

Ein Meta-Modell legt in Abstimmung mit der verwendeten Metapher das zur Spezifikation des Modellsystems verwendete Begriffssystem fest. Es definiert die verfügbaren Arten von Modellbausteinen, die Arten von Beziehungen zwischen diesen Modellbausteinen, sowie die Regeln für die Verknüpfung von Modellbausteinen durch Beziehungen [FeSi08, 132]. Ein Meta-Modell kann als dem eigentlichen Modellsystem hierarchisch übergeordnet betrachtet werden und spezifiziert somit das Spektrum an Darstellungsmöglichkeiten für die Modellsysteme [Lehn95, 85]. Es stellt somit eine Typdefinition für eine Klasse von Modellsystemen dar [Sinz96, 126], deren Instanzen dann wiederum als Extension ihres zugehörigen Meta-Modells zu interpretieren sind. Durch die Verwendung von Meta-Modellen kann zum einen die Konsistenz und Vollständigkeit des Modellsystems verifiziert werden, zum anderen werden die Struktur- und Verhaltenstreue des Modellsystems in Bezug auf das Objektsystem überprüfbar [FeSi08, 132].

Meta-Meta-Modell

Für die Spezifikation des zu verwendenden Meta-Modells der Informationssicherheit ist analog zur Spezifikation des Modellsystems ebenfalls ein Begriffssystem notwendig, das dem Meta-Modell hierarchisch übergeordnet ist. Dieser einheitliche Beschreibungsrahmen für Meta-Modelle wird als Meta-Meta-Modell bezeichnet. Als Grundlage für die vorliegende Arbeit findet das von SINZ eingeführte Meta-Meta-Modell Verwendung [Sinz96, 129].

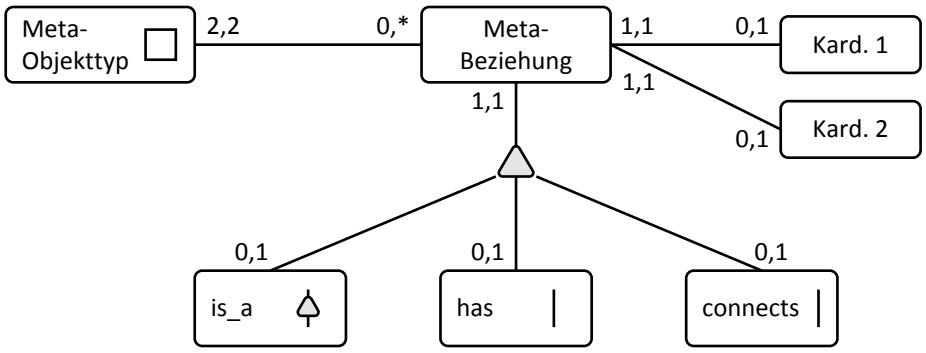

Abbildung 14: Meta-Meta-Modell nach SINZ ([FeSi08, 133])

Als Bausteine des Meta-Meta-Modells kommen **Meta-Objekttypen** (Symbol Rechteck) zum Einsatz, die durch **Meta-Beziehungen** (Symbol Kante) verbunden sind. Meta-Beziehungen sind dabei von Typ Generalisierungsbeziehung (is_a), Assoziationsbeziehung (connects) sowie Attribut-Zuordnungsbeziehung (has). Jede Meta-Beziehung kann mit referentiellen Integritätsbedingungen durch zwei Kardinalitäten in (min,max)-Notation versehen werden. Die hierarchische Ordnung zwischen Meta-Meta-Modell und Meta-Modell korrespondiert mit entsprechenden Metaebenen der Modellierung. Jede Spezifikation einer Ebene i stellt dabei eine Extension der Spezifikation der nächsthöheren Ebene (i+1) dar. Die Extension eines Meta-Modells wird als **Schema** eines Modellsystems bezeichnet, dessen Extension wiederum als **Ausprägung** eines Modellsystems [FeSi08, 133].

4.2.2. Modellbildung

Im Rahmen der vorliegenden Arbeit wird ein Modellierungsansatz vorgestellt, der durch die Spezifikation eines Meta-Modells auf der Grundlage des Meta-Meta-Modells nach SINZ bestimmt wird. Eine Extension dieses Meta-Modells stellt dann ein Strukturmodell der betrieblichen Informationssicherheit dar, das die entsprechenden Komponenten des Themenbereichs gemäß der jeweiligen Interpretation des Modellierers aufzeigt.

Im folgenden Kapitel werden das entsprechende Meta-Modell sowie die grundlegende Metapher des Modellierungsansatzes vorgestellt. Es beschreibt damit die Meta-Ebene der Modellierung und dient als Grundlage für die in Kapitel 5 durchzuführende Betrachtung der entsprechenden Schemaebene.

4.3. Ein Ansatz zur Strukturmodellierung betrieblicher Informationssicherheit

Die Darstellung des Modellierungsansatzes erfolgt anhand einer zu Grunde liegenden Metapher sowie eines entsprechenden Meta-Modells.

4.3.1. Metapher des Modellierungsansatzes

Als grundlegende Metapher fungiert die bereits in Kapitel 3.2 definierte Sichtweise der Informationssicherheit als betriebliche Aufgabe. Informationssicherheit wird in Bezug auf die Modellierung somit nicht als statische Eigenschaft einer Unternehmung oder eines Anwendungssystems interpretiert, sondern vielmehr aufgabenorientiert als kontinuierlicher Prozess [Ecke06, 5]. Aus dieser Perspektive ergibt sich die Ausrichtung des Modellierungsansatzes auf die Komponenten der betrieblichen Aufgabe, die sich aus deren Außen- und Innensicht ableiten lassen.

4.3.2. Meta-Modell des Modellierungsansatzes

Anhand der gewählten Metapher können die Objekttypen des **Meta-Modells** der betrieblichen Informationssicherheit spezifiziert werden. Sie korrespondieren mit den in Kapitel 3.3 vorgestellten Dimensionen der Informationssicherheit und werden dementsprechend als Meta-Objekttypen **Sicherheitsziel**, **Sicherheitsartefakt** und **Bezugsobjekt** erfasst. Die nachfolgende Darstellung des Meta-Modells folgt dem Meta-Meta-Modell nach SINZ, zu dem es eine gültige Extension darstellt.

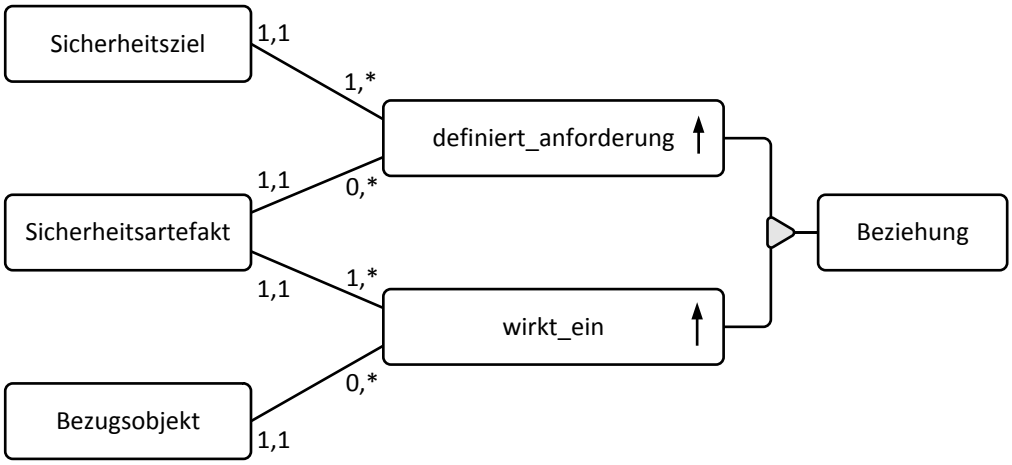

Abbildung 15: Meta-Modell betrieblicher Informationssicherheit

Die spezifizierten Beziehungen zwischen den drei Meta-Objekttypen, definiert_anforderung und wirkt_ein, sind als Spezialisierungen eines gerichteten Beziehungsobjekttyps anzusehen.

Bezugsobjekte der Informationssicherheit sind abzuleiten aus den unternehmensspezifischen Elementen der betrieblichen Realität. Als methodischer Rahmen zur Unterstützung dieser Aktivität kommt das Konstrukt der Unternehmensarchitektur der SOM-Methodik zum Einsatz. In Kapitel 5.2 werden die entsprechenden Ausprägungen im Detail erläutert.

Sicherheitsziele bzw. deren Definition bewirken die Realisierung von Sicherheitsartefakten. Untereinander können sie in Wirkungs- und Abhängigkeitsbeziehungen stehen, die wiederum Auswirkungen auf die Sicherung der Konsistenz von erstellten Modellschemata haben. Sicherheitsziele werden in Kapitel 5.4 näher betrachtet.

Sicherheitsartefakte beziehen sich auf mindestens ein oder mehrere Bezugsobjekte und stehen untereinander ebenfalls in Beziehung. In der Regel sind dies Ableitungs- oder Umsetzungsbeziehungen, die eine hierarchische Gliederung der Sicherheitsartefakte vorgeben. Eine inhaltliche Beschreibung der Sicherheitsartefakte erfolgt in Kapitel 5.3.

Der Beziehungstyp **definiert_anfoderung** verbindet die beiden Meta-Objekttypen Sicherheitsziel und Sicherheitsartefakt. Die Semantik dieser Relation besteht dabei aus der Zielvorgabe, die durch die Spezifikation von Sicherheitszielen an die zu etablierenden Sicherheitsartefakte gestellt wird. Die angegebenen Kardinalitäten besagen, dass kein Sicherheitsziel ohne Bezug zu einem Sicherheitsartefakt modelliert werden darf. Sicherheitsartefakte hingegen können ohne definierte Sicherheitsziele im Modell dargestellt werden.

Eine **wirkt_ein**-Beziehung verbindet den Meta-Objekttyp Sicherheitsartefakt mit einem Bezugsobjekt. Inhaltlich stellt diese Beziehung die sicherheitsrelevanten Auswirkungen auf ein Bezugsobjekt bzw. dessen Zustand dar, die durch die Realisierung eines Sicherheitsartefakts entstehen. Ein Sicherheitsartefakt muss dabei mindestens mit einem Bezugsobjekt verbunden sein, Bezugsobjekte können jedoch auch ohne zugeordnete Sicherheitsartefakte modelliert werden. Der Meta-Objekttyp Bezugsobjekt beinhaltet in dieser Sichtweise assoziierte Verwundbarkeiten, auf die sich Sicherheitsartefakte in der Innensicht der betrieblichen Informationssicherheit beziehen, die jedoch nicht explizit modelliert werden. Dies erfolgt zum einen aus Komplexitätsgründen, zum anderen erscheint eine Modellierung von Verwundbarkeiten im Rahmen eines Strukturmodells nicht zielführend. Da Verwundbarkeiten als Attribute eines Bezugsobjektes interpretierbar sind, ist dieser Ansatz im Rahmen der Metapher zulässig.

Im Meta-Modell weiterhin nicht explizit berücksichtigt, und damit auf Schemaebene nicht darstellbar, sind die internen Abhängigkeits- und Wirkungsbeziehungen zwischen einzelnen Schutzzielen sowie zwischen Bezugsobjekten oder Sicherheitsartefakten. Der Grund hierfür liegt darin, dass, analog zur voranstehenden Argumentation, durch eine Modellierung dieser Beziehungen die Komplexität resultierender Strukturmodelle unnötig erhöht wird. Von dem eigentlichen Ziel der Modellbildung betrieblicher Informationssicherheit würde somit zu stark abgelenkt werden.

4.3.3. Anwendung des Modellierungsansatzes

Ein Strukturmodell ermöglicht die individuelle Definition der unternehmensspezifischen Sichtweise auf die Informationssicherheit. Dies erfolgt durch die Spezifikation der Schemaebene des Modellierungsansatzes, in der die jeweils sicherheitsrelevanten Modellelemente als Extension der Meta-Objekttypen dargestellt werden. Dabei ist zu entscheiden, welche Bezugsobjekte in dem jeweiligen unternehmerischen Kontext zum einen vorhanden und zum anderen auch als sicherheitsrelevant erachtet werden. Darauf aufbauend sind die entsprechenden Sicherheitsartefakte zu definieren, die aus Unternehmenssicht auf Grund der jeweiligen Sicherheitsziele umzusetzen sind.

Konzept der modellgestützten Untersuchungssituation

Als methodischer Rahmen für die Modellbildung fungiert das Konzept der modellgestützten Untersuchungssituation nach FERSTL [Fers79, 79ff]. Hiernach wird die Findung eines Untersuchungsergebnisses durch die Komposition eines Originalproblems mit einem geeigneten Modellproblem unterstützt.

Ein allgemeines Untersuchungsproblem besteht dabei aus dem Untersuchungsobjekt und den entsprechenden Untersuchungszielen. Durch die Anwendung eines Untersuchungsverfahrens werden auf dieser Basis Untersuchungsergebnisse erzeugt [Fers79, 43][26]. Um Untersuchungssituationen, in denen in erster Näherung keine Untersuchungsverfahren zu Verfügung stehen, bearbeiten zu können, wird ein Ansatz zur **Transformation der Untersuchungssituation** verwendet. Dabei wird die Originalebene durch eine Transformation der Untersuchungsziele

[26] Anhand der Eigenschaften des Untersuchungsobjektes S können unterschiedliche Typen von Untersuchungsproblemen identifiziert werden, zum Beispiel Konstruktions- oder Analyseprobleme. Eine detaillierte Übersicht hierzu gibt [Fers79, 44ff].

sowie durch die Konstruktion von Modellsystemen des Bezugsobjektes auf eine Modellebene abgebildet. Auf dieser Ebene erfolgt dann die Erzeugung des Untersuchungsergebnisses, das dann als Lösung wiederum auf das Originalproblem zurücktransformiert wird. Die beiden Teilprobleme auf Originalebene und Modellebene werden hierbei durch Abbildungsbeziehungen verknüpft [Fers79, 79f].

Anwendung auf den Bereich der Informationssicherheit

Das abzubildende Originalproblem kann im vorliegenden Kontext als die Frage nach sicherheitsrelevanten Bezugsobjekten im Unternehmen sowie deren Systematisierung und Berücksichtigung durch sicherheitserzeugende Maßnahmen beschrieben werden. Es entspricht somit inhaltlich der Meta-Aufgabe zur Schaffung betrieblicher Informationssicherheit. Das Untersuchungsobjekt stellt dabei die Systematik der Komponenten betrieblicher Informationssicherheit dar. Als Untersuchungsziel dient die Spezifikation der Struktur dieser Systematik sowie im weiteren Verlauf das darauf basierende Verhalten des betrieblichen Systems in Bezug auf die Lenkungs- und Leistungsaufgaben der Informationssicherheit.

Durch die Nutzung des Modellierungsansatzes wird ein Strukturmodell der Informationssicherheit konstruiert, dass als Repräsentation des Untersuchungsobjekts fungiert. Anhand dieses Modells sind unternehmensspezifisch entsprechende Analysen im Rahmen des Untersuchungsverfahrens durchzuführen. Als Untersuchungsergebnis kann dann zum Beispiel die Identifikation konkreter Maßnahmen gewertet werden, die hinsichtlich der Umsetzung auf die Originalebene abzubilden sind. Die angesprochenen Abbildungsbeziehungen zwischen Original- und Modellebene werden dabei durch den vorgestellten Modellierungsansatz bestimmt. Hierbei ist insbesondere die genutzte aufgabenorientierte Metapher ausschlaggebend für die Konstruktion des zu verwendenden Modellsystems.

Die Ausprägungen der Meta-Objekttypen, als resultierende Modellelemente des Strukturmodells auf Schemaebene, werden im folgenden Kapitel 5 im Detail beschrieben. Im Anschluss erfolgt in Kapitel 6 mit der Darstellung eines generischen Strukturmodells betrieblicher Informationssicherheit als Referenzmodell der Abschluss des zweiten Teils der Arbeit.

5. Schemaebene der Strukturmodellierung

Auf Basis des vorgestellten Modellierungsansatzes können auf Schemaebene Strukturmodelle betrieblicher Informationssicherheit erstellt werden. Um konkrete Objekttypen als Extension der Meta-Objekttypen identifizieren zu können, ist im Vorfeld ein methodischer Rahmen zu definieren, der die, dem jeweiligen Verständnis folgend, verfügbaren Objekttypen strukturiert.

Vor diesem Hintergrund wird in Kapitel 5.1 ein diesbezüglicher Beschreibungsrahmen definiert, dessen Elemente in den folgenden Kapiteln im Detail vorgestellt werden. Bezugsobjekte der Informationssicherheit werden in Kapitel 5.2 besprochen, Sicherheitsartefakte in Kapitel 5.3 sowie Sicherheitsziele in Kapitel 5.4. Kapitel 5.5 beschließt die Beschreibung der Schemaebene der Modellierung anhand der Beschreibung technischer Sicherheitsmechanismen, die auf der Basis von Sicherheitsgrundfunktionen systematisiert werden.

5.1. Systematisierung der Schemaebene

Für die Meta-Objekttypen des Modellierungsansatzes sind auf Schemaebene die jeweiligen Extensionen zu spezifizieren, die für die Erstellung eines Strukturmodells genutzt werden können. Deren Identifikation ist jedoch wiederum abhängig von dem etablierten Begriffsverständnis der Informationssicherheit im Unternehmen sowie von vorhandenem Expertenwissen in diesem Bereich. Beide Aspekte sind nicht notwendigerweise in gewünschter Art und Weise verfügbar, sodass eine umfassende Betrachtung der verfügbaren Objekttypen nicht möglich ist. In der vorliegenden Arbeit wird aus diesem Grund die Nutzung eines methodischen Rahmens vorgeschlagen, anhand dessen die Extensionen der Meta-Objekttypen systematisch identifiziert und dargestellt werden können. Zum Einsatz kommt hierbei die Unternehmensarchitektur des Semantischen Objektmodells, die im folgenden Kapitel als zentraler Bezugsrahmen eingeführt wird.

5.1.1. Unternehmensarchitektur von SOM

Die SOM-Methodik ist eine geschäftsprozess- und objektorientierte Modellierungsmethodik für betriebliche Systeme sowie zur fachlichen Spezifikation von Anwendungssystemen [Schm01, 48]. Unter dem Begriff Methodik wird in diesem Zusammenhang das Tripel aus Modellierungsansatz, Unternehmensarchitektur und Vorgehensmodell verstanden, durch das

eine umfassende Modellierung betrieblicher Systeme ermöglicht wird [FeSi08, 192]. Relevant für die aktuelle Argumentation ist die SOM-Komponente der Unternehmensarchitektur, die eine Strukturierung des betrieblichen Modellsystems vorgibt. Hierzu wird das Modellsystem in Teilmodellsysteme unterteilt, die das Objektsystem jeweils unter einem bestimmten Blickwinkel beschreiben. Die in SOM verwendeten Teilmodellsysteme **Unternehmensplan**, **Geschäftsprozessmodell** und **Ressourcenmodell** sind mit ihren Beziehungen jeweils einer Betrachtungsebene zugeordnet und bilden in der Gesamtheit den Architekturrahmen[27] der Methodik.

Ebene 1 - Unternehmensplan

Der Unternehmensplan bildet das Teilmodellsystem eines betrieblichen Systems aus der Außenperspektive. Die grundlegende Metapher folgt der einer globalen Unternehmensaufgabe, die anhand ihrer Ziele sowie ihres Aufgabenobjekts, definiert durch die Abgrenzung von Diskurs- und Umwelt, beschrieben wird. Ergänzt werden diese Aspekte durch die Berücksichtigung der Leistungsbeziehungen zwischen Diskurswelt und Umwelt sowie durch die Betrachtung der zur Durchführung der Aufgaben notwendigen Ressourcen. Relevante Rahmenbedingungen des wirtschaftlichen Handelns sowie verfolgte bzw. zu verfolgende Strategien zur Umsetzung der Unternehmensaufgabe werden ebenfalls auf dieser Modellebene spezifiziert [FeSi08, 193].

Ebene 2 - Geschäftsprozessmodell

Geschäftsprozessmodelle repräsentieren als Teilmodellsystem die Innenperspektive eines betrieblichen Systems. Aus aufgabenorientierter Sicht können sie als Lösungsverfahren für die Umsetzung des Teilmodellsystems auf Ebene 1 interpretiert werden. Sie beschreiben das Aufgabensystem eines Unternehmens sowie die durch die beinhalteten Aufgaben zu erbringenden Leistungen. Geschäftsprozessmodelle bilden die zentrale Ebene der SOM-Methodik und stellen das Bindeglied zwischen Unternehmensplan und Ressourcenmodell dar [FeSi95b, 2f].

Ebene 3 – Ressourcenmodell

Das Ressourcenmodell beschreibt die Innenperspektive eines betrieblichen Systems auf Aufgabenträgerebene. Es werden Personal, Anwendungssysteme sowie Maschinen und Anlagen

[27] Vgl. hierzu das Konzept des generischen Architekturrahmens in [Sinz99a, 1036].

als Aufgabenträger zur Durchführung von Geschäftsprozessen differenziert. Personelle Aufgabenträger werden in Form einer Spezifikation der Aufbauorganisation modelliert, maschinelle Aufgabenträger anhand technischer Systemspezifikationen [FeSi08, 194]. Für das Fachgebiet der Informationsverarbeitung ist vor allem der Bereich der maschinellen Aufgabenträger, insbesondere der betrieblicher Anwendungssysteme von Interesse und findet im Rahmen der Modellbildung des SOM-Ansatzes Berücksichtigung.

5.1.2. Ein Beschreibungsrahmen der Schemaebene

Auf Basis des Architekturrahmens können die Meta-Objekte der Strukturmodellbildung betrieblicher Informationssicherheit anhand der vorgestellten Ebenen differenziert betrachtet werden. Für jeden Meta-Objekttyp ist dabei zu prüfen, ob auf der jeweiligen Architekturebene entsprechende Objekttypen der Schemaebene des Strukturmodells vorhanden sind. Dieses Vorgehen kann durch die folgende Matrix dargestellt werden.

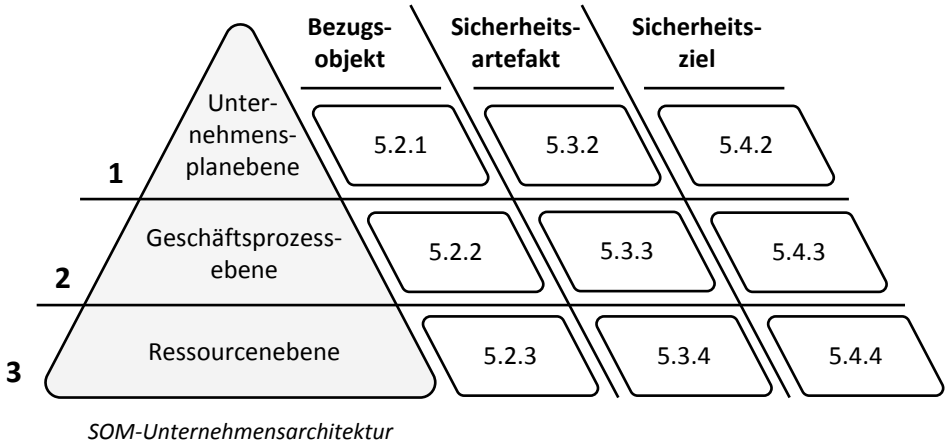

Abbildung 16: Beschreibungsrahmen der Schemaebene

Die Meta-Objekttypen Bezugsobjekt, Sicherheitsartefakt und Sicherheitsziel werden in der Matrix zu den Betrachtungsebenen des methodischen Rahmens in Beziehung gesetzt. Jedes Feld der Matrix symbolisiert dabei die Ausprägungen des jeweiligen Meta-Objekttypen auf der Schemaebene der Modellierung. Auf diese Weise wird ein Ansatz geschaffen, der nicht nur eine methodische Herangehensweise an die Modellierung der Informationssicherheit ermöglicht, sondern auch einen grundlegenden Mechanismus bereitstellt, um neue Entwicklung im Bereich der Informationssicherheit zu strukturieren und einzugliedern.

Im Falle der Bezugsobjekte erfolgt die Identifikation und Beschreibung der Modellelemente auf der Grundlage der Inhalte der Unternehmensarchitektur. Sicherheitsartefakte und Sicherheitsziele werden auf Basis grundlegender Erkenntnisse des Forschungsbereichs vorgestellt bzw. in Bezug auf die Modellbildung betrieblicher Informationssicherheit neu erarbeitet. Letzteres bezieht sich insbesondere auf die Ebene der Geschäftsprozesse und Ressourcen, für die im dritten Teil der Arbeit entsprechende Sicherheitsartefakte vorgestellt werden.

Im weiteren Verlauf dieses Kapitels werden die entsprechenden Objekttypen der Modellierung abgeleitet und inhaltlich vorgestellt. Kapitel 5.2 beschreibt die Bezugsobjekte der Informationssicherheit, Kapitel 5.3 die Sicherheitsartefakte und Kapitel 5.4 schließlich die Sicherheitsziele. Zur besseren Orientierung sind in den Feldern der Matrix in Abbildung 16 die entsprechenden Kapitelnummern hinterlegt. Am Ende eines jeden Teilkapitels werden die Ausführungen zudem jeweils in einer eigenen Systematik zusammengefasst.

5.2. Bezugsobjekte der Informationssicherheit

Basierend auf der Unternehmensarchitektur der SOM-Methodik werden im folgenden Abschnitt Bezugsobjekte der betrieblichen Informationssicherheit identifiziert und systematisiert. Ausgangspunkt des Vorgangs stellen die Beschreibungen bzw. Meta-Modelle des Semantischen Objektmodells auf den jeweiligen Ebenen dar.

5.2.1. Bezugsobjekte auf Ebene des Unternehmensplans

Auf Ebene des Unternehmensplans werden im SOM-Ansatz Objektsystem und Zielsystem in informaler Darstellung modelliert. Um Bezugsobjekte der betrieblichen Informationssicherheit zu identifizieren erfolgt im folgenden Abschnitt eine Analyse dieser Teilmodellsysteme aus betriebswirtschaftlicher Sicht. Als Bezugsrahmen dient hierbei eine Systematik von HAHN [Hahn06], die sich inhaltlich an dem St. Galler Management-Konzept[28] orientiert. Es werden potentiell relevante Bezugsobjekte identifiziert und abschließend hinsichtlich ihrer Eignung als Ansatzpunkt für betriebliche Informationssicherheit diskutiert.

[28] Vgl. hierzu [Blei04].

5.2.1.1. Elemente des Unternehmensplans

Die Erstellung des Teilmodellsystems Unternehmensplan ist aus betriebswirtschaftlicher Sicht Gegenstand der strategischen Unternehmensplanung [Schm01, 51]. Die **strategische Planung** kann als Prozess interpretiert werden, der Entscheidungen vorbereitet und darauf abzielt, bestehende Strategien zu bestätigen, zu verändern oder neue Strategien zu entwerfen [Krei87, 5]. Ihre Hauptaufgabe besteht darin, technisch-wirtschaftliche, politische, ökologische und gesellschaftliche Veränderungen der Unternehmensumwelt zu erkennen und unter deren Berücksichtigung zukünftige und erfolgversprechende Tätigkeitsfelder zielorientiert zu bestimmen [Dick07, 27]. Zusammen mit den Teildisziplinen der Strategieimplementierung und strategischen Kontrolle bildet die strategische Planung die Hauptaufgaben des **strategischen Managements** [Voig08, 39f].

Der Aufgabenbereich des strategischen Managements ist in der Makrosicht dem **strategischen Lenkungssystem** zuzuordnen. Unter Lenkung wird dabei die permanente, zyklische Abfolge von Tätigkeiten der Planung, Steuerung und Kontrolle verstanden [FeSi08, 2]. Die Teildisziplin der **strategischen Planung** kann, eingebettet in den Kontext des Planungssystems eines Unternehmens, zwischen der unternehmensweiten **generellen Zielplanung** und der **operativen Planung** eingeordnet werden [Hahn06, 33].

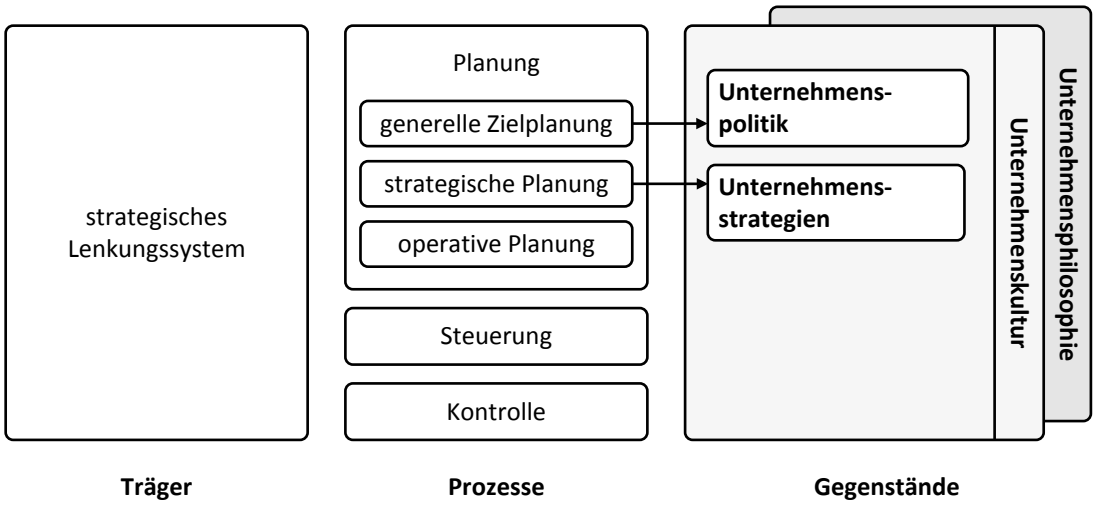

Abbildung 17: Strategisches Management nach HAHN ([Hahn06, 34])

HAHN differenziert in seiner Systematik der strategischen Unternehmensführung **Träger**, **Prozesse** und **Gegenstände**. Insbesondere die Elemente des Bereichs Gegenstände sind im

Rahmen der Identifikation von Bezugsobjekten der betrieblichen Informationssicherheit von Interesse.

Im Rahmen der generellen Zielplanung werden die qualitativ und quantitativ formulierten Ziele für die globale **Unternehmenspolitik** definiert. Sie bilden als Teilbereich der Unternehmenskultur den Ausgangspunkt für die strategische Unternehmensplanung, welche die **Strategien** für eine langfristige Tätigkeitsfeld-und Geschäftsfeldplanung formuliert. Die operative Planung definiert im Anschluss gemäß der definierten Strategien die Ziel- und Maßnahmenplanung in den einzelnen Geschäftsbereichen [Dick07, 28ff]. HAHN sieht diese Gegenstände vor dem Hintergrund der **Unternehmensphilosophie** und **Unternehmenskultur**, die in Form von Werten und Normen die entsprechende Grundlage des strategischen Managements darstellen.

Da das Teilmodellsystem Unternehmensplan des SOM-Ansatzes unter dem Blickwinkel einer globalen Unternehmenssicht gebildet wird, wird der Bereich der operativen Planung auf Grund seines Bezugs zu einzelnen Geschäftsbereichen im Folgenden nicht näher betrachtet. Die anderen spezifizierten Gegenstände werden in den folgenden Abschnitten beschrieben und im Anschluss im Hinblick auf das Themengebiet der betrieblichen Informationssicherheit analysiert.

Unternehmensziele / Unternehmenspolitik

Als Unternehmenspolitik wird die Gesamtheit der Festlegungen bezeichnet, welche die langfristigen Ziele des Unternehmens sowie sein Verhalten nach innen und außen determiniert. Die Unternehmenspolitik sollte allgemeingültige, klare und auf das Wesentliche beschränkte Aussagen beinhalten, die möglichst realistisch und operationalisierbar sind [DoSc05, 346f].

Unternehmenspolitische Ziele sind inhaltlich differenzierbar in die Kategorien Sach- und Formalziele. Als **Sachziele** gelten gemeinhin:

- Leistungsziele (Markt- und Produktziele)
- Finanzziele (angestrebte Vermögens- oder Kapitalstrukturen, Liquiditätsziele)
- Führungs- und Organisationsziele (angestrebte Führungs- oder Organisationsstrukturen)
- Soziale und ökologische Ziele (mitarbeiter- und gesellschaftsbezogene Ziele).

Formalziele hingegen beziehen sich primär auf den Erfolg der betrieblichen Tätigkeit, insbesondere auf die Art und Weise, wie ein optimaler Einsatz von Produktionsfaktoren im Rahmen ökonomischer Prinzipien erfolgen kann. Kennzahlen wie Produktivität, Wirtschaftlichkeit sowie Rentabilität und Gewinn sind dieser Kategorie zuzuordnen [ThAc06, 105ff].

Das sich ergebende Zielsystem aus Sach- und Formalzielen eines Unternehmens bildet schließlich die Grundlage für die Entwicklung und Umsetzung von Unternehmensstrategien.

Unternehmensstrategien

Abstrakt betrachtet bilden Strategien grundsätzliche Vorgehensweisen zur Gestaltung von Richtung, Ausmaß, Struktur und Trägern der Unternehmungsentwicklung, wobei in der Regel von bereits formulierten unternehmungspolitischen Zielen ausgegangen wird [Hahn06, 33]. Die Verwendung des Strategiebegriffs in der Betriebswirtschaftslehre ist als sehr vielfältig zu charakterisieren, insbesondere der Umfang der von ihm abgedeckten Aspekte wird oftmals unterschiedlich bewertet. Anhand ihrer Reichweite bzw. unternehmensspezifischer Bezugselemente können Strategien abstrakt in die drei Typen Unternehmensstrategie, Geschäftsfeldstrategie und Funktionsstrategie unterteilt werden [Voig08, 41f].

Unternehmensstrategien betreffen das Unternehmen als Ganzes und definieren, in welche Richtung sich eine Organisation mittel- bis langfristig entwickelt. **Geschäftsfeldstrategien** beziehen sich auf konkrete Geschäftsbereiche und machen bereichsspezifische Vorgaben, auf welche Weise entsprechende Beiträge zur Erreichung der Unternehmensziele erbracht werden. Als Beispiel können Produkt/Markt-Strategien nach ANSOFF [Anso66, 132] oder Wettbewerbsstrategien nach PORTER [Port98] angeführt werden. **Funktionsstrategien** beziehen sich auf bestimmte Funktionsbereiche eines Unternehmens, wie zum Beispiel Produktions-, IT- oder Vertriebsstrategien und bündeln diesbezügliche Entscheidungen.

Zwischen den Strategietypen existieren vielfältige Abhängigkeiten und Wechselbeziehungen. So definiert etwa die Unternehmensstrategie einerseits Vorgaben für die Geschäftsfeld- und Funktionsstrategien, muss andererseits aber auch durch Einflüsse aus den Geschäftsfeldern bzw. Funktionsbereichen abänderbar sein [Voig08, 42].

Unternehmensphilosophie und -kultur

Die Festlegung von globalen Unternehmenszielen und somit auch von Strategien, erfolgt auf Basis von gemeinsamen bzw. abgestimmten Werten der obersten Willensbildungszentren

eines Unternehmens, wie etwa dem Vorstand oder dem Aufsichtsrat [Hahn06, 33]. Diese Werte sind als Summe der ethischen und moralischen Leitmaximen einer Unternehmung anzusehen, die unter dem Begriff der **Unternehmensphilosophie** ein Orientierungsmuster für die Lenkung und Entwicklung eines Unternehmens bilden [Hopf00, 759].

Die Unternehmensphilosophie bildet zugleich die Grundlage für die Entwicklung der **Unternehmenskultur**, welche die unternehmungsgeschichtlich gewachsenen, gelebten und zumindest partiell gestaltbaren Denk-, Entscheidungs- und Verhaltensmuster der Mitarbeiter einer Unternehmung bezeichnet. Sie wird primär durch die Werthaltungen der obersten Führungskräfte geprägt und kommt in spezifischen Erscheinungsformen wie etwa Normen oder auch Symbolen zum Ausdruck [Hahn06, 35][29]. Ziel der Unternehmenskultur ist es, eine möglichst hohe Gleichorientierung zwischen den Interessen des Unternehmens und denen der Mitarbeiter zu schaffen. Dies wird erreicht, indem aus den verhaltenssteuerenden Wertvorstellungen Normen bestimmt werden, die gewisse Verhaltenserwartungen an Mitarbeiter definieren. Normen wiederum konkretisieren sich in Symbolen, wie etwa Gegenstände (Büroeinrichtung, Kleidung), ritualisierte Verhaltensweisen (Kundenumgang, Sitzungsablauf) oder Formen der Sprache (Kommunikationsstil, Dienstwege) [KuMa91, 892]. Das Konstrukt der Unternehmenskultur ist als Element des Unternehmensplans zu verstehen und bildet einen informalen Rahmen für die Entwicklung der Unternehmenspolitik [DySo08, 93]. Durch die starke Mitarbeiterorientierung besteht dabei ein direkter Bezug und Einfluss auf die Aufgabenträgerebene der Unternehmensarchitektur.

5.2.1.2. Identifikation sicherheitsrelevanter Bezugsobjekte

Die vorgestellten Gegenstände nach HAHN sind nicht alle in gleicher Weise aus sicherheitsorientierter Perspektive als relevant zu erachten. In den folgenden Abschnitten werden diese daher anhand der beiden Sichten Objektsystem und Zielsystem des SOM-Unternehmensplans bewertet.

Objektsystem

Das Objektsystem der Ebene Unternehmensplan beschreibt in einer hohen Aggregationsstufe die Kernprozesse der Leistungserstellung sowie die dazu notwendige Allokation von betrieblichen Ressourcen, somit das Leistungssystem des Unternehmens. Aus Sicht der Informati-

[29] Bezogen auf die Systematik des St. Galler Managementkonzepts wären Unternehmenskultur und -philosophie in engerer Begriffsfassung dem normativen Management zuzuordnen, vgl. hierzu [Blei04, 78ff].

onssicherheit ist diese Sichtweise als zu abstrakt einzustufen, da die dargestellten betrieblichen Objekte auf dieser Ebene eine zu geringen Modellierungstiefe (oder zu hohe Aggregationsstufe) aufweisen. Eine detailliertere Modellierung dieser Elemente erfolgt im Rahmen der Aufgaben- bzw. Aufgabenträgermodellierung, so dass auf diesen Ebenen eine ausreichend genaue Betrachtung sicherheitsrelevanter Bezugsobjekte erfolgen kann. Bestandteile des Objektsystems werden somit nicht als Bezugsobjekte der Informationssicherheit betrachtet.

Zielsystem

Das Zielsystem des Unternehmensplans bezieht sich insbesondere auf die Gegenstände Politik, Strategien, Kultur und Philosophie der strategischen Unternehmensführung nach HAHN.

Die **Unternehmenspolitik,** in Form eines Zielsystems aus Sach- und Formalzielen, bezieht sich primär auf die Hauptprozesse der betrieblichen Leistungserstellung. Sie ist ausgerichtet auf die wertschöpfungsorientierte Makrosicht eines Unternehmens und demzufolge auf unternehmensweite Vorgaben. Es ist jedoch nachvollziehbar, dass Aspekte der Informationssicherheit zu einem möglichst frühen Zeitpunkt in die Lenkung der Unternehmensentwicklung integriert werden müssen. Das wirtschaftlich orientierte Zielsystem muss zu diesem Zweck um sicherheitsrelevante Vorgaben erweitert werden, sodass die Bedeutung von Informationssicherheit sowie entsprechend zu erreichende Ziele definiert werden können. Die Unternehmenspolitik dient vor diesem Hintergrund als Bezugsobjekt der betrieblichen Informationssicherheit.

Der Gegenstand der **Unternehmensphilosophie** als paradigmatische Leitidee eines Unternehmens und Grundlage der Bildung von Unternehmenszielen ist ähnlich wie das globale Zielsystem selbst nicht als Bezugsobjekt für betriebliche Informationssicherheit geeignet. Selbst wenn eine Unternehmensphilosophie schriftlich dokumentiert ist und somit die Denkhaltung eines Unternehmens in wirtschaftlichen wie auch sozialen oder kulturellen Bereichen lenkt, so ist eine Verankerung von Informationssicherheit in diesem Kontext bereits rein inhaltlich nicht sinnvoll. Der fehlende direkte Bezug der Unternehmensphilosophie zu sicherheitsrelevanten Bereichen der Aufgabenträgerebene eines Unternehmens, wie etwa den Mitarbeitern, unterstützt diese Aussage.

Die **Unternehmenskultur**, als verhaltenssteuerndes Rahmenwerk für Mitarbeiter, ist in Bezug auf die genannte Sensibilisierung bzw. Verankerung von Belangen der Informationssicherheit als relevant einzustufen. Vor allem sozio-kulturelle Aspekte der Informationssicher-

heit wie das Erkennen der Bedeutung von Informationssicherheit (engl. *security awareness*), etwa im unternehmensinternen Umgang mit sensiblen Daten, ist durch dieses informelle Konstrukt abzubilden. Im Rahmen der aktiven Gestaltung einer Unternehmenskultur ist dies vor allem über die stetige Entwicklung von sicherheitsorientierten Werten zu erzielen, die sich sukzessive zu konkreten Handlungsweisen, Normen und Symbolen entwickeln. Die Unternehmenskultur ist somit als Bezugsobjekt der betrieblichen Informationssicherheit zu werten.

Strategien als Ergebnisse strategischer Planungsprozesse, sind durch unterschiedliche zeitliche Bezüge sowie durch verschiedene inhaltliche Ausprägungen charakterisiert. Aspekte der Informationssicherheit finden sich in diesem Sektor primär als Teilbereich der Funktionsstrategie für den Bereich der Informationsverarbeitung wieder. Dies deckt sich inhaltlich mit der Charakterisierung von Informationssicherheit als betriebliche Querschnittsaufgabe [PoWe93, 16], adressiert jedoch vordergründig die technischen Aspekte auf Aufgabenträgerebene.

Eine globale Strategie für Informationssicherheit hingegen, bezogen auf das gesamte Unternehmens, ist häufig nicht vorhanden, obwohl durch zahlreiche Gremien und Vorgehensmodelle gefordert[30]. Die Berücksichtigung sicherheitsrelevanter Aspekte in einzelnen Geschäftsbereichen hingegen ist durchaus gegeben. So ist es zum Beispiel eine geschäftsfeldbezogene strategische Entscheidung, genaue Arten und Mengen benötigter Rohmaterialen im Einkauf durch eine Streuung von Lieferanten und Bestellmengen zu verschleiern, um Rückschlüsse auf Fertigungsweisen oder Rezepturen zu erschweren. Diese Art der Berücksichtigung von Informationssicherheit durch strategische Entscheidungen zielt vornehmlich auf die Ebene der Geschäftsprozesse ab, Unternehmensstrategien sind somit als Bezugsobjekte der Informationssicherheit zu bewerten.

Zusammenfassend können somit die Gegenstände Unternehmenspolitik, Unternehmenskultur sowie Strategien als Bezugsobjekte der betrieblichen Informationssicherheit auf Ebene des Unternehmensplans identifiziert werden.

5.2.2. Bezugsobjekte der Geschäftsprozessebene

Geschäftsprozesse bilden gemäß des Architekturrahmens die Ebene zwischen dem Unternehmensplan und den Unternehmensressourcen. Sie können in Bezug auf das betriebliche Informationssystem somit als Bindeglied zwischen Unternehmensstrategie und betrieblichen

[30] Vgl. hierzu [BSI08a].

Anwendungssystemen verstanden werden [Öste95, 20f]. In der Literatur findet der Begriff des Geschäftsprozesses jedoch keine einheitliche Verwendung[31]. Im einfachsten Fall kann er als ereignisgesteuerter Ablauf von Aufgabendurchführungen interpretiert werden [FeSi08, 136].

Die **Aufgabendurchführungen** bilden in der betrieblichen Realität ein Bezugsobjekt der Informationssicherheit, da im Rahmen dieser Vorgänge Informationen als sicherheitsrelevante Assets verarbeitet und transportiert werden. Durch die Tätigkeit der Geschäftsprozessmodellierung werden diese realen Geschäftsprozesse der Diskurswelt auf entsprechende Modellinstanzen abgebildet. In Abhängigkeit vom Abstraktionsgrad und der gewählten Modellierungstiefe werden auf diese Weise untereinander gekoppelte Modellsysteme geschaffen, die in ihrer Gesamtheit ein Unternehmen als System von verbundenen Geschäftsprozessen[32] vollständig darstellen. Die Ausprägungen der Metapher und die des Meta-Modells eines genutzten Ansatzes zur Geschäftsprozessmodellierung bestimmen somit die Konkretisierung des Verständnisses darüber, welche Aspekte eines Geschäftsprozesses im Detail als sicherheitsrelevant zu erachten sind. Insbesondere die Meta-Objekttypen, die die modellierbaren Elemente eines Geschäftsprozesses vorgeben, haben hierauf großen Einfluss.

Die sicherheitsrelevanten Bezugsobjekte von Geschäftsprozessen lassen sich demzufolge auf der Grundlage des genutzten Modellierungsansatzes ableiten. In der vorliegenden Arbeit findet hierzu der SOM-Ansatz Verwendung, der in Bezug auf die sicherheitserweiterte Geschäftsprozessmodellierung in Kapitel 7.2.1 im Detail diskutiert wird. Hinsichtlich der Schemaebene der Strukturmodellbildung werden Geschäftsprozesse, unabhängig von der Art der Darstellung, als Bezugsobjekt der Informationssicherheit verstanden.

5.2.3. Bezugsobjekte der Ressourcenebene

Die dritte Ebene der SOM-Unternehmensarchitektur bezieht sich auf die Modellierung der Aufgabenträger, die als Ressourcen die auf zweiter Ebene beschriebenen Aufgaben durchführen. Betrachtet man diese Aufgabenträgergruppen als Teilsysteme des betrieblichen Objektsystems, so werden diese nach dem Aufgabenträgerprinzip in maschinelle (Anwendungssysteme, Maschinen und Anlagen) sowie personelle Aufgabenträger (Mitarbeiter) differenziert. Dem gleichen Bezugsrahmen folgend werden nach dem Objektprinzip die Teilsysteme Infor-

[31] Ein Überblick über verschiedene Definitionen ist u.a. in [Gada08, 45ff] oder [Stau06, 4ff] zu finden.

[32] Vgl. hierzu [PiFr95, 14].

mationssystem und Basissystem, sowie nach dem Phasenprinzip die Teilsysteme Lenkungssystem und Leistungssystem unterschieden [FeSi93, 4][33].

Die im Rahmen der betrieblichen Informationssicherheit relevanten Teilsysteme beziehen sich primär auf den automatisierten und nicht automatisierten Bereich des betrieblichen Informationssystems. Ausschlaggebendes Kriterium ist hierbei die Beziehungsart „Information“ im Rahmen der Teilsysteme, die sich mit dem Bezugsobjekt der globalen Meta-Aufgabe deckt.

Das Basissystem mit den maschinellen Aufgabenträgern aus **Maschinen und Anlagen** wird aus diesem Grund nicht als Bezugsobjekt berücksichtigt. Bezogen auf dieses Teilsystem stehen insbesondere Aspekte der Arbeitssicherheit, Produktionssicherheit oder genereller technischer Sicherheit im Vordergrund, die nicht als Gegenstand der vorliegenden Arbeit angesehen werden.

Personelle Aufgabenträger und **betriebliche Anwendungssysteme**, nebst relevanter IT-Infrastruktur, hingegen sind somit, gleichgültig ob Teil des Lenkungs- oder Leistungssystems, als Bezugsobjekte der betrieblichen Informationssicherheit zu werten.

5.2.4. Systematik der Bezugsobjekte

Die Aggregation der in den vorangegangen Abschnitten identifizierten Bezugsobjekte anhand der Unternehmensarchitektur von SOM führt zu nachfolgender Gesamtdarstellung. Dabei wird deutlich, dass die Bezugsobjekte über alle Ebenen der Unternehmensarchitektur verteilt sind. Die globale Meta-Aufgabe der Informationssicherheit nimmt somit auf alle Teilmodellsysteme der Unternehmung gleichermaßen Bezug und sollte entsprechend übergreifend auch in der Unternehmung verankert sein.

[33] Vgl. hierzu Kapitel 3.1.1.

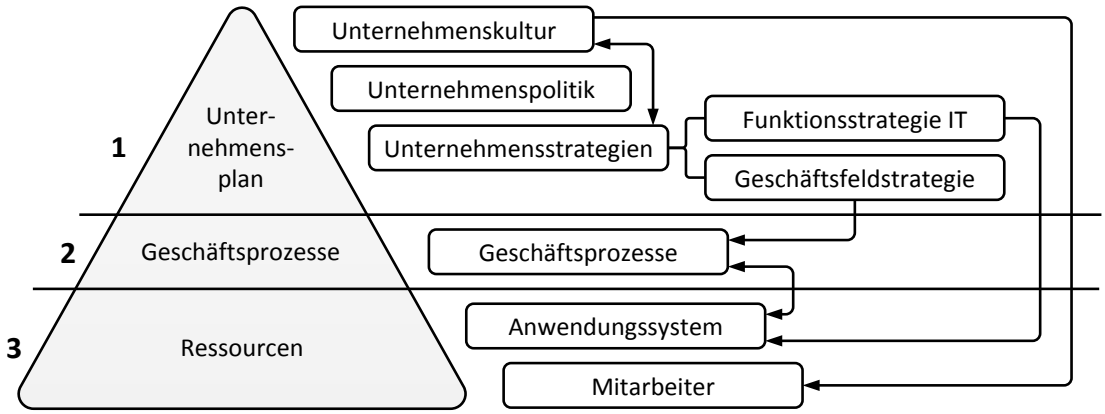

Abbildung 18: Systematik der Bezugsobjekte betrieblicher Informationssicherheit

Aus den dargestellten Beziehungen zwischen den Teilmodellsystemen, die implizit durch den Wechsel von Außen- zu Innenperspektive sowie von Aufgaben- zu Aufgabenträgerebene in der Unternehmensarchitektur der SOM-Methodik verankert sind, können Zusammenhänge zwischen einzelnen Bezugsobjekten der Informationssicherheit abgeleitet werden.

Auf Ebene des Unternehmensplans besteht zwischen den Bezugsobjekten Kultur und Strategie ein interdependenter Zusammenhang. Einerseits können strategische Entscheidungen zu Modifikationen der Unternehmenskultur führen, andererseits werden Inhalte und Umsetzbarkeit strategischer Entscheide auch durch die Kultur begrenzt. Im Rahmen einer kulturellen Transformation ist in diesem Zusammenhang dafür Sorge zu tragen, dass eine Übereinstimmung von Strategien und Unternehmenskultur gegeben ist oder generiert werden kann [Hopf00, 784f].

Strategien bilden in Bezug auf die Ebene der Geschäftsprozessmodellierung einen Gestaltungsraum für die Ausrichtung von Geschäftsprozessen. Diese sind abzustimmen auf die strategische Grundausrichtung der Unternehmung, demzufolge entsprechend der Strategien anzupassen bzw. zu instanziieren. Geschäftsprozesse selbst stehen wiederum in interdependenter Beziehung zur maschinellen und personellen Aufgabenträgern, die einerseits definierte Aufgaben umsetzen, andererseits auch regulierend auf die Gestaltung von Geschäftsprozessen einwirken können[34]. Die Unternehmenskultur und deren Entwicklung haben ebenfalls Auswirkungen auf die Ressourcenebene, jedoch, wie bereits dargestellt, ausschließlich auf den Bereich der personellen Aufgabenträger.

[34] Zum Beispiel kann die häufig zitierte „technische Machbarkeit“ einen solchen reglementierenden Faktor darstellen.

Aus Sicht der Informationssicherheit bedeuten diese Beziehungen und Abhängigkeiten, dass auch die Sicherheitsartefakte, welche die jeweiligen Bezugsobjekte adressieren, einer Abstimmung und Synchronisation bedürfen. Eine Einführung neuer Sicherheitsartefakte im Bereich von betrieblichen Anwendungssystemen im Rahmen einer Funktionsstrategie, zum Beispiel neue Authentifizierungsmechanismen, ist somit nur dann sinnvoll, wenn auch deren Nutzung, das „gelebt werden“ durch die Mitarbeiter, durch entsprechende Normen und Werte der Unternehmenskultur unterstützt wird.

5.3. Sicherheitsartefakte

Der Begriff des Sicherheitsartefakts wurde in Kapitel 3.1.3.3 als Teilergebnis des Lösungsverfahrens einer unternehmensweiten Meta-Aufgabe zur Realisierung betrieblichen Informationssicherheit eingeführt. Aufbauend auf dieser Definition werden Sicherheitsartefakte anhand des Beschreibungsrahmens in den folgenden Abschnitten identifiziert und beschrieben.

5.3.1. Einführung

Sicherheitsartefakte stellen sicherheitsrelevante Ergebnisse dar, die durch die Durchführung eines Lösungsverfahrens auf einem Aufgabenobjekt entstehen. Sie beziehen sich somit nicht auf die verhaltensorientierten Aktionen bzw. Aktionssteuerungen aus Innensicht des Lösungsverfahrens. Die Grundlage für diese Interpretation bildet die Zielsetzung, die mit der Definition eines Strukturmodells der Informationssicherheit verbunden ist. Diese besteht primär in der Schaffung einer Systematik, anhand derer Aspekte der Informationssicherheit im Kontext eines betrieblichen Systems verankert werden können. Verhaltensaspekte, somit die Ausgestaltung der Lösungsverfahren zur Erzeugung eines Sicherheitsartefakts, sind nicht Bestandteil dieser Systematik, sondern vielmehr als Teilbereich von Vorgehensmodellen zur Schaffung betrieblicher Informationssicherheit anzusehen.

Sicherheitsartefakte, wie zum Beispiel informelle Dokumente zur Planung von Sicherheitsmaßnahmen, verändern durch ihre Umsetzung den Sicherheitsgrad eines Aufgabenobjektes. Als Aufgabenobjekte fungieren in diesem Rahmen die in vorangegangenem Kapitel vorgestellten Bezugsobjekte der Informationssicherheit. Die im folgenden Abschnitt vorzustellenden Sicherheitsartefakte sind im Rahmen der Strukturmodellbildung der Informationssicherheit als Typen von Sicherheitsartefakten zu verstehen. In diesem Punkt entfernt sich das vor-

liegende Begriffsverständnis von dem der UML, da in deren Kontext keine Unterscheidung zwischen Typ- und Instanzebene in Bezug auf Artefakte vorgenommen wird [Jeck04, 145].

In der entsprechenden Literatur werden Sicherheitsartefakte sehr unterschiedlich bezeichnet, interpretiert und auch systematisiert[35]. Zur Festlegung der Semantik konkreter Sicherheitsartefakte sowie zur Eignungsprüfung für die weitere Verwendung werden bestehende Interpretationen analysiert und entsprechend der definierten Metapher dieser Arbeit interpretiert. Als Ausgangspunkt für dieses Vorgehen werden die Standards und Leitlinien des BSI herangezogen. Gegliedert anhand des Beschreibungsrahmens geben die folgenden Abschnitte einen Überblick über diese grundlegenden Definitionen.

5.3.2. Sicherheitsartefakte des Unternehmensplans

Anhand der identifizierten Bezugsobjekte sowie der allgemeinen Definitionen des BSI können die folgenden Sicherheitsartefakte abgeleitet werden.

5.3.2.1. Sicherheitskultur

Der Begriff der Sicherheitskultur findet seine Ursprünge im Bereich der Sicherheit technischer Industrieanlagen. Insbesondere nach der Katastrophe von Tschernobyl 1986 wurde er durch die International Nuclear Safety Group (INSAG) in den zu dem Vorfall entstandenen Gutachten geprägt[36]. Die Sicherheitskultur wurde in diesem Rahmen als Sammlung von Charakteristika und Einstellungen in Organisationen sowie bei Individuen eingeführt, welche sicherstellen, dass Sicherheitsaspekte beim Betrieb von Nuklearanlagen entsprechend ihrer Wichtigkeit Berücksichtigung finden. Als Elemente der Sicherheitskultur wurden zum Beispiel Aspekte des **Sicherheitsbewusstseins** bei Mitarbeitern oder aber Aspekte der Motivationsförderung auf Managementebene identifiziert [INSA91, 4f]. Das Konzept der Sicherheitskultur wird in diesem Sektor bis in die heutige Zeit weiterentwickelt. Es findet Verwendung, um die sicherheitsbezogenen Verhaltensweisen von Mitarbeitern einer Organisation zu beeinflussen, etwa im Rahmen von Ansätzen des Qualitäts- und Sicherheitsmanagements für die Kerntechnik [PrMi04, 5].

Im direkten Vergleich findet das Konzept der Sicherheitskultur im Bereich der Informationssicherheit erst seit Kurzem erweiterte Aufmerksamkeit. Unternehmen investierten beim Auf-

[35] Vgl. hierzu das Beispiel in Kapitel 4.1.

[36] Vgl. hierzu [INSA91] und [INSA92].

treten potentieller Bedrohungen primär in technologieorientierte Projekte mit direktem Bezug zu Anwendungssystemen oder der IT-Infrastruktur, um diese abzuwehren. Mitarbeiter und deren Verhaltensweisen in Bezug auf sicherheitsrelevante Daten und Prozesse blieben eher unbeachtet. Der **menschliche Faktor** rückt jedoch zunehmend in den Fokus, wird er doch mittlerweile in Studien sogar oftmals als größtes Hindernis bei der Umsetzung betrieblicher Informationssicherheit betrachtet [Delo05, 14].

Sicherheitskultur wird im betrieblichen Umfeld als Bestandteil der Unternehmenskultur betrachtet. Analog zu dieser stellt sie die Gesamtheit der in einer Unternehmung vorherrschenden kollektiven Werte, Normen sowie Denk- und Verhaltensmuster dar, die allen Mitarbeitern einen Rahmen für ihr Verhalten im Umgang mit sicherheitsrelevanten Belangen der Unternehmung vermittelt [HoPr03, 289]. Ziele der Etablierung einer Sicherheitskultur im Unternehmen sind demzufolge sowohl die Einstellung als auch das aktive Verhalten von Mitarbeitern in Bezug auf Informationssicherheit zu entwickeln. Mitarbeiter müssen sowohl die Risiken als auch ihre Verantwortlichkeiten im Umgang mit sensiblen Daten verinnerlichen [Vei+07, 149]. Ein Rahmenwerk der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (*Organisation for Economic Co-operation and Development,* OECD) identifiziert diesbezüglich neun Prinzipien, wie etwa Bewusstsein (awareness), Moralvorstellungen (ethics) oder demokratische Grundwerte (democracy), welche die Entwicklung einer Sicherheitskultur fördern. Die Prinzipien beziehen sich dabei auf Mitarbeiter aller Ebenen eines Unternehmens und zielen darauf ab, in Abhängigkeit von der Rolle des jeweiligen Mitarbeiters, im Rahmen innerbetrieblicher Weiterbildungen umgesetzt zu werden [OECD02, 9ff].

Die Etablierung einer Sicherheitskultur ist nicht als einmaliges Projekt anzusehen, sondern vielmehr als kontinuierlicher Prozess, der eine ständige Analyse, Anpassung und Förderung der jeweiligen Maßnahmen erfordert [ScTe06, 64]. Diesbezügliche Vorgehensmodelle nehmen oftmals Bezug auf das PDCA-Modell[37], wie es zum Beispiel im Rahmen des ISMS des BSI zum Einsatz kommt [BSI08a, 15f]. Die konkrete Umsetzung von Maßnahmen erfolgt dabei häufig in sogenannten **Security Awareness Kampagnen**, die in verschiedenen Phasen

[37] Das PDCA-Modell ist ein von DEMING entwickelter geschlossener Prozess für die kontinuierliche Verbesserung im Rahmen des Total Quality Managements. Der Zyklus gliedert sich in die vier namensgebenden Phasen Plan, Do, Check und Act. Eine Beschreibung ist in [WaDe88] zu finden.

entsprechendes Wissen vermitteln und, damit verbunden, die Grundeinstellungen zur Informationssicherheit ändern bzw. stärken[38].

Die Sicherheitskultur ist somit als Sicherheitsartefakt auf Ebene des Unternehmensplans zu werten. Analog zu dem Bezugsobjekt der Unternehmenskultur bestehen auch hier direkte Beziehungen zu Mitarbeitern auf Ebene der Aufgabenträger. Die Konzeption und Realisierung einer Sicherheitskultur kann jedoch nicht ohne organisatorisch verankerte Grundlage in einem Unternehmen erfolgen. Diese Rahmenbedingungen sind durch das Artefakt der Sicherheitsleitlinie zu definieren und zu realisieren.

5.3.2.2. Sicherheitsleitlinie

Die Unternehmenspolitik dient als Bezugsobjekt für die globale Verankerung relevanter Regeln und Ansichten der Lenkungsebene in Bezug auf die Informationssicherheit einer Unternehmung. Das resultierende Sicherheitsartefakt wird als **Sicherheitspolitik** oder auch **Sicherheitsleitlinie** bezeichnet. Der Begriff Sicherheitspolitik entstammt der direkten Ableitung aus dem englischen Terminus „*security policy*“, der oftmals ähnlich wie die eingangs dargestellte Beschreibung Verwendung findet. Die englische Variante ist jedoch mehrfach belegt, so wird sie etwa ebenso bei Betriebssystemen eines bekannten Softwareunternehmens aus Redmond, USA, zur Beschreibung von Zugriffsrechten eingesetzt. Eine im Englischen hierdurch notwendigerweise geschaffene Differenzierung, zum Beispiel in „*technical security policy*“ [BrSc95, 56], ist jedoch im deutschen Sprachraum nicht gebräuchlich. Aus diesem Grund folgt die vorliegende Arbeit der Begriffsauffassung des BSI und verwendet als Bezeichnung für ein Sicherheitsartefakt des Bezugsobjektes Unternehmenspolitik den Begriff Sicherheitsleitlinie [BSI09, 55].

Die in dieser Arbeit angewandte Definition lehnt sich ebenso inhaltlich an die Sichtweise des BSI an. Unter einer Sicherheitsleitlinie wird ein offizielles Bekenntnis der Lenkungsebene eines Unternehmens zu ihrer Verantwortung in Bezug auf die Umsetzung der Informationssicherheit verstanden [BSI09, 1513]. Die **IT-Sicherheitsleitlinie** beschreibt allgemeinverständlich für welche Zwecke, mit welchen Mitteln und mit welchen Ressourcen Informationssicherheit innerhalb eines Unternehmens hergestellt werden soll [BSI08b, 21]. Die zentralen Inhalte einer Sicherheitsleitlinie werden durch die folgenden vier Kernpunkte verkörpert.

[38] Ein Überblick zu diesem Thema wird zum Beispiel in [Fox03] oder [BrBu05] gegeben.

Sicherheitsvorgaben

Sicherheitsrelevante Vorgaben dienen in erster Linie der Festlegung grundlegender Aussagen zur unternehmensinternen Bedeutung von Informationssicherheit in Bezug auf Geschäftsbereiche und Kernprozesse. In gleicher Weise werden jedoch auch unternehmensexterne Auflagen durch Gesetze, Verordnungen oder Standards unter diesem Punkt subsumiert [Müll05, 72]. Aus Innensicht handelt es sich hierbei zum Beispiel um Zielsetzungen im Bereich der Sicherung investierter Werte, Gewährleistung des Vertrauens von Kunden sowie den Schutz der Reputation des Unternehmens [PoBl04, 90f]. Aus Außensicht werden insbesondere gesetzliche Vorgaben in den Bereichen des Datenschutzes (BDSG), der Verkehrssicherungspflichten (Mindestanforderungen an das Risikomanagement, MaRisk) oder aber bezüglich des Risikomanagements (KonTraG) betrachtet.

In einer Sicherheitsleitlinie definierte Sicherheitsvorgaben stehen demnach in direktem Bezug zu den in Kapitel 3.2.2 angesprochenen Formalzielen der Meta-Aufgabe zur Realisierung betrieblicher Informationssicherheit. In Kapitel 5.4.2 werden diese im Detail beschrieben.

Sicherheitsniveau

Die in sehr abstrakter Form qualitativ definierten Sicherheitsvorgaben einer Unternehmung sind im Anschluss quantitativ durch die Spezifikation eines unternehmensweiten Sicherheitsniveaus zu erweitern [BSI08b, 17]. Das anzustrebende Sicherheitsniveau leitet sich dabei insbesondere aus gesetzlichen Anforderungen und den damit verbundenen Sicherheitsvorgaben für ein Unternehmen ab. Von großer Bedeutung ist in diesem Zusammenhang die Schaffung eines unternehmensweit einheitlichen und auch akzeptierten Niveaus, das individuelle Sicherheitsempfinden und Vorstellungen einzelner Unternehmensbereiche vereint [HoPr03, 281].

Geltungsbereich

Als weiterer inhaltlicher Kernaspekt ist der Geltungsbereich einer Sicherheitsleitlinie festzulegen. Dieser beschreibt die organisatorischen Einheiten einer Unternehmung, auf die sich das Rahmenwerk der Sicherheitsleitlinie bezieht. Hierbei ist zu beachten, dass alle jeweiligen Geschäftsprozesse bzw. fachlichen Aufgaben eines Bereichs im Rahmen der Zieldefinitionen Berücksichtigung finden [BSI09, 1513].

Unternehmensweite Sicherheitsstrategie

Die Kombination aus globalen Sicherheitszielen, Sicherheitsniveaus und entsprechenden Geltungsbereichen bilden die Grundlage für die Festlegung einer zentralen unternehmensweiten Sicherheitsstrategie. Als Bestandteil der Sicherheitsleitlinie dient diese als abstrakter Rahmen für die Planung des weiteren Vorgehens zur unternehmensweiten Umsetzung der sicherheitsrelevanten Anforderungen [BSI08b, 22][39].

Das grundsätzliche Vorgehen bei der Erstellung einer Sicherheitsleitlinie beschreibt das BSI in der Maßnahme 2.192 ihrer Grundschutzkataloge. Es besteht aus sechs Einzelschritten, die sequenziell durchzuführen sind. Als erster Schritt ist die Verantwortlichkeit der Unternehmensleitung zu klären bzw. herzustellen. Danach sind in den Schritten zwei bis vier die oben beschriebenen inhaltlichen Kernpunkte auszuarbeiten, bevor in Schritt fünf die Bekanntgabe der Sicherheitsleitlinie im Unternehmen erfolgt. Als sechster Schritt ist die Aktualisierung und Anpassung der Sicherheitsleitlinie im Zeitverlauf iterativ durchzuführen [BSI09, 1513f].

Die **Formulierung und Strukturierung einer Sicherheitsleitlinie** ist wiederum Gegenstand unterschiedlicher Auffassungen. Das BSI empfiehlt hier als Rahmen eine nicht mehr als 20-seitige schriftliche Ausarbeitung [BSI08b, 22], andere Autoren schlagen eine stärker gegliederte Struktur mit stufenweiser Ausarbeitung unter Verwendung mehrerer Dokumente vor [Schm06, 92]. Als wichtiges Kriterium für die Wirksamkeit einer Sicherheitsleitlinie ist zudem festzuhalten, dass sowohl Inhalte, als auch Formulierung, Umfang und Gliederung, an den Zielgruppen, somit den jeweiligen Geltungsbereichen, sowie deren Interessen und Sprachgebräuchen auszurichten sind [Müll05, 76].

Die Sicherheitsleitlinie ist das zentrale Instrument des Managements zur Steuerung und Beeinflussung der Informationssicherheit im Unternehmen. Durch sie wird die an sich große Bandbreite an Ansätzen zur Schaffung von Informationssicherheit reduziert und fokussiert auf die für die jeweilige Unternehmung relevanten Bereiche. Die Sicherheitsleitlinie ist dabei direkt abzuleiten bzw. in Einklang zu bringen mit der Unternehmenspolitik sowie der grundlegenden strategischen Ausrichtung des Unternehmens. Nur so kann sie einen mittel- bis langfristig gültigen Orientierungsrahmen darstellen, der sowohl externe Anforderungen als auch interne Standpunkte berücksichtigt und für die Mitarbeiter und die Prozesse eines Unternehmens gleichermaßen die Grundlage für eine sicherheitsorientierte Ausrichtung bildet.

[39] Vgl. hierzu Kapitel 5.3.2.3.

5.3.2.3. Sicherheitsstrategie

Der Begriff Sicherheitsstrategie wird in der einschlägigen Literatur auf unterschiedliche Bezugsobjekte angewandt. Das BSI verwendet ihn als methodisches Konstrukt ausschließlich auf der Lenkungsebene, dokumentiert und expliziert durch die Sicherheitsleitlinie. ECKERT hingegen sieht in einer Sicherheitsstrategie ein Synonym zu einer „*security policy*“, einer Sammlung von Maßnahmen zur Erfüllung von Schutzbedarfen von Computer- oder Anwendungssystemen [Ecke06, 179f]. Als Bezugsobjekte fungieren in der letztgenannten Definition somit Elemente des Ressourcenmodells wohingegen die erste Interpretation Elemente des Unternehmensplans als Bezugsobjekte adressiert.

Allgemein definiert kann eine Sicherheitsstrategie als Festlegung strategischer Ziele und Verfahren zur planmäßigen Herstellung, Überwachung, Erhaltung und Weiterentwicklung der Informationssicherheit verstanden werden [HeLe05, 249]. Sie muss in diesem Zusammenhang zudem die Ausgangssituation im Unternehmen beschreiben, messbare Kriterien zur Erfolgsmessung definieren sowie das Vorgehen und die dazu notwendigen Ressourcen spezifizieren [Lip+92, 369].

In der vorliegenden Arbeit wird die Sicherheitsstrategie als **Sicherheitsartefakt der Unternehmensstrategien** verstanden. Das Bezugsobjekt Unternehmensstrategie ist wie beschrieben abzuleiten aus der zentralen strategischen Ausrichtung, die auf Ebene der Unternehmenspolitik definiert wird. Analog zu dieser Betrachtung sind Sicherheitsstrategien als diesbezügliches Sicherheitsartefakt zu interpretieren, somit als Konkretisierung der Vorgaben, die im Rahmen der Sicherheitsleitlinie gemacht werden. Im speziellen bedeutet dies eine Schärfung der unternehmensweiten Sicherheitsstrategie sowie eine Verfeinerung der Sicherheitsziele und der entsprechend definierten Sicherheitsniveaus, die ebenfalls zur Erfolgsmessung einsetzbar sind.

Der Nutzen dieses Sicherheitsartefaktes ergibt sich durch die Zuweisungsmöglichkeit von genaueren Sicherheitsvorgaben zu einzelnen Strategietypen, insbesondere den oben angeführten Geschäftsfeld- und Funktionsstrategien. Sicherheitsstrategien sind in diesem Zusammenhang ein Konzept, das konkret auf bestimmte Funktionsbereiche oder Geschäftsprozesse abgestimmt werden kann und somit eine deutliche Konkretisierung der Vorgaben, die durch die Sicherheitsleitlinie gegeben werden, ermöglicht. Dies bildet die Grundlage für eine genaue Bestimmung sicherheitsrelevanter Maßnahmen, Ressourcen und Vorgehen, die sich auf be-

stimmte Aufgabenträger- oder auch Geschäftsprozesstypen als zu schützende Objekte auf Ebene zwei bzw. drei des Beschreibungsrahmens beziehen.

Es wird deutlich, dass Sicherheitsstrategien im Vergleich zu der Sicherheitsleitlinie erweiterte Beziehungen zu Aufgabenträgertypen enthalten, sei es als benötigte Ressource oder als zu schützendes Objekt. Transferiert auf den SOM-Ansatz stellen sie ein methodisches Bindeglied zwischen Unternehmensplan und Geschäftsprozess- bzw. Aufgabenträgerebene dar, das eine exaktere Transformation von Sicherheitsanforderungen zwischen den Ebenen ermöglicht.

5.3.3. Sicherheitsartefakte der Geschäftsprozessebene

Geschäftsprozesse als Bezugsobjekte der Informationssicherheit werden in der Literatur nur in geringem Maße berücksichtigt. Oftmals erfolgen ausschließlich kurze Hinweise auf globale Zusammenhänge und Abhängigkeiten, eine umfassende Diskussion und Einbettung erfolgt jedoch nicht. Der folgende Abschnitt verdeutlicht dies exemplarisch anhand zweier Ansätze.

Ansatz des BSI

Im Rahmen der Standards des BSI und dessen Vorgehensmodellen wird die Umsetzung der Sicherheitsstrategien in einem Unternehmen durch ein Sicherheitskonzept und eine Sicherheitsorganisation realisiert. Letztere bezieht sich auf eine zu realisierende Aufbauorganisation eines Unternehmens, die die Umsetzung der Sicherheitsstrategien durch entsprechende Aufgaben- und damit Rollenverteilungen an Mitarbeiter ermöglicht. Das Sicherheitskonzept umfasst eine systematische Festlegung der im Rahmen der Strategien definierten konzeptionellen Sicherheitsanforderungen sowie eine Beschreibung des Vorgehens zu deren Umsetzung in Form konkreter Maßnahmen. Das IT-Sicherheitskonzept fungiert dabei als zentrales Dokument eines Unternehmens bei der Realisierung von Informationssicherheit, jede konkrete Sicherheitsmaßnahme muss sich letztlich auf dessen Inhalte zurückführen lassen [BSI09, 55]. Im Rahmen der Erstellung des Sicherheitskonzeptes nach BSI-Grundschutz erfolgt dabei unter anderem eine IT-Strukturanalyse, mit dem Ziel den IT-Verbund eines Unternehmens zu analysieren und zu dokumentieren [BSI08b, 39ff]. Zwar wird dabei auf die Zusammenhänge von IT-Infrastruktur bzw. Anwendungen und Geschäftsprozessen hingewiesen und zu deren Berücksichtigung aufgefordert [BSI08a, 27ff], eine dedizierte Aufnahme von Geschäftsprozessen als Bezugsobjekt ist jedoch nicht vorgesehen. Gemäß BSI sind unter Umständen jedoch einzelne Geschäftsprozesse als Entität im Rahmen der Erstellung der Sicherheitsleitlinie

hervorzuheben und mit Sicherheitsniveaus („normal“, „hoch“, „sehr hoch“) zu attributieren [BSI08b, 19f], die Aufgaben und Inhalte der Prozesse werden dabei jedoch nicht betrachtet. Es wird somit deutlich, dass Geschäftsprozesse im Rahmen des BSI-Ansatzes nur bedingt zum Tragen kommen. Vielmehr erfolgt eine direkte Abbildung strategischer Sicherheitsanforderungen durch ein Sicherheitskonzept auf die maschinellen Elemente bzw. die Mitarbeiter auf Aufgabenträgerebene.

Ansatz nach Müller

Die Relevanz von Geschäftsprozessen und deren Berücksichtigung in Form von Sicherheitsartefakten wird in diesem Zusammenhang dennoch in einigen Publikationen aufgegriffen. MÜLLER zum Beispiel basiert die Ableitung von Sicherheitsanforderungen auf einer Klassifikation von Geschäftsprozessen, anhand derer Auswirkungen von Sicherheitsverletzungen, durch Geschäftseinflussanalysen bestimmt, systematisiert werden. Diese Systematik beinhaltet neben Kern- und Supportprozessen auch deren benötigte Ressourcen, bezeichnet als Schutzobjekte. Die abzuleitenden Sicherheitsanforderungen beziehen sich in diesem Ansatz primär auf diese Schutzobjekte, zum Beispiel die Verfügbarkeit der Ressource „Server“, und nur sekundär auf Prozessanforderungen. Die Notwendigkeit Letzterer wird zwar erwähnt, im Rahmen des dargestellten Vorgehens jedoch nicht weiter expliziert. Als Hilfsmittel für die Beschreibung wird eine tabellarische Dokumentation vorgeschlagen, bei der vorwiegend benötigte Ressourcen sowie Folgen bei Sicherheitsverletzungen dargestellt werden [Müll05, 85ff].

Im Kern wird deutlich, dass ein dediziertes Sicherheitsartefakt im Sinne der vorliegenden Arbeit in den bisherigen Forschungsaktivitäten nicht adressiert oder benannt wurde. Im Ergebnis entsteht eine Lücke zwischen betriebswirtschaftlichen und sicherheitsorientierten Ansichten im Unternehmen, die nur durch eine integrierte Betrachtungsweise des Themas Informationssicherheit überbrückt werden kann [Neu+06, 458]. Ein erster Schritt hierzu ist die konkrete Benennung eines Sicherheitsartefaktes auf Geschäftsprozessebene und dessen Integration in die Strukturen der betrieblichen Informationssicherheit. In der vorliegenden Arbeit erfolgt dies durch die Einführung des Sicherheitsartefakts des „**sicherheitserweiterten Geschäftsprozesses**“, der auf die Integration von geschäftsprozess- und sicherheitsorientierten Perspektiven abzielt und somit die Grundlage bildet für die Entwicklung einer entsprechenden Modellierungsmethodik.

Das Bezugsobjekt des Artefaktes stellt die Gesamtheit der Geschäftsprozesse eines Unternehmens dar, somit die Aufgabenebene eines betrieblichen Systems. Zusammengefasst werden diese in Form eines Geschäftsprozessmodells, welches die Lösungsverfahren für die Umsetzung der Zielvorgaben des Unternehmensplans spezifiziert und somit alle Aufgaben beinhaltet, die im Rahmen der Durchführung von Haupt- und Serviceprozessen durchzuführen sind.

In Bezug auf die grundlegende Meta-Aufgabe „Herstellung und Aufrechterhaltung betrieblicher Informationssicherheit" beinhaltet die Teilaufgabe der Erstellung eines sicherheitserweiterten Geschäftsprozessmodells die Analyse und Erweiterung eines bestehenden Geschäftsprozessmodells um sicherheitsrelevante Eigenschaften. Das Artefakt kann dann als Bindeglied zwischen Unternehmensplan und Ressourcenmodell fungieren, um so die sicherheitsspezifische Abstimmung zwischen Lenkungs- und Leistungssystem zu verbessern. Eine diesbezügliche Modellierungsmethodik wird in Teil III der vorliegenden Arbeit im Detail vorgestellt.

5.3.4. Sicherheitsartefakte der Ressourcenebene

Personelle Aufgabenträger und betriebliche Anwendungssysteme, sowie deren IT-Infrastruktur, wurden in Kapitel 5.2.3 als relevante Bezugsobjekte der betrieblichen Informationssicherheit auf Ebene des Ressourcenmodells identifiziert. In der Literatur finden sich für diese Elemente in der jeweiligen Interpretation diverse Sicherheitsartefakte, eine einheitliche Systematik ist jedoch nicht gegeben. Das BSI zum Beispiel sieht auf dieser Ebene als zentrale Punkte die Sicherheitsorganisation mit Fokus auf personellen Aufgabenträgern sowie technische Sicherheitsmaßnahmen in Bezug auf maschinelle Aufgabenträger als Bestandteile des umfassenden Konstrukts des Sicherheitskonzepts [BSI08a, 14]. Die vorliegende Arbeit geht in Grundzügen konform mit diesem Ansatz, erweitert das Begriffssystem jedoch, um eine bessere Differenzierung der Sicherheitsaspekte auf Aufgabenträgerebene zu ermöglichen.

Die resultierenden Komponenten Sicherheitskonzept, Sicherheitsmaßnahme und Sicherheitsarchitektur, als relevante Artefakte des Ressourcenmodells, werden in den folgenden Abschnitten beschrieben.

5.3.4.1. Sicherheitskonzept

Ein Sicherheitskonzept bzw. eine Sicherheitskonzeption wird als globales Sicherheitsartefakt angesehen, das sich auf die gesamte Ebene des Ressourcenmodells bezieht. Es besteht unter anderem aus **Sicherheitsmaßnahmen**, die wiederum spezifische Elemente des Ressourcenmodells als Bezugsobjekte adressieren, sowie einer **Sicherheitsarchitektur** zur Einbettung und Strukturierung der Maßnahmen.

Die Inhalte eines Sicherheitskonzeptes sind abhängig von der jeweiligen Betrachtungsweise der Thematik. Als allgemein anerkannt gelten neben zu definierenden Sicherheitsmaßnahmen Punkte wie Schutzbedarfsfeststellungen, Sicherheitsniveaus, Risikodefinitionen oder administrative Vorgaben [EsAt06, 118], die grundlegend auch im Rahmen des Vorgehensmodells des IT-Grundschutzes definiert werden. Diese Einzelschritte werden im Detail jedoch nicht im Rahmen dieser Arbeit behandelt. Der Fokus der folgenden Ausführungen liegt auf den Sicherheitsartefakten des Ressourcenmodells, die in Form von Sicherheitsmaßnahmen dargestellt und in eine umfassende Sicherheitsarchitektur eingegliedert werden können. Eine Sicherheitskonzeption dient in diesem Zusammenhang als zentrales Dokumentationsmittel sowie Planungs- und Steuerungsgrundlage für entsprechende Teilaufgaben der zu Grunde liegenden Meta-Aufgabe der betrieblichen Informationssicherheit in Bezug auf die Ressourcenebene.

5.3.4.2. Sicherheitsmaßnahmen

Sicherheitsmaßnahmen stellen konkrete Handlungsvorgaben dar, die sich auf die Schaffung und Aufrechterhaltung von Informationssicherheit beziehen. Sie sind als Ergebnis der Umsetzung strategischer Sicherheitsziele und Sicherheitsgrundsätze auf Ebene des Unternehmensplans in operative Handlungsanweisungen zu interpretieren [HoPr03, 55]. Sicherheitsmaßnahmen stellen Sicherheitsartefakte im Sinne der vorliegenden Arbeit dar, im folgenden Abschnitt werden Klassifizierungsansätze sowie inhaltliche Ausprägungen vorgestellt.

Strukturierung von Sicherheitsmaßnahmen

Die Systematisierung von Sicherheitsmaßnahmen erfolgt in der Literatur auf verschiedene Arten. Ein Kriterium stellt dabei der Zweck von Sicherheitsmaßnahmen dar. Hierbei werden insbesondere präventive, detektive sowie korrigierende Maßnahmen unterschieden [vzMü95, 197ff]. Ein weiteres Differenzierungskriterium stellt der Beeinflussungsgrad von Arbeitsab-

läufen durch Sicherheitsmaßnahmen dar. In diesem Zusammenhang werden aktive Maßnahmen, die reguläre Arbeitsabläufe durch notwendige Zusatzaktionen beeinflussen, von passiven Maßnahmen, die sich für einen Aufgabenträger als transparent erweisen, unterschieden [HoPr03, 56]. Das Bezugsobjekt von Sicherheitsmaßnahmen stellt das am meisten genutzte Unterscheidungsmerkmal dar. Hierbei wird in Abhängigkeit von den Zielelementen auf hohem Abstraktionslevel in technische sowie nicht-technische Maßnahmen unterschieden, wohingegen im Detail unterschiedliche Bezugsobjekte wie etwa Abteilungen, Aufgabenträger oder Anwendungssystemarchitekturen zur Systematisierung Verwendung finden[40].

In der vorliegenden Arbeit kommt die letztgenannte Sichtweise zur Strukturierung von Sicherheitsmaßnahmen zum Einsatz. Diese ist angelehnt an die Unterteilung nach dem IT-Grundschutzhandbuch, wobei nicht alle der sechs Maßnahmenkataloge (Infrastruktur, Organisation, Personal, Hardware/Software, Kommunikation und Notfallvorsorge) betrachtet werden. Sicherheitsmaßnahmen werden demnach grundsätzlich in personelle, organisatorische, infrastrukturelle und technische Maßnahmen unterteilt [BSI09, 55]. Diese Abgrenzung korrespondiert mit der Differenzierung der Modellelemente auf Ressourcenebene der SOM-Methodik. Die folgende Abbildung gibt einen Überblick der Zusammenhänge zwischen Sicherheitskonzept, Sicherheitsmaßnahmen und den entsprechenden Bezugsobjekten.

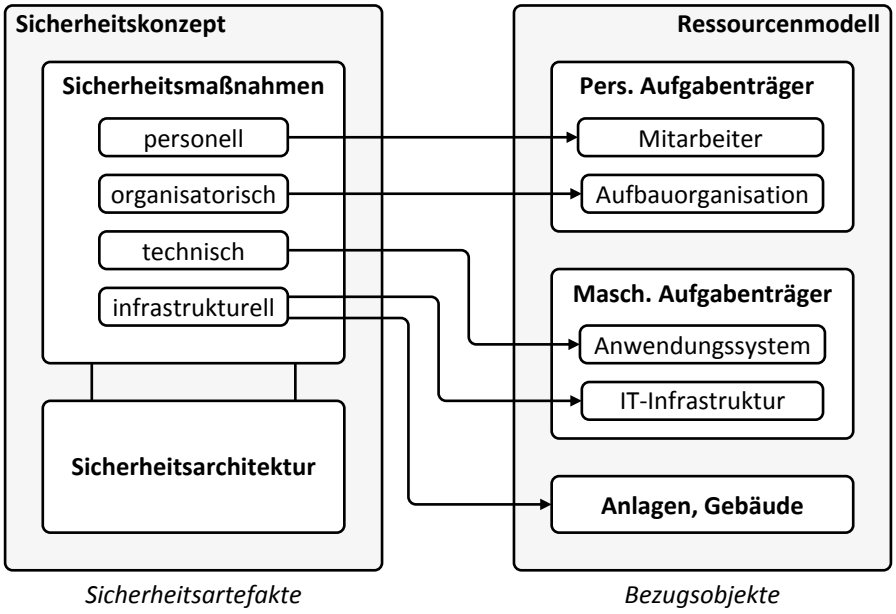

Abbildung 19: Sicherheitsartefakte auf Ressourcenebene

[40] Vgl. hierzu [Schö84], [Kral89] oder [GrSc82].

Personelle Maßnahmen beziehen sich auf die Mitarbeiter eines Unternehmens. Vorrangiges Ziel ist die Schaffung eines Sicherheitsbewusstseins, das die Etablierung einer Sicherheitskultur sowie den Einsatz entsprechender Verhaltensweisen in täglichen Arbeitsprozessen fördert. Entsprechende Maßnahmen des Bereichs Security Awareness wurden in Kapitel 5.3.2 bereits kurz angesprochen, das BSI geht im Baustein B 1.2 (Personal) der IT-Grundschutz-Kataloge dediziert auf entsprechende Aspekte ein [BSI09, 65ff].

Organisatorische Maßnahmen sind in der Regel in die Gestaltung der Aufbauorganisation eines Unternehmens eingebunden. Durch sie werden entsprechende Kompetenzen und Rollen bzw. Abteilungen im Unternehmen geschaffen, die sich auf die Erzeugung und Aufrechterhaltung der Informationssicherheit konzentrieren [TeSc00, 21]. Da sie stark organisationsabhängig sind, können sicherheitsrelevante Rollen jedoch nicht allgemeingültig definiert werden. Einen Überblick über mögliche Ausgestaltungen dieser Rollen sowie resultierende Sicherheitsorganisationen gibt [Schm06, 39ff], in Baustein B 1.1 (Organisation) erfolgen die entsprechenden Ausführungen des BSI [BSI09, 62ff].

Infrastrukturelle Maßnahmen schützen betriebliche Anwendungssysteme und entsprechende Basismaschinen vor unerlaubten physischen Beeinträchtigungen, die etwa durch Manipulation der Hardware oder aber auch durch höhere Gewalt, wie zum Beispiel Feuer oder Blitzschlag, entstehen können. Als Beispiele gelten spezielle CO_2- bzw. Halon-Löschanlagen für Rechenzentren oder auch physische Zugangskontroll- und Überwachungssysteme. Eine umfassende Darstellung möglicher Maßnahmen in diesem Bereich ist in Baustein B 2 (Infrastruktur) der IT-Grundschutz-Kataloge zu finden [BSI09, 113ff].

Technische Maßnahmen schließlich beziehen sich auf die maschinellen Aufgabenträger des betrieblichen Informationssystems. Sie sind weiterhin unterscheidbar in Maßnahmen auf Softwareebene, wie zum Beispiel Verschlüsselungsalgorithmen, sowie Maßnahmen bezüglich der Hardware, wie etwa der Einsatz von Firewalls zur Absicherung der Netzwerkinfrastruktur [TeSc00, 21]. In den IT-Grundschutz-Katalogen des BSI werden beide Bereiche in den Bausteinen B 3 (IT-Systeme), B 4 (Netze) sowie B 5 (Anwendungssysteme) adressiert.

Der Bereich der technischen Maßnahmen im Hinblick auf betriebliche Anwendungssysteme steht im weiteren Verlauf im Fokus der vorliegenden Arbeit. Bezogen auf den automatisierbaren Teil des betrieblichen Informationssystems spezifiziert dieser konkrete

sicherheitsrelevante Handlungsanweisungen, die aus den Sicherheitsvorgaben des Unternehmensplans abzuleiten sind.

Technische Sicherheitsmaßnahmen

Aus praktischer Perspektive stellen technische Sicherheitsmaßnahmen ein umfangreiches Themengebiet dar. Durch eine Differenzierung in die Konzepte **Sicherheitsmechanismus** und **Sicherheitsdienst** kann dieser Bereich weiter strukturiert werden.

Allgemeine Sicherheitsfunktionen können durch unterschiedliche technische Verfahren, sogenannte **Sicherheitsmechanismen**, realisiert werden [Kers95, 87]. Ein Sicherheitsmechanismus gibt in Bezug auf betriebliche Anwendungssysteme ein algorithmisch fassbares Lösungsprinzip vor, das die Umsetzung einer oder mehrerer Sicherheitsfunktionen unterstützt [FrDa93, 10]. Ein Sicherheitsmechanismus zur Realisierung der Funktion „Identifikation und Authentisierung“ ist zum Beispiel die Abfrage einer Kombination aus Nutzerkennung als Identifikationsmerkmal und Passwort als Authentifizierungsmerkmal.

Aufbauend auf konkreten Sicherheitsmechanismen wird ein **Sicherheitsdienst** dann definiert als Dienst, der durch ein System bereitgestellt wird und der sich auf die Erbringung einer spezifischen Sicherheitsfunktionalität bezieht [Shir07, 169]. Er stellt somit eine logische Kapselung entsprechend aggregierbarer Sicherheitsmechanismen dar. Als Beispiel für einen Authentifizierungsdienst unter Linux kann etwa PAM (engl. *pluggable authentication modules*) angeführt werden.

Die Spezifikation von Sicherheitsmechanismen oder Sicherheitsdiensten als Lösungsverfahren für bestimmte Sicherheitsanforderungen werden dann schlussendlich durch den Begriff der **Sicherheitsmaßnahme** zusammengefasst[41]. Die Art und Weise der Einbettung einer solchen Maßnahme in bestehende Systemstrukturen kann anhand des Artefakts der Sicherheitsarchitektur näher beschrieben werden.

5.3.4.3. Sicherheitsarchitektur

Die Sicherheitsarchitektur eines allgemeinen Systems kann als Beschreibung von Strukturen, Merkmalen und Prinzipien verstanden werden, die den sicherheitsrelevanten Anforderungen an das System Rechnung trägt. Sie bildet einen methodischen Rahmen, der Sicherheitsdienste

[41] In Kapitel 5.5 werden praktische Sicherheitsmechanismen vorgestellt.

und -mechanismen aufnimmt [FrDa93, 10]. Das Begriffsverständnis der Sicherheitsarchitektur in der Literatur ist dabei jedoch sehr vom jeweilig adressierten Bezugsobjekt abhängig. Unter Bezugsobjekten werden neben hardware- bzw. software-technischen Komponenten auch einzelne Programmiersprachen, logische Organisationsbereiche oder auch bauliche Strukturen eines Unternehmens subsumiert. Vor diesem Hintergrund ist es sinnvoll, nicht allgemeine Konzepte zu Sicherheitsarchitekturen zu betrachten, sondern das Sicherheitsartefakt auf die relevanten Bezugsobjekte auszurichten [Oppl07, 97]. In der vorliegenden Arbeit sind dies die relevanten Elemente der Ressourcenebene gemäß dem Architekturrahmen. Eine Sicherheitsarchitektur bezieht sich somit sowohl auf ein betriebliches Anwendungssystem als auch auf die grundlegende IT-Infrastruktur. Mithin erfolgt eine doppelte semantische Belegung dieses Sicherheitsartefakts, die jedoch auf Basis einer Differenzierung des allgemeinen Architekturbegriffs bzgl. der genannten Bezugsobjekte aufzulösen ist.

Differenzierung des Architekturbegriffs

Eine Architektur definiert die Grundstruktur eines Systems. Unter einer Struktur werden dabei die einzelnen Elemente eines Systems, sowie deren Schnittstellen und Beziehungen zueinander verstanden [Foeg03, 57]. In Analogie zum Bauwesen umfasst die Architektur somit den Bauplan eines Systems, im Sinne einer Spezifikation seiner Komponenten und deren Beziehungen unter allen relevanten Blickwinkeln, sowie die Konstruktionsregeln für die Erstellung dieses Bauplans. Ein Bauplan stellt somit ein auf bestimmte Anforderungen ausgerichtetes Abbild eines Systems dar [Sinz99a, 1035]. Diese Perspektive verdeutlicht den Modellcharakter des Architekturbegriffs. Das durch ein Architekturmodell abgebildete Objektsystem ist somit ausschlaggebend für die Arten bzw. Typen von Architekturen, die für das entsprechende System Verwendung finden können [Foeg03, 59]. In Bezug auf Anwendungssysteme sowie deren zu Grunde liegende IT-Infrastruktur können zwei unterschiedliche Arten von Architekturen identifiziert werden. Es wird hierbei zwischen der software-technischen Architektur und der Infrastrukturarchitektur unterschieden [FoBa01, 297].

Software-technische Architekturen nehmen eine Schlüsselrolle im Entwicklungsprozess von Anwendungssystemen ein, indem sie den Übergang zwischen der fachlichen Anforderungsdefinition und der technischen Implementierung durch ihre Darstellungsform gangbar, nachvollziehbar und überprüfbar machen [Garl00, 93f]. Software-technische Architekturen werden zum Beispiel durch Verwendung des ADK-Modells oder des Nutzer- / Basismaschi-

nenkonzepts[42] sowie durch Nutzung von Softwarebausteinen wie Klassen und Komponenten beschrieben. Um die Komplexität der Anwendungssysteme beherrschbar zu machen, werden sie dabei auf unterschiedlichen Granularitätsebenen spezifiziert und ermöglichen somit eine sukzessive Verfeinerung der strukturellen Darstellung eines Anwendungssystems [FeSi08, 468]. In Abhängigkeit von den zu Grunde liegenden Paradigmen und Metaphern der Softwareentwicklung können unterschiedliche Architekturstile unterschieden werden, etwa die Client-Server-Architektur bei verteilten Systemen oder die Schichtenarchitektur [Somm07, 249ff]. Ein klassifizierender Überblick hierzu ist in [ShGa96, 20ff] zu finden.

Die **Infrastrukturarchitektur** bezieht sich aus operationaler Sicht auf die Basismaschinen betrieblicher Anwendungssysteme, die in Form der technischen Infrastruktur bereitgestellt werden. Diese wird beschrieben durch die Aufnahme hardwaretechnischer Geräte, wie Server, Netzwerkgeräte oder Kabelverbindungen, sowie durch die Spezifikation der Beziehungen zwischen diesen technischen Komponenten. Auf diese Weise entstehen Schemata, die zum einen die Verteilung der Hardware sowie eine grundlegende Netzwerktopologie aufzeigen, zum anderen auch als Grundlage dienen für die Verteilung der Softwarekomponenten, etwa in Form dedizierter Dienste, auf die jeweiligen Basismaschinen [FoBa01, 299].

Bezogen auf die Betrachtung der Informationssicherheit ergeben sich somit zwei unterschiedliche Ausprägungen des Artefaktes Sicherheitsarchitektur in Abhängigkeit von dem jeweils adressierten Bezugsobjekt auf Ressourcenebene.

Sicherheitsarchitektur betrieblicher Anwendungssysteme

Die Sicherheitsarchitektur eines Anwendungssystems stellt einen Spezialfall der softwaretechnischen Architektur dar. Sie beschreibt nicht primär die Umsetzung funktionaler Anforderungen im Rahmen des Entwicklungsprozesses, sondern vielmehr die der non-funktionalen Anforderung der Informationssicherheit. Diese Anforderungen sind im Prozessverlauf durch sukzessive Verfeinerung zwar in gewissem Maße operationalisierbar, zum Beispiel der Schutz der Vertraulichkeit durch Spezifikation einer Verschlüsselungskomponente, ein allgemein gültiger Ansatz zur Erstellung und Positionierung einer Sicherheitsarchitektur ist jedoch nicht gegeben. Im Rahmen des Software-Engineering erfahren Sicherheitsaspekte im Allgemeinen und Sicherheitsarchitekturen im Besonderen hingegen vermehrte Aufmerksam-

[42] Eine Beschreibung beider Konzepte ist in [FeSi08, 310ff] zu finden.

keit, da eine möglichst frühe Integration von Sicherheitsaspekten in den Software-Lebenszyklus in zunehmenden Maße angestrebt wird [WaWa03, 75].

Eine Sicherheitsarchitektur beschreibt in diesem Zusammenhang Sicherheitsdienste eines Systems, die notwendig sind, um geforderte Sicherheitseigenschaften zu realisieren. Weiterhin werden die dafür notwendigen Systemkomponenten und deren Leistungsanforderungen spezifiziert sowie deren Eingliederung in die Struktur des Anwendungssystems definiert [Shir07, 264]. Analog zur Entwicklung software-technischer Architekturstile, haben sich ebenso verschiedene Formen von Sicherheitsarchitekturen entwickelt. Diese basieren in der Regel auf den bestehenden Ansätzen und erweitern sie um sicherheitsrelevante Konzepte.

SOMMERVILLE identifiziert diesbezüglich zum Beispiel die zwei grundlegenden Prinzipien der Absicherung (engl. *protection*) und Verteilung (engl. *distribution*). Hinter dem Prinzip der Absicherung steht die Frage wie die Struktur eines Systems organisiert werden sollte, um die sicherheitsrelevanten Informationen gegen unautorisierte Zugriffe zu schützen. Das Prinzip der Verteilung adressiert parallel die Entscheidungssituation, wie der Verteilungsgrad dieser schutzwürdigen Assets zu definieren ist, um die negativen Effekte eines erfolgreichen Angriffs zu minimieren. Vor dem Hintergrund dieser teilweise konfliktären Anforderungen wird aufbauend auf dem Ansatz der Schichtenarchitektur eine Sicherheitsarchitektur vorgestellt, in der relevante Informationen durch drei Sicherungsschichten (*plattform level protection*, *application level protection*, *record level protection*) vor fremdem Zugriff geschützt werden [Somm07, 729f].

Ein weiteres Beispiel ist die DGSA (engl. *The Department of Defense Goal Security Architecture*), ein konzeptuelles Framework, in dem die Architektur eines Systems an den Anforderungen der zu schützenden Informationen ausgerichtet wird [Sac+04, 372]. Dies wird erreicht durch die Systematisierung der entsprechenden Assets in sogenannte „Information Domains". Diese logischen Komponenten werden unabhängig von der software-technischen Architektur definiert und dienen als Grundlage für die weitere Festlegung von technischen Sicherheitsmaßnahmen. Die Spezifikation der DGSA ist in [FeMa98] zu finden, eine weiteführende beispielorientierte Diskussion gibt [Schn99].

Sicherheitsarchitektur der Infrastruktur

In Bezug auf die IT-Infrastruktur stellt eine Sicherheitsarchitektur topologische Konzepte zur Absicherung der Datenflüsse zwischen einzelnen Systemkomponenten dar. Sie ist Bestandteil

der IT-Infrastrukturarchitektur und setzt festgelegte Sicherheitsanforderungen durch die Realisierung entsprechender basistechnologischer Maßnahmen um [Ecke06, 30]. Die Umsetzung dieser Maßnahmen beschreiben sowohl das Verfahren als auch die Platzierung entsprechender Komponenten im Rahmen einer globalen Sicht auf die gesamte IT-Infrastruktur eines Unternehmens. Das Verfahren subsumiert dabei sowohl hardware- als auch software-technische Sicherheitskomponenten, zum Beispiel Firewallsysteme oder Virenscanner. Die Platzierung bezieht sich auf die Verteilung der Komponenten innerhalb der IT-Infrastruktur, somit deren Integration in Netzwerke oder ihre Installation auf relevanten Servern oder Clients. Dieser Aspekt ist primär unter dem Gesichtspunkt der Schutzwirkung zu verstehen, als sekundäre, teilweise auch gegenläufige Größen sind hierbei zudem die Wartbarkeit und Verwaltbarkeit der Komponenten zu beachten.

Sicherheitsarchitekturen der IT-Infrastruktur können je nach unternehmensinternem Verständnis unterschiedlich differenziert werden. Ist ein Betriebssystem nach der jeweiligen Auffassung Bestandteil der Infrastruktur, so sind zum Beispiel Aspekte der zentralen Authentifizierung, etwa per Kerberos an zentralen Directory-Services, Bestandteil der Betrachtung. Wird einzig die Hardware und Vernetzung als Infrastruktur angesehen, so liegt der Fokus einer Sicherheitsarchitektur hingegen in höherem Maße auf der Absicherung des Netzwerkverkehrs an sich. Es wird deutlich, dass insbesondere im technischen Bereich eine genaue Definition der relevanten Bezugsobjekte vorgenommen werden muss.

Als Beispiel einer Sicherheitsarchitektur kann bezogen auf ein Firmennetzwerk das Konzept der DMZ (engl. *demilitarized zone*) angeführt werden. Es basiert auf der Einteilung des Netzwerkes in einzelne Zonen mit unterschiedlichen Sicherheitseigenschaften. Serverdienste die von außerhalb des Firmennetzwerkes erreichbar sein sollen werden durch Firewalls von dem internen Bereich des Netzwerks abgeschottet. Werden diese Dienste kompromittiert, so sind interne Server hiervon nicht direkt betroffen. Einen Überblick zu dieser Art von Sicherheitsarchitektur auf Netzwerkebene gibt [Vacc07, 399ff].

Das zentrale Bezugsobjekt im Rahmen der vorliegenden Arbeit stellt das automatisierbare Teilsystem des betrieblichen Informationssystems dar. Auf Ressourcenebene liegt der diesbezügliche Fokus auf betrieblichen Anwendungssystemen und entsprechenden Sicherheitsaspekten. Sicherheitsarchitekturen der IT-Infrastruktur werden im weiteren Verlauf daher nicht näher betrachtet.

5.3.5. Systematik der Sicherheitsartefakte

Gemäß dem zu Grunde liegenden Modellierungsansatz beziehen sich Sicherheitsartefakte auf bestimmte Bezugsobjekte der Unternehmensarchitektur. Sie unterliegen damit ähnlichen inhaltlichen Abhängigkeitsbeziehungen, wie sie im Hinblick auf die vorgestellten Bezugsobjekte der Informationssicherheit dargestellt wurden. Analog zu dem methodischen Rahmen der Unternehmensarchitektur entsteht ein im Kern hierarchisches Ebenenmodell der Sicherheitsartefakte, dessen Beziehungen sich Top-Down als Ableitungsbeziehung, Bottom-Up als Realisierungsbeziehung charakterisieren lassen.

Die folgende Abbildung stellt die Systematik der Sicherheitsartefakte anhand des Beschreibungsrahmens dar.

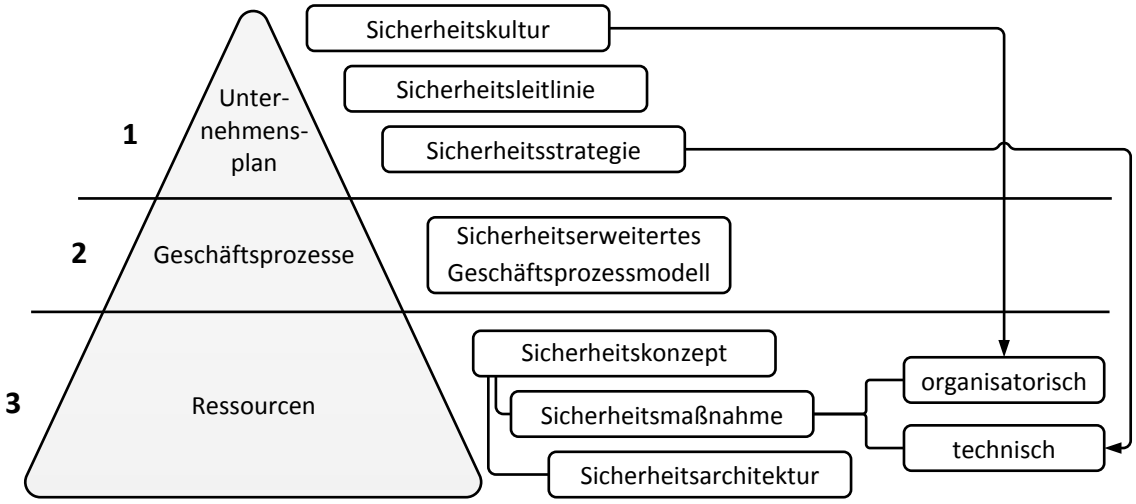

Abbildung 20: Systematik der Sicherheitsartefakte

Auf die vollständige Illustration inhaltlicher **Ableitungsbeziehungen** zwischen den einzelnen Artefakten wurde aus Darstellungsgründen verzichtet. Exemplarisch werden diese durch die Beziehungen zwischen Sicherheitskultur sowie Sicherheitsstrategie und der Differenzierung von Sicherheitsmaßnamen aufgezeigt. Diese direkte Verbindung zwischen Unternehmensplan und Ressourcenebene symbolisiert gleichermaßen den aktuell als sehr gering einzustufenden Beachtungsgrad der Geschäftsprozessebene im Kontext der Sicherheitsbetrachtung. Das Sicherheitsartefakt des sicherheitserweiterten Geschäftsprozessmodells fungiert in diesem Zusammenhang jedoch als sehr wichtiges Bindeglied zwischen den Artfakten des Unternehmensplans und des Ressourcenmodells, das eine unternehmensweite und durchgängige Berücksichtigung der betrieblichen Informationssicherheit überhaupt erst ermöglicht. Die Teil-

aufgabe der Erstellung eines sicherheitserweiterten Geschäftsprozessmodells ist Gegenstand des dritten Teils der vorliegenden Arbeit.

Neben den Beziehungen zwischen den Sicherheitsartefakten sind zusätzlich deren **Charakteristika hinsichtlich der Aufgabendurchführung** zu beachten. Wie durch die Ebenenzuordnung in der Unternehmensarchitektur bereits vorgegeben, sind Sicherheitskultur, Sicherheitsleitlinie und Sicherheitsstrategie dem Lenkungssystem zuzuordnen, Sicherheitskonzept, Sicherheitsmaßnahme und Sicherheitsarchitektur dem Leistungssystem. Top-Down betrachtet nimmt somit der strategische, oder auch organisatorische, Anteil der Aufgabencharakteristik ab, wohingegen der operationale, oder technische, Anteil zunimmt.

Einen weiteren charakteristischen Aspekt der Sicherheitsartefakte stellt deren unterschiedliche **Relevanz im Zeitverlauf** dar. Während die Artefakte des Unternehmensplans strategischer Natur sind, das sicherheitsorientierte Geschäftsprozessmodell ein taktisches Mittel darstellt, so ist die Erstellung der Artefakte auf Ressourcenebene dem operativen Bereich zuzuordnen. Insbesondere bei der Betrachtung betrieblicher Anwendungssysteme fallen hierbei weitere Unterschiede auf. Wird ein bestehendes Anwendungssystem zum Beispiel im Hinblick auf dessen Sicherheit aus Außensicht analysiert, so stehen primär die Sicherheitsarchitektur der entsprechenden Infrastruktur (Netzwerk) bzw. Sicherheitsmaßnahmen der Anwendung selbst (Verschlüsselungsstärke) im Vordergrund. In geringerem Maße werden jedoch interne Aspekte überprüft, wie etwa die zum Einsatz kommende software-technische Sicherheitsarchitektur. Ist jedoch ein Anwendungssystem zu entwickeln, so stehen diese Aspekte der Innensicht an erster Stelle der Betrachtung. Die Relevanz von Sicherheitsartefakten ist somit auch abhängig von den Prozessen, in denen eine sicherheitsbezogene Analyse durchgeführt wird. Eine diesbezügliche Gewichtung bzw. Entscheidung ist daher im Rahmen der entsprechenden bezugsobjektspezifischen Vorgehensmodelle zur Herstellung betrieblicher Informationssicherheit durchzuführen.

5.4. Sicherheitsziele

Die Beschreibung der Sicherheitsziele adressiert abschließend den dritten Meta-Objekttyp des vorgestellten Modellierungsansatzes für betriebliche Informationssicherheit. Analog zu den letzten beiden Abschnitten erfolgt die Systematisierung und inhaltliche Darstellung anhand des Beschreibungsrahmens.

5.4.1. Differenzierung des Zielsystems

Der Gesamtkomplex aus sicherheitsbezogenen Sach- und Formalzielen wird in der vorliegenden Arbeit unter dem Begriff **Sicherheitsziele** subsumiert. Wie in Kapitel 3.2.2 bereits dargestellt, können hierbei Sach- und Formalziele der Informationssicherheit unterschieden werden. Im Rahmen der globalen Meta-Aufgabe der Informationssicherheit, bestehen die Sachziele dieser Aufgabe primär in der Erreichung sogenannter **Schutzziele** für das betriebliche Informationssystem, wie zum Beispiel Vertraulichkeit oder Integrität. Formalzielorientiert beziehen sich **Sicherheitsvorgaben** der Aufgabe in diesem Zusammenhang auf den Grad sowie die Art der Zielerreichung. Spezifiziert zum Beispiel durch unternehmensexterne Gesetzgebungen oder auch interne ökonomische Vorgaben, grenzen die Sicherheitsvorgaben somit mögliche bzw. gewünschte Nachzustände einer Aufgabendurchführung ein [Loch05, 1212].

Es gilt zu beachten, dass die Sicherheitsziele in Teilaufgaben der Gestaltung und Verwaltung des betrieblichen Informationssystems nicht zwingend als alleiniger Zielkomplex fungieren. Im Rahmen der Entwicklung betrieblicher Anwendungssysteme zum Beispiel, sind Sicherheitsziele eingegliedert in das Zielsystem aus Sach- und Formalzielen der Entwicklungsaufgabe bezüglich des zu implementierenden Anwendungssystems. In diesem Kontext werden Sicherheitsziele oftmals als nicht-funktionale Anforderungen[43] an das Anwendungssystem verstanden [Somm07, 121f] oder als Subfaktoren zur Bewertung der Softwarequalität. Die ISO/IEC Norm 9126 führt Sicherheitsaspekte etwa als nachgeordnetes Charakteristikum zu dem Qualitätsmerkmal Funktionalität [Endr03, 20f], im Rahmen der Systematik von MCCALL wird das Schutzziel Integrität hingegen als direkter Qualitätsfaktor angeführt, eine weitere Betrachtung erfolgt allerdings nur bedingt in Form einer allgemeinen Qualitätsmetrik „Sicherheit“ [Pres01, 509ff].

Die vorliegende Arbeit abstrahiert in diesem Punkt von konkreten Teilaufgaben der Verwaltung des betrieblichen Informationssystems und damit verbundenen spezifischen Interpretationen der Sicherheitsziele. Die Betrachtung der Informationssicherheit anhand der Metapher einer globalen betrieblichen Aufgabe erlaubt eine unabhängige und ganzheitliche Analyse des Zielkomplexes dieser Aufgabe. Verbunden mit der orthogonalen Darstellung des Architekturrahmens kann somit eine vollständige Differenzierung hinsichtlich der jeweiligen Bezugsob-

[43] Die Modellierung von Sicherheitszielen im Sinne nicht-funktionaler Anforderungen werden auch in Kapitel 9.1.2 diskutiert.

jekte bzw. Sicherheitsartefakte erfolgen. Die folgenden Ausführungen gliedern den Zielkomplex in Sicherheitsvorgaben auf Ebene des Unternehmensplans, Schutzziele auf Ebene der Geschäftsprozesse sowie Sicherheitsanforderungen auf Ebene des Ressourcenmodells[44]. Der Fokus der Betrachtung liegt dabei auf den Schutzzielen der Informationssicherheit, da diese eine hohe Relevanz für den Fortgang der Arbeit aufweisen.

5.4.2. Sicherheitsziele auf Ebene des Unternehmensplans

Der Unternehmensplan stellt ein betriebliches System aus Außensicht dar. Die grundlegende Metapher ist die einer globalen Unternehmensaufgabe, anhand derer unter anderem auch unternehmensweite Sach- und Formalziele spezifiziert werden, die sich primär auf die betriebliche Leistungserstellung und entsprechende Rahmenbedingungen ausrichten. Sicherheitsaspekte sind in diesem Zusammenhang den letztgenannten Rahmenbedingungen zuzuordnen. Sie definieren aus Sicht der Informationssicherheit den Kontext, in dem die betriebliche Leistungserstellung erfolgen kann. Bezogen auf die Meta-Aufgabe der Informationssicherheit werden diese Rahmenbedingungen ebenfalls durch die entsprechenden Vorgaben abgedeckt, die in diesem Zusammenhang anhand ihrer jeweiligen Motivation in zwei Kategorien unterteilt werden können.

Extern motivierte Sicherheitsvorgaben beziehen sich auf Vorgaben und Regelungen, die durch unternehmensexterne Anspruchsgruppen definiert werden. Hierzu zählen insbesondere gesetzliche Regelungen des Staates sowie Richtlinien, Normen und Standards von Standardisierungsgremien, zum Beispiel dem Bundesamt für Sicherheit in der Informationstechnik und weiterer Organisationen, wie etwa dem Computer Emergency Response Team des deutschen Forschungsnetzes (DFN-CERT). **Intern motivierte Sicherheitsvorgaben** haben ihren Ursprung in der Regel in unternehmensspezifischen ökonomischen oder betriebswirtschaftlichen Fragestellungen und Zielsetzungen. Sie zielen dabei insbesondere auf die Adäquatheit, Effektivität und Effizienz der sicherheitsrelevanten Maßnahmen ab, sowie deren Betrachtung unter Kosten-Nutzen-Aspekten [Loch05, 1212].

Die Vorgaben beider Zielgruppen definieren ein gewünschtes **Sicherheitsniveau**, das durch die Durchführung der Meta-Aufgabe zu ermöglichen ist, um zum Beispiel die Zertifizierung

[44] Die dargestellte Strukturierung der Sicherheitsziele geht bedingt durch den differenzierteren Aufbau des Beschreibungsrahmens über die einführende Darstellung des allgemeinen Zielsystems in Kapitel 3.3 hinaus. Aus diesem Grund sind in Abbildung 10 die angesprochenen Sicherheitsanforderungen auf Ressourcenebene nicht aufgeführt.

nach einem bestimmten Standard zu erreichen. Dieses Sicherheitsniveau ist wiederum spezifizierbar durch einen bestimmten Zielerreichungsgrad der aufgabenspezifischen Sachziele in Form einzelner Schutzziele. Die Vorgaben und Zielsetzungen der beiden Gruppierungen sind somit ausschlaggebend für die Wahl eines Nachzustandes der Aufgabendurchführung und können unter formalzielorientiertem Blickwinkel als Sicherheitsvorgaben der Informationssicherheit interpretiert werden[45].

5.4.2.1. Rechtliche Vorgaben

Grundlegende rechtliche Vorgaben adressieren im Kern drei verschiedene Aspekte der Informationssicherheit. Zum einen den **Schutz von personenbezogenen Daten**, zum anderen die Vertraulichkeit und **Nachweisbarkeit von Transaktionen** sowie des Weiteren die entsprechenden zivil- und strafrechtlichen **Haftungen**, die sich bei der Verletzung der implizit definierten Schutzziele ergeben [HoPr03, 310]. Jeder dieser Aspekte findet auf nationaler Ebene durch unterschiedliche gesetzliche Regelungen Berücksichtigung, die sich über das Telekommunikationsgesetz (TKG), Telemediengesetz (TMG) bis hin zum Strafgesetzbuch (StGB) sowie der Strafprozessordnung (StPO) erstrecken. Ein konkretes Beispiel stellt das Bundesdatenschutzgesetz (BDSG) dar, das den Schutz personenbezogener Daten in den Vordergrund stellt. Es regelt dabei umfassend die Erhebung, Verwendung, Nutzung und Verarbeitung von personenbezogenen Daten in öffentlichen und nicht-öffentlichen Stellen [Heit07, 469].

Im Unternehmenskontext ergeben sich durch den Gesetzgeber zusätzliche Anforderungen an Firmen, die insbesondere im Zusammenhang mit der Berücksichtigung, Handhabung und **Kontrolle von Risiken** stehen. In Deutschland wird dieser Aspekt durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich geregelt. Das KonTraG ist dabei kein selbständiges, sondern ein Artikelgesetz, das verschiedene Gesetze ändert, ergänzt und präzisiert. Betroffen hiervon sind zum Beispiel das Aktiengesetz (AktG), das Handelsgesetzbuch (HGB), die Wirtschaftsprüferordnung (WPO) sowie das GmbH-Gesetz (GmbHG). Ziel des Gesetzes ist die Haftung von Vorstand, Aufsichtsrat und Wirtschaftprüfer zu erweitern sowie die Etablierung eines Risikomanagementsystems und die Ausweisung entsprechender Ergebnisse im Lagebericht des Jahresabschlusses zu forcieren[46]. Weitere Vorgaben bestehen auch auf internationaler Ebene, wie zum Beispiel durch den Sarbanes Oxley Act, ein US-Gesetz

[45] Vgl. hierzu Abbildung 13.

[46] Vgl. hierzu die Beschlussempfehlung des deutschen Bundestages zu KonTraG in [DeBu98].

von 2002 oder durch die Verordnung Basel II in Bezug auf die Kreditvergabe von Banken in 2004[47].

Die gewählten Beispiele für die gesetzlichen Vorgaben erheben keinen Anspruch auf Vollständigkeit und dienen lediglich der Verdeutlichung der unterschiedlichen rechtlichen Anforderungen, die sowohl im privaten als auch im gewerblichen Bereich an die Informationssicherheit bestehen.

5.4.2.2. Normen und Standards

Analog zu der rechtlichen Situation bestehen auch Unterschiede in den Standards, die sich auf die Informationssicherheit beziehen. Je nach Betrachtungsschwerpunkt werden unterschiedliche Teilaspekte der Sicherheit beleuchtet sowie entsprechend abweichende Anforderungen oder auch Umsetzungshinweise definiert.

Auf nationaler Ebene sind hierbei insbesondere die Standards des BSI zu nennen. Die Grundlage bilden die **IT-Grundschutzkataloge**, die als Zielsetzung die Erstellung und Umsetzung von Sicherheitsmaßnahmen in Form von Sicherheitskonzepten verfolgen [BSI09]. Ergänzt werden sie durch vier separate **Standards zum IT-Sicherheitsmanagement**, die sich mit dem Management von Informationssicherheit (BSI-Standard 100-1, [BSI08a]), der Vorgehensweise nach IT-Grundschutz (BSI-Standard 100-2, [BSI08b]), der Risikoanalyse auf Basis des IT-Grundschutzes (BSI-Standard 100-3, [BSI08c]) sowie dem Notfallmanagement (BSI-Standard 100-4, [BSI08d]) beschäftigen.

Im internationalen Kontext kann exemplarisch die Standardfamilie ISO/IEC 27000 angeführt werden. Der enthaltene Standard 27001 etwa basiert auf dem Standard BS7799-2 des British Standards Institute und thematisiert den prozessorientierten Aufbau eines ISMS sowie dessen Verankerung im Unternehmen anhand von Checklisten. ISO/IEC 27001 ist dabei der erste internationale Sicherheitsstandard, der eine Zertifizierung ermöglicht [Witt06, 42][48].

Für Unternehmen birgt die Orientierung an nationalen und internationalen Standards, neben der reinen Verbesserung der Informationssicherheit, eine Reihe von Vorteilen. Zum einen kann die Umsetzung eines Standards durch **Zertifizierungen** bestätigt werden. Dies wiede-

[47] Zu SOX und Basel II vgl. [Spei07, 338].

[48] Für eine Übersicht zu weiteren Standards wie ITIL oder COBIT und deren Differenzierung sei zum Beispiel auf [Köni06, 137ff] verwiesen.

rum ermöglicht den Nachweis, dass bestimmte rechtliche Anforderungen durch das Unternehmen erfüllt werden. So sind zum Beispiel die sicherheitsrelevanten Anforderungen durch KonTraG im Bereich des Risikomanagements durch eine Zertifizierung nach ISO/IEC 27001 vollständig erfüllt. Es resultiert somit eine Konformität zu rechtlichen Vorgaben, die sich auch im Falle von juristischen Auseinandersetzungen als vorteilhaft darstellt. Ebenso kann eine Einhaltung von Standards im Rahmen der Außenwirkung eines Unternehmens, gegenüber Kunden oder Lieferanten, als Qualitätsmerkmal dienen [Heit07, 88].

Ähnlich wie bei den gesetzlichen Regelungen ist nur ein exemplarischer Auszug von Sicherheitsstandards zu nennen. Festzuhalten bleibt die teilweise enge Verzahnung zwischen gesetzlichen Regelungen und Standards zur Informationssicherheit einerseits sowie die resultierende Motivation für Unternehmen sich nach entsprechenden externen Vorgaben zu richten und diese umzusetzen.

5.4.2.3. Unternehmensinterne Vorgaben

Neben der inhaltlichen Notwendigkeit von Informationssicherheit, getrieben durch externe Vorgaben, sind auch unternehmensinterne Kriterien ausschlaggebend für die Zielbildung auf Ebene des Unternehmensplans.

Relevante Aspekte sind hierbei zum einen die erzielbare **Außenwirkung**, die zum Beispiel bei Kunden eine sicherheitsbezogene Güte der erbrachten Leistungen vermitteln kann. Vor allem im Bereich des E-Commerce stehen Maßnahmen des Datenschutzes in Bezug auf Kundendaten in direktem Zusammenhang mit dem zu vermittelnden Image und der Seriosität des Unternehmens.

Neben diesen weichen Faktoren der Außenwirkung sind jedoch auch bestimmte Kriterien aus Innensicht für den Einsatz von Sicherheitsmaßnahmen zu überprüfen. Ein wichtiger Aspekt hierbei sind die möglichst transparenten **Integrationsmöglichkeiten** entsprechender Maßnahmen in die bestehenden betrieblichen Prozesse. Sicherheitsmaßnahmen müssen für die Mitarbeiter in einfacher Weise nutzbar und in den gewohnten Arbeitsablauf integrierbar sein, ohne die Effizienz der Prozesse zu verringern.

Ein weiterer Aspekt, der in diesem Zusammenhang Beachtung finden muss, ist die **Wirtschaftlichkeit** des Einsatzes von Sicherheitsmaßnahmen. Entsprechende Kosten müssen im Rahmen der Finanzplanung eines Unternehmens berücksichtigt werden und argumentativ

darstellbar sein. Als hauptsächlicher Kostentreiber wird in diesem Zusammenhang die immer größer werdende Komplexität im Bereich der Informationsverarbeitung angeführt, die ganzheitliche und vor allem nachhaltige Sicherheitsansätze notwendig macht [Lubi06, 10]. Die Grundlage entsprechender Methoden zur Wirtschaftlichkeitsbetrachtung besteht dabei maßgeblich in der monetären Quantifizierung der Risikobewertung und der resultierenden Risikovermeidung. Einen klassifizierenden Überblick über entsprechende Ansätze gibt [Müßi06, 38ff].

Als aktuell wichtiger Vertreter im Rahmen der Kosten-Nutzen-Betrachtung gilt die Berechnung des Return on Security Investment (ROSI), dessen konzeptuelle Grundlagen an der Universität von Idaho entwickelt wurden[49]. ROSI stellt eine sicherheitsbezogene Rentabilitätsbetrachtung in Anlehnung an das Konzept des Return on Investment (ROI) dar, ein Einführung in die Thematik anhand einer exemplarischen Berechnung ist in [Pohl06] zu finden.

Der diesbezügliche Forschungsbereich wird als **Ökonomie der Informationssicherheit** bezeichnet und ist eine vergleichsweise junge Disziplin, die in ihren Ansätzen gerade auf Grund der Schwierigkeit der Risikobewertung nicht frei ist von Kritik [Scha06, 21f]. Gleichwohl stellt sie für Unternehmen ein wichtiges Entscheidungskriterium für die Zielbildung auf Ebene des Unternehmensplans dar.

Allen Kategorien von Sicherheitsvorgaben ist gemein, dass sie auf abstrakter Ebene spezifizieren, welche Nachzustände einer globalen Meta-Aufgabe der Informationssicherheit zu präferieren sind. Die Konformität von bestimmten Teilprozessen der betrieblichen Leistungserstellung mit einer Sicherheitsnorm ist hierbei als Beispiel anzusehen. Welche konkreten Anforderungen diesbezüglich dann zu erfüllen sind, wird durch die Schutzziele der Informationssicherheit abgebildet.

5.4.3. Sicherheitsziele der Geschäftsprozessebene

Geschäftsprozessmodelle stellen die Innensicht eines betrieblichen Systems als Menge von Haupt- und Serviceprozessen dar. Entsprechende Sicherheitsziele nehmen daher konkreteren Bezug auf die betriebliche Leistungserstellung, als die vergleichsweise allgemeinen definierten Sicherheitsziele auf Ebene des Unternehmensplans. Komplementär zur Aufgabensicht der

[49] Vgl. hierzu [Beri02].

zweiten Ebene der Unternehmensarchitektur, nehmen sie als **Schutzziele** Bezug auf die in Geschäftsprozessen verarbeitete Information als Asset des jeweiligen Bezugsobjektes.

5.4.3.1. Der Begriff des Schutzziels

In der Literatur werden für Schutzziele in Abhängigkeit von der Betrachtungsweise unterschiedliche Begrifflichkeiten verwendet. Das BSI spricht allgemein gehalten über „Grundwerte der Informationssicherheit“ [BSI08a, 8], aus Sicht des Software- Engineering wird häufig der Begriff „Security Requirements“ [Fire03, 53], „Sicherheitsanforderungen“ [FrDa93, 10] oder „Security Objectives“ [CC06, 55] verwendet. Weitere geläufige Begriffe sind „Sicherheitsaspekte“ [HoPr03, 24] oder „dimensions of security“ [Bas+01, 29].

Das dieser Arbeit zu Grunde liegende Verständnis orientiert sich in Anlehnung an [Ecke06, 6] und [Hein99b, 1078] an einer zielorientierten Interpretation. Als Ziel kann allgemein betrachtet ein gewünschter Zustand verstanden werden, der, in der Zukunft liegend, als Resultat einer Aufgabendurchführung entsteht. Im Kontext der Informationssicherheit stellt die Zielerreichung eines konkreten Schutzziels einen solchen Zustand dar, den ein Bezugsobjekt zu erreichen hat und dessen Erhalt aus Sicherheitsgründen zu schützen ist.

Als „klassische Schutzziele“ [FePf00, S. 708] der Informationssicherheit werden in der Literatur **Vertraulichkeit** (engl. *confidentiality*), **Integrität** (engl. *integrity*) und **Verfügbarkeit** (engl. *availability*) geführt. In gewissem Maße datentechnisch orientiert, jedoch im Kern allgemeingültig darstellbar, wurden diese Schutzziele bereits 1980 durch das U.S. Department of Commerce im Rahmen eines Standardisierungsprozesses eingeführt [NBS80, 6]. Seitdem bilden sie als Tripel mit dem vielsagenden Akronym „C I A“ die Grundlage diverser Erörterungen zu diesem Thema. Eine verbreitete Erweiterung der klassischen Schutzziele erfolgt oftmals im Hinblick auf die Berücksichtigung geschäftlicher Transaktionen durch die Hinzunahme des Ziels **Verbindlichkeit** (engl. *liability*) [Röh+00, 500]. Diese vier Schutzziele sind zum aktuellen Zeitpunkt als in der Literatur gängig zu betrachten [HoPr03, 25], sie werden im Folgenden als **Schutzzielklassen** bezeichnet.

5.4.3.2. Aufbau eines Definitionsrahmens für Schutzziele

Die Beschreibung von Schutzzielklassen bildet eine wichtige Grundlage für das Verständnis der betrieblichen Informationssicherheit. Ihre Definition und somit implizit ihre Interpretation in Bezug auf einen bestimmten betrieblichen Kontext zieht weitreichende Auswirkungen nach

sich, beispielsweise im Hinblick auf die Auswahl einer bestimmten Sicherheitsmaßnahme zur Erreichung des gewünschten Schutzziels. In der Literatur bildet diesbezüglich oftmals das Subjekt/Objekt-Prinzip, entweder in Reinform oder begrifflich abgewandelt, die definitorische Grundlage[50]. Für eine ganzheitliche Betrachtung des Themenkomplexes sowie eine konsistente Definition und Abgrenzung der Schutzzielklassen, greift dieser Ansatz jedoch zu kurz. Im Folgenden wird daher ein erweiterter Definitionsrahmen auf Basis dieses Prinzips vorgestellt.

Subjekt/Objekt-Prinzip

Das Subjekt/Objekt-Prinzip ist ein Ansatz, mit dessen Hilfe Zugriffsstrukturen zwischen Nutzern (Subjekte) und Daten (Objekte) eines Systems verdeutlicht werden. Es hat seinen Ursprung im **Konzept des Referenz-Monitors**, einem frühen Architekturentwurf für die Konstruktion sicherer Anwendungssysteme[51]. Diesem Konzept folgend, werden Systeme als eine Menge von Subjekten und Objekten dargestellt, deren erlaubte Beziehungen in einer Datenbasis beschrieben sind und deren Einhaltung durch eine aktive Systemkomponente, dem Referenz-Monitor, gewährleistet wird [Weck93, 148]. Als **Objekte** werden alle Daten und datenverarbeitenden Komponenten eines Anwendungssystems bezeichnet. Diese sind differenzierbar in passive Objekte, etwa Dateien oder Datenbankeinträge, sowie aktive Objekte, wie Systemprozesse oder Anwendungsfunktionen. **Subjekte** bezeichnen die Nutzer eines Anwendungssystems, egal ob es sich um personelle Anwender oder maschinelle Nutzer (externe Anwendungssysteme) handelt, die über entsprechende Schnittstellen auf das System zugreifen. Weiterhin als Subjekte bezeichnet werden die systeminternen Prozesse, die im Auftrag von externen Nutzern im System ausgeführt werden. Objekte sind somit dem Anwendungssystem zuzuordnen, Subjekte dessen Umwelt.

Erfolgt eine Interaktion zwischen einem Subjekt und einem Objekt, so dass ein Informationsfluss zwischen beiden Elementen stattfindet, so spricht man von einem **Zugriff**. Im Kontext der Informationssicherheit sind diese Zugriffe zu kontrollieren, indem Zugriffsrechte für Objekte zu definieren und an entsprechende Subjekte zu vergeben sind [Ecke06, 3f]. Dies erfolgt durch entsprechende Einträge in einer Autorisierungs-Datenbank, die Überwachung zur Laufzeit sowie die Protokollierung der Zugriffsversuche wird durch die Komponente des Referenz-Monitors realisiert.

---

[50] Vgl. hierzu [Lip+92, 369f], [Pohl04, 679f] oder [Kers95, 75ff].

[51] Vgl. hierzu [Ande72].

Wie aus der Darstellung ersichtlich, werden bei der Definition von Schutzzielen anhand des Subjekt/Objekt-Prinzips diese Ziele ausschließlich auf die Informationen eines Systems, somit dessen Objekte, bezogen. Die entsprechenden Definitionen wirken in der Folge stark einschränkend auf die grundlegende Semantik der Schutzziele und in der Konsequenz negativ auf deren Anwendbarkeit in Bezug auf komplexe Prozesse im Rahmen von betrieblichen Informationssystemen. Zum Beispiel ist das Schutzziel der Vertraulichkeit nach dem Subjekt/Objekt-Prinzip darstellbar in Bezug auf den Schutz des Inhaltes einer übermittelten Nachricht vor unbefugter Einsichtnahme Dritter. Der Schutz der Aktion der Nachrichtenübermittlung an sich, etwa die Geheimhaltung eines E-Mail-Versandes, ist jedoch im Rahmen dieser Definition nicht abzubilden.

Um diese semantischen Einschränkungen aufzuheben, erfolgt eine Erweiterung des Subjekt/Objekt-Prinzips zu einem **Definitionsrahmen** für eine ganzheitliche Beschreibung von Schutzzielen. Die bisherige strukturorientierte Sichtweise, die ausschließlich Subjekte und Objekte eines Systems betrachtet, wird dabei zum einen um eine verhaltensorientierte Perspektive ergänzt und zum anderen, in Bezug auf die Reichweite des Konzepts, von der reinen Berücksichtigung eines Anwendungssystems hin zu einer ganzheitlichen Betrachtung des betrieblichen Informationssystems erweitert.

Bildung eines Definitionsrahmens für Schutzziele

Methodische Grundlage für die Bildung von Merkmalen des Definitionsrahmens bildet der Begriff des betrieblichen Informationssystems, seine Abgrenzung in Bezug auf das betriebliche Objektsystem sowie dessen Interpretation unter den Gesichtspunkten der allgemeinen Systemtheorie.

Die Aufgabenebene des Informationssystems besteht aus Informationsverarbeitungsaufgaben, die durch Informationsbeziehungen miteinander verbunden sind. Ebenfalls durch Informationsbeziehungen verbunden sind die Elemente der Aufgabenträgerebene, die in maschinelle und personelle Aufgabenträger unterschieden werden. Zwischen Aufgaben- und Aufgabenträgerebene bestehen Zuordnungsbeziehungen, die Aufgaben bestimmten Aufgabenträgern zuordnen. Basierend auf dieser Abgrenzung können **Aufgaben**, **Aufgabenträger** und **Aufgabenobjekte** als sicherheitsrelevante Elemente des betrieblichen Informationssystems identifiziert werden, die als Merkmale des Definitionsrahmens herangezogen werden können.

Ein weiterer Aspekt bei der Spezifizierung des Rahmens ergibt sich durch die Betrachtung des betrieblichen Informationssystems aus der Sicht der Systemtheorie. Hiernach besteht ein System aus Elementen und Beziehungen zwischen diesen Elementen und ist beschreibbar durch die Angabe seiner Struktur und seines Verhaltens [FeSi08, 13f]. Die oben identifizierten Elemente stellen demnach die Strukturansicht des betrieblichen Informationssystems dar, das Verhalten wird hierbei jedoch noch nicht berücksichtigt und ist zur Vervollständigung des Definitionsrahmens zu ergänzen.

Die verhaltensorientierte Sichtweise ist ableitbar aus den Charakteristika des allgemeinen Aufgabenbegriffs, speziell dem Aufgabenmerkmal der zielorientierten Verrichtung [Kosi76, 43]. Dieses beschreibt die eigentliche Durchführung einer Aufgabe, die, durch Ereignisse ausgelöst, in der Ausführung eines Lösungsverfahrens auf einem Aufgabenobjekt besteht [FeSi08, 97]. Dieser Sachverhalt wird auch als **Vorgang** bezeichnet und bildet als Merkmal die verhaltensorientierte Perspektive des Definitionsrahmens ab. Auf Grund der inhaltlichen Übereinstimmung mit dem oben definierten Merkmal Aufgabe, wird dieses durch das Merkmal Vorgang ersetzt. Im Ergebnis können die drei Definitionsmerkmale **Aufgabenträger**, **Aufgabenobjekt** und **Vorgang** identifiziert werden, die wie folgt zu dem Subjekt/Objekt-Prinzip in Beziehung gesetzt werden können.

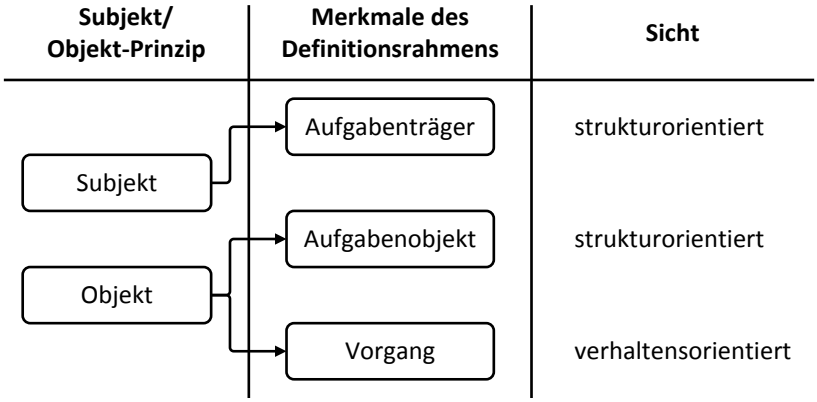

Abbildung 21: Merkmale des Definitionsrahmens für Schutzziele

Ein Subjekt korrespondiert unmittelbar mit dem **Merkmal Aufgabenträger**. Im Kontext der Informationssicherheit wird dabei unterschieden zwischen Personen, Anwendungssystemen (AWS) und Hardware (HW), auf denen die Anwendungssysteme betrieben werden.

Ein Objekt kann je nach Sichtweise abgebildet werden auf die Merkmale Information und Aufgabe, da sie, wie oben beschrieben, die Daten und datenverarbeitenden Komponenten

eines System repräsentieren. Um die semantische Eindeutigkeit der Merkmale zu wahren ist diese Mehrfachzuweisung jedoch nicht sinnvoll zu verwenden. Es erfolgt daher eine inhaltliche Differenzierung anhand der Unterscheidung von Außen- und Innensicht einer betrieblichen Aufgabe.

Die Außensicht einer Aufgabe spezifiziert das Aufgabenobjekt, auf dem die Aufgabe operiert, Ziele der Aufgabe sowie Vor- und Nachereignisse. Das Merkmal Information entspricht in dieser Sichtweise dem Aufgabenobjekt, auf dem die Aufgaben eines betrieblichen Informationssystems operieren. Diese Sichtweise korrespondiert primär mit der strukturorientierten Perspektive des Definitionsrahmens. Die Innensicht einer Aufgabe hingegen definiert das operative Lösungsverfahren der Aufgabe, somit den Ablauf des eigentlichen Verrichtungsvorgangs [FeSi08, 97]. Sie ist somit der verhaltensorientierten Perspektive zuzuordnen.

Aus dem Blickwinkel der Informationssicherheit ist in diesem Zusammenhang das Aufgabenobjekt einer Aufgabe, somit die Information, als relevantes Bezugsobjekt der Außensicht zu betrachten, da Informationen diejenigen Daten des betrieblichen Informationssystems definieren, für die bestimmte Schutzziele anzugeben sind. Aus strukturorientierter Sicht ist das Konzept des Objekts somit auf das **Merkmal Aufgabenobjekt** abzubilden.

Das **Merkmal Vorgang** deckt schließlich den sicherheitsrelevanten verhaltensorientierten Aspekt der betrieblichen Aufgabe ab. In Kombination mit dem Merkmal Information erfolgt somit eine vollständige Abbildung des Objektkonzepts auf das Konzept der betrieblichen Aufgabe aus Sicht der Informationssicherheit. Im Ergebnis wird somit das Konstrukt der Aufgabe nicht als designiertes Merkmal des definitorischen Rahmens benötigt, da es strukturorientiert durch das Merkmal Information und verhaltensorientiert durch das Merkmal Vorgang differenziert Berücksichtigung findet.

Ein Definitionsrahmen für Schutzziele

Die dargestellten Merkmale **Aufgabenobjekt**, **Aufgabenträger** sowie **Vorgang** bilden zusammen einen Rahmen, der eine Betrachtung unter verschiedenen Blickwinkeln sowie eine Systematisierung von Schutzzielen ermöglicht. Anhand der Merkmale kann überprüft werden, ob diesbezüglich sinnvolle Interpretationen von Schutzzielen gegeben sind und ob sich durch den einhergehenden Wechsel der Perspektive inhaltliche Änderungen im Verständnis der Schutzziele ergeben. Die folgende Abbildung zeigt den Aufbau des Definitionsrahmens mit den differenzierten Merkmalen.

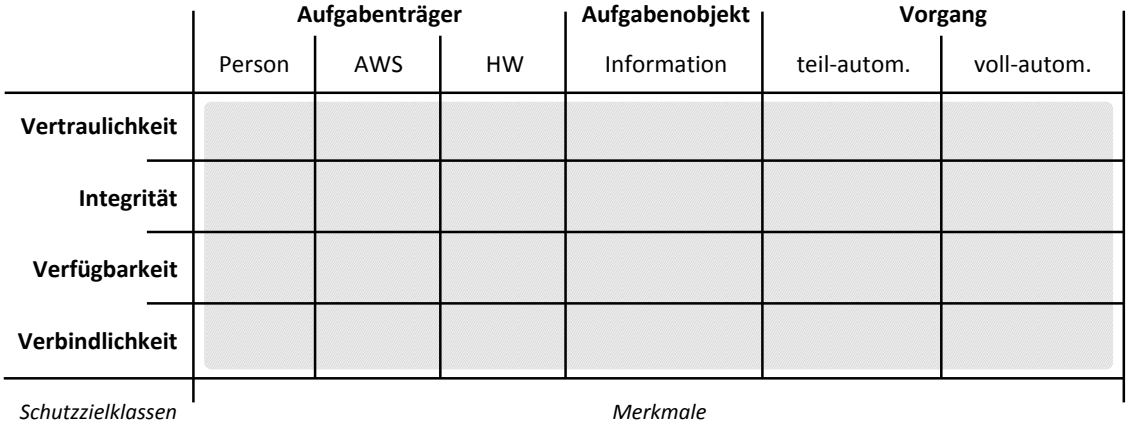

Abbildung 22: Ein Definitionsrahmen für Schutzziele

Das Merkmal **Aufgabenträger** subsumiert personelle und maschinelle Aufgabenträger. Unter personellen Aufgabenträgern werden sowohl realweltliche Nutzer eines Anwendungssystems verstanden, als auch deren virtuelle Repräsentation in Form von Kennungen, Rechten und Rollen. Maschinelle Aufgabenträger beziehen sich primär auf betriebliche Anwendungssysteme, können jedoch auch als entsprechende Basismaschinen wie Betriebssysteme oder Hardwareelemente verstanden werden. Das Merkmal **Aufgabenobjekt** bezieht sich im vorliegenden Kontext auf die im Rahmen einer Aufgabe verarbeiteten Informationen. Das Merkmal **Vorgang** nimmt, wie beschrieben, Bezug auf die konkrete Durchführung einer Aufgabe. Hierbei wird zusätzlich differenziert zwischen teilautomatisierten Vorgängen, somit Aufgaben die kooperativ von einer Person und einem Anwendungssystem durchgeführt werden und voll-automatisierten Vorgängen, die ausschließlich durch Anwendungssysteme durchgeführt werden [FeSi08, 215].

Analyse von Schutzzielen

Bei der Nutzung des Definitionsrahmens gilt zu beachten, dass nicht zwingend alle Ziele für jedes Merkmal sinnvoll beschreibbar sind. Das Schutzziel Integrität zum Beispiel ergibt in Bezug auf das Kriterium personeller Aufgabenträger realweltlich betrachtet wenig Sinn. Es gilt zudem, dass die grundlegende Bedeutung eines Schutzziels bei unterschiedlichen Merkmalsausprägungen naturgemäß erhalten bleibt. Gleichwohl werden durch den Perspektivenwechsel zwischen den Merkmalen semantische Abhängigkeiten zwischen den Zielen deutlich, sowie neue, nur auf bestimmte Merkmale bezogene, Unterziele aufgedeckt. Eben dieser Wechsel ermöglicht im Weiteren eine bessere Identifikation von Sicherheitsmaßnahmen, durch deren Einsatz Schutzziele umgesetzt werden. Bezogen auf das Beispiel des E-Mail-

Versandes ermöglicht eine Betrachtung nach dem Merkmal Vorgang etwa die Einforderung der Vertraulichkeit für den gesamten Kommunikationsvorgang. Erst durch diesen Perspektivenwechsel wird deutlich, dass für diese Anforderung zusätzliche Sicherheitsmaßnahmen notwendig wären, als zum Beispiel der ausschließliche Einsatz von kryptografischen Verfahren zur reinen Absicherung des Kommunikationsinhaltes.

Ein weiterer Aspekt, der sich bei der Analyse der Schutzziele eine Rolle spielt, ist die Unterscheidung, welche Personengruppen als befugt und welche als unbefugt zu betrachten sind. Die Erteilung von Befugnissen erfolgt zum Beispiel dadurch, dass der Sender einer E-Mail eine weitere Person als zusätzlichen Empfänger angibt, sie somit als befugt ansieht, die Nachricht zu lesen. Befugnisse werden somit durch intentionales Verhalten einer entscheidungsberechtigten Person definiert oder aber durch Berechtigungskonzepte, wie sie etwa in Anwendungssystemen durch Rechte und Rollen abgebildet werden. Die Art und Weise der Erteilung von Befugnissen, Rechtekonzepte oder auch Rollenhierarchien, sind dabei in hohem Maße geprägt von den Organisationsstrukturen eines Unternehmens bzw. deren Umsetzung in betrieblichen Anwendungssystemen. Die Frage welche Personengruppen nun berechtigt sind oder auch nicht, wird daher im Folgenden nicht weiter betrachtet. Falls benötigt, finden bei der Beschreibung der Schutzziele exemplarisch die zwei abstrakten Gruppen von Befugten und Unbefugten Verwendung.

Die Beschreibung und Klassifikation von Schutzzielen erfolgt in der Literatur oftmals im Hinblick auf konkrete Aufgabenstellungen bzw. Forschungsinteressen der jeweiligen Autoren [WoPf99, 114]. Der vorgestellte Definitionsrahmen erlaubt zwar eine vergleichsweise generische Analyse von Schutzzielen, strebt jedoch nicht an, eine allgemeingültige Spezifizierung und Systematisierung von Schutzzielen aufzustellen, die allen Bereichen und Sichtweisen genügt. Er dient im Rahmen dieser Arbeit ausschließlich als methodisch fundiertes Konstrukt zur systematischen Einführung und Definition von Schutzzielen. Als Grundlage der inhaltlichen Beschreibung der Schutzziele in den folgenden Abschnitten fungiert dabei der Aufgabentypus der Kommunikationsaufgabe am Beispiel einer E-Mail-basierten Übermittlung von Informationen zwischen einem Sender und einem Empfänger.

5.4.3.3. Definition von Schutzzielen

Die folgenden Abschnitte stellen die in dieser Arbeit verwendeten Definitionen bzw. Interpretationsmöglichkeiten der Schutzzielklassen auf Basis der spezifizierten Merkmale vor. In Ka-

pitel 5.4.3.4 erfolgt im Anschluss die integrierte Darstellung der Schutzziele anhand des Definitionsrahmens. Die allgemeinen definitorischen Grundlagen bilden Einschätzungen aus Publikationen des BSI, insbesondere den IT-Grundschutz-Katalogen [BSI09] und den Information Technology Security Evaluation Criteria (ITSEC) [BSI91].

Vertraulichkeit

Unter Vertraulichkeit wird im Allgemeinen der Schutz von Informationen vor unbefugter Preisgabe verstanden [BSI09, 56]. Im Rahmen des E-Mail-Versandes besagt dies, dass keine Person außer Sender und Empfänger der Nachricht Kenntnis der übermittelten Informationen erlangen darf. Im Hinblick auf den Definitionsrahmen beinhaltet die dargestellte Definition implizit die Ausrichtung auf das Merkmal Aufgabenobjekt. In ähnlicher Weise kann das Schutzziel der Vertraulichkeit jedoch auch bezüglich der Merkmale Aufgabenträger und Vorgang interpretiert werden.

Hinsichtlich des Merkmals Aufgabenträger bedeutet Vertraulichkeit, dass die Identität der Aufgabenträger, im Beispiel somit die des Senders und des Empfängers, gegen unbefugte Kenntnisnahme zu schützen ist. Unter **Identität** wird in diesem Zusammenhang eine Sammlung für eine natürliche Person charakterisierender Attribute verstanden [Hühn08, 161], deren Ausprägung diese Person realweltlich eindeutig identifizieren. Die realweltliche Identität eines Aufgabenträgers wird im Folgenden als **natürliche Identität** bezeichnet. Im Bereich der Informationsverarbeitung werden diese Eigenschaften in der Regel in Form eines Benutzerprofils hinterlegt, man spricht dann von einer **virtuellen Identität** [Wörn03, 7f]. Betrachtet man den Grad der Vertraulichkeit der Identitäten zwischen zwei Kommunikationspartnern, so sind Abstufungen identifizierbar, die im Folgenden als eigenständige Schutzziele eingeführt werden.

Das Schutzziel **Anonymität** (engl. *anonymity*) besagt, dass die Identität eines Aufgabenträgers bei der Nutzung von Diensten oder Ressourcen von Dritten nicht erfasst werden kann (Vertraulichkeit der Identität) [WoPf00, 175]. Das Schutzziel bezieht sich dabei auf den Schutz vor Offenbarung sowohl bezüglich der virtuellen Identität eines Aufgabenträgers als auch bezüglich der diese Identität nutzenden natürlichen Person. Unter **Pseudonymität** (engl. *pseudonymity*) wird eine abgestufte, schwächere Form der Anonymität verstanden. Sie besagt, dass prinzipiell eine Aufgabendurchführung ohne Identitätspreisgabe erfolgen kann, jedoch bleibt diese gegenüber Dritten der virtuellen Identität des Nutzers zurechenbar [WoPf00,

175]. Anonymität hat somit zum Ziel, sowohl die virtuelle als auch die natürliche Identität eines Aufgabenträgers zu schützen wohingegen Pseudonymität nur dessen natürliche Identität gegenüber Dritten absichert. Ein anonymer E-Mail-Versand erfolgt somit ohne Angabe eines Absenders und ohne technische Rückverfolgungsmöglichkeiten zu dem Sender, sodass keine Aufdeckung der virtuellen und damit auch kein Rückschluss auf die natürliche Identität erfolgen kann. Pseudonymität ist gegeben, wenn zwar die Angabe einer virtuellen Identität als Absender erfolgt, jedoch die technische Rückverfolgung keinen Rückschluss auf dessen natürliche Identität zulässt.

In Bezug auf das Merkmal Vorgang bedeutet Vertraulichkeit, dass die Aufgabendurchführung an sich durch Dritte nicht erkannt wird. Es ist in diesem Fall sicherzustellen, dass der Versand einer E-Mail nicht beobachtet oder belegt werden kann. Das sich aus dieser Vertraulichkeitsperspektive ergebende, eigenständige Schutzziel wird als **Unbeobachtbarkeit** (engl. *unobservability*) bezeichnet [WoPf99, 115]. Es ist sowohl für automatisierte als auch für teilautomatisierte Vorgänge sinnvoll zu interpretieren. Im Rahmen der vorliegenden Arbeit wird die Vertraulichkeit eines Vorgangs im Kontext betrieblicher Anwendungssysteme weiter präzisiert. In diesem Zusammenhang wird sie auf die Ausführung bestimmter Operationen des Anwendungssystems durch einen Nutzer bezogen. Das Schutzziel der Vertraulichkeit besagt dann, das nur Befugte die Erlaubnis besitzen, eine bestimmte Operation auszuführen. Die Vertraulichkeit von Vorgängen nimmt somit direkten Bezug auf die Sicherheitsgrundfunktion der Autorisierung und Zugriffskontrolle auf Ressourcenebene[52].

Gemäß den Ausführungen in Kapitel 3.1.3.3 handelt es sich auch bei dem Schutzziel Vertraulichkeit um ein dichotom nominalskaliertes Merkmal. Entweder ist Vertraulichkeit gegeben, dann haben nur Befugte Kenntnis der Information, des Vorgangs oder des Aufgabenträgers erlangt, oder aber sie wurde kompromittiert, wodurch eine unbefugte Preisgabe erfolgt ist. Die Kenntnis über die Differenzierung in befugte und unbefugte Aufgabenträger ist somit ausschlaggebend für eine Prüfung der Zielerreichung der Vertraulichkeit. In diesem Zusammenhang findet oftmals das Konzept der Sicherheitsstufen Verwendung. Eine geordnete Menge von Sensitivitätsklassen S = {streng geheim, geheim, vertraulich, öffentlich} in Verbindung mit einer linearen Ordnung über deren Elemente (streng geheim > geheim > vertraulich > öffentlich) werden dabei sowohl zur Klassifikation von Informationen verwendet (engl.

[52] In Kapitel 7.1.3.1 wird diese Beziehung im Detail analysiert, in Kapitel 8.5 anhand eines Beispiels dargestellt.

classification), als auch zur Erteilung von diesbezüglichen Nutzungsbefugnissen an Aufgabenträger (engl. *clearance*) [Ecke06, 212][53]. Je nach Art und vor allem Umfang der Gruppierung können auf diese Weise ordinal skalierende Vertraulichkeitsstufen definiert werden. Eine Information, die als geheim klassifiziert wurde, darf somit nur von Gruppen mit der Befugnis geheim oder aber streng geheim eingesehen werden. Es gilt zu beachten, dass die durch dieses Konzept generierten Vertraulichkeitsklassen für Informationen keinen direkten Bezug zu der Zielerreichung des Schutzziels Vertraulichkeit aufweisen. Ein vollständiger Verlust der Vertraulichkeit ist auf jeder Ebene der Sicherheitsstufen möglich, wenn Aufgabenträger mit zu geringen Befugnissen Zugriff erhalten können. Die ordinale Skalierbarkeit der Vertraulichkeit durch Sicherheitsstufen dient somit ausschließlich als Strukturierungskonzept für die Abgrenzung von befugten oder unbefugten Aufgabenträgern. Das Schutzziel Vertraulichkeit bleibt im definitorischen Sinn ein binäres Schutzziel, das entweder erreicht wird oder nicht. Eine quantitative Messung des Zielerreichungsgrades, zum Beispiel in Form von Prozentangaben, ist auch unter Verwendung von ordinalen Sicherheitsstufen nicht möglich.

Integrität

Das Schutzziel **Integrität** kann in Bezug auf alle drei Beschreibungsmerkmale definiert werden, das Hauptaugenmerk im Rahmen der Informationssicherheit liegt jedoch auf dem Merkmal des Aufgabenobjekts. Integrität beschreibt hierbei den Schutz vor unbefugter Veränderung von Informationen [BSI91, 1]. Im Umkehrschluss bedeutet dies, die Sicherstellung der Korrektheit und Unversehrtheit von Informationen zu gewährleisten. Der Begriff der Information inkludiert in diesem Zusammenhang explizit zusätzliche Meta-Angaben, wie etwa Autoren oder Zeitstempel, mit denen die eigentlichen Nutzdaten angereichert sind. Eine unbefugte Änderung dieser Attribute, ebenso wie eine Verfälschung der Nutzdaten, führt zu einem Verlust der Integrität [BSI09, 50]. Von besonderer Relevanz ist dieses Schutzziel im Hinblick auf Kommunikationsbeziehungen, bei denen während der Übertragungsphase Informationen von Dritten in unzulässiger Weise manipuliert werden könnten.

Die Wahrung der Integrität von Informationen muss ebenfalls bei internen Verarbeitungsaufgaben von Aufgabenträgern Beachtung finden. Hierbei liegt der Fokus auf maschinellen Aufgabenträgern, hinsichtlich personeller Aufgabenträger ist dieses Schutzziel nicht sinnvoll zu

[53] Die dargestellte Einteilung in vier Sicherheitsstufen wurde in den 1980ern in der Trusted Computer System Evaluation Criteria (TCSEC) spezifiziert [DoD85, 72], ihre mathematisch-formale Ausarbeitung erfolgte bereits eine Dekade zuvor durch Denning [Denn76].

interpretieren. In Bezug auf betriebliche Anwendungssysteme wird unter Integrität der Schutz vor unzulässiger Manipulation von Anwendungskomponenten bzw. -funktionen verstanden, die dazu führen, dass unvollständige oder verfälschte Ergebnisse generiert werden. Man spricht in diesem Zusammenhang auch von **Programmintegrität** [Witt06, 73].

Die **Integrität eines Vorgangs** ist zunächst sinnvoll zu interpretieren und bezeichnet inhaltlich die kontinuierliche Korrektheit einer Aufgabendurchführung gemäß der jeweiligen Spezifikation. Geschieht diese Aufgabendurchführung automatisiert auf Basis eines betrieblichen Anwendungssystems, so kann dieses Integritätsziel nur dann erfüllt werden, wenn die Programmintegrität des Systems sichergestellt ist. Die Integrität eines Vorgangs ist somit direkt abhängig von der Integrität des maschinellen Aufgabenträgers, der diesen Vorgang durchführt, Programmintegrität stellt somit eine zwingende Voraussetzung dar.

Bei teil-automatisierten Vorgängen sind in diesem Zusammenhang zusätzlich Manipulationsmöglichkeiten durch personelle Aufgabenträger zu berücksichtigen. Unter diesem Aspekt muss differenziert werden, ob ein personeller Aufgabenträger durch ihm übertragene Rechte und entsprechende Funktionalität des Anwendungssystems eine Aufgabendurchführung manipuliert, oder aber, ob die Vorgangsmanipulation durch unerlaubte Modifikationen der jeweiligen Basismaschinen erfolgt. Der letztgenannte Fall ist gleichzusetzen mit einer unerlaubten Manipulation der Programmintegrität und kann demzufolge vernachlässigt werden. Im ersten Fall hingegen handelt es sich um eine Fehlkonfiguration des Systems, durch die ein Nutzer potentiell Verwaltungsrechte erhalten kann, die eine unerlaubte Änderung von Aufgabendurchführungen erlauben. In dieser Beziehung ist die **Vorgangsintegrität** somit sinnvoll belegt und im Weiteren zu berücksichtigen.

Bei den vorgestellten Definitionen der Integrität im Sinne der Informationssicherheit ist es wichtig, die begriffliche **Abgrenzung zu anderen Disziplinen** zu beachten. Insbesondere im Bereich der Automatisierung betrieblicher Informationssysteme und der Integration betrieblicher Anwendungssysteme treten hierbei teilweise inhaltliche Überschneidungen aber auch Abhängigkeiten auf. Integrität wird in diesem Zusammenhang als spezielle Form des Integrationsziels Konsistenz betrachtet und in Bezug auf Anwendungssysteme in semantische und operationale Integrität differenziert. Semantische Integritätsbedingungen geben dabei an, welche Zustände von Datenobjekten aus Sicht der Modellierung als valide zu bewerten sind, operationale Integritätsbedingungen definieren welche Systemzuständen vor und nach einem Zustandsübergang konsistent sind. Das zentrale Merkmal beider Begriffe stellt die Forderung

nach einem konsistenten System- bzw. Datenobjektzustand dar. In diesem Punkt ist das Begriffsverständnis dem des Schutzziels Integrität sehr ähnlich, geht es dabei doch um die Verhinderung unbefugter Manipulation von Vorgängen oder Informationen. Der Unterschied beider Begriffe liegt in der Intention, mit der die Einhaltung der Ziele verfolgt wird. Semantische und operationale Integrität setzen die Korrektheit, d.h. die Eindeutigkeit, Widerspruchsfreiheit und Vollständigkeit der Aufgabendefinition und -durchführung in einem Anwendungssystem voraus [Fers92, 11ff]. Sie beziehen sich somit auf den Schutz vor unbeabsichtigten Fehlern im Rahmen der Entwicklung und Integration von Anwendungssystemen und sind daher inhaltlich näher an der Sicherheitsdisziplin Safety orientiert. Integrität im Sinne der Security hingegen hat den Schutz vor unbefugter Manipulation zum Ziel. Während der Laufzeit eines Anwendungssystems kann die Wahrung des Schutzziels Integrität somit als eine Voraussetzung für eine Unterstützung des Integrationsziels Konsistenz und damit der semantischen und operationalen Integrität verstanden werden.

Verfügbarkeit

Das Schutzziel **Verfügbarkeit** kann bezüglich der Merkmale Aufgabenobjekt und Aufgabenträger definiert werden. Es wird als Schutz vor unbefugter Vorenthaltung von Informationen und Betriebsmitteln verstanden [BSI91, 1]. Verfügbarkeit ist somit gegeben, wenn Informationen und Anwendungssysteme wie vorgesehen, d.h. in zugesicherter Form und Qualität, von befugten Personen genutzt werden können [BSI09, 59] [Ecke06, 10].

Die Verfügbarkeit eines Vorgangs ist vollständig abhängig von der Verfügbarkeit der Aufgabenträger, die die Aufgabendurchführung vornehmen. Dies gilt sowohl für teil-automatisierte als auch für voll-automatisierte Vorgänge, da in keinem der beiden Fälle eine Aufgabe durchgeführt werden kann, ohne dass zum Beispiel das relevante Anwendungssystem nutzbar ist. Die Interpretation des Schutzziels Verfügbarkeit in Bezug auf einen Vorgang ist auf Grund dieser Abhängigkeit gleichzusetzen mit der Verfügbarkeit des entsprechenden maschinellen Aufgabenträgers und wird im Weiteren nicht mehr explizit betrachtet.

Der Begriff der Verfügbarkeit ist in seiner ursprünglichen Form der Sicherheitsdisziplin Safety zuzuordnen. Er findet in diesem Bereich neben den Größen Zuverlässigkeit und Wiederherstellbarkeit als quantifizierbarer Faktor zur Bewertung der Fehlertoleranz eines Systems Verwendung. Unter Fehlertoleranz wird die Fähigkeit eines Systems verstanden, sich trotz einer begrenzten Anzahl von Fehlern spezifikationsgerecht zu verhalten. Verfügbarkeit

gibt in diesem Zusammenhang an, mit welcher Wahrscheinlichkeit ein System zu einem bestimmten Zeitpunkt korrekt funktioniert, auch wenn es vorher schon einmal ausgefallen war. Sie wird berechnet aus den Größen der MTTF als Repräsentation der Zuverlässigkeit und MTTR als Wert der Wiederherstellbarkeit [BoHe99, 417f][54]. In Abhängigkeit von den Ergebnissen lassen sich unterschiedliche Verfügbarkeitsstufen ableiten, aus denen im Umkehrschluss wiederum entsprechende erlaubte Ausfallzeiten pro Jahr berechnet werden können. Eine Verfügbarkeit von 99,9% etwa beschreibt eine maximale Ausfallzeit von ca. 8,8 Stunden pro Jahr. Verfügbarkeitsangaben in dieser Form finden oftmals in Service Level Agreements (SLA) Verwendung. Es wird deutlich, dass das Begriffsverständnis in diesem Bereich der Safety primär auf die Funktionssicherheit eines maschinellen Aufgabenträgers abzielt, somit dem Schutz vor unbeabsichtigten Fehlern wie zum Beispiel dem Ausfall einer Festplatte. Diese Betrachtungsweise ist zu differenzieren von dem Blickwinkel der Security, der dieser Arbeit zu Grunde liegt. Unter Verfügbarkeit wird hierbei der Schutz vor intentionaler Beeinträchtigung der Nutzbarkeit verstanden, etwa durch absichtliche Überlastung eines Anwendungssystems, so dass keine Anfragen weiterer Nutzer bedient werden können [Goll01, 7f]. Die Verfügbarkeit im Sinne der Safety und damit implizit die Berücksichtigung von Ausfällen der Hardware oder anderer technischer Infrastruktur, wird im weiteren Verlauf der Arbeit aus den dargelegten Gründen nicht weiter betrachtet. Das vorliegende Begriffsverständnis bezieht sich somit primär auf die Sicherstellung der Nutzbarkeit von Anwendungssystemen und der entsprechenden Informationen.

Verbindlichkeit

Das Schutzziel **Verbindlichkeit** besagt, dass ein Aufgabenträger die Durchführung einer Aufgabe im Nachhinein nicht abstreiten kann [Ecke06, 11]. In Bezug auf das Beispiel des E-Mail-Versandes wird somit eine zurechenbare und rechtsverbindliche Kommunikation zwischen Sender und Empfänger gefordert [Pohl04, 680]. Bereits aus der einführenden Definition wird ersichtlich, dass das Schutzziel Verbindlichkeit insbesondere bezüglich der Merkmale Vorgang und Aufgabenträger belegt ist. Wie im folgenden Abschnitt näher ausgeführt wird, ergeben sich bei detaillierter Analyse der genannten Merkmale zwei weitere Schutzziele. In Bezug auf das Merkmal der Aufgabenträger ist dies die **Authentizität** (engl. *authentcity*), im Hinblick auf Vorgänge die **Nichtabstreitbarkeit** (engl. *non-repudiation*). Verbindlichkeit

[54] Vgl. hierzu Kapitel 2.3.1.

kann somit als Zusammenfassung der Schutzziele Authentizität und Nichtabstreitbarkeit interpretiert werden [BSI09, 56].

Die **Nichtabstreitbarkeit** eines Vorgangs bedeutet, dass die Durchführung einer Aufgabe nicht in Abrede gestellt werden kann. Es wird weiterhin unterschieden zwischen der Nichtabstreitbarkeit der Herkunft und der Nichtabstreitbarkeit des Erhalts. In Bezug auf das Beispiel des E-Mail-Versandes besagt dies, dass weder das Absenden noch das Erhalten einer Nachricht durch die jeweiligen Aufgabenträger bestritten werden kann [BSI09, 52]. Überführt man diese Betrachtung verallgemeinernd in den Kontext der betrieblichen Aufgabe, so beziehen sich die Forderungen der Nichtabstreitbarkeit auf die Nachweisbarkeit der Existenz von Vor- bzw. Nachereignissen einer Aufgabe. Diese Nachweisbarkeit (engl. *accountability*) wird in einigen Veröffentlichungen als Synonym des Schutzzieles Nichtabstreitbarkeit oder als eigenes Schutzziel definiert [Goll01, 8] [HoPr03, 25]. Die vorliegende Arbeit folgt dieser Einschätzung hingegen nicht, vielmehr wird Nachweisbarkeit als Eigenschaft eines Systems interpretiert, die sicherstellt, dass Vorgänge und Zustandsübergänge über den Zeitverlauf hinweg nachvollziehbar bleiben [Shir07, 12] [Kail96, 315]. Die Nachweisbarkeit ist somit als grundlegende Systemeigenschaft zu interpretieren, die auf Ressourcenebene anzusiedeln ist. Sie wird daher nicht als eigenständiges Schutzziel betrachtet.

Das Schutzziel **Authentizität** bezieht sich auf die Echtheit von Aufgabenträgern. Sie ist gewährleistet, wenn sichergestellt ist, dass ein Aufgabenträger tatsächlich die Identität besitzt, die er vorgibt zu haben [BSI09, 45]. In Bezug auf Nutzer von betrieblichen Anwendungssystemen erfolgt diese Prüfung in der Regel im Rahmen von Anmeldeprozessen. Hierbei kann die erfolgreiche Annahme einer virtuellen Identität erst dann erfolgen, wenn charakterisierende Eigenschaften einer natürlichen Identität, wie etwa ein Passwort oder biometrische Merkmale, nachgewiesen worden sind. Ein ähnlicher Sachverhalt besteht bei maschinellen Aufgabenträgern, wie etwa Anwendungssystemen oder technischen Komponenten wie WLAN AccessPoints. Auch hier ist in bestimmten Fällen die Authentizität nachzuweisen, insbesondere wenn es sich um voll-automatisierte Aufgabendurchführungen mit mehreren beteiligten maschinellen Aufgabenträgern handelt. Der Austausch charakterisierender Eigenschaften sowie die Echtheitsprüfung erfolgt hier in der Regel automatisiert auf Basis von Zertifikaten, die die Identität einer Maschine repräsentieren [Ecke06, 7]. In Bezug auf Anwendungssysteme bzw. integrierte Geräte wird diese Form der Authentizität in der vorliegenden Arbeit nicht weiter betrachtet.

Die bisher dargestellten Definitionen der Nichtabstreitbarkeit und Authentizität beziehen sich primär auf die Verbindlichkeit von Vorgängen und personellen Aufgabenträgern. Die **Verbindlichkeit von Aufgabenobjekten** ist in diesem Zusammenhang differenziert zu betrachten.

Informationen, die zwischen verschiedenen Parteien ausgetauscht werden, gelten dann als verbindlich, wenn sie Gültigkeit in Bezug auf bestimmte Szenarien im Sinne der beteiligten Parteien besitzen. Die Informationen dokumentieren somit valide Willenserklärungen im rechtlichen Sinne. Ein elektronisch übermitteltes Angebot im Rahmen eines Bestellprozesses zum Beispiel, kann eine solche Willenserklärung darstellen oder aber ein Vertrag, der durch Übereinkunft, somit gleichgerichteten Willenserklärungen, zustande kommt. Die Forderung der Verbindlichkeit im Rahmen der Informationssicherheit besagt in diesem Fall, dass die übermittelten Willenserklärungen gegenüber Dritten beweisbar sein müssen. Ist dieser Beweis vor Gericht zu erbringen, spricht man auch von Rechtsverbindlichkeit als Schutzziel [Herr01, 123]. In der vorliegenden Arbeit wird dieser Fall als Spezialform angesehen, da die dritte Partei gegenüber der ein Beweis erbracht werden muss, auf offizielle Organe der Judikative eingeschränkt wird. In der realweltlichen Betrachtung stellt dies zwar die ultima ratio dar, im geschäftlichen Umfeld kann jedoch auch die Verbindlichkeit gegenüber anderen Parteien, wie etwa Lieferanten, eine Rolle spielen. Rechtsverbindlichkeit wird aus diesem Grund unter dem allgemeinen Begriffsverständnis der Verbindlichkeit subsumiert.

Aus Sicht der Informationssicherheit bilden analog zur Verbindlichkeit von Vorgängen die Authentizität und Nichtabstreitbarkeit die Grundlage für die Verbindlichkeit von Informationen. Gleichwohl muss zusätzlich sichergestellt werden, dass die verbindlichen Informationen bei elektronischer Übermittlung nicht unbefugt manipuliert wurden. Diese Anforderung wird durch die zusätzliche Berücksichtigung des Schutzziels Integrität erfüllt. Die Verbindlichkeit von Informationen ist somit dann gegeben, wenn die Aufgabendurchführung nicht abstreitbar, demzufolge die Authentizität der beteiligten Aufgabenträger sichergestellt und wenn die Integrität der Informationen im Rahmen der Übermittlung gewährleistet ist [Kers95, 77].

5.4.3.4. Schutzziele anhand des Definitionsrahmens

Anhand des Definitionsrahmens können die vorgestellten Schutzziele der Informationssicherheit zusammengefasst dargestellt werden.

Merkmale ▷ / *Schutzziel-klassen* ▽	Aufgabenträger			Aufgabenobjekt	Vorgang	
	Person	AWS	HW	Information	teil-autom.	voll-autom.
Vertraulichkeit	Anonymität	-	-	Vertrau-lichkeit	Unbeobacht-barkeit	Unbeobacht-barkeit
Integrität	-	Programm-integrität	-	Integrität	Vorgangs-integrität	AWS
Verfügbarkeit	-	Verfügbarkeit		Verfügbarkeit	AWS / HW	AWS / HW
Verbindlichkeit	Authentizität			Verbind-lichkeit	Nichtab-streitbarkeit	Nichtab-streitbarkeit

Abbildung 23: Systematik der Schutzziele

Die Reihen des Definitionsrahmens werden durch die allgemeinen Schutzzielklassen spezifiziert. Die Schutzziele, deren Definition sich für ein konkretes Merkmal sinnvoll darstellen lassen, sind in den jeweiligen Feldern verzeichnet. In diesem Sinne geben die belegten Felder somit Instanzen der jeweiligen Schutzzielklasse wider, die in Bezug auf das entsprechende Merkmal zu verfolgen sind. Felder mit hellgrauer Markierung sind zwar im Kontext der Sicherheit interpretierbar, werden jedoch im Rahmen der vorliegenden Arbeit nicht weiter betrachtet. Die Gründe hierfür sind im Rahmen der Diskussion in Kapitel 5.4.3.3 beschrieben. Dunkelgrau hinterlegte Felder sind prinzipiell durch eine Instanz einer Schutzzielklasse sinnvoll belegt, werden jedoch durch die Schutzzieldefinition eines anderen Merkmals in der entsprechenden Klasse hinreichend abgedeckt. Diese Schutzziele werden ebenfalls im weiteren Verlauf der Arbeit nicht berücksichtigt und unter den jeweils übergreifenden Schutzzielen subsumiert. Entsprechende Referenzen sind in den jeweiligen Feldern angegeben.

Die Spalte Aufgabenobjekt verdeutlicht den gewählten Systematisierungsansatz im Hinblick auf die gängige Fokussierung der Schutzziele auf Informationen. Alle Felder sind belegt und entsprechen in ihren Ausprägungen den Benennungen der Schutzzielklassen, so wie sie in der Regel in der Literatur eingeführt und interpretiert werden. Es wird jedoch auch deutlich, dass viele Instanzen der Schutzzielklassen sich erst durch einen Wechsel des Merkmals ergeben. Diese Schutzziele werden in manchen Veröffentlichungen dann entweder nicht betrachtet oder aber ohne Begründung analog zu den Instanzen Vertraulichkeit, Verbindlichkeit, Verfügbarkeit und Integrität positioniert[55].

[55] Vgl. hierzu zum Beispiel [Schi99, 25ff] oder [Swo+08, 14ff].

Eine klassifizierende Differenzierung ist daher als durchaus sinnvoll anzusehen, da hierdurch ein Rahmen etabliert wird, in dem neue Ansätze und Perspektiven auf einfache Weise integrierbar sind. Definitorische Mehrdeutigkeiten werden somit vermieden und die Instanzen der Schutzziele werden in Bezug auf ihre konkrete Nutzung, zum Beispiel im Rahmen der Geschäftsprozessmodellierung, einfacher operationalisierbar.

An dieser Stelle werden bereits Zusammenhänge und Abhängigkeiten zwischen verschiedenen Schutzzielen deutlich, wie sie auch teilweise bereits in Kapitel 5.4.3.3 angesprochen wurden. Im folgenden Abschnitt werden diese Beziehungen näher betrachtet.

5.4.3.5. Beziehungen zwischen Schutzzielen

Basierend auf den Definitionen und Eigenschaften von Schutzzielen können Beziehungen zwischen ihnen identifiziert werden. Auf Grund der Komplexität des Zielsystems hinsichtlich der Kombinationsmöglichkeiten der merkmalsorientierten Sichten auf Schutzziele, ist es jedoch nicht möglich, für jeden Betrachtungskontext im Detail eine entsprechend allgemeingültige Wechselwirkung zwischen zwei Schutzzielen abzuleiten. Bestehende Ansätze fokussieren daher zum Teil auf bestimmte Anwendungsbereiche, um Beziehungen für den jeweiligen Kontext aufzuzeigen, wie zum Beispiel durch die ausschließliche Betrachtung von Kommunikationsbeziehungen [WoPf99, 123]. Allgemeingültige Wechselwirkungen zwischen Schutzzielen sind somit nur schwerlich in umfassender Weise anzugeben. In der vorliegenden Arbeit wird daher eine abstrakte Sichtweise auf Basis des eingeführten Definitionsrahmens eingenommen und anhand dessen relevante Zielbeziehungen identifiziert. Die folgenden Ausführungen zu verwendeten Beziehungstypen bilden hierzu die Grundlage.

Beziehungstypen

Als grundlegende Typen von Zielbeziehungen gelten **Komplementarität**, **Konkurrenz** und **Indifferenz** [Hein91, 14f]. Eine komplementäre Beziehung liegt vor, wenn durch die Steigerung der Zielerreichung eines Zieles Z_1 auch die von Z_2 steigt. Sinkt die Zielerreichung von Z_2 in diesem Fall hingegen, spricht man von einer konkurrierenden Beziehung. Die Beziehung wird als indifferent beschrieben, wenn keinerlei Auswirkungen zwischen den Zielerreichungsgraden von Z_1 und Z_2 bestehen [Hein99a, 1025].

Als weitere Beziehungstypen können **Abhängigkeiten** zwischen Schutzzielen identifiziert werden, die auf Basis des aussagenlogischen Konstrukts der Implikation differenzierbar sind

[TeTe07, 8f]. Eine gerichtete Beziehung von Z_1 nach Z_2 wird als **hinreichend** bezeichnet, wenn Z_1 als Voraussetzung für Z_2 gilt und wenn bei Erfüllung von Z_1 das Schutzziel Z_2 automatisch eintritt. Die Zielerfüllung von Z_2 ist dabei jedoch nicht ausschließlich von Z_1 abhängig, sondern kann auch andere Ursache haben, d.h. Z_2 kann auch ohne Z_1 eintreten. Als **notwendig** wird eine Beziehung charakterisiert, wenn Z_1 im obigen Fall der Beziehung eine Voraussetzung für die Erfüllung von Z_2 darstellt. Ohne das Vorhandensein von Z_1 kann somit Z_2 nicht erreicht werden, das Eintreten von Z_1 führt jedoch nicht zwingend zur Erfüllung von Z_2. Abhängigkeitsbeziehungen dieser Art können als Form von Mittel-Zweck-Beziehungen zwischen Ober- und Unterzielen, die in einer Zielhierarchie systematisiert sind, interpretiert werden [ThAc06, 118]. Oberziele als abhängige Schutzziele können somit nur erreicht werden, wenn die Erfüllung entsprechender Unterziele gewährleistet ist.

Wechselwirkungen zwischen Schutzzielen

In Bezug auf Schutzziele der Informationssicherheit spiegeln sich die Grundtypen der Zielbeziehungen vor allem in der Wirkungsweise und dem Wirkungsgrad von Maßnahmen wider, die zur Erreichung entsprechender Schutzziele dienen. Eine konkurrierende Zielbeziehung zwischen zwei Zielen Z1 und Z2 sagt somit aus, das die entsprechenden Maßnahmen gegenläufig wirken. Zum Beispiel stehen Maßnahmen zum Schutz der Anonymität den Aktivitäten zur Gewährleistung der Authentizität eines Aufgabenträgers diametral gegenüber. Sie haben somit in Abhängigkeit von der Ausprägung der Schutzzielbeziehung entweder einen stärkenden oder schwächenden Effekt auf die jeweils anderen Maßnahmen. Diese Beziehungen werden in der Folge als **Wirkungsbeziehungen** bezeichnet.

Abhängigkeitsbeziehungen hingegen beziehen sich primär auf die Existenz der Maßnahmen. Nur wenn entsprechende Maßnahmen eines unabhängigen Schutzziels vorhanden sind, können auch die eines abhängigen Schutzziels greifen. Bei notwendigen Abhängigkeitsbeziehungen bedeutet dies, dass eine Kompromittierung eines unabhängigen Schutzziels die Erreichung eines abhängigen Schutzziels verhindert. Bei hinreichenden Abhängigkeitsbedingungen ist dieser semantische Zusammenhang hingegen nicht anzuwenden.

Mit Ausnahme der Indifferenz, die nicht separat dokumentiert wird, finden alle dargestellten Zielbeziehungen in der folgenden Ausarbeitung Verwendung. Es ergibt sich die folgende Beziehungsstruktur der vorgestellten Schutzziele.

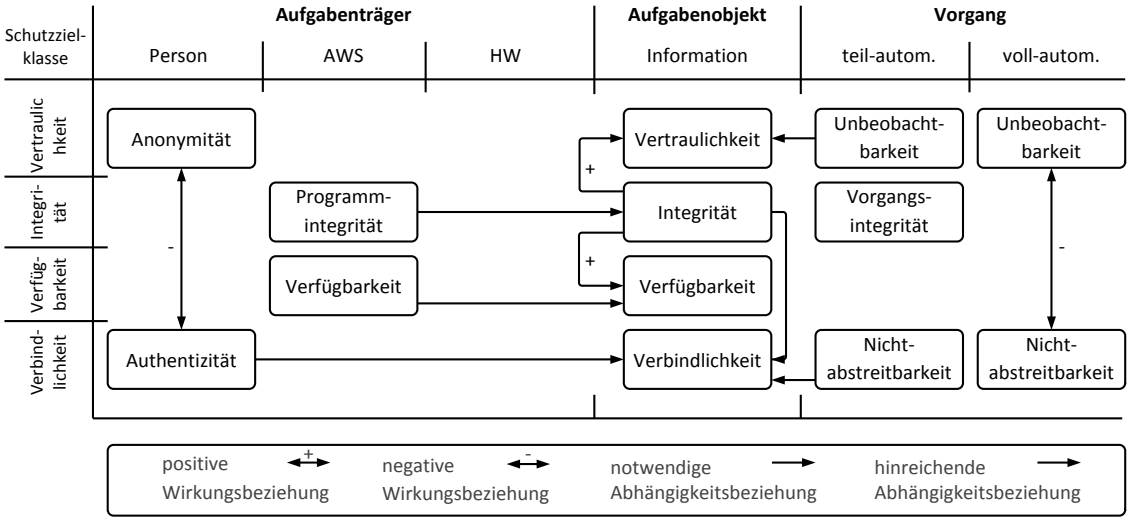

Abbildung 24: Wechselwirkungen zwischen Schutzzielen

Aus der Darstellung wird ersichtlich, dass **Wirkungsbeziehungen** ausschließlich innerhalb einer Merkmalsklasse von Schutzzielen bestehen, Abhängigkeitsbeziehungen hingegen primär zwischen den Klassen[56]. Einzig die Schutzzielklasse Integrität bildet hierbei eine Ausnahme, wobei dieser Effekt aus der Systematisierung der Schutzziele anhand des Definitionsrahmens ableitbar ist. Die Merkmale Aufgabenobjekt, Aufgabenträger und Vorgang stellen jeweils die Bezugsobjekte dar, auf die den Schutzzielen entsprechende Maßnahmen einwirken. Wirkungsbeziehungen bestehen insofern nur innerhalb einer Merkmalsklasse, als dass sich die Maßnahmen in diesem Fall auf das gleiche Bezugsobjekt beziehen. Denn nur wenn diese Gleichheit gegeben ist, kann demzufolge auch eine direkte Relation zwischen den Auswirkungen von Maßnahmen bestehen.

Abhängigkeitsbeziehungen zwischen den Klassen lassen sich ebenfalls anhand der Merkmalsbeziehungen ableiten. Im Rahmen betrieblicher Anwendungssysteme besteht zwischen Aufgabenobjekt bzw. Vorgang und Aufgabenträger eine Nutzer-Basismaschinenbeziehung. Schutzziele hinsichtlich des Merkmals Aufgabenträger als Basismaschine stellen somit in bestimmten Fällen eine notwendige Voraussetzung für die Erreichung eines Schutzziels der Nutzermaschinen dar.

[56] Die Klassifizierung von Schutzzielen erfolgt hier anhand der Merkmale des Definitionsrahmens, somit spaltenorientiert. Sie ist zu unterscheiden von der inhaltlichen Differenzierung der Schutzzielklassen in Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit.

Abhängigkeitsbeziehungen

Die oben dargestellten Charakteristika von Abhängigkeitsbeziehungen spiegeln sich insbesondere bei den Schutzzielklassen Integrität und Verfügbarkeit wider. Die Einforderung beider Schutzziele ist vergleichsweise unabhängig von dem situativen Kontext der beteiligten Parteien. Sie sind gewissermaßen Basisziele, die unabhängig von Sicherheitsanforderungen an betriebliche Transaktionen bestehen können. Ohne diese kontextbezogenen Anforderungen bestehen die grundlegenden Abhängigkeitsbeziehungen zwischen Nutzer- und Basismaschine, somit zwischen der Integrität bzw. Verfügbarkeit von Informationen und Vorgängen sowie den jeweiligen Aufgabenträgern. Dies ist exemplarisch nachvollziehbar bei dem Verlust der Verfügbarkeit eines Anwendungssystems. Alle durch das Anwendungssystem bereitgestellten Informationen sind in diesem Fall ebenfalls nicht verfügbar, es besteht somit eine notwendige Abhängigkeitsbeziehung.

Weiterhin bestehen notwendige Abhängigkeitsbeziehungen zwischen Authentizität und Verbindlichkeit sowie Nichtabstreitbarkeit und Verbindlichkeit. Wie bereits in der inhaltlichen Ausarbeitung zu Verbindlichkeit dargestellt wurde, müssen beide Schutzziele gewährleistet sein, damit Verbindlichkeit überhaupt erreicht werden kann.

Eine hinreichende Abhängigkeitsbeziehung besteht zwischen Unbeobachtbarkeit und Vertraulichkeit. Wenn eine Vorgangsdurchführung von Unbefugten an sich nicht zu bemerken ist, so sind automatisch auch die darin bearbeiteten Informationen als vertraulich zu bewerten. Dies gilt jedoch nur wenn die Menge der Befugten und Unbefugten im Zeitablauf identisch bleibt.

Als Sonderfall einer notwendigen Abhängigkeitsbeziehung gilt die Relation zwischen Integrität und Verbindlichkeit. Diese merkmalsklasseninterne Abhängigkeitsbeziehung ist primär inhaltlich motiviert und trägt der oben angeführt Definition von Verbindlichkeit Rechnung. Die Forderung nach Verbindlichkeit geht einher mit der letztendlichen Beweisbarkeit, dass eine Information mit einer entsprechenden Willenserklärung übereinstimmt. Ist die Integrität einer Information jedoch verletzt, so spiegelt diese nicht mehr die ursprüngliche Willenserklärung wider, die Verbindlichkeit der Information kann in der Konsequenz nicht mehr gegeben sein. Besteht hingegen Sicherheit über die Integrität einer Information, so kann die Information unbeanstandet als Grundlage für die Forderung der Beweisbarkeit verwendet werden.

Wirkungsbeziehungen

Inhaltlich eindeutig können wechselseitig negative Wirkungsbeziehungen zwischen Anonymität und Authentizität sowie zwischen Unbeobachtbarkeit und Nichtabstreitbarkeit identifiziert werden. Im letzten Fall zum Beispiel wirken Maßnahmen der Nichtabstreitbarkeit, wie etwa Protokollierung, der Unbeobachtbarkeit einer Aufgabendurchführung entgegen.

Eine positive Wirkungsbeziehung zwischen Integrität und Verfügbarkeit ist gegeben, da durch einen Verlust der Integrität einer Information deren Verfügbarkeit beeinträchtigt werden kann. Kommt es zu einem Integritätsverlust, so sind mehr oder minder aufwendige Rekonstruktionen notwendig, in deren Zeitspanne die Verfügbarkeit der Information potentiell nicht gewährleistet ist. Ab welchem Grad der Beeinträchtigung der Integrität die Verfügbarkeit gefährdet ist, wird somit primär durch die Einschätzung bedingt, welche Datenqualität für eine Bearbeitung notwendig ist. Es handelt sich in diesem Fall um eine gerichtete Wirkungsbeziehung. Maßnahmen zur Sicherung der Integrität erhöhen somit potentiell den Zielerreichungsgrad der Verfügbarkeit, der Umkehrschluss ist inhaltlich jedoch nicht zulässig.

Analog zu dieser Betrachtungsweise ist die positive Wirkungsbeziehung von Integrität zu Vertraulichkeit zu interpretieren. Ist die Integrität einer Information gegeben, ist davon auszugehen, dass keine unbefugte Manipulation stattgefunden hat. Eine unbefugte Einsichtnahme jedoch kann nicht ausgeschlossen werden. Umgekehrt betrachtet besagt ein Verlust der Integrität nicht zwingend den Verlust der Vertraulichkeit, da die unbefugte Änderung von Daten auch zum Beispiel durch eine fehlerhafte Übertragung erfolgt sein kann. Ein Verlust der Vertraulichkeit würde in diesem Fall nicht erfolgen. Maßnahmen der Integritätssicherung haben somit eine positive Wirkungsbeziehung zu Vertraulichkeit, es besteht jedoch keine Abhängigkeitsbeziehung.

Fazit

Wechselwirkungen zwischen Schutzzielen können grundlegend in Wirkungs- und Abhängigkeitsbeziehungen differenziert werden. In Bezug auf konkrete Szenarien sind diese Beziehungen sicherlich weiter detaillierbar, wie zum Beispiel in [WoPf99] dargestellt. Das im Vergleich hohe Abstraktionslevel der vorliegenden Ausführungen wurde jedoch gewählt, um die wesentlichen und allgemeingültigen Zusammenhänge aufzuzeigen. Die identifizierten Beziehungen beschreiben somit ausschließlich Tendenzen und grundsätzliche Auswirkungen der

Beziehungen, ohne konkrete Aussagen in Bezug auf Maßnahmen oder Zielerreichung zu treffen.

Die Relevanz der Bestimmung der Beziehungstypen hingegen ist gegeben und lässt sich aus dem oben bereits dargestellten Zusammenhang zu der Wirkungsweise entsprechender Maßnahmen ableiten. Nur wenn die Art einer Beziehung zwischen zwei Schutzzielen identifiziert ist, können auch Maßnahmen zielorientiert ausgewählt und implementiert werden, ohne dass Widersprüche bezüglich ihrer Wirkungsweise auftreten. Dies ist vor allem für den Übergang zwischen den einzelnen Ebenen der Bezugsobjekte in der Unternehmensarchitektur relevant. Insbesondere zwischen Geschäftsprozessebene und Ressourcenebene kommen diese Zusammenhänge zum Tragen, da bei diesem Schritt eine Transformation von der Schutzzielbetrachtung hin zu einer maßnahmenorientierten Betrachtung der Informationssicherheit erfolgt. Dieser Aspekt wird in Teil III der vorliegenden Arbeit erneut aufgegriffen und weiter detailliert.

5.4.3.6. Eigenschaften von Schutzzielen

Neben den Wechselwirkungen zwischen den Schutzzielen können zusätzlich weitere relevante Charakteristika identifiziert werden. Zum einen sind dies Gegensätze im **Monotonieverhalten**, zum anderen Unterschiede in der **Nachweisbarkeit** einer möglichen Beeinträchtigung der jeweiligen Schutzzielklasse.

Nachweisbarkeit von Schutzzielverletzungen

Kommt es zu einer Verletzung eines Schutzzieles, so muss diese Tatsache nicht zwingend sofort den Verantwortlichen bekannt werden. Es existieren erhebliche Unterschiede zwischen den Schutzzielklassen hinsichtlich der Art und Weise und insbesondere auch zu welchem Zeitpunkt eine Beeinträchtigung überhaupt identifiziert werden kann [Kers95, 78]. Diese beiden Aspekte werden unter dem Begriff der Nachweisbarkeit einer Schutzzielverletzung im folgenden Abschnitt näher betrachtet.

Als erster Punkt ist relevant, in welcher Form eine Überprüfung der Schutzziele erfolgen kann, sodass Verletzungen identifiziert werden können. Anhand der definierten Charakteristika der Schutzzielklassen ist ersichtlich, dass Verfügbarkeit und Integrität primär anhand direkter Attribute eines Datensatzes bzw. einer Ressource erkannt werden können, wohingegen eine Verletzung der Verbindlichkeit und Vertraulichkeit ausschließlich durch die Identifizierung von unerlaubten Operationen auf den jeweiligen Daten nachzuweisen ist. Entsprechende

Methoden, die in diesem Zusammenhang Verwendung finden, sind somit zum einen schutzzielklassenspezifisch zum anderen auch anhand ihrer Komplexität differenzierbar.

Verfügbarkeit und Integrität sind durch den Einsatz proaktiver Maßnahmen, wie zum Beispiel Monitoring oder die Verwendung von Hashfunktionen, grundlegend gegen Verletzungen abzusichern. Der nachträgliche Nachweis einer Beeinträchtigung kann demzufolge anhand der entsprechenden Prüfergebnisse geführt werden. Verfügbarkeit kann in diesem Zusammenhang bei kontinuierlichem Monitoring ex post quantitativ über den Zeitverlauf hinweg vollständig evaluiert werden. Aspekte der Schutzzielklasse Integrität sind zum Beispiel durch die Überprüfung der Hashwerte validierbar. Hierbei ist jedoch das Intervall bzw. die Frequenz der Prüfvorgänge ausschlaggebend, eine zeitkontinuierliche Überwachung wie bei der Verfügbarkeit ist technisch gesehen jedoch nicht praktikabel. Im Bereich der Vertraulichkeit und Verbindlichkeit ist die nachträgliche Nachweisbarkeit ungleich komplexer einzustufen. Hierbei müssen unerlaubte Operationen auf den relevanten Daten ex post identifiziert werden, die nur durch umfassende technische Maßnahmen aufgezeichnet und gesichert werden können. Sind diese Maßnahmen ex ante nicht in ausreichendem Maße realisiert, so müssen spezielle Methoden der Computer-Forensik zum Einsatz gebracht werden, um den Nachweis einer Schutzzielverletzung erbringen zu können.

Der zweite Aspekt der Nachweisbarkeit ergibt sich aus dem **Zeitpunkt**, an dem eine Schutzzielverletzung identifiziert werden kann. Analog zu den Charakteristika der Methoden ist auch hier eine Abhängigkeit von den Schutzzielklassen gegeben. Verletzungen der Schutzzielklasse Verfügbarkeit sind in diesem Zusammenhang sehr frühzeitig bemerkbar. Sie werden zu dem Zeitpunkt ersichtlich, an dem ein Dienst in Anspruch genommen werden soll bzw. bei dem Einsatz einer Monitoringlösung dann, wenn ein Dienst oder eine Ressource ausfällt. Verletzungen der Integrität können im Vergleich nicht im Moment des Zugriffs, sondern in der Regel nur mit zeitlicher Verzögerung erkannt werden. Dies erfolgt zumeist dann, wenn durch inkonsistente Daten bedingt, fehlerhafte Ergebnisse oder widersprüchliches Systemverhalten festgestellt werden können. Die Nutzung von Maßnahmen wie Hashfunktionen zur Sicherstellung der Integrität von Daten sowie deren periodische oder ereignisbezogene Validierung kann die Zeitspanne bis zur Entdeckung einer Verletzung jedoch verkürzen [Witt06, 47]. Beeinträchtigungen der Schutzzielklasse Vertraulichkeit lassen sich vergleichsweise am schlechtesten nachweisen. Ob und wann eine unautorisierte dritte Partei Kenntnis sensibler Daten erlangen konnte, kann anhand der gespeicherten Daten technisch gesehen

schwerlich nachgewiesen werden. Eine Verletzung wird in der Regel erst dann evident, wenn die widerrechtliche Nutzung der Daten in der Öffentlichkeit entsprechende Konsequenzen nach sich zieht. Die Situation der Schutzzielklasse Verbindlichkeit ist ähnlich gelagert wie die der Vertraulichkeit. Verletzungen können nicht direkt entdeckt bzw. nachgewiesen werden. Vielmehr wird ein Verlust der Verbindlichkeit in der Regel erst im Streitfall offensichtlich, also dann, wenn die Rechtsverbindlichkeit von Informationen relevant wird [Kers95, 78].

Neben den Charakteristika bezüglich Entdeckungszeitunkt und Methodenkomplexität ist ein weiterer Aspekt aus den Ausführungen abzuleiten. Als einzige Schutzzielklasse ist die Verfügbarkeit eines Dienstes oder einer Ressource ex post vollständig quantifizierbar. Dies ist primär bedingt durch die Verfügbarkeit entsprechender technischer Maßnahmen bzw. deren Praktikabilität und Effizienz im Vergleich zu Methoden anderer Schutzzielklassen. Wie bereits dargestellt wurde, bildet diese Quantifizierung die Grundlage für die Definition von SLAs. Eine ähnliche Nutzung der anderen Schutzzielklassen als Anforderungsgrundlage im Rahmen von Dienstleistungs- oder Serviceverträgen hingegen, ist zum aktuellen Zeitpunkt aus den dargestellten Gründen nicht gegeben.

Monotonieverhalten von Schutzzielen

Die Aufrechterhaltung von Schutzzielen kann über eine Folge von Operationen auf Daten hinweg variieren. Dabei sind in Abhängigkeit von einzelnen Schutzzielklassen bestimmte Tendenzen der Veränderung identifizierbar. Diese Tendenzen werden als Monotonieverhalten von Schutzzielen bezeichnet [WoPf00, 178].

Schutzziele der Klasse **Vertraulichkeit** können in diesem Zusammenhang als monoton abnehmend charakterisiert werden. Ist die Vertraulichkeit einer Information, einer Person oder eines Vorgangs von Unbefugten kompromittiert, besteht keine Möglichkeit dieses Schutzziel wieder zu erreichen.

Bei **Integritäts- und Verfügbarkeitszielen** ist kein eindeutiges Monotonieverhalten identifizierbar. Bei beiden Schutzzielklassen können die Zielerreichungsgrade durch entsprechende Maßnahmen erhöht werden. Kommt es hingegen zu einem Verlust, so kann das jeweilige Schutzziel im Gegensatz zu Vertraulichkeit dennoch wiederhergestellt werden, zum Beispiel durch die Nutzung von Datensicherungen.

Verbindlichkeit kann allgemein betrachtet nicht abnehmen, wenn entsprechende Maßnahmen wie zum Beispiel elektronische Signaturen zum Einsatz kommen. Deren Rücknahme ist auf Grund der entsprechenden Rechtsverbindlichkeit nicht ohne weiteres möglich, sie sind zu vergleichen mit der Unterschrift unter einem rechtsgültigen Dokument. Das Monotonieverhalten von Verbindlichkeit wird jedoch durch dessen Abhängigkeitsbeziehung zu der Integrität von Informationen indirekt beeinflusst. Verbindlichkeit kann demnach dennoch abnehmen, wenn die jeweiligen rechtlichen Beweismittel, wie zum Beispiel digitale Signaturen, verlorengehen bzw. in ihrer Integrität verletzt werden, sodass die Verwendbarkeit als rechtsverbindlicher Beweis schwindet [WoPf00, 178f].

Die Relevanz des Monotonieverhaltens von Schutzzielen ist insbesondere bei elektronischen Geschäftsbeziehungen gegeben. Vor allem die Vertraulichkeit von Informationen und Anonymität von Aufgabenträgern ist in diesem Zusammenhang von Interesse. Kommt es während einer geschäftlichen E-Business-Transaktion zu einem Austausch von Identitätsdaten zwischen den beteiligten Parteien, wird die Anonymität also aufgehoben, so kann diese im weiteren Verlauf des Prozesses nicht wiederhergestellt werden. Es ist somit relevant, im Vorfeld entsprechend der diesbezüglichen Grundhaltung der jeweiligen Partei, geeignete Sicherheitseinstellungen für die Durchführung der Geschäftsprozesse zu definieren. Die Verwaltung- und Anpassungsmöglichkeiten dieser individuellen Sicherheitseinstellungen, auch vor dem Hintergrund des Monotonieverhaltens, ist Gegenstand der Forschung im Bereich des Identitätsmanagements und wird zum Beispiel in [GeJe01] näher beleuchtet.

Ebenso wie die Wechselwirkungen zwischen einzelnen Schutzzielen sind deren charakteristische Eigenschaften relevant für einen sinnvollen Einsatz der Schutzziele. Beziehen sich die Wechselwirkungen verstärkt auf die Konsistenz eines Systems aus Schutzzielen, so zielen die Eigenschaften in höherem Maße auf eine fachlich und auch inhaltlich sinnvolle Zuweisung im Rahmen bestimmter Szenarien ab. Insbesondere im Rahmen der Ausführungen zur geschäftsprozessorientierten Modellierung von Sicherheit in Teil III der Arbeit sind diese Aspekte von Belang.

5.4.4. Sicherheitsziele auf Ressourcenebene

Auf Ebene des Ressourcenmodells sind umsetzbare Sicherheitsziele bestimmt durch das betrachtete Bezugsobjekt sowie entsprechende Sicherheitsartefakte. Betriebliche Anwendungssysteme im Fokus der vorliegenden Arbeit erfordern in diesem Zusammenhang die Spezifika-

tion technischer Sicherheitsmaßnahmen[57]. Die Auswahl der entsprechenden Artefakte ist dabei primär inhaltlich motiviert und in Abhängigkeit von der Ausprägung der Schutzziele auf Ebene des Geschäftsprozessmodells zu interpretieren. Es erfolgt somit eine weitere Konkretisierung der Zieldefinition auf Ressourcenebene, die konkrete inhaltliche Anforderungen an die technischen Sicherheitsmaßnahmen als Sicherheitsartefakte definiert. Sicherheitsziele sind auf dieser Ebene somit als fachliche Anforderungen zu verstehen, die durch entsprechende Maßnahmen umzusetzen sind. Im Folgenden werden diese Zielvorgaben als **Sicherheitsanforderungen** bezeichnet, die in Bezug auf betriebliche Anwendungssysteme durch das Konzept der **Sicherheitsgrundfunktionen** dargestellt werden.

5.4.4.1. Das Konzept der Sicherheitsgrundfunktion

Sicherheitsanforderungen werden als fachliche Vorgaben in die Entwicklung betrieblicher Anwendungssysteme eingebracht. Sie müssen dann in Maßnahmen umgesetzt werden, die wiederum durch Mechanismen bzw. Dienste zu realisieren sind. Es erfolgt somit ein Übergang der Zieldefinition von der fachlichen zur technischen Perspektive, der im Hinblick auf technische Sicherheitsmaßnahmen durch das Konzept der Sicherheitsgrundfunktionen (SGF) realisiert werden kann.

Eine **Sicherheitsfunktion** beschreibt eine grundlegende Funktionalität, die gegen potentielle Bedrohungen gerichtet ist, somit diese Bedrohung unschädlich macht bzw. deren Auswirkungen im Schadensfall begrenzen kann [Kers95, 87]. Sie beschreiben dabei möglichst überschneidungsfrei allgemeingültige, quasi standardisierte, Funktionsbereiche wie etwa Identifikation und Authentifizierung oder Zugriffskontrolle, die in Abhängigkeit von den individuellen Anforderungen an ein zu konstruierendes System einzusetzen bzw. zu kombinieren sind [Ecke06, 189]. In der Literatur werden sie auch als **Sicherheitsgrundfunktionen** bezeichnet [Weck93, 150][58].

In Bezug auf maschinelle Aufgabenträger kann der Zusammenhang der Begriffe wie folgt dargestellt werden. Sicherheitsgrundfunktionen definieren auf abstrakter Ebene den Typus der zu realisierenden Sicherheitsfunktionalität. Sie spezifizieren auf fachlicher Ebene, was geleistet werden soll. Sicherheitsmaßnahmen setzen diese Anforderungen auf technischer Ebene

[57] Vgl. hierzu Kapitel 5.3.4.2.

[58] Die Begriffe Sicherheitsfunktion und Sicherheitsgrundfunktion werden in der vorliegenden Arbeit synonym verwendet.

anwendungsbezogen um, beschreiben somit wie eine Sicherheitsgrundfunktion realisiert wird. Sie stellen somit auf technischer Ebene das Gegenstück zu den fachlich orientierten Sicherheitsgrundfunktionen dar.

Im Hinblick auf die Sicherheitsartefakte der dritten Ebene stellen Sicherheitsgrundfunktionen eine inhaltliche Kategorisierung möglicher Sicherheitsvorgaben dar und sind somit als Sicherheitsziele zu interpretieren. Im Rahmen der Anwendungsentwicklung werden sie beim Übergang von der Geschäftsprozess- auf die Ressourcenebene als Anforderungen spezifiziert. Dies erfolgt durch die Transformation identifizierter Schutzziele in fachliche Sicherheitsgrundfunktionen, denen dann wiederum technische Sicherheitsmaßnahmen als zu realisierende Sicherheitsartefakte zugeordnet werden können[59]. Sicherheitsgrundfunktionen im Sinne von Sicherheitsanforderungen bilden in der vorliegenden Arbeit somit das Bindeglied zwischen den Schutzzielen und technischen Sicherheitsmaßnahmen.

Die Veröffentlichung von Grundfunktionen der Informationssicherheit erfolgte bereits 1991 durch die ITSEC, zu dem damaligen Zeitpunkt jedoch unter der Bezeichnung „Generische Oberbegriffe“ [BSI91, 24]. Sie haben in leicht modifizierter Form bis heute Gültigkeit und finden somit auch in den IT-Grundschutzkatalogen Verwendung [BSI09, 1221ff]. In der Publikation des BSI findet eine inhaltliche Ergänzung der Grundfunktionen statt, die jedoch auch mit einem Wechsel der Sichtweise einhergeht. Grundfunktionen werden in höherem Maße als Sicherheitsanforderungen verstanden und um Punkte erweitert, die semantisch näher an den Begriffen Sicherheitsmechanismus bzw. Sicherheitsdienst orientiert sind. So wird zum Beispiel Verschlüsselung als zusätzlich Sicherheitsfunktion bzw. Sicherheitsanforderung definiert, die jedoch rein inhaltlich betrachtet dem Bereich der Sicherheitsmechanismen bzw. Sicherheitsdienste zuzuordnen ist.

Die vorliegende Arbeit abstrahiert in diesem Punkt von der erweiterten Interpretation des BSI und konzentriert sich sich auf die inhaltliche Darstellung der Sicherheitsgrundfunktionen nach ITSEC [BSI91, 24ff], auch in Anlehnung an weitere Autoren wie etwa POHL [Pohl04] oder KERSTEN [Kers95]. Im folgenden Abschnitt werden die einzelnen Sicherheitsgrundfunktionen vorgestellt und im Hinblick auf die weitere Verwendung untersucht.

[59] Vgl. hierzu Kapitel 7.

5.4.4.2. Ausprägungen von Sicherheitsgrundfunktionen

Auf der Grundlage bestehender Forschungsergebnisse können neun Sicherheitsgrundfunktionen identifiziert werden.

SGF Identifizierung

Die Grundfunktion Identifizierung dient zur Feststellung der Identität eines Aufgabenträgers. Ein typisches Beispiel ist die Eingabe eines Benutzernamens als Identifikator bei der Anmeldung an ein Anwendungssystem. Es handelt sich hierbei um die reine Bestimmung einer virtuellen Identität, die Prüfung ob diese angegebene Identität der Wahrheit entspricht ist jedoch keine Bestandteil der Sicherheitsfunktion Identifizierung.

SGF Authentisierung

Der Nachweis über die Korrektheit einer Identität wird durch die Grundfunktion der Authentisierung erbracht. Hier wird durch den Abgleich zweier Merkmale, dem angegebenen Identifikator und einem Referenzmerkmal, überprüft, ob ein Aufgabenträger wirklich die durch den Identifikator definierte Identität besitzt. In der Praxis erfolgt diese Überprüfung in der Regel zusammen mit der Identifizierung. Durch die Angabe eines Benutzernamens in Verbindung mit einem Passwort als Referenzmerkmal, erfolgt zeitgleich sowohl die Identifizierung als auch die Authentisierung des Aufgabenträgers [Kers95, 89f]. Er wird somit als Benutzer[60] eines Systems zugelassen. Es sei darauf hingewiesen, dass in manchen Publikationen die Begriffe Authentisierung und Authentifizierung unterschieden werden. Authentifizierung wird dabei meist vorgangsorientiert verwendet und bezeichnet dann den technischen Prozess der Überprüfung von Identifikator und Referenzmerkmal, etwa den Abgleich des Datentupels mit einem zentralen Verzeichnisdienst. In der vorliegenden Arbeit wird auf diese Unterscheidung verzichtet und die Begriffe Authentisierung und Authentifizierung synonym verwendet.

SGF Zugriffskontrolle

Die Grundfunktion der Zugriffskontrolle hat zum Ziel, nur solche Zugriffe von Benutzern auf Informationen und Ressourcen zu erlauben, zu deren Nutzung sie auch berechtigt sind. Es muss somit eine Kontrolle des Informationsflusses zwischen Benutzer und System erfolgen sowie eine Überwachung der Ressourcennutzung innerhalb des Systems. Die Zugriffskontrolle schließt die Spezifikation, Vergabe und Zurücknahme dieser Berechtigungen in Form von

[60] Identifizierte und authentisierte Aufgabenträger werden im Weiteren als Benutzer eines Systems bezeichnet.

Zugriffsrechten für Benutzer ein [BSI91, 25]. Diese Rechteverwaltung dient als Grundlage für die **Autorisierung** eines Benutzers, somit dessen initiale Konfiguration mit Berechtigungen sowie deren Zuweisung nach erfolgter Anmeldung am System. Weiterhin muss durch die Zugriffskontrolle sichergestellt werden, dass diese Rechte im laufenden Betrieb überprüft werden. Diese Überprüfung kann nach diversen Ansätzen und Konzepten erfolgen, ist jedoch insbesondere davon abhängig, in welcher Form die Berechtigungen spezifiziert wurden. Man spricht in diesem Zusammenhang von **Zugriffskontrollmodellen** [Weck93, 105][61].

SGF Beweissicherung

Die Grundfunktion Beweissicherung fordert, dass alle sicherheitsrelevanten Aktivitäten in einem System aufgezeichnet werden. Die Beweissicherung erfolgt in der Regel durch die Protokollierung der Ausübung bzw. der versuchten Ausübung von Rechten durch einen Benutzer. Hierdurch können einzelne Operationen einem Benutzer zugeordnet und dieser somit zur Verantwortung gezogen werden [Kers95, 94].

SGF Protokollauswertung

Die Grundfunktion der Protokollauswertung baut auf der Sammlung an Verlaufsdaten durch die Beweissicherung auf. Ziel dieses Vorgehens ist es, sicherheitsrelevante Ereignisse eines Systems dahingehend auszuwerten, ob Sicherheitsverletzungen aufgetreten sind, von wem sie verursacht wurden und welche Systemressourcen davon betroffen sind [BSI91, 26].

SGF Wiederaufbereitung

Wiederaufbereitung als Sicherheitsgrundfunktion hat zum Ziel, die exklusive Verwendung von gemeinsamen Betriebsmitteln ohne einen unerlaubten Informationsfluss zwischen den Nutzern zu ermöglichen. Als klassisches Beispiel gilt das valide Löschen von persönlichen Daten auf Speichermedien in Mehrbenutzersystemen oder aber die korrekte Bereinigung von Adressbereichen des Arbeitsspeichers, die als gemeinsame Ressource für unterschiedliche Prozesse dienen. Die Grundfunktion der Wiederaufbereitung legt fest, für welche Betriebsmittel eine Aufbereitung für die erneute Nutzung zu erfolgen hat und wann diese Maßnahmen zu erfolgen haben [Ecke06, 192].

---

[61] Vgl. hierzu Kapitel 5.5.3.

SGF Unverfälschtheit

Die Grundfunktion der Unverfälschtheit besagt, dass Daten nicht in unzulässiger Art und Weise geändert werden dürfen [BSI91, 27]. Diese Grundfunktion bezieht sich somit direkt auf das Schutzziel der Integrität und schließt die Betrachtung der Beziehungen zwischen den Daten sowie deren Korrektheit und Konsistenz ein [Kers95, 97].

SGF Zuverlässigkeit

Die Zuverlässigkeit eines Dienstes besagt, dass angeforderte Ressourcen für Nutzer oder Prozesse eines Systems zeitnah zur Verfügung stehen müssen. Zeitkritische Aufgaben dürfen durch die Zurückhaltung oder die unnötige Anforderung von Betriebsmitteln somit nicht beeinträchtigt werden. Neben der korrekten Funktionsweise dieser Systemkomponenten ist somit auch deren Verfügbarkeit sicherzustellen [BSI91, 27]. Der Begriff der Zuverlässigkeit wird in diesem Zusammenhang im Sinne der Gewährleistung von Funktionalität verwendet. Als Eigenschaften eines Systems zur Erfüllung der Grundfunktion in diesem Sinne werden die Kenngrößen Betriebsbereitschaft, Rechtzeitigkeit, Fehlererkennung, Fehlerüberbrückung sowie Fehlerbehebung angesehen [Kers95, 98ff].

SGF Übertragungssicherung

Die Grundfunktion der Übertragungssicherung bezieht sich auf die Absicherung von Daten während eines Kommunikationsvorgangs, somit deren fehlerfreie und ungestörte Übertragung zwischen zwei Kommunikationspartnern. Als zusätzliche Funktionen werden Aspekte der Authentisierung, Zugriffskontrolle und der Unverfälschtheit benötigt, die sich direkt auf die Schutzzielerreichung im Bereich der Integrität, Vertraulichkeit und Verbindlichkeit beziehen [BSI91, 28]. Die Übertragungssicherung stellt somit eine Grundfunktion dar, die als Kombination bestehender Grundfunktionen betrachtet werden kann. Ihre Relevanz ergibt sich aus ihrer speziellen Perspektive, die sich im Gegensatz zu bestehenden Grundfunktionen nicht auf die interne Bearbeitung von Informationen in einem System, sondern ausschließlich auf deren Übertragung zwischen verschiedenen Systemen bezieht.

5.4.4.3. Kategorisierung von Sicherheitsgrundfunktionen

Die beschriebenen neun Sicherheitsgrundfunktionen können inhaltlich zu sieben Kategorien zusammengefasst werden. Jede Kategorie bezieht sich dabei auf eine bestimmte Menge an technischen Sicherheitsmaßnahmen, die die spezifischen Anforderungen der jeweiligen

Sicherheitsgrundfunktion umsetzen. In der vorliegenden Arbeit werden die folgenden Kategorien von Sicherheitsgrundfunktionen gebildet:

- Identifizierung und Authentisierung (I&A)
- Zugriffskontrolle und Autorisierung (Z&A)
- Beweissicherung und Auditing (B&A)
- Unverfälschtheit (U)
- Übertragungssicherung (Ü)
- Zuverlässigkeit (Z)
- Wiederaufbereitung (W)

Die beschriebenen Kategorien dienen im weiteren Verlauf der Arbeit als Bindeglied zwischen Schutzzielen auf Geschäftsprozessebene und konkreten technischen Sicherheitsmaßnahmen, die diese Ziele in Bezug auf betriebliche Anwendungssysteme umsetzen. In Kapitel 5.5 werden entsprechende Sicherheitsmechanismen anhand der Kategorien von Sicherheitsgrundfunktionen systematisiert und exemplarisch vorgestellt.

5.4.5. Systematik der Sicherheitsziele

Gemäß der vorgestellten Differenzierung von Sicherheitszielen kann die folgende Systematik anhand der Unternehmensarchitektur dargestellt werden.

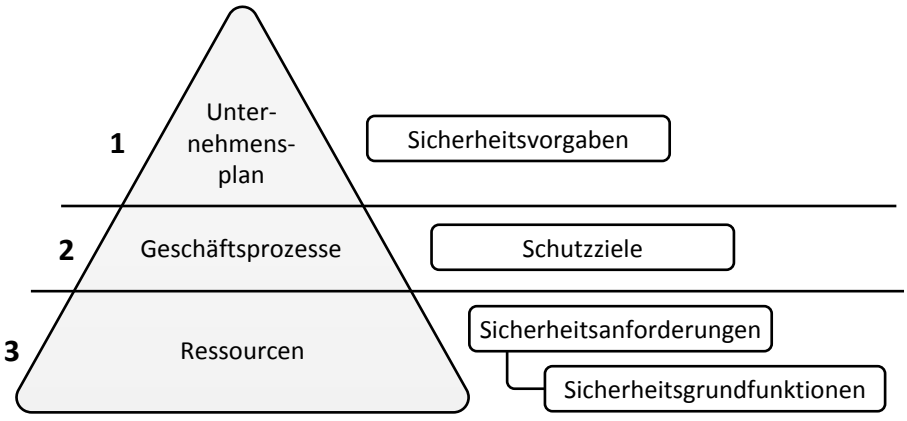

Abbildung 25: Systematik der Sicherheitsziele

Es wird deutlich, dass, in Abhängigkeit von der betrachteten Ebene der Unternehmensarchitektur, unterschiedliche Zielvorgaben der Informationssicherheit zu spezifizieren sind. Maßgeblich dabei ist die Umsetzbarkeit dieser Ziele auf der jeweiligen Ebene. Es ergibt somit

keinen Sinn, gesetzliche Regelungen erst bei der Anforderungsanalyse im Rahmen der Entwicklung eines Anwendungssystems zu berücksichtigen. Ebenso wenig sinnhaft erscheint es, im Laufe der strategischen Planung eines Unternehmens über Schutzziele wie Vertraulichkeit von Informationen zu diskutieren. Schlussendlich sind alle Zielvorgaben der Informationssicherheit an den jeweiligen Ebenen des Architekturmodells auszurichten und aufeinander abzustimmen.

Neben den ebeneninternen Beziehungen, insbesondere im Bereich der Schutzziele, sind in diesem Zusammenhang insbesondere die ebenenübergreifenden Beziehungen der Sicherheitsziele von Relevanz. Diese sind, analog zu Bezugsobjekten und Sicherheitsartefakten, auch im Bereich der Sicherheitsziele maßgeblich durch den Übergang von Lenkungs- zu Leistungssystem geprägt. Anhand der Systematik wird daher deutlich, dass aus Top-Down-Perspektive eine zunehmende Konkretisierung der Sicherheitsziele erfolgt. Stehen auf Ebene des Unternehmensplans eher strategische, allgemeingültige Zielsetzungen im Mittelpunkt, so sind diese im Bereich des Ressourcenmodells in konkrete Sicherheitsanforderungen bzw. Sicherheitsgrundfunktionen der entsprechenden Sicherheitsmaßnahmen zu übersetzen. Ebenso wie bei Sicherheitsartefakten ist bei diesem Transformationsvorgang eine semantische Lücke auf Ebene der Geschäftsprozessmodelle zu verzeichnen, die einen konsistenten und einheitlichen Übergang der Zielbildung erschwert. Eine Möglichkeit diese nachteilige Situation zu überwinden besteht in der expliziten Berücksichtigung von Schutzzielen sowie deren Modellierung auf der Ebene der Geschäftsprozessmodelle. Ein entsprechender Ansatz wird in Teil III der Arbeit vorgestellt.

5.5. Beschreibung technischer Sicherheitsmechanismen

Im Rahmen der Beschreibung möglicher Ausprägungen der Meta-Objekttypen auf Ressourcenebene wurden bisher insbesondere Bezugsobjekte und Sicherheitsziele auf Schemaebene vorgestellt. Um diese Darstellung zu komplettieren, wird auf der Grundlage der vorgestellten Systematik der Sicherheitsgrundfunktionen eine überblicksartige Beschreibung technischer Sicherheitsmechanismen ergänzt. Diese beziehen sich gemäß der Ausrichtung der vorliegenden Arbeit ausschließlich auf das Bezugsobjekt des betrieblichen Anwendungssystems.

Entsprechend der Kategorisierung der Sicherheitsgrundfunktionen werden im Folgenden einzelne Sicherheitsmechanismen exemplarisch vorgestellt und in Bezug zu den jeweils unter-

stützten Schutzzielen gesetzt[62]. Den Ausgangspunkt der Darstellung bildet das allgemeine Themengebiet der Kryptologie, das für einen Großteil der Sicherheitsmechanismen die Grundlage darstellt.

5.5.1. Grundlagen der Kryptologie

Kryptologische Verfahren sind dafür geeignet, sowohl die Schutzzielklassen Vertraulichkeit und Integrität als auch die der Verbindlichkeit zu unterstützen [FuKe99, 218]. Es finden sich somit Mechanismen in fast allen Klassen der Sicherheitsgrundfunktionen, die auf entsprechenden Verfahren aufbauen. Kryptologie bezeichnet die Wissenschaft von sicherer und vertraulicher Kommunikation und vereint dabei die zwei Hauptdisziplinen Kryptographie und Kryptoanalyse, die sich gegenseitig ergänzen [Ble+05, 25] [63]. Die nachfolgenden Ausführungen beschränken sich auf die Kryptographie und erläutern die Grundbereiche der Verschlüsselungsverfahren, Hashfunktionen sowie digitalen Signaturen.

Verschlüsselungsverfahren

Verschlüsselungsverfahren können in die zwei Klassen der symmetrischen und asymmetrischen Verschlüsselung untergliedert werden. Bei **symmetrischen Verfahren** wird ein gemeinsames Geheimnis zwischen einem Sender Alice (A) und einem Empfänger Bob (B) als Schlüssel für Ver- und Entschlüsselung der übermittelten Nachricht verwendet[64]. Ein aktuelles Verschlüsselungsverfahren ist zum Beispiel der Advanced Encryption Standard (AES) [NIST01], der als Blockchiffre mit variabler Schlüssellänge in vielen derzeitigen Anwendungsformen zum Einsatz kommt.

Den Schwachpunkt symmetrischer Verschlüsselungsverfahren stellt der gemeinsame Schlüssel von Sender und Empfänger dar, der vor der Verschlüsselung sicher und geheim ausgetauscht werden muss. **Asymmetrische Verfahren** setzen an diesem Punkt an und verwenden für Ver- und Entschlüsselung zwei unabhängige und nicht aufeinander rückführbare Schlüs-

---

[62] Die Verweise auf die entsprechenden Schutzziele dienen der inhaltlichen Abrundung der Beschreibung der Schemaebene der Modellierung. In Kapitel 7.1.3.1 wird diese Beziehung zwischen Sicherheitsgrundfunktionen und Schutzzielen im Detail erörtert.

[63] Für eine detailliert Betrachtung des Themengebiets der Kryptologie sei zum Beispiel auf [Baue07] oder [Men+01] verwiesen.

[64] Die Bezeichnung Alice und Bob stehen politisch korrekt und in langer Tradition stellvertretend für den Sender und den Empfänger einer Nachricht. 1978 fanden diese Bezeichnungen das erste Mal Verwendung [Riv+78], seitdem sind beide, gerne auch im Bunde mit einem Angreifer Mallory, insbesondere in Schriften zum Thema Informationssicherheit zu finden. Die vorliegende Arbeit folgt diesem Quasi-Standard der Nomenklatur.

sel. Für die Verschlüsselung einer Nachricht an B wird dessen öffentlicher Schlüssel von A verwendet. Der entstehende Chiffretext kann daraufhin nach Übermittlung nur mit dem privaten Schlüssel von B entschlüsselt werden. Man spricht demzufolge auch von **Public-Key-Verfahren**, die erstmals bereits im Jahr 1976 durch DIFFIE und HELLMANN vorgestellt wurden [DiHe76]. Aktuell am weitesten verbreitet sind das nach seinen Erfindern RIVEST, SHAMIR und ADLEMAN benannte RSA-Verfahren [Riv+78] sowie der Ansatz von EL-GAMAL [ElGa85].

Die Ver- bzw. Entschlüsselung bei asymmetrischen Verfahren erfordert einen relativ hohen Rechenaufwand, der die Geschwindigkeit der jeweiligen Operation im Vergleich zu symmetrischen Verfahren ca. um den Faktor 1000 verringert. Aus diesem Grund kommen in der Praxis häufig Mischformen beider Ansätze zum Einsatz, die als Verfahren der **hybriden Kryptographie** bezeichnet werden [Swo+08, 28]. Hierbei wird durch den Absender A ein symmetrischer Sitzungsschlüssel erzeugt, mit dem der Klartext chiffriert wird. Der Sitzungsschlüssel wird im Anschluss mit dem öffentlichen Schlüssel von B verschlüsselt und zusammen mit dem Chiffretext an diesen übertragen. Der Empfänger kann mit seinem privaten Schlüssel den Sitzungsschlüssel dechiffrieren und damit den gesendeten Chiffretext entschlüsseln. Hybride Ansätze verbinden somit die Geschwindigkeitsvorteile symmetrischer Verfahren mit dem besseren und sichereren Schlüsselkonzept asymmetrischer Methoden. Beispiele solcher Verfahren sind Pretty Good Privacy (PGP) [Zimm95] oder S/MIME [Rams04] zur Verschlüsselung von E-Mail-basierter Kommunikation.

Durch die reine Verschlüsselungsleistung symmetrischer und asymmetrischer Verfahren wird ausschließlich die Schutzzielklasse der Vertraulichkeit von Informationen adressiert. Weitere Aspekte wie die Authentizität des Absenders bzw. der Nachricht selbst, oder aber deren Integrität, werden nicht unterstützt. Um diese Ziele zu erreichen und somit die Grundlage der Schutzzielklasse Verbindlichkeit zu schaffen, sind zusätzliche Mechanismen wie digitale Signaturen und Hashverfahren notwendig [Men+01, 283].

Digitale Signaturen und Hashfunktionen

Der Zweck einer digitalen Signatur ist es, die Identität einer Person an digitale Informationen zu binden, sodass, analog zur handschriftlichen Unterschrift eines Dokuments, die Echtheit und Zurechenbarkeit der Information verifiziert werden kann [Men+01, 22]. Anhand dieses realweltlichen Bezugs ergeben sich somit verschiedene Anforderungen, wie etwa die einfache

Überprüfbarkeit einer digitalen Unterschrift durch den Empfänger oder die Nicht-Trennbarkeit von digitaler Unterschrift und den signierten Informationen, die durch entsprechende technische Verfahren erbracht werden müssen [Ble+05, 77f].

Auf technischer Ebene werden digitale Signaturen durch Public-Key-Verfahren realisiert. Hierbei werden aus den zu signierenden Informationen und dem privaten Schlüssel des Senders eine **digitale Signatur** berechnet, die nur durch den öffentlichen Schlüssel des Senders auf Seiten des Empfängers verifiziert werden kann. Eine Signatur kann dabei im Prinzip auf zwei Arten erstellt werden.

Zum einen kann die gesamte Nachricht mit dem privaten Schlüssel signiert und somit chiffriert werden. Dies beinhaltet zweifelsfrei keinen Schutz der Vertraulichkeit, da der öffentliche Schlüssel frei verfügbar ist, jedoch kann der Chiffretext nur durch den öffentlichen Schlüssel des Senders rücküberführt werden und somit die Signatur verifiziert werden. Man spricht in diesem Fall von einer digitalen Signatur mit Nachrichtrückgewinnung.

Weiterhin kann die Signatur auch nur für einen Hashwert der Nachricht erstellt werden, nicht für die gesamte Nachricht. Der Empfänger dechiffriert mit dem öffentlichen Schlüssel den Hashwert und vergleicht ihn mit einem von ihm erstellten Hashwert der Nachricht. Stimmen sie überein ist sowohl die Authentizität des Senders als auch der Information sichergestellt. Diese Variante wird als digitale Signatur mit Hashwert-Anhang bezeichnet und ist auf Grund des geringen Verschlüsselungsumfangs des Hash-Wertes auch für größere Nachrichten geeignet [Swo+08, 28ff].

Hashfunktionen stellen in diesem Zusammenhang kryptografische Hilfsfunktionen dar. Sie bilden eine Zeichenfolge beliebiger Länge auf eine Zeichenfolge fester Länge, den sogenannten Hash-Wert ab [Buch08, 191]. Dabei darf es nicht möglich sein, eine weitere Ausgangszeichenfolge zu finden, die nach Anwendung der Funktion den gleichen Hash-Wert liefert (Kollisionsresistenz). Weiterhin wird gefordert, dass eine Ausgangszeichenfolge nicht aus einem Hash-Wert rekonstruiert werden kann (Urbildresistenz). Hashverfahren, die dies realisieren, werden auch als kryptografische Einwegfunktionen bezeichnet [Ble+05, 57]. Beispiele aktuell verwendeter Algorithmen sind der Secure Hash Algorithm 1 (SHA-1) [EaJo01] oder der Message-Digest Algorithm 5 (MD5) [Rive92].

Hashverfahren zielen durch ihre Eigenschaften und die Überprüfbarkeit des Hashwertes primär auf die Sicherstellung der Integrität einer übermittelten Nachricht ab. Jedoch kann es ei-

nem potentiellen Angreifer durchaus möglich sein, bei einer abgefangenen Nachricht sowohl den Inhalt, als auch den entsprechenden Hash-Wert zu verändern. Um diese Möglichkeit im Rahmen der Integritätssicherung zu unterbinden, kommen Verfahren mit gesicherten Hashwerten (engl. *message authentication codes*, MAC) wie etwa HMAC oder CBC-MAC zum Einsatz[65].

Zertifikate

Digitale Signaturen in Verbindung mit kryptografischen Hashfunktionen zielen auf die Sicherstellung der Integrität und Authentizität einer übermittelten Nachricht ab. Jedoch ist durch diese technischen Verfahren noch nicht sichergestellt, dass ein öffentlicher Schlüssel zur Dechiffrierung einer digital signierten Nachricht auch wirklich eindeutig der sendenden Person zugeordnet werden kann. Dieser Schwachpunkt wird durch den Einsatz von **Zertifikaten** adressiert. Zertifikate werden von vertrauenswürdigen Dritten (engl. *trusted third parties*, TTP), sogenannten Zertifizierungsstellen (engl. *certification authorities*, CA), ausgestellt. Sie bestätigen die Zuordnung eines öffentlichen Schlüssels zu einer Person, die im Rahmen des Zertifikats durch bestimmte charakterisierende Attribute, wie etwa Name oder Geburtsdatum, identifiziert wird. Zertifizierungsstellen sind hierarchisch strukturiert, die Überprüfung des Zertifikates eines beliebigen Teilnehmers wird somit global ermöglicht [HeBe00, 229]. Technisch gesehen stellen Zertifikate elektronische Dokumente dar, die durch die Zertifizierungsstelle digital signiert wurden. Eine Überprüfung erfolgt demnach durch die Validierung dieser elektronischen Signatur anhand des öffentlichen Schlüssels der Zertifizierungsstelle. Ist dieser Prozess erfolgreich, so kann darauf vertraut werden, dass das Zertifikat authentisch ist und somit auch dessen Inhalt, also die Zuordnung einer Person zu einem öffentlichen Schlüssel, korrekt ist. Das Vertrauen in die Arbeitsweise und Identifikationsleistung einer Zertifizierungsstelle wird somit implizit auf den Inhalt des Zertifikats übertragen [Ble+05, 353].

Public-Key Infrastruktur

Der Aufbau von Zertifizierungsstellen bzw. die Nutzungsmöglichkeit entsprechender Prozesse zur Identitätsprüfung, Zertifikatsvergabe und -verwaltung sowie der Schlüsselverwaltung, erfolgen im unternehmerischen Umfeld durch die Implementierung einer sogenannten **Public-Key Infrastruktur** (PKI). Diese muss Funktionen bereitstellen, um die öffentlichen Schlüssel der Nutzer zugreifbar zu machen, deren Sperrung bzw. Rückruf ermöglichen sowie die Zu-

[65] Für eine Einführung zu message authentication codes sei auf [Stam06, 85ff] verwiesen.

ordnung zu Identitäten sicherstellen. Ihre Struktur besteht im Kern aus der bereits angesprochenen CA sowie weiteren technischen Basiskomponenten, wie der Registration Authority (RA), Zertifikat-Revokationslisten (engl. *certificate revocation list*, CRL) oder Verzeichnisdiensten.

In der Praxis haben sich für den Betrieb einer PKI die zwei grundlegenden Verfahren PGP und S/MIME etabliert, die jedoch in ihren konzeptuellen Grundlagen auf zwei unterschiedlichen Philosophien aufbauen. Während PGP den Ansatz des „Web of Trust" verfolgt, bei dem jeder Nutzer als zertifizierende Instanz fungieren kann, indem er den öffentlichen Schlüssel eines anderen Nutzers signiert, verwendet S/MIME zentrale staatlich oder private Instanzen, die als vertrauenswürdige Instanz die Identität eines Schlüsselinhabers zertifizieren[66].

Für Unternehmen stellen der Aufbau einer PKI und deren Integration in bestehende betriebliche Prozesse ein komplexes Unterfangen dar [HoTe00, 316ff]. Aus diesem Grund haben sich, auch im Hinblick auf den Aufbau und den Inhalt von Zertifikaten, diverse Richtlinien und Profile auf Basis des Standards X.509 des Telecommunication Standardization Sectors entwickelt, die ein Einführung im unternehmerischen Kontext erleichtern[67].

Elektronische Signatur

Das Konzept der digitalen Signaturen stellt für sich genommen einen kryptographischen Ansatz dar, um die Authentizität von Personen bzw. Informationen in elektronischer Form überprüfbar zu machen. In Bezug auf die reale Verwertbarkeit dieser Validierungsmöglichkeit, zum Beispiel im Rahmen juristischer Fragestellungen, greift dieses Konzept jedoch zu kurz. Im rechtlichen Sinn findet in diesem Zusammenhang daher der Begriff der **elektronischen Signatur** Verwendung. Dieser baut auf dem technischen Konzept der digitalen Signatur auf, ist jedoch um bestimmte Anforderungen erweitert, um die Beweiskraft einer elektronischen Willenserklärung auch vor Gericht zu gewährleisten. In der Bundesrepublik Deutschland werden diesbezüglich die drei Abstufungen „einfache elektronische Signatur", „fortgeschrittene elektronische Signatur" sowie „qualifizierte elektronische Signatur" unterschieden. Ihre Charakteristika sind in dem Gesetz über Rahmenbedingungen für elektronische Signaturen

[66] Vgl. hierzu [HeMö00].

[67] Vgl. hierzu [Wölf06].

(SigG) [Bund01a] sowie der Verordnung zur elektronischen Signatur (SigV) [Bund01b] verankert[68].

Bei der Darstellung der Themengebiete der Kryptologie wurde auf eine vergleichende Bewertung der einzelnen Verfahren bewusst verzichtet, da dies auf Grund der hohen Komplexität des Bereichs nur anwendungsfallbezogen in fundierter Weise erfolgen könnte. Die vorgestellten kryptografischen Methoden finden als technisches Konzept bzw. Verfahren in verschiedensten Sicherheitsmechanismen Verwendung. In den folgenden Abschnitten werden sie bei der Erläuterung der Sicherheitsmechanismen entsprechend referenziert.

5.5.2. Sicherheitsmechanismen der Identifikation und Authentisierung

Identifikation als Sicherheitsgrundfunktion hat zum Ziel, die Identität eines Aufgabenträgers zu ermitteln. Methoden der Authentisierung werden darauf aufbauend genutzt, um diese behauptete Identität zu bestätigen oder zu widerlegen, der entsprechende Prozess wird auch als Verifikation bezeichnet. Im Folgenden liegt der Schwerpunkt der Betrachtung auf Sicherheitsmechanismen, die eine solche Verifikation ermöglichen. Der Teilbereich der Identifikation wird daher unter dem Aspekt der Authentisierungs-Mechanismen subsumiert.

Authentisierung personeller Aufgabenträger

Authentisierungs-Mechanismen können anhand der drei grundlegenden Prinzipien **Wissen**, **Besitz** und **Merkmal** sowie Kombinationen aus diesen kategorisiert werden. Der Bereich Wissen kann weiterhin differenziert werden in die Kenntnis von fachverfahrensspezifischen Informationen, wie etwa eine Studenten- oder Mitarbeiterkennung, sowie in die Kenntnis von Geheimnissen, wie zum Beispiel Passwörtern[69], die zwischen einer zu authentisierenden Person P und einem authentisierenden System S geteilt werden. Die Kategorie Besitz bezieht sich auf einen physikalischen Gegenstand, dessen Vorlage von P als Grundlage der Authentisierung von S verlangt wird. Konkrete Beispiele hierfür sind Chipkarten oder Dongles, allgemein wird in diesem Zusammenhang von sogenannten (physischen) Tokens[70] gesprochen

---

[68] Eine umfassende Darstellung des Themengebiets wird in [Gru+07] gegeben.

[69] Passwörter können weitergehend differenziert werden in Dauer-Passwörter, die bei jedem Anmeldevorgang gleich bleiben und dynamische Verfahren mit Einmal-Passwörtern (engl. *one-time-passwords*, OTP), die listenbasiert oder auf Grundlage von Sequenznummern jeweils nur einmal genutzt werden. Einen Einblick hierzu gibt [Swo+08, 150f].

[70] Vgl. hierzu [Davi07].

[BSI06, 35ff]. Der Bereich Merkmal bezieht sich schließlich auf physiologische oder auch verhaltensbezogene Eigenschaften von P, die zur Authentisierung herangezogen werden. Entsprechende Mechanismen werden als biometrische Authentisierungsverfahren bezeichnet. Beispiele hierfür sind die Iris-, Stimm- sowie Fingerabdruckerkennung oder auch die Prüfung des Tipprhythmus auf einer Tastatur [BSI07][71].

Authentisierungsprotokolle

Authentisierungsmechanismen können durch verschiedene technische Verfahren realisiert werden, etwa online im Browser durch eine HTTP-Authentifizierung [Fra+99] oder lokal an einem Rechner bei der Anmeldung am Betriebssystem. Auf Protokollebene betrachtet stellen diese Mechanismen uni-direktionale Verfahren dar, die als Spezialform sogenannter Challenge-Response-Verfahren zum aktuellen Zeitpunkt sehr häufig zum Einsatz kommen [Ecke06, 440].

Challenge-Response-Verfahren sind in gewisser Weise ein grundlegendes, bidirektionales Protokoll zwischen P und S, das zur Umsetzung des Geheimnis-Prinzips im Rahmen der Authentisierung zum Einsatz kommt. Die authentisierende Partei S sendet dabei eine sogenannte Challenge, zu verstehen als eine Art Aufgabe, welche die zu authentisierende Partei P zum Beispiel nur durch Kenntnis eines Geheimnisses lösen kann und in Form einer Response als Antwort zurücksendet. Dieses Verfahren kann auf Basis unterschiedlicher Ansätze verwendet werden, so zum Beispiel mit symmetrischen oder asymmetrischen Schlüsseln, Einwegfunktionen oder aber auch in Kombination mit digitalen Signaturen wie sie bei der SSL-Verschlüsselung zum Einsatz kommen [Swo+08, 152f]. Das Challenge-Response-Verfahren ist somit nicht auf das Geheimnis-Prinzip der Authentisierung eingeschränkt sondern kann als grundlegendes Authentisierungsprotokoll auch mit anderen Prinzipien verwendet werden.

Einen Spezialfall des Challenge-Response-Verfahrens stellt das **Zero-Knowledge Verfahren** dar. Im Gegensatz zu passwort-basierten Mechanismen werden hier mehrfache bidirektionale Kommunikationsschritte zwischen P und S verwendet, sogenannte Protokoll-Runden, um die Authentifizierung durchzuführen [Swo+08, 155ff]. Das Verfahren basiert im Kern auf der Frage, wie ein zu authentisierender Nutzer P die authentisierende Instanz S davon überzeugen kann, dass sie ein Geheimnis G kennt, ohne dass P auch nur einen Teil von G gegenüber S

[71] Eine detaillierte Betrachtung verschiedener Aspekte zu biometrischen Mechanismen wird in [Tele06] gegeben.

oder auch Dritten preisgeben muss [Ecke06, 462]. Implementiert wurde dieses Verfahren erstmals 1986 durch das Fiat-Shamir-Verfahren [FiSh86][72].

Authentisierung maschineller Aufgabenträger

Die bisher dargestellten Authentisierungsmechanismen beziehen sich primär auf personelle Aufgabenträger als Benutzer eines Systems. In Bezug auf maschinelle Aufgabenträger, somit Anwendungssysteme, Prozesse oder (mobile) Geräte, sind diese Mechanismen hingegen nur bedingt geeignet. In diesem Zusammenhang werden Authentifizierungsmechanismen benötigt, die automatisiert und gleichsam sicher zumeist eine Zwei-Wege-Authentisierung ermöglichen. Ein konkretes Beispiel hierfür stellt der Zugriff auf einen durch das Protokoll Transport Layer Security (TLS) [DiRe08] geschützten Webserver dar. In der Regel erfolgt hier implizit eine durch den Browser durchgeführte Ein-Weg-Authentisierung, indem das präsentierte Zertifikat des Webservers überprüft wird. Bei einer Zwei-Wege-Authentisierung wird dieses Verfahren zusätzlich invertiert, sodass der Webserver ebenfalls sicher sein kann, mit dem rechtmäßigen Client zu kommunizieren. Der Client signiert in diesem Fall die gestellte Challenge des Servers mit seinem privaten Schlüssel, der Server verifiziert im Anschluss die damit erstellte Response mit dem öffentlichen Schlüssel des Clients. Als Grundlage fungieren somit elektronische Zertifikate, die im Rahmen einer PKI für maschinelle Aufgabenträger erstellt wurden. Anhand der dargestellten Systematik von Authentisierungsverfahren, kann diese Form mittels digitaler Signatur dem Besitz-Prinzip zugeordnet werden.

Bezug zu Schutzzielen

Die dargestellten Sicherheitsmechanismen der Grundfunktion Identifikation und Authentisierung beziehen sich im Kern auf die Sicherstellung der Authentizität von Informationen und Aufgabenträgern. Sie bilden damit die Grundlage für die Grundfunktion der Autorisierung und somit auch für die Erreichung des Schutzziels Verbindlichkeit.

5.5.3. Sicherheitsmechanismen der Zugriffskontrolle und Autorisierung

Die Kernaufgaben der Zugriffskontrolle und Autorisierung beziehen sich auf die Bereitstellung von Mechanismen zur Verwaltung von Zugriffsrechten, somit deren Erstellung, Vergabe und Rücknahme sowie die entsprechende Überprüfung im laufenden Betrieb. Die Grundlage

[72] Eine durchaus unterhaltsame Einführung in die grundlegende Problemstellung ist in [Qui+90] zu finden.

bildet eine zentrale Rechteverwaltung, die für jede zu schützende Information entsprechende Zugriffsrechte für bestimmte Aufgabenträger spezifiziert [Ecke06, 539f]. Der Begriff der Autorisierung kann dabei in zweifacher Weise interpretiert werden. Zum einen bezeichnet er vorgangsorientiert den initialen Zuweisungsprozess der Rechte an einen Benutzer nach dessen Authentisierung am System. Zum anderen bezeichnet er ergebnisorientiert das Resultat des Prüfprozess, der beim Zugriff auf ein geschütztes Objekt durchlaufen wird. Im Laufe der Zeit haben sich im Kern drei unterschiedliche Ansätze dieser Sicherheitsgrundfunktion herausgebildet, man bezeichnet sie als **Zugriffskontrollstrategien** [WoWi07, 440].

Discretionary Access Control

Die **benutzerbestimmte Zugriffskontrolle** (engl. *discretionary access control*, DAC) basiert auf Berechtigungen, die einem Benutzer auf Grund seiner Identität zugeteilt sind und die definieren, welche Aktionen dieser Benutzer auf welchem Aufgabenobjekt durchführen darf. Das Attribut „benutzerbestimmt“ wird deshalb verwendet, da ein Benutzer seine Berechtigungen auch an andere Aufgabenträger weitergeben kann. Die Berechtigungen des Zugriffs und der Weitergabe werden dabei zwar in einer zentralen Rechteverwaltung administriert, systemglobale Regelsätze des Zugriffs, die unabhängig von der Identität eines Benutzers greifen, existieren jedoch nicht. In der Konsequenz entsteht durch fehlerhafte Weitergabe von Rechten die Gefahr, dass inkonsistente Berechtigungsstrukturen entstehen [SaCa01, 3ff].

Mandatory Access Control

Systembestimmte Zugriffskontrollstrategien (engl. *mandatory access control*, MAC) adressieren den Kritikpunkt der fehlenden globalen Kontrolle und führen diese unter der Verwendung von globale Sicherheitsmarken ein [Pern95, 170]. Diese Berechtigungen beziehen sich sowohl auf Aufgabenobjekte als auch auf Aufgabenträger und dienen systemweit, neben der reinen Identität, als weiteres Kriterium der Zugriffskontrolle. Je nach Aufbau und Systematik der Sicherheitsmarken können unterschiedliche Arten der MAC unterschieden werden. Am weitesten verbreitet ist dabei die sogenannte Multilevel Security (MLS), die Zugriffe anhand von Schutzstufen reguliert. Dabei werden Schutzmarken als hierarchische Einstufung von Aufgabenträgern (engl. *clearances*) und Aufgabenobjekten (engl. *classifications*) verwendet. Nur wenn die clearance eines Aufgabenträgers die entsprechende Stufe der

classification des Aufgabenobjekts erreicht bzw. übertrifft, wird der Zugriff erlaubt [Stam06, 181f][73].

Role-based Access Control

Rollenbasierte Zugriffsstrategien (engl. *role-based access control*, RBAC) bilden die letzte und auch jüngste Klasse an Zugriffskontrollstrategien. Hierbei werden Berechtigungen nicht direkt an Aufgabenträger, sondern an Rollen gebunden, denen im Anschluss dann die Aufgabenträger zugeordnet werden [WoWi07, 439]. Die Hauptmotivation hinter diesem Vorgehen besteht in der Notwendigkeit, Berechtigungsstrukturen möglichst nahe an tatsächliche Organisationsstrukturen anzulagern, um die Abbildungskomplexität der Berechtigungen sowie den administrativen Aufwand zu reduzieren. Zusätzlich ist im betrieblichen Umfeld relevant, dass Rechte auf bestimmten Aufgabenobjekten weniger mit der Identität eines Benutzers korrelieren, als vielmehr mit dessen Verantwortung im Unternehmen. Diese Anforderungen können durch DAC und MAC nicht in gewünschtem Maße erfüllt werden. Rollenbasierte Zugriffsstrategien hingegen bieten prinzipiell die Möglichkeit, diese Ansprüche mit der notwendigen Flexibilität zu berücksichtigen [SaCa01, 41].

Sicherheitsmodelle

Die drei vorgestellten Zugriffskontrollstrategien DAC, MAC und RBAC sind als Sicherheitsmechanismen im definierten Sinne dieser Arbeit zu verstehen. Jede Strategie kann nun durch bestimmte Verfahren umgesetzt werden, man spricht in diesem Zusammenhang von sogenannten **Sicherheitsmodellen**. Allgemein betrachtet kann ein Sicherheitsmodell als sicherheitsorientierte Abstraktion eines betrieblichen Anwendungssystems verstanden werden [Ecke06. 261]. Es spezifiziert dabei implizit den Ansatz bzw. das Verfahren, anhand dessen Zugriffsschutz bzw. Zugriffskontrolle in einem Anwendungssystem realisiert werden [Sch+05, 1250]. Für jede Zugriffskontrollstrategie sind somit dedizierte Sicherheitsmodelle anzugeben.

Sicherheitsmodelle im Bereich DAC

Im Bereich DAC basieren Sicherheitsmodelle in der Regel auf dem Ansatz der **Zugriffskontrollmatrix** (engl. *access control matrix*). Dieses Modell wurde ursprünglich zur Abbildung von Zugriffsrechten in Betriebssystemen von LAMPSON [Lamp74] entworfen und nach weite-

[73] Vgl. hierzu das Beispiel zu Vertraulichkeit in Kapitel 5.4.3.3.

ren Entwicklungsschritten durch HARRISON, RUZZO und ULLMANN unter der Bezeichnung HRU-Model [Har+76] formalisiert. Um Zugriffskontrollmatrizen praktisch einsetzbar zu gestalten, muss eine Aufteilung der Matrix erfolgen. Hierbei wird unterschieden zwischen einer Aufteilung anhand der Spalten und deren Zuweisung zu Informationsobjekten sowie einer Aufteilung nach Reihen und deren Zuweisung zu Benutzern. Im ersten Fall spricht man von der Verwendung von **Access Control Lists** (ACL), im zweiten Fall von **Capabilities** (C-List) [Stam06, 179].

Sicherheitsmodelle im Bereich MAC

Für Sicherheitsmodelle des Sektors MAC existieren unterschiedliche Kategorien. Neben der bereits angesprochenen MLS können weiterhin zum Beispiel die Modelltypen Multilateral Security, Inference Control oder Covert Channel identifiziert werden. Der folgende Abschnitt zeigt exemplarisch Modelle des ersten Typs MLS auf, für einen Überblick der anderen Modelltypen sei zum Beispiel auf [Ecke06] oder [Stam06] verwiesen.

Als populärstes Sicherheitsmodell des Typs MLS kann das **Bell-LaPadula-Modell** [BeLa73] angeführt werden. Es wurde in den 1970ern für die US Air Force entwickelt und gilt als das erste vollständig formalisierte Zugriffskontrollmodell, das sich im Wesentlichen auf das Schutzziel der Vertraulichkeit von Informationen bezieht. Weitere bekannte Sicherheitsmodelle sind zum Beispiel das Biba-Modell [Biba77] mit Fokus auf der Integrität von Informationen, das Brewer-Nash-Modell (Chinese-Wall-Modell) [BrNa89] oder das Clark-Wilson-Modell [ClWi87]. Eine allgemeine Klassifikation von Sicherheitsmodellen der Zugriffskontrollstrategie MAC ist in [Mura01] zu finden, eine inhaltliche Darstellung in [StHu06].

Sicherheitsmodelle im Bereich RBAC

Rollenbasierte Zugriffskontrollstrategien wurden in Form des namensgebenden Sicherheitsmodells RBAC bereits 1992 durch FERRAIOLO und KUHN formal beschrieben [FeKu92]. Eine Standardisierung erfolgte nach diversen Erweiterungen als vereinheitlichtes Modell für RBAC im Jahr 2004 durch das American National Standards Institute / International Committee for Information Technology Standards (ANSI/INCITS) als Norm ANSI INCITS 359-2004. Das hierin beschriebene Referenzmodell wird in die drei zentralen Segmente **Core RBAC**, **Hierarchical RBAC** und **Constrained RBAC** unterteilt. Der Teil Core RBAC definiert dabei die grundlegenden Zusammenhänge zwischen Benutzern, Rollen und Sessions, Hierarchical RBAC spezifiziert darauf aufbauend die Grundlagen zur Bildung von Rollenhie-

rarchien. Im Bereich Constrained RBAC schließlich wird der Grundsatz der Separation of Duty (SoD) in das Modell integriert[74]. Zusammen bilden diese Komponenten die Grundlage, auf der die Implementierung konkreter RBAC-Systeme in der Praxis in Konformität zu der Norm erfolgen sollte [Clar07, 753ff].

Bezug zu Schutzzielen

Zugriffskontrollstrategien als Sicherheitsmechanismen beziehen sich primär auf die Erreichung der Schutzzielklassen Vertraulichkeit und Integrität. Analog zu den identifizierten Abhängigkeits- und Wirkungsbeziehungen dieser Schutzzielklassen werden weiterhin indirekt die Bereiche Verfügbarkeit und Verbindlichkeit adressiert. Sicherheitsmodelle, als Verfahren zur Umsetzung dieser Zugriffskontrollstrategien, geben hierbei durch ihre unterschiedlichen formalen Ansätze die Ausrichtung des jeweiligen Mechanismus auf entsprechende Schutzzielklassen vor. Im Bereich der MAC sind zum Beispiel insbesondere das Biba- oder das Clark-Wilson-Modell primär auf die Integrität zu schützender Informationen ausgerichtet, wohingegen der Fokus des Bell-LaPadula-Modells sowie des Brewer-Nash-Modells eher auf der Schutzzielklasse Vertraulichkeit liegt [Kers95, 105] [Schi99, 125ff].

5.5.4. Sicherheitsmechanismen der Beweissicherung und des Auditing

Die Sicherstellung von Beweisen sicherheitsrelevanter Vorfälle erfolgt in betrieblichen Informationssystemen durch den Sicherheitsmechanismus der **Protokollierung.** Diese kann für verschiedene Komponenten und Ereignisse eines betrieblichen Informationssystems definiert werden. Das BSI verzeichnet zum Beispiel für Server in der Maßnahme 5.9 der IT-Grundschutz-Kataloge aufzeichnungsrelevante Vorkommnisse bzw. Messgrößen wie falsche Passworteingaben, Versuche von unberechtigten Zugriffen, Stromausfällen oder allgemeinen Daten zur Netzauslastung [BSI09, 3416]. Jedoch ist dieses Themenfeld nicht ausschließlich auf den technischen Bereich zu reduzieren. Die Erfassung von Protokolldaten zur Erbringung des Nachweises über den korrekten Ablauf eines Prozesses stellt, auch im Hinblick auf deren rechtsverbindliche Nutzbarkeit, einen zentralen und auch kritischen Sicherheitsmechanismus dar.

[74] SoD bezeichnet ein allgemeines Sicherheitsprinzip, das die Möglichkeit der alleinigen Durchführung von sicherheitsverletzenden Aktionen durch ein Individuum zu verhindern hilft. Einen umfassenden Einblick hierzu gibt [Sand90].

Protokollierung

Vor dem skizzierten Hintergrund ergeben sich vielfältige prozess-, sicherheits- und organisationsbezogene Anforderungen an die Güte, Vertraulichkeit, Integrität und Vollständigkeit der Protokolldaten sowie an die sie generierende Prozesskette[75]. Eine Verletzung dieser Anforderungen, zum Beispiel durch die Möglichkeit der unautorisierten nachträglichen Manipulation von Protokolldaten, führt zum Verlust der Integrität der Daten und kann somit eine rechtsverbindliche Analyse und Nutzung verhindern. Insbesondere im Bereich der Kompromittierung von Rechnern und Betriebssystemen durch sogenannte Rootkits wird dieser Ansatz oftmals verfolgt, um die Präsenz der Schadsoftware zu verschleiern. Neben der reinen Erfassung der Protokolldaten ist somit auch deren integritätssichere Speicherung von großer Bedeutung für die Verwertbarkeit der gesammelten Daten. Aus Sicht von technischen Lösungen ist dies, vor allem für heterogene Systemumgebungen, zum aktuellen Zeitpunkt jedoch noch nicht umfassend realisiert [Wolt06, 284]. Insbesondere die exakte Identifizierung eines Zeitpunktes, ab dem eine Kompromittierung stattgefunden hat und Protokolldaten daher potentiell nicht mehr vertrauenswürdig sind, ist zum Beispiel Gegenstand der aktuellen Forschung [Wolt07, 743].

Weitere Aspekte stellen die Menge an Protokolldaten sowie deren Inhalte dar, die, auch in Abhängigkeit von dem jeweiligen Schutzbedarf, auf verschiedenen Abstraktionsstufen von den technischen Abläufen bis hin zur Semantik von Geschäftsprozessen vorliegen können [Wolt06, 281]. Neben der rein wirtschaftlichen Betrachtung der Kostensituation für die sichere Speicherung solcher Datenmengen, sind jedoch auch gesetzliche oder vertragliche Regelungen bezüglich Protokollinhalten, Aufbewahrungsfristen oder Zweckbindungen zu berücksichtigen. In der Bundesrepublik Deutschland greifen hierbei primär die Regelungen des Bundesdatenschutzgesetzes, hinsichtlich der Zweckbindung die Paragraphen 14 und 31, in Bezug auf Fristen der Paragraph 20 [Bund90].

Auditing

Zusammengefasst werden die dargestellten Anforderungen und Rahmenbedingungen oftmals durch die Verwendung des Begriffs der „**revisionssicheren Protokollierung**“. Das zu Grunde liegende Begriffsverständnis ist dabei analog zu dem der revisionssicheren Archivierung elektronischer Informationen im Rahmen des Handelsgesetzbuches [Bund97] zu verstehen

[75] Für eine allgemeine Darstellung dieser Anforderungen sei auf [Wolt06] verwiesen, konkret werden sie zudem in der Maßnahme M 2.110 der IT-Grundschutz-Kataloge aufgeführt [BSI09, 1286ff].

und schließt die Beachtung entsprechender Prozesse der Erfassung, Speicherung aber auch der korrekten Auswertung und Analyse mit ein. Die beiden letztgenannten Teilprozesse beziehen sich dabei auf die Verwertung der gesammelten Protokolldaten und werden in der Regel unter dem englischsprachigen Begriff **Auditing** in der Literatur subsumiert. Hiervon zu differenzieren ist jedoch der Bereich des allgemeinen IT- oder Sicherheits-Audits, der sich mittlerweile als umfassender Begriff für in gewisser Weise standardisierte Prüfungen im Umfeld der IT-Compliance etabliert hat[76]. Prozesse der Protokollauswertung können in diesem Zusammenhang als Teilbereich betrachtet werden.

Bezug zu Schutzzielen

Alle exemplarisch genannten Anwendungen stellen konkrete Sicherheitsmechanismen der Grundfunktion Beweissicherung und Auditing dar, die sich auf die Schutzzielklasse der Verbindlichkeit beziehen. Sie bauen dabei im Prinzip jedoch auf weiteren Sicherheitsgrundfunktionen wie der Authentisierung oder der Zugriffskontrolle auf. Nur wenn diese Grundfunktionen realisiert und deren Schutzzielklassen Vertraulichkeit und Integrität gesichert sind, wird schlussendlich auch eine revisionssichere Protokollierung und entsprechendes Auditing ermöglicht. Diese Zusammenhänge korrelieren mit den Abhängigkeitsbeziehungen, die im Rahmen der Schutzzielanalyse spezifiziert wurden.

5.5.5. Sicherheitsmechanismen der Unverfälschtheit

Die Grundfunktion der Unverfälschtheit zielt auf die Erhaltung der **Integrität** von Informationen ab. Dabei wird hauptsächlich der Aspekt der absichtlichen, unautorisierten Manipulation betrachtet. Ein Verlust der Integrität, die zum Beispiel durch maschinell fehlerhaftes Speichern der Informationen auf Massenspeicher verursacht wird, ist nicht Bestandteil dieser Grundfunktion und dem Bereich der Safety zuzuordnen.

Sicherheitsmechanismen der Grundfunktion Unverfälschtheit variieren kontextabhängig, je nachdem in welchem Bearbeitungszustand sich die Informationen befinden. Hauptsächlich zu unterscheiden sind hierbei die Zustände der **Speicherung**, der **Bearbeitung** oder der **Übertragung**.

Im ersten Fall greifen Mechanismen, die die Integrität von Daten in Datenbanken bzw. auf Massenspeichern sicherstellen. Diese Funktionalität wird zum Beispiel von speziellen Datei-

[76] Zum Bereich der IT-Compliance vgl. z. B. [Rath09] sowie Kapitel 6.3.2.

systemen erbracht oder im Rahmen der Sicherung von Integritätsbedingungen durch Datenbankmanagementsysteme (DBMS).

Befinden sich Informationen in Bearbeitung, so obliegt es dem entsprechenden Anwendungssystem deren Integrität sicherzustellen. Erreicht wird dies durch entsprechend implementierte Komponenten, die Benutzereingaben und Datenmanipulationen validieren. Die Erbringung der Grundfunktionen Identifikation und Authentisierung sowie Zugriffskontrolle und Autorisierung in Bezug auf die Applikation sind hierbei zusätzlich als Voraussetzung zu verstehen, um eine semantische Unverfälschtheit der Informationen erreichen zu können.

Im Bereich der Übertragung von Informationen werden die Sicherheitsmechanismen primär durch Methoden der Kryptologie bereitgestellt. Hierbei sind es insbesondere die bereits vorgestellten Verfahren der digitalen Signatur und Hashfunktionen, die in diesem Rahmen zum Einsatz kommen.

5.5.6. Sicherheitsmechanismen der Wiederaufbereitung

In Rechnersystemen sind hardwareabhängige Ressourcen nur in begrenztem Umfang verfügbar. Aus diesem Grund kommt es zu einem hohen Grad an Wiederverwendung dieser Betriebsmittel, insbesondere im Bereich des Massen- und Hauptspeichers. Durch die Sicherheitsmechanismen der **Wiederaufbereitung** soll sichergestellt werden, dass über diese Speichermedien kein unzulässiger Informationsfluss von vergangenen Nutzungen zur aktuellen Verwendung stattfinden kann. Das primäre Ziel ist somit die Sicherstellung der Vertraulichkeit. Erreicht wird dies durch Mechanismen, die eine valide und somit nicht rekonstruierbare Löschung von Speicherbereichen ermöglichen [Kurt93, 100]. Ein typisches Beispiel sind Anwendungen zum sicheren Löschen von Dateien auf Festplatten, die durch mehrmaliges Überschreiben entsprechender Speicherbereiche mit Zufallswerten eine spätere Rekonstruktion der Daten verhindert.

Zu beachten gilt, dass diese Mechanismen insbesondere in Ausnahmefällen des täglichen Betriebs zum Einsatz kommen sollten. Dies ist immer dann der Fall, wenn Dritte, zum Beispiel im Rahmen einer Reparatur oder Geräteentsorgung, physischen Zugriff auf die entsprechenden Geräte erhalten könnten. Die Art und der Zeitpunkt der Wiederaufbereitungsaktionen sind somit entsprechend der jeweiligen Sicherheitsanforderungen und Situationen festzulegen.

5.5.7. Sicherheitsmechanismen der Übertragungssicherung

Wie bereits dargestellt wurde, bezieht sich der Bereich **Übertragungssicherung** ausschließlich auf die Sicherstellung der Vertraulichkeit von Daten beim Transfer zwischen Systemen. Zum Einsatz kommende Sicherheitsmechanismen sind hierbei insbesondere Lösungen der Kryptologie, wie zum Beispiel symmetrische oder asymmetrische Verschlüsselungsverfahren oder auch der im Umfeld von Unternehmen häufige Einsatz einer PKI.

Technische Realisierungsformen dieser Sicherheitsmechanismen stellen Implementierungen der jeweiligen kryptographischen Verfahren dar, oftmals in Abstimmung mit der Integration in bestehende IT-Infrastrukturen. Ein konkretes Beispiel sind etwa Verschlüsselungsgateways für den E-Mail-Verkehr, die auf Basis einer PKI ausgehende Nachrichten für Nutzer transparent verschlüsseln.

5.5.8. Sicherheitsmechanismen der Zuverlässigkeit

Die **Betriebsbereitschaft**, als zentraler sicherheitsrelevanter Aspekt der Sicherheitsgrundfunktion Zuverlässigkeit, adressiert die Verfügbarkeit von Anwendungssystemen und Informationen.

Entsprechende Sicherheitsmechanismen beziehen sich darauf, dass Informationen oder Anwendungssysteme gemäß ihrer Bestimmung nutzbar sind. Konkrete Formen sind zum Beispiel Geräte zur Lastverteilung (Load-Balancer), die eingehende Anfragen anhand spezifischer Verfahren last- und damit reaktionszeitoptimierend auf einen Pool an Anwendungssystemen verteilen. Weiterhin können sogenannte Intrusion Detection Systeme (IDS) in dieser Kategorie aufgeführt werden, da durch sie Verfügbarkeitseinschränkungen durch möglichst frühzeitige Erkennung eines Angriffs vermieden werden können [NiJa06].

5.5.9. Zusammenfassung

Mechanismen der Grundfunktionen Identifikation und Authentisierung sowie der Zugriffskontrolle und Autorisierung sind zum aktuellen Zeitpunkt als sehr relevant für die Praxis einzustufen. Dies ist zum einen darin begründet, dass Firmen ihre internen Netzwerke für externe bzw. mobile Mitarbeiter zunehmend öffnen müssen, um entsprechende Arbeitsprozesse des Außendienstes auch unterstützen zu können. In der Folge sind die grundlegenden Kanäle für einen Zugriff auf interne Netzwerke aus technischer Sicht für jedermann gegeben, es liegt

somit an der Zugriffskontrollverfahren, diese Zugriffe in korrekter Weise zu autorisieren. Begleitet wird diese Entwicklung auch durch eine zunehmende Konsolidierung der angebotenen Dienste und Anwendungssysteme, die in ihrer Gesamtheit in diesem Zuge mit möglichst nur einer Authentisierungsaktion für Benutzer erreichbar sein sollen. Dieser als Single-Sign-On bezeichnete Bereich der Identifikation und Authentisierung stellt hohe Ansprüche an die Migration und Aufbereitung von bestehenden Nutzerdaten und wird im Rahmen des Identity Management aktuell in hohem Maße diskutiert. Als Basismaschine fungiert in diesem Zusammenhang eine Authentisierungs- und Autorisierungsinfrastruktur (engl. *authentication and authorization infrastructure*, AAI), die den Austausch von sicherheitsrelevanten Informationen, wie zum Beispiel Nutzerattributen in einem Dienstverbund, unterstützt [Pri+07, 27].

Einhergehend mit dieser Entwicklung steigt auch die Forderung nach wirkungsvoller Verschlüsselung, die gerade die in externe Netze übertragenen Daten wirkungsvoll gegen unautorisierten Zugriff schützt. Ziel für Unternehmen muss in diesem Zusammenhang sein, die diesbezüglichen Mechanismen und Verfahren zu integrieren und für Nutzer möglichst aufwandsfrei zur Verfügung zu stellen. Als grundlegender Ansatz wird hierbei oftmals eine PKI gewählt, um über zentrale Ver- und Entschlüsselungsgateways in Unternehmen die Verwendung der Kryptographie für Benutzer transparent zu gestalten. Analog dazu bilden die Funktionen der Protokollierung eine querschnittliche Grundlage, auf Basis derer auch die Wirksamkeit der besprochenen Verfahren analysiert werden kann. Im Rahmen der Neuentwicklung von Anwendungssystemen haben diese Themen aus Sicht der Informationssicherheit somit einen hohen Stellwert.

Die Bereiche Zuverlässigkeit, Unverfälschtheit und Wiederaufbereitung hingegen können aus dieser Perspektive als vergleichsweise infrastrukturnah interpretiert werden. Die Zuverlässigkeit wird primär durch dedizierte Systeme und Redundanzen in Hardware gesichert, das Thema Wiederaufbereitung ist weniger von Mechanismen als vielmehr von organisatorischen Richtlinien abhängig, entsprechende Werkezuge sind problemlos verfügbar. Gleiches gilt für die Sicherheitsgrundfunktion der Unverfälschtheit, die sich in hohem Maße auf systemnahe Komponenten zur Integritätssicherung bezieht. Im Bereich der digitalen Kommunikation werden Mechanismen der Integritätssicherung zudem durch die Ansätze der Kryptologie abgedeckt, die im Rahmen der Übertragungssicherung bereits zum Einsatz kommen. Die drei letztgenannten Sicherheitsgrundfunktionen haben vor diesem Hintergrund im Rahmen der

vorliegenden Arbeit nur geringere Bedeutung und werden, insbesondere in Teil III der Arbeit, nicht weiter betrachtet.

Mit der exemplarischen Darstellung technischer Sicherheitsmechanismen wurde die Schemaebene der Strukturmodellierung betrieblicher Informationssicherheit vollständig beschrieben. Auf der Grundlage dieser inhaltlichen Erläuterungen zu dem in Kapitel 4 definierten Meta-Modell, wird im folgenden Kapitel ein Referenzmodell betrieblicher Informationssicherheit vorgestellt.

6. Ein Referenzmodell betrieblicher Informationssicherheit

Auf Basis der dargestellten Ausprägungen der Schemaebene anhand der Systematisierungsmatrix, kann ein Referenzmodell der betrieblichen Informationssicherheit gebildet werden. Die folgenden Ausführungen nehmen dabei explizit Bezug auf das betriebliche Informationssystem einer Unternehmung. Die inhaltliche Ausrichtung bezieht sich somit auf Ressourcenebene ausschließlich auf maschinelle Aufgabenträger in Form betrieblicher Anwendungssysteme.

Kapitel 6.1 beschreibt den Aufbau des Referenzmodells, bevor in Kapitel 6.2 unterschiedliche Interpretationsmöglichkeiten auf Basis des Modells vorgestellt werden. In Kapitel 6.3 werden im Anschluss bestehende Disziplinen und Verfahren der Informationssicherheit auf der Grundlage des Referenzmodells evaluiert. Mit einem zusammenfassenden Fazit in Kapitel 6.4 wird Teil II der vorliegenden Arbeit abgeschlossen.

6.1. Aufbau des Referenzmodells

Referenzmodelle beziehen sich auf eine Klasse von Anwendungsfällen und stellen für die Entwicklung spezifischer Modelle einen Bezugspunkt dar [Thom06, 5]. Als wesentliche Merkmale des Begriffs werden die Allgemeingültigkeit sowie der Empfehlungscharakter beschrieben, jeweils eingeschränkt auf die entsprechende Klasse von Anwendungsfällen, auf die sich ein Referenzmodell bezieht [Thom06, 12f].

Im Rahmen der vorliegenden Arbeit wird ein **Referenzmodell betrieblicher Informationssicherheit** als Instanz des Typs Strukturmodell angesehen. Es ist dadurch gekennzeichnet, das alle vorgestellten Ausprägungen der Meta-Objekttypen auf Schemaebene in diesem Modell zueinander in Beziehung gesetzt sind. In Bezug auf die vorgestellte Systematisierungsmatrix besteht es somit aus der Belegung und Kombination aller aufgeführten Felder. Auf diese Weise entsteht ein Strukturmodell, das, unter dem Blickwinkel der vorliegenden Arbeit, eine umfassende Einbettung des Themengebiets der Informationssicherheit in den Kontext eines betrieblichen Systems darstellt. Es bildet daher eine Referenz, anhand derer auch weitere Aspekte der Informationssicherheit integriert und systematisiert werden können. Die folgende Abbildung stellt das in dieser Arbeit verwendete Referenzmodell dar.

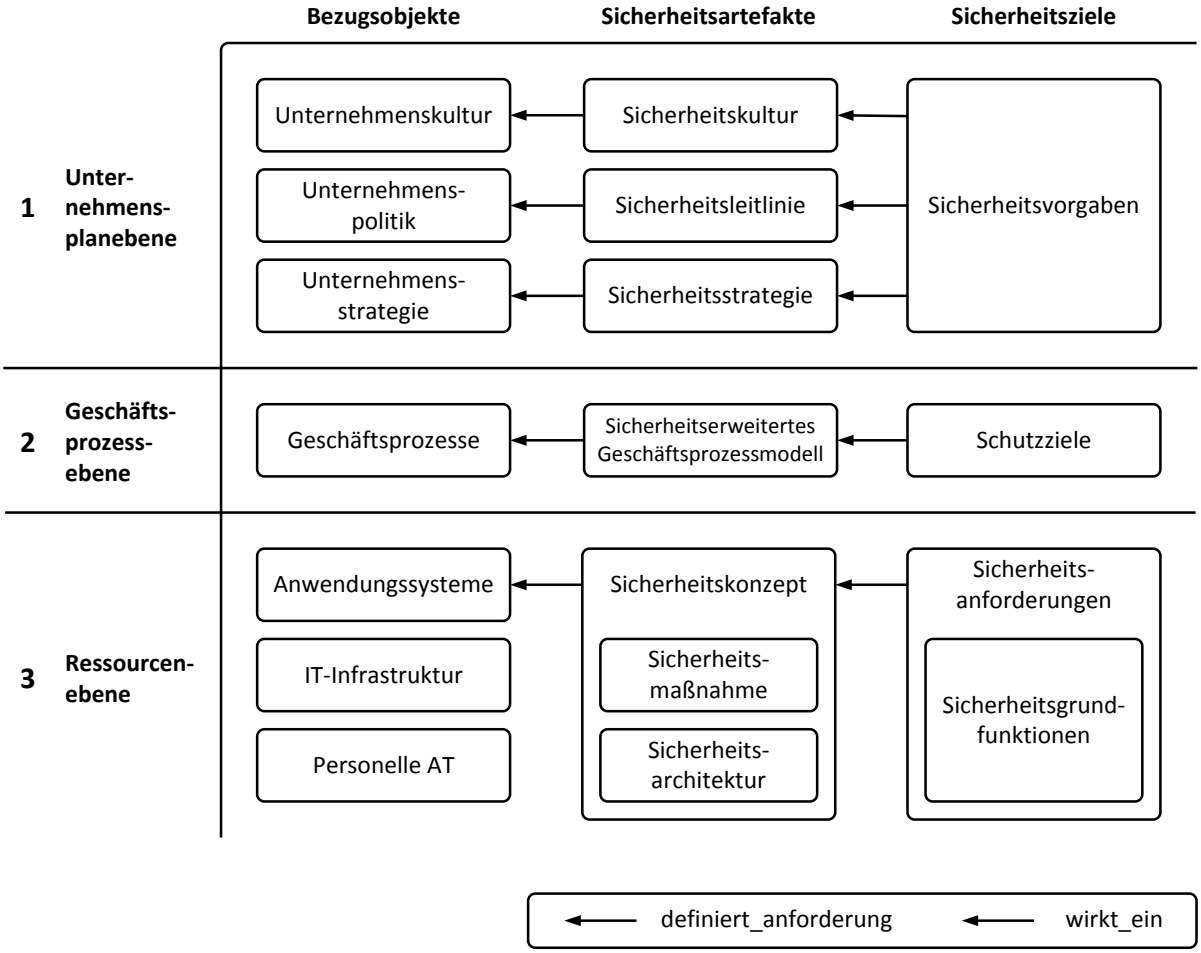

Abbildung 26: Referenzmodell betrieblicher Informationssicherheit

Die Modellelemente des Referenzmodells entsprechen den in Kapitel 5 vorgestellten Extensionen der Meta-Objekttypen auf Schemaebene. Die Beziehungen zwischen den Objekttypen werden anhand der Pfeildarstellungen symbolisiert[77]. Die Zusammenhänge sind dabei ebenenspezifisch zu betrachten und entsprechen als Tripel inhaltlich den Komponenten der zu Grunde liegenden Teilaufgaben betrieblicher Informationssicherheit.

Die dargestellten Objekttypen des Referenzmodells stellen in gewisser Weise einen Idealzustand dar, da jede Dimension der Informationssicherheit (Bezugsobjekt, Sicherheitsartefakt, Sicherheitsziel) auf jeder Ebene der Unternehmensarchitektur (Unternehmensplan, Geschäftsprozesse, Ressourcen) Berücksichtigung findet. Dieser Sachverhalt korrespondiert mit dem eingangs dargestellten Merkmal Empfehlungscharakter eines Referenzmodells, da auf diese

[77] Auf Ressourcenebene wird nur die Wirkungsbeziehung zwischen Sicherheitskonzept und Anwendungssystem dargestellt, um den Fokus der Ausführungen hervorzuheben.

Weise eine umfassende Berücksichtigung der Informationssicherheit im betrieblichen Kontext erfolgen kann.

Die ebenfalls angesprochene Allgemeingültigkeit des Referenzmodells, wird durch eine sehr abstrakte Definition der Modellbausteine unterstützt. Zwar wurden in vorhergehenden Kapiteln die inhaltliche Ausgestaltung der Elemente detailliert beschrieben, eine inhaltliche Festlegung im Hinblick auf zwingende Zusammenhänge auf Ausprägungsebene wurde jedoch explizit vermieden. Dieser Aspekt ermöglicht die flexible Nutzung des Referenzmodells als Analyseinstrument bzw. methodischer Rahmen für die Überprüfung bestehender Ansätze im Hinblick auf die Unterstützung der betrieblichen Informationssicherheit.

In den folgenden Abschnitten werden weitere Interpretationsmöglichkeiten auf Basis des Referenzmodells diskutiert.

6.2. Interpretation des Referenzmodells

Anhand des Referenzmodells können unterschiedliche Ableitungen vorgenommen und Rückschlüsse auf die Etablierung der Informationssicherheit im Unternehmen gezogen werden. Aus methodischen Gesichtspunkten erfolgt dies auf der Grundlage einer ebenenorientierten sowie einer hierarchischen Interpretation der dargestellten Beziehungen.

6.2.1. Ebenenorientierte Interpretation

Aus horizontaler Sichtweise können anhand des Tripels aus Bezugsobjekt, Sicherheitsartefakt und Sicherheitsziel entsprechende Tätigkeitsdisziplinen der betrieblichen Informationssicherheit abgeleitet werden. Die Sicherheitsziele einer Ebene definieren dann die Vorgaben einer abstrakten Aufgabe, die sich auf das Bezugsobjekt als Aufgabenobjekt bezieht und bei deren Durchführung das entsprechende Sicherheitsartefakt erzeugt wird.

Diese Teilaufgaben der grundlegenden Meta-Aufgabe können analog zur Differenzierung des Informationsmanagements nach FERSTL und SINZ [FeSi08, 439ff] untergliedert werden. Es ergeben sich **strategische**, **taktische** und **operative Aufgabenbereiche**, die mit den Ebenen des Referenzmodells aus Top-Down-Sicht korrespondieren. In der Praxis haben sich für diese Aufgabenbereiche stark abweichende Bezeichnungen und auch Systematiken herausgebildet. Aktuell werden strategische und taktische Aspekte der Informationssicherheit zum Beispiel in

die Tätigkeitsfelder IT-Governance und IT-Compliance abgebildet, im operativen Bereich der Anwendungsentwicklung wird die Teilaufgabe der Informationssicherheit unter dem Begriff Security Engineering subsumiert[78]. Die angesprochenen Teildisziplinen werden inhaltlich in Kapitel 6.3.2 bzw. 6.3.3 auf der Grundlage des Referenzmodells erläutert.

6.2.2. Hierarchische Interpretation

Neben der horizontalen ist auch eine vertikale Analyse der Modellelemente des Referenzmodells möglich. Auf Basis der getroffenen Unterteilung in strategische, taktische und operative Aufgaben der Informationssicherheit, sind hierbei in Bezug auf die einzelnen Merkmale inhaltlich ähnliche Beziehungsarten festzustellen. Aus Top-Down-Sicht betrachtet sind diese allgemein durch eine zunehmende **Konkretisierung** charakterisiert.

Ausprägungen des Meta-Objekttyps Bezugsobjekt sind dabei maßgeblich durch den Übergang von Lenkungs- zu Leistungssystem beeinflusst. Hierbei erfolgt eine zunehmende Konkretisierung einer strategischen Unternehmensplanung hin zu konkreten, operativen Ressourcen. Analog zu diesem Zusammenhang entwickeln sich auch die Charakteristika der Sicherheitsartefakte. Hier ist eine Transformation von organisatorisch, rechtlichen Inhalten hin zu technisch orientierten Lösungsverfahren zu verzeichnen. In ähnlicher Weise erfolgt ein entsprechender Wandel der ebenenspezifischen Schutzziele, von rechtlichen oder ökonomischen Zielen ausgehend hin zu konkreten Sicherheitsanforderungen für betriebliche Anwendungssysteme.

Legt man hierzu die im vorangehenden Abschnitt dargestellte aufgabenorientierte Sichtweise zu Grunde, so wird deutlich, dass ein sequenzieller Durchlauf der Teildisziplinen von oben nach unten den abstrakten Aufgabenbereich eines umfassenden, unternehmensweiten Sicherheitsprozesses vollständig umfasst. In Kapitel 6.3.1 erfolgt eine exemplarische Darstellung dieser Zusammenhänge anhand des durch das BSI vorgeschlagenen Sicherheitsprozesses.

6.2.3. Erkenntnisgewinn

Anhand der Ausführungen der letzten beiden Abschnitte wird bereits ersichtlich, dass die Geschäftsprozessebene in der praktischen Wahrnehmung der Informationssicherheit nur eine

[78] In Anlehnung an die Untergliederung des Themenkomplexes der Informationssicherheit in Kapitel 3.1.2 kann das Security Engineering als Bestandteil des Bereichs IT-Sicherheit betrachtet werden. IT-Governance und -Compliance haben entsprechende Berührungspunkte zum Bereich der Prozesssicherheit.

untergeordnete Rolle spielt. So hat sich in der Literatur weder ein Begriff für die Berücksichtigung von Informationssicherheit auf Geschäftsprozessebene herausgebildet, noch gibt es populäre Ansätze, die diesen Aufgabenbereich adressieren. Ebenfalls können in der vertikalen Betrachtung des Modells keinerlei existente Ansätze erkannt werden, die in der Praxis den sicherheitsorientierten Übergang zwischen strategischer Planung und operativer Umsetzung durch geeignete Mittel, wie es die Geschäftsprozessmodellierung darstellt, ermöglichen.

Dieser Sachverhalt stellt den zentralen Ansatzpunkt und auch die Motivation dar, um den in Teil III der Arbeit beschriebenen Ansatz zur **Modellierung betrieblicher Informationssicherheit auf Geschäftsprozessebene** vorzustellen. Durch diesen Modellierungsansatz entsteht ein Sicherheitsartefakt, das sich explizit auf Geschäftsprozesse bezieht und die entsprechenden Sicherheitsziele in Form der Schutzziele in adäquater Weise integrieren kann. Der Übergang zwischen erster und dritter Ebene des Referenzmodells wird somit im Hinblick auf jedes Merkmal in konsistenter Weise unterstützt und die bereits angesprochene semantische Lücke im Kontext der betrieblichen Informationssicherheit vermieden.

6.3. Analysen auf Basis des Referenzmodells

Auf Basis des vorgestellten Referenzmodells können bestehende Ansätze der Informationssicherheit analysiert bzw. evaluiert werden. Dies erfolgt zum einen durch den Abgleich der jeweiligen Ansätze mit dem Referenzmodell, zum anderen durch die Ableitung von Teildisziplinen anhand der ebenenorientierten Interpretation des Referenzmodells. Im weiteren Verlauf dieses Kapitels werden diese Vorgehen exemplarisch anhand von drei Beispielen aufgezeigt. Die fachliche Zielsetzung liegt dabei einerseits in der exemplarischen Eingliederung praxisrelevanter Teilaufgaben in den Themenkomplex der Informationssicherheit sowie, damit einhergehend, in der Evaluation des Referenzmodells im Sinne einer generischen Verwendbarkeit.

6.3.1. BSI Sicherheitsprozess

Das BSI stellt mit vier BSI-Standards zur Informationssicherheit sowie den IT-Grundschutzkatalogen eine umfassende Sammlung an Publikationen zum Thema Informationssicherheit bereit[79]. Das Vorgehensmodell aus dem BSI-Standard 100-2 verfolgt in diesem

[79] Vgl. hierzu Kapitel 5.4.2.2.

Zusammenhang einen schrittweisen Ansatz für den Aufbau und auch den Betrieb eines ISMS in der Praxis. Kernaspekte sind dabei unter Anderem relevante Management- und Organisationstrukturen auf der einen sowie die praktische Realisierung eines Sicherheitskonzeptes und die Auswahl von Sicherheitsmechanismen auf der anderen Seite. Diese einzelnen Aspekte werden in Form des **Sicherheitsprozesses des BSI** systematisiert, der aus den folgenden Hauptphasen besteht [BSI08b]:

- Initiierung des Sicherheitsprozesses
- Erstellung einer Sicherheitskonzeption
- Umsetzung der Sicherheitskonzeption
- Aufrechterhaltung der Informationssicherheit im laufenden Betrieb und kontinuierliche Verbesserung

Die erste und zweite Phase werden in der Standardbeschreibung noch weiter detailliert. Die folgende Abbildung stellt alle Haupt- und Teilphasen des Sicherheitsprozesses grafisch dar.

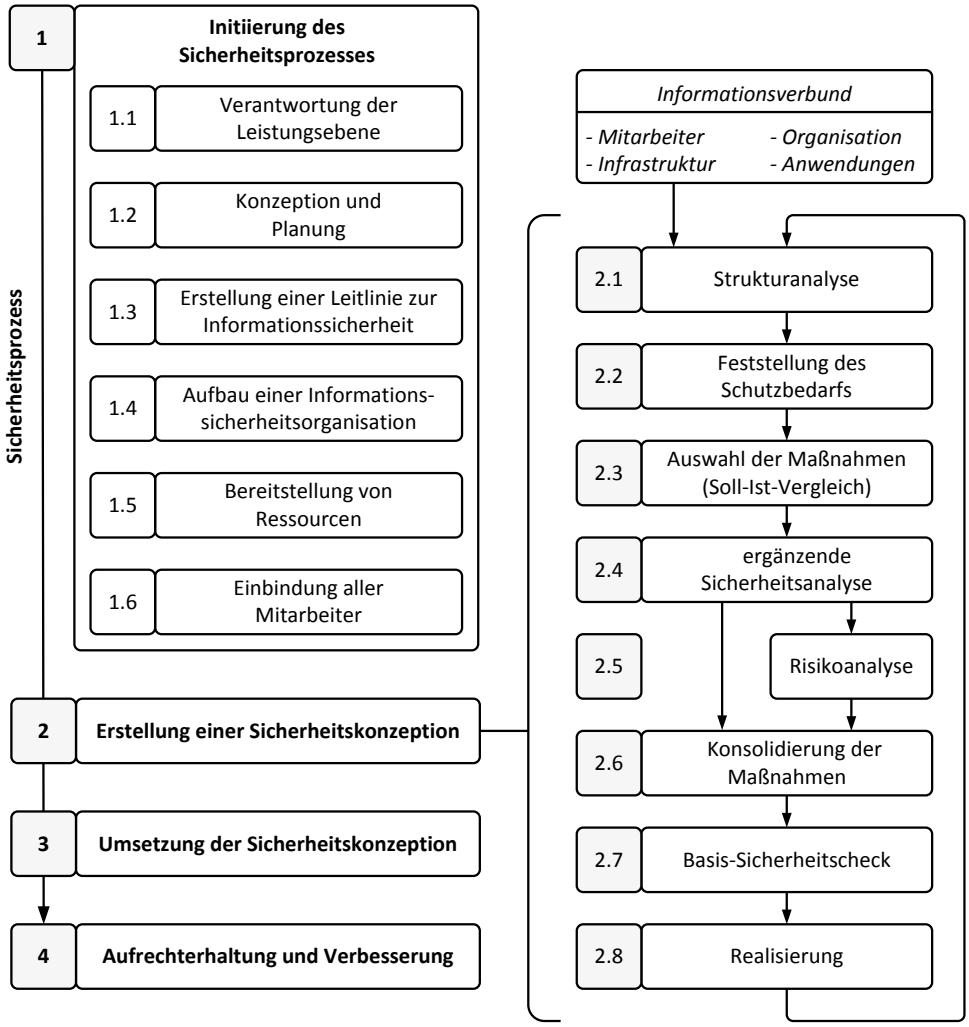

Abbildung 27: Sicherheitsprozess des BSI (nach [BSI08b, 13], [BSI08b,36])

Insbesondere die zweite Phase der **Erstellung einer Sicherheitskonzeption** wird anhand eines eigenen Vorgehensmodells weiter verfeinert. Als Basis dient der sogenannte Informationsverbund, der, in der Sichtweise der vorliegenden Arbeit, die Bezugsobjekte des Prozesses abbildet.

Als Bezugsobjekte des Sicherheitsprozesses können hauptsächlich Elemente der Ressourcenebene identifiziert werden. Die Ebene des Unternehmensplans findet jedoch in Phase eins zumindest teilweise Berücksichtigung, wohingegen auf Geschäftsprozesse keinerlei Bezug genommen wird. Nutzt man diesen Sachverhalt als Ausgangsbasis, so können in einem nächsten Schritt die unterstützten Sicherheitsartefakte des Sicherheitsprozesses analysiert werden. Hierunter werden insbesondere die Teilaufgaben des Sicherheitsprozesses verstanden, deren Zielsetzung einen gewissen Ergebnischarakter im Sinne der Definition der Sicherheitsartefak-

te in dieser Arbeit aufweisen. Anhand der Systematik der Sicherheitsartefakte des Referenzmodells lassen sich dann die entsprechenden Phasen des BSI-Sicherheitsprozesses einordnen.

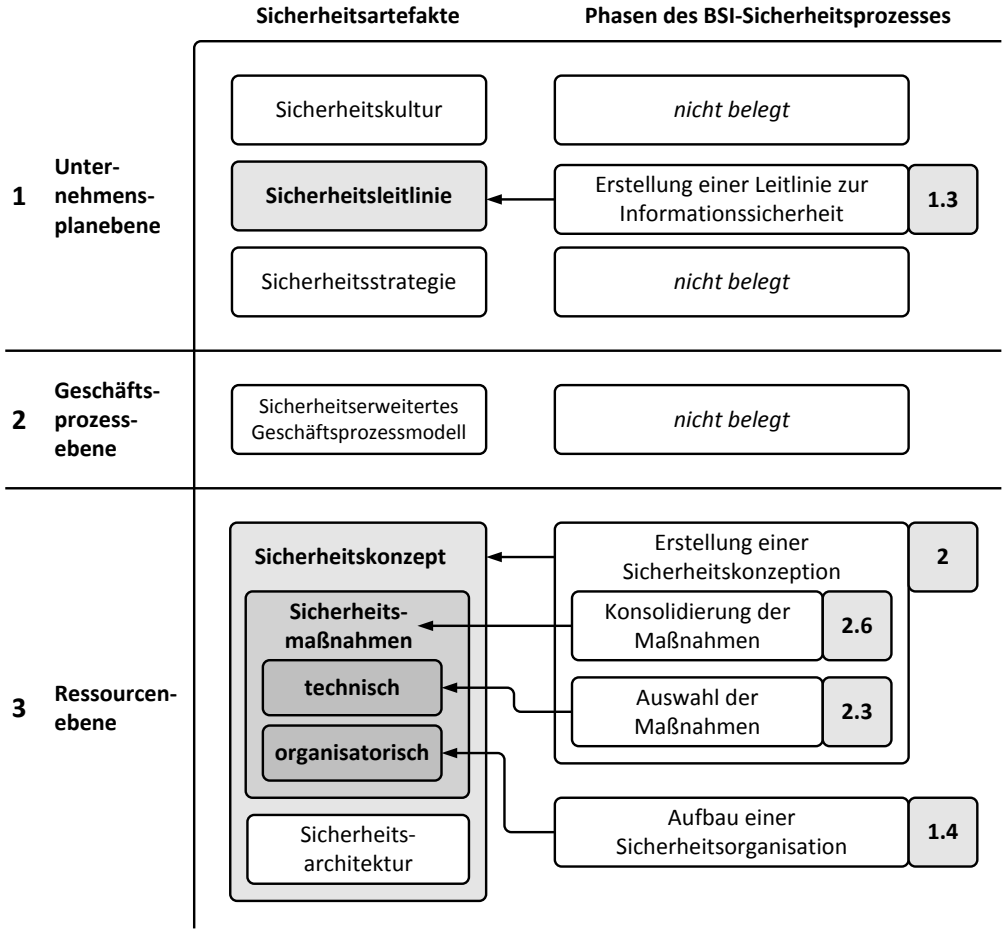

Abbildung 28: Sicherheitsprozess des BSI anhand des Referenzmodells

Die in der rechten Spalte dargestellten Teilphasen des Sicherheitsprozesses finden ihre Entsprechung in den jeweils grau markierten Sicherheitsartefakten des Referenzmodells. Die in Phase 1.4 angesprochene Sicherheitsorganisation umfasst dabei primär die Organisation der Lenkungsebene im Sinne der Definition sicherheitsverantwortlicher Stellen, wie zum Beispiel die eines Datenschutzbeauftragten. Mögliche Auswirkungen auf das Sicherheitsartefakt der Sicherheitskultur in Bezug auf personelle Aufgabenträger auf Ressourcenebene sind in diesem Zusammenhang jedoch nicht zu identifizieren. Alle anderen Teilphasen sind in direkter Weise und eindeutig auf die Sicherheitsartefakte des Referenzmodells abbildbar.

Anhand dieser Analyse wird deutlich, auf welche Bereiche eines Unternehmens der Sicherheitsprozess des BSI Bezug nimmt. Der Schwerpunkt liegt mit der Spezifikation einer Sicherheitskonzeption klar auf der Ressourcenebene, die sowohl durch technische als auch durch

organisatorische Sicherheitsmaßnahmen umfassend adressiert wird. Der Grund hierfür dürfte sicherlich in der Einbindung der IT-Grundschutzkataloge in den BSI-Sicherheitsprozess liegen, die ebendiese Zielsetzung verfolgen. Die Ebene des Unternehmensplans wird weniger umfassend aber dennoch durch das Artefakt der Sicherheitsleitlinie berücksichtigt, wohingegen die Ebene der Geschäftsprozesse keinerlei Berücksichtigung im Rahmen des Sicherheitsprozesses findet. Vielmehr erfolgt ein direkter Übergang zwischen erster und dritter Ebene, der bereits in Kapitel 6.2.3 als großes Manko der aktuellen Situation beschrieben wurde.

Ein Vorgehen nach dem BSI-Sicherheitsprozess in Verbindung mit dem Einsatz von Sicherheitsmaßnahmen nach den IT-Grundschutzkatalogen ist zertifizierbar und beinhaltet dabei immer eine offizielle ISO-Zertifizierung nach ISO 27001. Vor diesem Hintergrund ist das Fehlen der Berücksichtigung von Geschäftsprozessen unter einer globaleren Sichtweise betrachtet als sehr kritisch einzustufen, da zu schließen ist, dass dieser Aspekt somit auch in den entsprechenden ISO-Standards nicht erfasst wird. Zu begründen ist dies durch die mangelnde Verfügbarkeit von Konzepten und Ansätzen, die eine entsprechende Berücksichtigung dieser Ebene auch im praktischen Einsatz erlauben. Mit der Vorstellung eines geschäftsprozessgetriebenen Modellierungsansatzes für betriebliche Informationssicherheit in Teil III will die vorliegende Arbeit einen Beitrag leisten, diesen Mangel zu reduzieren.

6.3.2. IT-Governance und IT-Compliance

IT-Governance und IT-Compliance gehen inhaltlich auf die umfassenderen Konzepte der Governance und Compliance im Unternehmenskontext zurück. **Corporate Governance** bezeichnet dabei die grundlegende Zielsetzung, entsprechende Bedingungen dafür herzustellen, dass die Unternehmensführung im Interesse des Unternehmens selbst sowie anderer Anspruchsgruppen, wie etwa Anteilseigner oder Mitarbeiter, zu handeln befähigt ist. Tätigkeitsschwerpunkte bilden dabei Führungs-, Überwachungs- und Prüfungsfunktionen, die durch entsprechende Stellen der Organisation auszufüllen sind [Köni06, 53f]. Unter **Corporate Compliance** wird in diesem Zusammenhang dann speziell die Umsetzung der notwendigen Kontrollmaßnahmen verstanden, die Konformität mit gesetzlichen Vorgaben oder auch Normen sicherstellen sollen [Rath09, 149].

IT-Governance und -Compliance sind analog zu den dargestellten Definitionen zu verstehen, mit der Einschränkung, dass sich die Inhalte der Lenkungsaufgaben nicht auf das ganze Unternehmen, sondern auf die Domäne der Informationsverarbeitung eines Unternehmens

beziehen. Die IT-Governance zielt somit speziell auf das Handeln des IT-Managements bzw. den Aufgabenbereich des Informationsmanagements ab und ist als Teilbereich der Corporate Governance zu verstehen [TeFe08, 403]. Der Bereich der IT-Compliance adressiert dann im Besonderen die Einhaltung von Vorgaben im Bezug auf Transparenz und Sicherheit im Rahmen der Aufgaben des betrieblichen Informationssystems. Die Spannweite der Aufgabenstellung reicht dabei von der Etablierung eines ISMS über die Sicherstellung der technischen Informationssicherheit bis hin zu Fragestellungen der gesetzeskonformen elektronischen Archivierung [Rath09, 149][80].

Einordnung in das Referenzmodell

Im Rahmen des Referenzmodells werden die spezifischen Ziele von IT-Governance und IT-Compliance über die **Sicherheitsvorgaben** der globalen Meta-Aufgabe definiert. Wie in Kapitel 5.4.2 bereits dargestellt wurde, sind dies insbesondere gesetzliche Regelungen sowie Normen und Standards, deren Umsetzung die Einhaltung der Regularien für Unternehmen vereinfachen. So werden zum Beispiel durch SOX Vorgaben an die Korrektheit des Rechnungswesens in Unternehmen gestellt. Da dieses in der Regel automatisiert als Teil des betrieblichen Informationssystems durchgeführt wird, ergeben sich spezifische Anforderungen bei der Prüfung der Konformität, die dann durch IT-Compliance Prozesse abgebildet werden können. Die Sicherheitsartefakte der ersten Ebene des Referenzmodells, insbesondere die **Sicherheitsstrategie**, berücksichtigen sodann die Anforderungen, die sich aus den Teilaufgaben der IT-Compliance und IT-Governance ergeben. Die genaue Darstellung, welche Formalziele sich auf welchen Teilbereich im Unternehmen beziehen und somit Einfluss auf die Inhalte der Sicherheitsartefakte nehmen, ist auf Grund des Umfangs nicht Bestandteil der vorliegenden Arbeit. Hierzu sei zum Beispiel auf [TeTe05] oder [TeFe08] verwiesen, die einen entsprechenden Überblick geben.

6.3.3. Security Engineering

Mit dem Begriff Security Engineering wird in der Literatur ganz allgemein der Entwicklungsprozess zur **Konstruktion sicherer Systeme** bezeichnet. Im Rahmen der Informationsverarbeitung ist diese Aussage bezogen auf die Entwicklung von Anwendungssystemen, die die Anforderungen der Informationssicherheit erfüllen. Security Engineering steht zum aktuellen

[80] Die Bildung dieser eigenständigen Disziplinen verdeutlicht die steigende Relevanz der Informationssicherheit, die zunehmend auch als strategischer Faktor in Unternehmen anerkannt wird.

Zeitpunkt jedoch nicht für systematische und etablierte Entwicklungsmethodiken, da dedizierte Ansätze und Vorgehensmodelle zwar Gegenstand der Forschung sind, sich jedoch noch nicht in der Praxis etabliert haben. Um Aspekte der Informationssicherheit in der Softwareentwicklung zu berücksichtigen, werden somit in der Regel bestehende Vorgehensmodelle um Sicherheitsaspekte erweitert [Ecke06, 152]. Security Engineering als Disziplin bezieht sich dabei jedoch nicht ausschließlich auf Anwendungssysteme, sondern auch auf die IT-Infrastruktur als deren Basismaschine. Unterschieden werden demzufolge unter anderem die Bereiche der „application security“ und der „infrastructure security“, die sich im Kern in der Art und Weise unterscheiden, mit welchen Methoden entsprechende Sicherheit erreicht werden kann [Somm07, 718f].

Ein zentraler Aspekt des Security Engineerings ist die Definition korrekter und vor allem konsistenter Sicherheitsanforderungen, die für ein Anwendungssystem im Rahmen der Anforderungsanalyse zu erfassen sind. Diese Teilaufgabe ist nicht nur aus technologischer Sicht als komplex einzustufen, sondern auch aus fachlicher Sicht im Rahmen der grundlegenden Festlegung benötigter Funktionen der Sicherheit. Oftmals kommt es bereits zu diesem Zeitpunkt zu widersprüchlichen Spezifikationen bzw. zu Anforderungen, die in Bezug auf eine bestimmte Bedrohungslage als ungeeignet zu bezeichnen sind [Ande01, 4].

Einordnung in das Referenzmodell

In Bezug auf das Referenzmodell kann die Disziplin des Security Engineering auf der dritten Ebene angesiedelt werden. Betrachtet werden die beiden Bezugsobjekte Anwendungssystem und Infrastruktur, die durch ein Sicherheitskonzept, das wiederum Maßnahmen und Sicherheitsarchitekturen beinhaltet, vor unautorisierten Zugriffen zu schützen sind. Die Sicherheitsanforderungen, die im Rahmen der Anwendungsentwicklung zu definieren sind, werden durch Sicherheitsgrundfunktionen als Sicherheitsziel auf dieser Ebene erfasst.

6.4. Fazit

Anhand des Referenzmodells können verschiedene Aspekte der betrieblichen Informationssicherheit verdeutlicht werden. Auf Schemaebene werden für den Unternehmenskontext relevante Ziele, deren entsprechende Bezugsobjekte sowie aus den Aufgabendurchführungen resultierende Sicherheitsartefakte dargestellt. Durch deren Systematisierung auf Basis einer gemeinsamen Metapher und eines einheitlichen Strukturrahmens entsteht ein allgemeingülti-

ges Modell, das als Referenz für die Betrachtung von betrieblicher Informationssicherheit in Unternehmen genutzt werden kann.

Neben der grundlegenden Metapher ist zudem die praktische Interpretation des Sicherheitsbegriffs ausschlaggebend für die Berücksichtigung von Modellelementen im Referenzmodell. Die vorliegende Arbeit baut auf einem risikoorientierten Grundverständnis auf[81], sodass Bedrohungen oder konkrete Angriffsverfahren nicht als Modellelemente berücksichtigt werden.

Vor dem Hintergrund der Entwicklungsaufgabe von betrieblichen Anwendungssystemen ist auf Grundlage dieser Erkenntnisse der aktuelle Stand in Forschung und Praxis zu analysieren. Es wird deutlich, dass insbesondere auf der Ebene der Geschäftsprozesse die Berücksichtigung von Informationssicherheit nur ungenügend erfolgt. Schutzziele werden im Rahmen der Anforderungsanalyse zwar genutzt, jedoch in der Regel vor allem auf Objekte der Ressourcenebene bezogen. Eine konsistente Modellierung der Schutzziele auf Aufgabenebene findet nicht statt. Diesen Aspekt verdeutlicht auch die bisher vorgenommene inhaltliche Beschreibung der Modellelemente: Auf Schemaebene wurden alle Sektoren des Referenzmodells, die im Fokus der Arbeit liegen, im Detail beschrieben. Eine Darstellung des geforderten Artefakts des **sicherheitsrelevanten Geschäftsprozessmodells** ist jedoch nicht erfolgt, da keine entsprechenden Ansätze vorliegen.

Die diesbezüglich notwendige Modellierung von Schutzzielen auf Aufgabenebene bildet aus geschäftsprozessorientierter Perspektive die Grundlage für die Identifikation und Auswahl sowie die Parametrisierung von Sicherheitsmechanismen, die dann im Rahmen des Entwicklungsprozesses betrieblicher Anwendungssysteme zum Einsatz kommen können. Der dritte Teil der Arbeit stellt eine Modellierungsmethodik vor, die diese Anforderungen aufgreift und im Ergebnis die Erstellung des Sicherheitsartefakts auf Ebene des Geschäftsprozesses in Form eines sicherheitserweiterten Geschäftsprozessmodells ermöglicht. Die Beschreibung der Sicherheitsartefakte des Referenzmodells wird auf diese Weise komplettiert.

[81] Vgl. hierzu Kapitel 3.1.4.

Teil III

Geschäftsprozessgetriebene Modellierung betrieblicher Informationssicherheit

Teil III der Arbeit beschreibt mit SOMsec eine Methodik zur geschäftsprozessgetriebenen Sicherheitsmodellierung, die konzeptuell auf dem Referenzmodell betrieblicher Informationssicherheit aufbaut. Im Ergebnis wird durch diese Methodik das Sicherheitsartefakt des sicherheitserweiterten Geschäftsprozessmodells geschaffen, sowie darauf aufbauende fachliche und technische Sicherheitsspezifikationen in Bezug auf die Entwicklung betrieblicher Anwendungssysteme.

Kapitel 7 führt in die Grundlagen der betrieblichen Sicherheitsmodellierung ein und stellt die konzeptuelle Ausrichtung von SOMsec vor. Kapitel 8 beschreibt darauf aufbauend die Ansätze der Modellierungsmethodik im Rahmen der Geschäftsprozessmodellierung. Kapitel 9 und Kapitel 10 führen die Beschreibung in Bezug auf die fachliche und software-technische Anwendungssystemspezifikation fort. Kapitel 11 beschließt die vorliegende Arbeit mit einer Darstellung des aktuellen Forschungsstandes sowie einer abschließenden Diskussion des vorgestellten Ansatzes.

7. Modellierung betrieblicher Informationssicherheit

Auf Grundlage des Referenzmodells betrieblicher Informationssicherheit kann das Artefakt des sicherheitserweiterten Geschäftsprozessmodells als zentrale Komponente der betrieblichen Sicherheitsmodellierung identifiziert werden. Es bildet das Bindeglied zwischen der Ebene des Unternehmensplans und der Ressourcenebene und damit den Ausgangspunkt für die Berücksichtigung von Schutzzielen und entsprechenden Bezugsobjekten im betrieblichen Kontext.

Im Anschluss an eine allgemeine Einführung in Kapitel 7.1 wird in Kapitel 7.2 eine grundlegende Methodik zur geschäftsprozessorientierten Sicherheitsmodellierung auf Basis der SOM-Ansatzes vorgestellt. In Kapitel 7.2.5 werden dann die Zielsetzungen der Methodik erörtert, Kapitel 7.2.4 beschreibt das Vorgehensmodell im Überblick. Abschließend wird in Kapitel 7.3 ein Anwendungsfall anhand des SOM-Ansatzes vorgestellt, der im weiteren Verlauf der Arbeit als durchgängiges Szenario für die Erläuterung der entwickelten Modellierungsmethodik fungiert.

7.1. Methodische Grundlagen

Der eingangs genannte Begriff der **betrieblichen Sicherheitsmodellierung** beschreibt die umfassende Modellierung von Sicherheitsaspekten in allen Bereichen eines betrieblichen Systems. Dies umfasst die Betrachtung verschiedenster Sicherheitsaspekte bzw. Sicherheitsartefakte, sowohl aus technischer wie auch aus personeller oder infrastrukturbezogener Perspektive. Er ist somit als Oberbegriff für alle sicherheitsrelevanten Modellierungsvorgänge in einem Unternehmen zu verstehen. Bezogen auf den Erstellungsprozess eines Sicherheitskonzepts zum Beispiel, sind Modellbildungen im Bereich der personellen Sicherheitsmaßnahmen, wie etwa die Erstellung eines Organigramms mit Berechtigungsstufen, Bestandteile dieser Disziplin.

7.1.1. Geschäftsprozessgetriebene Sicherheitsmodellierung

In der vorliegenden Arbeit wird der Bereich der betrieblichen Sicherheitsmodellierung eingegrenzt, indem zum einen eine Einschränkung auf das betriebliche Informationssystem erfolgt, zum anderen die Betrachtung dieses Systems aus geschäftsprozessorientierter Perspektive

durchgeführt wird. In Bezug auf das Referenzmodell der Informationssicherheit resultiert aus dieser Eingrenzung das Sicherheitsartefakt des sicherheitserweiterten Geschäftsprozessmodells, das im Rahmen der Disziplin der **geschäftsprozessgetriebenen Sicherheitsmodellierung** erstellt wird. Diese Disziplin ist als Teilgebiet der betrieblichen Sicherheitsmodellierung zu verstehen und bezieht sich auf die durchgehende und konsistente Berücksichtigung von Sicherheitsaspekten im Rahmen der Geschäftsprozessmodellierung und darauf aufbauender Aktivitäten. Der Entwurf einer Methodik zur Durchführung der geschäftsprozessgetriebenen Sicherheitsmodellierung vor dem Hintergrund der Anwendungsentwicklung ist das inhaltliche Kernthema dieses dritten Teils der vorliegenden Arbeit.

7.1.2. Konzeptuelle Einordnung anhand des Referenzmodells

Die in dieser Arbeit vorgestellte Modellierungsmethodik bezieht sich gemäß der Ausrichtung der geschäftsprozessgetriebenen Sicherheitsmodellierung primär auf die zweite und dritte Ebene des Referenzmodells.

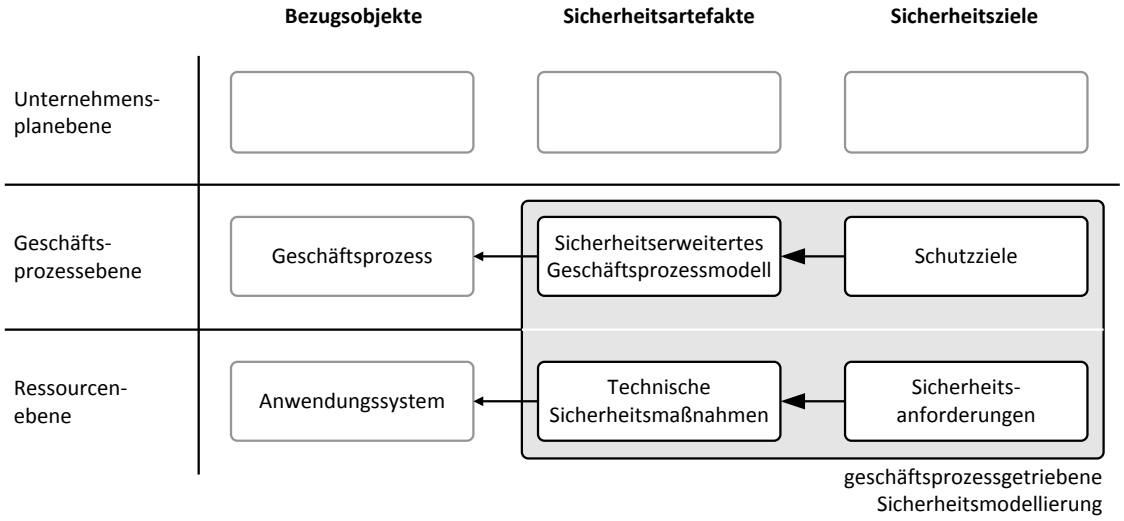

Abbildung 29: Konzept der geschäftsprozessgetriebenen Sicherheitsmodellierung anhand des Referenzmodells

Ein zentraler Aspekt der Modellierung von Sicherheitsaspekten besteht darin, welche Modellinformationen im Laufe der Modellierung generiert und in welcher Weise sie weiter genutzt werden. Im Kontext der Informationssicherheit sind diese relevanten Modellinformationen die Sicherheitsziele, die im Hinblick auf das jeweilige Bezugsobjekt durch den Modellierer zu spezifizieren sind. In Bezug auf die Ausrichtung der Modellierungsmethodik sind dies die **Schutzziele auf Geschäftsprozessebene** sowie, daraus abzuleiten, die entsprechenden

Sicherheitsanforderungen in Bezug auf ein die jeweiligen Prozesse unterstützendes Anwendungssystem. Im Ergebnis wird durch die Modellierung der Schutzziele im Rahmen der Methodik das Sicherheitsartefakt des **sicherheitserweiterten Geschäftsprozessmodells** generiert. Dieses dient dann als Grundlage für die Ableitung von **Sicherheitsanforderungen**, deren Modellierung die Vorgabe für die Umsetzung und Parametrisierung technischer Sicherheitsmaßnahmen in Bezug auf ein Anwendungssystem darstellt[82].

Gemäß des verwendeten Architekturrahmens sind die Schutzziele grundlegend in Abhängigkeit von den definierten Sicherheitsvorgaben der ersten Ebene zu betrachten. Aus inhaltlicher Sicht ist hierbei relevant, wie sich bestimmte Anforderungen, zum Beispiel aus gesetzlichen Vorgaben, in konkreter Form auf die Schutzzielspezifikation auf Geschäftsprozessebene auswirken. Die hierzu notwendige Analyse entsprechender Gesetze oder auch Normen liegt jedoch nicht im Fokus dieser Arbeit. Der Übergang zwischen erster und zweiter Ebenen und somit auch die Definition einer Transformationsbeziehung zwischen Sicherheitsvorgaben und Schutzzielen, wird somit im weiteren Verlauf nicht betrachtet.

Im Mittelpunkt der Modellierungsmethodik liegt vielmehr das sicherheitsrelevante Beziehungsgefüge zwischen zweiter und dritter Ebene des Referenzmodells. Im Rahmen der geschäftsprozessorientierten Softwareentwicklung gemäß der SOM-Methodik ist diese Beziehung zwischen Geschäftsprozessmodell und einem zugehörigen Anwendungssystem anhand des Konzepts der Automatisierung von Aufgaben und Transaktionen vollständig beschreibbar. Im Rahmen der Modellierung von Informationssicherheit ist dies zu erweitern um die Überführung der modellierten Sicherheitsziele auf Geschäftsprozessebene in die Anforderungsdefinition der entsprechend umzusetzenden technischen Sicherheitsmaßnahmen.

Sicherheitsziele sind demzufolge als Schutzziele auf Geschäftsprozessebene zu spezifizieren und in ein sicherheitserweitertes Geschäftsprozessmodell zu integrieren. Dieses Modell dient dann als Ausgangspunkt für die fachliche Spezifikation eines betrieblichen Anwendungssystems. Im Rahmen dieser Abbildung sind die spezifizierten Schutzziele in Sicherheitsanforderungen an das Anwendungssystem zu transformieren, die im Rahmen der fachlichen Spezifikation zu berücksichtigen sind. Sicherheitsgrundfunktionen, als Repräsentation dieser Anforderungen, können auf dieser Ebene dann als qualitative Anforderungen an das zu entwickeln-

[82] Die Erläuterungen zur geschäftsprozessgetriebenen Sicherheitsmodellierung nehmen im Rahmen dieser Arbeit direkten Bezug zu dem Sicherheitsartefakt der technischen Sicherheitsmaßnahme. Die Spezifikation eines Sicherheitskonzepts (vgl. Kapitel 5.3.4.1) für eine zu erstellendes Anwendungssystem wird nicht dediziert betrachtet.

de Anwendungssystems interpretiert werden[83]. Anhand der spezifizierten Sicherheitsgrundfunktionen ist schließlich zu ermitteln, welche konkreten Sicherheitsmechanismen im Rahmen der Entwicklung des Anwendungssystem Berücksichtigung finden müssen, um die zu Beginn spezifizierten Schutzziele auf Geschäftsprozessebene zu erreichen. Auf diese Weise besteht die Möglichkeit, die bereits beschriebene Lücke im Übergang zwischen Lenkungs- uns Leistungssystem durch die explizite Berücksichtigung von Sicherheitszielen auf Geschäftsprozessebene zu überbrücken.

Die aufgezeigten Zusammenhänge können anhand des Referenzmodells auf Schemaebene nachvollzogen werden. Die inhaltliche Grundlage für diese Ableitungsbeziehungen wird jedoch auch auf Ausprägungsebene der jeweiligen Sicherheitsziele und Sicherheitsartefakte gebildet. Im Rahmen der bisherigen Ausführungen wurden in Kapitel 5 die Bereiche Schutzziele sowie Sicherheitsgrundfunktionen hierzu bereits ausführlich erläutert. Von Relevanz für den beschriebenen Ansatz sind darüber hinaus jedoch auch die inhaltlichen Beziehungen zwischen Schutzzielen und Sicherheitsgrundfunktionen. In dem folgenden Kapitel werden diese Zusammenhänge erläutert, die dann im weiteren Verlauf der Arbeit als Grundlage für die Beschreibung der Transformationsbeziehungen zwischen den Betrachtungsebenen dienen.

7.1.3. Transformationsbeziehung der Sicherheitsziele

Sicherheitsgrundfunktionen stellen eine Kategorisierung für die technischen Aspekte der Sicherheitsanforderungen auf Ressourcenebene dar. Sie bilden somit ein Bindeglied zwischen den definierten Schutzzielen auf Geschäftsprozessebene und der Auswahl konkreter Sicherheitsmechanismen als entsprechend unterstützende Sicherheitsartefakte im Rahmen der Anwendungssystementwicklung.

7.1.3.1. Schutzziele und Sicherheitsgrundfunktionen

Die in Kapitel 5.4.4.2 definierten Grundfunktionen der Informationssicherheit entsprechen Sicherheitsanforderungen, die durch die Implementierung entsprechender Sicherheitsmechanismen realisiert werden [Ecke06, 193]. Eine solche Umsetzung von Sicherheitsgrundfunktionen unterstützt dabei unmittelbar die Zielerreichung entsprechender Schutzziele [Pohl04, 681]. Durch diesen Zusammenhang wird implizit auch die transitive Ableitung einer Zuordnung zwischen Schutzzielen und Sicherheitsmechanismen ermöglicht. Sicherheitsmechanis-

[83] Zu Sach- und Formalzielen der Systementwicklungsaufgabe vgl. [FeSi08, 475].

men implementieren demzufolge Sicherheitsgrundfunktionen und sind über diese entsprechenden Schutzzielen zuzuordnen. In dieser Betrachtungsweise finden Grundfunktionen als logisches Kriterium der Kategorisierung von Sicherheitsmechanismen Verwendung. Sie stellen jedoch kein eigenständiges Sicherheitsartefakt im Sinne der Arbeit dar, sondern sind vielmehr als Ausprägung der Sicherheitsanforderungen zu interpretieren.

Durch die Nutzung von Sicherheitsgrundfunktionen werden Sicherheitsmechanismen und Schutzziele auf Ausprägungsebene inhaltlich entkoppelt. Dies ist insbesondere dann von Vorteil, wenn strategische Sicherheitsanforderungen des Unternehmensplans bzw. der Geschäftsprozessebene auf operative Handlungsanweisungen transformiert werden. Sicherheitsmechanismen können so unabhängig evaluiert und in Abhängigkeit von bestehenden Anwendungssystemarchitekturen auch ausgetauscht werden, ohne potentiell relevante Anforderungen fälschlicherweise nicht zu berücksichtigen.

Sicherheitsgrundfunktionen stellen ein taktisches Mittel dar, das die semantische Lücke der Sicherheitsbetrachtung zwischen strategischen und operativen Ebenen der Unternehmensarchitektur reduziert und somit den Übergang erleichtert. Als Basis für diesen Effekt sind jedoch die Beziehungen zwischen Schutzzielen und Sicherheitsgrundfunktionen aus inhaltlicher Sicht grundlegend zu spezifizieren.

7.1.3.2. Beschreibungsrahmen der Beziehung

Die nachfolgende Abbildung verdeutlicht dieses Beziehungsgefüge anhand eines Beschreibungsrahmens, der den im Rahmen des Zielsystems der Informationssicherheit definierten Schutzzielen die entsprechenden Sicherheitsgrundfunktionen zuordnet. Als Repräsentation der Grundfunktionen kommen die in Kapitel 5.4.4.3 bereits vorgestellten Kategorien zum Einsatz. Die Differenzierung der Schutzziele folgt der ebenfalls bereits eingeführten Systematik der Schutzzielklassen in Kapitel 5.4.3.4.

Bezugsobjekt		Schutzzielklasse	Schutzziel	Sicherheitsgrundfunktionen						
				I&A	Z&A	B&A	U	W	Z	Ü
Aufgabenobjekt	Information	Vt	Vertraulichkeit	I&A	Z&A	B&A		W		Ü
		I	Integrität		Z&A	B&A	U			Ü
		Vf	Verfügbarkeit		Z&A				Z	
		Vb	Verbindlichkeit	I&A	Z&A	B&A				
Aufgabenträger	Person	Vt	Anonymität					W		
		Vb	Authentizität	I&A	Z&A	B&A				
	AWS	I	Programmintegrität		Z&A	B&A	U			
		Vf	Verfügbarkeit		Z&A				Z	
Vorgang	vollautomatisiert	Vt	Unbeobachtbarkeit					W		
		I	Vorgangsintegrität		Z&A	B&A	U			
		Vb	Nichtabstreitbarkeit	I&A	Z&A	B&A				
	teilautomatisiert	Vt	Unbeobachtbarkeit					W		
		Vb	Nichtabstreitbarkeit	I&A	Z&A	B&A				

Abbildung 30: Beziehung zwischen Sicherheitsgrundfunktionen und Schutzzielen

Eine Zuordnung zwischen Schutzziel und Grundfunktion bedeutet grundsätzlich, dass die Erreichung eines Schutzziels durch den Einsatz der notierten Grundfunktion entsprechender Mechanismen unterstützt wird. In Anlehnung an den zweckbezogenen Klassifizierungsansatz von Sicherheitsmaßnahmen, kann dieser Zusammenhang weiter differenziert werden. Unterschieden wird zum einen eine unmittelbare Beziehung zwischen Grundfunktion und Schutzzielklasse, die sich direkt und positiv auf die Zielerreichung auswirkt. Dieser Typus, in der Matrix durch ein grau hinterlegtes und benanntes Feld symbolisiert, kann als **präventiv** charakterisiert werden, da entsprechende Grundfunktionen ein Schutzziel ex ante unterstützen. Hiervon wird eine mittelbare Beziehung unterschieden, die nur indirekte Auswirkungen von Grundfunktionen auf Schutzzielklassen aufweist. Sie ist als **detektiv** zu beschreiben, die ausschließlich ex post zu der Zielerreichung beiträgt. Dargestellt wird dieser Typ durch ein nicht ausgefülltes benanntes Feld. Ein leeres Feld schließlich beschreibt, dass keine Beziehung zwischen Grundfunktion und Schutzziel besteht.

7.1.3.3. Ausgestaltung der Transformationsbeziehung

Die dargestellte Systematik bezieht sich auf das detaillierte Zielsystem der Informationssicherheit, dessen Relevanz in diesem Zusammenhang deutlich wird. Im Vergleich zu der in der Literatur oftmals genutzten, einfachen Zuordnung von Grundfunktionen zu den vier Schutz-

zielklassen, werden in dieser erweiterten Systematik inhaltliche Unterschiede in Abhängigkeit von den Bezugsobjekten ersichtlich. So ist die Grundfunktion **Identifizierung und Authentisierung** nicht vollständig der Erreichung der Schutzzielklasse Vertraulichkeit zuzuordnen, da zum Beispiel die Vertraulichkeit einer Person, somit deren Anonymität, durch diese Funktionen nicht gestärkt, sondern eher geschwächt wird. Identifikation und Authentisierung beziehen sich somit präventiv auf die Vertraulichkeit und Verbindlichkeit von Informationen, in Bezug auf Aufgabenträger und Vorgänge jedoch nur auf das Schutzziel der Verbindlichkeit. Dies geschieht vornehmlich durch die Verifizierung der Authentizität der entsprechenden Instanzen.

In ähnlicher Weise ist dieser Effekt bei der Grundfunktion **Zugriffskontrolle und Autorisierung** zu erkennen. Der Fokus liegt hierbei im Kern auf den Schutzzielen Integrität und Vertraulichkeit, wobei die Letztere in Bezug auf Aufgabenträger und Vorgänge nicht unterstützt wird. Die Grundfunktion Zugriffskontrolle und Authentisierung ist ebenfalls als präventiv zu kategorisieren, als indirekte Zielbezüge sind Auswirkungen auf die Schutzziele Verfügbarkeit und Verbindlichkeit zu verzeichnen.

Die Grundfunktion **Beweissicherung und Audit** bezieht sich primär auf das Schutzziel Verbindlichkeit. Zwar kann argumentiert werden, dass hierdurch prinzipiell auch Vertraulichkeit und Integrität sichergestellt wird, jedoch muss zusätzlich anhand des Einsatzzwecks unterschieden werden. Bezüglich der Verbindlichkeit dient die Beweissicherung als Mittel um das Schutzziel zu erreichen, d.h. durch den Einsatz entsprechender Mechanismen wird die Prüfung der Verbindlichkeit überhaupt erst ermöglicht. In Bezug auf Vertraulichkeit und Integrität hingegen, können nur deren Verletzung durch diese Grundfunktion verifiziert werden, ihre Nutzung dient daher nicht primär der Zielerreichung sondern vielmehr der Erkennung ob unberechtigte Manipulationen vorliegen. Beweissicherung und Audit werden daher nur in Bezug auf die Verbindlichkeit in der dargestellten Systematik verwendet. In diesem Fall kann die Grundfunktion als präventiv eingestuft werden, im Falle der Vertraulichkeit bzw. Integrität würde sie rein detektiv fungieren.

Die Grundfunktionen **Unverfälschtheit** und **Wiederaufbereitung** sind bezüglich ihrer Ausrichtung ähnlich strukturiert. Beide beziehen sich ausschließlich auf jeweils eine Schutzzielklasse, adressieren in diesem Bereich auch alle Bezugsobjekte und agieren als präventive Maßnahmen. Unverfälschtheit unterstützt dabei die Integrität von Informationen, Aufgabenträgern und Vorgängen, die Wiederaufbereitung entsprechend deren Vertraulichkeit.

Die **Zuverlässigkeit** eines Dienstes bezieht sich ausschließlich auf die Schutzzielklasse der Verfügbarkeit. Hierbei ist die grundlegende Sichtweise auf diese Schutzzielklasse ausschlaggebend für die Interpretation dieser Grundfunktion. Gemäß der in Kapital 5.4.4.1 getroffenen Aussagen, ist sie somit ausschließlich auf Verfügbarkeit von Anwendungssystemen und den verarbeiteten Informationen zu beziehen. Eine Betrachtung der spezifizierten Charakteristika, wie etwa Fehlererkennung oder -behebung im Sinne der Safety, erfolgt im weiteren Verlauf der Arbeit nicht.

Übertragungssicherung als Kombination der Grundfunktionen Authentisierung, Autorisierung und Unverfälschtheit bezieht sich ausschließlich auf die Übertragung von Informationen. In diesem Zusammenhang werden alle Schutzziele unterstützt, die bereits durch die ursprünglichen Grundfunktionen abgedeckt werden. Ihr Anwendungsbereich ist jedoch auf Grund der eingeschränkten Perspektive auf das Bezugsobjekt Information begrenzt.

Es gilt zu beachten, dass die identifizierten Abhängigkeits- und Wirkungsbeziehungen zwischen den Schutzzielen ebenfalls auf die entsprechenden Grundfunktionen anwendbar sind. Die Grundfunktion der Wiederaufbereitung, die die Vertraulichkeit einer Information schützt, kann sich zum Beispiel kontraproduktiv auf die Grundfunktion Beweissicherung und Audit auswirken, die die Verbindlichkeit der Information unterstützt. Ebenso die Grundfunktion der Unverfälschtheit, die primär auf das Schutzziel der Integrität abzielt, durch dessen Beziehung zu der Schutzzielklasse der Verbindlichkeit jedoch auch diesbezüglich Berührungspunkte aufweist. Aus Gründen der Übersichtlichkeit wurden diese Beziehungen nicht in die Abbildung eingearbeitet, die grundlegenden Zusammenhänge sind jedoch aus der Darstellung in Kapitel 5.4.3.5 abzuleiten.

Auf Grund der bereits dargestellten Abhängigkeiten bzw. Einschränkungen in der Anwendbarkeit von Grundfunktionen in Bezug auf einzelne Bezugsobjekte wird deutlich, dass die inhaltlich korrekte Zuordnung zwischen Schutzzielen und Grundfunktionen einen großen Einfluss auf die Auswahl von operativen Sicherheitsmechanismen hat. Es ist daher als wichtig anzusehen, die Zusammenhänge auf dieser Detailierungsstufe zu analysieren, um spätere Konflikte bei der Auswahl zu vermeiden.

7.1.4. Fazit

Auf Basis des Referenzmodells konnte die konzeptuelle Begründung für die Relevanz der geschäftsprozessgetriebenen Sicherheitsmodellierung dargestellt werden. Weiterhin können Transformationsbeziehungen zwischen Sicherheitszielen, die eine Voraussetzung der Methodik darstellen, auf dieser Grundlage inhaltlich dargestellt werden.

Ein Ziel der vorzustellenden Methodik selbst besteht nun darin, aus den sicherheitsrelevanten Modellinformationen auf Geschäftsprozessebene konkrete Sicherheitsmechanismen auf Aufgabenträgerebene abzuleiten. Zusätzlich muss neben der reinen Definition dieser Mechanismen auch deren Konfiguration in möglichst hohem Maße aus der Modellierung auf Aufgabenebene ableitbar sein. Die folgenden Kapitel geben hierzu eine Einführung in die entwickelte Modellierungsmethodik.

7.2. Eine Methodik zur geschäftsprozessgetriebenen Sicherheitsmodellierung

Die folgenden Abschnitte geben eine Einführung in die Grundlagen und Konzepte der in dieser Arbeit entwickelten **Methodik zur geschäftsprozessgetriebenen Sicherheitsmodellierung auf Basis des Semantischen Objektmodells (SOMsec)**. Hierzu wird zunächst eine kurze Einführung in den Modellierungsansatz der SOM-Methodik gegeben, bevor im Anschluss die konzeptuellen Grundlagen und Zielsetzungen von SOMsec vorgestellt werden.

7.2.1. Grundlagen der SOM-Methodik

SOMsec basiert im Kern auf den Konzepten und Methoden von SOM, erweitert jedoch die bestehenden Modellierungsansätze zur Geschäftsprozess- und fachlichen Anwendungsbeschreibung um die Berücksichtigung von Sicherheitsaspekten. Vor diesem Hintergrund sind die bisherigen Ausführungen zur SOM-Methodik[84] um die Beschreibung des Vorgehensmodells sowie des genutzten Modellierungsansatzes zu ergänzen. Die folgenden Kapitel stellen beide Aspekte im Überblick dar[85].

[84] Das Architekturmodell von SOM wurde in Kapitel 5.1.1 vorgestellt.

[85] Für einen umfassenden Einblick zu SOM sei auf die originären Quellen verwiesen, u.a. [FeSi93], [FeSi95a], [FeSi95b], [FeSi97] oder [FeSi08].

7.2.1.1. Vorgehensmodell von SOM

Um die hohe Komplexität betrieblicher Systeme abbilden zu können, strukturiert die SOM-Methodik die Teilmodelle betrieblicher Systeme anhand des bereits vorgestellten Konzepts der Unternehmensarchitektur. Zur Bewältigung der Komplexität innerhalb der Teilmodelle, werden zusätzlich Sichten als Projektionen auf das jeweilige Teilmodellsystem definiert. Diese Sichten werden korrespondierend zu den Ebenen des Architekturrahmens im Vorgehensmodell (V-Modell) des SOM-Ansatzes beschrieben [FeSi95b, 1]. Die folgende Abbildung zeigt eine integrierte Darstellung der beiden Komponenten (nach [FeSi08,193ff]).

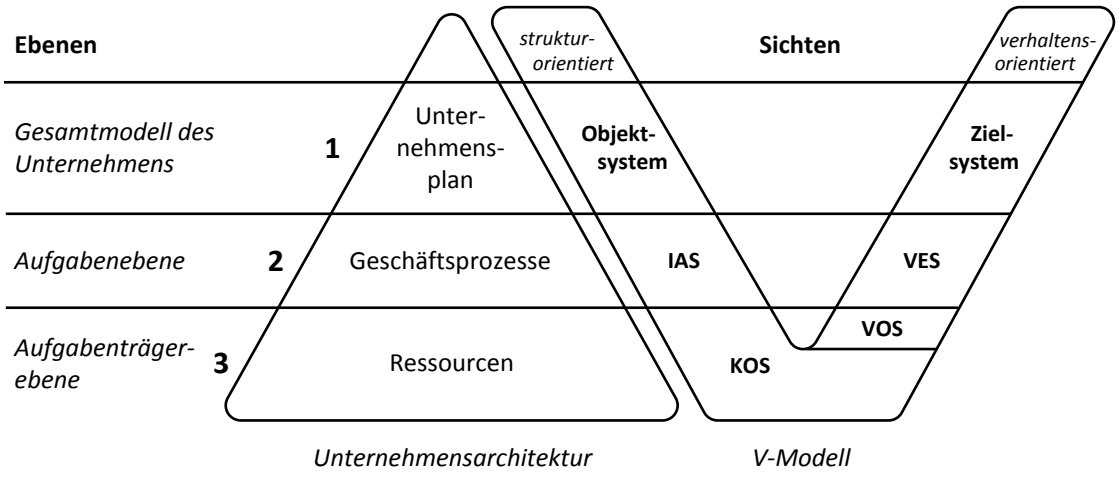

Abbildung 31: Unternehmensarchitektur und Vorgehensmodell der SOM-Methodik

Das Vorgehensmodell definiert die Art und Weise, wie die Modellbildung im Rahmen der SOM-Methodik erfolgt. Je Teilmodellsystemebene der Unternehmensarchitektur werden hierzu zwei Sichten gebildet, die anhand der Systemmerkmale Struktur und Verhalten abgrenzbar sind. Der methodische Ablauf der Modellierung erfolgt entlang der Ebenen von oben nach unten. Grundsätzlich sind im Modellierungsverlauf dabei die Modellierungsartefakte innerhalb der Sichten einer Ebene aufeinander abzustimmen. Die Abstände zwischen den Schenkeln des V-Modells symbolisieren die diesbezüglichen Freiheitsgrade, die nach unten hin abnehmen.

Ebene 1 - Unternehmensplan

Der Unternehmensplan beschreibt das Gesamtmodell eines Unternehmens auf einem hohen Abstraktionsgrad. Aus strukturorientierter Sicht beinhaltet der Unternehmensplan das sogenannte **Objektsystem**, das die Ressourcen eines betrieblichen Systems in Form von interagie-

renden betrieblichen Objekten sowie deren Leistungsbeziehungen aus globaler Perspektive beschreibt [FeSi95a, 211]. Aus verhaltensorientierter Sicht wird das diesbezügliche **Zielsystem** definiert, bestehend aus den Sach- und Formalzielen sowie den Strategien und Rahmenbedingungen [Schm01, 50f].

Das Objektsystem bildet den initialen Rahmen für die weitere Ableitung relevanter Ressourcen und Objekte, die für die betriebliche Leistungserstellung von Bedeutung sind und die auf den folgenden Ebenen weiter differenziert werden. Es wird abgegrenzt aus der dem Modellierungsprojekt zu Grunde liegenden betrieblichen Diskurswelt sowie dem zugehörigen relevanten Ausschnitt der betrieblichen Umwelt [FeSi93, 3]. Die Modellbildung von Objekt- und Zielsystem erfolgt in der Regel durch die Nutzung informaler Darstellungsformen, eine valide Überprüfung von Konsistenz und Vollständigkeit obliegt aus diesem Grund dem Modellierer selbst [FeSi95a, 213].

Ebene 2 – Geschäftsprozessmodell

Geschäftsprozesse bilden in SOM die Aufgabenebene eines Unternehmens. Sie werden auf der zweiten Ebene strukturorientiert in Form des **Interaktionsschemas** (IAS) und verhaltensorientiert in Form des **Vorgangs-Ereignis-Schemas** (VES) modelliert. Hierzu wird die informale Modellierung von Objekt- und Zielsystem der ersten Ebene in eine semi-formale Darstellung gemäß der SOM-Meta-Modelle der Geschäftsprozessmodellierung überführt [Mali97, 17]. Das IAS beschreibt die Struktur von Geschäftsprozessen durch betriebliche Objekte, die durch Transaktionen verknüpft sind. Im VES wird die Verhaltenssicht in Form von Aufgabendurchführungen und deren Ereignisbeziehungen spezifiziert. Beide Modelltypen können dabei durch Zerlegung sukzessive verfeinert werden [FeSi08, 195f].

Ebene 3 – Ressourcenmodell

Auf der dritten Ebene erfolgt die fachliche Spezifikation von Anwendungssystemen, die als maschinelle Aufgabenträger zur Umsetzung der modellierten Geschäftsprozesse fungieren. Sie beschreibt somit die Aufgabenträgerebene des Unternehmens aus dem Blickwinkel des betrieblichen Informationssystems. Die Modellbildung zur fachlichen Anwendungssystemspezifikation umfasst aus strukturorientierter Sicht ein **konzeptuelles Objektschema** (KOS), bestehend aus **konzeptuellen Objekttypen** (KOT) und deren Beziehungen untereinander. Konzeptuelle Objekttypen kapseln Struktur (Attribute) und Verhalten (Operatoren) und können zu anderen KOT in einer Interaktions-, Generalisierungs- oder Aggregationsbeziehung

stehen. Aus verhaltensorientierter Sicht wird ein **Vorgangsobjektschema** (VOS) spezifiziert, das anhand von **Vorgangsobjekttypen** (VOT) die Durchführung von Aufgaben durch das Zusammenwirken von konzeptuellen Objekttypen beschreibt. VOT stehen dazu untereinander in Interaktionsbeziehungen [Schm01, 52].

Den Ausgangspunkt für die fachliche Spezifikation eines Anwendungssystems bildet ein hinreichend detailliertes Geschäftsprozessmodell. Anwendungssysteme werden als Teilbereiche des IAS bzw. VES durch die Abgrenzung relevanter betrieblicher Objekte identifiziert und in Form von KOS und darauf aufbauendem VOS fachlich spezifiziert [FeSi08, 218].

7.2.1.2. Modellierungsansatz von SOM

Die SOM-Methodik berücksichtigt drei korrespondierende Sichten auf Geschäftsprozesse, die sowohl auf deren Struktur als auch auf deren Verhalten Bezug nehmen [FeSi95a, 214].

Aus **Leistungssicht** betrachtet erstellt ein Geschäftsprozess eine oder mehrere betriebliche Leistungen und übergibt diese an die ihn beauftragenden Geschäftsprozesse. Die **Lenkungssicht** beschreibt die Koordination der im Rahmen der Durchführung eines Geschäftsprozesses beteiligten betrieblichen Objekte. Als Koordinationsformen finden hierbei das Verhandlungs- sowie das Regelungsprinzip Verwendung. Aus **Ablaufsicht** betrachtet, stellt ein Geschäftsprozess schließlich einen ereignisgesteuerten Ablauf von Aufgaben dar, die den partizipierenden betrieblichen Objekten zugeordnet sind [FeSi08, 197f].

Lenkungs- und Leistungssicht stellen strukturorientierte Sichtweisen dar, die Ablaufsicht ein verhaltensorientierte Sichtweise. Entsprechend dieser Differenzierung werden in SOM die zwei bereits angesprochenen Teil-Modellsysteme des IAS und VES zur Abbildung von Geschäftsprozessen erstellt.

Metapher des SOM-Ansatzes

Der Modellierungsansatz für Geschäftsprozesse in der SOM-Methodik basiert auf der Metapher eines verteilten Systems, bestehend aus autonomen, lose gekoppelten betrieblichen Objekten, die anhand von Transaktionen in Bezug auf eine gemeinsame Zielerfüllung koordiniert werden.

Ein b**etriebliches Objekt** kapselt dabei einen Zustandsspeicher sowie zugehörige Operatoren [Schm01, 51]. Es umfasst eine Menge von Aufgaben, die eine gleichgelagerte Zielsetzung

verfolgen und die auf einem gemeinsamen Aufgabenobjekt, dem objektinternen Speicher, operieren. Aufgabendurchführungen selbst werden dabei durch Ereignisse ausgelöst bzw. synchronisiert. Der Austausch von Lenkungsnachrichten sowie Leistungspaketen zwischen betrieblichen Objekten erfolgt mittels **betrieblicher Transaktionen**. Lenkungsnachrichten dienen dabei zur Koordination der Erstellung und Übergabe von Leistungspaketen. Jeder erbrachten Leistung eines betrieblichen Objekts sind damit eine oder mehrere Transaktionen zugeordnet [FeSi08, 199ff].

Meta-Modell des SOM-Ansatzes

Das Begriffssystem des Modellierungsansatzes ist aus den Konzepten der Objekt- und Transaktionsorientierung der vorgestellten Modellierungsmetapher ableitbar. Die resultierenden Bausteine „betriebliches Objekt“, „Transaktion“, „Leistung“, „Aufgabe“ und „Ereignis“ bilden in SOM die Elemente für die Erstellung von Geschäftsprozessmodellen. Die folgende Abbildung zeigt das entsprechende Meta-Modell.

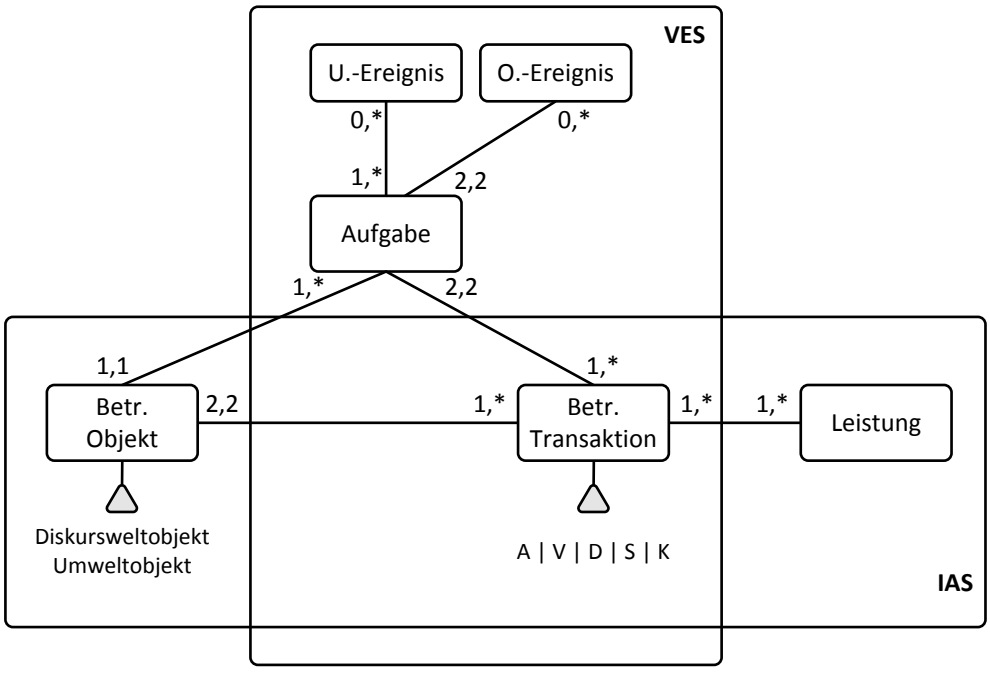

Abbildung 32: Meta-Modell von SOM (nach [FeSi08, 210])

Betriebliche Objekte werden in SOM entweder als Umwelt- oder Diskursweltobjekte modelliert. Sie sind mit einer bis beliebig vielen betrieblichen Transaktionen untereinander verbunden. **Transaktionen** verbinden dabei genau zwei betriebliche Objekte. Sie sind differenzierbar in Transaktionen zur **hierarchischen Koordination** nach dem Regelungsprinzip (Steuer-

und Kontrolltransaktionen) sowie zur **nicht-hierarchischen Koordination** nach dem Verhandlungsprinzip (Anbahnungs-, Vereinbarungs- und Durchführungstransaktion). Eine Transaktion wird dabei durch genau zwei **Aufgaben** realisiert, zwischen denen Lenkungs- bzw. Leistungspakete transferiert werden. Die entsprechenden Aufgabendurchführungen werden durch **Ereignisse** ausgelöst. Umweltereignisse dienen der Modellierung objektexterner Ereignisse, wohingegen objektinterne Ereignisse zum Beispiel Reihenfolgebeziehungen zwischen zwei Aufgaben eines betrieblichen Objekts herstellen [FeSi08, 210f].

Aufbauend auf den dargestellten Grundlagen der SOM-Methodik, werden in den folgenden Abschnitten die entsprechenden einführenden Konzepte zu SOMsec vorgestellt.

7.2.2. Konzeptuelle Grundlagen von SOMsec

SOMsec ist als Modellierungsmethodik konzipiert, durch die der Bereich der geschäftsprozessgetriebenen Sicherheitsmodellierung in betrieblichen Systemen vollständig abgedeckt werden kann. Die folgenden Abschnitte gehen auf die grundlegenden konzeptuellen Ansätze der Methodik ein.

7.2.2.1. Modellierungsumfang von SOMsec

Analog zur methodischen Grundlage des SOM-Ansatzes, ist die Ausrichtung von SOMsec vor dem Hintergrund der geschäftsprozessgetriebenen Anwendungssystementwicklung zu sehen. Die Modellierungsmethodik nutzt einen Top-Down-Ansatz und erstreckt sich dabei von Geschäftsprozessmodellen ausgehend, über den fachlichen Entwurf von Anwendungssystemen, bis hin zum software-technischen Entwurf des Systems.

In Anlehnung an die in Kapitel 6 dargestellten Zusammenhänge sowie die Bezüge zum Referenzmodell betrieblicher Informationssicherheit, kann der Modellierungsumfang von SOMsec in nachfolgender Weise dargestellt werden.

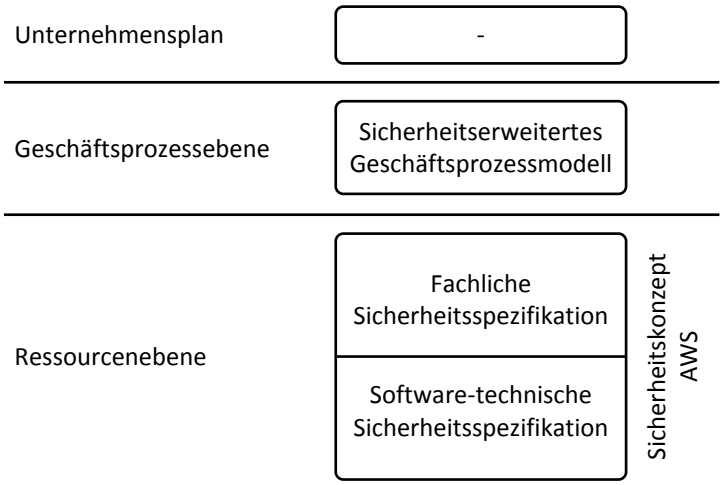

Abbildung 33: Konzeptueller Modellierungsumfang von SOMsec

Den Ausgangspunkt der Modellierung in SOMsec bildet die Erstellung eines **sicherheitserweiterten Geschäftsprozessmodells** unter Berücksichtigung relevanter Schutzziele. Diese werden auf Ressourcenebene in entsprechende Sicherheitsvorgaben **der fachlichen Sicherheitsspezifikation** überführt. Die fachliche Sicherheitsspezifikation dient dann als Ausgangspunkt für die Ableitung der **software-technischen Sicherheitsspezifikation**, die sich auf die Modellierung notwendiger Sicherheitsmechanismen im Rahmen der Softwarearchitektur des zu entwickelnden Anwendungssystems bezieht. Die Modelle der fachlichen und softwaretechnischen Sicherheitsspezifikation repräsentieren dabei das Sicherheitskonzept eines Anwendungssystems im Sinne des Referenzmodells betrieblicher Informationssicherheit.

Das Hauptaugenmerk von SOMsec liegt dabei auf der Spezifikation durchgängiger und konsistenter Ableitungsbeziehungen von Schutzzielen und Sicherheitsanforderungen beim Übergang zwischen den verschiedenen Ebenen der Modellierung. Die Spezifikation sicherheitsorientierter Beziehungen der Geschäftsprozessebene zur Ebene des Unternehmensplans sind dabei nicht expliziter Bestandteil von SOMsec. Gleichwohl können mit SOMsec erstellte Modelle durchaus als Grundlage für entsprechende Aktivitäten auf Ebene des Unternehmensplans herangezogen werden. Entsprechende Aufgaben und Lösungsverfahren, etwa im Bereich der Corporate Governance, sind jedoch nicht Gegenstand der vorliegenden Arbeit.

7.2.2.2. Abgrenzung zu SOM

Eine der fachlichen Grundlagen von SOMsec bildet der Ansatz der geschäftsprozessgetriebenen Anwendungssystementwicklung, der durch die SOM-Methodik unterstützt wird. SOMsec

stellt in diesem Zusammenhang eine domänenspezifische Erweiterung der SOM-Methodik dar, die speziell auf den Bereich der Modellbildung betrieblicher Informationssicherheit abzielt. Analog zu SOM basiert sie daher ebenfalls auf dem konzeptuellen Tripel aus Architekturrahmen, Vorgehensmodell und Modellierungsansatz. Um die angestrebten domänenspezifischen Modellierungsziele[86] der Methodik zu erreichen, sind jedoch Anpassungen an diesen Komponenten erforderlich.

Den methodischen Ausgangspunkt dieser Anpassungen stellt die Modifikation des Modellierungsansatzes dar, der durch die drei Merkmale **Modellierungsreichweite**, **Modellumfang** und **Modellierungszweck** charakterisiert werden kann. Anhand der Ausprägung dieser Merkmale, in Verbindung mit den teilweise abhängigen Komponenten des **Architekturrahmens** und des **Vorgehensmodells**, können die Unterschiede zwischen SOM und SOMsec aufgezeigt werden[87].

Modellumfang

Der Modellumfang der SOM-Methodik kann durch das zu Grunde liegende Untersuchungsproblem spezifiziert werden. Er ist charakterisiert durch das Untersuchungsobjekt der betrieblichen Lenkungs- und Leistungsflüsse in Form von Geschäftsprozessen und dem Untersuchungsziel der Realisierung entsprechend unterstützender Anwendungssysteme. In SOMsec wird das Untersuchungsobjekt beibehalten, jedoch ergeben sich Änderungen im Untersuchungsziel. Hier wird nicht nur die reine Implementierung der fachlichen Funktionalität beachtet, sondern ebenfalls die Berücksichtigung von Sicherheitsaspekten, die im Laufe der Top-Down-Modellierung identifiziert wurden. Dem erweiterten Modellumfang von SOMsec wird durch eine Anpassung der jeweiligen Meta-Modelle zur Modellerstellung Rechnung getragen.

Modellierungsreichweite

Die Modellierungsreichweite des Ansatzes ist entsprechend dem Modellumfang ebenfalls zu modifizieren. SOM führt von der Abgrenzung der zu modellierenden Diskurswelt sowie des zugehörigen Zielsystems über mehrere Modellierungs- und Spezifikationsschritte hinweg zu einem objektorientierten Fachkonzept des zu erstellenden Anwendungssystems [FeSi93, 3].

---

[86] Vgl. hierzu Kapitel 7.2.5.

[87] Die Modellierungsreichweite wird anhand des verwendeten Architekturrahmens ersichtlich, der Modellumfang anhand des Vorgehensmodells.

In SOMsec wird dies dahingehend erweitert, dass sicherheitsrelevante Aspekte im softwaretechnischen Konzept eines Anwendungssystems ebenso modelliert werden können, wie auch deren Transformation in Konfigurationsparameter für entsprechende technische Sicherheitsmaßnahmen.

Modellierungszweck

Bei beiden Ansätzen gleich bleibt der Modellierungszweck, der sich in der Zielsetzung von Gestaltungs- und Erklärungsmodellen widerspiegelt. Lediglich der Nutzungsrahmen der erstellten Modelle wird durch die Fokussierung auf die Domäne der Informationssicherheit in SOMsec modifiziert. Auf der Lenkungsebene können sicherheitserweiterte Geschäftsprozessmodelle auch im Rahmen des Sicherheits- bzw. Risikomanagements genutzt werden, im Rahmen des taktischen bzw. operativen Informationsmanagements ebenso bei der Softwareentwicklung bzw. dem Softwarebetrieb.

Architekturrahmen

Mit den Änderungen des Modellierungsansatzes einher geht die Notwendigkeit einer Anpassung des Architekturrahmens. Zum einen erfolgt eine Fokussierung auf die Entwicklung betrieblicher Anwendungssysteme, so dass andere Aufgabenträgertypen auf der dritten Ebene der Unternehmensarchitektur nicht betrachtet werden. Weiterhin ist eine zusätzliche Ebene in die Unternehmensarchitektur zu integrieren, um die angestrebte Modellierungsreichweite von SOMsec bis hin zur Implementierung von Anwendungssystemen umsetzen zu können. Dieser Aspekt wird in Kapitel 7.2.3 im Detail betrachtet.

Vorgehensmodell

Das Vorgehensmodell von SOM wird in SOMsec im Kern beibehalten. Teilmodellsysteme der einzelnen Ebenen werden erstellt und hierarchisch in Beziehung gesetzt. Der Übergang zwischen den Ebenen wird durch Beziehungs-Meta-Modelle bzw. Ableitungsfunktionen realisiert. Erweiterungen erfolgen zum einen im Hinblick auf die Anzahl der zu berücksichtigenden Ebenenübergänge und die damit verbundene Entwicklung der Ableitungsschritte und -beziehungen. Weiterhin werden domänenspezifische Zwischenschritte integriert, die neben der reinen fachlichen Funktionalität auf die konsistente Betrachtung der Sicherheitsaspekte abzielen. Das Vorgehensmodell von SOMsec wird in Kapitel 7.2.4 vorgestellt.

Modelltypen

Die Modelltypen auf Ebene der Geschäftsprozesse (IAS/VES) und der fachlichen Spezifikation (KOS/VOS) werden in SOMsec in ihrer bisherigen Ausgestaltung übernommen und in Bezug auf die Berücksichtigung von Sicherheitsaspekten erweitert. Zusätzlich werden im Hinblick auf den erweiterten Architekturrahmen neue Modellierungsansätze definiert und in Verbindung mit den bisherigen gebracht. Diese einzelnen Modellierungsansätze werden im weiteren Verlauf der Arbeit ebenenbezogen in den jeweiligen Kapiteln 8, 9 und 10 vorgestellt.

7.2.3. Architekturrahmen von SOMsec

Wie im vorangehenden Abschnitt ausgeführt, muss die SOM-Unternehmensarchitektur als Grundlage angepasst werden, um die angestrebte Modellierungsreichweite von SOMsec abbilden zu können. Die SOM-Unternehmensarchitektur weist hierbei eine Unterteilung des betrieblichen Systems in drei Ebenen auf. Die folgende Abbildung zeigt auf, wie diese im Kontext der vorliegenden Arbeit zu erweitern sind.

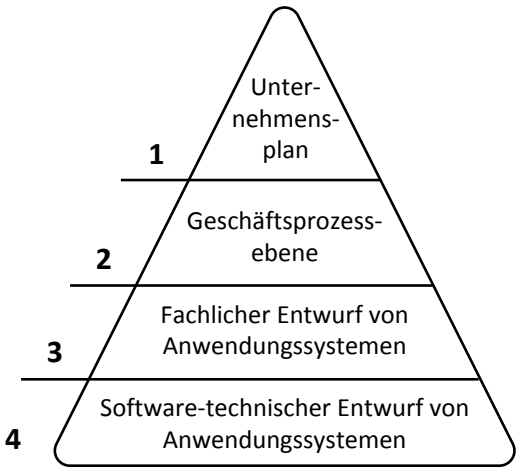

Abbildung 34: Erweiterte Unternehmensarchitektur (nach [Mali97, 6])

Der dargestellte erweiterte Architekturrahmen folgt einem Ansatz von MALISCHEWSKI [Mali97] und ergänzt die Unternehmensarchitektur um eine weitere Ebene des softwaretechnischen Entwurfs. Diese Ebene beinhaltet in SOMsec die technischen Sicherheitsspezifikationen, die in Bezug auf die Implementierung eines Anwendungssystems relevant sind. Die Ebenen eins bis drei des Architekturrahmens entsprechen inhaltlich den Beschreibungen aus

Kapitel 5.1.1, die Bezeichnung der dritten Ebene als „Fachlicher Entwurf von Anwendungssystemen“ wurde auf den Kontext der Systementwicklung angepasst.

Software-technischer Entwurf von Anwendungssystemen

Der fachliche Entwurf des Anwendungssystems wird auf dieser Ebene im Hinblick auf die Implementierung unter Beachtung eines Software-Architekturmodells weiter detailliert [Mali97, 7]. Zu diesem Zweck kommt das objektorientierte Software-Architekturmodell (ooAM) zum Einsatz, das ein Anwendungssystem komponentenorientiert in fachliche, technische sowie Basisfunktionalität unterteilt und diese Komponenten im Modell abbildet [Ambe93].

Implementierungsrelevante Aspekte entstehen in SOMsec auf dieser Ebene dadurch, dass durch die technische Sicherheitsspezifikation Modellinformationen generiert werden können, die für die sicherheitsrelevanten Basismaschinen der technischen Funktionalität des ooAM als Konfigurationsparameter dienen können. Diese Informationen werden in SOMsec jedoch konzeptuell der technischen Funktionalität zugeordnet und nicht gesondert im Rahmen einer eigenen Modellierungsebene betrachtet.

Die erweiterte Unternehmensarchitektur dient als Grundlage für die Umsetzung des Vorgehensmodells von SOMsec sowie die Eingliederung der Modellierungsansätze bzw. Ableitungsbeziehungen. Das entsprechende Vorgehensmodell von SOMsec wird im folgenden Abschnitt vorgestellt.

7.2.4. Vorgehensmodell von SOMsec

Das Vorgehensmodell von SOMsec basiert im Kern auf dem bereits vorgestellten Vorgehensmodell der SOM-Methodik. Es wird jedoch abgestimmt auf den im Vergleich erweiterten Modellierungsansatz bzw. Architekturrahmen, wodurch weitere Modellierungsschritte und Ableitungsbeziehungen entstehen.

Um die inhaltliche Anpassung der Methodik an den Sicherheitskontext besser darstellen zu können, wurden neben dem Architekturbezug des Vorgehensmodells in Kapitel 7.2.2.2 auch die Modelltypen der einzelnen Ebenen sowie die jeweiligen sicherheitsspezifischen Modellierungserweiterungen angesprochen. Letztere sind initial abzuleiten aus der Betrachtungsweise der Informationssicherheit als betriebliche Aufgabe, bei der sie das Zielsystem der Informationssicherheit darstellen. Dieses Zielsystem wird im Rahmen von SOMsec als Grundlage herangezogen, um die Modellbildung auf Geschäftsprozessebene durch **Schutzziele** sicherheits-

spezifisch zu erweitern sowie um die so generierten Modellinformationen in fachliche und technische Sicherheitsanforderungen auf die weiteren Ebenen zu transformieren. Die so entstehenden Sicherheitsanforderungen auf dritter und vierter Ebene des Architekturrahmens werden in SOMsec durch **fachliche und technische Sicherheitsobjekttypen** modelliert. Die folgende Abbildung stellt das Vorgehensmodell von SOMsec im Detail vor.

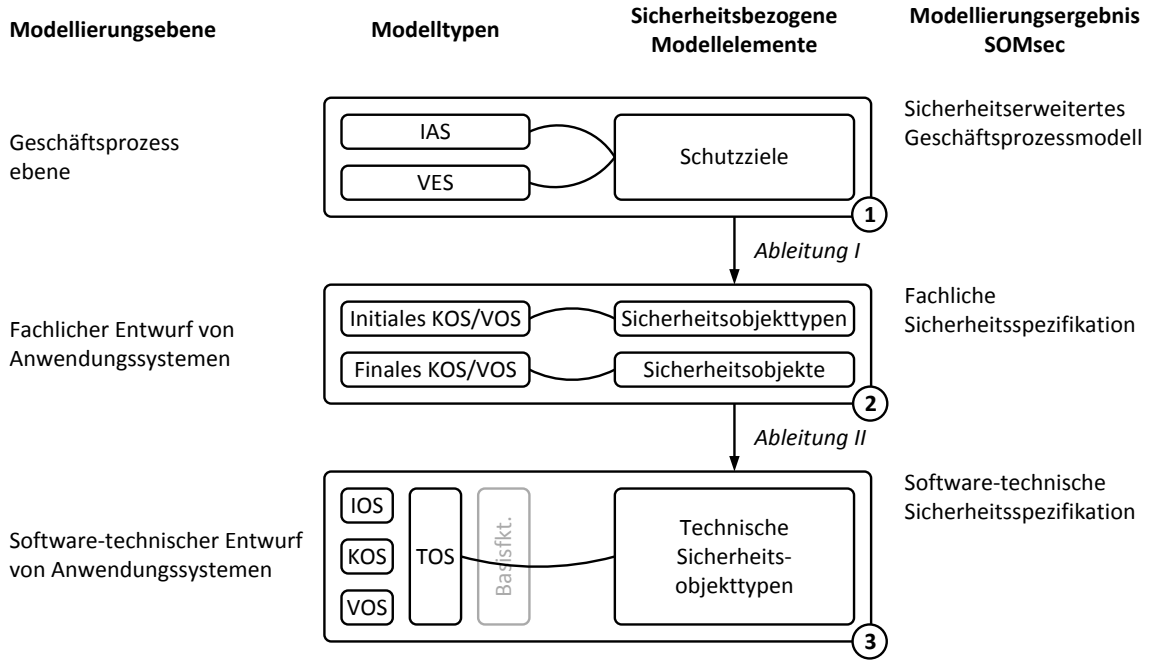

Abbildung 35: Globales Vorgehensmodell von SOMsec

Die Modellbildung in SOMsec folgt einem Top-Down-Ansatz von der Geschäftsprozessebene ausgehend über den fachlichen Entwurf von Anwendungssystemen bis hin zum softwaretechnischen Entwurf. Die erste Ebene des Unternehmensplans wird bei diesem Vorgehen nicht berücksichtigt. Das entsprechende Vorgehensmodell gliedert sich in drei Stufen.

- In der ersten Stufe erfolgt auf Geschäftsprozessebene die initiale Berücksichtigung von Sicherheitsaspekten in Form von **Schutzzielen**. Diese werden im Rahmen der Erstellung von IAS und VES in den Modellen annotiert und anhand entsprechender Modellierungstechniken sukzessive über die jeweiligen Zerlegungsschritte von IAS und VES hinweg verfeinert. Im Ergebnis entsteht ein sicherheitserweitertes Geschäftsprozessmodell, das Sicherheitsaspekte in Bezug auf prozessorientierte Informationsflüsse durch Schutzziele abbildet.

- Die zweite Stufe beinhaltet die Integration der Sicherheitsaspekte in den fachlichen Entwurf von Anwendungssystemen. Erreicht wird dies durch die Modellierung von sogenannten **Sicherheitsobjekttypen** in den fachlichen Modellschemata, die über das Konzept der Sicherheitsgrundfunktionen aus der Schutzzielmodellierung der ersten Stufe abgeleitet werden können (Ableitung I). Im Zuge der Überarbeitung der Modellschemata werden die abstrakten Sicherheitsobjekttypen instanziiert und in Form konkreter Sicherheitsobjekte modelliert[88]. Sicherheitsobjekte beziehen sich dann auf bestimmte Teilgraphen der Modelle und symbolisieren dadurch die fachlichen Sicherheitsanforderungen, die in diesen Bereich zu berücksichtigen sind. Die Summe der fachlichen Sicherheitsobjekte bildet ein **Sicherheitsobjektschema**, das die fachliche Sicherheitsspezifikation eines Anwendungssystems repräsentiert.
- In der dritten Stufe von SOMsec werden aus der fachlichen Sicherheitsspezifikation **technische Sicherheitsobjekttypen** abgeleitet. Die inhaltliche Grundlage hierfür bildet die Beziehung zwischen Sicherheitsgrundfunktionen und technischen Sicherheitsmaßnahmen (Ableitung II). Technische Sicherheitsobjekttypen stellen die Sicherheitsanforderungen aus technischer Perspektive im Rahmen der Architekturbetrachtung dar und bilden die technische Sicherheitsspezifikation eines Anwendungssystems.

Das Vorgehensmodell von SOMsec beschreibt die Erstellung von drei sicherheitserweiterten Modellformen, deren konzeptuelle Ausrichtung mit den Inhalten des Referenzmodells betrieblicher Informationssicherheit korrespondiert. Auf jeder Modellierungsstufe werden die Modellinformationen dabei schrittweise um Sicherheitsspezifika erweitert, die auf den jeweiligen Betrachtungsebenen inhaltlich zu berücksichtigen sind und durch einen Modellierer auf Grund seiner Expertise auch entsprechend angewandt werden können[89]. Charakteristisch ist hierbei die durch SOM bedingte Trennung zwischen struktur- und verhaltensorientierter Modellierung, die sich im Hinblick auf die Modellierung von Sicherheitsaspekten als sehr vorteilhaft erweist. In einem ersten Schritt können durch den Modellierer strukturelle Aspekte in Form von Transaktionen aus Sicherheitsgesichtspunkten in sehr abstrakter Form analysiert werden. Im Anschluss können die erzeugten Sicherheitsannotationen aus verhaltensorientierter Sichtweise aufgabenbezogen ergänzt und präzisiert werden.

---

[88] Der Schritt der Instanziierung von Sicherheitsobjekttypen wird im weiteren auch als „Präzisierung“ bezeichnet. Diese Benennung trägt dem Umstand Rechnung, dass mit der Instanziierung eine Verfeinerung der Referenzen der Sicherheitsobjekte auf fachliche Modellelemente einhergeht. Weitere Ausführungen hierzu sind in den Kapiteln 9.3.2 und 9.4.2.2 zu finden.

[89] Vgl. hierzu die Zielsetzungen von SOMsec in Kapitel 7.2.5.

Die Verknüpfungen zwischen den Modellierungsergebnissen von SOMsec sind durch die dargestellten Ableitungsbeziehungen charakterisierbar, die eine zunehmende Operationalisierung der Sicherheitsaspekte im Rahmen der Modellbildung erkennen lassen. Fachliche Sicherheitsanforderungen lassen sich inhaltlich aus den Schutzzieldefinitionen ableiten und zielen semantisch auf deren Umsetzung ab. Sie spiegeln somit den Realisierungscharakter wider, der durch eine Transformation von Zielen beim Übergang zwischen der Aufgaben- und Aufgabenträgerebene entsteht. Technische Sicherheitsanforderungen stellen schließlich die den Schutzzielen entsprechenden abstrakten Mittel dar, die zur Erschaffung eines Sicherheitsartefaktes auf Ressourcenebene notwendig sind.

7.2.5. Zielsetzungen von SOMsec

Ausgehend von den grundlegenden Nutzen der Geschäftsprozessmodellierung, die sich in Bezug auf die Anwendungssystementwicklung ergeben, lassen sich im Hinblick auf den Bereich der geschäftsprozessgetriebenen Sicherheitsmodellierung mit SOMsec weitere Zielsetzungen und damit verbundene Vorteile für den vorzustellenden Ansatz identifizieren.

Ausgangspunkt der Diskussion bildet die **Berücksichtigung von Sicherheitsaspekten im Rahmen des Softwareentwicklungsprozesses**, die lange Zeit als sehr gering zu bezeichnen war. Im besten Fall wurden sie in der Entwicklungsphase[90] in den Prozess integriert, oftmals ausschließlich in Abhängigkeit von den fachlichen Fähigkeiten auf Seiten der Entwickler [DeSt00, 228]. Mit der Zunahme der Relevanz betrieblicher Anwendungssysteme für den unternehmerischen Erfolg und der damit verbundenen Steigerung des Schadensrisikos, entstanden Ansätze, die eine explizite Beachtung der Sicherheitsaspekte als eigenständige Aufgabe in den Softwareentwicklungsprozess integrierten. In vielen Fällen wurden hierzu Erweiterungen bestehender Softwareentwicklungsmodelle vorgenommen, etwa die Einordnung von IT-Sicherheitsaspekten als nicht-funktionale Anforderungen in den OEP (oose Engineering Process, vgl. [Oest07]) oder deren Betrachtung als allgemeine Systemsicherheit im V-Modell XT (vgl. [RaBr06]). Es entstanden jedoch auch dedizierte Vorgehensmodelle, wie etwa der Comprehensive Lightweight Application Security Process (CLASP, vgl. [OWAS07]), die Sicherheit als zentrales Element in den Softwareentwicklungsprozess integrieren. Zusammen-

[90] Als vereinfachter Rahmen zur Einordnung der angesprochenen Entwicklungsphasen dient als allgemeingültiger Ansatz das Wasserfallmodell, vgl. hierzu u.a. [Royc87].

fassend können diese Ansätze unter dem Bereich des bereits angesprochenen **Security Engineering** subsumiert werden[91].

Getrieben durch diese Entwicklung, wurde der früheste Betrachtungszeitpunkt von Sicherheitsaspekten im Softwareentwicklungsprozess jedoch nur marginal von der Entwicklungsphase in die Entwurfsphase verschoben. Bestehen bleibt dabei die semantische Lücke zwischen dem Ursprung und der Definition von Sicherheitsanforderungen aus geschäftlicher Perspektive auf der einen Seite und deren Berücksichtigung und Implementierung aus technologischer Sicht auf der anderen Seite. In der Literatur wird diese Situation auch als **Security Gap** bezeichnet [ViMc08, 40f].

Frühe Integration von Sicherheitsaspekten in den Entwicklungszyklus

Ein Weg, um diese Lücke zu schließen, besteht in einer möglichst frühen Integration von Sicherheitsaspekten in den Softwareentwicklungsprozess und somit in die Analysephase. Im Kontext der geschäftsprozessmodellgetriebenen Anwendungssystementwicklung wird in dieser Phase die Aufgabenebene des umzusetzenden Systems in Form von Geschäftsprozessmodellen spezifiziert. Ziel muss es somit sein, Sicherheitsaspekte bereits bei der Modellierung von Geschäftsprozessen zu berücksichtigen und Möglichkeiten zu schaffen, die erfassten Aspekte strukturiert in den entsprechenden Modellen zu hinterlegen. Entwickler können sich auf diese Weise auf die eigentliche Kernaufgabe, der Umsetzung der fachlichen Anforderungen, konzentrieren, da die Sicherheitsanforderungen in vorgelagerten Phasen von Experten vollständig erfasst und spezifiziert werden können.

Diese grundlegende Zielsetzung des vorliegenden Ansatzes korrespondiert mit den Erkenntnissen, die bei der Entwicklung des Referenzmodells betrieblicher Informationssicherheit gewonnen wurden. Aus Sicherheitsgesichtspunkten konnte auf der Ebene der Geschäftsprozesse kein Sicherheitsartefakt ermittelt werden, das Sicherheitsaspekte als Bindeglied zwischen Lenkungssystem und Leistungssystem transportiert bzw. transformiert. Ein Ansatz zur Modellierung von Sicherheitsaspekten auf Geschäftsprozessebene adressiert ebendiesen Übergang und dient im Kontext der geschäftsprozessgetriebenen Anwendungsentwicklung weiterhin als Ausgangspunkt für eine durchgängige Betrachtung von Informationssicherheit.

---

[91] Vgl. hierzu Kapitel 6.3.3.

Plattformunabhängige Modellierung von Sicherheitsaspekten

Die Modellierung von Schutzzielen auf Geschäftsprozessebene muss unabhängig von einzusetzenden Technologien im Bereich der Anwendungssysteme erfolgen. Durch die Trennung von Aufgaben- und Aufgabenträgerebene in der SOM-Methodik wird diese Anforderung bereits initial unterstützt. Weiterhin müssen die erstellten Modelle als Basis für zu definierende Ableitungsbeziehungen verwendbar sein, um die Modellinformationen auf die technischen Ebenen transformieren zu können. Durch den Einsatz dieser Ableitungsbeziehungen wird die fachliche Modellierung der Sicherheitsaspekte von der technischen Umsetzung entkoppelt, sodass neben der Softwareentwicklung weitere Nutzungsmöglichkeiten der generierten Modelle entstehen, wie zum Beispiel im Rahmen von Sicherheits- oder Risikomanagementprozessen.

Flexibilität und Erweiterbarkeit

Durch die Ableitungsbeziehungen zwischen den verschiedenen Ebenen ergeben sich Automatisierungspotentiale hinsichtlich der Transformation der Modellinformationen. Änderungen der Sicherheitsanforderungen während des Entwicklungsprozesses erfolgen dann auf Modellebene und werden anhand der definierten Beziehungen auf entsprechende Modellierungsartefakte der technischen Ebenen der Softwarespezifikation und -implementierung automatisiert übertragen[92]. Bedingt durch eine solche Konzeption entsteht weiterhin die Möglichkeit der einfachen Erweiterbarkeit des Ansatzes. Durch die Abänderung bzw. Erweiterung der Ausgestaltung der Ableitungen, können neue Beziehungen zwischen Modellebenen flexibel und bedarfsgetrieben integriert werden. In der praktischen Umsetzung bezieht sich dies zum Beispiel auf die Integration neuer Elemente zur Modellierung von Sicherheitsanforderungen und die entsprechende Abänderung diesbezüglicher Beziehungsstrukturen zwischen den Modellebenen.

Domänenspezifisches Modellierungsverständnis

Wie in Teil I der Arbeit methodisch aufgezeigt wurde, ist das Verständnis des Sicherheitsbegriffs unter anderem abhängig von der Wahl des Bezugsobjektes. Folglich ändert sich das Modellierungsverständnis von Sicherheitsaspekten dann, wenn eine Änderung des Untersu-

[92] Dieser Aspekt folgt inhaltlich weitgehend dem Konzept der modellgetriebenen Softwareentwicklung (engl. *model driven software development*, MDSD), vgl. hierzu u.a. [StBe07]. Eine explizite Einordnung von SOM-sec in dieses Konzept wird im Rahmen der vorliegenden Arbeit jedoch nicht vorgenommen.

chungsobjektes der Modellbildung erfolgt. Im Kontext von SOMsec ist dies immer dann der Fall, wenn Modelltransformationen durch Ableitungsbeziehungen zwischen den Modellebenen zwei bis vier des Architekturrahmens erfolgen.

Im Ergebnis bedeutet dies, dass die Rolle des Modellierers in SOMsec domänenabhängig auszugestalten ist. Die einzelnen Domänen orientieren sich in SOMsec dabei an den Ebenen des Architekturrahmens und umfassen somit geschäftsprozessorientierte sowie fachliche und software-technische Perspektiven. Experten können auf diese Weise in ihrer Domäne mit gewohnten Metaphern und Werkzeugen Sicherheitsaspekte in ihre Modellierungstätigkeit einfließen lassen. Beispielsweise modelliert die Rolle des Business Analyst auf Ebene der Geschäftsprozesse Sicherheitsaspekte in Form von Schutzzielen, wohingegen ein Security Engineer im Rahmen der Systementwicklung Sicherheitsgrundfunktionen bzw. Sicherheitsmaßnahmen definiert.

Vor dem Hintergrund der aufgezeigten, konzeptuellen Grundlagen von SOMsec, wird in der Folge jede Stufe des Vorgehensmodells in einem eigenen Kapitel erläutert. Kapitel 8 befasst sich mit der Schutzzielmodellierung auf Geschäftsprozessebene, Kapitel 9 und 10 mit der fachlichen bzw. software-technischen Sicherheitsspezifikation. Als Grundlage für die exemplarische Erläuterung der Methodik in diesen Kapiteln wird im folgenden Abschnitt ein Anwendungsfall vorgestellt, der im Weiteren als durchgängiges Modellierungsbeispiel fungiert.

7.3. Vorstellung Anwendungsfall „Medizinisches Versorgungszentrum“

Die Domäne des genutzten Szenarios bezieht sich auf den Gesundheitssektor, speziell auf die Prozesse der Behandlung von Patienten in medizinischen Versorgungszentren (MVZ)[93]. Diese Geschäftsprozesse eines MVZ bildeten das Untersuchungsobjekt einer Fallstudie, die in 2009 im Rahmen des bayerischen Forschungsverbundes forFLEX[94] an der Universität Bamberg durchgeführt wurde. Die Zielsetzung von forFLEX besteht in der Untersuchung von Potenzia-

[93] MVZ sind in 2004 eingeführte medizinische Einrichtungen, die eine fachübergreifende ambulante Behandlung von Patienten durchführen. Sie werden ärztlich geleitet und umfassen mindestens zwei Fachärzte unterschiedlicher Fachrichtungen, die als Angestellte bzw. Vertragsärzte tätig sind. Gegen Ende 2009 waren ca. 1.400 MVZ in Deutschland zugelassen [KBV10, 3].

[94] Vgl. www.forflex.de.

len dienstorientierter IT-Systeme, die als Schlüsseltechnologie für die Flexibilisierung von Geschäftsprozessen fungieren können. Die nachfolgenden Geschäftsprozessmodelle basieren auf den diesbezüglichen Untersuchungen von MVZ, die in [Püt+09] und [Püt+10] publiziert wurden.

Das gesamte Szenario beschreibt die Abläufe von der Aufnahme eines Patienten bis hin zu dessen Behandlung in den Leistungsbereichen eines MVZ, das auf die fachärztlichen Disziplinen der Orthopädie und Chirurgie spezialisiert ist. Für die Darstellung der Modellierungsmethodik von SOMsec im Rahmen der vorliegenden Arbeit ist die vollständige Verwendung der durchgeführten Geschäftsprozessanalyse jedoch als zu umfangreich einzustufen, so dass nur ein angepasster Teilbereich der Fallstudie als Beispiel betrachtet wird. Das Ziel der Modellbildung ist die Erstellung eines Geschäftsprozessmodells anhand von SOM, das als Ausgangspunkt für die Ableitung einer fachlichen Spezifikation eines betrieblichen Anwendungssystems dient. Das vorgestellte Szenario wird in den folgenden Kapiteln dann als Basis für die Erstellung eines sicherheitserweiterten Geschäftsprozessmodells sowie den fachlichen und technischen Sicherheitsspezifikationen anhand von SOMsec herangezogen.

7.3.1. Struktursicht

Die zu modellierenden Prozesse beziehen sich auf die Erstbehandlung eines Patienten im MVZ durch den Fachbereich der Orthopädie. Nach der initialen Terminvereinbarung erfolgt die Erstellung einer Kurzanamnese, die im Rahmen der ärztlichen Leistung durch eine vollständige Anamnese komplettiert wird. Darauf aufbauend erfolgt die medizinische Diagnose sowie die resultierende Behandlung des Patienten. Abschließend wird die erbrachte Leistung des Arztes gegenüber der Kassenärztlichen Vereinigung (KV) abgerechnet und durch diese vergütet. Das entsprechende IAS wird über drei Zerlegungsstufen hinweg entwickelt[95].

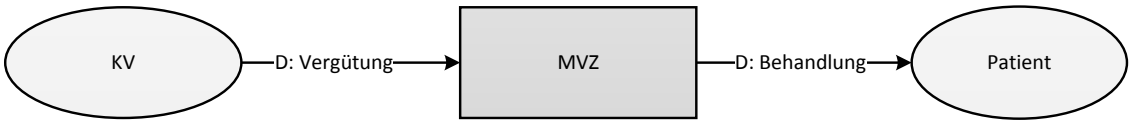

Abbildung 36: Szenario MVZ - IAS (erste Zerlegungsstufe)

[95] Für die Beschreibung der Zerlegungsregeln von SOM sei auf [FeSi08, 201ff] verwiesen. Ein Überblick über alle durchgeführten Objekt- und Transaktionszerlegungen ist in Anhang A bzw. Anhang B zu finden.

In der ersten Zerlegungsstufe gibt das `MVZ` als Diskursweltobjekt eine Behandlungsleistung an das Umweltobjekt `Patient` ab und erhält eine entsprechende Vergütungsleistung durch das Umweltobjekt `KV`. In der zweiten Zerlegungsstufe wird das `MVZ` durch Schritte der Objekt- und Transaktionszerlegung weiter detailliert.

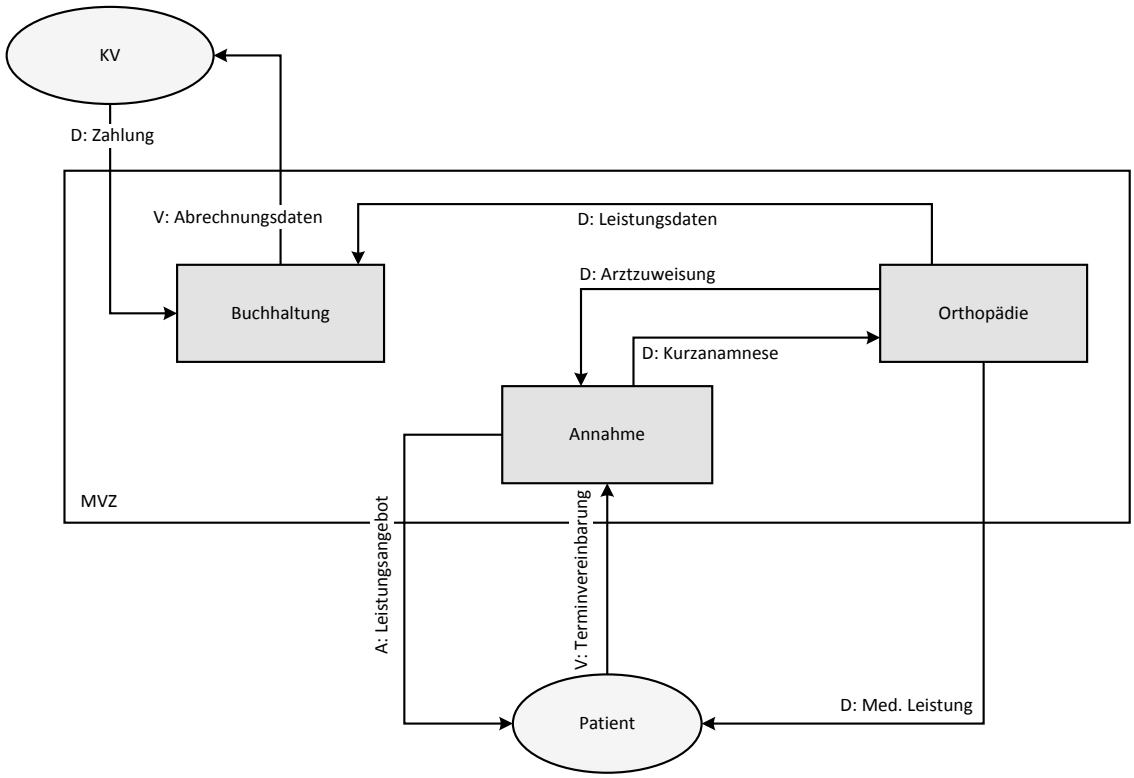

Abbildung 37: Szenario MVZ - IAS (zweite Zerlegungsstufe)

Das `MVZ` wird in die Objekte `Buchhaltung`, `Annahme` und `Orthopädie` zerlegt. Der Leistungsfluss `Behandlung` wird gemäß dem Verhandlungsprinzip als nicht-hierarchisch koordiniert modelliert. Auf die Anbahnungstransaktion `Leistungsangebot` zwischen Annahme und Patient folgt die `Terminvereinbarung` als Vereinbarungstransaktion sowie die abschließende Durchführungstransaktion `Med. Leistung` zwischen `Orthopädie` und `Patient`. Zwischen den MVZ-internen Diskursweltobjekten entstehen weitere Durchführungstransaktionen, die sich auf die Terminvereinbarung sowie die Leistungsdaten und deren Abrechnung beziehen.

In einem dritten Schritt wird das Interaktionsschema weiter verfeinert. Parallel dazu erfolgt im Hinblick auf die spätere Ableitung der fachlichen Spezifikation eines unterstützenden Anwendungssystems eine zusätzliche Kartierung der Transaktionen und Aufgaben. Dieser Schritt würde gemäß Vorgehensmodell von SOM erst zu einem späteren Zeitpunkt erfolgen,

wird jedoch aus Umfangsgründen vorgezogen und in die dritte Zerlegungsstufe des IAS integriert.

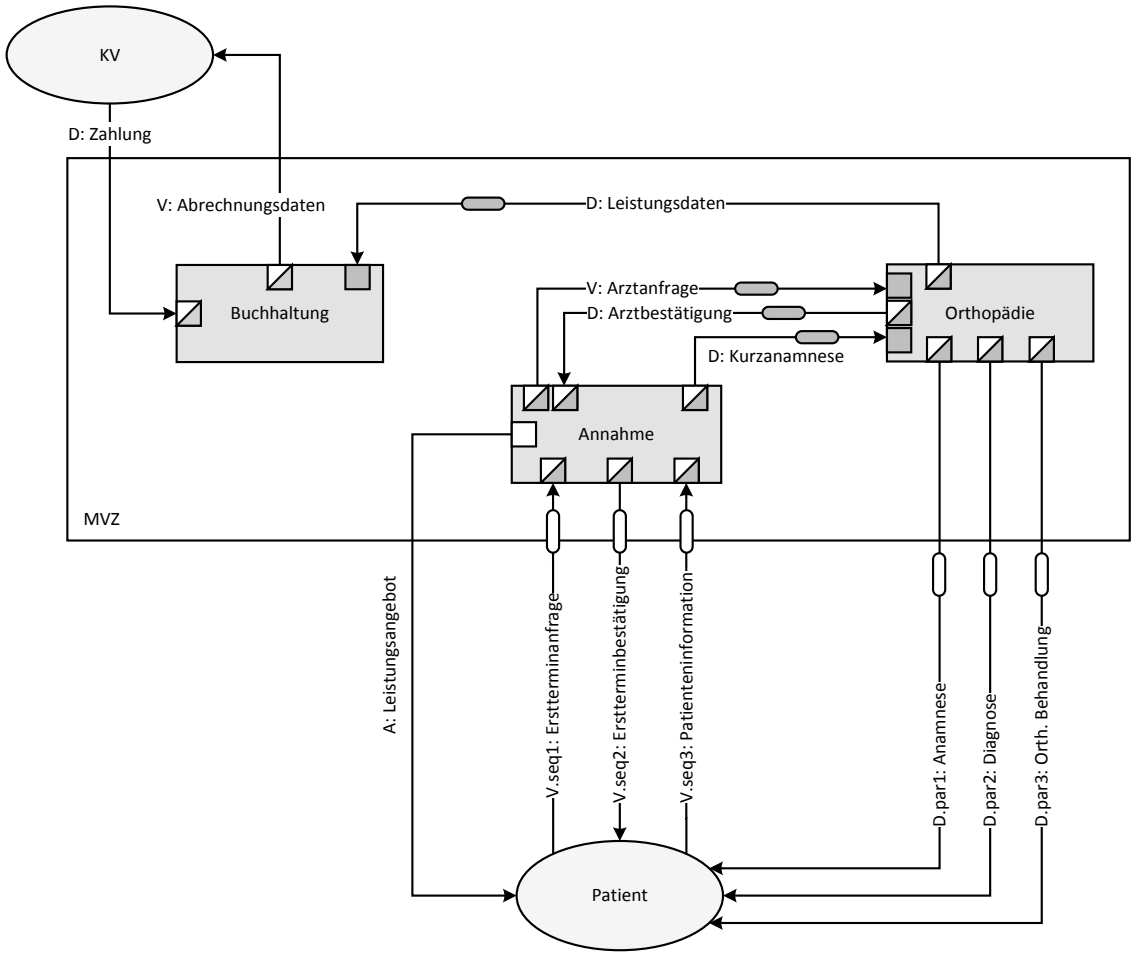

Abbildung 38: Szenario MVZ - IAS (dritte Zerlegungsstufe)

In dieser Zerlegungsstufe des IAS wurden die Leistungsflüsse durch Transaktionszerlegungen weiter verfeinert. Zum einen wurde die Transaktion `Med. Leistung` in die Teilleistungen `Anamnese`, `Diagnose` und `Orth. Behandlung` differenziert, zum anderen die Transaktionen des Terminvereinbarungsprozesses gemäß der Abbildung weiter detailliert.

Kartierung

Die Beziehung zwischen einem Geschäftsprozessmodell und einem diesbezüglich zu entwickelndem Anwendungssystem ist anhand des Konzepts der Automatisierung von Aufgaben und Transaktionen vollständig beschreibbar. Die Kartierung des IAS dient der Visualisierung dieses Konzepts, indem sowohl die Automatisierbarkeit als auch die Automatisierung der

Aufgaben und Transaktionen im Modell dargestellt werden [FeSi08, 216]. Die Automatisierung von Aufgaben wird dabei durch Quadrate in den betrieblichen Objekten symbolisiert, die von Transaktionen durch abgerundete Rechtecke. In dem Szenario wird davon ausgegangen, dass die modellierten Aufgaben und Transaktionen in der Realität nicht automatisiert durchgeführt werden. Die Kartierung stellt somit einen Soll-Zustand dar, der durch die Einführung des zu entwickelnden Anwendungssystems zu erreichen ist. Durch ein ausgefülltes Quadrat wird eine Aufgabe als zu vollautomatisieren dargestellt, ein halbgefülltes kartiert eine geforderte Teilautomatisierung und ein weißes Quadrat eine Nichtautomatisierung der jeweiligen Aufgabe. Bei den Transaktionen wird ein ausgefülltes Symbol zur Darstellung der Vollautomatisierung verwendet, ein weißes Symbol zeigt eine nicht-automatisierte Transaktion[96].

In dem vorgestellten Szenario werden zum Beispiel die Transaktionen der Terminvereinbarung zwischen Patient und Annahme als nicht-automatisiert charakterisiert, da diese persönlich oder fernmündlich durch eine Mensch-zu-Mensch Kommunikation erfolgen. Die zugehörigen Aufgaben auf Seiten der Annahme sind hingegen als teilautomatisiert zu betrachten, da diese durch das Anwendungssystem zu unterstützen sind, so zum Beispiel die Aufnahme und Speicherung der Patientendaten im System.

7.3.2. Verhaltenssicht

Die Verhaltenssicht des Geschäftsprozesses wird anhand von Vorgangstypen und deren Ereignisbeziehungen modelliert. Auf der Grundlage der dritten Zerlegungsstufe des IAS kann das folgende VES erstellt werden.

[96] Für eine weiterführende Darstellung des Automatisierungskonzepts sowie der Kartierung des IAS sei auf [FeSi08, 215ff] verwiesen.

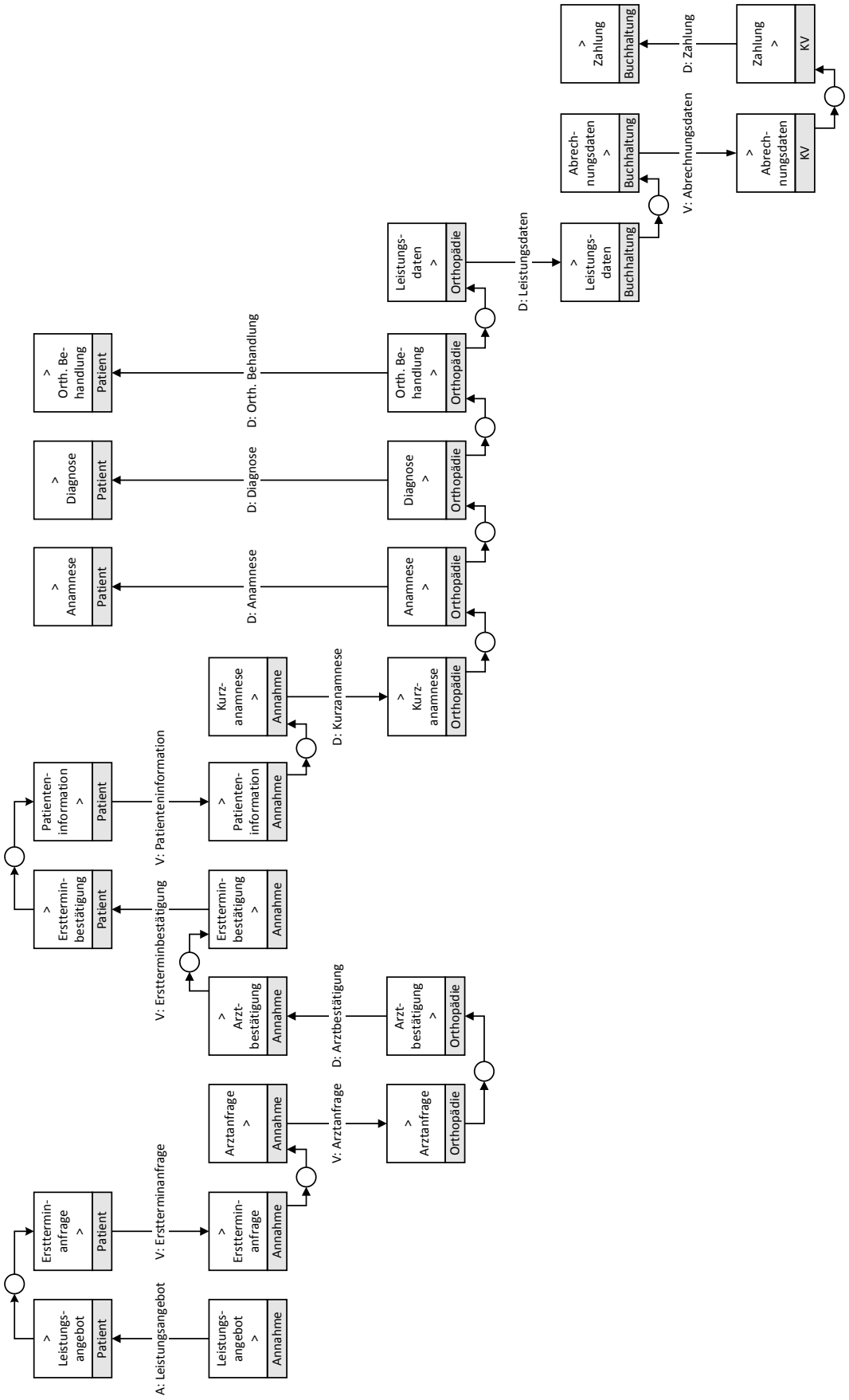

Abbildung 39: Szenario MVZ - VES

Der betrachtete Geschäftsprozess wird im VES als durchgängiger Standardfall modelliert, d.h. es werden aus Komplexitätsgründen keine Varianten in den Entscheidungsprozessen, zum Beispiel die Ablehnung einer Terminanfrage, abgebildet. Diese Einschränkung erfolgt vornehmlich aus Gründen der Komplexitäts- und Umfangsreduktion und hat keine inhaltliche Auswirkung auf die spätere Darstellung der Sicherheitsmodellierung in SOMsec.

Nach der Erstterminanfrage der `Patienten` erfolgt die Verfügbarkeitsanfrage für einen Arzt durch die `Annahme` bei der `Orthopädie`. Nach dem Erhalt der Arztbestätigung wird der Termin dem `Patienten` gegenüber bestätigt und dessen Stammdaten erfasst. Basierend auf diesen Patienteninformationen wird im Anschluss durch die `Annahme` eine Kurzanamnese erstellt, die der `Orthopädie` als behandelndem Leistungsbereich übergeben wird. Dort wird darauf aufbauend eine Anamnese des Patienten erstellt, die wiederum als Grundlage für die Diagnose und die resultierende Behandlung dient. Ist Letztere erfolgt, kann durch die `Orthopädie` die diesbezügliche Leistungsdatenerfassung durchgeführt und der `Buchhaltung` zum Zweck der Abrechnung übergeben werden. Dort erfolgt sodann die Abrechnungserstellung für die `KV`, die abschließend in einer Zahlung an die `Buchhaltung` für die erbrachten Behandlungsleistungen resultiert.

7.3.3. Definition und Abgrenzung des Anwendungssystems

Für die Unterstützung der Durchführung der modellierten Geschäftsprozesse ist ein Anwendungssystem zu entwickeln, das die integrierte Bearbeitung der Patientenaufnahme sowie der Verwaltung und Durchführung der ärztlichen Leistungen ermöglicht. In Bezug auf die Geschäftsprozessmodelle erfolgt dies durch die Umsetzung der als voll- oder teilautomatisiert kartierten Aufgaben eines oder mehrerer betrieblicher Objekte. Geht man von weitgehend homomorphen Strukturen auf Geschäftsprozess- und Anwendungssystemebene aus, so kann ein Anwendungssystem somit anhand eines oder mehrerer modellierter betrieblichen Objekte abgegrenzt werden [FeSi08, 217]. Im vorliegenden Szenario erfolgt dies mittels der Objekte `Annahme` und `Orthopädie`, mit dem Ziel ein integriertes Anwendungssystem zur Patienten- und Leistungsverwaltung des `MVZ` zu spezifizieren. Beide Objekte bilden dabei jeweils eine funktionale Komponente des Anwendungssystems, die über interne Nachrichten kommunizieren. Das betriebliche Objekt `Buchhaltung` wird dabei als bestehendes, externes Anwendungssystem interpretiert, das die entsprechenden Daten der Leistungserfassung in elektronischer

Form über eine Computer-Computer-Schnittstelle durch das zu entwickelnde Anwendungssystem empfängt.

7.3.4. Fachliche Spezifikation des Anwendungssystems

Die fachliche Spezifikation eines Anwendungssystems erfolgt in SOM objektorientiert und -integriert durch ein konzeptuelles Objektschema (KOS) sowie ein darauf aufbauendes Vorgangsobjektschema (VOS). Das KOS bezieht sich auf die strukturorientierten Aspekte der fachlichen Anwendungssystemspezifikation und ist als objektorientierte Erweiterung eines konzeptuellen Datenschemas im SERM (Strukturiertes Entity-Relationship-Modell)[97] interpretierbar [FeSi08, 219]. Es besteht aus untereinander in Beziehungen stehender konzeptuellen Objekttypen (KOT), die durch ihren Namen, einer Menge von Attributen sowie Methoden und Nachrichtendefinitionen beschrieben werden. Als Beziehungsarten stehen interacts_with, is_a und is_part_of zur Verfügung, durch die das KOS in Anlehnung an das SERM in quasi-hierarchischer Struktur dargestellt wird.

Das VOS spezifiziert das zugehörige Verhalten des zu entwickelnden Anwendungssystems. Es besteht aus einer Menge von Vorgangsobjekttypen (VOT), die das Zusammenwirken von KOT bei der Durchführung einer betrieblichen Aufgabe (Vorgang) beschreiben. Ein VOT besteht analog zu den KOT aus einem Namen, Attributen, Methoden sowie Nachrichtendefinitionen. Durch die Ausprägungen der Attribute wird dabei das Aufgabenobjekt der durch das VOT durchzuführenden Aufgabe in Form eines Teilgraphen des KOS definiert. Die Beziehungen zwischen den VOT sind vom Typ interacts_with und korrespondieren mit den Ereignisbeziehungen im VES [FeSi08, 225].

Initiales KOS

Nach der fachlichen Abgrenzung des Anwendungssystems sind sowohl KOS als auch VOS initial aus den zugehörigen IAS und VES abzuleiten[98]. Das initiale Vorgangsobjektschema stellt dabei für jedes der betrieblichen Objekte eine Projektion auf die durch das Anwen-

[97] Das SERM wurde 1989 von SINZ als Erweiterung des Entity-Relationship-Models vorgestellt. Für einen ausführliche Beschreibung sei auf [Sinz93] verwiesen.

[98] Für die detaillierte Darstellung der Ableitungsregeln sei auf [FeSi08, 221ff].

dungssystem zu erfüllenden Aufgaben des VES dar. Das initiale KOS bildet das zugehörige konzeptuelle Datenschema[99].

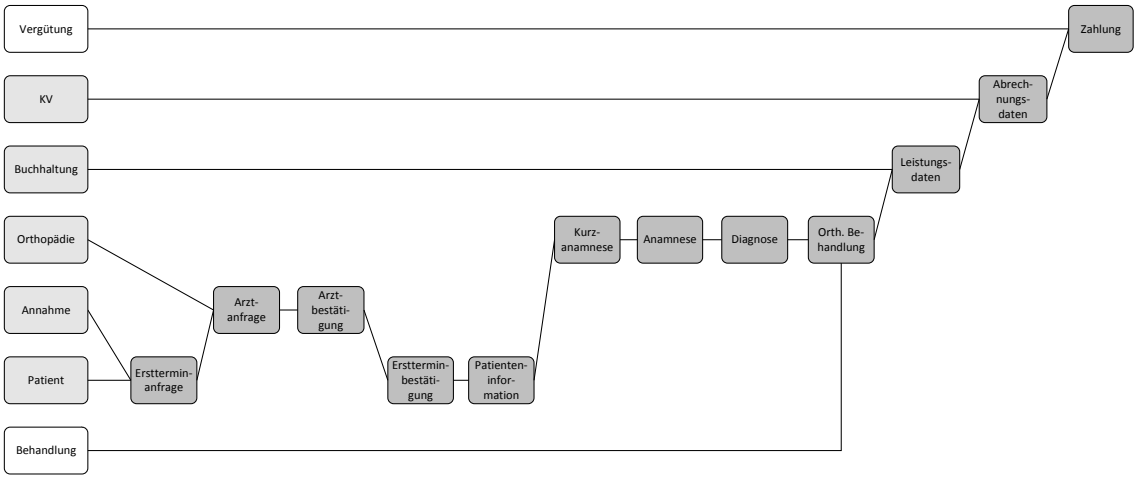

Abbildung 40: Szenario MVZ - initiales KOS

Die Leistungstransaktionen des initialen IAS werden in die leistungsspezifischen KOT (weiß hinterlegt) `Vergütung` und `Behandlung` überführt, die objektspezifischen KOT (hellgrau hinterlegt) werden abgeleitet aus den modellierten betrieblichen Objekten. Die transaktionsspezifischen KOT (dunkelgrau hinterlegt) entsprechen den im Geschäftsprozessmodell modellierten Transaktionen, die gemäß ihrer Reihenfolgebeziehung im KOS unter Berücksichtigung der resultierenden Existenzabhängigkeiten dargestellt werden.

Initiales VOS

Die Darstellung des initialen VOS bezieht sich auf die betrieblichen Objekte `Annahme` und `Orthopädie`. Aufgeführt werden alle Aufgaben, die aus dem VES der feinsten Detailierungsstufe zu ersehen sind. Zudem werden die entsprechenden objektinternen Ereignisse sowie die objektübergreifenden Transaktionen aus Sicht des Anwendungssystems in Form von Interaktionsbeziehungen abgebildet. Die Vorgangsobjekttypen sowie die Beziehungen sind in der Darstellung jeweils durch eine zusammenfassende Beschreibung erweitert.

[99] Auf eine Darstellung der Attribute und Operatoren in den initialen Schemata wurde aus Komplexitätsgründen verzichtet.

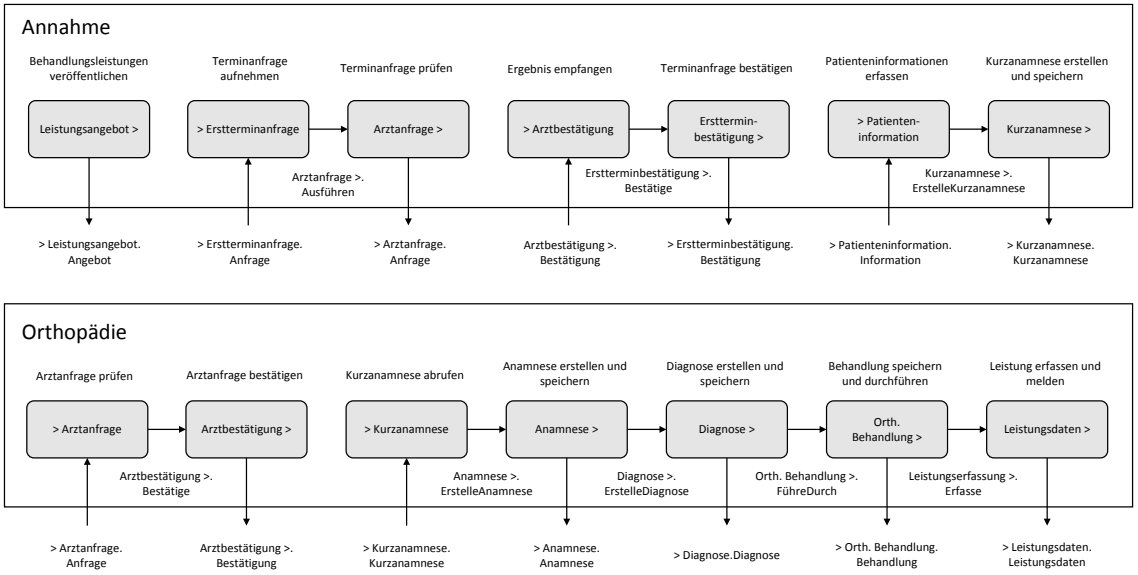

Abbildung 41: Szenario MVZ - initiales VOS

In die Ableitung des initialen KOS wurden unabhängig von der fachlichen Abgrenzung des Systems alle modellierten betrieblichen Objekte einbezogen, im VOS ebenso alle Aufgaben ungeachtet des jeweiligen Automatisierungsgrades berücksichtigt. In den weiteren Schritten ist daher eine entsprechende Konsolidierung von KOS und VOS im Hinblick auf die Abgrenzung des Anwendungssystems durchzuführen.

Aus den Geschäftsprozessmodellen sind für die initialen KOT und VOT keine Attribute, Nachrichtendefinitionen oder Operatoren ableitbar. Sie sind durch den Modellierer zu spezifizieren und weiterzuentwickeln. Dies geht einher mit einer Differenzierung und Konsolidierung des KOS hinsichtlich der Zerlegung von komplexen Objekttypen bzw. der Zusammenfassung von Objekten mit sich überlappenden Attributen. Parallel dazu erfolgt eine analoge Bearbeitung des VOS, sodass jedem VOT ein Teilgraph des KOS als Repräsentation des durch diese Aufgabe zu bearbeitenden Aufgabenobjekts zugeordnet werden kann. Die folgenden Abbildungen zeigen das entsprechend überarbeitete KOS und VOS, die im Rahmen der vorliegenden Arbeit als finaler Detaillierungsgrad der fachlichen Spezifikation des Anwendungssystems Verwendung finden.

Überarbeitetes KOS

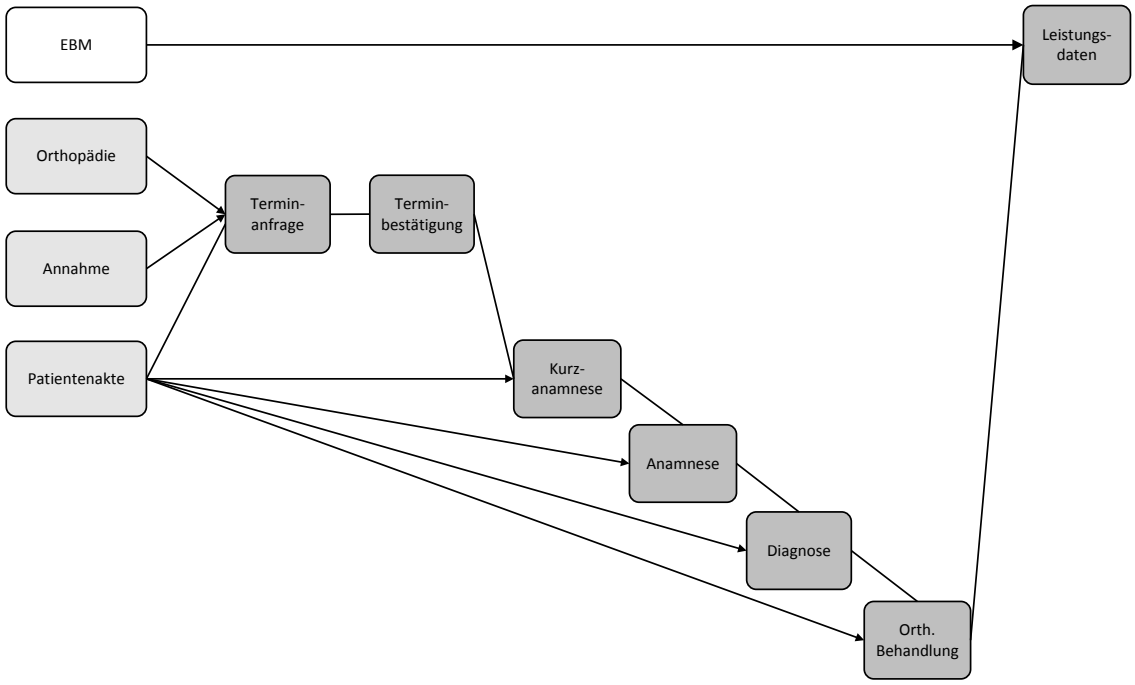

Abbildung 42: Szenario MVZ - überarbeitetes KOS

Im Rahmen der schrittweisen Überarbeitung wurden die KOT `KV` und `Buchhaltung` entfernt, da sie nicht im definierten Bereich der Anwendungssystemspezifikation liegen. Die leistungsspezifischen Objekttypen `Vergütung` und `Behandlung` werden in den Objekttypen `EBM` (einheitlicher Bewertungsmaßstab) umbenannt, als Verweis auf das in Deutschland für die ambulante Versorgung gültige Vergütungssystem hinsichtlich der Abrechnung erbrachter Leistungen gegenüber der gesetzlichen Krankenversicherung. Die in diesem Verzeichnis erfassten Punktzahlen für einzelne medizinische Leistungen spezifizieren aus Sicht des Anwendungssystems diese Teilleistungen der Behandlung und werden in bestimmten Intervallen dann gegenüber der `KV` zur Abrechnung gebracht. Weiterhin wurden die transaktionsspezifischen KOT, die den Terminvereinbarungsprozess zwischen `Patient` und `Annahme` abbilden, auf Grund von weitgehend identischen Attributen und Operatoren zu den KOT `Terminanfrage` und `Terminbestätigung` zusammengefasst. Die transaktionsspezifischen KOT `Kurzanamnese`, `Anamnese`, `Diagnose` und `Orth. Behandlung` wurden durch is_part_of-Beziehungen zu dem Objekttyp `Patientenakte` aggregiert, der aus Sicht des Anwendungssystems einen im System angelegten Patienten repräsentiert. Die Existenzabhängigkeiten des initalen KOS wurden durch die interacts_with-Beziehungen zwischen `Terminbestätigung` und `Kurzanamnese` sowie `Behandlung` und `Leistungsdaten` gewahrt. Das Schema sagt demnach aus, dass

eine Patientenakte zum Beispiel mit Stammdaten des Patienten generell angelegt werden kann, eine Kurzanamnese jedoch nur nach einer erfolgten Terminbestätigung erstellt wird. Die spezifizierten KOT bilden in dieser Form die konzeptuelle Datenbasis für das überarbeitete VOS.

Überarbeitetes VOS

Die VOT des initialen VOS wurden größtenteils im Hinblick auf die Wahrung der semantischen Integrität des Anwendungssystems zusammengefasst. Auf diese Weise werden Aufgaben, die in der Regel parallel oder sequentiell durchzuführen sind, zu einem VOT eines betrieblichen Objekts aggregiert. Damit einhergehend erfolgt eine Neubenennung der VOT sowie eine Redefinition der zu interpretierenden Nachrichten. Letztere korrespondieren dabei mit dem Vorliegen der entsprechend benötigten Informationen im System im Sinne von erstellten Datenobjekten.

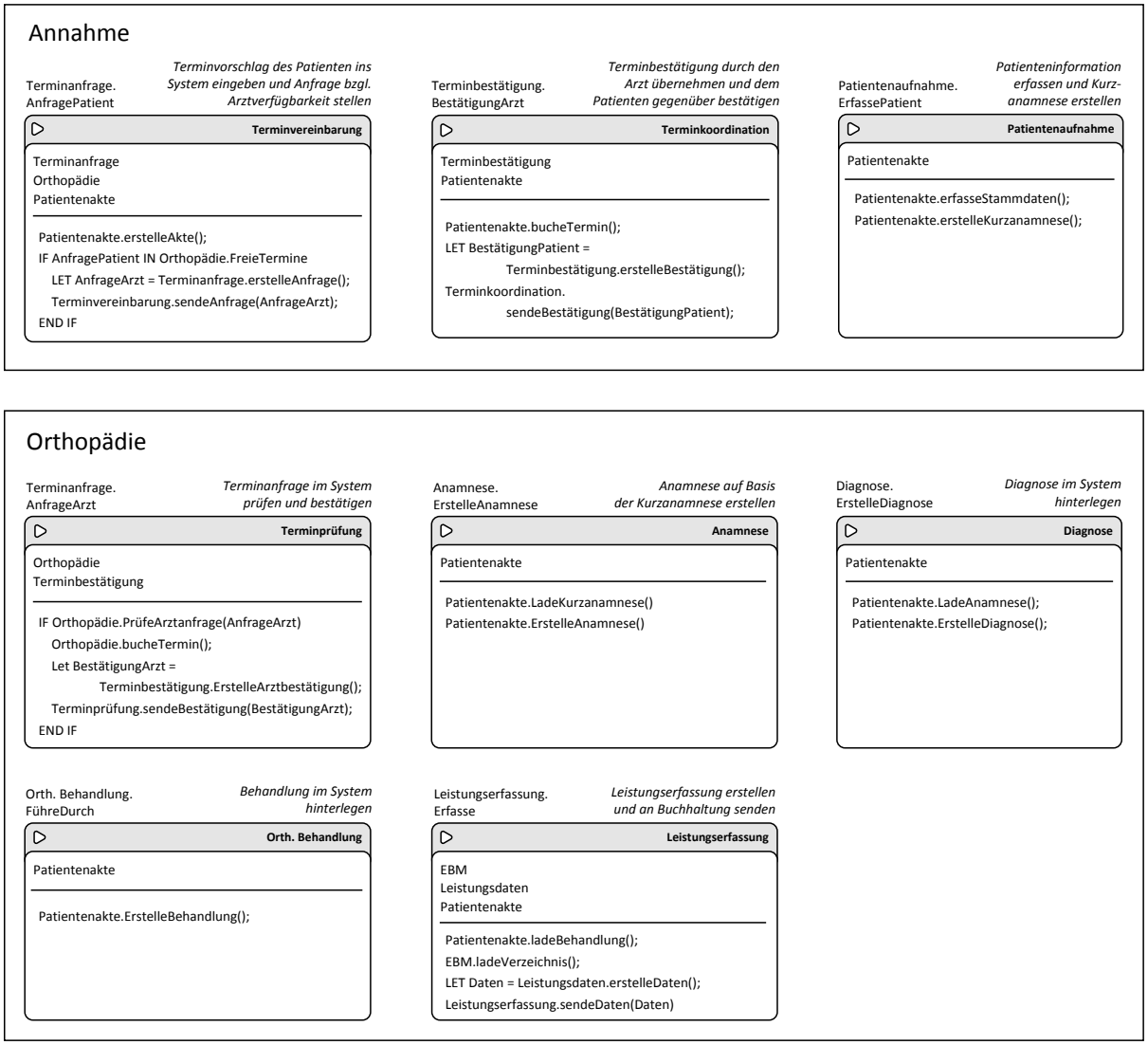

Abbildung 43: Szenario MVZ - überarbeitetes VOS

Die Aufgaben `>Erstterminanfrage` und `Arztanfrage>`, `>Arztbestätigung` und `Erstterminbestätigung>` sowie `>Patienteninformation` und `Kurzanamnese>` wurden zu den VOT `Terminvereinbarung`, `Terminkoordination` sowie `Patientenaufnahme` der `Annahme` zusammengefasst. Die Aufgaben `>Arztanfrage`, Arztbestätigung> sowie `>Kurzanamnese` und `Anamnese>` der `Orthopädie` wurden zu den VOT `Terminprüfung` und `Anamnese` konsolidiert. Zusätzlich wurde die Aufgabe `Leistungsdaten>` in den VOT `Leistungserfassung` transformiert. Die entsprechenden Nachrichtendefinitionen bzw. Ereignisse wurden in Bezug auf die Modellierung des KOS angepasst.

Die Operatoren der VOT sind in Pseudocode notiert und geben einen groben Einblick in die fachlich relevanten Aktionen, die im Rahmen des Vorgangs durchzuführen sind[100]. Anhand der Notation der Methodenaufrufe ist die jeweilige Navigation in dem entsprechenden Teilgraphen des KOS ersichtlich, der all diejenigen KOT umfasst, die das Aufgabenobjekt des Vorgangs darstellen. Diese KOT werden als Attribute im oberen Bereich der VOT dargestellt.

Die überarbeiteten Schemata des KOS und VOS bilden gemeinsam die fachliche Spezifikation des zu entwickelnden Anwendungssystems. Sie stellen damit den Ausgangspunkt für den systemtechnischen Entwurf und für die Realisierung des Anwendungssystems dar [FeSi08, 226].

Mit der vorgestellten Modellierung des Szenarios wurde das grundlegende Vorgehen hinsichtlich der geschäftsprozessgetriebenen Anwendungssystementwicklung von SOM verdeutlicht. Die erstellen Modellschemata dient in den folgenden Abschnitten als Grundlage für die Darstellung der Erweiterungen und Modellierungsschritte, die im Rahmen der geschäftsprozessgetriebenen Sicherheitsmodellierung durch SOMsec vorgenommen werden.

[100] Die Spezifikation der Operatoren erhebt keinen Anspruch auf Vollständigkeit. Das Ziel der Darstellung liegt alleine in der Verdeutlichung der Modellierungsweise und dient im weiteren Verlauf der Arbeit als Bezugspunkt für die Referenzierung durch Sicherheitsobjekttypen.

8. Sicherheitsmodellierung auf Geschäftsprozessebene

Basierend auf den bisherigen Ausführungen zur Modellierung von Informationssicherheit ist zu erörtern, in welcher Weise eine Integration von Schutzzielen in die Geschäftsprozessmodellierung erfolgen kann. Gemäß der Betrachtungsweise des Referenzmodells, werden Geschäftsprozessmodelle, und somit deren Modellelemente, zu Bezugsobjekten der betrieblichen Informationssicherheit. Das Ziel der Sicherheitsmodellierung auf Geschäftsprozessebene ist somit die Schaffung eines sicherheitserweiterten Geschäftsprozessmodells, das als Sicherheitsartefakt für diese Ebene fungiert.

Kapitel 8.1 beschreibt einleitend die für eine Integration von Schutzzielen zu beantwortenden Fragestellungen, bevor in den Kapitel 8.2, 8.3 und 8.4 die entsprechenden Themenbereiche der Schutzzielintegration diskutiert werden. Kapitel 8.5 stellt im Anschluss die Ergebnisse anhand des Szenarios MVZ exemplarisch dar. Abschließend wird eine identitätsbezogene Erweiterung der Schutzzielmodellierung in Kapitel 8.6 vorgestellt.

8.1. Schutzziele in Geschäftsprozessen

Geschäftsprozessmodelle beschreiben die zweite Ebene der SOM-Unternehmensarchitektur und somit die Aufgabenebene eines betrieblichen Systems. Sie ist klar abzugrenzen von der Aufgabenträgerebene, mit der Implikation, dass weder Personen noch maschinelle Aufgabenträger in Form von Anwendungssystemen oder Hardware als Modellelemente referenziert werden. Für die Integration von Sicherheitsaspekten bedeutet dies, dass keine aufgabenträgerspezifischen Bezugsobjekte modelliert werden und somit die entsprechenden Schutzziele, die im Definitionsrahmen anhand der aufgabenträgerspezifischen Merkmale definiert wurden, auf dieser Betrachtungsebene keine Beachtung finden. Um eine vollständige Integration der verbleibenden Schutzziele in die Geschäftsprozessmodellierung durchzuführen, sind die drei folgenden Fragestellungen zu klären.

- Zum einen ist zu identifizieren, welche Modellelemente in den einzelnen Modellsichten für welche Schutzziele relevant sind (**semantische Integration**).
- Weiterhin ist zu klären, wie die Modellierung der Schutzziele im Rahmen des Modellierungsansatzes erfolgen kann (**syntaktische Integration**).

- Schließlich ist zu definieren, wie die grundlegenden Zusammenhänge zwischen den Modellsichten im Rahmen eines sicherheitsorientierten Modellierungsvorgehens spezifiziert werden können (**methodische Integration**).

In den folgenden Kapiteln werden diese drei Fragestellungen erörtert.

8.2. Semantische Integration von Schutzzielen

Das Ziel der semantischen Integration von Schutzzielen ist die Darstellung, welche Schutzziele in welcher Modellsicht der Geschäftsprozessmodellierung Verwendung finden können, bzw. auf welche Modellelemente sie zu beziehen sind. Der Themenkomplex der semantischen Integration ist demnach zu gliedern in die beiden Teilbereiche der Identifikation schutzzielrelevanter Modellelemente des IAS und VES sowie die Identifikation diesbezüglich modellierbarer Schutzzieltypen.

8.2.1. Identifikation relevanter Modellelemente

Auf der Grundlage der bisherigen Ausführungen dieser Arbeit kann die Identifikation relevanter Modellelemente durch eine Verknüpfung des Definitionsrahmens zur Systematisierung der Schutzziele[101] mit dem Meta-Modell der zu Grunde liegenden SOM-Methodik durchgeführt werden.

8.2.1.1. Vorgehen

Dem Meta-Modell sowie dem Definitionsrahmen gemein ist der Bezugsrahmen des betrieblichen Informationssystems sowie die zentrale methodische Fundierung auf Basis der Systemtheorie mit struktur- und verhaltensorientierten Sichtweisen. Anhand einer Abbildung der Elemente beider Komponenten aufeinander, können die grundlegenden sicherheitsrelevanten Beziehungen aufgezeigt werden. Eine Abbildungsbeziehung zwischen Modellelement und Merkmal besagt dann, dass das jeweilige Modellelement des Meta-Modells als Bezugsobjekt für die im Definitionsrahmen identifizierten Schutzziele des jeweiligen Merkmals fungieren kann. Die folgende Abbildung zeigt identifizierbare Beziehungen im Überblick, bevor im Anschluss die Herleitung für die jeweiligen Modellelemente im Detail diskutiert wird.

[101] Vgl. hierzu Kapitel 5.4.3.2.

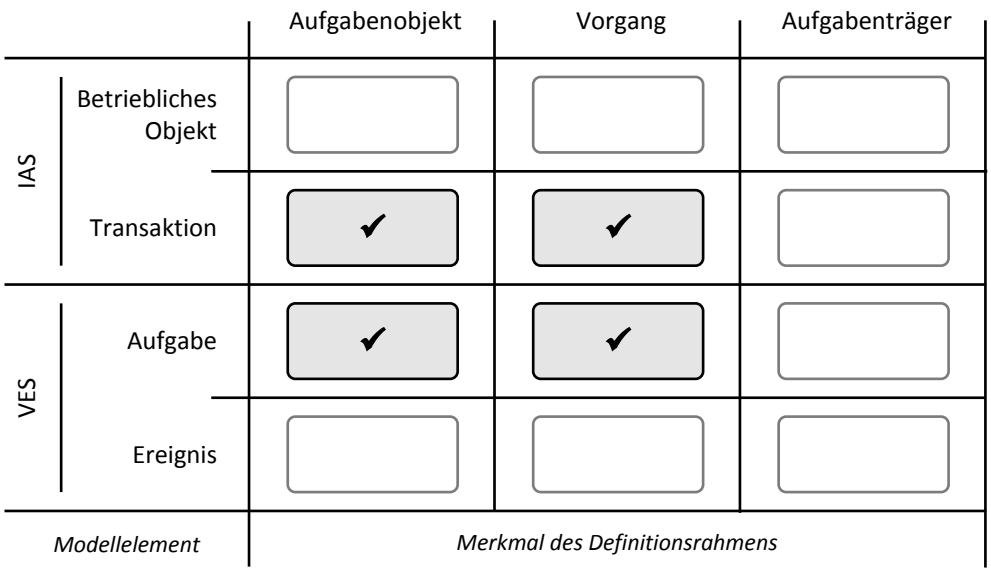

Abbildung 44: Ableitung sicherheitsrelevanter Modellelemente

Realisierbare Verknüpfungsbeziehungen zwischen Modellelement und Merkmal werden in Abbildung 44 durch ein Hakensymbol in einem grau hinterlegten Feld dargestellt. Gestrichelte Felder symbolisieren, dass das jeweilige Modellelement nicht als Bezugsobjekt im Rahmen der Geschäftsprozessmodellierung fungieren kann. Die Ableitung der vier aufgezeigten Abbildungsbeziehungen zwischen den Modellelementen und den Definitionsmerkmalen sowie deren Interpretation wird in den folgenden Abschnitten im Detail erläutert. Als grundlegender Indikator für die Identifikation der Modellelemente, die als Bezugsobjekte für Schutzziele relevant sind, dient dabei deren semantischer Gehalt in Bezug auf sicherheitsrelevante Eigenschaften.

8.2.1.2. Schutzzielrelevante Modellelemente im IAS

Die Modellelemente eines Interaktionsschemas sind Instanzen der Meta-Modellelementtypen „Betriebliches Objekt“ und „Transaktion“. Für beide Elemente ist die Eignung als mögliche Bezugsobjekte für die Modellierung von Schutzzielen zu diskutieren.

Modellelement betriebliches Objekt

Ein betriebliches Objekt umfasst eine Menge von Aufgaben, die zusammengehörige Sach- und Formalziele verfolgen und auf einem gemeinsamen Aufgabenobjekt operieren. Das Konzept der Objektorientierung, als Element der grundlegenden Modellierungsmetapher von SOM, wird dabei auf die Bildung betrieblicher Aufgabenstrukturen angewandt [FeSi08, 200].

Betriebliche Objekte bilden somit logische Komponenten, die über das Konzept der losen Kopplung mit anderen Komponenten interagieren.

Das Modellelement des betrieblichen Objekts wird aus der Sicht der vorliegenden Arbeit insbesondere durch die letztgenannte Interpretation charakterisiert. Es dient als logischer Container für Aufgaben, die im Interaktionsschema selbst nicht explizit modelliert werden und fungiert in Bezug auf das Konzept der losen Kopplung als Sender und Empfänger von Nachrichten. Wird das Modellelement sowohl aus inhaltlicher wie auch aus modelltheoretischer Sicht analysiert, so sind in diesem Zusammenhang keine sicherheitsrelevanten Eigenschaften identifizierbar, die durch das Modellelement transportiert werden. Betriebliche Objekte bieten somit keine semantische Grundlage für eine direkte Zuweisungsmöglichkeit von Schutzzielen. In der Konsequenz kann durch eine Zuweisung von Schutzzielen auch keine inhaltliche Anreicherung der Modellaussage im Kontext der Informationssicherheit erfolgen. Betriebliche Objekte fungieren somit nicht als Bezugsobjekte von Schutzzielen im Interaktionsschema.

Modellelement Transaktion

Durch das Modellelement Transaktion wird im Interaktionsschema das Konzept der losen Kopplung zwischen betrieblichen Objekten abgebildet und somit die Koordination betrieblicher Objekte modelliert. Aus inhaltlicher Sicht betrachtet, stellt eine Transaktion einen Kommunikationskanal in Form eines Leistungs- oder Lenkungsflusses dar, der die objektinternen Speicher beteiligter betrieblicher Objekte verbindet. Auf dem Kommunikationskanal werden Leistungspakete und Lenkungsnachrichten transportiert, wobei Letztere zur Koordination der Erstellung und Übergabe von Leistungspakten dienen. Die Erzeugung von Nachrichten und Leistungspakten erfolgt dabei ereignisgetrieben in Form eines fachlichen Kommunikationsprotokolls, das den Austausch der Transaktionsinhalte regelt [FeSi08, 200f].

Aus Aspekten der Informationssicherheit sind primär die angesprochenen Transaktionsinhalte als schutzzielrelevant zu charakterisieren. Ein konkretes Beispiel etwa ist die Anforderung an die Modellierbarkeit von Vertraulichkeit eines im Rahmen einer Transaktion versendeten Angebots. Die Transaktion würde somit als Bezugsobjekt des Schutzziels im Rahmen der Modellierung fungieren. Um diesen Ansatz zu verifizieren und die Semantik einer Annotation von Schutzzielen an Transaktionen herauszuarbeiten, wird das Konstrukt der Transaktion im Folgenden weitergehend analysiert. Als Grundlage dient dabei die Einordnung der inhaltli-

chen Bestandteile einer Transaktion in ein einheitliches Kommunikationsmodell sowie deren Abbildung auf das Konzept der betrieblichen Aufgabe.

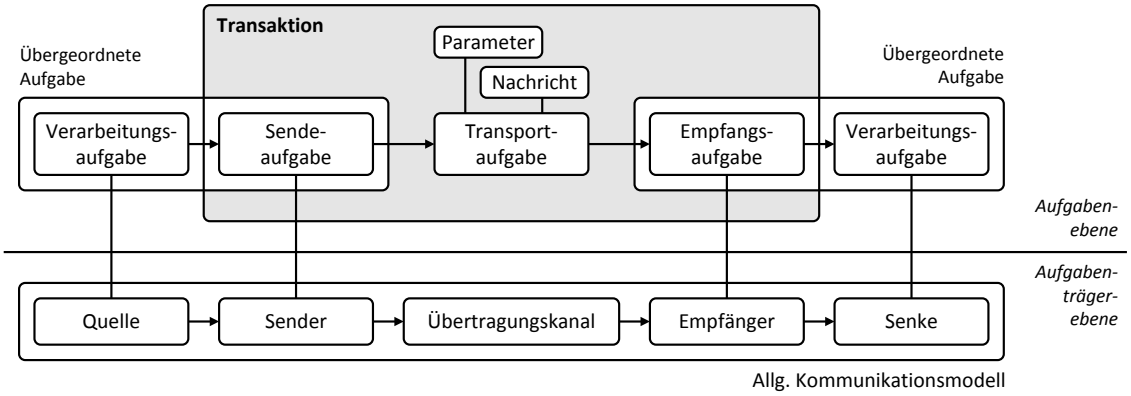

Abbildung 45: Betriebliche Transaktionen anhand des allgemeinen Kommunikationsmodells

Das **allgemeine Kommunikationsmodell** [Shan48, 380] spezifiziert eine Punkt-zu-Punkt-Verbindung zwischen einer Nachrichtenquelle und einer Nachrichtensenke in Form eines Nachrichtenkanals, über den die zu übermittelnde Nachricht durch eine Sendeeinheit verschickt und eine Empfangseinheit entgegengenommen wird. Quelle und Sender sowie Senke und Empfänger können hierbei paarweise als Aufgabenträger von Teilaufgaben zum Versand bzw. zum Empfang einer Nachricht interpretiert werden. Analog hierzu können die Aufgaben eines Geschäftsprozesses in einen Teil zerlegt werden, der die Leistung bzw. die Koordinationsnachricht erstellt, und einen Teil, der die Transaktion zur Übergabe des Leistungspakets bzw. der Nachricht an den Empfänger abwickelt. Der erste Teil wird allgemein als Verarbeitungsaufgabe bezeichnet, der zweite Teil als Sende- bzw. auf Seiten des Empfängers als Empfangsaufgabe [Schm01, 54f]. In Abbildung 45 werden beide Teile als Teilaufgaben einer abstrakten, übergeordneten Aufgabe dargestellt.

Die eigentliche Übertragung der zu sendenden Informationen wird durch den Übertragungskanal realisiert. Differenziert man das skizzierte System aus Verarbeitungs- und Sende- bzw. Empfangsaufgaben sowie dem allgemeinen Kommunikationsmodell in Aufgaben- und Aufgabenträgerebene, so ist dieser der Aufgabenträgerebene zuzuordnen. Die Sendeaufgabe interagiert mit dem Übertragungskanal, indem Nachrichteninhalt sowie weitere Parameter zu Erfüllung des Kommunikationsprotokolls an ihn angelegt werden, in analoger Weise agiert die Empfangsaufgabe. Die Sende- und Empfangsteile der beteiligten Aufgaben werden dabei der Transaktion zugerechnet, die die Nachricht überträgt. Der eigentliche Übertragungsvor-

gang kann als Transportaufgabe interpretiert werden, die durch den Inhalt der Nachricht und das Kommunikationsprotokoll parametrisiert wird. Die Sendeaufgabe generiert diese Parameter und ruft damit die Transportaufgabe auf. Eine betriebliche Transaktion besteht somit aus der sequentiellen Durchführung einer **Sende-, Transport- und Empfangsaufgabe**, die auf den Aufgabenobjekten Nachrichteninhalt und Kommunikationsprotokoll operieren. Aufgabenträger dieser Aufgaben sind die Einheiten Sender, Übertragungskanal und Empfänger. Verhaltensorientiert betrachtet wird dies als **Übertragungsvorgang** bezeichnet.

Auf der Grundlage dieser Betrachtungsweise kann der Modellobjekttyp Transaktion mit dem Definitionsrahmen in Beziehung gesetzt werden. Ein sicherheitsrelevantes Element stellt in diesem Zusammenhang, wie eingangs erwähnt, das Aufgabenobjekt Nachrichteninhalt der Übertragungsaufgabe dar, das mit dem Definitionsmerkmal Information korrespondiert. Ein weiterer Aspekt ergibt sich aus der vorgangsorientierten Betrachtung der Sende- und Empfangsaufgaben, deren Durchführung unter gewissen Umständen ebenfalls als sicherheitsrelevant einzustufen ist. So können zum Beispiel für den Versand eines Angebots, somit der Durchführung der Sendeaufgabe, andere Berechtigungsstrukturen notwendig sein, als für die Erstellung des Angebots im Rahmen der eigentlichen Verarbeitungsaufgabe. Transaktionen sind in SOMsec somit sowohl in aufgabenobjektorientierter wie auch in vorgangsorientierter Sichtweise aus Sicherheits-gesichtspunkten zu berücksichtigen.

Aus **Modellierungsperspektive** wird das **Aufgabenobjekt der Transaktion** im IAS nicht explizit modelliert. Es ist jedoch implizit aus der Spezifikation des Transaktionstyps sowie der Benennung der Transaktion ableitbar. Die Zuweisung des Schutzziels Vertraulichkeit zu einer Vereinbarungstransaktion „Vertragsbestätigung“ etwa bezieht sich somit implizit auf den Transaktionsinhalt, somit das Aufgabenobjekt der Vertragsbestätigung, die potentiell schützenswerte Informationen über die Ausgestaltung eines Vertragsverhältnisses beinhaltet. Ein an eine Transaktion annotiertes Schutzziel bezieht sich somit initial auf die Sicherheit des Aufgabenobjekts im Rahmen der Transaktion. Ein Schutzziel stellt dabei eine Anforderung dar, die im Rahmen der Transaktionsdurchführung gewahrt sein muss.

Ebenfalls nicht expliziert in den Modellschemata werden die **Sende- und Empfangsaufgaben**, die als Ansatzpunkte für die vorgangsorientierte Sicherheitsanalyse einer Transaktion dienen. Aus konzeptueller Sicht sind diese Teilaufgaben, wie oben beschrieben, der jeweiligen Transaktion zuzuordnen. Aus Modellierungssicht werden sie in SOMsec jedoch auch als Bestandteil der entsprechenden Verarbeitungsaufgabe betrachtet, die die jeweilige Transakti-

on auslösen. Die sicherheitsbezogene Berücksichtigung der Sende- und Empfangsaufgaben erfolgt somit im Rahmen der verhaltensorientierten Sicht bei der Integration von Schutzzielen im Vorgangs-Ereignis-Schema. Transaktionen stellen daher ein Bezugsobjekt für die Modellierung von Schutzzielen sowohl im Interaktionsschema, als auch im Rahmen des Vorgangs-Ereignis-Schemas dar.

8.2.1.3. Schutzzielrelevante Modellelemente im VES

Das Vorgangs-Ereignis-Schema stellt die Ablaufsicht eines Geschäftsprozessmodells dar. Es beschreibt diese durch einen ereignisgesteuerten Ablauf von Aufgaben, die in Form von Vorgängen durchgeführt werden. Als Modellierungselemente kommen Instanzen der Objekttypen „Aufgabe“, „Transaktion“ und „Ereignis“ zum Einsatz. Jedes VES korrespondiert dabei mit genau einer Modellierungsstufe des IAS. Analog zum Vorgehen des vorangehenden Abschnitts werden die Modellelemente im Hinblick auf ihre Eignung als Bezugsobjekt der Sicherheitsmodellierung analysiert.

Modellelement Aufgabe

Die Aufgaben eines VES beschreiben das Verhalten desjenigen betrieblichen Objekts, dem sie zugeordnet sind [Mali97, 22]. Aus Modellierungssicht werden sie abgeleitet aus den Transaktionen zwischen betrieblichen Objekten, die im IAS spezifiziert wurden. Modelliert werden dabei diejenigen Aufgaben eines übergebenden und empfangenden Objekts, die die jeweilige Transaktion durchführen [FeSi08, 197f].

Die Semantik im VES modellierter Aufgaben kann in zweifacher Hinsicht interpretiert werden. Zum einen können sie als **Vorgangstypen** verstanden werden, die die Durchführung eines Lösungsverfahrens auf einem Aufgabenobjekt spezifizieren [FeSi08, 97]. Die Bedeutung des Modellelements bezieht sich somit auf die Innensicht der Aufgabe. Zum anderen spezifiziert eine im VES modellierte Aufgabe sowohl Aufgabenobjekt, wie auch Vor- und Nachereignisse der Aufgabe. Diese Merkmale charakterisieren in erster Linie die **Außensicht** einer Aufgabe, die auf Grundlage dieser Sichtweise ebenfalls im VES dargestellt wird [FeSi08, 205].

Auf Grund dieser Doppelsemantik des Modellelements Aufgabe kann es zwei Merkmalen des Definitionsrahmens für Schutzziele zugeordnet werden. Analog zur Argumentation bezüglich der Schutzzielzuweisung zu Transaktionen, kann die Außensicht einer Aufgabe verstanden

werden. In dieser Weise betrachtet korrespondiert das Modellelement Aufgabe mit dem Merkmal Aufgabenobjekt der Schutzzielcharakterisierung und ist mit diesbezüglichen Schutzzielen zu annotieren. Die Schutzziele spiegeln in diesem Verständnis die Sicherheit des Aufgabenobjekts der jeweiligen Aufgabe wider, beziehen sich somit auf den strukturellen Aspekt der Aufgabe. Aus Innensicht betrachtet korrespondiert eine Aufgabe mit dem Merkmal Vorgang. Hierdurch wird der verhaltensorientierte Charakter der Aufgabe aus Sicht der Informationssicherheit adressiert, die Schutzziele beziehen sich somit auf die konkrete Durchführung der Aufgabe.

Das Modellelement Aufgabe fungiert demnach als Bezugsobjekt für die Schutzziele, die für die Merkmale Aufgabenobjekt und Vorgang definiert wurden. Es fungiert somit als Bindeglied für die Verknüpfung der struktur- und verhaltensorientierten Sicherheitsmodellierungen, da aufgabenobjektbezogene Modellannotationen des IAS durch die Doppelsemantik in das VES transformiert werden können. In diesem Zusammenhang kommen auch die oben erwähnten Sende- und Empfangsaufgaben der betrieblichen Transaktionen zum Tragen, durch die eine sicherheitsorientierte Betrachtung der Transaktionen unter Vorgangsgesichtspunkten ermöglicht wird. Die diesbezüglichen Annotationen sind auf Grund der Aufgabencharakteristik im VES durchzuführen und komplettieren auf diese Weise die Sicherheitsanalyse der Transaktionen.

Modellelement Ereignis

Ein Ereignis ist allgemein definiert als Menge von Zuständen betrieblicher Objekte oder von Umweltobjekten. Ein Ereignis löst dann einen Vorgang aus, wenn es mit dem spezifizierten Anfangszustand einer Aufgabe übereinstimmt oder diesen Anfangszustand enthält [FeSi08, 61]. Im VES werden in diesem Zusammenhang Umwelt- und Objektereignisse unterschieden. Während Umweltereignisse als unabhängig existent vorausgesetzt werden und ausschließlich eine Vorgangsauslösung anstoßen können, werden Objektereignisse durch Vorgänge erzeugt und koppeln aus Modellierungssicht die durch sie verbundenen Aufgaben innerhalb eines betrieblichen Objekts [Mali97, 23]. Zusätzlich werden Transaktionen, die im IAS spezifiziert sind, in das VES übernommen und verhaltensorientiert als Transaktionsereignis interpretiert

[Mali97, 17]. Eine Transaktion als Modellelement verbindet in dieser Interpretation objektübergreifend die sie erzeugende Aufgabe mit der sie empfangenden Aufgabe[102].

Umweltereignisse und **Objektereignisse** werden im VES zwar modelliert, im Hinblick auf ihre inhaltliche Ausprägung jedoch nicht konkretisiert. Ein objektinternes Ereignis E, das zwei Aufgaben A_1 und A_2 verbindet, stellt einen Zwischenzustand dar, der zugleich Endzustand von A_1 und Anfangszustand von A_2 ist. Das Ereignis E symbolisiert somit ausschließlich den Auslöser einer Aufgabendurchführung. Auf welche Art das Ereignis erzeugt wird oder welche Variablen entscheidend dafür sind, dass genau dieses Ereignis erzeugt und somit der entsprechende Nachzustand eingenommen wird, liegt nicht im Bereich der Ereignisspezifikation. Auf Grund dieses geringen semantischen Gehalts des Modellelements aus Sicht der Informationssicherheit eignet es sich nicht als Bezugsobjekt für Schutzziele.

Transaktionsereignisse hingegen charakterisieren Zustände durch den Inhalt der Nachrichten, die durch sie transportiert werden. Ein derartiges Ereignis wird somit durch eine konkrete Nachricht repräsentiert, deren Existenz durch die Durchführung einer Transaktion geschaffen wird. Bezogen auf den Nachrichteninhalt eines Transaktionsereignisses werden Schutzziele jedoch bereits aus strukturorientierter Sicht im IAS zugewiesen. Weiterhin wird die Durchführung einer Transaktion im VES nicht als eigenständiger Vorgang interpretiert, sondern, wie beschrieben, als Ereignis. Eine Zuweisung von verhaltensorientierten Schutzzielen ist somit auf Basis des der Arbeit zu Grunde liegenden Verständnisses semantisch als nicht korrekt zu bewerten. Transaktionsereignisse stellen somit ebenfalls kein Bezugsobjekt für Schutzziele dar.

Auf Grund der Übernahme von Transaktionen als Modellelemente aus dem IAS, sind jedoch deren potentiell beschriebene strukturorientierte Schutzziele auch im VES zu berücksichtigen. So ergeben sich mögliche Ableitungsbeziehungen, durch die sich modellierungsrelevante Hinweise auf verhaltensorientierte Schutzzieldefinitionen aufdecken lassen. Dies ist zum Beispiel im Hinblick auf die Berücksichtigung von Sende- und Empfangsaufgaben der Fall, wie bereits in Kapitel 8.2.1.2 beschrieben wurde. Auf diese Weise wird in SOMsec eine sicherheitserweiterte Modellierung einer Transaktion im IAS durch die vorgangsorientierte Perspektive und die damit verbundenen Schutzzielannotationen auf die durch sie verbundenen Aufgaben im VES komplettiert.

[102] Im VES liegt somit eine Doppelsemantik des Modellelements Transaktion vor. Einerseits wird es als Transaktionskanal interpretiert, andererseits als Transaktionsereignis.

8.2.1.4. Zusammenfassung

Durch die Identifikation der sicherheitsrelevanten Modellelemente wird deutlich, dass sich das Grundverständnis zur Modellierung von Sicherheitsaspekten in Geschäftsprozessen in SOMsec nahtlos in die Modellierungsmethodik des SOM-Ansatzes integriert. Der Grund hierfür besteht darin, dass die Sicherheitsmodellierung auf dem grundlegenden Modellkonzept der Transaktionsorientierung von SOM aufbaut ohne zusätzliche Änderung an der Modellierungsmetapher notwendig zu machen. Dieser Sachverhalt unterstützt ebenfalls die praktische Anwendbarkeit des vorliegenden Ansatzes, da auf dieser Ebene keine designierten Sicherheitsexperten zur Annotation von Modellen benötigt werden. Aus Sicht des Modellierers ist die Semantik der initialen, transaktionsorientierten Integration von Schutzzielen in das Modell des Interaktionsschemas einfach nachzuvollziehen und anzuwenden, da es das natürliche Verständnis von Sicherheitsanforderungen in Bezug auf eine potentiell unsichere Übertragung von Informationen unterstützt.

8.2.2. Identifikation modellierbarer Schutzziele

Durch die durchgeführte inhaltliche Analyse der Modellelemente in Bezug auf die Eignung als Bezugsobjekt der Sicherheitsmodellierung wird die Grundlage geschaffen für die weitergehende Identifikation und Abgrenzung von modellierungsrelevanten Schutzzielen in SOMsec.

8.2.2.1. Ableitung relevanter Schutzzielklassen

Die Identifikation modellierbarer Schutzziele erfolgt über die inhaltliche Verknüpfung der bereits dargestellten Matrix aus relevanten Modellelementen und Definitionsmerkmalen. Auf diese Weise kann eine Zuordnung zwischen den Modellelementen und den für sie jeweils relevanten Schutzzielklassen angegeben werden kann. Die folgende Abbildung stellt diesen Ansatz im Überblick dar.

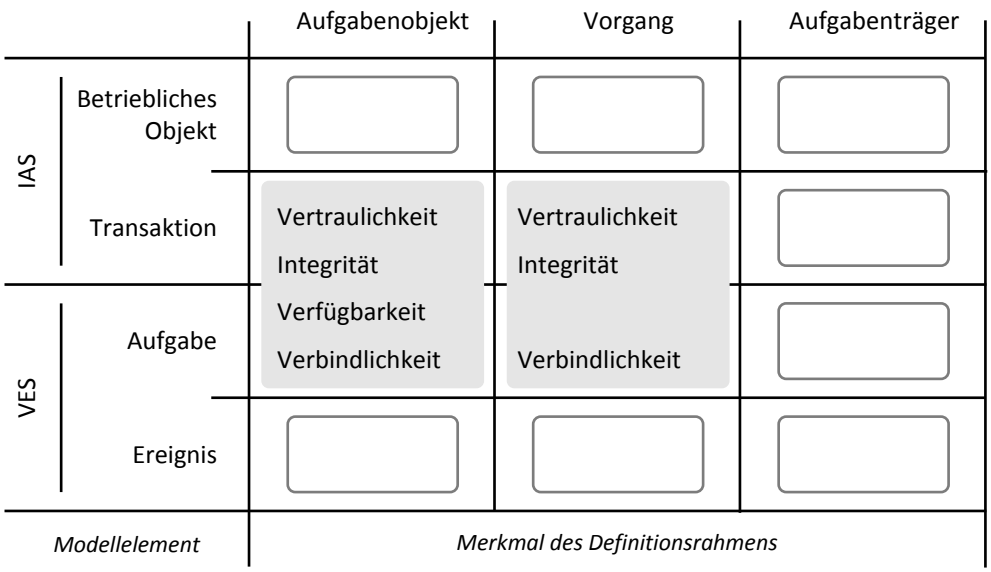

Abbildung 46: Schutzzielklassen sicherheitsrelevanter Modellelemente

Hinsichtlich des Elements Transaktion nimmt die Spalte Aufgabenobjekt Bezug auf die übermittelten Inhalte der Transaktion, die Spalte Vorgang referenziert die Durchführung der entsprechenden Sende- und Empfangsaufgaben. In Bezug auf das Modellelement Aufgabe werden bezeichnungsgemäß jeweils das Aufgabenobjekt bzw. die Durchführung der Aufgabe betrachtet. Die Felder der resultierenden Matrix sind bei beiden sicherheitsrelevanten Modellelementen mit den entsprechend definierten Schutzzielklassen des Definitionsrahmens belegt[103].

Sowohl Transaktionen im IAS als auch Aufgaben im VES können aufgabenobjektorientiert mit allen Instanzen der Schutzzielklassen Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit annotiert werden. Diese beziehen sich auf die schützenswerten Informationen, die sowohl als Inhalte von Transaktionen als auch als Aufgabenobjekte fungieren. Vorgangsorientiert können für beide Elemente Instanzen der Klassen Vertraulichkeit, Integrität und Verbindlichkeit annotiert werden. In Bezug auf Transaktionen sind diese Schutzziele bezogen auf die jeweiligen Sende- und Empfangsaufgaben, hinsichtlich des Modellelements Aufgabe beziehen sie sich auf die entsprechende Aufgabendurchführung.

Auf der Grundlage der identifizierten Schutzzielklassen werden in den folgenden Abschnitten die in SOMsec konkret modellierbaren Schutzzielinstanzen spezifiziert.

[103] Vgl. hierzu Abbildung 23.

8.2.2.2. Abgrenzung der Schutzzielmodellierung

Gemäß Abbildung 46 sind Instanzen aller Schutzzielklassen auf die unterschiedlichen Modellelemente anwendbar. Der Modellierungsschwerpunkt von SOMsec liegt jedoch ausschließlich auf den beiden Schutzzielklassen **Vertraulichkeit** und **Verbindlichkeit**, Verfügbarkeit und Integrität werden im Rahmen der Methodik daher nicht weiter betrachtet.

Die Begründung für dieses Vorgehen liegt in der grundlegenden Orientierung von SOMsec an den Konzepten der geschäftsprozessgetriebenen Anwendungsentwicklung. Die Zielsetzung der Erstellung sicherheitserweiterter Geschäftsprozessmodelle ist die Schaffung eines Modellsystems, das als Ausgangspunkt für die Ableitung von fachlichen Anwendungssystemspezifikationen dienen kann. In diesem Zusammenhang sind die Schutzzielklassen Verfügbarkeit und Integrität als Anforderungen zu interpretieren, die im Prinzip umfassend an jegliche Transaktion bzw. Aufgabe eines Geschäftsprozessmodells zu stellen sind. Sie sind daher in der Regel aufgabenträgerorientiert zu interpretieren und durch entsprechende grundlegende Mechanismen eines Anwendungssystems zu erbringen. Ihre explizite Modellierung im Rahmen eines Geschäftsprozessmodells würde daher im Sinne der Modellqualität und Modellierungstiefe keine Verbesserung sondern vielmehr eine Komplexitätssteigerung für den Modellierer bedeuten. Zwar sind Szenarien denkbar, in denen Verfügbarkeit und Integrität explizit im Fokus stehen, etwa bei der Modellierung hochverfügbarer Geschäftsprozesse, im Rahmen der vorliegenden Arbeit werden diese jedoch nicht berücksichtigt.

Die Schutzzielklassen Vertraulichkeit und Verbindlichkeit sind somit für ihre Verwendung im Rahmen von SOMsec zu präzisieren. Dies erfolgt anhand einer weitergehenden Typisierung dieser Schutzzielklassen im Hinblick auf deren Modellsemantik in Abhängigkeit von den jeweils genutzten Sichten der Geschäftsprozessmodellierung. Im Ergebnis sind dabei die **Schutzzieltypen** der Klassen Vertraulichkeit und Verbindlichkeit zu identifizieren, deren Instanzen auf Schemaebene modellierbar sind. Als Grundlage der Beschreibung dient im Folgenden eine schutzzielspezifische Variante der in Abbildung 46 dargestellten Matrix aus Modellelementen und Merkmalen des Definitionsrahmens. Die Ausführungen zum Modellierungsverständnis der Schutzziele erfolgen dabei vor dem Hintergrund des in SOMsec fokussierten Konzepts der geschäftsprozessgetriebenen Anwendungsentwicklung.

8.2.2.3. Vertraulichkeit

Die grundlegende Zielsetzung der Modellierung von Vertraulichkeit in Geschäftsprozessmodellen bezieht sich primär auf die Festlegung, welche Aufgabenobjekte und welche entsprechenden Aufgaben und Transaktionen aus fachlicher Sicht als vertraulich zu behandeln sind. Vertraulichkeit bedeutet in diesem Zusammenhang die Abgrenzung eines befugten von einem unbefugten Kreis an Identitäten im Hinblick auf die Interaktion mit dem jeweiligen Modellelement.

Vertraulichkeit	Aufgabenobjekt	Vorgang
Transaktion	Transaktions-vertraulichkeit **Vt.T**	Sende-vertraulichkeit **Vt.T(S)** Empfangs-vertraulichkeit **Vt.T(E)**
Aufgabe	Aufgabenobjekt-vertraulichkeit **Vt.A**	Vorgangs-vertraulichkeit **Vt.V**

Abbildung 47: Modellierbare Schutzzieltypen der Vertraulichkeit

Aus aufgabenobjektorientierter Sichtweise bedeutet Vertraulichkeit, dass das Aufgabenobjekt nur Befugten in zulässiger Art und Weise zugänglich gemacht wird. Aus vorgangsorientierter Sichtweise bezieht sich diese Abgrenzung von Befugten und Unbefugten auf die Aufgabendurchführung. In Bezug auf die Modellierung ergeben sich für diese Sichtweise drei Schutzzieltypen, die grundsätzlich in IAS und VES modelliert werden können.

Vertraulichkeitsaspekte von Transaktionen

Der Schutzzieltyp **Transaktionsvertraulichkeit Vt.T** bezieht sich auf die Vertraulichkeit von Informationen als Aufgabenobjekte einer Transaktion. Er besagt, dass die Information während der Übertragung Unbefugten nicht zugänglich sein darf. Vorgangsorientiert werden die Vertraulichkeitseigenschaften einer Transaktion durch die Berücksichtigung der beteiligten Sende- und Empfangsaufgaben bestimmt. Die Schutzzieltypen **Sendevertraulichkeit Vt.T(S)** und **Empfangsvertraulichkeit Vt.T(E)** besagen, dass der Vorgang zum Versand bzw. Empfang einer Transaktion nur durch Befugte durchführbar sein darf. Die Transaktionsvertraulichkeit wird initial im IAS spezifiziert und kann im VES durch die Angabe von Sende- bzw. Empfangsvertraulichkeit präzisiert werden. Eine zwingende Präzisierung ist jedoch nicht ge-

geben, sodass die transaktionsbezogenen Schutzzieltypen grundsätzlich unabhängig voneinander modelliert werden können.

Vertraulichkeitsaspekte von Aufgaben

Die Vertraulichkeit von Aufgabenobjekten während der Durchführung eines Lösungsverfahrens wird durch den Schutzzieltyp der **Aufgabenobjektvertraulichkeit Vt.A** adressiert. Er besagt, dass ein Aufgabenobjekt, unabhängig von der Art des Zugriffs, nur für Befugte zur Verfügung stehen darf. Die Aufgabenobjektvertraulichkeit zielt im Kontext der Anwendungssystementwicklung auf die Berechtigungsvergabe auf Datensatzebene ab. Auf Geschäftsprozessebene sind diese Datenstrukturen jedoch noch nicht zu erfassen, ihre weitere Spezifikation im Rahmen der fachlichen Modellierung ist ebenfalls für eine dedizierte Berechtigungsvergabe als zu grobgranular zu betrachten. Im Ergebnis ist es somit nicht sinnvoll, dieses Schutzziel auf Geschäftsprozessebene zu modellieren, da die angestrebten Ableitungsbeziehungen des Schutzziels zur fachlichen Spezifikation in einem sinnvollen Detailierungsgrad nicht gegeben sind. Der Zweck der Integration von Sicherheitszielen in die geschäftsprozessgetriebene Anwendungsentwicklung ist somit nicht zu erfüllen. Aus diesem Grund wird die Aufgabenobjektvertraulichkeit im weiteren Verlauf der Arbeit nicht mehr berücksichtigt.

Die **Vorgangsvertraulichkeit Vt.V** bezieht sich auf die Vertraulichkeit der Aufgabendurchführung. In Kapitel 5.4.3.3 wurde dieses Schutzziel allgemein als Unbeobachtbarkeit eines Vorgangs eingeführt. Im Kontext von Geschäftsprozessen ist dies dahingehend zu präzisieren, dass Vorgangsvertraulichkeit nicht nur auf die bloße Kenntnis einer Aufgabendurchführung abzielt, sondern sich vielmehr auf die Befugnis zu einer Aufgabendurchführung bezieht. Im Rahmen der geschäftsprozessgetriebenen Anwendungsentwicklung adressiert dies die Berechtigungsvergabe für Operationen des Systems, die im Rahmen der fachlichen Anwendungssystemspezifikation präzisiert werden.

8.2.2.4. Verbindlichkeit

Verbindlichkeit in Geschäftsprozessen bezieht sich grundlegend auf die inhaltliche und auch rechtliche Gültigkeit von Informationen im Sinne der bei der Erzeugung, Übertragung oder Verarbeitung beteiligten Parteien. Diese Gültigkeit ist im Gesamten anzusehen als die Summe aus der Authentizität der die Information erstellenden Identität, der Informationsintegrität während der Übermittlung sowie der Nichtabstreitbarkeit des Erstellungs- und Übertragungsprozesses.

Aus aufgabenobjektorientierter Sichtweise sind in diesem Zusammenhang die Authentizität sowie die Integrität der Information relevant. Im Kontext der Geschäftsprozessmodellierung wirft dies jedoch zwei Problembereiche auf, da zum einen Aufgabenträger nicht modelliert werden und damit deren Authentizität auch nicht abzubilden ist. Zum anderen wird die Integrität, wie bereits beschrieben, als grundsätzliche Voraussetzung für alle Transaktionen in SOMsec angesehen, eine explizite Berücksichtigung erfolgt somit nicht. Eine vollständige Übernahme der allgemeinen Spezifikation der Schutzzielklasse Verbindlichkeit in SOMsec ist somit nicht durchführbar, es ergeben sich die folgenden modellierbaren Schutzzieltypen.

Verbindlichkeit	Aufgabenobjekt	Vorgang
Transaktion	Transaktions-Verbindlichkeit **Vb.T**	Nichtabstreitbarkeit d. Sendung **Na.T(S)** Nichtabstreitbarkeit d. Empfangs **Na.T(E)**
Aufgabe	-	Nichtabstreitbarkeit des Vorgangs **Na.V**

Abbildung 48: Modellierbare Schutzzieltypen der Verbindlichkeit

Verbindlichkeitsaspekte von Transaktionen

Aus aufgabenobjektorientierter Sichtweise modelliert die **Transaktionsverbindlichkeit Vb.T** in SOMsec die grundsätzliche Aussage, dass die übermittelte Information inhaltlich der bewussten Willenserklärung des Senders entspricht. Dabei geht es nicht um die Art des Inhalts, sondern rein um die Gültigkeit dieser Information im Rahmen von fachlichen Kommunikationsprotokollen, wie zum Beispiel einem Bestellvorgang.

Vorgangsorientiert betrachtet wird dieser Aspekt komplettiert durch die Modellierung der Nichtabstreitbarkeit der zugehörigen Sende- und Empfangsaufgaben. Es muss somit sichergestellt werden, dass zusätzlich zum Aufgabeninhalt auch die Durchführung der Versendung bzw. des Empfangs ex post für Dritte nachvollziehbar und beweisbar ist. Modelliert wird dies durch die Schutzzieltypen **Nichtabstreitbarkeit der Sendung Na.T(S)** und **Nichtabstreitbarkeit des Empfangs Na.T(E)**, die im VES spezifiziert werden können.

Verbindlichkeitsaspekte von Aufgaben

Die Verbindlichkeit von Aufgaben wird in SOMsec ausschließlich durch den Schutzzieltyp **Nichtabstreitbarkeit des Vorgangs Na.V** abgebildet, da die Verbindlichkeit eines Aufgabenobjekts im Rahmen einer Verarbeitungsaufgabe aus inhaltlichen Gesichtspunkten nur schwerlich zu belegen ist. Im Gegensatz zu der Transaktionsverbindlichkeit, bei der eine übermittelte Information dediziert, zum Beispiel durch eine digitale Signatur, zu verifizieren ist, ist dieser Aspekt für Verarbeitungsaufgaben nicht zutreffend. In SOMsec wird die Nichtabstreitbarkeit des Vorgangs daher ausschließlich im VES modelliert, mit der Implikation, dass ein Beweis für die Durchführung eines Vorgangs im Sinne der Nichtabstreitbarkeit zu erbringen ist.

Der Schutzzieltyp Nichtabstreitbarkeit nimmt aus vorgangsorientierter Sicht im Rahmen der Schutzzielklasse Verbindlichkeit eine zentrale Rolle ein. In Bezug auf Durchführungen von Verarbeitungsaufgaben ist dessen zentrale Anforderung der Belegbarkeit in einfacher Weise nachvollziehbar. In Bezug auf Transaktionen ist Nichtabstreitbarkeit jedoch differenzierter zu betrachten, da entsprechende fachliche Transaktionsprotokolle Auswirkungen auf die Anforderungen an die Sende- und Empfangsaufgaben aufweisen können. Der folgende Exkurs gibt hierzu einen Einblick.

Exkurs: Transaktionsprotokolle der Nichtabstreitbarkeit

Die Nichtabstreitbarkeit einer Transaktionen kann als zentrale Anforderung in den fachlichen Austauschprotokollen elektronisch abgewickelter Geschäftsprozesse angesehen werden, da diese Übermittlungen von Daten die Grundlage für die Verbindlichkeit von Verträgen und anderen gewerblichen Verpflichtungen bildet [GüRu03, 229]. Die Sicherstellung der Nichtabstreitbarkeit wird plattformunabhängig betrachtet durch die Verwendung von speziellen Transaktionsprotokollen (engl. *non-repudiation protocols*) erreicht. In ihrem Ablauf werden bestimmte Artefakte als Beweismittel erzeugt, die die Nichtabstreitbarkeit einer Transaktion sicherstellen. Der folgenden Abschnitt gibt einen kurzen allgemeinen Überblick dieser Protokolle als Grundlage für die Ableitung des Modellierungsverständnisses in SOMsec.

Grundsätzlich werden in Bezug auf Nichtabstreitbarkeit zwei Arten von Transaktionsmodellen unterschieden. Einerseits kann eine direkte Transaktion zwischen einem Sender S und einem Empfänger E stattfinden (Modell I) , andererseits kann die Transaktion über einen Mittler M von S an E übertragen werden (Modell II). Unter der Prämisse, dass keine Vertrau-

ensbasis zwischen S und E besteht, ist der Einsatz von M, im Folgenden als Trusted Third Party (TTP) bezeichnet, als eine Erweiterung des direkten Kommunikationsmodells anzusehen. Dies hat zum Ziel, benötigte Dienste zur Wahrung der Nichtabstreitbarkeit durch die TTP zu bündeln und im Rahmen der Transaktion erzeugte Beweismittel für die beteiligten Parteien verfügbar zu machen [Oni+09, 17].

Unabhängig von der Verwendung eines bestimmten Transaktionsmodells müssen im Kern die folgenden beiden Anforderungen durch einen Dienst zur Wahrung der Nichtabstreitbarkeit erbracht werden können [Oni+09, 18].

- Sicherstellung der **Nichtabstreitbarkeit der Herkunft** (engl. *non-repudiation of origin*, NRO). Dies beinhaltet den Schutz gegen die fälschliche Behauptung eines Senders, eine Nachricht nicht erzeugt zu haben. Der Beweis der Herkunft (engl. *evidence of origin*, EOO) ist in Modell I durch den Sender bzw. in Modell II durch eine TTP zu erzeugen und für den Empfänger verfügbar zu machen.
- Sicherstellung der **Nichtabstreitbarkeit des Erhalts** (engl. *non-repudiation of receipt*, NRR) entspricht dem Schutz gegen die fälschliche Behauptung eines Empfängers, eine Nachricht nicht erhalten zu haben. Der Beweis des Erhalts (engl. *evidence of receipt*, EOR) ist in Modell I durch den Empfänger bzw. in Modell II durch die TTP zu erzeugen und für den Sender verfügbar zu machen.

Findet ausschließlich das Transaktionsmodell II Verwendung, so müssen zusätzlich zwei weitere Anforderungen berücksichtigt werden, um potentielle Unstimmigkeiten zwischen Sender und TTP bzw. Sender und Empfänger beilegen zu können.

- Sicherstellung der **Nichtabstreitbarkeit der Einreichung** (engl. *non-repudiation of submission*, NRS). Dies ermöglicht den Schutz gegen die fälschliche Behauptung der TTP, eine Nachricht nicht erhalten zu haben. Der Beweis der Einreichung (engl. *evidence of submission*, EOS) ist durch die TTP zu erstellen und für den Sender verfügbar zu machen.
- Sicherstellung der **Nichtabstreitbarkeit der Zustellung** (engl. *non-repudiation of delivery*, NRD) fungiert als Schutz gegen die fälschliche Behauptung der TTP, eine Nachricht nicht zugestellt zu haben. Der Beweis der Zustellung (engl. *evidence of delivery*, EOD) ist durch die TTP zu erstellen und für den Sender verfügbar zu machen.

Die Bereitstellung der entsprechenden Nachweise über Herkunft, Erhalt, Einreichung und Zustellung hat für die Überprüfung der Nachweisbarkeit eines Vorgangs zentralen Charakter. Im Rahmen der Geschäftsprozessmodellierung in SOMsec werden die jeweiligen Transaktionsmodelle jedoch nicht dediziert berücksichtigt, da zu diesem Zeitpunkt der Modellierung noch keine Entscheidung über die sicherheitsrelevanten fachlichen Protokolle der Informationsübermittlung durch den Modellierer zu treffen ist bzw. getroffen werden kann. Diese Betrachtung erfolgt erst im Rahmen der software-technischen Anwendungsentwicklung mit der Spezifikation entsprechender technischer Sicherheitsobjekttypen. Auf Geschäftsprozessebene wird in SOMsec daher die Nichtabstreitbarkeit der Herkunft und die Nichtabstreitbarkeit der Einreichung zu dem Konzept der Nichtabstreitbarkeit des Sendens Na.T(S) aggregiert. Nichtabstreitbarkeit des Erhalts und Nichtabstreitbarkeit der Zustellung werden analog zur Nichtabstreitbarkeit des Empfangs Na.T(E) zusammengefasst**.**

8.2.3. Zusammenfassung

Die Aspekte der Vertraulichkeit und Verbindlichkeit werden in SOMsec durch die Verwendung der drei abstrakten Schutzzieltypen Verbindlichkeit, Vertraulichkeit und Nichtabstreitbarkeit abgebildet. Konkret erfolgt dies in SOMsec aus aufgabenobjektorientierter Sicht durch die Modellierung der Transaktionsvertraulichkeit und -verbindlichkeit. In Bezug auf Vorgänge wird differenziert in die Vorgangs- bzw. Sende- und Empfangsvertraulichkeit, sowie Nichtabstreitbarkeit des Vorgangs, des Sendens und des Empfangs. Die folgende Abbildung stellt die modellierbaren Schutzziele in SOMsec in Abhängigkeit von Modellelementen und den jeweiligen Modellschemata im Überblick dar.

	Interaktionsschema		Vorgangs-Ereignis-Schema	
Transaktion	Transaktionsvertraulichkeit	**Vt.T**	Sendevertraulichkeit Empfangsvertraulichkeit	**Vt.T(S)** **Vt.T(E)**
	Transaktionsverbindlichkeit	**Vb.T**	Nichtabstreitbarkeit d. Sendung Nichtabstreitbarkeit d. Empfangs	**Na.T(S)** **Na.T(E)**
Aufgabe	-		Vorgangsvertraulichkeit	**Vt.V**
	-		Nichtabstreitbarkeit d. Vorgangs	**Na.V**
Modellelement	*Modellschema*			

Abbildung 49: Überblick modellierbarer Schutzzieltypen in SOMsec

Grundsätzlich gilt, dass alle Schutzziele unabhängig voneinander modelliert werden können, die Annotation eines bestimmten Schutzziels somit nicht zwangsläufig die Annotation weiterer Ziele bedingt. Gleichwohl können aus inhaltlichen Gesichtspunkten bestimmte Schutzziele als Indikatoren aufgefasst werden, deren Modellierung zumindest die Überprüfung weiterer sicherheitsrelevanter Aspekte nahelegt. Dieser Sachverhalt ist insbesondere bei der Annotation von Transaktionsvertraulichkeit und Transaktionsverbindlichkeit im IAS gegeben, wodurch die nachfolgende Analyse der beteiligten Sende- und Empfangsaufgaben im VES aus Sicherheitsaspekten an Relevanz gewinnt. Dieser Aspekt wird im Rahmen der Fragestellung der methodischen Integration nochmals aufgegriffen.

Die semantische Unabhängigkeit der Modellierung ist weiterhin anhand der in Kapitel 5.4.3.5 vorgestellten allgemeinen Beziehungen zwischen den Schutzzielklassen zu verifizieren. Relevant ist in diesem Zusammenhang die spezifizierte negative Wirkungsbeziehung zwischen Unbeobachtbarkeit und Nichtabstreitbarkeit. Im Kontext von SOMsec ist die allgemeine Anforderung der Unbeobachtbarkeit zu dem Konzept der Abgrenzung von Befugten und Unbefugten zur Aufgabendurchführung präzisiert. Das Schutzziel der Nichtabstreitbarkeit, im Sinne der Beweisbarkeit eines Vorgangs durch eine rechtsverbindliche Speicherung der jeweiligen Aktion, ist somit nicht als gegenläufig zu bezeichnen, da die in SOMsec genutzte Vorgangsvertraulichkeit nicht mehr auf die Vermeidung dieser Speicherung abzielt. Vielmehr geht es darum, nur Befugten die entsprechenden Rechte zur Aufgabendurchführung einzuräumen. Eine Vermeidung der Beweisbarkeit dieser Durchführung wird hierdurch hingegen nicht gefordert. Die Schutzziele Vorgangsvertraulichkeit und Nichtabstreitbarkeit sind somit unabhängig voneinander modellierbar.

8.3. Syntaktische Integration von Schutzzielen

Die Ausführungen zur syntaktischen Integration haben zum Ziel, die Art der Einbindung von Schutzzielen in die Modellierungsmethodik zu spezifizieren. Anhand des Meta-Modells von SOMsec wird festgelegt, welche Modellelementtypen durch Schutzziele erweitert werden können, wie diese Erweiterung syntaktisch auf Schemaebene erfolgen kann und welcher Grundgedanke hinter der vorzustellenden Erweiterung des Modellierungsansatzes liegt. In Kapitel 8.5 werden die nachfolgenden Ausführungen am Beispiel vorgestellt.

8.3.1. Meta-Modell von SOMsec

Die Integration von Schutzzielen in einen bestehenden Modellierungsansatz ist grundlegend abhängig von dessen **Modellierungsmetapher** sowie den darauf aufbauenden **Sichten** der Modellierungsmethodik und den entsprechenden **Meta-Modellen**. Im Hinblick auf die für SOMsec zu Grunde liegende SOM-Methodik erfolgt dieser Vorgang in zwei Schritten. Zum einen muss die Modelldarstellung um die Möglichkeit zur Angabe von Schutzzielen erweitert werden. Zum anderen müssen Zuweisungsbeziehungen zwischen Schutzzielen und Modellelementen angegeben werden, sodass definiert ist, welche Schutzziele an welchen Modellelementen annotiert werden können.

Der erste Integrationsschritt erfolgt durch die syntaktische Erweiterung der Modellsichten des IAS und VES. Zu diesem Zweck wird das Meta-Modell um einen weiteren Modellelementtyp „Eigenschaft“ erweitert, der als generalisierter Supertyp der Schutzziele zu interpretieren ist. Der zweite Schritt erfolgt durch die Angabe von Attribut-Zuordnungsbeziehungen, die die Zuweisungsmöglichkeiten der Schutzziele, wie sie im Rahmen der semantischen Integration diskutiert wurden, abbilden. Diese Erweiterungsmöglichkeit der SOM-Methodik basiert methodisch auf der Tatsache, dass alle im V-Modell genutzten Modellelemente auf einem einheitlichen, generischen SOM-Objekttypen beruhen, der die Basis für die Begründung des Konzeptes der Objektorientierung im SOM-Ansatz bildet. Dieser SOM-Objekttyp besteht aus einem Namen sowie einem oder mehreren Attributen und Operatoren. Durch die Attribute erfolgt dabei die Spezifikation der Struktur des jeweiligen SOM-Objekttyps. Sie werden auf Meta-Meta-Ebene als generisch betrachtet und erst in Bezug auf die jeweilige Ausprägung des SOM-Objekttyps konkretisiert [FeSi92, 7f]. Transaktionen, betriebliche Objekte und Aufgaben, als Modellelemente des Meta-Modells, stellen solche Konkretisierungen des generischen Objekttyps dar. In der bisher vorgestellten Version des SOM Meta-Modells[104] werden Attribute von Modellobjekttypen jedoch nicht explizit modelliert. Der zu ergänzende Objekttyp „Eigenschaft“ ermöglicht nun genau diese Darstellung und bildet somit die Basis für die syntaktische Integration von Schutzzielen. Das Meta-Modell von SOMsec, in Form einer Erweiterung des Meta-Modells von SOM, kann wie folgt dargestellt werden.

[104] Vgl. Kapitel 7.2.1.2.

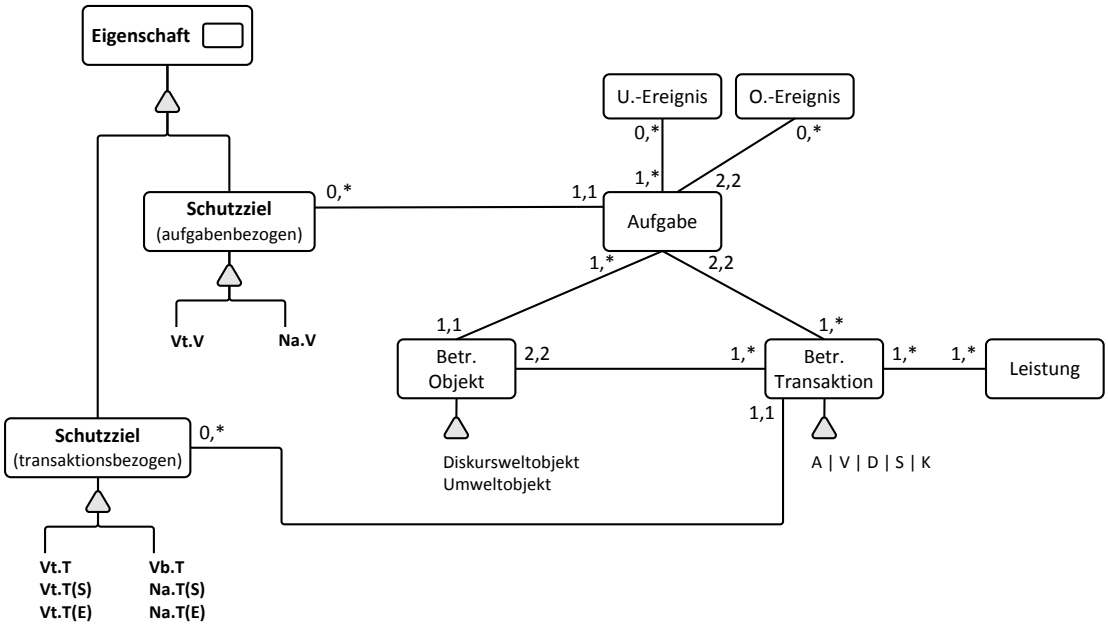

Abbildung 50: Meta-Modell von SOMsec

Der Objekttyp „Eigenschaft“ als Supertyp ist grundsätzlich allen Modellelementen zuzuordnen. Werden jedoch Spezialisierungen definiert, so ist es sinnvoll, durch das Meta-Modell entsprechende Einschränkungen in der Zuordnung vorzunehmen, die die gewünschte semantische Korrektheit eines resultieren Modells sicherstellt. So mag zum Beispiel eine Eigenschaft „Laufzeit“ für den Objekttyp Aufgabe inhaltlich zutreffend erscheinen, in Bezug auf ein betriebliches Objekt ist sie jedoch nicht sinnvoll zu interpretieren. Das vorgestellte Meta-Modell adressiert diesen Sachverhalt im Hinblick auf die Informationssicherheit und schränkt die Zuweisung von Schutzzielen explizit anhand zweier „has“-Beziehungen zwischen den Objekttypen „Schutzziel (aufgabenbezogen)“ und „Aufgabe“ bzw. „Schutzziel (transaktionsbezogen)“ und „Transaktion“ ein. Diese beiden Beziehungen wirken somit einschränkend in Bezug auf die angesprochenen generellen Beziehungen zu allen Modellelementen des Supertyps „Eigenschaft“[105]. Die Objekttypen „Schutzziel (aufgabenbezogen)“ und „Schutzziel (transaktionsbezogen) wiederum sind als Generalisierung der in Kapitel 8.2.3 spezifizierten Schutzzielklassen zu verstehen, die, wie im Rahmen der semantischen Integration erörtert wurde, im Rahmen von SOMsec einzuschränken sind auf Sicherheitsaspekte der Vertraulichkeit und Verbindlichkeit.

[105] Aus Gründen der Übersichtlichkeit sind dessen „has“-Beziehungen im Meta-Modell von SOMsec nicht explizit dargestellt.

Das Meta-Modell von SOMsec ist als konform zu dem Meta-Meta-Modell nach SINZ[106] anzusehen und stellt somit, analog zu SOM, weiterhin eine gültige Extension dar. In Bezug auf die für SOMsec grundlegenden Vorgehensweisen der Geschäftsprozessmodellierung von SOM sind somit keine Änderungen vorzunehmen.

8.3.2. Notationsform

Die grafische Notation einer Eigenschaft auf Schemaebene erfolgt generell über die Darstellung eines gepunkteten, abgerundeten Rechtecks, das optional über eine ebenfalls gepunktete Linie mit dem jeweiligen Zielobjekt verbunden ist. Die Darstellung der Schutzziele in SOMsec folgt diesem Ansatz, ergänzt zu Identifikationszwecken die Modellform jedoch um eine Abkürzung der jeweiligen Schutzzielbezeichnung. In Bezug auf die Schutzziele, die sich auf die nicht explizit modellierten Bezugsobjekte der Sende- und Empfangsaufgabe beziehen, hat sich die gerichtete Positionierung des Modellelements jeweils am Anfang bzw. am Ende einer Transaktion im VES von vorteilhaft erwiesen.

Textuelle Kurzdarstellung

In textueller Form folgt die Notation eines Schutzziels dem folgenden Muster:

```
Schutzzieltyp ( Referenz ) [ Bezeichnung ] : Attribute
```

Die Bezeichnung ist dabei eine frei zu definierende Zeichenkette, die eine eindeutige Identifizierung der Schutzzielinstanz in den Modellschemata erlaubt. Als Referenz wird ein optionaler Verweis auf ein Bezugsobjekt verstanden, das nicht zwingend in einem Schema dargestellt sein muss, das Schutzziel jedoch inhaltlich konkretisiert. Dieser Mechanismus findet insbesondere im Hinblick auf die Darstellung der Verweise auf die Sende- und Empfangsaufgaben Verwendung. Die Attribute beziehen sich schließlich auf die durch die Annotation generierten Eigenschaften des Schutzziels, die aus dem zu Grunde liegenden Modellschema abgeleitet werden können. Sie beziehen sich auf diejenigen Modellelemente, die durch das Schutzziel beeinflusst werden, je nach Schutzziel sind diese Attribute somit unterschiedlich ausgeprägt.

XML-Notation

Um die textuelle Notation der Attribute besser zu strukturieren, kann die Darstellung der modellierter Schutzziele in XML-Notation erfolgen. Jeder Schutzzieltyp entspricht dabei einem

[106] Vgl. hierzu Kapitel 4.2.1.

Hauptelement in Form eines komplexen XML-Typen, der die im Rahmen der grafischen Modellierung gewählte Bezeichnung als Attribut `name` beinhaltet. Die Subelemente beziehen sich dann auf die aus den Modellschemata abzuleitenden Modellelemente, mit denen das annotierte Schutzziel in Beziehung steht.

Im IAS modellierte, transaktionsbezogene Schutzziele, werden beschrieben durch die XML-Elemente `sender`, `empfänger` sowie `transaktion`. Die ersten beiden beziehen sich dabei auf die entsprechenden betrieblichen Objekte, Letzteres auf die Transaktion als direktes Bezugsobjekt. Aufgabenorientierte Schutzziele des VES beinhalten hingegen das betriebliche Objekt in Form des Elements `objekt` sowie die jeweilige betriebliche Aufgabe, die durch das XML-Element `aufgabe` referenziert wird. Beiden Ausprägungstypen eines XML-Hauptelements kann optional ein Subelement `beschreibung` hinzugefügt werden, um natürlichsprachliche Zusatzinformationen anzugeben[107].

Transaktionsorientierte Schutzziele sind somit durch die folgende XML-Notation beschreibbar, dargestellt am Beispiel der Transaktionsvertraulichkeit.

```
<Vt.T name="bezeichnung">
    <sender> betr. objekt </sender>
    <empfänger> betr. objekt </empfänger>
    <transaktion> transaktion </transaktion>
    <beschreibung> text </beschreibung>
</Vt.T>
```

Quelltext 1: XML-Notation transaktionsbezogener Schutzziele

Darstellbar in dieser Form sind die Schutzzieltypen

- Transaktionsvertraulichkeit Vt.T
- Transaktionsverbindlichkeit Vb.T

Für aufgabenorientierte Schutzziele wird die folgende Notationsform genutzt, aufgezeigt am Beispiel der Nichtabstreitbarkeit des Vorgangs.

[107] Die XML-Notation dient ausschließlich der textuellen Veranschaulichung der generierten Modellinformationen. Auf die Darstellung einer entsprechenden Schemadefinition wird daher verzichtet.

```
<Na.V name="bezeichnung">
    <objekt> betr. objekt </objekt>
    <aufgabe> aufgabe </aufgabe>
    <beschreibung> text </beschreibung>
</Na.V>
```

Quelltext 2: XML-Notation aufgabenbezogener Schutzziele

Anzuwenden ist diese Darstellung für folgende Schutzzieltypen:

- Sendevertraulichkeit Vt.T(S)
- Empfangsvertraulichkeit Vt.T(E)
- Vorgangsvertraulichkeit Vt.V
- Nichtabstreitbarkeit des Sendens Na.T(S)
- Nichtabstreitbarkeit des Sendens Na.T(E)
- Nichtabstreitbarkeit des Vorgangs Na.V

Durch die Spezifikation der dargestellten Attribute bzw. XML-Elemente weisen Schutzziele in textueller bzw. XML-Notation den identischen Grad an Modellinformation auf, wie er durch eine initiale Darstellung in einem Modellschema erreicht wird.

In der grafischen Notation wird der erste Teil der textuellen Notation aus Schutzzieltyp, Referenz und Bezeichnung in die Modellierung übernommen. Die sende- und empfangsaufgabenspezifischen Schutzzieltypen werden auf Grund ihrer konzeptuellen Zuordnung zu den jeweiligen Transaktionen weiterhin mit dem Kürzel „.T“ für das Bezugselement Transaktion geführt. Auf diese Weise wird in komplexeren Modellen die Lesbarkeit in Bezug auf die inhaltliche Zugehörigkeit der modellierten Schutzziele erhöht.

8.4. Methodische Integration von Schutzzielen

Die methodische Integration hat zum Ziel, die Modellierungstechnik von Schutzzielen sowie grundsätzliche Abhängigkeiten zwischen der strukturorientierten und der verhaltensorientierten Sicht in der Geschäftsprozessmodellierung in SOMsec aufzuzeigen. Als Grundlage dient die syntaktische Integration in die Modelle des IAS und VES.

8.4.1. Modellierungsvorgehen in SOMsec

Den Ausgangspunkt der Modellbildung in SOMsec bildet analog zu SOM die Spezifikation eines IAS, das die grundlegenden Leistungsbeziehungen der Diskurswelt abbildet. Durch die sukzessive Zerlegung von Objekten und Transaktionen wird dieses initiale IAS bis zur gewünschten Modellierungstiefe verfeinert. Dabei wird durch die Zerlegung nach dem Verhandlungsprinzip die Lenkung von Transaktionen, durch die Zerlegung nach dem Objektprinzip die Lenkung von Objekten aufgedeckt [FeSi08, 202ff][108]. Durch die mehrfache und kombinierbare Anwendungsmöglichkeit der Zerlegungsregeln entstehen so im Laufe der Modellierung Interaktionsschemata auf verschiedenen Zerlegungsstufen.

Das VES wird im Modellierungsverlauf bedarfsgetrieben für die gewünschte Zerlegungsstufe auf Basis des IAS entwickelt. Die folgende Abbildung skizziert das darauf aufbauende Modellierungsvorgehen von SOMsec.

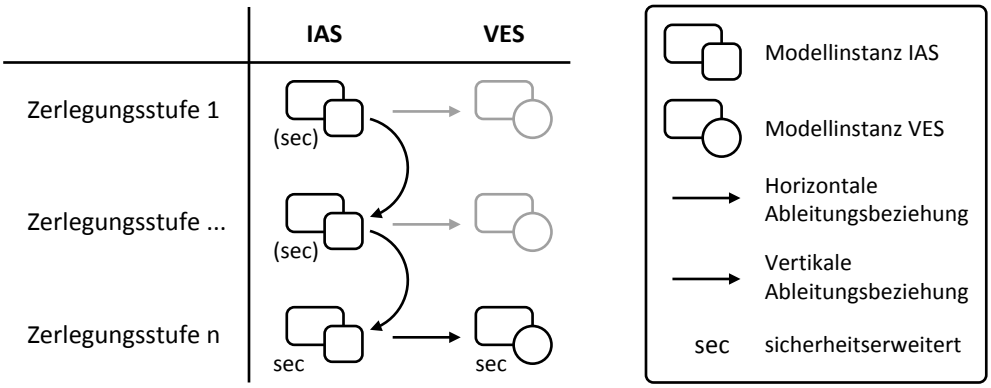

Abbildung 51: Modellierungsvorgehen in SOMsec

Aus der Perspektive der Sicherheitsmodellierung ist im Grunde nur die letzte Zerlegungsstufe der Modelle relevant, um die Annotation der Schutzziele durchführen zu können. Aus dieser Stufe des IAS ist dann ein finales VES abzuleiten, sodass sowohl die Struktur- als auch die Verhaltenssicht des Geschäftsprozesses mit Schutzzielen modelliert sind und inhaltlich übereinstimmen. Gleichwohl können Schutzziele auch optional über die einzelnen Zerlegungsstufen des IAS hinweg aufgedeckt und verfeinert werden. Das sicherheitserweiterte VES wird jedoch bedarfsorientiert immer unabhängig von vorhergehenden VES anhand der aktuellen Stufe des IAS gebildet. Im Vergleich zur Modellierung im IAS entstehen somit keine direkten vertikalen Ableitungsbeziehungen zwischen Zerlegungsstufen des VES, jedoch ist die hori-

[108] Ein Überblick über die Zerlegungsregeln ist in [FeSi08, 203] zu finden.

zontale Ableitung des VES aus dem IAS im Hinblick auf die Übernahme von Schutzzielen zu berücksichtigen. Das resultierende VES fungiert in SOMsec somit als Aggregation aller modellierten Sicherheitsaspekte.

Konkret ergibt sich für diesen ersten Schritt im Rahmen der geschäftsprozessgetriebenen Sicherheitsmodellierung nach SOMsec das folgende Vorgehen.

- Annotation der Schutzziele an Modellelemente des IAS unter Berücksichtigung möglicher vertikaler Ableitungsbeziehungen
- Erstellung des VES und Übertrag der im IAS spezifizierten Schutzziele
- Analyse der an den annotierten Transaktionen beteiligten Aufgaben hinsichtlich der horizontalen Ableitbarkeit entsprechender vorgangsbezogener Schutzziele
- Annotation zusätzlicher, transaktionsunabhängiger Schutzziele im VES
- Analyse der generierten Modellinformationen und gegebenenfalls Erweiterung auf Basis vorherrschenden Expertenwissens

In SOMsec werden auf diese Weise sicherheitserweiterte Varianten des IAS und VES erzeugt, die dann die Grundlage bilden für die weitere Berücksichtigung von Sicherheitsaspekten im Rahmen der fachlichen Spezifikation von Anwendungssystemen. Die einzelnen Schritte werden anhand des vorgestellten Szenarios in Kapitel 8.5 in der praktischen Anwendung dargestellt. Zuvor werden in den folgenden Abschnitten die angesprochenen vertikalen und horizontalen Ableitungsbeziehungen der Schutzziele im Kontext der Modellierungstechnik in IAS und VES im Detail erörtert.

8.4.2. Modellierungstechnik von Schutzzielen im IAS

Den Ausgangspunkt der Modellierung von Informationssicherheit bildet das IAS mit dem Modellelement „Transaktion“ als Bezugsobjekt für die Annotation von Schutzzielen. Im Hinblick auf die sukzessive Verfeinerung des IAS über mehrere Zerlegungsstufen hinweg ist im Kontext der Sicherheitsmodellierung zu klären, wie bereits modellierte Schutzziele einer Stufe i auf einer entstehenden Stufe i+1 zu berücksichtigen sind. Dieser Zusammenhang wird in der vorliegenden Arbeit als **vertikale Ableitungsbeziehung von Schutzzielen** bezeichnet, deren Grundlage durch die Entstehungsmöglichkeiten von Transaktionen im Modellierungsverlauf des IAS definiert wird.

Transaktions- und Objektzerlegung im IAS

Sowohl durch die Zerlegung von Objekten als auch durch die Zerlegung von Transaktionen auf Stufe i können neue Transaktionen auf Stufe i+1 entstehen. Im Falle einer **Objektzerlegung** sind dies hierarchische Steuer- und Kontroll-Transaktionen (S, K), im Falle einer **Transaktionszerlegung** nicht-hierarchische Anbahnung-, Vereinbarungs- und Durchführungstransaktionen (A, V, D).

Durch Transaktionszerlegungen entsteht über die Zerlegungsstufen hinweg eine Baumstruktur aller Transaktionen. Ausgehend von einer Wurzeltransaktion, die in Modellierungsstufe 0 eine Leistung zwischen zwei betrieblichen Objekten beschreibt, werden durch die Zerlegungen neue Transaktionen erzeugt, die unterhalb der Wurzeltransaktion anzuordnen sind. Diese Transaktionen werden allgemein als Kindknoten bezeichnet, die zu dem jeweiligen Elternknoten in hierarchischer Beziehung stehen. Die Wurzeltransaktion stellt in diesem Zusammenhang einen speziellen Knoten dar, der keinen Elternknoten aufweist. Sind für einen Knoten keine Kindknoten spezifiziert, so wird er als Blatt bezeichnet. Es handelt sich somit um eine allgemeine **Baumstruktur**[109] von Transaktionen im Sinne der Algorithmik bzw. Software-Technik, die durch Transaktionszerlegungen erzeugt wird.

Durch Objektzerlegungen entstehen zusätzliche Transaktionen, die unabhängig von dem Transaktionsbaum sind und nicht aus dessen Wurzeltransaktion hervorgehen. Sie werden im Folgenden als **originäre Transaktionen** bezeichnet, die im Lauf der Modellierung generiert werden. Originäre Transaktionen können ebenfalls weiter zerlegt werden, sie stellen somit potentielle Wurzeln eigener Transaktionsbäume dar.

Der durch die Transaktionszerlegung entstehende Baum sowie originäre Transaktionen und potentiell daraus entstehende Bäume bilden aus graphentheoretischer Sicht einen Wald [Mali97, 19]. Die Menge aller Blattknoten dieses Waldes zu einem bestimmten Zeitpunkt repräsentieren alle Transaktionen, die in der jeweiligen Zerlegungsstufe eines IAS enthalten sind[110]. Hinsichtlich der Modellierungsaktivitäten des IAS beschreiben die Kanten der Bäume dann den Typ der Zerlegungsregel, der angewandt wurde, um die Elterntransaktion zu verfeinern.

---

[109] Vgl. hierzu zum Beispiel [Balz99, 599].

[110] Ein spezielles Niveau der Baumstrukturen hingegen kann diesbezüglich nicht sinnvoll interpretiert werden, da es nicht zwangsläufig mit der entsprechenden Zerlegungsstufe des IAS korrespondiert.

Modellierungsheuristik

Grundsätzlich gilt, dass die Annotation neuer Schutzziele auf jeder Zerlegungsstufe des IAS möglich ist. Aus graphentheoretischer Sicht bedeutet dies, das ein Blattknoten des Transaktionsbaums zu jedem Zeitpunkt mit neuen Schutzzielen annotiert werden kann. Wird ein Blattknoten jedoch weiter differenziert, so ist zu definieren, welche Auswirkung dessen bereits annotierte Schutzziele auf die durch die Differenzierung entstehenden Kindknoten haben.

Einen Ansatz stellt in diesem Zusammenhang die Nutzung des **Vererbungsprinzips** dar. Demnach werden Schutzziele, die für eine Transaktion t annotiert sind, auf alle Kindtransaktionen von t übertragen. Dieses Verfahren ist jedoch nicht grundlegend anwendbar, wie anhand der Semantik von Schutzzielannotationen nachvollziehbar ist. So bedingt die Annotation von Vertraulichkeit an eine beispielhafte Durchführungstransaktion „Zahlung“ zwischen den fiktiven Objekten „Gast“ und „Hotel“ nicht zwangsläufig, dass eine durch Zerlegung entstehende Anbahnungstransaktion „Abreisewunsch“ ebenfalls vertraulich zu behandeln ist. Im Beispiel ist dies begründet durch das dieser Zerlegungsregel zu Grunde liegende nichthierarchische Koordinationsmuster nach dem Verhandlungsprinzip. Die hierbei modellierte Anbahnungs-, Vereinbarungs- und Durchführungsphase sind durch sequentielle Reihenfolgebeziehungen miteinander verknüpft und beziehen sich als Teiltransaktionen jeweils auf unterschiedliche Aspekte der Elterntransaktion. Es wird somit deutlich, dass allgemeingültige Vererbungskonzepte für vertikale Ableitungsbeziehungen von Schutzzielen im Rahmen des IAS nicht angegeben werden können.

In diesem Zusammenhang sind vielmehr ausschließlich **Modellierungsheuristiken** definierbar, die in der Regel jedoch in Abhängigkeit von der Schutzzielklasse und der gewählten Zerlegungsform separat zu spezifizieren sind. Allgemein jedoch gilt, das auf einer Modellierungsstufe i des IAS an Transaktionen annotierte Schutzziele auf nachgelagerten Stufen i+x ebenfalls vorhanden sein müssen, somit durch Zerlegung nicht aus dem Modell eliminiert werden dürfen. Wird eine annotierte Transaktion zerlegt, so muss das entsprechende Schutzziel an mindestens einer der resultierenden Kindtransaktionen als Instanz des gleichen Schutzzieltyps fortgeführt werden. Analog zu dem Konzept der SOM-Methodik, durch sukzessive Verfeinerung von Objekten und Transaktionen Lenkungs- und Leistungsbeziehungen aufzudecken, ist somit auch die Modellierung von Schutzzielen schrittweise zu überdenken und zu präzisieren. Die diesbezügliche Fertigkeit eines Modellierers kann nur durch die ange-

sprochenen Indikatoren zur Modellierungstechnik unterstützt, nicht aber durch konkrete Ableitungs- oder Vererbungsregeln ersetzt werden.

Modellierungstiefe

In ähnlicher Weise ist die Frage nach der geeigneten Modellierungstiefe des IAS zu beantworten, auf der eine Modellierung von Schutzzielen erfolgen kann. Bedingt durch die nicht vorhandenen inhaltlichen Ableitungsbeziehungen von Schutzzielen ist anzuraten, die Annotationen immer dann vorzunehmen, wenn im Hinblick auf die Anwendungsentwicklung anhand der entsprechenden Detailierungsstufe des IAS die Abgrenzung von Anwendungssystemen ersichtlich wird. Dies hat zum einen den Vorteil, dass durch mögliche Systemgrenzen einem Modellierer zumindest auf abstrakter Ebene verdeutlicht wird, dass entsprechend ein- bzw. ausgehende Transaktionen aus Sicherheitsaspekten potentiell gesondert zu behandeln sind. Zum anderen ist zu diesem Zeitpunkt in der Regel ein Grad der Verfeinerung erreicht, der auf Grund der bereits erfolgten Zerlegungsschritte eine ausreichende detaillierte Ansicht sicherheitsrelevanter Transaktionen bietet. In Bezug auf die Ableitung der Schutzziele im VES wird dieser Aspekt in den folgenden Abschnitten nochmals aufgegriffen.

8.4.3. Modellierungstechnik von Schutzzielen im VES

Zentrales Modellelement der Sicherheitsmodellierung im VES ist die betriebliche Aufgabe. Die Modellierung neuer Schutzziele erfolgt hierbei aus methodischer Sicht analog zur Modellierung im IAS. Sie werden als Eigenschaft einer im VES modellierten Aufgabe angegeben und in grafischer Form gemäß der definierten syntaktischen Notation in dem Modelldiagramm dem jeweiligen Element zugeordnet.

Neben diesen neuen Schutzzielen, die unabhängig vom IAS im VES modelliert werden, sind potentiell auch Schutzziele zu berücksichtigen, die aus dem IAS abgeleitet werden können. Der Verknüpfungsansatz liegt hierbei im Konzept der schutzzielannotierten Transaktionen des IAS, die bei der Ableitung des VES unter dem Aspekt der semantischen Uminterpretation als Ereignis zu übernehmen sind. Dieser Zusammenhang wird als **horizontale Ableitungsbeziehung von Schutzzielen** bezeichnet. Im Kontext der Sicherheitsmodellierung sind diese Transaktionsereignisse zu analysieren, indem eine explizite Betrachtung der an der Transaktion beteiligten Sende- und Empfangsaufgaben zu erfolgen hat. Die initial im IAS modellierten Schutzzieltypen Transaktionsvertraulichkeit und -verbindlichkeit stellen somit Indikatoren

dar, anhand derer mögliche sicherheitsrelevante Aspekte aus vorgangsorientierter Sicht abgeleitet werden können.

Wird zum Beispiel ein modelliertes Schutzziel Transaktionsvertraulichkeit in das VES übernommen, so ist durch den Modellierer abzuwägen, ob sich die Vertraulichkeitsanforderung nur auf die Transaktionsinhalte oder eben auch auf die Sende- und Empfangsaufgaben erstreckt. Ist Letzteres der Fall kann dem mit der Annotation der Sende- bzw. Empfangsvertraulichkeit Rechnung getragen werden. Analog hierzu ist die Transaktionsverbindlichkeit zu interpretieren, mit dem Unterschied, dass hier die Nichtabstreitbarkeit des Sendens bzw. des Empfangs als vorgangsorientierte Schutzziele modelliert werden können.

Durch die dargestellte Beziehung zwischen IAS und VES aus Sicht der Sicherheitsmodellierung in SOMsec, können die Schutzziele des IAS im VES präzisiert und im Sinne der generierten Modellinformation erweitert werden. Es bleibt jedoch festzuhalten, dass die horizontale Ableitungsbeziehung keine verbindliche Modellierungsvorschrift darstellt. Im Gegensatz zur vertikalen Ableitungsbeziehung wird dem Modellierer zwar ein methodischer Ansatz an die Hand gegeben, um die realweltlichen Sicherheitsaspekte möglichst umfassend und flexibel in Geschäftsprozessmodellen abzubilden, die letztliche Entscheidung, ob aus horizontalen Ableitungsbeziehungen resultierende Schutzziele aufzunehmen sind, obliegt jedoch alleine dessen Expertise.

8.4.4. Zusammenfassung

Die Ausführungen zur Integration von Schutzzielen in die Geschäftsprozessmodellierung machen deutlich, dass sowohl aus semantischen wie auch aus syntaktischen und methodischen Gesichtspunkten die Erstellung eines sicherheitserweiterten Geschäftsprozessmodells auf Grundlage von SOMsec realisierbar ist.

Auf Basis der theoretischen Fundierung aus Teil I und II der vorliegenden Arbeit kann die inhaltliche Einbindung der Schutzziele anhand der Beziehung zwischen Definitionsrahmen der Schutzziele und des Meta-Modells von SOM abgeleitet werden. Durch das in der Folge diesbezüglich erweiterte Meta-Modell von SOMsec, werden die identifizierten Zusammenhänge aus Modellierungssicht operationalisiert. Durch die identifizierten vertikalen und horizontalen Ableitungsbeziehungen von Schutzzielen sind sicherheitserweiterte Geschäftsprozessmodelle somit methodisch fundiert anhand von IAS und VES zu erstellen. Das VES bein-

haltet im Ergebnis, durch die Ableitung und Präzisierung der Schutzziele aus dem IAS sowie die zusätzliche Modellierung neuer Schutzziele, die höchste Modellierungstiefe in Bezug auf die Sicherheitsmodellierung. Aus Sicherheitsgesichtspunkten stellt es somit die Grundlage für die Ableitung des KOS und VOS bei der fachlichen Spezifikation von Anwendungssystemen dar.

8.5. Szenario: Schutzzielmodellierung

Ausgehend von dem skizzierten Szenario können die vorgestellten Schutzzieltypen in die Modelle des IAS und VES integriert werden. Die hierbei exemplarisch modellierten Schutzziele erheben keinen Anspruch auf Vollständigkeit im Sinne einer umfassenden Absicherung der dargestellten Geschäftsprozesse. Sie stellen vielmehr einen Querschnitt der erläuterten Konzepte von SOMsec dar und werden daher an entsprechend nachvollziehbaren Beispielen erläutert.

8.5.1. Modellierung im IAS

Den Ausgangspunkt der Sicherheitsmodellierung bildet das IAS der dritten Zerlegungsstufe. Durch die Modellcharakteristik des Szenarios bedingt, sind auf früheren Zerlegungsstufen keine Schutzziele in inhaltlich sinnvoller Weise zu annotieren, so dass eine Berücksichtigung der heuristischen vertikalen Ableitungsbeziehungen nicht notwendig ist.

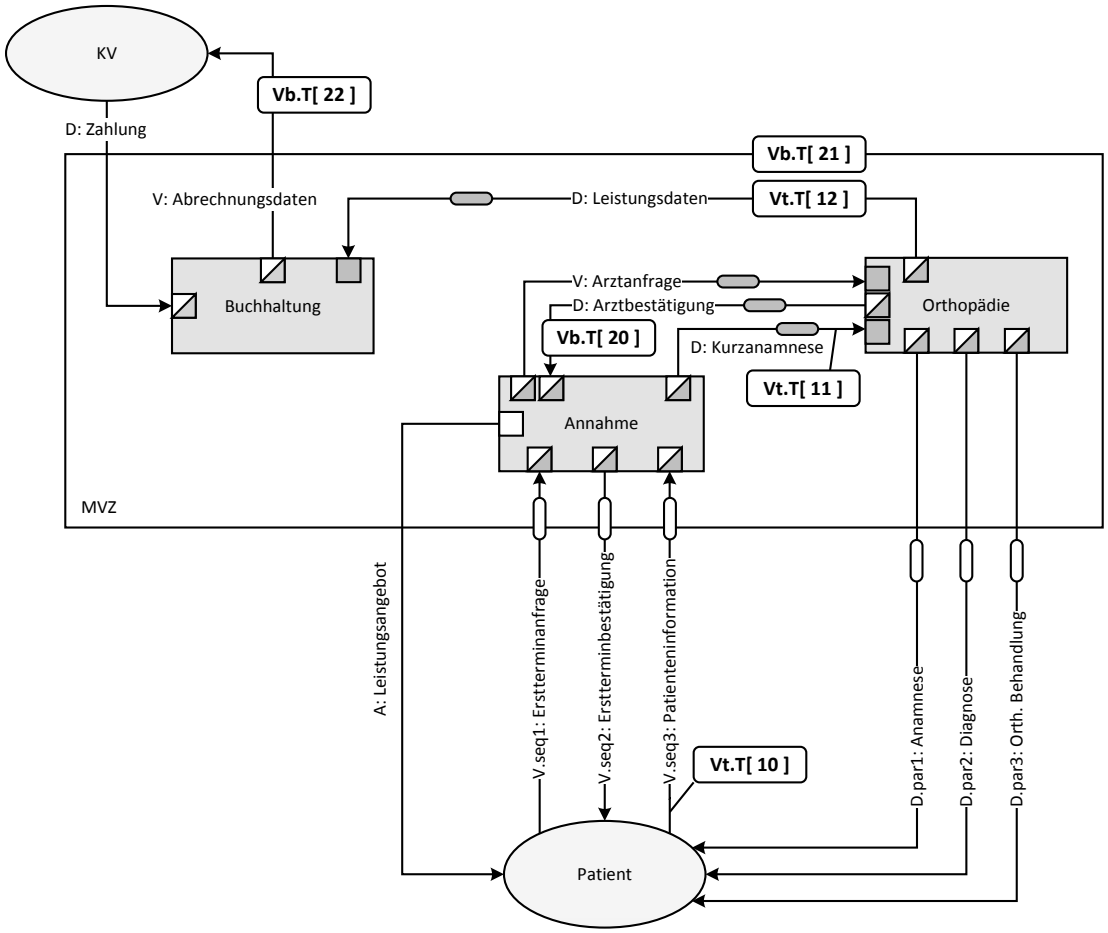

Abbildung 52: Szenario MVZ - sicherheitserweitertes IAS

Die modellierten Schutzziele sind in der Abbildung fett hervorgehoben. Aus Gründen der Übersichtlichkeit ist in der Darstellung als Bezeichner eine natürliche Zahl gewählt, die in der textuellen Notationsform durch zusätzlichen Text ergänzt werden kann[111]. Durch die Modellierung im IAS ergeben sich die nachfolgenden Schutzziele, die jeweils um eine natürlichsprachliche Beschreibung ergänzt wurden.

```
<Vt.T name="10 - Pat.Information">
    <sender> Patient </sender>
    <empfänger> Annahme </empfänger>
    <transaktion> V.seq3:Patienteninformation </transaktion>
    <beschreibung>
          Die Übermittlung der Patienteninformationen muss
          vertraulich erfolgen
    </beschreibung>
```

[111] Zur Verbesserung der Unterscheidung der beiden Schutzzielklassen beginnt der Index für Vertraulichkeit bei 10, der für Verbindlichkeit bei 20.

```
</Vt.T>

<Vt.T name="11 - Kurzanamnese">
    <sender> Annahme </sender>
    <empfänger> Orthopädie </empfänger>
    <transaktion> D:Kurzanamnese </transaktion>
    <beschreibung>
          Die Übermittlung der Kurzanamnese zwischen Annahme und
          Orthopädie muss vertraulich erfolgen
    </beschreibung>
</Vt.T>

<Vt.T name="12 - Leistungsdaten">
    <sender> Orthopädie </sender>
    <empfänger> Buchhaltung </empfänger>
    <transaktion> D:Leistungsdaten </transaktion>
    <beschreibung>
          Die Leistungsdaten müssen zur Buchhaltung vertraulich
          übertragen werden
    </beschreibung>
</Vt.T>

<Vb.T name="20 - Arztbestätigung">
    <sender> Orthopädie </sender>
    <empfänger> Annahme </empfänger>
    <transaktion> D:Arzbestätigung </transaktion>
    <beschreibung>
          Die Arztbestätigung durch die Orthopädie ist verbindlich
    </beschreibung>
</Vb.T>

<Vb.T name="21 - Leistungsdaten">
    <sender> Orthopädie </sender>
    <empfänger> Buchhaltung </empfänger>
    <transaktion> D:Leistungsdaten </transaktion>
    <beschreibung>
          Die Leistungsdaten zwischen Orthopädie und Buchhaltung sind
          verbindlich. Sowohl die Sendung als auch der Empfang der
          Leistungsdaten sind zu bestätigen
    </beschreibung>
</Vb.T>

<Vb.T name="22 - Abrechnung">
```

```
    <sender> Buchhaltung </sender>
    <empfänger> KV </empfänger>
    <transaktion> V:Abrechnungsdaten </transaktion>
    <beschreibung>
          Die Übermittlung der Abrechnungsdaten muss verbindlich sein,
          eine Eingangsbestätigung der KV ist erforderlich
    </beschreibung>
</Vb.T>
```

Quelltext 3: Szenario MVZ - Schutzzielspezifikation des IAS

Die modellierten Schutzziele sind prinzipiell unabhängig von der Entwicklung eines betrieblichen Anwendungssystems zu sehen. So wird zum Beispiel die geforderte Transaktionsvertraulichkeit `Vt.T [10 - Pat.Information]` in diesem Szenario auf Grund der Nicht-Automatisierbarkeit der zu Grunde liegenden Transaktion nicht in einem Anwendungssystem abgebildet, gleichwohl kann die Anforderung auf den ansonsten verwendeten Kommunikationskanal transferiert werden. Im Falle eines Telefonates ergäbe sich aus dieser Annotation auf technischer Ebene somit die Forderung nach der Abhörsicherheit der genutzten Leitung. Wäre in einer zukünftigen Ausbaustufe hingegen eine anwendungsgestützte Übermittlung der Information gefordert, zum Beispiel über eine Webschnittstelle, so hätte die modellierte Anforderung wiederum Relevanz für die Anwendungsentwicklung. Für Modellierer gilt aus diesem Grund, die Schutzzielannotationen für einen Prozess möglichst vollständig und unabhängig von potentiell bereits vorhandenen Designentscheidungen im Hinblick auf die Automatisierungsunterstützung des Prozesses durchzuführen. Zum einen, um dadurch eine umfassende und konsistente Sicht auf die Sicherheitsanforderungen des Geschäftsprozesses zu erstellen, zum anderen um spätere technische Entscheidungen bzw. deren Änderungen nicht vorwegzunehmen und so möglicherweise sicherheitsrelevante Interaktionen fälschlicherweise unberücksichtigt zu lassen.

8.5.2. Modellierung im VES

Aus dem IAS der dritten Zerlegungsstufe resultiert das in Abbildung 39 dargestellte VES. Als zweiter Schritt der Sicherheitsmodellierung in SOMsec werden die im IAS annotierten Schutzziele in dieses Modellschema übernommen und im Anschluss um weitere aufgabenbezogene Schutzziele ergänzt. Es ergibt sich das folgende Modellschema.

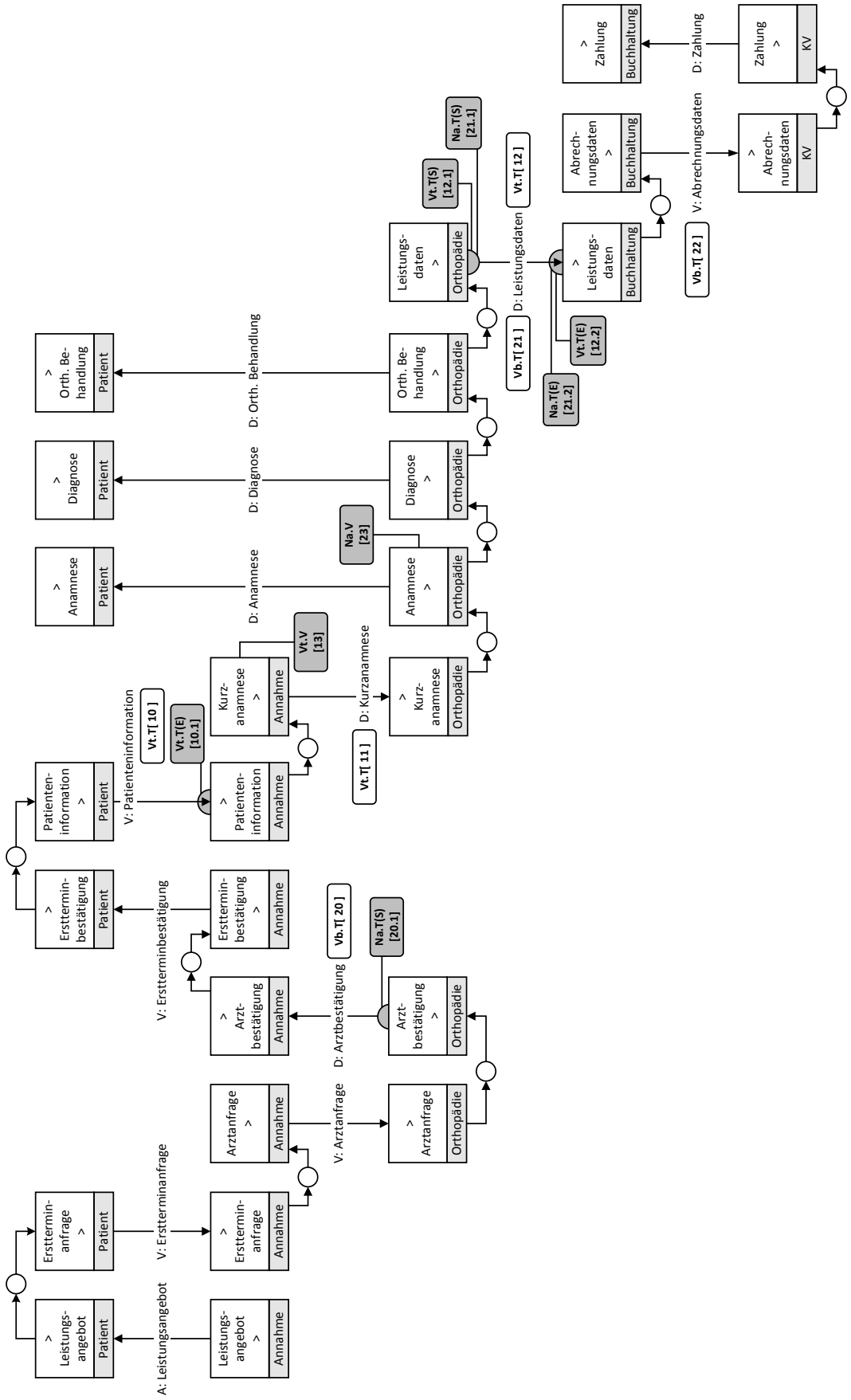

Abbildung 53: Szenario MVZ - sicherheitserweitertes VES

Die Übertragung der im IAS annotierten Schutzziele ins VES, in der Darstellung weiß hinterlegt, bildet die Basis für die Analyse möglicher horizontaler Ableitungsbeziehungen hinsichtlich der Schutzzieltypen Transaktionsvertraulichkeit und Transaktionsverbindlichkeit. Die neu abgeleiteten Schutzziele werden dabei im Bezeichner durch einen Unterpunkt des Index des Ausgangsschutzziels gekennzeichnet. Für neu modellierte vorgangsorientierte Schutzziele wird der Index des Bezeichners um eins erhöht. Durch diesen zweiten Schritt entstehen die folgenden vorgangsorientierten Schutzzielspezifikationen.

```
<Vt.T(E) name="10.1 - Empfang Patienteninformation">
    <objekt> Annahme </objekt>
    <aufgabe> >Patienteninformation </aufgabe>
    <beschreibung>
          Die Annahme der Patienteninformation ist nur durch Befugte
          durchzuführen
    </beschreibung>
</Vt.T(E)>

<Vt.T(S) name="12.1 - Versand Leistungsdaten">
    <objekt> Orthopädie </objekt>
    <aufgabe> Leistungsdaten> </aufgabe>
    <beschreibung>
          Der Versand der erstellten Leistungsdaten ist nur durch
          Befugte durchzuführen
    </beschreibung>
</Vt.T(S)>

<Vt.T(E) name="12.2 - Empfang Leistungsdaten">
    <objekt> Buchhaltung </objekt>
    <aufgabe> >Leistungsdaten </aufgabe>
    <beschreibung>
          Der Empfang der Leistungsdaten in der Buchhaltung darf nur
          durch Befugte erfolgen
    </beschreibung>
</Vt.T(E)>

<Vt.V name="13 - Erstellung Kurzanamnese">
    <objekt> Annahme </objekt>
    <aufgabe> Kurzanamnese> </aufgabe>
```

```
<beschreibung>
          Die Erstellung der Kurzanamnese darf nur durch befugte
          Mitarbeiter erfolgen
    </beschreibung>
</Vt.V>

<Na.T(S) name="20.1 - Sendung Arztbestätigung">
    <objekt> Orthopädie </objekt>
    <aufgabe> Arztbestätigung> </aufgabe>
    <beschreibung>
          Der Versand der Arztbestätigung muss belegbar sein
    </beschreibung>
</Na.T(S)>
<Na.V name="23 - Anamnese">
    <objekt> Orthopädie </objekt>
    <aufgabe> Anamnese> </aufgabe>
    <beschreibung>
          Die Erstellung der Anamnese darf nicht abstreitbar sein
    </beschreibung>
</Na.V>

<Na.T(S) name="21.1 - Sendung Leistungsdaten">
    <objekt> Orthopädie </objekt>
    <aufgabe> Leistungsdaten> </aufgabe>
    <beschreibung>
          Das Versenden der Leistungsdaten durch die Orthopädie muss
          belegbar sein
    </beschreibung>
</Na.T(S)>

<Na.T(E) name="21.2 - Empfang Leistungsdaten">
    <objekt> Buchhaltung </objekt>
    <aufgabe> >Leistungsdaten </aufgabe>
    <beschreibung>
          Der Empfang der Leistungsdaten durch die Buchhaltung muss
          belegbar sein
    </beschreibung>
</Na.T(E)>
```

Quelltext 4: Szenario MVZ - Schutzzielspezifikation des VES

Eine exemplarische Darstellung einer horizontalen Ableitungsbeziehung kann anhand des Schutzziels `Vb.T[20 - Arztbestätigung]` erfolgen. Im IAS wurde durch dieses spezifiziert, dass die Bestätigung der Arztverfügbarkeit zu dem vorgeschlagenen Termin verbindlichen Charakter besitzen muss. Im Hinblick auf die spätere technische Implementierung könnte diese Anforderung zum Beispiel durch die Nutzung von digitalen Signaturen umgesetzt werden. Die Betrachtung der anteiligen Sendeaufgabe im VES führt zu dem Ergebnis, dass auch diese im Hinblick auf den Schutzzieltyp Verbindlichkeit relevant ist, da dieser Teilvorgang, bedingt durch zusätzliche Anforderungen, im Nachhinein belegbar sein soll. Ein denkbares Szenario ist hier zum Beispiel die Forderung nach einer bestimmten Reaktionszeit für die Antwort auf eine Arztanfrage, die, wiederum aus technischer Sicht betrachtet, durch eine explizite Protokollierung des Sendevorgangs belegbar ist. In diesem Zusammenhang entspricht die modellierte Nichtabstreitbarkeit des Sendens `Na.T(S)[20.1 - Sendung Arztbestätigung]` den geforderten Charakteristika der Transaktion.

Wie das Beispiel belegt, wird die Modellierung der Sicherheitsaspekte auf Geschäftsprozessebene nicht ausschließlich von Risiken oder externen Gefahren durch Angreifer getrieben, sondern kann auch durch interne Ansprüche an die spätere Ausgestaltung des Prozesses beeinflusst werden. Hier obliegt es dem Modellierer, die entsprechenden informalen Anforderungen zu interpretieren und unter dem Blickwinkel der Informationssicherheit in geeignete Schutzziele zu transferieren.

Durch die vorgestellte Modellierung der vorgangsorientierten Schutzziele im VES wird die Sicherheitsanalyse des Geschäftsprozesses im Hinblick auf die initiale Zuweisung der Schutzziele vervollständigt. Die letzte Aktion dieses ersten Schrittes des Vorgehensmodells von SOMsec bezieht sich nun auf die Anreicherung bzw. Präzisierung der generierten Modellinformation, um zusätzliche sicherheitsrelevante Aspekte durch den Modellierer zu ergänzen.

8.6. Identitätsorientierte Erweiterung der Schutzzielmodellierung

Die Erweiterung der Modellinformation in SOMsec bezieht sich auf die Ausgestaltung von Eigenschaften von Schutzzielen, die sich nicht aus der eigentlichen Ableitung aus den Modellschemata ergeben.

Einen Ansatzpunkt für die inhaltliche Erweiterung des vorgestellten Modellierungsansatzes stellt die Differenzierung der modellierten Schutzziele anhand des Kriteriums der **Identitätsabhängigkeit** dar. Eine Identität beschreibt dabei eine Entität, im Sinne einer realweltlichen Person oder eines Anwendungssystems, eindeutig anhand der Menge ihrer charakterisierenden Attribute [Hühn08, 163]. Identitätsabhängigkeit besagt dann, dass die Spezifikation eines Schutzziels durch die Angabe von Identitäten aus inhaltlicher Sicht präzisiert werden und somit die Qualität der Modellinformation gesteigert werden kann. Im Rahmen der Schutzzielklassifikation von SOMsec ist die Verbindlichkeit als identitätsunabhängig zu charakterisieren, wohingegen der Schutzzieltyp Vertraulichkeit als identitätsabhängig zu interpretieren ist. Im Kontext der Geschäftsprozessmodellierung entspricht dieser Aspekt dann der Abgrenzung von befugten und unbefugten Entitäten, die zur Durchführung einer Aufgabe berechtigt sind. Die fachliche Eingliederung dieser Aspekte in den betrieblichen Kontext sowie die Berücksichtigung in SOMsec wird in den folgenden Abschnitten beschrieben.

8.6.1. Identitätsmanagement

Die Sicherheitsrelevanz von Identitätsinformationen im betrieblichen Kontext basiert im Wesentlichen auf der Erkenntnis, dass durch die hohe Anzahl von zu verwaltenden Identitäten in Unternehmen Fehlkonfigurationen entstehen und zu ungewollten Berechtigungsstrukturen führen können. Dieser Aspekt wird in der Literatur auch als „Identity Chaos“ bezeichnet. Als Gegenmaßnahme hat sich die Lenkungsaufgabe des **Identitätsmanagements** (engl. *Identity Management*, IdM) etabliert, die sich mit der Speicherung, Verwaltung und Nutzung der betrieblichen Identitäten befasst [FuPe07, 375]. Der Bezugsrahmen des IdM bezieht sich dabei sowohl auf technische als auch auf organisatorische Aspekte der Identitätsverwaltung. Sein Ziel besteht in der Verknüpfung der beiden Ebenen im Hinblick auf eine konsistente Abbildung organisationsorientierter Identitätsinformationen auf technische Berechtigungskonzepte von Anwendungssystemen [FuPr08, 128f].

Die Methoden und Prozesse des IdM orientieren sich dabei an den beiden angesprochenen Betrachtungsebenen. Insbesondere die Spezifikation von Berechtigungen im Umgang mit betrieblichen Anwendungssystemen stellt für Nutzer das wohl erkennbarste Resultat des IdM

dar. Diese Strukturen sind zudem im Kontext gesetzlicher Regelungen[112] zu verifizieren und den jeweiligen Anforderungen anzupassen [Kla+08, 2].

8.6.2. Identitätsinformationen in Geschäftsprozessmodellen

Die Berücksichtigung von Berechtigungskonzepten auf Anwendungssystemebene gilt als akzeptiertes Verfahren des IdM und wird in Literatur sowie Praxis anhand unterschiedlicher Strategien diskutiert und durchgeführt[113]. In Bezug auf die organisatorische Betrachtungsebene des IdM ist jedoch keine einheitliche Vorgehensweise erkennbar. Einen Ansatz bildet in diesem Zusammenhang die Integration von Identitätsanforderungen in die Geschäftsprozessmodellierung, sodass eine möglichst enge Verzahnung zur Disziplin des IdM gegeben ist und eine entsprechend dynamische Verwaltung der Berechtigungsstrukturen ermöglicht wird [Kla+08, 3].

Ein Schlüsselkonzept stellt in diesem Zusammenhang das Konstrukt der **Rolle** dar, die auf Geschäftsprozessebene als Träger von Berechtigungen zu berücksichtigen ist. Motiviert ist dieses Vorgehen vornehmlich durch die auf technischer Ebene bereits etablierten rollenbasierten Zugriffskontrollstrategien, wie zum Beispiel RBAC. Eine eindeutige Abbildung dieses Rollenverständnisses ist jedoch nicht immer möglich oder sinnvoll, da die zu Grunde liegenden Begriffsverständnisse sich ebenenabhängig unterscheiden. Ist auf technischer Ebene vornehmlich eine berechtigungsorientierte Interpretation der Rolle gegeben, so ist auf Geschäftsprozessebene vielmehr ein aufgaben- bzw. organisationsorientiertes Verständnis vorherrschend [Kla+09b, 136]. Das Konzept einer direkten Integration von Rollen auf Basis der etablierten technischen Interpretation in die Geschäftsprozessmodellierung ist somit methodisch fundiert nicht realisierbar und bedarf der Erweiterung. Aktuelle Ansätze adressieren diesen Aspekt vornehmlich durch die explizite Unterscheidung von verschiedenen Rollentypen auf Basis unterschiedlicher Perspektiven auf Geschäftsprozesse und Anwendungssysteme. Gleichwohl erfolgt die Betrachtung auf technischer Ebene stets auf der Grundlage einer rollenbasierten Zugriffskontrollstrategie[114].

Im Rahmen der geschäftsprozessgetriebenen Anwendungsentwicklung ist ein solcher Ansatz durch die Aufnahme von **Identitätsinformationen** in die Schutzzielmodellierung von SOM-

[112] Vgl. hierzu Kapitel 5.4.2.1.

[113] Vgl. hierzu Kapitel 5.5.3.

[114] Aktuelle Ansätze auf Basis von RBAC werden unter anderem in [Kla+09a] sowie [FuPr08] beschrieben.

sec realisierbar. Den Ansatzpunkt für die Integration bilden hierbei die modellierbaren Schutzzieltypen der Transaktions- und Vorgangsvertraulichkeit sowie der Sende- und Empfangsvertraulichkeit, die um eine entsprechende Spezifikation zu erweitern sind. Da SOMsec jedoch als möglichst unabhängiges Rahmenwerk konzipiert ist, erfolgt bei der Berücksichtigung der Identitätsinformationen keine Festlegung auf bestimmte technische Umsetzungen. Die folgenden Abschnitte erläutern das zu Grunde liegende Konzept im Detail.

8.6.3. Modellierung von Identitätsinformationen in SOMsec

Die Berücksichtigung von Identitätsinformationen zur Erweiterung der Vertraulichkeitsmodellierung orientiert sich an dem in SOMsec genutzten Architekturrahmen.

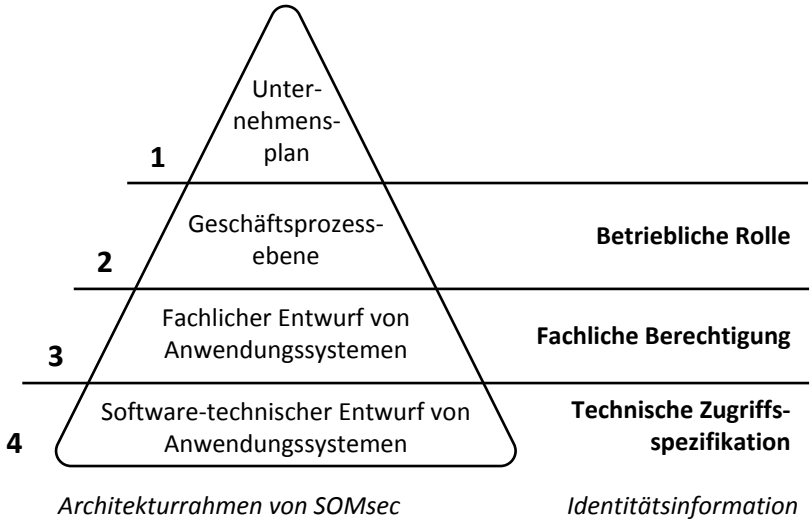

Abbildung 54: Struktur der Identitätsinformationen in SOMsec

Auf Geschäftsprozessebene bildet das Konzept der **betrieblichen Rolle** die Grundlage für die Spezifikation von Identitätsinformationen. Auf der Ebene der fachlichen Anwendungsspezifikation werden diese Rollen in **fachliche Berechtigungen** überführt, die sich auf die Zugriffskontrollstrukturen in dem zu entwickelndem Anwendungssystem beziehen. Die technische Umsetzung dieser Strukturen erfolgt schließlich in Form einer **technischen Zugriffsspezifikation**, die durch entsprechende Basismaschinen zur Zugriffskontrolle interpretier- und umsetzbar ist.

Durch diesen Ansatz entsteht im Rahmen der geschäftsprozessgetriebenen Anwendungsentwicklung eine ebenenspezifische Betrachtungsweise der Identitätsinformationen sowie eine

diesbezüglich resultierende Entkopplung zwischen der Aufgaben- und Aufgabenträgerebene. Der Vorteil dieser Vorgehens besteht darin, dass domänenspezifische Perspektiven auf die Identitätsinformationen erhalten bleiben. Ein Geschäftsprozessmodellierer kann somit die Rollen aus Sicht der Fachabteilungen betrachten wohingegen im Rahmen der Anwendungsspezifikation bereits Berechtigungsstrukturen im Sinne der technischen Implementierung spezifiziert werden können. Die verbindenden Elemente zwischen den Ebenen stellen die Konzepte der betrieblichen Aufgabe sowie der Transaktion dar, die auf beiden Ebenen der Modellierungsmethodik genutzt werden.

Im folgenden Abschnitt wird die Modellierung der betrieblichen Rollen in SOMsec erläutert sowie im Anschluss die praktische Erweiterung des vorgestellten Szenarios MVZ. Die Beschreibung der fachlichen Berechtigungen und technischen Zugriffspezifikation erfolgt im weiteren Verlauf in Kapitel 9.3.1.3 sowie in Kapitel 10.4.4.

8.6.4. Betriebliche Rollen in der Geschäftsprozessmodellierung

Auf Geschäftsprozessebene wird in SOMsec das Konzept der Rolle auf Grund seiner semantischen Nähe zu betrieblichen Strukturen und Organisationsformen genutzt. Unter einer betrieblichen Rolle wird dabei eine Menge von Berechtigungen verstanden, die einer Identität in dieser Rolle zugestanden werden. Die Berechtigungen beziehen sich dabei auf die Ausführung von Aufgaben und Transaktionen, die im Rahmen von IAS und VES modelliert werden. In SOMsec erfolgt hierbei keine Vorgabe, in welcher Weise das Rollenkonzept semantisch zu interpretieren ist. Rollen können durch den Modellierer beliebig genutzt werden, zum Beispiel in Form von aufgabenorientierten, kompetenzorientierten oder auch organisationsorientierten Rollenkonzepten[115].

Modellierung betrieblicher Rollen

Aus Modellierungssicht wird eine betriebliche Rolle in SOMsec als Attribut eines Schutzziels der Klasse Vertraulichkeit modelliert. Eine Rolle besteht dabei aus einer eindeutigen Bezeichnung sowie einer optionalen Beschreibung. Die Bezugsobjekte der Rolle ergeben sich indirekt durch die entsprechenden Referenzen des zu Grunde liegenden Schutzziels. Die Angabe einer Rolle entspricht dabei einer entsprechenden Befugnis zur Durchführung einer Aufgabe bzw. Transaktion, für die das Schutzziel annotiert ist. Die Modellierung von Rollen in

[115] Eine mögliche Klassifikation von Rollen in Unternehmen wird in [SüGi03] vorgestellt.

SOMsec folgt somit dem Konzept der Positivliste, sodass nur modellierte Rollen entsprechende Berechtigungen zur jeweiligen Durchführung besitzen. Dies entspricht der eingangs angesprochenen Abgrenzung von Befugten und Unbefugten hinsichtlich der Erweiterung der Vertraulichkeitsmodellierung.

Betriebliche Rollen werden in SOMsec als logische Container verstanden, denen im weiteren Verlauf der Modellierung entsprechende Identitäten zugeordnet werden können. Auf Geschäftsprozessebene erfolgt dies jedoch nicht, da Identitäten als Repräsentation von Nutzern eines Anwendungssystems konzeptuell der Aufgabenträgerebene zugewiesen sind. Eine betriebliche Rolle symbolisiert somit eine Referenz auf die Aufgabenträgerebene, um im Sinne der Informationssicherheit entsprechende Vertraulichkeitsziele zu präzisieren. Im Kontext der Sicherheitsmodellierung ist die Ausgestaltung dieser Beziehung von großem Vorteil, da hierdurch bereits auf Aufgabenebene entsprechendes sicherheitsrelevantes Wissen des Modellierers in die Modellierung einfließen kann.

Relevante Modellelemente

Die identitätsabhängig erweiterbaren Schutzziele wurden im bisherigen Verlauf als Vertraulichkeitsziele beschrieben. Dies ist dahingehend einzugrenzen, dass nur aufgabenbezogene Vertraulichkeitsziele für eine Erweiterung in Frage kommen. Der Grund hierfür liegt in den Anforderungen zur Abgrenzung der Gruppen von Befugten und Unbefugten. In Bezug auf transaktionsbezogene Vertraulichkeitsziele wird eine Befugnis implizit durch die Angabe von Befugten auf Sende- und Empfangsseite spezifiziert. Eine Transaktion selbst kann dabei keine zusätzlichen separaten Befugnisse besitzen. Für die Einsicht in eine Transaktion ist im Sinne der Vertraulichkeit somit grundsätzlich jede Entität unbefugt, mit Ausnahme der entsprechend erteilten Befugnisse im Sinne betrieblicher Rollen der Sende- und Empfangsaufgaben. Die Spezifikation betrieblicher Rollen erfolgt somit ausschließlich für die aufgabenorientierten Vertraulichkeitsziele der Sende-, Empfangs- und Vorgangsvertraulichkeit.

Strukturierung von Rollen

Aus methodischer Sicht werden Rollen in SOMsec als flache Liste dargestellt. Um die Strukturierung zu vereinfachen, können Rollen den betrieblichen Objekten zugeordnet werden, für deren Aufgaben die entsprechenden Schutzziele spezifiziert wurden. Diese Zuordnung orientiert sich am Konzept der Namensräume, sodass ein Modellierer auch gleiche Bezeichnungen für Rollen von unterschiedlichen betrieblichen Objekten vergeben kann. Durch diesen Struk-

turierungsmechanismus ergibt sich für Modellierer auch ein zusätzlicher Vorteil, indem das Verständnis der Rollenspezifikation in die grundlegende Metapher der betrieblichen Objekte auf Geschäftsprozessebene integriert wird.

Weiterführende Konzepte der Rollenmodellierung, wie zum Beispiel die Modellierung von Aufgabentrennung oder der Hierarchisierung und Vererbung von betrieblichen Rollen werden im Rahmen der Arbeit nicht betrachtet.

8.6.5. Identitätsinformationen im Szenario MVZ

Im Hinblick auf die Geschäftsprozessmodellierung werden Identitäten als Attribut eines Schutzziels aufgefasst, jedoch nicht explizit in die graphische Modellierung integriert. Vielmehr können sie in einem abschließenden Schritt der Schutzzielspezifikation zur Präzisierung der Modellinformation in die textuelle Darstellung der annotierten Schutzziele integriert werden. Den Ausgangspunkt hierfür bildet die Analyse des sicherheitserweiterten VES in Bezug auf modellierte Vertraulichkeitsziele. Für jedes identitätsabhängige Schutzziel ist dabei die Notwendigkeit zur Angabe einer oder mehrerer betrieblicher Rollen zu prüfen. In syntaktischer Form erfolgt die Erweiterung der Modellinformation dann durch die Angabe eines zusätzlichen XML-Subelements `rolle`, das in der XML-Spezifikation der Vertraulichkeitsziele ergänzt werden kann.

Im Szenario MVZ werden hinsichtlich der modellierten Vertraulichkeitsanforderungen im Rahmen der definierten Anwendungsabgrenzung die folgenden relevanten Sicherheitsziele und Rollen identifiziert.

Für den Empfang der Patienteninformationen ist ein Rolle „Rezeptionist“ vorzusehen, die die Befugnis hat die Stammdaten von Patienten zu erfassen und im System einzupflegen (`Vt.T(E)[10.1]`). Die Erstellung der Kurzanamnese ist auf Grund der medizinischen Relevanz jedoch nur medizinischen Fachangestellten in der Rolle „Arzthelfer“ erlaubt (`Vt.V[13]`). Im Bereich Orthopädie darf der Versand der Leistungsdaten nur leitenden Angestellten in der Rolle „Chefarzt“ möglich sein (`Vt.T(S)[12.1]`).

Die aufgeführten Rollen sind gemäß ihrer Zugehörigkeit zu Aufgaben dem Namensraum der entsprechenden betrieblichen Objekte zuzuordnen. Es ergibt sich die folgende erweiterte Spezifikation der Schutzziele.

```
<Vt.T(E) name="10.1 - Empfang Patienteninformation">
    <objekt> Annahme </objekt>
    <aufgabe> >Patienteninformation </aufgabe>
    <rolle> Annahme.Rezeptionist </rolle>
</Vt.T>

<Vt.V name="13 - Erstellung Kurzanamnese">
    <objekt> Annahme </objekt>
    <aufgabe> Kurzanamnese> </aufgabe>
    <rolle> Annahme.Arzthelfer </rolle>
</Vt.T>

<Vt.T(S) name="12.1 - Versand Leistungsdaten">
    <objekt> Orthopädie </objekt>
    <aufgabe> Leistungsdaten> </aufgabe>
    <rolle> Orthopädie.Chefarzt </rolle>
</Vt.T>
```

Quelltext 5: Notation von Identitätsinformationen

Die identitätsbezogene Erweiterung der Schutzzielspezifikation vervollständigt das sicherheitserweiterte Geschäftsprozessmodell gemäß der Methodik von SOMsec. Dieses dient im nächsten Schritt der fachlichen Anwendungssystemspezifikation als Grundlage für die inhaltliche Ableitung und Parametrisierung der Sicherheitsgrundfunktionen.

9. Fachliche Sicherheitsspezifikation

Das Konzept der Automatisierung von Aufgaben und Transaktionen erlaubt in der SOM-Methodik, die Beziehung zwischen Geschäftsprozessmodell und Anwendungssystem herzustellen. Auf dieser Basis ist eine fachliche Spezifikation des Anwendungssystems zur Automatisierung der Geschäftsprozesse in Form des KOS und VOS ableitbar. Im Rahmen der Sicherheitsmodellierung von SOMsec ist dieser Ansatz um die Überführung der modellierten Schutzziele auf Geschäftsprozessebene in die fachliche Spezifikation des Anwendungssystems zu erweitern. Dies erfolgt gemäß den Ausführungen des Referenzmodells durch die Transformation von Schutzzielen in Sicherheitsgrundfunktionen sowie deren Integration in die Modellschemata der fachlichen Anwendungsmodellierung.

Kapitel 9.1 erläutert hierzu die Grundlagen, indem es allgemeine Sicherheitsaspekte im Rahmen der Systementwicklung beleuchtet. Analog zu Kapitel 8 werden im Anschluss die Fragestellungen der semantischen, syntaktischen und methodischen Integration von Sicherheitsanforderungen in die fachliche Anwendungsspezifikation in den Kapiteln 9.2, 9.3 und 9.4 beschrieben. Kapitel 9.5 stellt abschließend die exemplarische Erstellung einer fachlichen Sicherheitsspezifikation anhand des Szenarios MVZ vor.

9.1. Sicherheit in der Systementwicklung

Die Entwicklung betrieblicher Anwendungssysteme, kurz **Systementwicklung**, hat zum Ziel, den Lösungsverfahren der zu automatisierenden Aufgaben eines betrieblichen Informationssystems geeignete Basismaschinen zur Verfügung zu stellen. Diese agieren selbst wiederum als Nutzermaschinen, die unter Verwendung entsprechenden technischer Basismaschinen, wie zum Beispiel Hardware- oder Softwarekomponenten, realisiert und betrieben werden. Anwendungssysteme stellen somit maschinelle Aufgabenträger für (teil-)automatisierte Teilaufgaben eines betrieblichen Informationssystems dar [FeSi08, 457ff].

9.1.1. Sicherheitsaspekte der Systementwicklungsaufgabe

Die Systementwicklung durchläuft von der Spezifikation der zu automatisierenden Aufgaben bis hin zur Implementierung des Anwendungssystems verschiedene Beschreibungsebenen, die durch entsprechende Modelle bzw. Spezifikationen auszugestalten sind. Interpretiert man

dieses Vorgehen unter dem Blickwinkel des Konzepts der betrieblichen Aufgabe, so besteht das Lösungsverfahren der resultierenden Systementwicklungsaufgabe in der sukzessiven Ausgestaltung der Übergänge zwischen diesen Beschreibungsebenen [FeSi08, 476]. Die folgende Abbildung stellt dies im Überblick dar.

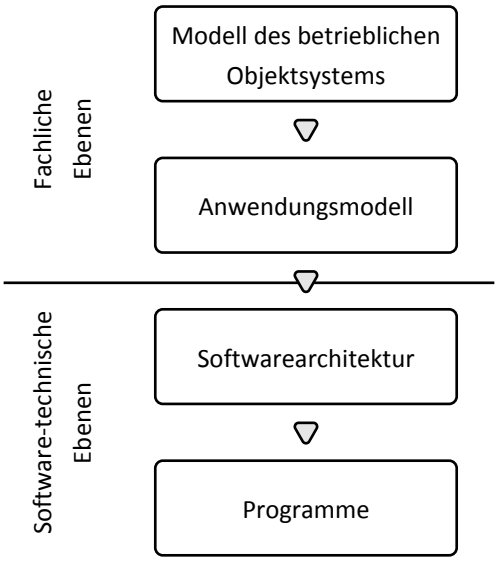

Abbildung 55: Ebenen der Systementwicklung (nach [FeSi08, 460])

Hinsichtlich des Architekturrahmens von SOMsec[116] korrespondiert das Modell des betrieblichen Objektsystems mit der Modellklasse des sicherheitserweiterten Geschäftsprozessmodells. Das Anwendungsmodell entspricht dann der fachlichen Spezifikation eines Anwendungssystems unter Berücksichtigung von sicherheitsrelevanten Anforderungen, die sich aus den modellierten Schutzzielen des Geschäftsprozessmodells ergeben. In Bezug auf das Referenzmodell betrieblicher Informationssicherheit entspricht dies dem sicherheitszielorientierten Übergang von der Geschäftsprozess- auf die Ressourcenebene[117].

Der zentrale Aspekt der Betrachtung bezieht sich in diesem Zusammenhang auf die Einordnung und Modellierbarkeit von Sicherheitsanforderungen hinsichtlich der fachlichen Ebene der Systementwicklungsaufgabe. Dabei wird das Lösungsverfahren der Aufgabe nicht phasenorientiert im Sinne eines Vorgehensmodells interpretiert, sodass die vorzunehmende Analyse der Sicherheitsaspekte dieses Kapitels sich ausschließlich auf die Einordnung und Systematisierung von Sicherheitsanforderungen in das Anwendungsmodell bezieht. Eine Integra-

[116] Vgl. hierzu Kapitel 7.2.3.

[117] Vgl. hierzu Abbildung 26 in Kapitel 6.1.

tion des Ansatzes vor dem Hintergrund spezifischer Vorgehensmodelle der Softwareentwicklung erfolgt im Rahmen der vorliegenden Arbeit hingegen nicht.

9.1.2. Sicherheitsanforderungen im Anwendungsmodell

Das Sachziel der Systementwicklungsaufgabe besteht aus der Entwicklung eines betrieblichen Anwendungssystems, das vorgegebene Anforderungen erfüllt [FeSi08, 475]. Im Kontext von SOMsec sind diese Anforderungen um sicherheitsrelevante Aspekte zu ergänzen, die sich auf das zu entwickelnde Anwendungssystem beziehen. In der Softwareentwicklung werden in diesem Zusammenhang **funktionale** und **nicht-funktionale Anforderungen** unterschieden. Da diese Unterscheidung nicht einheitlich definiert ist, dient als Grundlage für die vorliegende Arbeit eine Differenzierung, wie sie im Rahmen des V-Modells XT getroffen wird.

Anforderungstypen

Unter funktionalen Anforderungen werden die Fähigkeiten eines Anwendungssystems verstanden, die ein Anwender erwartet, um mit dessen Hilfe ein fachliches Problem zu lösen. Die entsprechenden Anforderungen werden dabei aus den zu unterstützenden Geschäftsprozessen sowie den Ablaufbeschreibungen des Systems abgeleitet [KBSt09, 5-97]. Nicht-funktionale Anforderungen auf der anderen Seite sind Eigenschaften eines Systems, die nicht fachlicher Natur sind, jedoch entscheidend zur Anwendbarkeit eines Anwendungssystems beitragen. Demzufolge sind auch nicht-funktionale Anforderungen im Verlauf der Anwendungsentwicklung zu berücksichtigen, die sich zum Beispiel auf Qualitäts- oder Performanceanforderungen beziehen [KBSt09, 5-98].

Nicht-funktionale Anforderungen

Im Gegensatz zu funktionalen Anforderungen, deren Definition in der Literatur vergleichsweise einheitlich erfolgt, werden nicht-funktionale Anforderungen stark unterschiedlich interpretiert und damit auch klassifiziert [Glin07]. Sicherheitsaspekte werden in diesem Zusammenhang in der Regel als nicht-funktionale Anforderungen geführt und je nach Vorgehensmodell unterschiedlich gewichtet und berücksichtigt [DeSt00, 228][118].

[118] Vgl. hierzu Kapitel 7.2.5.

Fachliche Sicherheitsanforderungen in SOMsec

In SOMsec werden die Sicherheitsanforderungen an ein zu entwickelndes Anwendungssystem ebenfalls als nicht-funktionale Anforderungen interpretiert. Im Rahmen des fachlichen Modells des Anwendungssystems werden durch die Entwicklung von KOS und VOS jedoch ausschließlich die funktionalen Anforderungen an das Anwendungssystem spezifiziert. Nicht-funktionale Anforderungen werden hierbei nicht berücksichtigt, da diese im Verlauf der geschäftsprozessgetriebenen Anwendungsentwicklung des SOM-Ansatzes in Geschäftsprozessmodellen nicht explizit, zum Beispiel in Form von Zieldefinitionen, modelliert werden.

Durch den Ansatz von SOMsec erfolgt auf Geschäftsprozessebene jedoch eine explizite Modellierung von Schutzzielen in Form von Eigenschaften von Modellelementen. Diese Eigenschaften spezifizieren in Summe einen sicherheitsrelevanten Soll-Zustand, den ein Geschäftsprozess, bzw. dessen Ausführung, aus Sicherheitsgesichtspunkten aufzuweisen hat. Die modellierten Schutzziele beinhalten somit Anforderungscharakter, der demzufolge auch auf die Ebene des Anwendungsmodells zu transferieren ist. Die resultierenden nicht-funktionalen Sicherheitsanforderungen sind in SOMsec somit initial aus dem Geschäftsprozessmodell abzuleiten und in die fachliche Spezifikation des Anwendungsmodells zu integrieren.

9.1.3. Zielmodellschema der Sicherheitsmodellierung

Das Anwendungsmodell wird in SOM durch die Modellschemata des KOS und VOS gebildet. Für die Berücksichtigung der Sicherheitsanforderungen ist in diesem Zusammenhang festzulegen, welches Modellschema als Zielsystem für die sicherheitserweiterte Sicht auf die fachliche Spezifikation eines Anwendungssystems fungiert. In SOMsec stellt das VOS dieses Modellschema dar, das dann im Hinblick auf die fachlichen Sicherheitsanforderungen die gleiche Stellung einnimmt, wie das sicherheitserweiterte VES auf Ebene der Geschäftsprozessmodellierung. Der Grund hierfür liegt in der aus Sicherheitsgesichtspunkten erweiterten Modellsemantik des VOS gegenüber dem KOS, die ein besseres Verständnis der fachlichen Vorgänge des Anwendungssystems zulässt. Zum Beispiel wird aus der isolierten Betrachtung eines transaktionsorientierten Objekttypen des KOS nicht ersichtlich, in welchen Anwendungsteilen oder bei welchen Operationen er Verwendung findet. Es ist nicht festzustellen, ob er nur während einer Transaktion oder auch im Rahmen weiterer Verarbeitungsaufgaben genutzt wird. Aus Sicherheitsperspektive ist dieses Wissen jedoch von Bedeutung, da fallabhängig jeweils unterschiedliche Sicherheitsanforderungen relevant sein können. Die Aussagekraft

einer primären Modellierung von Sicherheitsobjekttypen im KOS ist daher nicht eindeutig und kann zu unpräzisen Anforderungsdefinitionen führen.

Das Zielsystem der fachlichen Sicherheitsmodellierung bildet somit die im VOS abgebildete, fachliche Vorgangs-Funktionalität eines Anwendungssystems[119]. Die Außensicht des VOS beschreibt hierbei den funktionalen Kern eines Anwendungssystems, der die entsprechenden betrieblichen Vorgänge, die durch das Anwendungssystem unterstützt werden, repräsentiert. Aus Innensicht beschreibt das VOS die Gestaltung des Lösungsverfahrens dieser Vorgänge, indem durch Operatoren und Attribute der VOT die entsprechenden Aktionen aus fachlicher Sicht spezifiziert werden [Ambe93, 37]. Sowohl Außen- als auch Innensicht werden im Rahmen der fachlichen Sicherheitsmodellierung von SOMsec berücksichtigt. Sichtbar wird dies anhand eines zwei-stufigen Vorgehensmodells, das zur fachlichen Sicherheitsmodellierung in SOMsec genutzt wird[120].

Analog zur Strukturierung des Kapitels 8 erfolgt die weitere Darstellung anhand der Erörterung semantischer, syntaktischer und methodischer Integrationsaspekte von Sicherheitsanforderungen.

9.2. Semantische Integration von Sicherheitsanforderungen

Gemäß dem Referenzmodell betrieblicher Informationssicherheit sind Sicherheitsanforderungen an ein Anwendungssystem der Ressourcenebene des Architekturrahmens zuzuordnen. Aus fachlicher Sicht werden sie hier durch Sicherheitsgrundfunktionen repräsentiert, die als allgemeingültige Abstraktionen der primär technisch orientierten Sicherheitsmechanismen und -dienste fungieren. Die Ableitung der Sicherheitsanforderungen an ein Anwendungssystem aus einem zugehörigen sicherheitserweiterten Geschäftsprozessmodell erfolgt somit über die inhaltliche Beziehung zwischen Sicherheitsgrundfunktionen und Schutzzielen. In Kapitel 7.1.3.1 der vorliegenden Arbeit wurde diese Beziehung zur Vervollständigung der Beschreibung des Referenzmodells bereits inhaltlich ausgestaltet. Die dort vorgestellte Matrix dient im Folgenden als Grundlage der Spezifikation der diesbezüglich notwendigen Ableitungsbeziehungen. Sicherheitsgrundfunktionen dienen dabei als konzeptuelle Grundlage für den sicherheitsorientierten Übergang zwischen Geschäftsprozessmodell und Anwendungsmodell. Die

[119] Vgl. hierzu [Ambe93, 35].

[120] Vgl. hierzu Kapitel 9.4.2.

konkrete Repräsentation dieser Konzepte in den entsprechenden Modellschemata werden dann im Rahmen der syntaktischen Integration erörtert.

9.2.1. Identifikation relevanter Sicherheitsgrundfunktionen

Als inhaltlich relevant für die Beziehung zwischen Geschäftsprozessmodell und Anwendungsmodell sind ausschließlich die für eine Schutzzielklasse als präventiv markierten Sicherheitsgrundfunktionen zu interpretieren. Bezogen auf die in SOMsec betrachteten Schutzzielklassen Vertraulichkeit und Verbindlichkeit, sind auf Basis der Matrix aus Abbildung 30 die folgenden Beziehungen zu Sicherheitsgrundfunktionen zu identifizieren.

Schutzzielklassen	*Sicherheitsgrundfunktionen*
Vertraulichkeit	▪ Authentisierung (Identifikation und Authentisierung) ▪ Autorisierung (Zugangskontrolle und Autorisierung) ▪ (Wiederaufbereitung) ▪ Übertragungssicherung
Verbindlichkeit	▪ Authentisierung (Identifikation und Authentisierung) ▪ Autorisierung (Zugangskontrolle und Autorisierung) ▪ Beweissicherung

Abbildung 56: Relevante Beziehungen zwischen Schutzzielklassen und Sicherheitsgrundfunktionen

Die Grundfunktion Wiederaufbereitung ist im Kontext der Anwendungsentwicklung nur von geringer Bedeutung, da sie einen sehr starken Bezug zu Aufgabenträgern im Sinne von Hardware aufweist. Sie wird aus diesem Grund im weiteren Verlauf nicht berücksichtigt. Im Falle der Authentisierung, Autorisierung und Beweissicherung wurden weiterhin aus Gründen der Übersichtlichkeit die ursprünglichen Bezeichnungen der Kategorien der Sicherheitsgrundfunktionen für die weitere Verwendung abgekürzt.

9.2.2. Ableitung von Sicherheitsgrundfunktionen

Auf Basis der grundlegenden Ableitungsbeziehungen sind die im Rahmen von SOMsec modellierbaren Sicherheitsgrundfunktionen im Detail zu analysieren. Nicht jeder Schutzzieltyp muss dabei zwingend durch alle Sicherheitsgrundfunktionen der jeweiligen Zuordnungen aus Abbildung 56 umgesetzt werden. Vielmehr kann auf Grund der getroffenen Differenzierung

der Schutzzieltypen in SOMsec eine eindeutige Ableitungsempfehlung angegeben werden. Gegliedert nach den Meta-Objekttypen der Modellierung werden diese Zusammenhänge im Folgenden dargestellt.

Aufgaben

Aufgaben werden in SOMsec aus vorgangsorientierter Sichtweise mit Schutzzielen annotiert. In Bezug auf Vertraulichkeit sind hierbei die Sicherheitsgrundfunktionen Authentisierung und Autorisierung als Anforderungen abzuleiten[121]. Die Verbindlichkeit eines Vorgangs wird durch die Sicherheitsgrundfunktionen Authentisierung und Beweissicherung unterstützt.

Transaktionen

Durch die Aufgliederung des Transaktionskonzepts in Sendeaufgabe, Empfangsaufgabe und Transaktion sowie die dedizierte Modellierung der Schutzziele für jede dieser Komponenten, ist die Angabe individueller Sicherheitsgrundfunktionen möglich. Die Annotierung von Sende- und Empfangsaufgaben sind vorgangsbezogen zu interpretieren, sodass je nach Schutzzielklasse die entsprechenden Sicherheitsgrundfunktionen des vorhergehenden Abschnitts relevant sind. Für die Schutzzieltypen Sende- und Empfangsvertraulichkeit sind dies Authentisierung und Autorisierung, für die Nichtabstreitbarkeit des Sendens bzw. des Empfangs die Sicherheitsgrundfunktionen Beweissicherung und Authentisierung. Transaktionen selbst werden in SOMsec aufgabenobjektorientiert betrachtet. Der Schutzzieltyp Transaktionsvertraulichkeit bedingt hierbei die Sicherheitsgrundfunktion Übertragungssicherung, Transaktionsverbindlichkeit wird durch die Grundfunktion Authentisierung unterstützt.

Die folgenden Tabelle zeigt die beschriebenen Ableitungsbeziehungen zwischen Schutzzielen und Sicherheitsgrundfunktionen im Überblick.

[121] In Bezug auf die Ausgestaltung der grundlegenden Matrix aus Kapitel 7.1.3.2 sind hierbei die Ausführungen in Kapitel 8.2.2.3 zu berücksichtigen. Hierdurch wird die Darstellung in Bezug auf die Unbeobachtbarkeit eines Vorgangs im Kontext von SOMsec erweitert, sodass die angesprochene Ableitung der Sicherheitsgrundfunktionen Authentisierung und Autorisierung ermöglicht wird.

Schutzziele	Sicherheitsgrundfunktionen: Authentisierung	Autorisierung	Beweissicherung	Übertragungssicherung
Transaktionvertraulichkeit				✓
Sendevertraulichkeit	✓	✓		
Empfangsvertraulichkeit	✓	✓		
Vorgangsvertraulichkeit	✓	✓		
Transaktionsverbindlichkeit	✓			
Nichtabstreitbarkeit des Sendens	✓		✓	
Nichtabstreitbarkeit des Empfangs	✓		✓	
Nichtabstreitbarkeit des Vorgangs	✓		✓	

Abbildung 57: Beziehungen zwischen Sicherheitsgrundfunktionen und Schutzzielen in SOMsec

In Bezug auf die dargestellten Beziehungen gilt grundsätzlich, dass die Anwendung der Ableitung für einen Schutzzieltyp als optional zu betrachten ist und individuelle Modellzusammenhänge zu berücksichtigen sind. So ist durch den Modellierer etwa in Bezug auf die Transaktionsvertraulichkeit zu überprüfen, ob es sich um eine anwendungssysteminterne oder eine systemexterne Transaktion handelt. Ist Ersteres der Fall, so kann unter Umständen auf die Grundfunktion der Übertragungssicherung verzichtet werden, wenn die jeweilige Transaktion zum Beispiel nur zwischen zwei Prozessen auf einer Basismaschine durchgeführt wird und keine externen, ungesicherten Transportkanäle verwendet werden. Natürlich setzt dies eine gewisse technische Kenntnis des Modellierers voraus, zeigt aber auch die Freiheitsgrade, die durch SOMsec im Rahmen der fachlichen Modellierung von Anwendungssystemen gewährt werden.

Aus inhaltlicher Sicht betrachtet wird deutlich, dass die Grundfunktion der Authentisierung als notwendige Bedingung für die Erreichung aller Schutzziele mit Ausnahme der Transaktionsvertraulichkeit fungiert. Auf welche Weise diese und die weiteren Grundfunktionen in die fachliche Systemspezifikation integriert werden, wird in den nächsten Abschnitten im Detail erörtert.

9.3. Syntaktische Integration von Sicherheitsanforderungen

Im Rahmen der syntaktischen Integrationsfrage ist zu klären, wie das Konzept der Sicherheitsgrundfunktion in das Modellschema des VOS eingebunden werden kann. Ausschlaggebender Faktor ist hierbei die grundlegende objektorientierte und objektintegrierte Metapher, anhand derer Anwendungssysteme in SOMsec zu spezifizieren sind. Gemäß dem entsprechenden Meta-Modell erfolgt dies durch konzeptuelle Objekttypen und Vorgangsobjekttypen, die als Spezialisierung eines allgemeines Objekttyps modelliert werden [FeSi08, 228]. Die darzustellenden Sicherheitsgrundfunktionen sind auf dieses Verständnis abzustimmen und werden syntaktisch als **Sicherheitsobjekttypen (SOT)**, bzw. als deren Instanzen (**Sicherheitsobjekte, SO**) in das fachliche Anwendungsmodell integriert.

9.3.1. Differenzierung der Sicherheitsobjekttypen

Gemäß der in Kapitel 9.2 definierten inhaltlichen Beziehungen, werden in SOMsec vier Sicherheitsobjekttypen spezifiziert, die die Schutzzielklassen Vertraulichkeit und Verbindlichkeit im Anwendungsmodell vollständig erfassen. In Anlehnung an die Bezeichnung der Sicherheitsgrundfunktionen werden die folgenden SOT unterschieden.

- authentisierungsspezifischer Sicherheitsobjekttyp - SOT.Auth
- autorisierungsspezifischer Sicherheitsobjekttyp - SOT.Auto
- beweisspezifischer Sicherheitsobjekttyp - SOT.Beweis
- übertragungsspezifischer Sicherheitsobjekttyp - SOT.ÜS

Sicherheitsobjekttypen kapseln in SOMsec die sicherheitsrelevanten, nicht-funktionalen Anforderungen an ein Anwendungssystem, die über das Konzept der Sicherheitsgrundfunktion aus den modellierten Schutzzieltypen ableitbar sind. Die unterschiedlichen Ausrichtungen der einzelnen SOT sind dabei anhand der Ausgestaltung ihrer Attribute identifizierbar. Ein **generischer Sicherheitsobjekttyp** (SOT.Gen) bildet dabei einen Supertypen im Sinne der Objektorientierung, mit dem die vier Subtypen SOT.Auth, SOT.Auto, SOT.Beweis und SOT.ÜS in einer Vererbungsbeziehung stehen. Die folgende Abbildung stellt die Struktur der zu skizzierenden Sicherheitsobjekttypen in Form eines UML-Klassendiagramms im Überblick dar.

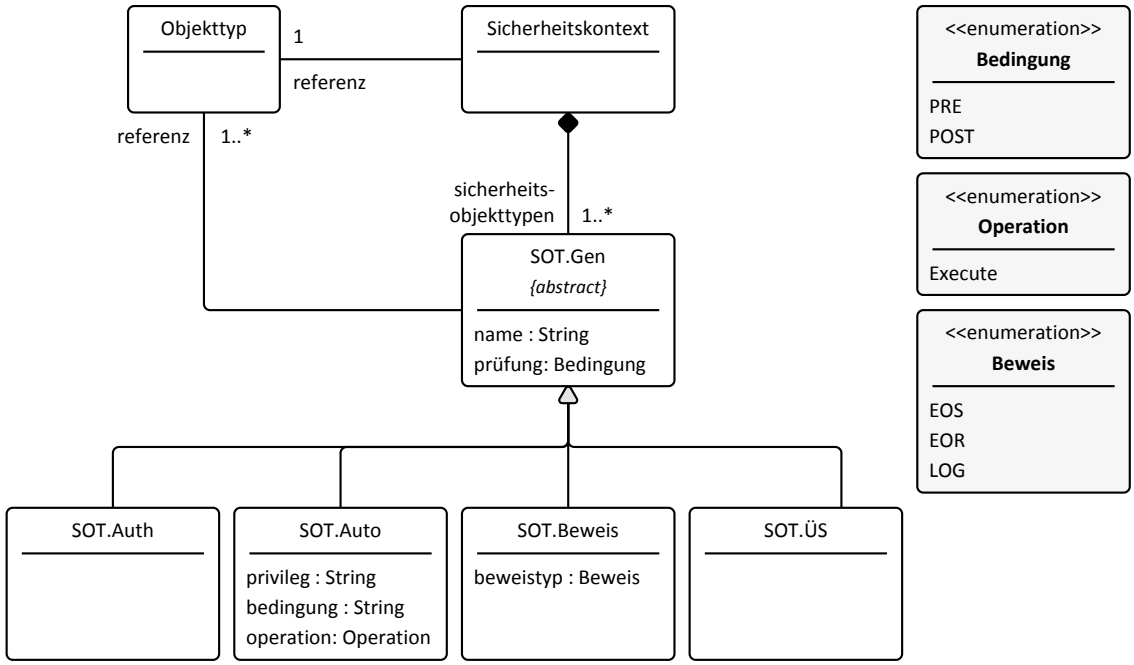

Abbildung 58: Struktur der Sicherheitsobjekttypen

Die Assoziationsbeziehungen in der Abbildung sind in Leserichtung mit der entsprechenden Multiplizität und zugehörigem Rollennamen annotiert[122]. Die Meta-Objekttypen der fachlichen Modellschemata werden generisch in Form des Modellelements „Objekttyp“ zur Komplettierung der Referenzen des Modells in die Darstellung aufgenommen. Mögliche Ausprägungen von Attributen werden durch die Angabe der Enumerationen auf der rechten Seite des Modells dargestellt[123].

Im Rahmen der Modellierung werden **Sicherheitskontext** und **Sicherheitsobjekttypen** graphisch im Anwendungsmodell dargestellt. Die Spezifikation der Instanzen in Form von Sicherheitsobjekten erfolgt hingegen textuell, analog zur Repräsentation von Schutzzielen in Form einer XML-Notation[124]. Als Hauptelement dient dabei ein komplexer XML-Typ für die Angabe des Sicherheitskontextes, der durch ein Attribut `name` eindeutig identifizierbar ist. Als dessen Subelemente fungieren die entsprechend modellierten Sicherheitsobjekte. Jeder zu Grunde liegende Sicherheitsobjekttyp wird dabei durch einen eigenen komplexen XML-Typ abgebildet, dessen Subelemente sich wiederum aus der jeweiligen Attributdefinition ergeben.

[122] Aus Implementierungssicht sind Rollen ebenfalls als Attribute der assoziierenden Klasse zu interpretieren. Eine Instanz von Sicherheitskontext würde somit ein Attribut „referenz“ führen, dem genau eine Instanz von Objekttyp zugeordnet ist.

[123] In SOMsec wird für das Attribut „operation“ nur ein Wert „EXECUTE“ verwendet. Aus Gründen der Darstellungskonsistenz wird dieser ebenfalls in Form der Enumeration „Operation“ dargestellt.

[124] Die Instanziierung von Sicherheitsobjekten wird in Kapitel 9.3.2 beschrieben.

Im Rahmen der nachfolgenden Erläuterungen zu den einzelnen Subtypen werden die entsprechenden XML-Notationen ebenfalls dargestellt.

9.3.1.1. Generischer Sicherheitsobjekttyp

Der generische Sicherheitsobjekttyp kann als abstrakte Klasse interpretiert werden, die alle gemeinsamen Attribute enthält, die an die Subklassen weitergegeben werden. Das allgemeine Attribut `name` enthält dabei einen eindeutigen Bezeichner, der eine Instanz im Modell identifiziert und durch den Modellierer frei wählbar ist.

Attribut „referenz“

Das Attribut `referenz` beinhaltet eine Auflistung aller Objekttypen, denen der Sicherheitsobjekttyp zugeordnet ist. Durch die Multiplizität der Assoziation wird spezifiziert, das dabei mindestens eine Referenz vorhanden sein muss, ein Sicherheitsobjekttyp ohne Zuordnung zu einem Objekttypen ist somit nicht zulässig. Unabhängig von der dargestellten Typisierung der Referenz in UML-Notation, kann die Beziehung zu einen Objekttyp in SOMsec weiter verfeinert werden, indem direkt auf Attribute bzw. Operatoren des jeweiligen Objekttypen verwiesen wird. Die Ausprägung `VOT_A.Operator_B` des Attributs `referenz` eines Sicherheitsobjekts Autorisierung bedeutet somit zum Beispiel, dass für den Zugriff auf den Operator B eines Vorgangsobjekttypen A eine Autorisierung notwendig ist. Die weiteren Anforderungen der Zugriffskontrolle werden dann anhand der Attribute des spezialisierten SOT.Auto detailliert.

Attribut „prüfung“

Das allgemeine Attribut `prüfung` bezieht sich auf die Anwendung und Überprüfung der jeweiligen Sicherheitsanforderung. Es werden die zwei Ausprägungen `PRE` und `POST` unterschieden, die die jeweiligen Zeitpunkte beschreiben, an denen die jeweilige Anforderung im Rahmen der Durchführung von Aufgaben und Aktionen erfüllt sein muss. `PRE` bezieht sich dabei auf einen beliebigen Zeitpunkt vor der Durchführung, `POST` auf einen danach.

9.3.1.2. SOT Authentisierung

Der Sicherheitsobjekttyp Authentisierung beschreibt die generelle fachliche Anforderung, dass die Identität einer mit dem System interagierenden Entität dem Anwendungssystem bekannt sein muss. In SOMsec wird diese Anforderung grundsätzlich identitätsunabhängig mo-

delliert, d.h. es muss keine dedizierte Angabe einer speziellen Identität erfolgen. Dies ist dadurch begründet, dass der SOT.Auth niemals alleine modelliert wird, sondern nur in Verbindung mit den SOT Beweissicherung oder Autorisierung, für die er eine notwendige Bedingung darstellt[125]. Der SOT Beweissicherung wird dabei ebenfalls identitätsunabhängig modelliert, der SOT Autorisierung ist zwar identitätsabhängig, spezifiziert jedoch entsprechend notwendige Identitäten selbst. Eine explizite Angabe einer Identität ist in diesem Zusammenhang somit bereits aus inhaltlicher Perspektive nicht notwendig. Aus methodischer Sicht wird der SOT.Auth des Weiteren nicht explizit in der Modellierung erfasst, wenn mindestens einer der beiden Sicherheitsobjekttypen SOT.Auto bzw. SOT.Beweis an dem gleichen Referenzobjekt modelliert wurde. Der Grund hierfür ist ebenfalls durch die dargestellte Beziehung zwischen Authentisierung und Beweissicherung bzw. Autorisierung gegeben, zudem wird auf diese Weise die Lesbarkeit der erzeugten Modellschemata erhöht.

Die einzige Ausnahme bildet die Spezifikation der Authentisierung, wenn sie unabhängig von Autorisierungs- bzw. Beweissicherungsanforderungen aus dem Schutzziel der Transaktionsverbindlichkeit abgeleitet werden kann. In diesem Zusammenhang bezieht sich der SOT.Auth nicht auf die Authentisierung einer Entität sondern vielmehr auf die **Authentisierung der Information**, die durch die Transaktion übertragen wird. Die Spezifikation erfolgt in diesem Fall analog zu der obigen Ausführung ebenfalls identitätsunabhängig.

In Bezug auf die Attribute des SOT.Auth ergibt sich somit eine Deckungsgleichheit mit dem abstrakten SOT.Gen. Die Ausprägung des Attributs `prüfung` von SOT.Auth ist dabei immer mit `PRE` zu spezifizieren, da die Authentisierungsanforderung stets vor der Durchführung einer Transaktion zu überprüfen ist. Die XML-Notation einer Instanz des SOT.Auth wird durch die folgende Struktur beschrieben.

```
<SO.Auth name="bezeichung">
    <referenz> VOT / Operator </referenz>
    <prüfung> PRE </prüfung>
</SO.Auth>
```

Quelltext 6: XML-Notation SOT.Auth

[125] Vgl. Abbildung 57.

9.3.1.3. SOT Autorisierung

Die Autorisierungsanforderung besagt, dass vor der Durchführung einer Aufgabe eine Berechtigungsprüfung der diesen Vorgang initiierenden Entität zu erfolgen hat. Zentraler Aspekt hierbei ist die Auswahl der Kriterien, anhand derer diese Überprüfung erfolgt. In SOMsec wird diesbezüglich der Ansatz der **attribut-basierten Zugriffskontrolle** (engl. *attribute-based access control*, ABAC) genutzt und dessen konzeptuelle Ausrichtung übernommen. Im folgenden Abschnitt wird dieser Ansatz kurz vorgestellt, bevor im Anschuss seine Integration in SOMsec durch den SOT Autorisierung erläutert wird.

Attribute-based Access Control

Das Konzept von ABAC wird in der vorliegenden Arbeit analog zur Positionierung von RBAC[126] als Sicherheitsmodell verstanden, das auf einer attributbasierten Zugriffskontrollstrategie fußt. Die Grundidee attributbasierter Zugriffskontrollmodelle besteht darin, Zugriffsrechte zwischen Subjekten und Objekten nicht statisch zu definieren, sondern ihre Eigenschaften dynamisch als Grundlage der Autorisierung zu nutzen[127]. Attribute eines Subjekts stellen zum Beispiel allgemeine Eigenschaften dar, wie etwa die Position im Unternehmen, oder auch dynamische Eigenschaften, wie etwa das Alter oder den aktuellen Standort. In Bezug auf Objekte können Attribute als Metadaten interpretiert werden, wie sie etwa im Rahmen des Dublin Core Metadatenstandards beschrieben werden[128] [Pri+05, 286]. Ein erweitertes Modell von ABAC lässt sich wie folgt darstellen.

[126] Vgl. hierzu Kapitel 5.5.3.

[127] Grundlage der Beschreibung von ABAC bildet das Subjekt/Objekt-Prinzip, vgl. hierzu Kapitel 5.4.3.2.

[128] Vgl. hierzu [DCMI08].

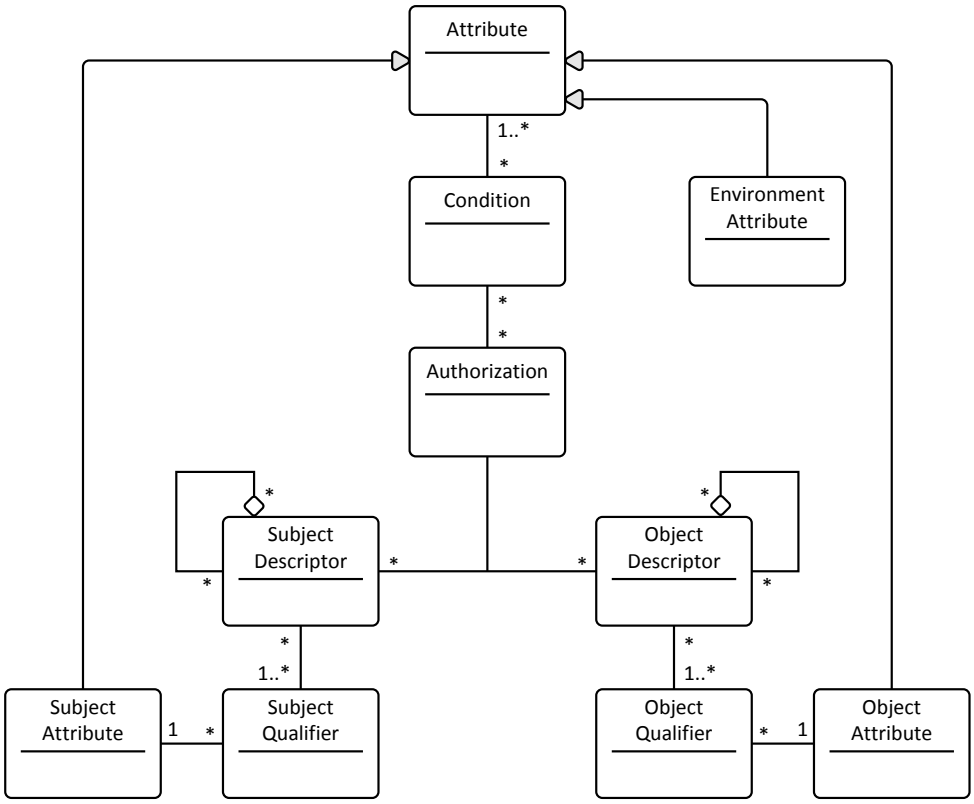

Abbildung 59: Erweitertes ABAC-Modell (nach [DoPe06, 39])

Alle Subjekte und Objekte werden im Konzept von ABAC durch eine Menge an Attributen (*SubjectAttribute*, *ObjectAttribute*) charakterisiert. Eine Unterteilung von Subjekten bzw. Objekten wird erreicht durch die Spezifikation sogenannter Deskriptoren (*SubjectDescriptor*, *ObjectDescriptor*), die jeweils Gruppen von Subjekten bzw. Objekten repräsentieren, die ein bestimmtes Bündel an Eigenschaften aufweisen. Die Spezifikation dieser Eigenschaften wird in Form von *Qualifiern* angegeben, die, als Attributbedingungen formuliert, einem Deskriptor zugeordnet werden. Eine Autorisierung (*Authorization*) wird dann zwischen einem Subjekt- und einem Objektdeskriptor angegeben. Sie besagt, dass die durch den Subjektdeskriptor beschriebenen Subjekte die durch die Autorisierung benannte Operation auf den durch den Objektdeskriptor definierten Objekten ausführen dürfen. Zusätzlich können Bedingungen (*Condition*) als Einschränkungen für die Autorisierungen spezifiziert werden. Sie ermöglichen zum Beispiel den direkten Vergleich von Subjekt- und Objektattributen, zum anderen können auch Umgebungsattribute in die Spezifikation einbezogen werden [DoPe06, 37ff].

Integration von ABAC in SOMsec

Der Hintergrund für die Nutzung von ABAC in SOMsec besteht in der konzeptuellen Ausrichtung des Ansatzes, der von der Modellierung konkreter Identitäten und Ressourcen abstrahiert und diese durch die Nutzung von Attributen ersetzt. Im Vergleich zu bestehenden Ansätzen wie RBAC sind hierdurch flexiblere Spezifikationen erstellbar, die vor allem im Hinblick auf hohe Zahlen von Subjekten und Objekten einfacher zu administrieren sind [DoPe06, 36f]. Außerdem kann ABAC als Generalisierung traditioneller Zugriffskontrollmodelle angesehen werden, sodass zum Beispiel die Konzepte MAC, DAC oder auch RBAC in ABAC abgebildet werden können [Pri+07, 28].

Das Grundkonzept der attributbasierten Zugriffskontrolle wird in SOMsec durch die Integration der relevanten Eigenschaften in die Spezifikation des Sicherheitsobjekttyp Autorisierung übernommen. Dabei werden aus Komplexitätsgründen jedoch nur relevante Teilbereiche berücksichtigt.

Eine Autorisierung wird in SOMsec durch das Attribut `operation` abgebildet, dessen zulässiger Wert `EXECUTE` sich auf die Berechtigung zur Ausführung eines Vorgangs bzw. eines Operators als Teil-Lösungsverfahren eines VOT bezieht. Der entsprechende Verweis im Attribut `referenz` stellt im Sinne von ABAC das Objekt dar, dessen Zugriffe zu autorisieren sind. Auf die explizite Angabe eines Objektdeskriptors kann in diesem Zusammenhang verzichtet werden, da ein Operator eines VOT selbst bereits als Attribut des VOT gilt und demzufolge keine weiteren Eigenschaften anzugeben sind. Ein Subjektdeskriptor wird durch das Attribut `privileg` abgebildet, das in Form von zwei Operanden und einem binären Vergleichsoperator anzugeben ist. Es erfasst somit alle Attributbedingungen, die ein Subjekt aufweisen muss, um eine Berechtigung gemäß dem Attribut `operation` auf ein Objekt `referenz` zu erhalten. Weiterhin wird das Konzept der Conditions durch das Attribut `bedingung` abgebildet. Es ist analog zum Attribut `privileg` zu spezifizieren. Das von SOT.Gen geerbte Attribut `prüfung` ist abschließend immer mit PRE zu belegen. Eine Verifikation der Autorisierung ist somit immer vor der Durchführung eines Operators durchzuführen.

Zusammenfassend ergibt sich die folgende Struktur einer Instanz des Sicherheitsobjekttyps Autorisierung.

```
<SO.Auto name="bezeichung">
    <referenz> VOT / Operator </referenz>
    <prüfung> PRE </prüfung>
    <privileg> Attributbedingung </privileg>
    <bedingung> Attributbedingung </bedingung>
    <operation> EXECUTE </operation>
</SO.Auto>
```

Quelltext 7: XML-Notation SOT.Auto

Durch die dargestellte Nutzung des attributbasierten Konzepts kann in SOMsec im Anwendungsmodell auf eine explizite Modellierung von Identitäten verzichtet werden.

9.3.1.4. SOT Beweissicherung

Die allgemeine Anforderung der Beweissicherung wird durch das Attribut `beweistyp` des SOT.Beweis genauer spezifiziert. Gemäß der vorgestellten inhaltlichen Ausprägungen der Nichtabstreitbarkeit sowie der rechtsverbindlichen Protokollierung sind hierbei drei Arten von Beweisen darstellbar. Die Werte `EOR` sowie `EOS` beziehen sich auf die Aspekte der Nichtabstreitbarkeit und fordern einen Beweis des Empfangs (EOR) bzw. des Versandes (EOS) einer Transaktion. In Bezug auf allgemeine Verarbeitungsaufgaben spezifiziert der Wert `LOG` zudem, dass eine Protokollierung der Aktion durchzuführen ist.

Die Sicherheitsanforderung Beweis ist identitätsunabhängig zu spezifizieren, d.h. es wird die generelle Aussage getroffen, dass eine Beweiserbringung zu erfolgen hat. Die Angabe einer speziellen Identität, die als Beweiserbringer fungieren muss, ist dabei nicht zielführend, da sie inhaltlich nicht sinnvoll zu interpretieren ist. Gleichwohl ist die Authentisierung an sich Vorbedingung für die Beweiserbringung, da ansonsten zur Laufzeit des Systems eine entsprechende Protokollierung nur unvollständig erfolgen könnte. Die Beweiserbringung als Anforderung bezieht sich somit auf alle Identitäten eines Systems, die authentisiert und unter Umständen berechtigt sind, die jeweils referenzierte Operation durchzuführen.

Das Attribut `prüfung` des SOT.Beweis ist immer mit `POST` zu belegen, da die Beweiserbringung stets der jeweiligen Aktion nachgelagert ist. Es ergibt sich die folgende Struktur einer Instanz des SOT.Beweis.

```
<SO.Beweis name="bezeichnung">
    <referenz> VOT / Operator </referenz>
    <prüfung> POST </prüfung>
    <beweistyp> EOS | EOR | LOG </beweistyp>
</SO.Beweis>
```

Quelltext 8: XML-Notation SOT.Beweis

9.3.1.5. SOT Übertragungssicherung

In SOMsec wird die Anforderung der Übertragungssicherung bedarfsorientiert immer dann modelliert, wenn eine systemexterne Transaktion auf Geschäftsprozessebene als vertraulich annotiert wurde. Als Referenz fungiert dabei theoretisch ein transaktionsspezifischer KOT des KOS, aus methodischen Gesichtspunkten erfolgt in SOMsec jedoch eine Präzisierung der beteiligten Sende- und Empfangsaufgaben im VOS.

Unabhängig von der Modellierung spezifiziert der SOT.ÜS eine fachliche Sicherheitsanforderung, die hauptsächlich auf technischer Ebene durch den Einsatz von Verschlüsselungsalgorithmen ausgestaltet werden kann. Im Rahmen der fachlichen Modellierung sind demzufolge keine weiteren charakterisierenden Attribute für diese Sicherheitsanforderung notwendig. Das Attribut `prüfung` ist analog zu SOT.Auth und SOT.Auto mit `PRE` zu belegen, da die Anforderung der Übertragungssicherung eine Vorbedingung für die Durchführung der Transaktion darstellt. Instanzen des SOT.ÜS werden in folgender Form in XML-Notation dargestellt.

```
<SO.ÜS name="bezeichnung">
    <referenz> VOT / Operator </referenz>
    <prüfung> PRE </prüfung>
</SO.ÜS>
```

Quelltext 9: XML-Notation SOT.ÜS

9.3.1.6. Sicherheitskontext

Als weiterer Aspekt wird die Spezifikation eines **Sicherheitskontextes** (SK) in Abbildung 58 aufgeführt. Hierbei handelt es sich um ein Konzept, das die Gruppierung aller Sicherheitsobjekttypen ermöglicht, die einem Objekttyp zugeordnet sind. Diese Aggregation der entsprechenden SOT erlaubt zum einen die einfachere Referenzierung der modellierten Sicherheits-

anforderungen, zum anderen kann durch die Gruppierung aller Sicherheitskontexte eines Modells eine vollständige Sicht auf die sicherheitsrelevanten Modellelemente erzeugt werden. Diese Sichtweise wird in SOMsec als **Sicherheitsobjektschema** (SOS) bezeichnet und in Kapitel 9.5.3 erläutert.

9.3.2. Meta-Modell der fachlichen Sicherheitsspezifikation

Für jedes modellierte Schutzziel ist ein eigenständiger SOT zu spezifizieren, der die jeweiligen inhaltlichen Anforderungen im VOS abbildet. In Abbildung 60 werden Sicherheitsobjekttypen[129] zu einem objekttypspezifischen **Sicherheitskontext** in Verbindung gesetzt, der als Referenz auf die fachlichen Sicherheitsanforderungen in das Meta-Modell der Anwendungssystemspezifikation integriert werden kann.

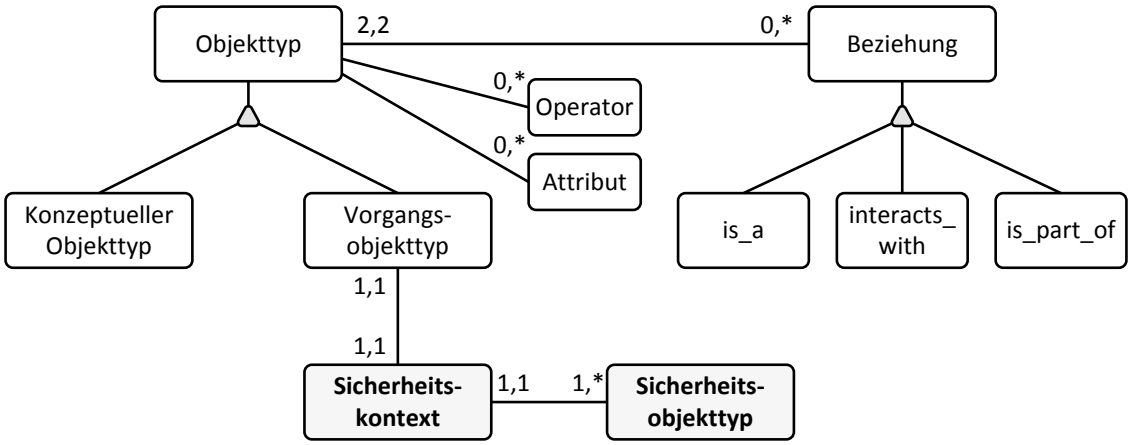

Abbildung 60: Meta-Modell der fachlichen Sicherheitsspezifikation in SOMsec

In SOMsec wird ein Sicherheitskontext für einen Vorgangsobjekttyp analog zur Modellierung von Schutzzielen durch ein gepunktetes, abgerundetes Rechteck dargestellt. Zur Erhöhung der Lesbarkeit ist es optional durch eine nicht-typisierte, gepunktete Linie mit dem referenzierten Objekttypen zu verbinden.

Erweiterung des Meta-Modells von SOM

Das dargestellte Meta-Modell der fachlichen Sicherheitsmodellierung in SOMsec stellt eine Erweiterung des entsprechenden Meta-Modells von SOM dar. Es gilt zu beachten, dass die Zielsetzung dieses Meta-Modells nicht in einer exakten Sprachdefinition besteht, sondern

[129] Bezüglich der Differenzierung und Struktur von Sicherheitsobjekttypen vgl. Kapitel 9.3.1, insbesondere Abbildung 58.

vielmehr die Eingliederung von Sicherheitskontext und Sicherheitsobjekttypen in die Modellschemata sowie deren referentielle Beziehungen zu den Modellelementen des VOS beschreibt. Der Grund hierfür besteht in der Unterscheidung zwischen funktionalen und nicht-funktionalen Anforderungen im Rahmen der Erstellung des Anwendungsmodells. Das VOS repräsentiert aus fachlicher Sicht die funktionale Spezifikation des Anwendungssystems, wohingegen Sicherheitsobjekttypen nicht-funktionale Anforderungen darstellen. Grundsätzlich würde hierdurch ein zweite Modellierungsdimension erzeugt, die in einem separaten Sicherheitsmodellschema zu behandeln wäre. Auf Grund der konzeptuellen Schnittstelle in Form der Beziehung zwischen Sicherheitsanforderungen und funktionaler Modellierung, die aus dem Geschäftsprozessmodell ableitbar ist, wird dieser Ansatz in SOMsec jedoch nicht verfolgt und eine integrierte Modellierung in den Modellschemata des VOS durchgeführt. Das erweiterte Meta-Modell von SOMsec zeigt einerseits diesen Sachverhalt auf, andererseits erfolgt die Sprachdefinition für das VOS gemäß der SOM-Methodik, die unverändert übernommen wurde. Im Rahmen der Modellierung werden SOT somit ohne typisierte Beziehungen als unabhängige Modellelemente modelliert.

Sicherheitsobjekte

Ein weiterer Aspekt, der sich an diesen Ansatz anschließt, ist die Tatsache, dass nicht-funktionale Anforderungen in der Regel nicht in Form von Objekttypen zu modellieren sind, sondern als deren Instanzen. Sicherheitsanforderungen werden somit als **Sicherheitsobjekte** modelliert, die sich auf bestimmte VOT beziehen. Dies ist dadurch begründet, dass Sicherheitsanforderungen nicht den Instanziierungszyklen der fachlichen Objekttypen während der Laufzeit eines Anwendungssystems unterworfen sind, sondern eine grundlegende Gültigkeit aufweisen. Jede Instanz eines SOT spezifiziert somit eine konkrete, durch eine entsprechend eindeutige Attributausprägung charakterisierte, sicherheitsrelevante Anforderung an ein VOT, die sich zur Laufzeit des Anwendungssystems auf alle Instanzen der referenzierten VOT bezieht. Sicherheitsanforderungen werden in SOMsec daher auf Schemaebene sowohl als Sicherheitsobjekttypen im Rahmen der initialen Ableitung als auch als präzisierte Instanzen dieser Sicherheitsobjekttypen modelliert. Im initialen Modellschema des VOS werden zunächst Sicherheitsobjekttypen modelliert, die sich als Resultat der Ableitung ergeben. Im Rahmen der Überarbeitung des VOS werden die modellierten SOT dann instanziiert und anhand konkreter Attributwerte als Repräsentation der fachlichen Sicherheitsanforderungen prä-

zisiert. Dieser zweistufige Ansatz entspricht dem Vorgehensmodell von SOMsec im Rahmen der fachlichen Sicherheitsspezifikation, das in 9.4.2 im Detail vorgestellt wird.

Operationalisierung von Sicherheitsanforderungen

Neben der konzeptuellen Grundlage dieses Ansatzes, besteht ein weiterer Vorteil in der einfacheren Operationalisierbarkeit der Sicherheitsanforderungen. Durch die Bildung von Sicherheitsobjekten sind die jeweiligen Attribute durch konkrete Werte belegbar, die in SOMsec inital aus den Eigenschaften der modellierten Schutzziele ableitbar sind. Auf diesem Wege werden die nicht-funktionalen Anforderungen bereits auf fachlicher Ebene so spezifiziert, dass sie auf technischer Ebene dann auf Basis ihrer jeweiligen Attributausprägung durch den Einsatz entsprechender Sicherheitsmechanismen realisierbar sind. Der Grad der Umsetzung der spezifizierten Sicherheitsanforderungen spiegelt sich dann zum einen in der grundlegenden technischen Stärke eines Sicherheitsmechanismus gegenüber möglichen Angriffen wider, zum anderen durch die Vollständigkeit der Parametrisierung des Mechanismus auf Basis der fachlichen Modellierung.

9.4. Methodische Integration von Sicherheitsanforderungen

Die Fragestellung der methodischen Integration bezieht sich auf die Ableitungsbeziehung zwischen Schutzzielen auf Geschäftsprozessebene und Sicherheitsanforderungen im Anwendungsmodell. In einem ersten Schritt ist dabei zu klären, welche Schutzziele auf welche Sicherheitsanforderungen im Rahmen der Modellerstellung abzubilden sind, sodass die spezifizierten fachlichen Abhängigkeiten zwischen Schutzzielen und Sicherheitsgrundfunktionen gewahrt bleiben. Zum anderen ist darzustellen, wie die inhaltliche Ableitung der im ersten Schritt definierten Beziehungen erfolgen kann.

9.4.1. Modellierungsrelevante Sicherheitsobjekttypen

Auf Basis der in Abbildung 57 dargestellten inhaltlichen Beziehungen zwischen Schutzzielen und Sicherheitsgrundfunktionen kann die Ableitung entsprechender Sicherheitsobjekttypen vorgenommen werden.

Schutzziele	Sicherheitsobjekttypen	
Transaktionvertraulichkeit	SOT.ÜS (S)	
Sendevertraulichkeit	SOT.Auto (S)	SOT.Auth
Empfangsvertraulichkeit	SOT.Auto (E)	SOT.Auth
Vorgangsvertraulichkeit	SOT.Auto (V)	SOT.Auth
Transaktionsverbindlichkeit	SOT.Auth (S)	
Nichtabstreitbarkeit des Sendens	SOT.Beweis (S)	SOT.Auth
Nichtabstreitbarkeit des Empfangs	SOT.Beweis (E)	SOT.Auth
Nichtabstreitbarkeit des Vorgangs	SOT.Beweis (V)	SOT.Auth

Abbildung 61: Modellierbare Sicherheitsobjekttypen in SOMsec

Die in Abbildung 61 dargestellte Zuweisung entspricht in Grundzügen der vorgestellten Beziehung zwischen Schutzzielen und Sicherheitsgrundfunktionen. Ein Unterschied im Hinblick auf die konkrete Modellierung von Sicherheitsobjekttypen besteht jedoch in der Berücksichtigung des Sicherheitsobjekttyps Authentisierung. Dieser wird, wie bereits in Kapitel 9.3.1 beschrieben, nicht bei jeder fachlichen Notwendigkeit auch zwingend in SOMsec modelliert. Die Angabe eines SOT.Auth bedeutet, eine bestimmte Identität im Modell zu benennen und weitere sicherheitsrelevante Anforderungen an diese Identität zu knüpfen. Dieser Ansatz ist jedoch nur in Verbindung mit der Transaktionsverbindlichkeit sinnvoll einsetzbar. In Verbindung mit dem Sicherheitsobjekttyp Autorisierung ist dies hingegen nicht notwendig, da dieser zwar identitätsbezogen zu modellieren ist, jedoch ein eigenes Attribut dafür aufweist. Weiterhin ist der SOT Beweissicherung generell identitätsunabhängig zu modellieren, sodass eine Angabe des SOT.Auth in diesem Fall ebenfalls nicht gegeben ist.

Um in Abbildung 61 die vollständige Darstellung der Beziehung zwischen Schutzzielen und Sicherheitsobjekttypen zu wahren, ist der SOT.Auth in gepunkteter Form in der Abbildung aufgeführt. In SOMsec modelliert wird er jedoch nur in Bezug auf das Schutzziel Transaktionsverbindlichkeit, wenn eine Konkretisierung der Identität in diesem Fall gewünscht ist. Die Sicherheitsobjekttypen Übertragungssicherung, Autorisierung und Beweissicherung werden

hingegen, wie in der Abbildung dargestellt, aus den entsprechenden Schutzzielen abgeleitet und in die Modellschemata der fachlichen Anwendungssystemspezifikation integriert.

In Anlehnung an die Notation der Schutzzielmodellierung ist auch bei der Spezifikation der Sicherheitsobjekttypen eine Darstellung der referenzierten Komponenten eines VOT möglich. Die Abkürzungen S und E stehen dabei für die Teillösungsverfahren des Sendens und Empfangens einer Transaktion, die Abkürzung V bezieht sich auf den gesamten Vorgang. Im Rahmen der Modellierung werden diese **Bezugsparameter** in runden Klammern hinter der Typbezeichnung des Sicherheitsobjekttypen notiert. Die Bezugsparameter ergeben sich dabei gemäß Abbildung 61 eindeutig aus der Bezeichnung, und damit dem Typ, der modellierten Schutzziele. Einzig die Transaktionsvertraulichkeit weicht von diesem Schema ab. In diesem Fall wird der Sicherheitsobjekttyp Übertragungssicherung stets der an der Transaktion beteiligten Sendeaufgabe zugeordnet.

9.4.2. Modellierungsvorgehen

Das konkrete Modellierungsvorgehen von SOMsec auf Ebene der fachlichen Spezifikation umfasst zwei Schritte, die wiederum eine bestimmte Abfolge von Einzelschritten beinhalten. Zu Beginn wird die initiale Transformation der Schutzziele auf Sicherheitsobjekttypen durchgeführt, die im Anschluss in Verbindung mit dem Sicherheitskontext modelliert werden. Im zweiten Schritt werden die modellierten Sicherheitsobjekttypen dann im Hinblick auf ihre Semantik und, damit verbunden, auf die Ausprägung ihrer Attributwerte verfeinert. Der erste Schritt wird im weiteren Verlauf als **initiale Ableitung** bezeichnet, der zweite Schritt als **Präzisierung** der Sicherheitsobjekttypen.

9.4.2.1. Initiale Ableitung der fachlichen Sicherheitsspezifikation

Die initiale Ableitung der Sicherheitsobjekttypen in SOMsec schließt sich an die Ableitung der initialen Modellschemata gemäß der SOM-Methodik an. Die abzuleitenden Sicherheitsobjekttypen werden auf diese Weise in ein bestehendes VOS integriert. Dieser Vorgang besteht aus zwei Teilschritten:

- Für jeden Vorgangsobjekttyp, der aus einem Modellelement des Geschäftsprozessmodells hervorgeht, das im Rahmen der Systemabgrenzung liegt und mit mindestens einem Schutzziel annotiert wurde, ist ein zugehöriger Sicherheitskontext zu erstellen.

- Aus den Schutzzielen sind die inhaltlich zutreffenden Sicherheitsobjekttypen abzuleiten und dem Sicherheitskontext der jeweiligen Modellelemente zuzuordnen.

Die im vorangehenden Abschnitt erläuterte Fokussierung der Sicherheitsmodellbildung auf das VOS bedeutet eine Anpassung der Ableitungsbeziehung für diejenigen Schutzziele, die im Geschäftsprozessmodell an Elemente annotiert wurden, die gemäß der SOM-Methodik auf konzeptuelle Objekttypen abgeleitet werden. Die resultierenden Sicherheitsobjekttypen sind in diesem Zusammenhang an die zugehörigen Vorgangsobjekttypen zu überführen.

Dieser Fall ist gegeben für die Schutzziele der Transaktionsvertraulichkeit sowie der Transaktionsverbindlichkeit, deren Bezugselemente im Rahmen der fachlichen Spezifikation auf transaktionsorientierte Objekttypen abgebildet werden. In beiden Fällen ist aus Sicherheitsgesichtspunkten die zu dem transaktionsspezifischen KOT gehörige Sendeaufgabe um die jeweilige Sicherheitsanforderung zu erweitern, da durch dieses Teillösungsverfahren des VOT eine Transaktion schlussendlich veranlasst und durchgeführt wird. Aus technischer Sichtweise betrachtet, ist der Anforderung der Vertraulichkeit an eine Transaktion somit zum Beispiel durch ein entsprechendes Verschlüsselungsverfahren zu entsprechen, das durch die Sendeaufgabe zu implementieren oder aufzurufen ist. Analog dazu ist die Verbindlichkeit einer Transaktion zum Beispiel durch einen Signierungsvorgang der Sendeaufgabe vor der Übertragung sicherzustellen. Die Transaktionsverbindlichkeit ist somit durch den Sicherheitsobjekttypen SOT.ÜS(S) für das sendende VOT zu modellieren, analog dazu die Transaktionsverbindlichkeit, die durch SOT.Auth(S) auf fachlicher Ebene abzubilden ist.

Im Ergebnis entsteht durch den ersten Modellierungsschritt ein sicherheitserweitertes initiales VOS des zu entwickelnden Anwendungssystems, dessen Sicherheitsanforderungen durch die abgeleiteten Sicherheitsobjekttypen dargestellt werden.

9.4.2.2. Präzisierung der Sicherheitsobjekttypen

Im zweiten Schritt werden die modellierten Sicherheitsobjekttypen des VOS, insbesondere im Hinblick auf den Spezifikationsgrad der referenzierten Bezugselemente, präzisiert.

- Für jeden abgeleiteten Sicherheitsobjekttyp sind gemäß der Modellierung der Schutzziele entsprechend parametrisierte Sicherheitsobjekte zu instanziieren und dem zugehörigen Sicherheitskontext zuzuordnen. Ausgenommen hiervon sind Sicherheitsob-

jekttypen, die sich auf VOT beziehen, welche im Rahmen der Anwendungsentwicklung auf Grund ihrer Automatisierbarkeit nicht weiter betrachtet werden.

- Im Rahmen des Überarbeitungsprozesses von KOS und VOS sind ebenfalls die fachlichen Sicherheitsanforderungen anzupassen. Dies wird realisiert durch die Aggregation der Sicherheitskontexte der VOT, die einem Konsolidierungsvorgang unterzogen wurden.
- Gleichzeitig erfolgt eine Präzisierung der Referenzen der Sicherheitsobjekte, sodass die Sicherheitsanforderungen eine spezifischere Beziehung zu konkreten Operatoren bzw. Attributen der VOT aufweisen.

Durch den letzten Schritt des Präzisierungsvorgangs erfolgt in SOMsec die indirekte Bezugnahme auf Modellelemente des KOS. Die Spezifikation eines VOT beinhaltet eine Abfolge von Operatoren, die aus fachlicher Sicht das Lösungsverfahren des VOT spezifizieren. Diese Operatoren können aus objektorientierter Sicht sowohl dem VOT selbst, als auch den KOT zugeordnet sein, auf die sich ein VOT bezieht. Je nach inhaltlicher Zuordnung dieser Operatoren können sich im VOS modellierte Sicherheitsobjekttypen somit indirekt auf Objekte des KOS beziehen, wenn die jeweiligen Operatoren auf einem KOT aufgerufen werden. Diese Beziehung wird in SOMsec jedoch nicht explizit im KOS modelliert, da sich der Informationsgehalt des Modells aus Sicherheitsaspekten durch eine solche Vorgehensweise nicht signifikant verbessern würde.

Im Ergebnis werden durch dieses Vorgehen Sicherheitsobjekte als Repräsentation konkreter fachlicher Sicherheitsanforderungen erzeugt, die sich auf das gesamte bzw. Teile des Lösungsverfahrens von VOT beziehen. Die Menge aller so erzeugter Sicherheitsobjekte des VOS stellt die Gesamtheit der aus den Schutzzielen auf Geschäftsprozessebene ableitbaren Sicherheitsanforderungen dar, die für das zu entwickelnde Anwendungssystem von Relevanz sind.

9.4.3. Beziehungs-Meta-Modell

Aus konzeptueller Sichtweise betrachtet, kann der Übergang zwischen Geschäftsprozessebene und Anwendungsmodell durch die Überbrückung zweier hierarchisch angeordneter Modellebenen charakterisiert werden. Gemäß dem Konzept des generischen Architekturrahmens nach SINZ, ist damit für jede paarweise Beziehung zwischen den Modellebenen ein Beziehungs-Metamodell anzugeben, das die Meta-Objekte der ersten Modellebene mit den Meta-

Objekten der zweiten Modellebene verbindet [Sinz99a, 1038]. Im Kontext von SOMsec sind die abzubildenden Meta-Modellelemente die Schutzziele der Geschäftsprozessebene sowie die Sicherheitsobjekttypen des Anwendungsmodells, für die eine Ableitungsbeziehung darzustellen ist.

Beim Übergang zwischen Geschäftsprozessmodell und Anwendungsmodell in der SOM-Methodik werden in einem initialen Schritt die betrieblichen Objekte der Geschäftsprozessmodellierung in konzeptuelle Objekttypen abgebildet. Aus dem IAS werden betriebliche Objekte in objektspezifische Objekttypen sowie Transaktionen in transaktionsorientierte Objekttypen des KOS überführt[130]. Aus dem VES werden die modellierten Aufgaben in Vorgangsobjekttypen des VOS abgebildet. Analog zu dieser Abbildungsvorschrift sind somit die sicherheitsrelevanten Attribute, die die modellierten Schutzziele inhaltlich beschreiben, im Hinblick auf den Übergang zur fachlichen Spezifikation in entsprechend typisierte Attribute der Sicherheitsobjekttypen abzubilden. In Bezug auf die Ableitungsregeln von SOM ist hierbei insbesondere das Attribut `referenz` der Sicherheitsobjekttypen von Bedeutung, da dies an die Transformation anzupassen ist.

Die folgenden Ausführungen beschreiben den skizzierten Transformationsprozess. Als Ausgangspunkt dienen die in Kapitel 8.3 sowie 9.3.1 vorgestellten Attributzuweisungen zu Schutzzielen bzw. Sicherheitsobjekttypen in XML-Format[131], die als Meta-Modell der jeweiligen Sicherheitsspezifikationen zu interpretieren sind. Die Abbildung der Attribute wird durch einen Pfeil symbolisiert, mögliche Ausprägungen werden gepunktet unterstrichen. Die Darstellung ist gegliedert anhand der Sicherheitsobjekttypen als Zielelemente der Abbildung.

SOT Autorisierung

Auf den SOT.Auto werden die Schutzziele der Sende- und Empfangsvertraulichkeit sowie der Vorgangsvertraulichkeit abgebildet.

[130] Eine Beschreibung der konzeptuellen Objekttypen ist in [FeSi08, 221] zu finden.

[131] Auf die Angabe des Elements „Beschreibung“ wird verzichtet.

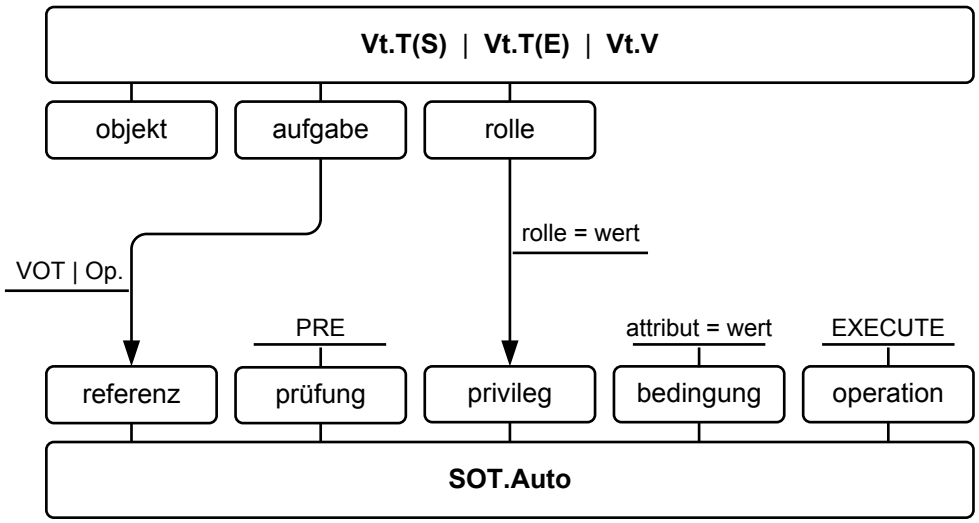

Abbildung 62: Beziehungs-Meta-Modell I

Die Aufgabe, die mit den Schutzzielen annotiert ist, wird in der initialen Ableitung als VOT in den Sicherheitsobjekttypen referenziert. Im Rahmen des Präzisierungsschrittes erfolgt dann die Verfeinerung auf einen entsprechenden Operator des VOT. Hierbei ist zu beachten, dass im Fall der Vorgangsvertraulichkeit nicht zwingend zu einzelnen Operatoren zu verfeinern ist, da sich diese auch auf alle Operatoren eines VOT beziehen kann. Mögliche Werte des Attributs `referenz` stellen somit Verweise auf VOT bzw. auf deren Operatoren (Op.) dar.

Die Attribute `prüfung` und `operation` sind vollständig aus der Schutzzieldefinition zu übernehmen. Das Attribut `privileg` enthält schließlich die Attributbedingung, die für den Zugriff auf den referenzierten Operator bzw. VOT ausschlaggebend ist. Aus inhaltlicher Sicht erfolgt in diesem Schritt die Abbildung des Konzepts der betrieblichen Rolle auf das Konzept des attributbasierten Privilegs. Hierzu wird die betriebliche Rolle als Subjektdeskriptor interpretiert und als Attribut `rolle` in der Eigenschaft `privileg` entsprechend der Bezeichnung der betrieblichen Rolle in der Schutzzielmodellierung als Attributbedingung dargestellt[132]. Im Beispiel der Sendevertraulichkeit `Vt.T(S)[12.1]` entspräche dieses Vorgehen einer Ausprägung des Attributs `privileg` des SOT.Auto in Form von „rolle = Orthopädie.Chefarzt“. Alle im System vorhandenen Nutzer, die durch diesen Subjektdeskriptor identifizierbar sind, somit als Objekt eine Eigenschaft `rolle` mit der Ausprägung „Chefarzt“ besitzen, sind dann befugt, den referenzierten Operator auszuführen. Erweiterungen der Zugriffskontrolle können durch

[132] Die konzeptuelle Basis für diese attributbasierte Abbildung des Rollenkonzepts bildet die Anforderung, dass für jede Rolle ein abstrakter Subjektdeskriptor zu definieren ist. Dies wird in SOMsec jedoch nicht explizit modelliert.

den Modellierer optional durch das Attribut `bedingung` oder durch entsprechende Anreicherung der abgeleiteten Rolleninformation im Attribut `privileg` durchgeführt werden.

SOT Übertragungssicherung und SOT Authentisierung

Der SOT.ÜS stellt das Zielelement der Ableitung des Schutzziels Transaktionsvertraulichkeit dar. Transaktionsverbindlichkeit wird auf den SOT.Auth abgebildet. Die Ableitungsbeziehungen sind in beiden Fällen identisch, sodass die Zusammenhänge gemeinsam dargestellt werden.

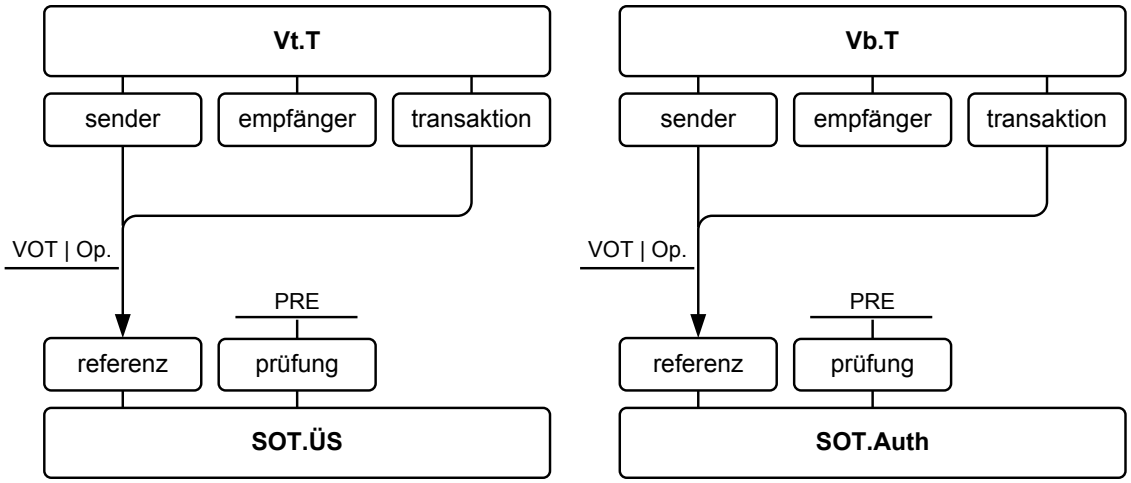

Abbildung 63: Beziehungs-Meta-Modell II

Wie bereits dargelegt wurde, erfolgt in SOMsec keine Ableitung von Sicherheitsanforderungen in das konzeptuelle Objektschema. In Bezug auf die Transaktionsvertraulichkeit und Transaktionsverbindlichkeit wird daher das Attribut Transaktion nicht auf den entsprechenden transaktionsspezifischen KOT, sondern auf den VOT, der die Transaktion steuert, abgebildet. In der Darstellung der Ableitungsbeziehung wird dies durch die zusätzliche Beziehung zwischen `Sender` und dem Attribut `referenz` dargestellt. Zu verweisen ist diesbezüglich dann auf den Operator, der die Sendeaufgabe als Teil-Lösungsverfahren des VOT durchführt.

Das Attribut `prüfung` beider SOT ist gemäß der inhaltlichen Spezifikation auf `PRE` zu setzen. Sowohl SOT.Auth als auch SOT.ÜS sind in SOMsec identitätsunabhängig zu modellieren, sodass keine Ableitung von Identitätsinformationen erfolgt. SOT.Auth und SOT.ÜS kommen aus diesem Grund oftmals in Verbindung mit der Modellierung der Sendevertraulichkeit und der damit verbundenen Identitätsspezifikation zum Einsatz, sodass auf diese Weise sicherheitsrelevante Transaktionsszenarien sehr flexibel beschreibbar sind.

SOT Beweissicherung

Die Schutzziele der Nichtabstreitbarkeit sind auf den SOT.Beweis abzubilden. Diese Beziehung ist im Wesentlichen charakterisiert durch die Referenzierung des der jeweiligen Aufgabe entsprechenden VOT.

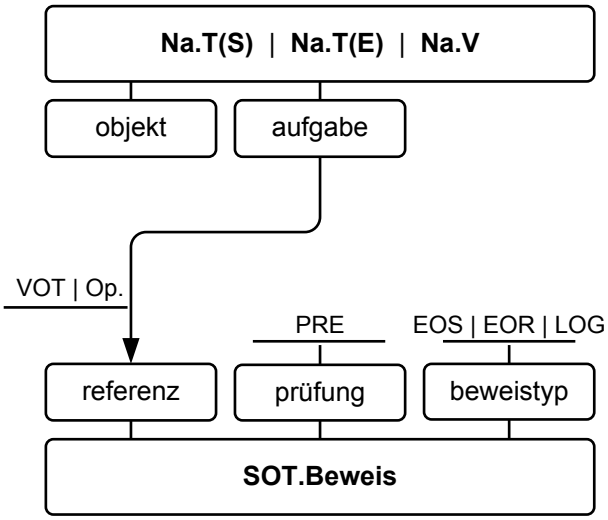

Abbildung 64: Beziehungs-Meta-Modell III

In Bezug auf Sende- und Empfangsaspekte erfolgt hierbei, analog zu der diesbezüglichen Darstellung der Vertraulichkeitsanforderungen, eine nachgelagerte Präzisierung der Referenz hin zu konkreten Operatoren des VOT. Die Nichtabstreitbarkeit des Vorgangs hingegen bezieht sich in der Regel auf den gesamten VOT. Je nach Schutzziel ist weiterhin das Attribut `beweistyp` entsprechend der Art der geforderten Beweissicherung zu setzen.

9.5. Szenario: Fachliche Sicherheitsspezifikation

Auf der Grundlage der in Kapitel 8.5 modellierten Schutzziele, kann die Ableitung und Integration der Sicherheitsanforderungen in die Modellschemata der fachlichen Anwendungssystemspezifikation des Beispielszenarios erfolgen.

9.5.1. Initiale Ableitung der Sicherheitsobjekttypen

Die folgende Abbildung zeigt das sicherheitserweiterte VOS auf Basis des vorgestellten initialen VOS des Szenarios MVZ. Integriert wurden die Elemente des Sicherheitskontextes sowie

die Sicherheitsobjekttypen, die sich aus der Ableitung der Schutzziele auf Geschäftsprozessebene ergeben.

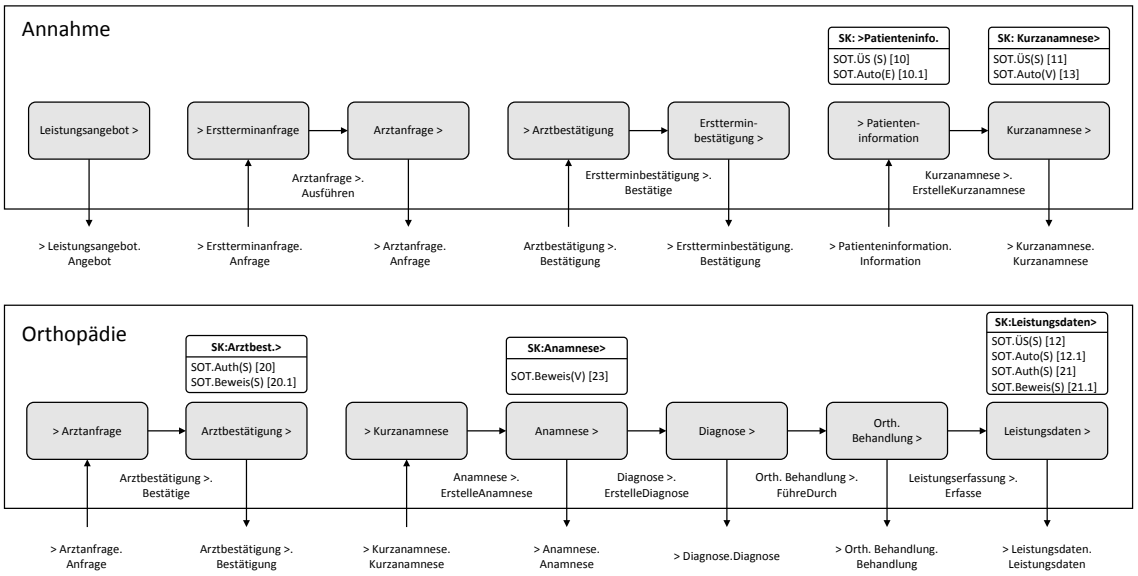

Abbildung 65: Szenario MVZ - Sicherheitserweitertes VOS (initial)

In der Darstellung des VOS sind die Sicherheitskontexte über den entsprechenden VOT notiert. Ihre Bezeichnung besteht aus dem Namen des zugehörigen VOT, dem das Präfix „SK:“ vorangestellt wird. Innerhalb des Sicherheitskontextes sind dann die abgeleiteten Sicherheitsobjekttypen notiert, denen zur besseren Darstellung der Ableitungsbeziehung in eckigen Klammern die Bezeichnung der originären Schutzziele beigefügt wird. Zusammen mit den Abkürzungen der Bezugsparameter der Sicherheitsobjekttypen dient dies vor allem bei der Ableitung des initialen VOS zur Sicherstellung der Eindeutigkeit der Ableitung.

Die im initialen VOS modellierten Sicherheitsobjekttypen entsprechen im Ergebnis der Anwendung der in Kapitel 9.4.1 spezifizierten Ableitungsbeziehungen. So wird zum Beispiel das im VES an die Aufgabe `Kurzanamnese>` annotierte Schutzziel Vorgangsvertraulichkeit `VT.V[13]` in den Sicherheitsobjekttyp `SOT.Auto(V)[13]` transformiert. In der Darstellung nicht berücksichtigt und im Weiteren ebenfalls nicht betrachtet, sind die Sicherheitsobjekttypen, die sich aus den Schutzzielen ergeben, die in Verbindung mit den betrieblichen Objekten `Buchhaltung` und `KV` modelliert wurden. Konkret sind dies die Empfangsvertraulichkeit `Vt.T(E)[12.2]`, die Nichtabstreitbarkeit des Empfangs `Na.T(E)[21.2]` sowie die Transaktionsverbindlichkeit `Vb.T[22]`. Die Gründe hierfür bestehen in der definierten Systemabgrenzung, die sich ausschließlich auf die Betrachtung der betrieblichen Objekte `Annahme` und `Or-`

thopädie konzentriert. Alle weiteren diesbezüglichen SOT werden im anschließenden Modellierungsschritt zu Sicherheitsobjekten verfeinert.

9.5.2. Präzisierung der Sicherheitsobjekttypen

Mit der Überarbeitung der initialen Modellschemata einher geht im Szenario auch die Berücksichtigung der für die Unterstützung durch ein Anwendungssystem sicherheitsrelevanten VOT. Im Hinblick auf die Sicherheitsmodellierung führt dies potentiell dazu, dass Sicherheitskontexte, die an nicht zu automatisierenden Objekttypen des VOS modelliert wurden, aus der weiteren Betrachtung entfallen. Im Szenario MVZ ist dies zum Beispiel bei der Transaktion V:Patienteninformation der Fall, die nicht automatisierbar ist und daher nicht in dem zu entwickelnden Anwendungssystem implementiert wird. Der im Anwendungsmodell modellierte Sicherheitsobjekttyp SOT.ÜS(S)[10] ist daher im Rahmen der Überarbeitung von KOS und VOS nicht weiter zu berücksichtigen. Alle anderen Schutzziele sind im Szenario hingegen weiterhin von Relevanz.

9.5.2.1. Integration der Sicherheitskontexte

Neben der Spezifikation und Zuordnung von Attributen und Operatoren im Rahmen der Überarbeitung von KOS und VOS, findet auch ein Konsolidierungsprozess der Modellelemente statt, der inhaltlich überlappende KOT bzw. stets gemeinsam durchzuführende VOT jeweils zu einem KOT bzw. VOT zusammenfasst. Diese Aktionen sind vor allem im Hinblick auf die Referenzbeziehungen der Sicherheitsobjekttypen zu beachten. Das allgemeine Attribut referenz ist in diesem Zusammenhang zum einen in Bezug auf die den VOT zugewiesenen Attribute und Operatoren zu präzisieren, zum anderen sind die Konsolidierungsschritte inhaltlich nachzuvollziehen, sodass die referenzierten Attribute bzw. Operatoren der SOT die fachlichen Sicherheitsanforderungen semantisch korrekt widerspiegeln. Hinsichtlich des Modellierungsvorgehens hat sich diesbezüglich bewährt, in einem ersten Schritt den Konsolidierungsprozess durch die Aggregation der Sicherheitskontexte der beteiligten Objekttypen abzubilden. Im Anschluss ist dann die resultierende Menge an Sicherheitsobjekten in Bezug auf die Referenzbeziehungen zu präzisieren.

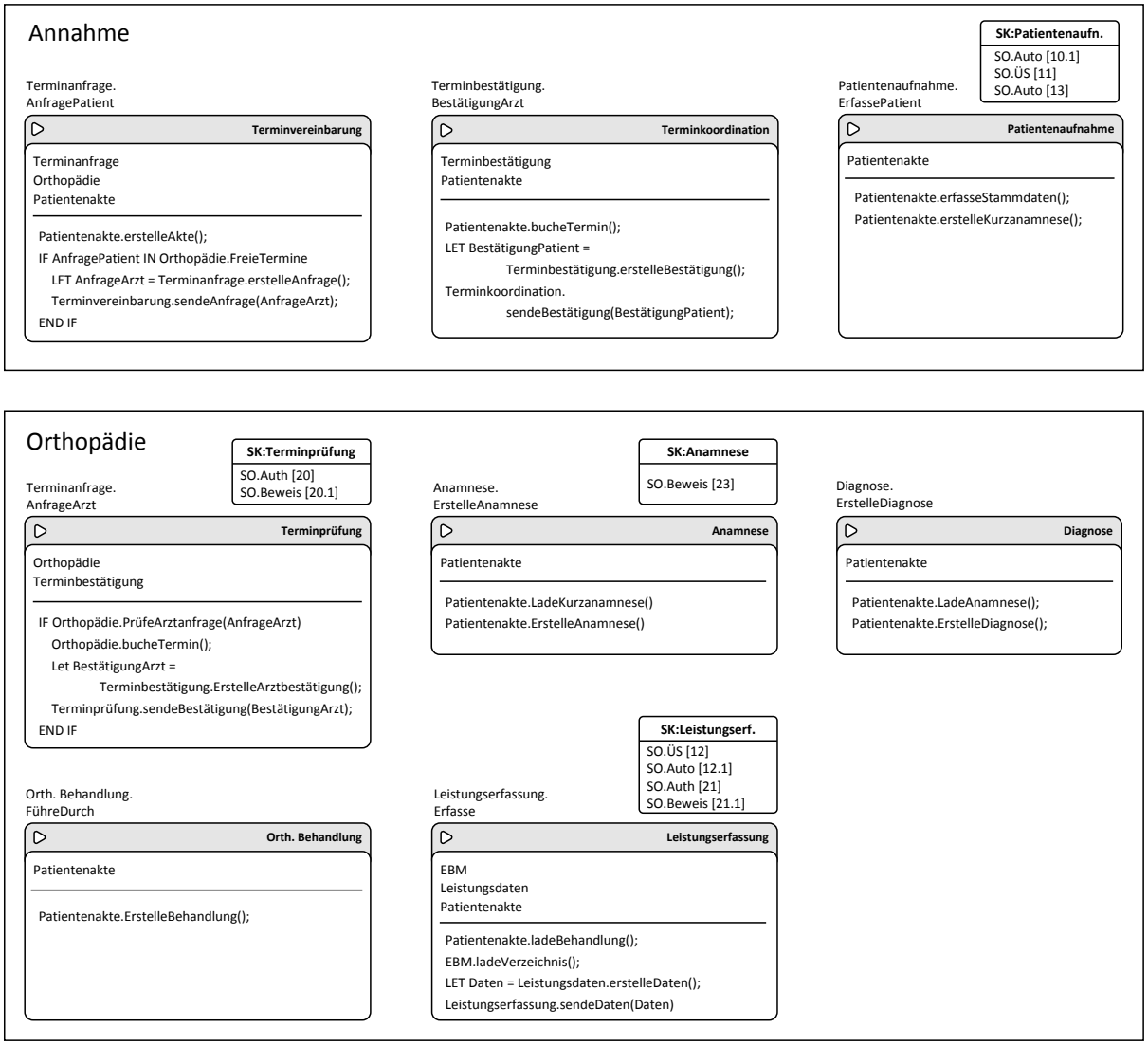

Abbildung 66: Szenario MVZ - Sicherheitserweitertes VOS (überarbeitet)

In der Abbildung werden die durch die Überarbeitung neu erstellten Sicherheitskontexte in gleicher Weise wie bei der initialen Ableitung dargestellt. Als Bestandteile werden jedoch nicht mehr Sicherheitsobjekttypen geführt, sondern konkrete Sicherheitsobjekte, die durch die Ausprägung ihrer Attribute die fachlichen Sicherheitsanforderungen widerspiegeln. Auf die Angabe der Bezugsparameter kann in der Darstellung verzichtet werden, da diese in der textuellen Notation durch das Attribut `referenz` präzisiert werden. Im folgenden Abschnitt werden die resultierenden Sicherheitsobjekte im Detail beschrieben.

9.5.2.2. Spezifikation der fachlichen Sicherheitsanforderungen

Die Darstellung der Sicherheitsobjekte erfolgt neben ihrer grafischen Referenzierung im VOS in Form einer allgemeinen XML-Notation, die im Folgenden anhand der modellierten SO des Szenarios MVZ vorgestellt wird.

Annahme

Die VOT `>Patienteninformation` und `Kurzanamnese>` wurden zu dem VOT `Patienten-aufnahme` zusammengefasst, das sowohl die Stammdaten des Patienten erfasst als auch dessen Kurzanamnese erstellt. Durch die Zusammenfassung bedingt, werden auch die Sicherheitskontexte der ursprünglichen VOT aggregiert und an das VOT angepasst. Der `SOT.Auto(E)[10.1]` bezieht sich dann auf den Operator zur Erfassung der Patienteninformation, `SOT.Auto(V)[13]` auf die Erstellung der Kurzanamnese sowie `SOT.ÜS(S)[11]` auf die Übertragungssicherung der erstellten Kurzanamnese.

```
<SK name="Patientenaufnahme">
    <SO.Auto name="10.1">
          <referenz> Patientenakte.erfasseStammdaten </referenz>
          <prüfung> PRE </prüfung>
          <privileg> rolle = Rezeptionist </privileg>
          <bedingung> </bedingung>
          <operation> EXECUTE </operation>
    </SO.Auto>

    <SO.Auto name="13">
          <referenz> Patientenakte.erstelleKurzanamnese </referenz>
          <prüfung> PRE </prüfung>
          <privileg> rolle = Arzthelfer </privileg>
          <bedingung> </bedingung>
          <operation> EXECUTE </operation>
    </SO.Auto>

    <SO.ÜS name="11">
          <referenz> Patientenaufnahme.sendeKurzanamnese </referenz>
          <prüfung> PRE </prüfung>
    </SO.ÜS>
</SK>
```

Quelltext 10: Szenario MVZ - Sicherheitskontext „Annahme“

Die spezifizierten Sicherheitsobjekte besagen, dass die Operatoren zur Erfassung der Stammdaten sowie zur Erstellung der Kurzanamnese nur durch Entitäten in den jeweils angegebenen Rollen erfolgen darf. Dies entspricht den fachlichen Sicherheitsanforderungen, die aus den Schutzzielen der Empfangsvertraulichkeit sowie Vorgangsvertraulichkeit abzuleiten sind. Die abschließende Übermittlung der Kurzanamnese ist weiterhin gegen unbefugte Kenntnisnahme abzusichern.

Die Präzisierung der initialen fachlichen Sicherheitsanforderungen spiegelt sich im Kern in der Ausprägung des Attributs `referenz` wider. Sind im ersten Schritt die Anforderungen noch vergleichsweise unspezifisch auf nicht genau definierte Teillösungsverfahren eines VOT bezogen, werden diese im zweiten Schritt auf konkrete Operatoren des VOT transformiert. Im Beispiel sind hierbei auch die Beziehungen zum KOS erkennbar, die durch die Referenzierung der Operatoren `erfasseStammdaten` und `erstelleKurzanamnese` des konzeptuellen Objekttyps `Patientenakte` verdeutlicht werden. Es gilt zu beachten, dass die Entscheidung, welcher Objekttyp die spezifizierten Sicherheitsanforderungen aus technischer Sicht letztendlich umzusetzen hat, an dieser Stelle noch nicht getroffen wird. Dies kann erst zu einem späteren Zeitpunkt erfolgen, an dem die vollständige Architektur des zu entwickelnden Anwendungssystems definiert ist. Die fachliche Spezifikation der Sicherheitsanforderungen im VOS nach SOMsec alleine trifft hierzu somit keine Aussage.

Orthopädie

Die VOT `>Arztanfrage` und `Arztbestätigung>` wurden zu dem VOT `Terminprüfung` aggregiert. Die Referenzen der initial modellierten Sicherheitsobjekttypen `SOT.Beweis(S)[20.1]` und `SOT.Auth(S)[20]` sind daher entsprechend zu präzisieren. In Bezug auf die Anforderung der Beweissicherung wird hierbei der Bezugsparameter des SOT.Beweis als Indikator für die Ausprägung des Attributes `beweistyp` genutzt. Der Parameter `S` wird dabei in den Typ `EOS` überführt, `E` wird auf den Attributwert `EOR` abgebildet sowie `V` auf den Wert `LOG`. Es ergeben sich die folgenden Sicherheitsobjekte.

```
<SK name="Terminprüfung">
    <SO.Beweis name="20.1">
          <referenz> Terminprüfung.sendeBestätigung </referenz>
          <prüfung> POST </prüfung>
          <beweistyp> EOS </beweistyp>
    </SO.Beweis>
```

```
    <SO.Auth name="20">
          <referenz> Terminprüfung.sendeBestätigung </referenz>
          <prüfung> PRE </prüfung>
    </SO.Auth>
</SK>
```

Quelltext 11: Szenario MVZ - Sicherheitskontext „Terminprüfung“

Bevor die Terminbestätigung durch das System erfolgen kann, muss diese zum Beispiel durch eine valide Signatur als verbindlich gekennzeichnet werden. Weiterhin ist gemäß der spezifizierten Sicherheitsanforderung nach der Durchführung des Sendeoperators ein rechtsverbindlicher Beweis über den Vorgang im System vorzuhalten.

Die Erstellung einer Anamnese ist im Geschäftsprozessmodell als vorgangsverbindlich annotiert, der entsprechend abgeleitete VOT war zudem nicht Bestandteil eines Konsolidierungsprozesses. Somit ergibt sich der folgende Sicherheitskontext.

```
<SK name="Anamnese">
    <SO.Beweis name="23">
          <referenz> Patientenakte.erstelleAnamnese </referenz>
          <prüfung> POST </prüfung>
          <beweistyp> LOG </beweistyp>
    </SO.Beweis>
</SK>
```

Quelltext 12: Szenario MVZ - Sicherheitskontext „Anamnese“

Gemäß Sicherheitsspezifikation ist nach der Erstellung der Anamnese diesbezüglich ein rechtsverbindlicher Beweis vorzuhalten, in dem zum Beispiel auch der Zeitpunkt oder der Autor der Anamnese erfasst werden kann. Die Sicherheitsanforderung selbst referenziert hierbei keine bestimmte Identität, da dies bedeuten würde, dass der zu erbringende Beweis immer dieser Identität zuzuordnen ist. Die fachliche Sicherheitsspezifikation trifft somit keine Aussagen in Bezug auf die Inhalte des zu erbringenden Beweises.

Hinsichtlich der Leistungserfassung werden auf Geschäftsprozessebene diverse Schutzziele definiert. Der folgende Sicherheitskontext kann abgeleitet werden.

```
<SK name="Leistungserfassung">
    <SO.Auth name="21">
          <referenz> Leistungserfassung.sendeDaten </referenz>
          <prüfung> PRE </prüfung>
    </SO.Auth>

    <SO.Beweis name="21.1">
          <referenz> Leistungserfassung.sendeDaten </referenz>
          <prüfung> POST </prüfung>
          <beweistyp> EOS </beweistyp>
    </SO.Beweis>

    <SO.ÜS name="12">
          <referenz> Leistungserfassung.sendeDaten </referenz>
          <prüfung> PRE </prüfung>
    </SO.ÜS>

    <SO.Auto name="12.1">
          <referenz> Leistungserfassung.sendeDaten </referenz>
          <prüfung> PRE </prüfung>
          <privileg> rolle = Chefarzt </privileg>
          <bedingung> </bedingung>
          <operation> EXECUTE </operation>
    </SO.Auto>
</SK>
```

Quelltext 13: Szenario MVZ - Sicherheitskontext „Leistungserfassung“

Die modellierten Schutzziele auf Geschäftsprozessebene beziehen sich in diesem Fall vollständig auf die Sendeaufgabe zur Übermittlung der Leistungsdaten, die im VOS als Teillösungsverfahren durch den Operator `sendeDaten` spezifiziert wird. Um die Verbindlichkeit zu gewährleisten, ist sowohl ein Beweis des Versands als auch die verbindliche Übermittlung der Leistungsdaten sicherzustellen. Weiterhin sind nur autorisierte Identitäten berechtigt die Daten zu versenden, deren Übertragung an das externe System der Buchhaltung gegen unautorisierten Zugriff abzusichern ist.

9.5.3. Erzeugte Modellinformation im Sicherheitsobjektschema

Durch die aggregierte Betrachtung aller im Modell spezifizierten Sicherheitskontexte ist eine umfassende fachliche Darstellung relevanter Sicherheitsanforderungen für das zu entwickelnde Anwendungssystem möglich. Gegliedert nach dem Typ der spezifizierten Sicherheitsobjekte ergibt sich eine Übersicht der fachlichen Anforderungen, die dann durch entsprechende Komponenten auf der Ebene der technischen Anwendungssystemspezifikation umzusetzen sind. In SOMsec wird diese Sicht als **Sicherheitsobjektschema** (SOS) bezeichnet.

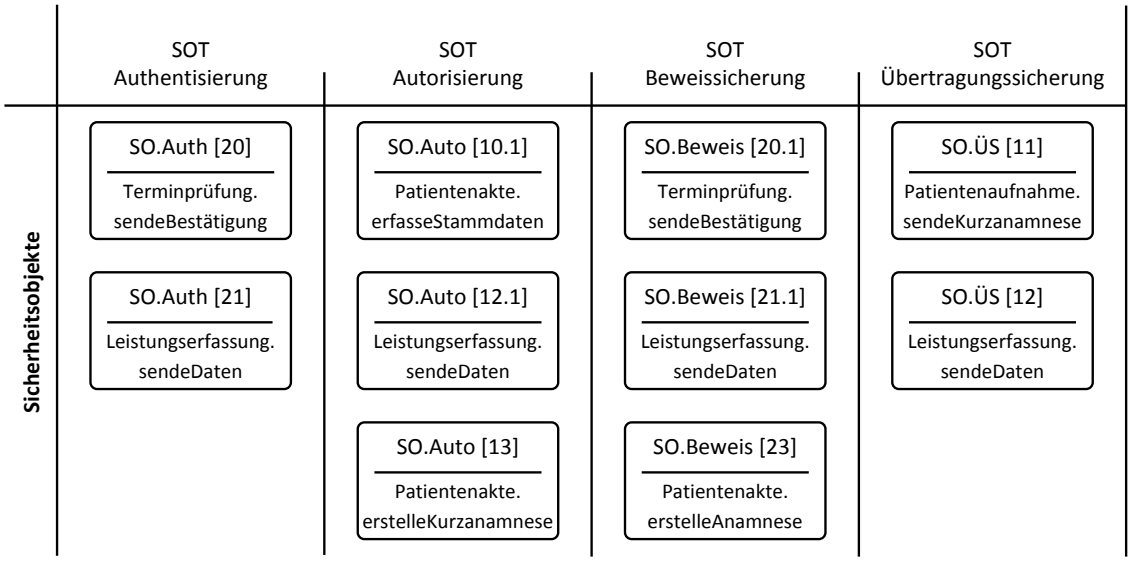

Abbildung 67: Szenario MVZ - Sicherheitsobjektschema

Das Sicherheitsobjektschema umfasst zehn Sicherheitsobjekte, die durch ihre jeweilige Bezeichnung und Referenz in Kurzform dargestellt werden. Im Rahmen des vorgestellten Szenarios ergeben sich im Detail drei Autorisierungs- und Beweisanforderungen für modellierte Transaktionen und Aufgaben sowie zwei Authentisierungs- und Übertragungssicherungsanforderungen. Diese zusammenfassende Sicherheitsspezifikation des Anwendungssystems ergibt sich gemäß SOMsec aus der Modellierung von 14 Schutzzielen auf Geschäftsprozessebene. Die geringere Anzahl der Sicherheitsobjekte resultiert dabei einerseits aus der funktionalen Abgrenzung des Anwendungssystems, andererseits aus der Berücksichtigung der modellierten Automatisierungsgrade von Aufgaben bzw. Transaktionen.

Durch die Referenzen der Sicherheitsobjekttypen auf Modellelemente des VOS, und damit indirekt auf Elemente des KOS, ergibt sich eine direkte Integrationsmöglichkeit des Sicherheitsobjektschemas in die fachliche Spezifikation des Anwendungssystems. Es dient sodann

als Ausgangspunkt für die sicherheitsorientierte Spezifikation des Anwendungssystems auf technischer Ebene. Zu jedem Sicherheitsobjekt sind entsprechende technische Komponenten zu implementieren, die die jeweiligen Anforderungen abbilden können. Die initiale Parametrisierung dieser Komponenten ergibt sich dabei aus den weiteren Attributen der Sicherheitsobjekte, zum Beispiel durch die Angabe von Identitäten zur Zugriffskontrolle. In Kapitel 10 wird dieser Aspekt von SOMsec im Detail beschrieben.

10. Software-technische Sicherheitsspezifikation

Auf der Ebene des software-technischen Spezifikation eines Anwendungssystems wird die Struktur des Anwendungssystems im Sinne einer Software-Architektur definiert. Hierzu wird der fachliche Entwurf im Hinblick auf die Implementierung unter Beachtung eines Software-Architekturmodells weiter detailliert [Mali97, 7]. In der Methodik von SOMsec kommt diesbezüglich analog zu SOM das objektorientierte Software-Architekturmodell (ooAM) nach AMBERG[133] zum Einsatz. Im Rahmen der Sicherheitsbetrachtung ist in diesem Schritt zu prüfen, auf welche Weise die modellierten Sicherheitsanforderungen der fachlichen Spezifikation in den software-technischen Entwurf des Anwendungssystems und somit in das ooAM zu überführen sind.

Kapitel 10.1 gibt hierzu einen einführenden Überblick der konzeptuellen Grundlagen des ooAM sowie entsprechender sicherheitsbezogener Erweiterungen in Form von technischen Sicherheitsobjekttypen. Kapitel 10.2 beschreibt darauf aufbauend das Vorgehen, das die Ableitung der technischen Sicherheitsfunktionalität aus der fachlichen Sicherheitsspezifikation steuert. Im Anschluss werden die dargestellten theoretischen Grundlagen anhand des Szenarios MVZ in Kapitel 10.3 am Beispiel verdeutlicht. Kapitel 10.4 beschließt die Ausführungen mit einer Darstellung ableitbarer technischer Konfigurationsparameter im Bereich der Zugriffskontrolle.

10.1. Technische Sicherheitsfunktionalität

Die Berücksichtigung von Sicherheitsaspekten im Rahmen des software-technischen Entwurfs bezieht sich auf die Identifikation und Umsetzung technischer Sicherheitsfunktionalität[134], die die fachlichen Sicherheitsanforderungen eines Anwendungssystems auf technischer Ebene abbildet. Unter technischer Sicherheitsfunktionalität wird dabei anwendungsneutrale Funktionalität verstanden, die in SOMsec auf Basis des Software-Architekturmodells in den Prozess der software-technischen Spezifikation integriert wird.

---

[133] Vgl. hierzu [Ambe93].

[134] Der Begriff der technischen Sicherheitsfunktionalität orientiert sich an der Terminologie des ooAM. In Bezug auf die bisherigen Ausführungen ist er inhaltlich gleichzusetzen mit dem Begriff der technischen Sicherheitsmaßnahme (vgl. Kapitel 5.3.4.2) und wird in Bezug auf die Anwendungssystementwicklung im weiteren Verlauf synonym verwendet.

10.1.1. Konzeptuelle Grundlagen

Die sicherheitsrelevanten Inhalte der Modellierungsstufe des software-technischen Entwurfs können anhand des Referenzmodells betrieblicher Informationssicherheit differenziert werden. Auf Basis der fachlichen Sicherheitsanforderungen eines Anwendungssystems, die als Sicherheitsziele auf Ressourcenebene aus den Schutzzielen der Geschäftsprozessmodellierung abgeleitet werden, sind entsprechend unterstützende Sicherheitsfunktionen zu spezifizieren. Hierbei erfolgt im Referenzmodell ein Übergang von einer sicherheitszielorientierten Betrachtung hin zu einer sicherheitsartefaktorientierten Sichtweise. Gesucht sind somit diejenigen Sicherheitsmaßnahmen im Sinne von Sicherheitsartefakten, die in Bezug auf ein Anwendungssystem als Bezugsobjekt die modellierten Sicherheitsanforderungen abbilden und umsetzen können. Dieser Übergang charakterisiert die bereits angesprochene Operationalisierbarkeit der non-funktionalen fachlichen Sicherheitsanforderungen[135], die auf diese Weise durch SOMsec unterstützt wird.

Die Grundlage für die Eingliederung der Sicherheitsmaßnahmen bildet das Software-Architekturmodell ooAM, das die entsprechenden Softwarekomponenten eines Anwendungssystems zueinander in Beziehung setzt. Im folgenden Abschnitt wird dieser Ansatz kurz vorgestellt.

10.1.2. Das objektorientierte Software-Architekturmodell

Das ooAM gliedert die Funktionalität eines Anwendungssystems in fachliche, technische und Basisfunktionalität, deren Interaktion letztendlich den Betrieb eines Anwendungssystems ermöglicht [Amb93, 33f].

[135] Vgl. hierzu Kapitel 9.3.2.

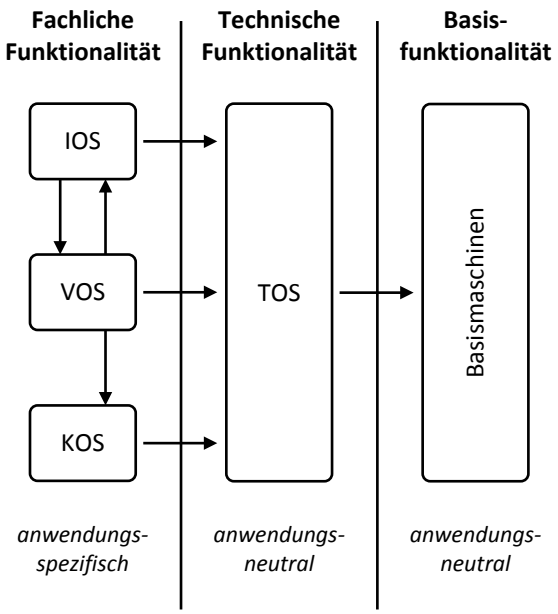

Abbildung 68: Struktur des ooAM (nach [Amb93, 37])[136]

Die **fachlicher Funktionalität** beschreibt die anwendungsspezifische Funktionalität eines Anwendungssystems, die sich aus der fachlichen Spezifikation des Anwendungssystems ergibt. Orthogonal zur Modellierung in SOM kann sie untergliedert werden in konzeptuelle, Vorgangs- und Schnittstellen-Funktionalität, die in Form von KOS, VOS und IOS[137] abgebildet werden können.

Unter **technischer Funktionalität** ist die anwendungsneutrale Funktionalität zu verstehen, auf Basis derer die fachliche Funktionalität eines Anwendungssystems realisiert wird. Im ooAM wird die technische Funktionalität durch das technische Objektschema (TOS) abgebildet, das in Form von technischen Objekttypen und deren Eigenschaften spezifiziert wird [Ambe93, 130].

Die **Basisfunktionalität** bildet schließlich die anwendungsneutrale Grundlage für die Realisierung der technischen Funktionalität. Sie umfasst grundlegende Komponenten der Softwareentwicklung, wie zum Beispiel Datenbanksysteme oder Programmiersprachen. Die Ba-

[136] Die dargestellten Pfeile in Abbildung 68 symbolisieren die Schnittstellen bzw. Zugriffsbeziehungen zwischen den Komponenten des ooAM. Für eine detaillierte Erläuterung sei diesbezüglich auf [Ambe93, 36ff] verwiesen.

[137] Das Interface-Objektschema (IOS) beschreibt die Anforderungen an Schnittstellen eines Anwendungssystems, die aus den betrieblichen Vorgängen ableitbar sind. Hierbei werden Schnittstellen zu Personen oder anderen Anwendungssystemen unterschieden [Ambe93, 35]. Die Spezifikation des IOS wird im weiteren Verlauf der Arbeit nicht berücksichtigt.

sisfunktionalität ist im ooAM konzeptuell dem TOS zugeordnet, sie wird jedoch nicht explizit modelliert [Amb93, 130].

Das Software-Architekturmodell kommt im Rahmen der software-technischen Spezifikation des Anwendungssystems zum Einsatz. In diesem Rahmen gilt die Zielsetzung, ein möglichst basismaschinenunabhängiges Modell des Anwendungssystems zu erstellen, das das fachliche Anwendungsmodell um softwarespezifische Faktoren erweitert [Mali97, 73]. Diese Modell bildet dann die Grundlage für die Implementierung des Anwendungssystems unter Nutzung der jeweiligen Basismaschinen.

10.1.3. Technische Sicherheitsfunktionalität im ooAM

In Bezug auf Anwendungssysteme wird die technische Sicherheitsfunktionalität durch technische Sicherheitsmaßnahmen abgebildet, wie sie in Kapitel 5.5 vorgestellt wurden. Der Begriff der technischen Sicherheitsmaßnahme ist demnach differenzierbar in Sicherheitsdienste und Sicherheitsmechanismen sowie eine zu Grunde liegende Sicherheitsarchitektur. Letztere beschreibt in Bezug auf Anwendungssysteme die Sicherheitsdienste die notwendig sind, um die geforderten Sicherheitseigenschaften des Systems zu realisieren[138].

In Bezug auf das ooAM ist die technische Sicherheitsfunktionalität dem TOS zuzuordnen. Aus Sicht der anwendungsspezifischen fachlichen Funktionalität werden entsprechende Funktionen in Form von technischen Sicherheitsdiensten genutzt, die ihrerseits wiederum durch Sicherheitsmechanismen auf der Grundlage der Basisfunktionalität erbracht werden.

[138] Vgl. Kapitel 5.3.4.3.

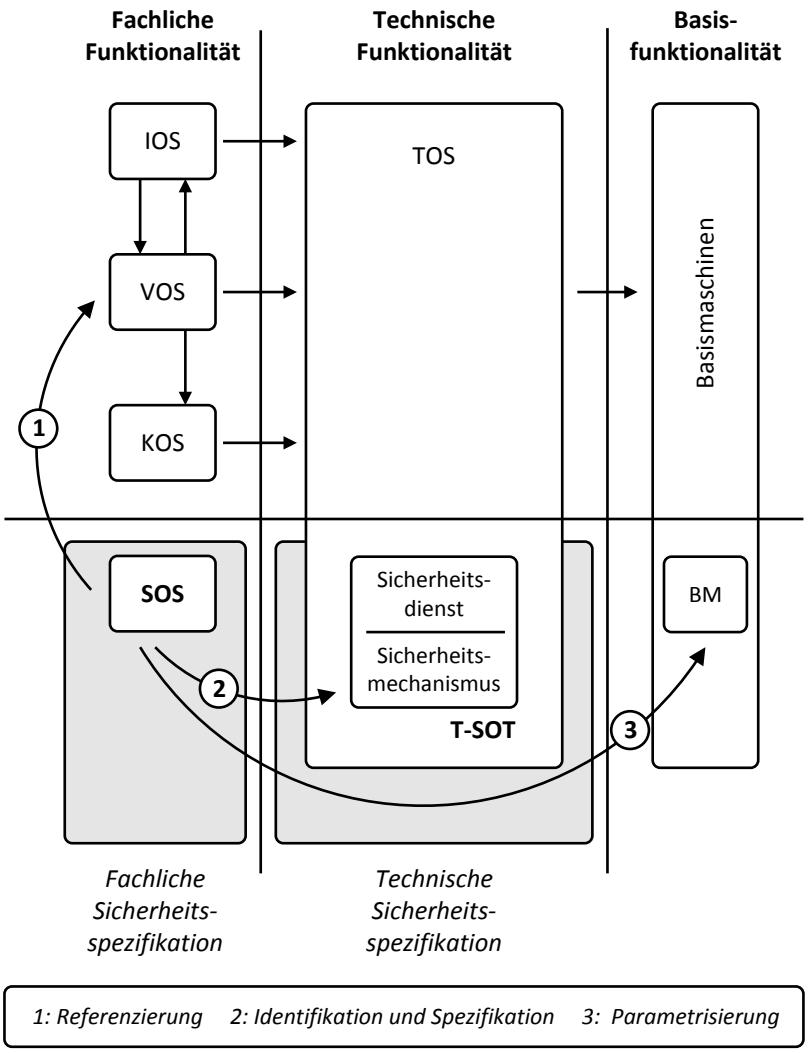

Abbildung 69: Technische Sicherheitsfunktionalität im ooAM

Das SOS bildet in diesem Zusammenhang das Bindeglied zwischen der fachlichen Funktionalität und der technischen Sicherheitsspezifikation. Für die Identifikation benötigter Sicherheitsfunktionen sind jedem fachlichen Sicherheitsobjekttyp entsprechende Sicherheitsdienste zugeordnet. Über das Attribut `referenz` eines modellierten Sicherheitsobjekts ist dann die Beziehung zwischen Elementen des VOS und den zugehörigen Sicherheitsdiensten herzustellen. Auf diese Weise können aus Anwendungssicht benötigte technische Sicherheitsfunktionen aus der fachlichen Modellierung initial abgeleitet und auch entsprechenden Operatoren einzelner VOT zugeordnet werden. Zudem ist unter bestimmten Umständen auch eine Parametrisierung der für die Sicherheitsdienste relevanten Basismaschinen (BM) auf der Grundlage der fachlichen Anforderungsdefinition möglich. In Kapitel 10.5 wird dieser Sachverhalt anhand des Szenarios MVZ näher beschrieben. Aus Modellierungssicht wird die technische

Sicherheitsfunktionalität in SOMsec durch **technische Sicherheitsobjekttypen** (T-SOT) abgebildet, die dem TOS zugeordnet sind. Der folgende Abschnitt erläutert dieses Konzept.

10.2. Technische Sicherheitsobjekttypen

Technische Sicherheitsobjekttypen stellen aus Sicht des Anwendungssystems anwendungsneutrale Funktionen bereit, durch deren Nutzung die spezifischen Sicherheitsanforderungen des Anwendungssystems abgedeckt werden können. Aus dem Blickwinkel der Modellierung können sie sowohl aus Außen- wie auch aus Innensicht betrachtet werden. Beide Sichtweisen korrespondieren dabei konzeptuell mit dem dargestellten Zusammenhang zwischen Sicherheitsdienst und Sicherheitsmechanismus[139].

10.2.1. Sichten auf technische Sicherheitsobjekttypen

Die **Außensicht** eines T-SOT kann im Sinne der Spezifikation eines anwendungsneutralen Sicherheitsdienstes interpretiert werden. Sie definiert die Schnittstelle, die ein T-SOT der fachlichen Anwendungsfunktionalität zur Verfügung stellt. In SOMsec wird diese Schnittstelle in Form von abstrakten Methoden definiert, die dann durch anwendungsspezifische Elemente des VOS genutzt werden können. Die **Innensicht** eines T-SOT entspricht dem Verständnis eines Sicherheitsmechanismus, der die Erbringung des Sicherheitsdienstes auf Grundlage der Basisfunktionalität ermöglicht. Die Innensicht eines T-SOT charakterisiert in SOMsec die Art und Weise der Implementierung der technischen Sicherheitsfunktionalität, zum Beispiel im Hinblick auf die Integration in bestehende Systemlandschaften.

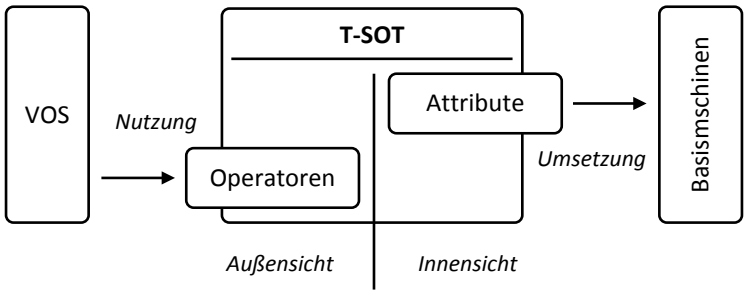

Abbildung 70: Konzept des technischen Sicherheitsobjekttyps

[139] Vgl. Kapitel 5.3.4.2.

Die Außensicht eine T-SOT spezifiziert somit, welche technische Funktionalität im Sinne eines Lösungsverfahrens für fachliche Sicherheitsanforderungen im Hinblick auf das Anwendungssystem zu erbringen ist. Die Innensicht charakterisiert, auf welche Art und Weise eine entsprechende Umsetzung zu erfolgen hat. Im Sinne der Objektorientierung wird die Außensicht durch die öffentlichen Operatoren eines T-SOT dargestellt, die Innensicht durch die Ausprägung der entsprechenden Attribute. Operatoren und Attribute für die in SOMsec genutzten T-SOT werden in Kapitel 10.2.3 dargestellt.

10.2.2. Relevanz für die Modellierung

Für den Modellierer ist sowohl die Betrachtung der Außen- als auch die der Innensicht von Relevanz. Aus Sicht des Anwendungssystems wird durch die konzeptuellen Beziehung eines T-SOT zu fachlichen Sicherheitsobjekttypen die Identifikation der benötigten Außensicht charakterisiert. Die Betrachtung der Innensicht ist dann ausschlaggebend dafür, ob ein T-SOT in der jeweiligen Ausprägung im Kontext bestehender Strukturen für die Umsetzung der technischen Funktionalität in Frage kommt. Bei bestehen Strukturen, zum Beispiel bereits existenten Authentifizierungsdiensten in der Systemlandschaft, ist die Innensicht somit auf Kompatibilität zu diesen Strukturen zu evaluieren. Bei neu zu erstellender Sicherheitsfunktionalität hingegen charakterisiert die Innensicht die Anforderungen, die in Bezug auf die Umsetzung auf Grundlage der Basisfunktionalität erfüllt werden müssen.

Die Trennung der Betrachtung in Außen- und Innensicht von T-SOT beinhaltet aus Modellierungssicht zudem einen weiteren Vorteil, indem die Nutzungsschnittstelle von der Realisierungsform logisch getrennt wird. Durch diese Strukturform ist die technische Implementierung eines T-SOT unabhängig und kann flexibel modifiziert oder substituiert werden. Aus Modellierungssicht trägt dies zur Stabilität und Konsistenz der Modellsysteme des softwaretechnischen Entwurfs bei.

10.2.3. Ableitung technischer Sicherheitsobjekttypen

Die Grundlage für die inhaltliche Ableitung der technischen Sicherheitsobjekttypen stellt das Konzept der Sicherheitsgrundfunktionen dar. Sowohl die fachlichen Sicherheitsanforderungen als auch technische Sicherheitsfunktionalität kann anhand dieser Systematik differenziert werden. Für jeden Sicherheitsobjekttyp in SOMsec sind somit technische Sicherheitsfunktionen spezifizierbar, die dann durch die Außensicht eines T-SOT dargestellt werden. Diese Be-

schreibung der Außensicht ist in SOMsec gleichzeitig charakterisierend für den Typ des T-SOT und wird im folgenden Abschnitt erläutert. Im zweiten Teil dieses Abschnitts erfolgt darauf aufbauend eine abschließende Betrachtung möglicher Attributdefinitionen, die die entsprechende Innensicht der technischen Sicherheitsobjekttypen beschreiben.

10.2.3.1. Spezifikation der Außensicht

Anhand der in SOMsec genutzten fachlichen Sicherheitsobjekttypen, werden in den folgenden Abschnitten die Ableitungsbeziehungen zu entsprechenden technischen Sicherheitsobjekttypen sowie deren Schnittstellendefinition vorgestellt. Die Ableitungsbeziehung bildet dabei den Übergang zwischen der zweiten und dritten Modellierungsstufe von SOMsec[140]. Die Benennung der Operatoren der Schnittstellendefinition folgt dabei dem Ziel, die anwendungsneutrale technische Funktionalität des verkörperten Sicherheitsdienstes für die Modellnutzung möglichst eingängig darzustellen. Aus diesem Grund werden stark abstrahierende Bezeichnungen genutzt, die keinen Anspruch auf eine umfassende Spezifikation der Schnittstellen im technischen Sinn erheben.

SOT Authentisierung - T-SOT Zertifizierung

Die modellierten Sicherheitsanforderungen der Authentisierung sind abgeleitet aus dem Schutzziel der Transaktionsverbindlichkeit und beziehen sich auf die Authentisierung der im Rahmen einer Transaktion zu übertragenden Informationen. Dies bedeutet, dass die Information eindeutig dem jeweiligen Absender zuzuordnen ist und dass diese Zuordnung durch den Empfänger verifizierbar ist. In Bezug auf die technische Umsetzung ist die Funktionalität der **Zertifizierung**[141] ein Lösungsverfahren, durch dessen Nutzung diesen Anforderungen entsprochen werden kann.

Aus Anwendungssicht sind für die Nutzung dieser Funktionalität zwei grundlegende Operatoren relevant. Zum einen ist dies das Signieren einer ausgehenden Nachricht (`NachrichtSignieren`), zum anderen die Verifikation der Signatur einer eingehenden Nachricht (`Signatur-Validieren`). Beide Operatoren bilden die Außensicht des T-SOT Zertifizierung.

[140] Da die Ableitungsbeziehungen anhand der Sicherheitsgrundfunktionen ausgestaltet werden und zudem inhaltlich einfach nachvollziehbar sind, wird an dieser Stelle auf die Angabe eines Beziehungs-Meta-Modells verzichtet.

[141] Zertifizierung wird im Folgenden als stellvertretende Bezeichnung für Sicherheitsmaßnahmen verwendet, die auf der Grundlage des Konzepts der digitalen Signatur basieren (vgl. hierzu Kapitel 5.5.1) Diese Bezeichnung wird umfassend verwendet, eine differenzierte Betrachtung, zum Beispiel durch die Abgrenzung des Konzepts der elektronischen Signatur, erfolgt nicht.

SOT Übertragungssicherung - T-SOT Verschlüsselung

Die Übertragungssicherung bezieht sich auf die Vertraulichkeit der zu übertragenenden Information. Nur autorisierte Identitäten dürfen während des Übertragungsvorgangs Zugriff auf die Information erhalten. Aus technischer Sicht sind Sicherheitsmaßnahmen der **Verschlüsselung** somit entsprechende Lösungsverfahren, die diese Anforderung umsetzen können.

Die Außensicht des T-SOT Verschlüsselung wird durch Operatoren zur Ver- und Entschlüsselung von Informationen gebildet. Sie werden in SOMsec als `NachrichtVerschlüsseln` sowie `NachrichtEntschlüsseln` bezeichnet.

SOT Beweissicherung - T-SOT Protokollierung

Die fachliche Anforderung der Beweissicherung bezieht sich auf die revisionssichere Speicherung von Beweisen, die die Durchführung eines Vorgangs ex post für Dritte nachvollziehbar machen. Aus technischer Perspektive sind Sicherheitsmaßnahmen der **Protokollierung** anzuwenden, um diese Anforderungen zu erfüllen.

Die Außensicht des T-SOT Protokollierung bietet Dienste zur Erzeugung und zur Validierung von Beweisen an. Die entsprechenden Operatoren werden als `BeweisErzeugen` und `BeweisValidieren` bezeichnet.

SOT Autorisierung - T-SOT Zugriffskontrolle

Autorisierungsanforderungen beziehen sich auf die Kontrolle von Nutzungsbefugnissen in einem Anwendungssystem. Nur autorisierte Identitäten dürfen befähigt sein, entsprechende Aktionen durchzuführen. Die technische Sicherheitsfunktionalität wird in diesem Zusammenhang als **Zugriffskontrolle** bezeichnet, anhand derer die entsprechenden Zugriffsstrukturen in einem Anwendungssystem abzubilden sind.

Technische Maßnahmen der Zugriffskontrolle können aus Sicht des Anwendungssystems durch einen Operator zur Überprüfung der Berechtigungen des jeweils aktuellen Nutzers charakterisiert werden. In SOMsec wird die resultierende Außensicht des T-SOT Zugriffskontrolle durch den Operator `BerechtigungPrüfen` spezifiziert.

10.2.3.2. Spezifikation der Innensicht

Die Spezifikation der Innensicht eines T-SOT erfolgt in SOMsec anhand von Attributen, die sich primär auf die genutzten Verfahren und weitere Aspekte der technischen Umsetzung der Sicherheitsfunktionalität beziehen. Auf Grund der Unterschiedlichkeit der technischen Ansätze, ist es in diesem Zusammenhang nicht möglich ein übergreifend einheitliches Schema an Attributdefinitionen vorzugeben, anhand dessen eine differenzierte Betrachtung und Auswahl der möglichen Umsetzungen von Sicherheitsfunktionen durch den Modellierer erfolgen könnte. In SOMsec werden daher exemplarisch die zwei abstrahierenden Attribute „Ansatz“ und „Implementierung“ genutzt, um die Innensicht der technischen Sicherheitsfunktionalität für den Modellierer charakterisierbar zu gestalten.

Das Attribut **Ansatz** bezieht sich auf die Bündelung technischer Konzepte zu einem allgemeinen Lösungsverfahren, das aus fachlicher und logischer Sicht für die Realisierung eines T-SOT herangezogen werden kann. Das Attribut **Implementierung** beschreibt dann die Umsetzungsform eines Lösungsverfahren, wie sie im Kontext der jeweiligen Anwendungsentwicklung zu erfolgen hat. Die folgende Abbildung zeigt mögliche Attributausprägungen der vier technischen Sicherheitsobjekttypen exemplarisch auf.

T-SOT	Ansatz	Implementierung
Zertifizierung	S/MIME	extern, PKI
Verschlüsselung	SSL	extern, Protokoll
Zugriffskontrolle	ABAC	intern, API
Protokollierung	Logdatei	intern, API

Abbildung 71: Exemplarische Ausprägungen der Innensicht eines T-SOT

Das Attribut Ansatz bezieht sich inhaltlich vornehmlich auf die in Kapitel 5.5 vorgestellten Beschreibungen der technischen Sicherheitsmechanismen. Der T-SOT Zertifizierung zum Beispiel, wird durch ein S/MIME-basiertes Verfahren zur digitalen Signierung umgesetzt. Realisiert werden sollen die entsprechenden Funktionalitäten durch die Nutzung einer PKI. Das Schlüsselwort „extern“ bezeichnet dabei die Verwendung anwendungsexterner Funktionalität aus Sicht der Basismaschine. Im Vergleich spezifiziert der T-SOT Zugriffskontrolle in

diesem Zusammenhang die Nutzung einer anwendungsinternen API (engl. *application programming interface*) zur Erzeugung einer Logdatei.

Die Auswahl konkreter Ausprägungen der Attribute obliegt dem Modellierer im Rahmen des software-technischen Entwurfs. Diese ist in der Regel jedoch stark beeinflusst durch den betrieblichen Kontext bzw. die bestehenden Systemlandschaften, in deren Rahmen die Anwendungssystementwicklung angesiedelt ist. Als Entscheidungsunterstützung für den Modellierer können diesbezüglich daher nur Heuristiken genutzt werden, die sich primär auf dessen Erfahrung stützen.

10.3. Modellierungsvorgehen

Auf Basis der Einordnung der sicherheitsrelevanten Konzepte in die Modellbildung des software-technischen Entwurfs können für die Sicherheitsmodellierung im Wesentlichen drei Vorgehensschritte abgeleitet werden.

10.3.1. Identifikation relevanter T-SOT

In einem ersten Schritt sind die in SOMsec spezifizierten Sicherheitsobjekte zu analysieren und auf entsprechende technische Sicherheitsobjekttypen abzubilden. Jede spezifizierte fachliche Sicherheitsanforderung des Anwendungssystems muss im Ergebnis durch einen T-SOT realisiert werden, um eine vollständige Absicherung gemäß der fachlichen Modellierung zu realisieren. Hierbei ist ebenfalls zu prüfen, ob die fachliche Anforderung auch unter software-technischen Aspekten weiterhin relevant sind. Ist dies nicht der Fall, so können einzelne Anforderungen auf dieser Modellierungsebene verworfen werden[142]. Durch die Referenzierung konkreter Operatoren von VOT wird durch die fachlichen Sicherheitsobjekte die Beziehung zwischen Außensicht der T-SOT und VOT hergestellt. Diese kann als Aufrufbeziehung charakterisiert werden, die weiterhin durch das Attribut `prüfung` der Sicherheitsobjekte hinsichtlich des Nutzungszeitpunktes der Sicherheitsfunktionalität präzisiert wird.

[142] Bei transaktionsbezogenen Sicherheitsanforderungen kann dies durch den Modellierer anhand der Unterscheidung von internen und externen Transaktionen erfolgen. Ein Beispiel für diesen Fall wird in den Kapiteln 10.4.1 und 10.4.2 beschrieben.

10.3.2. Spezifikation der Innensicht der T-SOT

Im Anschluss an die initiale Identifikation ist die Innensicht der spezifizierten T-SOT zu charakterisieren, sodass eine bestmögliche Integration der technischen Sicherheitsfunktionalität in das TOS sowie den Anwendungskontext ermöglicht wird. In diesem Zusammenhang sind ebenfalls redundante T-SOT zu konsolidieren, wenn sie in Bezug auf ihre Innensicht identisch sind. Durch diesen Vorgang werden mehrere fachliche Sicherheitsanforderungen mit unterschiedlichen Referenzen im VOS auf einen technischen Sicherheitsobjekttyp abgebildet. Die Metapher des Sicherheitsdienstes aus Außensicht wird auf diese Weise im Modellsystem deutlich.

10.3.3. Parametrisierung der Basisfunktionalität

Der optionale dritte Vorgehensschritt bezieht sich auf die Ableitung von Parametern aus der fachlichen Sicherheitsmodellierung, die zur Konfiguration der Basismaschinen technischer Sicherheitsfunktionalität genutzt werden können. Dieser Schritt ist jedoch nur für identitätsgebundene Sicherheitsanforderungen sinnvoll durchzuführen. In SOMsec wird daher ausschließlich die Ableitung von Konfigurationsparametern für Zugriffskontrollmechanismen einer AAI aus fachlichen Autorisierungsinformationen unterstützt. Eine diesbezügliche Erläuterung dieser Ableitungsbeziehung erfolgt auf Basis des Szenarios MVZ in Kapitel 10.5.

10.3.4. Zusammenfassung

Das Ergebnis der ersten beiden Schritte stellt eine Spezifikation derjenigen Sicherheitsfunktionalität dar, die die fachlichen Sicherheitsanforderungen des Anwendungssystems umsetzt. Die Außensicht der T-SOT steht dabei in Beziehung zu den relevanten Operatoren des VOS und spezifiziert die Aufrufbeziehungen der Sicherheitsfunktionalität aus Sicht des Anwendungssystems. Die Innensicht spiegelt die Realisierungseigenschaften der T-SOT wider und ermöglicht auf diese Weise eine Integration in bestehende Strukturen. Durch den dritten Schritt können fachliche Autorisierungsparameter schließlich zur Konfiguration konkreter technischer Sicherheitsfunktionalität genutzt werden. Auf diese Weise werden die fachlichen Sicherheitsanforderungen des Anwendungsmodells im Rahmen des software-technischen Entwurfs im TOS eines Anwendungssystems operationalisiert.

10.4. Szenario: technische Sicherheitsspezifikation

Anhand des vorgestellten Szenarios MVZ wird in den folgenden Abschnitten die Spezifikation des software-technischen Entwurfs unter Sicherheitsaspekten dargestellt. Hierbei bildet das anwendungsspezifische Sicherheitsobjektschema die Grundlage für die Ableitung relevanter technischer Sicherheitsobjekttypen. Aus Sicht des Modellierers ist gemäß den dargestellten Vorgehensschritten zu prüfen, ob, und wenn ja welche, technischen Sicherheitsobjekte notwendig sind, um die spezifizierten Anforderungen zu erfüllen. Entsprechend notwendige Annahmen über den Kontext der Systementwicklung werden in den folgenden Ausführungen dargestellt.

10.4.1. Authentisierung / Zertifizierung

Die fachliche Sicherheitsanforderung der Authentisierung wird im Szenario durch zwei Sicherheitsobjekte `SO.Auth[20]` und `SO.Auth[21]` modelliert. Anhand der Unterscheidung in systeminterne und systemexterne Transaktionen kann durch den Modellierer der erste Schritt der Identifikation relevanter T-SOT durchgeführt werden.

SO.Auth[20]

`SO.Auth[20]` bezieht sich auf den Operator `Terminprüfung.sendeBestätigung()`, der eine Terminbestätigung der Komponente `Orthopädie` an die Komponente `Annahme` versendet. Auf Grund der angestrebten Integration der beiden Komponenten in ein Anwendungssystem ist davon auszugehen, dass die entsprechende Transaktion intern durchgeführt wird. Dadurch wird der Transaktionscharakter deutlich reduziert, da aus technischer Sicht für die Durchführung lokale Funktionsaufrufe genutzt werden. Die Authentisierungsanforderung an die Terminbestätigung wird vor diesem Hintergrund bereits durch die Integrität und Konsistenz der Implementierung der entsprechenden Funktionen zur Speicherung der entsprechenden Datensätze abgesichert. Technische Sicherheitsobjekttypen sind für dieses Sicherheitsobjekt somit nicht zu spezifizieren.

SO.Auth[21]

Die durch `SO.Auth[21]` referenzierte Transaktion `Leistungserfassung.sendeDaten()` hingegen kann als externe Transaktion klassifiziert werden, da die entsprechenden Inhalte durch den Operator an das bestehende Buchhaltungssystem zu übergeben sind. Der T-SOT

Zertifizierung kann somit grundlegend als relevant für das Anwendungssystem charakterisiert werden.

Durch den Modellierer ist nun zu klären, in welcher Form die Übertragung der Leistungserfassung durchgeführt werden soll. Erfolgt diese zum Beispiel durch ein E-Mail-basiertes Verfahren, somit als teil-automatisierte Aufgabe, die durch einen Nutzer des Systems veranlasst wird, stellt die Nutzung einer PKI ein probates Mittel zur Signierung der zu übermittelnden Nachricht dar. Erfolgt sie hingegen durch eine automatisierte Kopplung der Anwendungssysteme, zum Beispiel durch RPC-Aufrufe (engl. *remote procedure call*), so sind spezifische Anwendungskomponenten zu entwickeln, die eine Authentisierung der Leistungsdaten ermöglichen.

Im vorliegenden Szenario wird die Transaktion, wie im ersten Fall dargestellt, übermittelt. Als technischer Ansatz kann somit die digitale Signatur einer Nachricht zum Einsatz kommen. Als Infrastruktur für die technischen Sicherheitsfunktionen wird eine bereits existente PKI genutzt, die zentralisiert alle E-Mails des MVZ signieren kann. Der resultierende technische Sicherheitsobjekttyp kann somit wie folgt dargestellt werden.

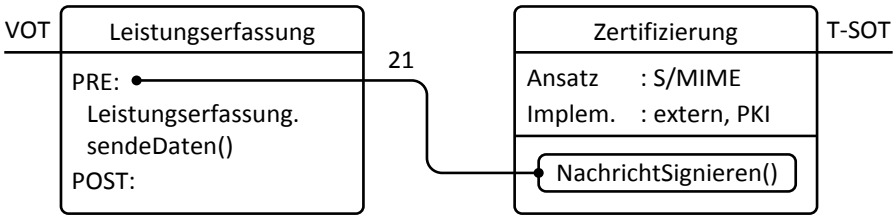

Abbildung 72: T-SOT zur Anforderung SO.Auth[21]

In der Abbildung zusätzlich aufgeführt ist die Beziehung des T-SOT zu dem durch den `SO.Auth[21]` referenzierten VOT `Leistungserfassung`. Dargestellt wird nur der sicherheitsrelevante Operator, der durch die Schlüsselwörter `PRE` und `POST` gekapselt wird. Diese entsprechen dem Attribut `prüfung` des zu Grunde liegenden Sicherheitsobjekts und beziehen sich auf notwendige Vor- bzw. Nachbedingungen der Durchführung des Operators. Im vorliegenden Fall ist die Sicherheitsanforderung als Vorbedingung modelliert, die durch einen Aufruf des abstrakten Operators `NachrichtSignieren()` des T-SOT zu erfüllen ist. Die dargestellten Attribute des T-SOT spiegeln die oben ausgeführten Überlegungen zur Umsetzung der Authentisierungsanforderung wider. Als Referenz auf das jeweilige fachliche Sicherheitsobjekt wird dessen Bezeichnung an der Assoziation notiert.

10.4.2. Übertragungssicherung / Verschlüsselung

Die fachliche Sicherheitsanforderung Übertragungssicherung wurde im Szenario MVZ zweimalig in Form der `SO.ÜS[11]` sowie `SO.ÜS[12]` modelliert.

SO.ÜS[11]

Durch das Sicherheitsobjekt referenziert wird der Operator `Patientenaufnahme.sendeKurzanamnese()`. Analog zu der Beschreibung im letzten Kapitel wird durch diesen Operator eine interne Transaktion ausgelöst, die aus technischer Sicht durch die Speicherung des Datensatzes in einer anwendungsweit zugreifbaren Datenbank erfolgt. Es erfolgt somit keine Übertragung der Information über ungesicherte Netze, sodass die geforderte Übertragungssicherung nicht durch technische Sicherheitsfunktionalität zu realisieren ist.

SO.ÜS[12]

Die Sicherheitsanforderung bezieht sich auf den Operator `sendeDaten()` des VOT `Leistungserfassung`. Gemäß den Ausführung des letzten Kapitels, wird durch diesen eine externe Transaktion ausgelöst, die demzufolge auch durch entsprechende technische Sicherheitsfunktionalität in Form von Verschlüsselungsdiensten abzusichern ist. Wie bereits spezifiziert, handelt es sich um ein E-Mail-basiertes Verfahren, sodass sowohl anwendungs- als auch transportorientierte Verschlüsselungsverfahren zum Einsatz kommen können[143]. Auf Grund der bereits spezifizierten Sicherheitsfunktionalität der PKI zur Zertifizierung, können in diesem Fall Synergien genutzt werden, indem die Verschlüsselungsdienste ebenfalls auf dieser Infrastruktur aufbauen.

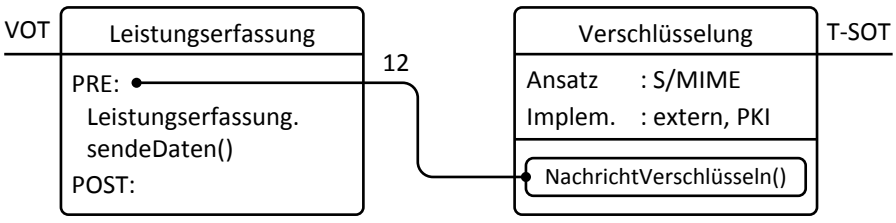

Abbildung 73: T-SOT zur Anforderung SO.ÜS[12]

[143] In Anlehnung an das OSI-Referenzmodell (vgl. zum Beispiel [FiSc05, 45]) bezieht sich die anwendungsorientierte Sicht auf die Realisierung der Verschlüsselung über zu implementierende Anwendungsfunktionalität, wohingegen aus transportorientierter Sichtweise die Verschlüsselung durch entsprechende Protokolle der Nachrichtenübertragung erfolgt.

Der Operator `NachrichtVerschlüsseln()` der T-SOT Verschlüsselung wird ebenfalls als Vorbedingung des anwendungsspezifischen Operators `sendeDaten()` modelliert.

10.4.3. Beweissicherung / Protokollierung

Beweissicherung als fachliche Sicherheitsanforderung wurde im Szenario MVZ in dreifacher Weise modelliert. Spezifiziert wurden die Sicherheitsobjekte `SO.Beweis[20.1]`, `SO.Beweis[21.1]` sowie `SO.Beweis[23]`. Wie in Kapitel 9.3.1.4 beschrieben, sind diese Sicherheitsanforderungen in unterschiedliche Subtypen unterteilbar, die anhand der Ausprägung des Sicherheitsobjektattributs `beweistyp` bestimmbar sind. In Bezug auf die technische Sicherheitsfunktionalität sind diese Subtypen von Relevanz, da sie direkten Einfluss auf die praktische Umsetzungsform der Sicherheitsanforderungen haben können. Für die Subtypen `EOR` und `EOS` bildet den zentralen Aspekt für den Modellierer hierbei die Frage, in welcher Form die Beweiserbringung technisch gesehen erfolgen kann. Dies wiederum ist abhängig von dem genutzten Transaktionsmodell, somit der Entscheidung, ob eine direkte Übermittlung zwischen Sender und Empfänger stattfindet oder ob diese indirekt über eine TTP erfolgt[144]. Im Falle der lokalen Vorgangsprotokollierung (Subtyp `LOG`) ist diese Fragestellungen jedoch nicht von Bedeutung, da in diesem Zusammenhang die Beweiserzeugung immer im Kontext der Anwendung selbst erfolgt.

SO.Beweis [20.1]

`SO.Beweis[20.1]` ist als Subtyp `EOS` modelliert und referenziert den Operator `sendeBestätigung()` des VOT `Terminprüfung`. In diesem Fall handelt es sich um das Auslösen einer internen Transaktion, deren Durchführung aus Gründen der Nachweisbarkeit für Dritte beweisbar sein muss. Die Beweiserbringung muss in diesem Fall jedoch nicht in direktem Zusammenhang mit dem Zeitpunkt der Transaktionsdurchführung erfolgen. Weiterhin ist keine Bereitstellung des Beweises für externe Anspruchsgruppen notwendig, da die Beweissicherung ausschließlich der internen Prozesskontrolle des MVZ dient. Aus technischen Gesichtspunkten ist demzufolge, auch in Anbetracht der angestrebten Anwendungsarchitektur, eine lokale Speicherung der Beweisdaten für die Übermittlung der Bestätigung ausreichend.

[144] Vgl. hierzu Kapitel 8.2.2.4.

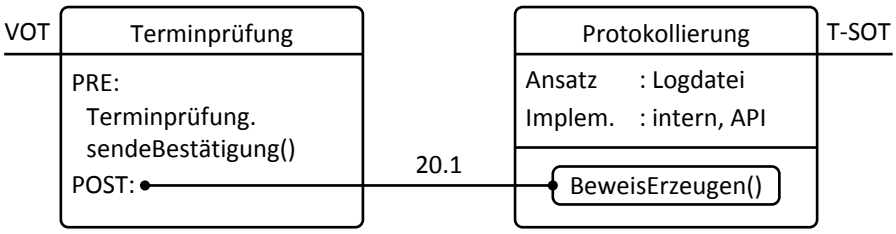

Abbildung 74: T-SOT zur Anforderung SO.Beweis[20.1]

Die Beweiserzeugung und -speicherung erfolgt auf Basis einer Programmbibliothek, die durch einen Aufruf des Operators `BeweisErzeugen()` die entsprechenden Datensätze in einer lokalen Logdatei ablegt. Gemäß der Ausprägung des Sicherheitsobjektattributs `prüfung` erfolgt dies nach der Durchführung des fachlichen Operators. Die Innensicht wird durch das interne Protokollierungsverfahren gekennzeichnet, das aus Implementierungssicht applikationsspezifische Protokollierungsmechanismen nutzt. Diese werden auf der Grundlage einer API erbracht. Im Hinblick auf den notwendigen Inhalt des Beweises sind entsprechende Vorschriften des Datenschutzes zu beachten[145].

SO.Beweis [23]

Für den Operator `Patientenakte.erstelleAnamnese()` wurde der Subtyp `LOG` der Sicherheitsanforderung Beweiserbringung modelliert. Hierbei handelt es sich um die Anforderung, dass der Vorgang zur Erstellung der Anamnese nachweisbar ist. In diesem Fall greifen die gleichen Faktoren, wie sie bereits im vorherigen Kapitel definiert wurden.

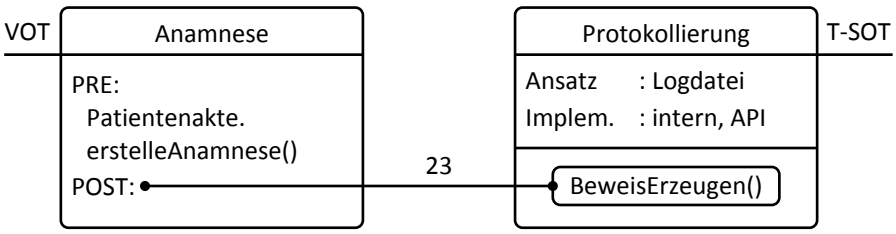

Abbildung 75: T-SOT zur Anforderung SO.Beweis[23]

Aus technischer Sicht kann somit die gleiche technische Sicherheitsfunktionalität genutzt werden, wie durch das fachliche Sicherheitsobjekt `SO.Beweis[20.1]`. Durch eine Programmbibliothek wird unter Nutzung der entsprechenden API die Beweiserzeugung somit für beide Anforderungen durch die Applikation gesteuert.

[145] Vgl. hierzu Kapitel 5.5.4.

SO.Beweis [21.1]

Der referenzierte Operator des `SO.Beweis[21.1]` ist `sendeDaten()` des VOT `Leistungserfassung`. Die fachliche Anforderung besagt hier, dass der Versand der Leistungsdaten nachweisbar sein muss. Im Zusammenhang mit der anwendungsexternen Verarbeitung der Daten durch das Buchhaltungssystem ist dieser Beweis nicht ausschließlich intern vorzuhalten, sondern muss auch für Dritte nachvollziehbar sein. Aus technischer Perspektive ist daher die interne Beweiserzeugung, wie zum Beispiel im Fall des `SO.Beweis[20.1]` beschrieben, nicht ausreichend und wird durch das Konzept der TTP ersetzt.

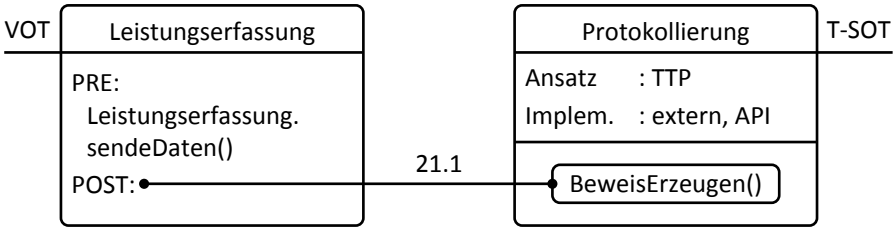

Abbildung 76: T-SOT zur Anforderung SO.Beweis[21.1]

Die Grundlage für die Nutzung einer TTP stellt ein entsprechendes Protokoll dar, durch das die zu übertragenden Informationen und die entsprechende Beweiserzeugung bestimmt wird. In der Literatur werden hierzu verschiedene Vorschläge unterbreitet[146], die sich in der Regel in der Art der zu übertragenden Information sowie dem entsprechenden Ablauf der Kommunikation zwischen den Parteien unterscheiden. Eine Grundidee dieser Ansätze besteht aus Sicht des Senders in der Übermittlung einer verschlüsselten Nachricht über die TTP an den Empfänger sowie der zusätzlichen Übertragung des Schlüssels zur Dekodierung an die TTP. Nachdem der Empfänger den Beweis des Erhalts an die TTP erbracht hat, erhält er den Schlüssel und kann die Nachricht entschlüsseln [RaRa02, 13]. Bezogen auf das Szenario ist der geforderte Nachweis des Versands somit durch die TTP belegbar[147].

Aus technischer Sicht betrachtet ist der relevante Operator `BeweisErzeugen()` somit auf Basis einer bestehenden technischen Infrastruktur in Verbindung mit vertraglichen Nutzungsregelungen hinsichtlich der TTP zu erbringen. Die Implementierung auf Seiten der Anwendung

[146] Vgl. zum Beispiel [Den+96].

[147] Auf Grund der Abgrenzung des Anwendungssystems wird die Funktionalität der Beweisverifikation nicht erläutert. Für weitere Informationen hierzu sei zum Beispiel auf [Oni+09] verwiesen.

erfolgt dabei auf Basis einer externen API, die die entsprechend notwendigen Vorgänge in Verbindung mit der TTP zur Verfügung stellt.

10.4.4. Autorisierung / Zugriffskontrolle

Fachliche Autorisierungsinformationen wurden im Szenario in Form der Sicherheitsobjekte `SO.Auto[10.1]`, `SO.Auto[12.1]` sowie `SO.Auto[13]` modelliert. Für alle Anforderungen gilt, dass sie auf der Grundlage einer gemeinsamen Autorisierungsinfrastruktur realisiert werden.

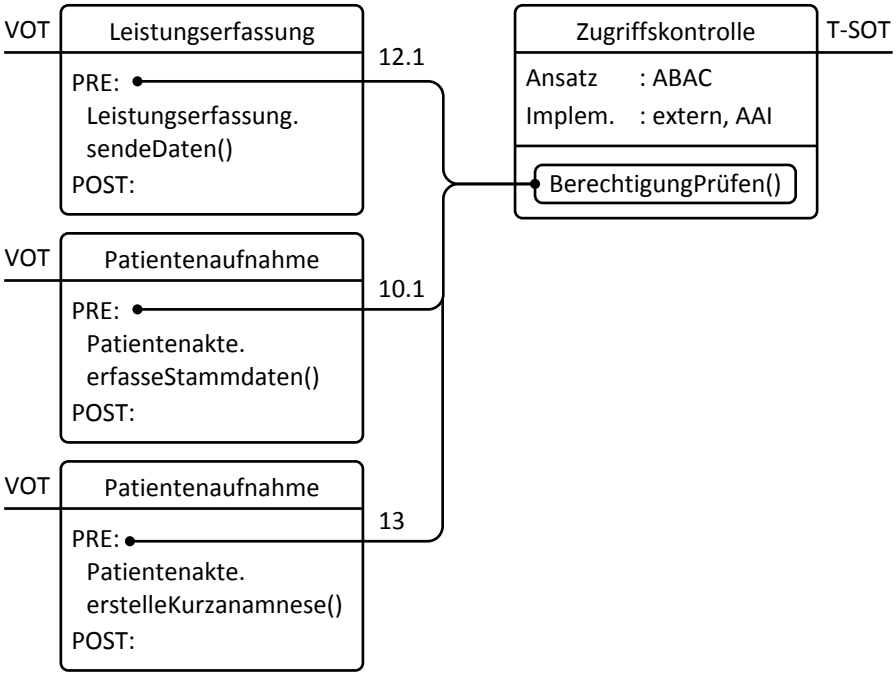

Abbildung 77: T-SOT zu den Anforderungen SO.Auto

Das zu verwendende Verfahren der Autorisierung bezieht sich auf die Wahl der grundlegenden Zugriffskontrollstrategie. In SOMsec wird diesbezüglich ein attribut-basiertes Verfahren genutzt, ein entsprechender Ansatz wird durch das in Kapitel 9.3.1.3 beschriebene Sicherheitsmodell ABAC dargestellt. In einem Anwendungssystem wird diese technische Sicherheitsfunktionalität in der Regel durch eine entsprechende API abgebildet, die selbst wiederum eine bestehende Autorisierungsinfrastruktur als Basismaschine verwenden kann. Eine mögliche Form der Parametrisierung wird exemplarisch in Kapitel 10.5 beschrieben.

10.4.5. Modellierungsergebnis

Das Ergebnis der technischen Sicherheitsspezifikation besteht in vier technischen Sicherheitsobjekttypen, die die entsprechenden fachlichen Sicherheitsanforderungen umsetzen.

Im Bereich der Zertifizierung und Verschlüsselung können Synergien in der technischen Umsetzung genutzt werden. Beide spezifizierten Lösungsverfahren setzen auf der gemeinsamen Infrastruktur der PKI auf, sodass die entsprechende Funktionalität für beide Bereiche einheitlich erbracht werden kann.

Im Bereich der Protokollierung hingegen sind zwei konzeptuell unterschiedliche Ansätze notwendig, um die fachlichen Anforderungen umzusetzen. Vornehmlicher Grund hierfür ist die Nutzung unterschiedlicher Protokolle zur Beweiserzeugung. Aus Sicht der technischen Basisfunktionalität sind somit zwei entsprechende Infrastrukturen bereitzustellen.

Der Sektor Zugriffskontrolle ist durch die Nutzung einer einheitlichen technischen Funktionalität realisierbar. Diese wird gemäß der Modellierung im Szenario MVZ auf Basis eines attribut-basierten Ansatzes umgesetzt. Neben der Ableitung der technischen Sicherheitsobjekttypen ist in diesem Bereich auch eine weiterführende Parametrisierung der technischen Basisfunktionalität möglich. Dieser Aspekt wird abschließend im folgenden Kapitel im Detail erläutert.

10.5. Ableitung von Zugriffsberechtigungen

Zugriffsberechtigungen werden in SOMsec auf Basis von betrieblichen Rollen auf Geschäftsprozessebene modelliert und in Form attribut-basierter Privilegien in die fachliche Anwendungsspezifikation integriert. Diese modellierten Anforderungen gehen inhaltlich über die reine Definition benötigter T-SOT hinaus und können aus diesem Grund zur Parametrisierung verwendeter Autorisierungsinfrastrukturen als Basisfunktionalität herangezogen werden.

Die Grundlage für dieses Vorgehen in SOMsec bildet XACML (eXtensible Access Control Markup Language), ein XML-Schema zur Repräsentation von Autorisierungsinformationen, das in Version 2.0 im Jahre 2005 als OASIS-Standard verabschiedet wurde [OASI05].

10.5.1. Grundlagen von XACML

XACML stellt XML-Schemata zur Verfügung, um Zugriffkontrollrichtlinien (engl. *access control policies*) zu spezifizieren. Diese Richtlinien (XACML Policy) können dann auf Basis einer bestimmten Autorisierungsinfrastruktur erstellt und im Zugriffsfall evaluiert werden. Die folgende Abbildung zeigt diese Struktur im Überblick.

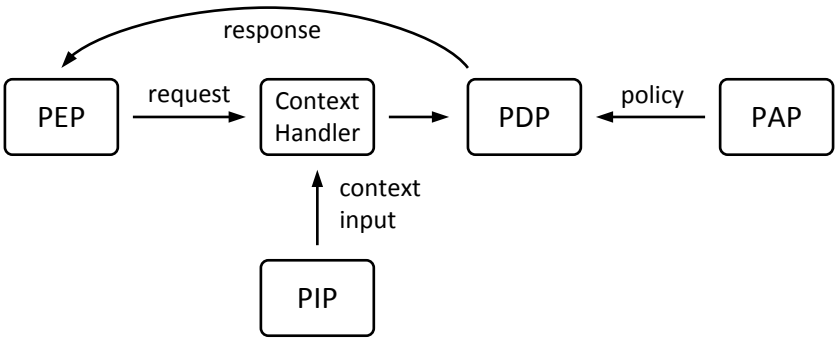

Abbildung 78: Autorisierungsstruktur von XACML

Durch die Nutzung eines Policy Administration Points (PAP) werden XACML Policies erstellt und im Policy Decision Point (PDP) hinterlegt. Ein Zugriffsversuch wird durch einen Policy Enforcement Point (PEP) entgegengenommen und an den Context Handler weitergereicht. Dieser erzeugt einen Zugriffskontext, indem er unter Nutzung verschiedener Policy Information Points (PIP) unterschiedliche Attribute, wie zum Beispiel Zeitstempel oder Nutzerinformationen aus weiteren Quellen, zugriffsbezogen speichert. Dieser attribut-basierte Kontext, zusammen mit der Spezifikation der angefragten Ressource, wir dann durch den PDP anhand zutreffender XACML-Policies evaluiert. Das Resultat wird abschließend an den PEP übermittelt, der es entsprechend der Implementierung umsetzt[148].

Der Aufbau einer XACML-Policy kann durch das folgende, vereinfacht dargestellte Meta-Modell in UML-Notation veranschaulicht werden.

[148] Eine exakte Darstellung des Datenflusses zwischen den Komponenten ist in [OASI05, 16f] zu finden.

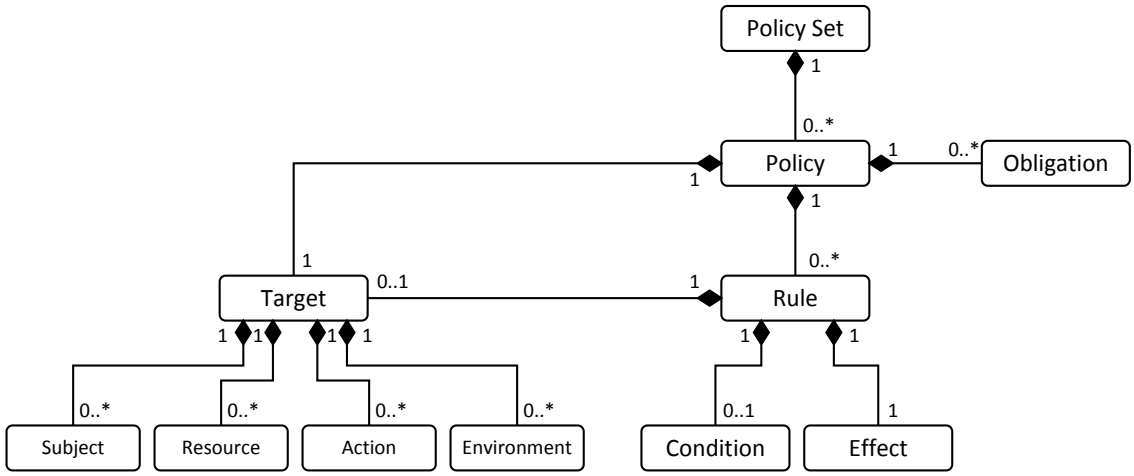

Abbildung 79: Vereinfachtes Meta-Modell von XACML (nach [OASI05, 19])

Das Wurzelelement stellt ein Policy Set dar, das eine oder mehrere Policy Elemente enthalten kann. Eine `Policy` stellt eine Zugriffsrichtlinie dar, die durch Regeln (engl. *rules*) definiert wird. `Targets` bilden den Kontext, für den eine `Rule` anzuwenden ist. Ein `Subject` steht diesbezüglich für eine zugreifende Entität, eine `Resource` spezifiziert das Objekt auf das zugegriffen werden soll. `Action` definiert die entsprechende Zugriffsoperation und Environment zusätzliche Kontextattribute. Das Element `Condition` ermöglicht es, das Zutreffen einer Rule an weitere Bedingungen zu binden. Es wird in Form eines booleschen Ausdrucks angegeben. Wird durch den PDP eine passende Rule für einen Zugriffskontext identifiziert, so wird das Ergebnis der Evaluation in Form eines `Effects` zurückgeliefert. Hierfür sind die Werte `permit` und `deny` vorgesehen. Weiterhin kann durch eine `Obligation` eine zusätzliche Operation spezifiziert werden, die nach dem Anwenden einer Regel in der Antwort des PDP an den PEP enthalten und durch diesen umzusetzen ist [OASI05, 20ff].

Die Spezifikation von XACML Policies kann schnell einen großen Umfang sowie einen hohen Komplexitätsgrad erreichen. Aus diesem Grund wird bewusst auf eine vollständige Vorstellung des Standards verzichtet. Bestimmte Elemente, wie zum Beispiel PolicyCombiningAlgorithms oder Targets für Policy-Sets, die keine direkte Relevanz für die Integration des Ansatzes in SOMsec aufweisen, werden daher nicht berücksichtigt.

10.5.2. XACML in SOMsec

Durch die Angabe einer XACML-Policy können die im Rahmen der fachlichen Sicherheitsspezifikation definierten Berechtigungen in die technische Sicherheitsspezifikation transfor-

miert werden. Die notwendige Autorisierungsinfrastruktur wird dabei als Bestandteil der technischen Basisfunktionalität angesehen. Die Angabe einer XACML-Policy stellt somit eine Parametrisierung dar, die sich auf den T-SOT Zugriffskontrolle bezieht, der durch diese Basisfunktionalität realisiert wird.

Beziehungs-Meta-Modell

Der Übergang zwischen fachlicher und technischer Sicherheitsspezifikation kann in Bezug auf Autorisierungsaspekte anlog zum Übergang zwischen Geschäftsprozessmodell und Anwendungsmodell in Form eines Beziehungs-Meta-Modells angegeben werden. Als Ausgangspunkt dienen die jeweiligen Meta-Modelle des SOT.Auto sowie von XACML.

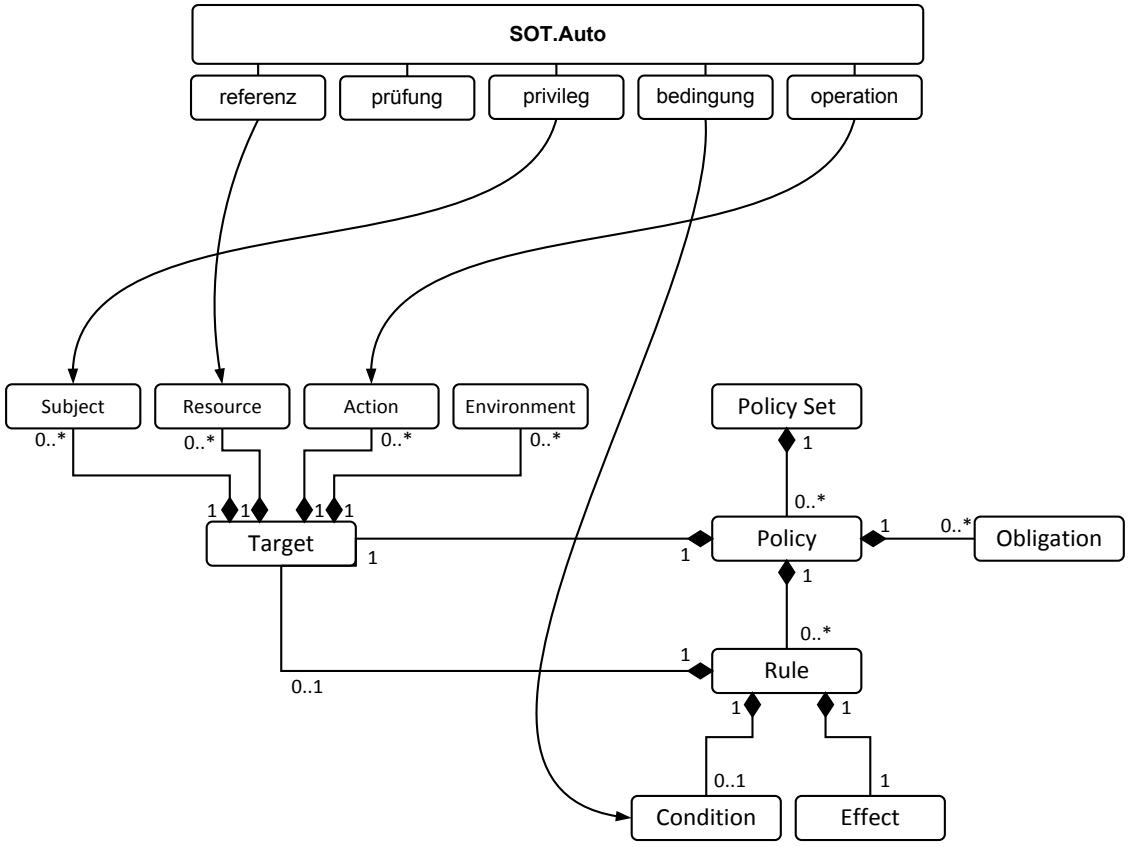

Abbildung 80: Beziehungs-Meta-Modell zwischen fachlicher und technischer Sicherheitsspezifikation (SOT.Auto)

In der Spezifikation der fachlichen Autorisierungsanforderung werden Subjektdeskriptoren von ABAC durch das Attribut `privileg` angegeben. Dieses entspricht dem Element `Subject` in der Target-Definition einer `Rule`. Weiterhin kann das Attribut `operation` auf das Element `Action` abgeleitet werden. In SOMsec ist hierfür die Ausprägung EXECUTE vorgesehen.

Das Attribut `referenz` des SOT.Auto bezieht sich auf einen Operator eines VOT. Der Aufruf dieses Operators stellt somit die `Resource` einer Berechtigungsprüfung in XACML dar. Eine `bedingung` des SOT.Auto entspricht weiterhin dem Element `condition`, als Bedingung für die Anwendbarkeit einer Regel.

Anhand der spezifizierten Beziehungen können fachliche Autorisierungsanforderungen in ein verwertbares Parametrisierungsformat für Autorisierungsinfrastrukturen überführt werden. Im folgenden Abschnitt wird dieses Vorgehen für das Szenario MVZ beschrieben.

10.5.3. Szenario: XACML-Policy

Im Szenario MVZ wurden drei fachliche Autorisierungsanforderungen spezifiziert, die zu Parametern einer Autorisierungsinfrastruktur transformierbar sind. Die folgende Darstellung stellt diese als XACML Policy dar.

```
<?xml version="1.0" encoding="UTF-8" ?>
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
 PolicySetId="Berechtigungen_AWS" Version="1.0">
<Target />

<Policy PolicyId="Berechtigungen_Operatorzugriff">
<Target />
  <Rule Effect="Permit"
   RuleId="13-Berechtigung_Erstellung_Kurzanamnese">
  <Description />
  <Target>
  <Subjects>
    <Subject>
      <SubjectMatch
       MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
         DataType="http://www.w3.org/2001/XMLSchema#string">Arzthelfer
        </AttributeValue>
        <SubjectAttributeDesignator AttributeId="rolle"
         DataType="http://www.w3.org/2001/XMLSchema#string" />
      </SubjectMatch>
    </Subject>
  </Subjects>
<Resources>
    <Resource>
```

```
      <ResourceMatch
       MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
         DataType="http://www.w3.org/2001/XMLSchema#string">
         Patientenakte.erstelleKurzanamnese
        </AttributeValue>
        <ResourceAttributeDesignator
         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
         DataType="http://www.w3.org/2001/XMLSchema#string" />
      </ResourceMatch>
    </Resource>
  </Resources>
  </Target>
  </Rule>
  <Rule Effect="Permit"
   RuleId="12.1-Berechtigung_Senden_Leistungsdaten">
  <Description />
  <Target>
  <Subjects>
    <Subject>
      <SubjectMatch
       MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
         DataType="http://www.w3.org/2001/XMLSchema#string">Chefarzt
        </AttributeValue>
        <SubjectAttributeDesignator AttributeId="rolle"
         DataType="http://www.w3.org/2001/XMLSchema#string" />
      </SubjectMatch>
    </Subject>
  </Subjects>
  <Resources>
    <Resource>
      <ResourceMatch
       MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
         DataType="http://www.w3.org/2001/XMLSchema#string">
         Leistungserfassung.sendeDaten
        </AttributeValue>
        <ResourceAttributeDesignator
         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
         DataType="http://www.w3.org/2001/XMLSchema#string" />
      </ResourceMatch>
    </Resource>
  </Resources>
```

```
  </Target>
  </Rule>
  <Rule Effect="Permit"
   RuleId="10.1-Berechtigung_Erfassung_Stammdaten">
  <Description />
  <Target>
  <Subjects>
    <Subject>
      <SubjectMatch
       MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
         DataType="http://www.w3.org/2001/XMLSchema#string">Rezeptionist
        </AttributeValue>
        <SubjectAttributeDesignator AttributeId="rolle"
         DataType="http://www.w3.org/2001/XMLSchema#string" />
      </SubjectMatch>
    </Subject>
  </Subjects>
  <Resources>
    <Resource>
      <ResourceMatch
       MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue
         DataType="http://www.w3.org/2001/XMLSchema#string">
         Patientenakte.erfasseStammdaten
        </AttributeValue>
        <ResourceAttributeDesignator
         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
         DataType="http://www.w3.org/2001/XMLSchema#string" />
      </ResourceMatch>
    </Resource>
  </Resources>
  </Target>
  </Rule>
</Policy>
</PolicySet>
```

Quelltext 14: Szenario MVZ - XACML Policy

Im Beispiel werden die drei Autorisierungsanforderungen in vereinfachter Form als einzelne Regeln einer globalen Policy für das gesamte Anwendungssystem dargestellt. Ausschlaggebend für die Überprüfung der Regeln ist die Definition des Targets, das anhand der Elemente

`Subject` und `Resource` dargestellt ist. Ersteres bezieht sich auf die Identifikation berechtigter Subjekte, die im Beispiel anhand des Attributs `rolle` selektiert werden. Die zu überwachende Ressource stellt der jeweilige Operator des entsprechend referenzierten VOT dar, der durch den Identifier `resource-id` in Form seiner Bezeichnung repräsentiert wird. Für das Zutreffen einer Regel, und damit verbunden für die Erteilung der Berechtigung, ist demnach relevant, ob ein zugreifendes Subjekt die spezifizierte Rolle innehat.

Die Identifikation von relevanten Werten in den Elementen `Subject` und `Resource` erfolgen im Beispiel auf Basis einfacher Vergleiche von Zeichenketten. Eine Typisierung der entsprechenden Datentypen ist grundlegend anzustreben, erfolgt jedoch aus Gründen des Umfangs in der vorliegenden Arbeit nicht. Ebenfalls werden weitere Aspekte, wie zum Beispiel Kombinationsalgorithmen für Regeln, nicht diskutiert.

Die dargestellte XACML-Policy würde durch einen Verantwortlichen an einem PAP erstellt und im Anschluss mit den entsprechenden Policies der weiteren Autorisierungsanforderungen an den PDP übertragen. An dieser Stelle erfolgt dann die Evaluierung der Zugriffe, die durch die Ableitung im Sinne der fachlichen Anforderungsspezifikation durchgeführt werden kann.

Die vorgestellte Ableitung der Zugriffsberechtigungen als Parameter der Basisfunktionalität beschließt die Vorstellung der Modellierungsmethodik SOMsec und damit den dritten Teil der vorliegenden Arbeit. Im folgenden Kapitel erfolgt eine abschließende Zusammenfassung und Diskussion der Ergebnisse sowie eine Einordnung anhand aktueller Forschungsaktivitäten.

11. Schlussbetrachtung

Die Notwendigkeit einer Modellierungsmethodik für betriebliche Informationssicherheit kann auf Basis des in Teil II vorgestellten Referenzmodells abgeleitet werden. Ein entsprechendes Lösungsverfahren im Form von SOMsec wurde im dritten Teil der Arbeit besprochen. Anhand eines Szenarios wurde weiterhin dargestellt, dass eine durchgängige Betrachtung der Informationssicherheit von der Geschäftsprozessebene, über die fachliche Anwendungsspezifikation, bis hin zur technischen Architekturmodellierung konzeptuell und methodisch realisierbar ist.

In diesem Zusammenhang beleuchtet das folgende Kapitel 11.1 den aktuellen Stand der Forschung, bevor in Kapitel 11.2 eine zusammenfassende Diskussion von SOMsec erfolgt. Kapitel 11.3 beschließt im Anschluss die vorliegende Arbeit mit einem Ausblick auf mögliche zukünftige Forschungsaspekte in dem vorgestellten Themengebiet.

11.1. Stand der Forschung

Im Bereich verwandter Arbeiten sind zwei grundlegende Tendenzen in den Forschungsaktivitäten festzustellen. Auf der einen Seite besteht ein sehr starker Fokus auf dem Segment der Geschäftsprozessmodellierung, in dessen Rahmen Sicherheitsaspekte jedoch nur einen geringen Anteil einnehmen. Auf der anderen Seite werden diese im Bereich der fachlichen und technischen Anwendungssystemspezifikation gerade in den letzten Jahren verstärkt berücksichtigt, jedoch zumeist isoliert und nur bezogen auf das zu entwickelnde Anwendungssystem betrachtet [Kla+09a, 169]. In den folgenden Abschnitten werden Beispiele zu den beiden Forschungsbereichen vorgestellt, die nachstehende Abbildung stellt diese anhand ihrer Bezugsebenen im Überblick dar.

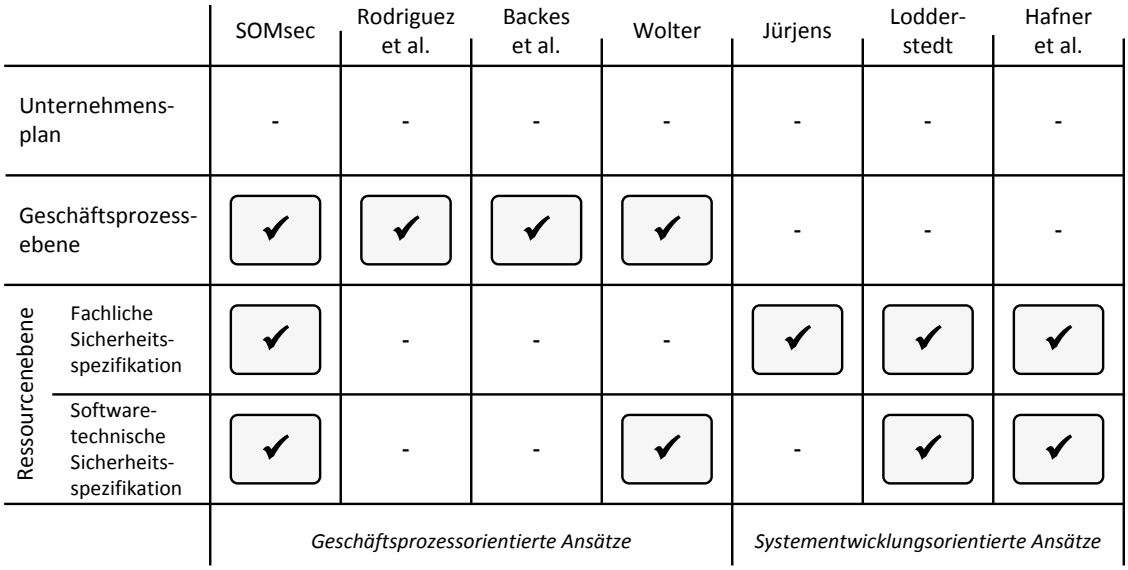

Abbildung 81: Vergleich bestehender Forschungsansätze

Die Forschungsansätze können grob anhand ihrer inhaltlichen Fokussierung in geschäftsprozess- und systementwicklungsorientierte Ansätze untergliedert werden. In der Abbildung werden sie vergleichend in Beziehung zu dem in dieser Arbeit genutzten Rahmen der SOM-Unternehmensarchitektur gesetzt. Ein Haken symbolisiert dabei die Unterstützung der jeweiligen Modellierungsebene.

Geschäftsprozessorientierte Ansätze

RODRIGUEZ et al. adressieren in ihren Arbeiten den Aspekt der Integration von Sicherheitsanforderungen in Geschäftsprozesse. Sie beschreiben dies auf Basis mehrerer Modellierungsansätze, wie zum Beispiel anhand von UML-Aktivitätsdiagrammen [Rod+06] oder Erweiterungen zur BPMN [Rod+07]. Dabei erfolgt jedoch keine methodische Klassifikation der zu modellierenden Anforderungen, sodass Schutzziele ebenso wie Sicherheitsmechanismen auf gleicher Ebene in die Modelle integriert werden. Weiterhin besteht keine Ableitungsbeziehung zu weiterführenden Modellen, sodass die Modellierung der Sicherheitsaspekte auf einer rein beschreibenden Ebene verweilt.

Ebenfalls in diesem Bereich erläutern BACKES et al. einen Ansatz, dessen Ziel die Integration von Sicherheitsanforderungen in die Entwicklung von Geschäftsprozessen ist [Bac+03]. Das Hauptaugenmerk liegt dabei nicht auf elementaren Schutzzielen sondern auf abstrakten Sicherheitseigenschaften, wie zum Beispiel der gerechte Ablauf von Transaktionen oder Privatheitsanforderungen in unterschiedlichen Vertrauensstellungen. Für die Umsetzung wird

vornehmlich der Einsatz von Kryptografie sowie der formale Verifikation der entsprechenden Modellierungsergebnisse propagiert. BACKES spezifiziert auf diese Weise einen vergleichsweise isolierten Ansatz, dessen Zielsetzung sich nicht auf eine ganzheitliche Betrachtung geschäftsprozessgetriebener Sicherheitsmodellierung bezieht. Weiterhin sind die genutzten formalen Ansätze unter Umständen auf Ebene der Geschäftsprozessmodellierung nicht problemlos einsetzbar.

WOLTER adressiert in [Wol+08] die Modellierung von Schutzzielen auf Geschäftsprozessebene. Als grundlegender Ansatz dient die BPMN, die durch entsprechende Sicherheitsbedingungen erweitert wird. Das Ziel des Ansatzes ist die Transformation der Modellierungsergebnisse in umsetzbare Sicherheitspolitiken auf technischer Ebene, die zur Laufzeit der entsprechenden Anwendungssysteme genutzt werden können. Den Schwerpunkt bilden hierbei Sicherheitsaspekte service-orientierter Architekturen, für die entsprechende Konfigurationen auf Basis eines Transformations-Frameworks aus den Geschäftsprozessmodellen erzeugt werden [Wol+09]. WOLTER verfolgt im Kern den gleichen Ansatz wie SOMsec, integriert jedoch nicht explizit die fachlichen Aspekte der Anwendungsentwicklung.

Systementwicklungsorientierte Ansätze

JÜRJENS stellt in [Jür05] mit UMLsec einen Ansatz vor, der als UML-Profil die Modellierung von Sicherheitsanforderungen durch Anreicherung von UML Modellen adressiert. Der angestrebte Nutzungskontext bezieht sich auf den Bereich der Anwendungsentwicklung, JÜRJENS spricht hierbei von „model-based security engineering“. Auf Grund der starken formalen Ausrichtung kommen als Nutzer des Ansatzes vornehmlich Entwickler in Betracht, die bereits Erfahrungen im Bereich der Informationssicherheit aufweisen.

Einen weiteren UML-basierten Ansatz stellt LODDERSTEDT in [Lodd03] mit SecureUML vor. Das verfolgte Ziel besteht in der Etablierung von Sicherheitsaspekten als integraler Bestandteil der Softwareentwicklung. Als Methodik wird der Ansatz der „Model Driven Security“ etabliert, der die Beschreibung von anwendungsspezifischen Sicherheitsmodellen fordert, auf deren Basis dann vollständige Sicherheitsmechanismen werkzeuggestützt generiert werden können. Die Grundlage der Modellbildung bildet mit SecureUML eine formale Sprachdefinition, die auf Zugriffskontrollstrategien fokussiert ist und die in Klassen- sowie Zustandsdiagramme integrierbar ist.

HAFNER et al. beschreibt mit SECTET in [Haf+06] ein Framework, das auf die Entwicklung und Verwaltung sicherheitskritischer Workflow-Systeme auf Basis von Web Services ausgerichtet ist. Auf Basis von Workflow-Modellen in Form von UML Diagrammen werden ausführbare Konfigurationen für Workflow-Managementsysteme generiert sowie entsprechende Sicherheitskomponenten für die Services der Zielarchitekturen. SECTET zielt dabei auf die korrekte Umsetzung der technischen Sicherheitsspezifikationen ab, die aus unabhängigen Modellen ableitbar sind. In Kombination mit ProSecO, einem Vorgehensmodell für die sicherheitsorientierte Anwendungsentwicklung, wird SECTET als umfassender Ansatz zum „Model Driven Security Engineering“ positioniert [HaBr09].

11.2. Zusammenfassende Diskussion der Arbeit

Im Vergleich zu den vorgestellten Ansätzen verfolgt die vorliegende Arbeit das Ziel, den Themenkomplex der betrieblichen Informationssicherheit auf einer fundierten und methodischen Grundlage umfassend darzustellen. Die Erarbeitung des Referenzmodells betrieblicher Informationssicherheit bildet hierbei den konzeptuellen Rahmen, anhand dessen die betrieblich relevanten Elemente der Informationssicherheit systematisch dargestellt werden können. Ein besonderes Augenmerk liegt hierbei auf der Beschreibung einer durchgängigen Terminologie, die eine konsistente und trennscharfe Erfassung des Themenkomplexes erlaubt. Auf dieser Grundlage werden im Anschluss die relevanten Zielbereiche und Bezugselemente einer Modellierungsmethodik für Informationssicherheit identifiziert, die dann in Form des vorgestellten Ansatzes SOMsec entsprechend erarbeitet werden können.

Das Ziel von SOMsec selbst besteht in der Bereitstellung einer Methodik zur strukturellen Erarbeitung und Ableitung von Sicherheitsaspekten im Rahmen der geschäftsprozessgetriebenen Anwendungsentwicklung. Dies geschieht auf der konzeptuellen Basis des Referenzmodells betrieblicher Informationssicherheit. Der Schwerpunkt der Methodik liegt dabei weniger in der Fokussierung auf spezifische Modellierungsansätze für bestimmte Teilaspekte der Informationssicherheit, sondern auf der Bereitstellung eines flexiblen Rahmens, in den bestehende konzeptuelle und technische Ansätze integriert werden können. Insbesondere gilt dies für technische Sicherheitsfunktionalität, die in SOMsec durch technische Sicherheitsobjekttypen spezifiziert werden.

Den zentralen Ansatzpunkt für diese Flexibilität stellen die in SOMsec spezifizierten Beziehungen zwischen den Modellebenen dar. Diese sind in der Beschreibung der Methodik zwar inhaltlich ausgestaltet, stellen jedoch nur eine potentielle Ableitungsmöglichkeit dar. Durch eine Änderung der Modellierungstiefe für Sicherheitsaspekte können, den Fähigkeiten des Modellierers entsprechend, auf den unterschiedlichen Betrachtungsebenen auch über die dargestellten hinausgehende Modellinformationen generiert werden. Dies kann in SOMsec erreicht werden, indem zum Beispiel durch die Erweiterung der Attribute von Schutzzielen eine umfassenderer Beschreibung der Sicherheitsaspekte ermöglicht wird. Diese Attributstruktur ist dann durch ein entsprechend anzupassendes Beziehungs-Meta-Modell auf die ebenfalls zu überarbeitende Struktur der Sicherheitsobjekttypen abzubilden. SOMsec stellt somit eine flexible Modellierungsmethodik bereit, die nicht ausschließlich auf den vorgestellten Modellierungsansatz beschränkt ist, sondern bedarfsorientiert an spezifische Modellierungsanforderungen angepasst werden kann.

Im Vergleich zu den vorgestellten Forschungsaktivitäten ist SOMsec somit als übergreifender Ansatz zu verstehen, der in Bezug auf den Aspekt der Modellierungsreichweite einen größeren Bereich abdeckt. Die vorgestellten Ansätze adressieren im Vergleich hierzu entweder die Aufgaben- oder die Aufgabenträgerebene. Eine Ausnahme hierbei bildet der Ansatz von WOLTER, der im direkten Vergleich jedoch die Ebene der fachlichen Anwendungssystemspezifikation unberücksichtigt lässt.

Gleichwohl gilt jedoch zu berücksichtigen, dass die Ausgestaltung der Modellierungsansätze auf den einzelnen Ebenen stark abhängig ist von der grundlegenden Modellierungsmetapher. SOMsec basiert konzeptuell auf dem Ansatz des Semantischen Objektmodells, das einen ebenenorientierten Top-Down-Ansatz in der Modellierung nativ unterstützt. Eine sukzessive Anreicherung der sicherheitsrelevanten Modellinformation unter Berücksichtigung der jeweiligen Betrachtungsebene in SOMsec wird dadurch unterstützt. Der Fokus der vorgestellten Forschungsansätze hingegen liegt in der Regel weniger auf der ganzheitlichen Perspektive sondern auf einer detaillierten Betrachtungsweise einzelner Ausschnitte der betrieblichen Informationssicherheit. Hierbei sind fachliche Spezialthemen in detaillierterer Weise analysierbar, als sie im Rahmen der vorliegenden Arbeit, auch auf Grund des Umfangs, zu berücksichtigen wären. Grundsätzlich kann somit die Aussage getroffen werden, dass die vorgestellten Ansätze in punktuellen Fragestellungen detailliertere Lösungsverfahren aufzeigen, SOMsec hingegen eine fundiertere Basis und einen größeren Modellierungsumfang aufweist. Dieses Ergeb-

nis korrespondiert mit den grundlegenden Zielsetzungen der Arbeit sowie den definierten Anforderungen an die zu entwickelnde Methodik[149].

11.3. Ausblick

Die Entwicklung der Modellierungsmethodik SOMsec ist mit der vorgestellten Beschreibung aus konzeptueller Sichtweise zwar beendet, jedoch ist die inhaltliche Erweiterung vor dem Hintergrund der realweltlichen Entwicklungen im Bereich betrieblicher Informationssicherheit weiterhin voranzutreiben.

Werkzeugunterstützung

Eine Anforderung besteht hierbei sicherlich in der Schaffung einer durchgängigen Werkzeugunterstützung, die von der Geschäftsprozessmodellierung bis hin zur technischen Sicherheitsspezifikation den Rollen der Modellierer entsprechende Funktionen bereitstellt. Erst wenn eine diesbezügliche Plattform bereitsteht, können die Modellierungsergebnisse auch im Rahmen anderweitiger Prozesse, wie zum Beispiel im Rahmen der IT-Compliance, genutzt werden.

Konsistenzprüfung

Ein weiterer Aspekt stellt die Vertiefung der Konsistenzprüfungen der Modellierungsergebnisse dar. Insbesondere auf Geschäftsprozessebene und im Rahmen der fachlichen Anwendungssystemspezifikation ist dies von Relevanz um konfliktäre Sicherheitsspezifikationen zu vermeiden. Hierbei wurde in Bezug auf die in SOMsec modellierbaren Schutzzieltypen der Vertraulichkeit und Verbindlichkeit aus methodischer Sicht kein Konfliktpotential identifiziert[150]. Vor dem Hintergrund der Erweiterbarkeit des Ansatzes ist ein entsprechend allgemeingültiger Mechanismus jedoch von Vorteil. Einen Ansatzpunkt, um Inkonsistenzen in der Modellierung zu vermeiden, stellt zum Beispiel die Verwendung der Object Constraint Language (OCL) dar. Um die entsprechenden Constraints jedoch formulieren und verifizieren zu können, bildet eine formale Repräsentation der Modelle, zum Beispiel auf Basis eines XML-Schemas, die Voraussetzung.

[149] Vgl. Kapitel 1.2 und 7.2.5.

[150] Vgl. hierzu Kapitel 5.4.3.5.

Automatisierung

Die angesprochene Repräsentation der Modelle bildet weiterhin die Grundlage für die Automatisierbarkeit der Verifikations- und Ableitungsprozesse im Kontext der Modellbildung. Dieser Aspekt zielt ab auf die Nutzung von SOMsec im Rahmen eines modellgetriebenen Entwicklungsprozesses ab, bei dem die Transformationen zwischen den Betrachtungsebenen automatisiert vollzogen werden können. Eine Möglichkeit stellt in diesem Zusammenhang die Nutzung von XSLT dar, um die XML-Spezifikationen auf Basis formeller Transformationsregeln von einer Ebene zur anderen zu überführen.

Werden die genannte Aspekte in zukünftigen Forschungsaktivitäten adressiert, so kann auf der konzeptuellen Grundlage von SOMsec eine Überbrückung der beschriebenen Lücke zwischen Lenkungs- und Leistungssystem in Bezug auf die Berücksichtigung betrieblicher Sicherheitsaspekte erfolgen. Durch die aus der geschäftsprozessgetriebenen Sicherheitsmodellierung resultierende Kopplung zwischen Aufgaben- und Aufgabenträgerebene können Änderungen besser propagiert sowie die Übereinstimmung der technischen Sicherheitseigenschaften von Anwendungssystemen mit betrieblichen Sicherheitsanforderungen nachvollziehbar und administrierbar ausgestaltet werden.

Literaturverzeichnis

[Ambe93] AMBERG, M.: *Konzeption eines Software-Architekturmodells für die objektorientierte Entwicklung betrieblicher Anwendungssysteme.* Dissertation, Otto-Friedrich-Universität Bamberg, 1993

[Ande01] ANDERSON, R.: *Security Engineering: a guide to building dependable distributed systems.* New York: Wiley & Sons, 2001

[Ande72] ANDERSON, J. P.: *Computer Security Technology Planning Study.* URL http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf - Überprüfungsdatum 09.12.2008

[Anso66] ANSOFF, H. I.: *Management Strategie.* München: Verlag Moderne Industrie, 1966

[Bac+03] BACKES, M.; PFITZMANN, B.; WAIDNER, M.: *Security in Business Process Engineering.* In: VAN DER AALST, W.; TER HOFSTEDE, A.; WESKE, M. (Hrsg.): *Business process management : BPM 2003.* Berlin , New York: Springer-Verlag, 2003, S. 168–183

[Balz99] BALZERT, H.: *Lehrbuch Grundlagen der Informatik.* Heidelberg: Spektrum Akademischer Verlag, 1999

[Bas+01] BASHIR, I.; SERAFINI, E.; WALL, K.: *Securing network software applications.* In: *Communications of the ACM ,* 44 (2001), Nr. 2, S. 28–30

[Baue07] BAUER, F. L.: *Decrypted Secrets : Methods and Maxims of Cryptology.* Fourth, Revised and Extended Edition. Berlin, Heidelberg: Springer-Verlag, 2007

[BeLa73] BELL, D.; LAPADULA, L.: *Secure Computer Systems: Mathematical Foundations.* Bedford, 1973

[Beri02] BERINATO, S.: *Calculated Risk: Return on Security Investment.* URL http://www.csoonline.com/article/217727 /Calculated_Risk_Return_on_Security_Investment – Überprüfungsdatum 15.04.2010

[BeVo96] BECKER, J.; VOSSEN, G.: *Geschäftsprozessmodellierung und Workflow-Management : Eine Einführung.* In: VOSSEN, G.; BECKER, J. (Hrsg.): *Geschäftsprozeßmodellierung und Workflow-Management : Modelle, Methoden, Werkzeuge.* Bonn: Thompson, 1996, S. 17–26

[Biba77] BIBA, K. J.: *Integrity Considerations for Secure Computer Systems.* In: MITRE CORP. (HRSG.): *Technical Report ESD-TR-76-372,* 1977

[Ble+05] BLESS, R.; BLAß, E. O.; CONRAD, M.; HOF, H. J.; KUTZNER, K.; MINK, S.; SCHÖLLER, M.: *Sichere Netzwerkkommunikation : Grundlagen, Protokolle und Architekturen.* Berlin, Heidelberg: Springer-Verlag, 2005

[Blei04] BLEICHER, K.: *Das Konzept integriertes Management.* 7., überarb. und erw. Aufl. Frankfurt/Main: Campus-Verlag, 2004

[BoHe99] BODE, A.; HELLWAGNER, H.: *Leistungsbewertung und Fehlertoleranz.* In: RECHENBERG, P.; POMBERGER, G. (Hrsg.): *Informatik-Handbuch.* 2., aktualisierte und erw. Aufl. München: Hanser, 1999, S. 409–422

[Bor+05] BORN, M.; HOLZ, E.; KATH, O.: *Softwareentwicklung mit UML 2.* München: Addison-Wesley, 2005

[BrBu05] VOM BROCKE, J.; BUDDENDICK, C.: *Security Awareness Management - Konzeption, Methoden und Anwendung.* In: FERSTL, O. K.; ECKERT, S.; ISSELHORST, T.; SINZ, E. J. (Hrsg.): *Wirtschaftsinformatik 2005.* Heidelberg: Physica-Verlag, 2005, S. 1227–1246

[BrNa89] BREWER, D. F. C.; NASH, M. J.: *The Chinese Wall security policy.* In: IEEE (HRSG.): *Proceedings IEEE Symposium on Security and Privacy.* Washington, DC: IEEE Computer Society, 1989, S. 206–214

[Brom10] BROMBA, M.: *Stochastische Sicherheitstheorie.*
URL http://www.bromba.com/knowhow/Was_ist_Sicherheit.htm – Überprüfungsdatum 11.08.2010

[BrSc95] BRINKLEY, D. L.; SCHELL, R. R.: *Concepts and Terminology for Computer Security.* In: ABRAMS, M. D. (Hrsg.): *Information security : An integrated collection of essays.* Los Alamitos, Calif.: IEEE Computer Society, 1995, S. 40–97

[BSI06] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Authentisierung im E-Government : Mechanismen und Anwendungsfelder der Authentisierung.* In: BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (HRSG.): *E-Government-Handbuch.* Köln: Bundesanzeiger-Verlagsges., 2006

[BSI07] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Kurzinformation Biometrie.*
URL http://www.bsi.bund.de/literat/faltbl/F23Biometrie.pdf – Überprüfungsdatum 09.10.2009

[BSI08a] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS).* Version 1.5.
URL https://www.bsi.bund.de/cae/servlet/contentblob/471450/publicationFile/30749/standard_1001.pdf – Überprüfungsdatum 06.04.2010

[BSI08b] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Standard 100-2: IT-Grundschutz - Vorgehensweise.* Version 2.0.
URL https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30748/standard_1002.pdf – Überprüfungsdatum 14.04.2010

[BSI08c] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz.* Version 2.5.
URL https://www.bsi.bund.de/cae/servlet/contentblob/471454/publicationFile/30747/standard_1003.pdf – Überprüfungsdatum 14.04.2010

[BSI08d] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *BSI-Standard 100-4: Notfallmanagement.* Version 1.0.
URL https://www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30746/standard_1004.pdf – Überprüfungsdatum 14.04.2010

[BSI09] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *IT-Grundschutz-Kataloge.* 11. Ergänzungslieferung.
URL https://www.bsi.bund.de/cae/servlet/contentblob/478418/publicationFile/54741/it-grundschutz-kataloge_2009_EL11_de.pdf – Überprüfungsdatum 06.04.2010

[BSI91] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *ITSEC : Information Technology Security Evaluation Criteria.*
URL http://www.bsi.de/zertifiz/itkrit/itsec-dt.pdf – Überprüfungsdatum 26.02.2008

[Buch08] BUCHMANN, J.: *Einführung in die Kryptographie.* Vierte, erweiterte Auflage. Berlin, Heidelberg: Springer-Verlag, 2008

[Bund01a] BUNDESMINISTERIUM DER JUSTIZ: *Gesetz über Rahmenbedingungen für elektronische Signaturen* (2001).
URL http://bundesrecht.juris.de/bundesrecht/sigg_2001/gesamt.pdf – Überprüfungsdatum 25.03.2009

[Bund01b] BUNDESMINISTERIUM DER JUSTIZ: *Verordnung zur elektronischen Signatur* (2001).
URL http://bundesrecht.juris.de/bundesrecht/sigv_2001/gesamt.pdf – Überprüfungsdatum 16.04.2009

[Bund90] BUNDESMINISTERIUM DER JUSTIZ: *Bundesdatenschutzgesetz* (1990).
URL http://bundesrecht.juris.de/bundesrecht/bdsg_1990/gesamt.pdf – Überprüfungsdatum 16.04.2009

[Bund97] BUNDESMINISTERIUM DER JUSTIZ: *Handelsgesetzbuch* (1997).
URL http://bundesrecht.juris.de/bundesrecht/hgb/gesamt.pdf – Überprüfungsdatum 16.04.2009

[CC06] *Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model.*
URL http://www.commoncriteriaportal.org/public/files/CCPART1V3.1R1.pdf - Überprüfungsdatum 26.02.2008

[Clar07] CLARK, I.: *An Introduction to Role-Based Access Control.* In: TIPTON, H. F.; KRAUSE, M. (Hrsg.): *Information security management handbook.* 6th ed. Boca Raton: Auerbach Publications, 2007, S. 751–763

[ClWi87] CLARK, D.; WILSON, D. R.: *A Comparison of Commercial and Military Computer Security Policies.* In: IEEE (HRSG.): *IEEE Symposium of Security and Privacy,* 1987, S. 184–194

[Coyl08] COYLE, R. G.: *System dynamics modelling : A practical approach.* London: Chapman & Hall, 2008

[Davi07] DAVIS, J.: *Authentication and the Role of Tokens.* In: TIPTON, H. F.; KRAUSE, M. (Hrsg.): *Information security management handbook.* 6th ed. Boca Raton: Auerbach Publications, 2007, S. 153–160

[DCMI08] DCMI: *DCMI Metadata Terms.*
URL http://dublincore.org/documents/dcmi-terms/ – Überprüfungsdatum 25.08.2010

[DeBu98] DEUTSCHER BUNDESTAG: *Drucksache 13/10038* (1998). URL http://dip21.bundestag.de/dip21/btd/13/100/1310038.pdf – Überprüfungsdatum 11.12.2009

[Delo05] DELOITTE: *2005 Global Security Survey.* URL http://www.deloitte.com/dtt/cda/doc/content /dtt_financialservices_2005GlobalSecuritySurvey_2005-07-21.pdf – Überprüfungsdatum 22.10.2008

[Den+96] DENG, R. H.; GONG, L.; LAZAR, A.; WANG, W.: *Practical protocols for certified electronic mail.* In: *Journal of Network and Systems Management ,* 4 (1996), Nr. 3, S. 279–297

[Denn76] DENNING, D.: *A lattice model of secure information flow.* In: *Communications of the ACM ,* 19 (1976), Nr. 5, S. 236–243

[DeSt00] DEVANBU, P. T.; STUBBLEBINE, S.: *Software engineering for security: a roadmap.* In: FINKELSTEIN, A. (Hrsg.): *The future of software engineering 2000 : 22nd International Conference on Software Engineering.* New York: Association for Computing Machinery, 2000, S. 227–239

[Dick07] DICKE, R.: *Strategische Unternehmensplanung mit Hilfe eines Assumption-based-Truth-Maintenance-Systems (ATMS).* Wiesbaden: Deutscher Universitäts-Verlag, 2007

[Dier04] DIERSTEIN, R.: *Sicherheit in der Informationstechnik - der Begriff IT-Sicherheit.* In: *Informatik Spektrum ,* 27 (2004), Nr. 4, S. 343–353

[DiHe76] DIFFIE, W.; HELLMAN, M. E.: *New Directions in Cryptography.* In: *IEEE Transactions on Information Theory ,* IT-22 (1976), Nr. 6, S. 644–654

[DIN87] DEUTSCHES INSTITUT FÜR NORMUNG; VERBAND DEUTSCHER ELEKTROTECHNIKER, DIN VDE 31000-2: *Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse,* 1987

[DiRe08] DIERKS, T.; RESCORLA, E.: *The Transport Layer Security (TLS) Protocol Version 1.2.* URL http://www.ietf.org/rfc/rfc5246.txt – Überprüfungsdatum 10.07.2009

[DoD85] DEPARTMENT OF DEFENSE: *Trusted Computer System Evaluation Criteria (TCSEC).* DoD 5200.28-STD. URL http://csrc.nist.gov/publications/history/dod85.pdf – Überprüfungsdatum 14.01.2009

[DoPe06] DOBMEIER, W.; PERNUL, G.: *Modellierung von Zugriffsrichtlinien für offene Systeme.* In: WESKE, M.; NÜTTGENS, M. (Hrsg.): *Methoden, Konzepte und Technologien für die Entwicklung von dienstbasierten Informationssystemen : EMISA 2006.* Bonn: Ges. für Informatik, 2006, S. 35–48

[DoSc05] DOMSCHKE, W.; SCHOLL, A.: *Grundlagen der Betriebswirtschaftslehre.* 3., verb. Aufl. Berlin, Heidelberg: Springer-Verlag, 2005

[DySo08] DYCKHOFF, H.; SOUREN, R.: *Nachhaltige Unternehmensführung.* Berlin: Springer-Verlag, 2008

[EaJo01] EASTLAKE, D.; JONES, P.: *RFC 3174 - US Secure Hash Algorithm 1 (SHA1).* URL http://www.ietf.org/rfc/rfc3174.txt – Überprüfungsdatum 24.03.2009

[Ecke06] ECKERT, C.: *IT-Sicherheit : Konzepte, Verfahren, Protokolle.* 4., überarb. Aufl. München: Oldenbourg, 2006

[ElGa85] EL GAMAL, T.: *A public key cryptosystem and a signature scheme based on discrete logarithms.* In: BLAKLEY, G. R. (Hrsg.): *Advances in cryptology : CRYPTO '84.* Berlin: Springer-Verlag, 1985, S. 10–18

[Endr03] ENDRES, A.: *Softwarequalität aus Nutzersicht und ihre wirtschaftliche Bewertung.* In: *Informatik Spektrum ,* 26 (2003), Nr. 1, S. 20–25

[EsAt06] ESCHWEILER, J.; ATENCIO PSILLE, D. E.: *Security@Work : Pragmatische Konzeption und Implementierung von IT-Sicherheit mit Lösungsbeispielen auf Open-Source-Basis.* Berlin, Heidelberg: Springer-Verlag, 2006

[FeKu92] FERRAIOLO, D. F.; KUHN, D. R.: *Role-Based Access Controls.* In: *Proceedings of the 15th National Computer Security Conference,* S. 554–563

[FeMa98] FEUSTEL, E. A.; MAYFIELD, T.: *The DGSA: unmet information security challenges for operating system designers.* In: *ACM SIGOPS Operating System Review ,* 32 (1998), Nr. 1, S. 3–22

[FePf00] FEDERRATH, H.; PFITZMANN, A.: *Gliederung und Systematisierung von Schutzzielen in IT-Systemen.* In: *DuD - Datenschutz und Datensicherheit ,* 24 (2000), Nr. 12, S. 704–710

[Fers79] FERSTL, O. K.: *Konstruktion und Analyse von Simulationsmodellen.* Königstein/Ts.: Hain, 1979

[Fers92] FERSTL, O. K.: *Integrationskonzepte Betrieblicher Anwendungssysteme.* Fachbericht Informatik, Universität Koblenz-Landau, 1992

[FeSi08] FERSTL, O. K.; SINZ, E. J.: *Grundlagen der Wirtschaftsinformatik.* 6. Aufl. München: Oldenbourg, 2008

[FeSi84] FERSTL, O. K.; SINZ, E. J.: *Software-Konzepte der Wirtschaftsinformatik.* Berlin: de Gruyter, 1984

[FeSi92] FERSTL, O. K.; SINZ, E. J.: *Glossar zum Begriffssystem des Semantischen Objektmodells (SOM).* Bamberger Beiträge zur Wirtschaftsinformatik, Nr. 11, Otto-Friedrich-Universität Bamberg, 1992

[FeSi93] FERSTL, O. K.; SINZ, E. J.: *Der Modellierungsansatz des Semantischen Objektmodells (SOM).* Bamberger Beiträge zur Wirtschaftsinformatik, Nr. 18, Otto-Friedrich-Universität Bamberg, 1993

[FeSi95a] FERSTL, O. K.; SINZ, E. J.: *Der Ansatz des Semantischen Objektmodells (SOM) zur Modellierung von Geschäftsprozessen.* In: *Wirtschaftsinformatik ,* 37 (1995), Nr. 3, S. 209–220

[FeSi95b] FERSTL, O. K.; SINZ, E. J.: *Re-Engineering von Geschäftsprozessen auf der Grundlage des SOM-Ansatzes.* Bamberger Beiträge zur Wirtschaftsinformatik, Nr. 26, Otto-Friedrich-Universität Bamberg, 1995

[FeSi97] FERSTL, O. K.; SINZ, E. J.: *Modeling of Business Systems Using the Semantic Object Model (SOM) - A Methodological Framework.* In: BERNUS, P.; MERTINS, K.; SCHMIDT, G. (Hrsg.): *Handbook on architectures of information systems.* Berlin: Springer-Verlag, 1997

[Fire03] FIRESMITH, D. G.: *Engineering Security Requirements.* In: *Journal of Object Technology ,* 2 (2003), Nr. 1, S. 53–68

[Fire04] FIRESMITH, D. G.: *Specifying Reusable Security Requirements.* In: *Journal of Object Technology ,* 3 (2004), Nr. 1, S. 61–75

[Fire05] FIRESMITH, D. G.: *Analyzing the Security Significance of System Requirements.* In: IEEE (HRSG.): *Proceedings Symposium on Requirements Engineering for Information Security : SREIS 2005,* 2005

[FiSc05] FINK, A.; SCHNEIDEREIT, G.; VOß, S.: *Grundlagen der Wirtschaftsinformatik.* 2., überarb. Aufl. Heidelberg: Physica-Verlag, 2005

[FiSh86] FIAT A.; SHAMIR, A.: *How to Prove Yourself: Practical Solutions to Identification and Signature Problems.* In: ODLYZKO, A. M. (Hrsg.): *Advances in cryptology : CRYPTO '86.* Berlin: Springer-Verlag, 1987, S. 186–194

[FoBa01] FOEGEN, M.; BATTENFELD, J.: *Rolle der Architektur in der Anwendungsentwicklung.* In: *Informatik Spektrum ,* 24 (2001), S. 290–301

[Foeg03] FOEGEN, M.: *Architektur und Architekturmanagement.* In: *HMD - Praxis der Wirtschaftsinformatik* (2003), Nr. 232, S. 57–65

[Fox03] FOX, D.: *Security Awareness.* In: *DuD - Datenschutz und Datensicherheit ,* 27 (2003), Nr. 11, S. 676–680

[Fra+99] FRANKS, J.; HALLAM-BAKER, P.; HOSTETLER, J.; LAWRENCE, S.; LEACH, P.; LUOTONEN, A.; SINK, E.; STEWART, L.: *RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication.*
URL http://www.ietf.org/rfc/rfc2617.txt – Überprüfungsdatum 20.03.2009

[FrDa93] FRIES, O.; DAMM, F.: *Sicherheitsmechanismen.* In: FRIES, O.; DAMM, F. (Hrsg.): *Sicherheitsmechanismen : Bausteine zur Entwicklung sicherer Systeme.* München: Oldenbourg, 1993, S. 9–30

[FuKe99] FUMY, W.; KESSLER, V.: *Kryptologie und Datensicherheit.* In: RECHENBERG, P.; POMBERGER, G. (Hrsg.): *Informatik-Handbuch.* 2., aktualisierte und erw. Aufl. München: Hanser, 1999, S. 217–238

[FuPe07] FUCHS, L.; PERNUL, G.: *Supporting Compliant and Secure User Handling - A Structured Approach for In-House Identity Management.* In: IEEE (HRSG.): *The Second International Conference on Availability, Reliability and Security, 2007 : ARES 2007.* Los Alamitos CA: IEEE Computer Society, 2007, S. 374–384

[FuPr08] FUCHS, L.; PREIS, A.: *BusiROLE: A Model for Integrating Business Roles into Identity Management.* In: FURNELL, S.; KATSIKAS, S. K.; LIOY, A. (Hrsg.): *Trust, Privacy and Security in Digital Business : TrustBus 2008.* Berlin, Heidelberg: Springer-Verlag, 2008, S. 128–138

[Gada08] GADATSCH, A.: *Grundkurs Geschäftsprozess-Management : Methoden und Werkzeuge für die IT-Praxis.* 5., erw. und überarb. Aufl. Wiesbaden: Friedr. Vieweg & Sohn Verlag, 2008

[Garl00] GARLAN, D.: *Software architecture: a roadmap.* In: FINKELSTEIN, A. (Hrsg.): *The future of software engineering 2000 : 22nd International Con-*

ference on Software Engineering. New York: Association for Computing Machinery, 2000, S. 91–101

[GeJe01] GERD TOM MARKOTTEN, D.; JENDRICKE, U.: *Identitätsmanagement im E-Commerce.* In: *it+ti Informationstechnik und Technische Informatik ,* 43 (2001), Nr. 5, S. 236--245

[GeKo08] GEIGER, W.; KOTTE, W.: *Handbuch Qualität : Grundlagen und Elemente des Qualitätsmanagements ; Systeme, Perspektiven.* 5., vollst. überarb. und erw. Aufl. Wiesbaden: Vieweg, 2008

[Glae02] GLAEßNER, G. J.: *Sicherheit und Freiheit.* In: *Aus Politik und Zeitgeschichte* (2002), 10-11, S. 3–13

[Glin07] GLINZ, M.: *On Non-Functional Requirements.* In: SUTCLIFFE, A. (Hrsg.): *15th IEEE International Requirements Engineering Conference.* Los Alamitos, Calif.: IEEE Computer Society, 2007, S. 21–26

[Goll01] GOLLMANN, D.: *Computer security.* Repr. Chichester: Wiley & Sons, 2001

[GrSc82] GROCHLA, E.; SCHACKERT, H. R.: *Datenschutz im Betrieb : Organisation und Wirtschaftlichkeitsaspekte.* Braunschweig: Vieweg, 1982

[Gru+07] GRUHN, V.; HAASE, C.; KÖHLER, A.; KRESSE, T.; WOLFF-MARTING, V.: *Elektronische Signaturen in modernen Geschäftsprozessen.* Wiesbaden: Friedr. Vieweg & Sohn Verlag, 2007

[GüRu03] GÜRGENS, S.; RUDOLPH, C.: *Security Analysis of (Un-) Fair Non-repudiation Protocols.* In: ABDALLAH, A. E. (Hrsg.): *Formal aspects of security : First international conference, London, UK, December 16-18 , 2002.* Berlin: Springer-Verlag, 2003, S. 229–232

[HaBr09] HAFNER, M.; BREU, R.: *Security engineering for service-oriented architectures.* Berlin: Springer-Verlag, 2009

[Haf+06] HAFNER, M.; BREU, R.; AGREITER, B.; NOVAK, A.: *SECTET: an extensible framework for the realization of secure inter-organizational workflows.* In: *Internet Research ,* 16 (2006), Nr. 5, S. 491–506

[Hahn06] HAHN, D.: *Strategische Unternehmensführung - Grundkonzept.* In: HAHN, D.; TAYLOR, B. (Hrsg.): *Strategische Unternehmungsplanung - Strategische Unternehmungsführung : Stand und Entwicklungstendenzen.* Berlin, Heidelberg: Springer-Verlag, 2006, S. 29–50

[Hamm99] HAMMEL, C.: *Generische Spezifikation betrieblicher Anwendungssysteme.* Aachen: Shaker, 1999

[Har+76] HARRISON, M. H.; RUZZO, W. L.; ULLMAN, J. D.: *Protection of operating systems.* In: *Communications of the ACM ,* 19 (1976), Nr. 8, S. 461–471

[HeBe00] HERFERT, M.; BERGER, A.: *Persistente digitale Identitäten ohne globalen Namen.* In: HORSTER, P. (Hrsg.): *Systemsicherheit : Grundlagen, Konzepte, Realisierungen, Anwendungen.* Braunschweig: Vieweg, 2000, S. 227–242

[Hein91] HEINEN, E.: *Industriebetriebslehre als entscheidungsorientierte Unternehmensführung.* In: HEINEN, E.; DIETEL, B. (Hrsg.): *Industriebetriebslehre.* 9., vollst. neu bearb. u. erw. Aufl. Wiesbaden: Gabler Verlag, 1991, S. 1–72

[Hein99a] HEINRICH, L. J.: *Grundlagen der Wirtschaftsinformatik.* In: RECHENBERG, P.; POMBERGER, G. (Hrsg.): *Informatik-Handbuch.* 2., aktualisierte und erw. Aufl. München: Hanser, 1999, S. 1019–1034

[Hein99b] HEINRICH, L. J.: *Informationsmanagement.* In: RECHENBERG, P.; POMBERGER, G. (Hrsg.): *Informatik-Handbuch.* 2., aktualisierte und erw. Aufl. München: Hanser, 1999, S. 1065–1080

[Heit07] HEITMANN, M.: *IT-Sicherheit in vertikalen F&E-Kooperationen der Automobilindustrie.* Wiesbaden: Deutscher Universitäts-Verlag, 2007

[HeLe05] HEINRICH, L. J.; LEHNER, F.: *Informationsmanagement : Planung, Überwachung und Steuerung der Informationsinfrastruktur.* 8., vollst. überarb. und erg. Aufl. München: Oldenbourg, 2005

[HeMö00] HENHAPL, B.; MÖLLER, B.: *Public-Key-Infrastrukturen.* In: *HMD - Praxis der Wirtschaftsinformatik* (2000), Nr. 216, S. 58–66

[Herr01] HERRMANN, G.: *Verläßlichkeit von Geschäftsprozessen : Konzeptionelle Modellbildung und Realisierungsrahmen.* Dissertation, Universität Essen, 2001

[Hopf00] HOPFENBECK, W.: *Allgemeine Betriebswirtschafts- und Managementlehre : Das Unternehmen im Spannungsfeld zwischen ökonomischen, sozialen und ökologischen Interessen.* 13., vollst. überarb. und erw. Aufl. Landsberg/Lech: Verlag Moderne Industrie, 2000

[HoPr03] HOPPE, G.; PRIEß, A.: *Sicherheit von Informationssystemen : Gefahren, Maßnahmen und Management im IT-Bereich.* Herne/Berlin: Neue Wirtschafts-Briefe, 2003

[HoTe00] HORSTER, P.; TEIWES, S.: *Strategien zu Aufbau und Betrieb von Public-Key-Infrastrukturen.* In: HORSTER, P. (Hrsg.): *Systemsicherheit : Grundlagen, Konzepte, Realisierungen, Anwendungen.* Braunschweig: Vieweg, 2000, S. 315–330

[Hühn08] HÜHNLEIN, D.: *Identitätsmanagement : Eine visualisierte Begriffsbestimmung.* In: *DuD - Datenschutz und Datensicherheit ,* 32 (2008), Nr. 3, S. 161–163

[INSA91] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP: *Safety culture.* Vienna: International Atomic Energy Agency, 1991

[INSA92] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP: *The Chernobyl accident - Updating of INSAG-1.* Vienna: International Atomic Energy Agency, 1992

[Jeck04] JECKLE, M.: *UML 2 glasklar.* München: Hanser, 2004

[Jür05] JÜRJENS, J.: *Secure Systems Development with UML.* Berlin, Heidelberg: Springer-Verlag, 2005

[Kail96] KAILAR, R.: *Accountability in Electronic Commerce Protocols.* In: *IEEE Transactions on Software Engineering ,* 22 (1996), Nr. 5, S. 313–328

[KBSt09] KOORDINIERUNGS- UND BERATUNGSSTELLE DER BUNDESREGIERUNG FÜR INFORMATIONSTECHNIK: *V-Modell XT : Teil 1: Grundlagen des V-Modells.* URL http://ftp.tu-clausthal.de/pub/institute/informatik/v-modell-

xt/Releases/1.3/V-Modell-XT-Gesamt.pdf – Überprüfungsdatum 12.07.2010

[KBV10] KASSENÄRZTLICHE BUNDESVEREINIGUNG: *Medizinische Versorgungszentren aktuell : 3. Quartal 2009.* URL http://daris.kbv.de/daris/link.asp?ID=1003760536 – Überprüfungsdatum 06.06.2010

[Kers95] KERSTEN, H.: *Sicherheit in der Informationstechnik : Einführung in Probleme, Konzepte und Lösungen.* 2., vollst. überarb. Aufl. München: Oldenbourg, 1995

[Kizz05] KIZZA, J. M.: *Computer Network Security.* Boston, MA: Springer Science+Business Media LLC, 2005

[Kla+08] KLARL, H.; WOLFF, C.; EMIG, C.: *Abbildung von Zugriffskontrollaussagen in Geschäftsprozessmodellen.* In: GESELLSCHAFT FÜR INFORMATIK. (HRSG.): *Verhaltensmodellierung - Best Practices und neue Erkenntnisse : Modellierung 2008.* Berlin, 2008

[Kla+09a] KLARL, H.; WOLFF, C.; EMIG, C.: *Identity Management in Business Process Modelling: A Model-driven Approach.* In: HANSEN, H. R.; KARAGIANNIS, D.; FILL, H. G. (Hrsg.): *Business Services: Konzepte, Technologien, Anwendungen : 9. Internationale Tagung Wirtschaftsinformatik.* Wien, 2009, S. 161–170

[Kla+09b] KLARL, H.; MOLITORISZ, K.; EMIG, C.; KLINGER, K.; ABECK, S.: *Extending Role-based Access Control for Business Usage.* In: *IEEE Conference on Emerging Security Information, Systems and Technologies : SECURWARE '09.* Athen, 2009, S. 136–141

[Köni06] KÖNIGS, H. P.: *IT-Risiko-Management mit System.* 2., korrigierte Auflage. Wiesbaden: Friedr. Vieweg & Sohn Verlag, 2006

[Konr98] KONRAD, P.: *Geschäftsprozeß-orientierte Simulation der Informationssicherheit : Entwicklung und empirische Evaluierung eines Systems zur Unterstützung des Sicherheitsmanagements.* Lohmar: Eul, 1998

[Kosi76] KOSIOL, E.: *Organisation der Unternehmung.* 2. Aufl. Wiesbaden: Gabler Verlag, 1976

[Kral89] KRALLMANN, H.: *EDV-Sicherheitsmanagement : Integrierte Sicherheitskonzepte für betriebliche Informations- und Kommunikationssysteme.* Berlin: Schmidt, 1989

[Krei87] KREILKAMP, E.: *Strategisches Management und Marketing.* Berlin: de Gruyter, 1987

[KuMa91] KUPSCH, P. U.; MARR, R.: *Personalwirtschaft.* In: HEINEN, E.; DIETEL, B. (Hrsg.): *Industriebetriebslehre.* 9., vollst. neu bearb. u. erw. Aufl. Wiesbaden: Gabler Verlag, 1991, S. 729–896

[Kurt93] KURTH, H.: *Grundlagen der Informationssicherheit.* In: POHL, H.; WECK, G. (Hrsg.): *Einführung in die Informationssicherheit.* München: Oldenbourg, 1993, S. 85–122

[Lamp74] LAMPSON, B. W.: *Protection.* In: ACM (HRSG.): *Operating Systems Review,* 1974

[Lehn95] LEHNER, F.: *Wirtschaftsinformatik : Theoretische Grundlagen.* München: Hanser, 1995

[Lip+92] LIPPOLD, H.; STELZER, D.; KONRAD, P.: *Sicherheitskonzepte und ihre Verknüpfung mit Sicherheitsstrategie und Sicherheitsmanagement.* In: *Wirtschaftsinformatik ,* 34 (1992), Nr. 4, S. 367–377

[Loch05] LOCHER, C.: *Ein Steuerungsmodell für das Management von IV-Sicherheitsrisiken bei Kreditinstituten.* In: FERSTL, O. K.; ECKERT, S.; ISSELHORST, T.; SINZ, E. J. (Hrsg.): *Wirtschaftsinformatik 2005.* Heidelberg: Physica-Verlag, 2005, S. 1207–1225

[Lodd03] LODDERSTEDT, T.: *Model Driven Security : From UML Models To Access Control Architectures.* Dissertation, Albert-Ludwigs-Universität Freiburg, 2003

[Lubi06] LUBICH, H. P.: *IT-Sicherheit: Systematik, aktuelle Probleme und Kosten-Nutzen-Betrachtungen.* In: *HMD - Praxis der Wirtschaftsinformatik* (2006), Nr. 248, S. 6–15

[Mali97] MALISCHEWSKI, C.: *Generierung und Spezifikation betrieblicher Anwendungssysteme auf der Basis von Geschäftsprozessmodellen.* Aachen: Shaker, 1997

[Men+01] MENEZES, A. J.; VAN OORSCHOT, P. C.; VANSTONE, S. A.: *Handbook of applied cryptography.* Boca Raton: CRC Press, 2001

[MiSi06] MITNICK, K. D.; SIMON, W. L.: *Die Kunst der Täuschung : Risikofaktor Mensch.* Heidelberg: mitp-Verlag, 2006

[Müll05] MÜLLER, K. R.: *Handbuch Unternehmenssicherheit : Umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System.* Wiesbaden: Vieweg, 2005

[Mura01] MURAUER, J.: *Informationsflussorientierte Verfahren zum Zugriffschutz in Computersystemen.* Dissertation, Johannes Kepler Universität Linz, 2001

[Müßi06] MÜßIG, S.: *Haben Sicherheitsinvestitionen eine Rendite?* In: *HMD - Praxis der Wirtschaftsinformatik* (2006), Nr. 248, S. 35–43

[NBS80] NATIONAL BUREAU OF STANDARDS, FIPS 73: *Guidelines for Security of Computer Appliances,* 1980

[Neu+06] NEUBAUER, T.; KLEMEN, M.; BIFFL, S.: *Secure Business Process Management: A Roadmap.* In: *The First International Conference on Availability, Reliability and Security : ARES 2006.* Los Alamitos, Calif.: IEEE Computer Society, 2006, S. 457–464

[NiJa06] NING, P.; JAJODIA, S.: *Intrusion Detection Systems Basics, Bd.* 3. In: BIDGOLI, H. (Hrsg.): *Handbook of information security.* Hoboken NJ: Wiley & Sons, 2006, S. 685–700

[NIST01] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FIPS 197: *Advanced Encryption Standard (AES),* 2001

[Nohl09] NOHLBERG, M.: *Why Humans are the weakest Link.* In: GUPTA, M.; SHARMAN, R. (Hrsg.): *Social and human elements of information security : Emerging trends and countermeasures.* Hershey PA: Information Science Reference, 2009, S. 15–26

[OASI05] OASIS: *eXtensible Access Control Markup Language (XACML) : Version 2.0.*
URL http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf – Überprüfungsdatum 07.09.2010

[OECD02] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT: *OECD Guidelines for the Security of Information Systems and Networks.*
URL http://www.oecd.org/dataoecd/16/22/15582260.pdf – Überprüfungsdatum 22.10.2008

[Oest07] OESTEREICH, B.: *OEP - oose Engineering Processes : Vorgehensleitfaden für agile Softwareprojekte.* Heidelberg: dpunkt Verlag, 2007

[Oni+09] ONIEVA, J. A.; LOPEZ, J.; ZHOU J.: *Fundamentals of Non-repudiation.* In: *Secure Multi-Party Non-Repudiation Protocols and Applications.* Boston, MA: Springer-Verlag US, 2009, S. 1–15

[Oppl07] OPPLIGER, R.: *IT Security: In Search of the Holy Grail.* In: *Communications of the ACM ,* 50 (2007), Nr. 2, S. 96–98

[Oppl97] OPPLIGER, R.: *IT-Sicherheit : Grundlagen und Umsetzung in der Praxis.* Braunschweig: Vieweg, 1997

[Öste95] ÖSTERLE, H.: *Business Engineering : Prozeß- und Systementwicklung I: Entwurfstechniken.* 2., verbess. Aufl. Berlin: Springer-Verlag, 1995

[OWAS07] OWASP: *CLASP v1.2.*
URL http://www.list.org/~chandra/clasp/OWASP-CLASP.zip – Überprüfungsdatum 29.01.2010

[Pern95] PERNUL, G.: *Informations Systems Security - Scope, State-of-the-art and Evaluation of Techniques.* In: *International Journal of Information Management ,* 15 (1995), Nr. 3, S. 239–255

[Petz96] PETZEL, E.: *Management der Informationssicherheit : Grundlagen, kritische Bestandsaufnahme und Neuansatz.* Weiden, Regensburg: Eurotrans, 1996

[PiFr95] PICOT, A.; FRANCK, E.: *Prozeßorganisation - Eine Bewertung der neuen Ansätze aus Sicht der Organisationslehre.* In: NIPPA, M.; PICOT, A. (Hrsg.): *Management prozeßorientierter Unternehmen - Ansätze, Methoden und Fallstudien.* 2. Aufl. Frankfurt am Main: Campus-Verlag, 1995, S. 13–38

[PoBl04] POHLMANN, N.; BLUMBERG, H. F.: *Der IT-Sicherheitsleitfaden.* Bonn: mitp-Verlag, 2004

[Pohl04] POHL, H.: *Taxonomie und Modellbildung in der Informationssicherheit.* In: *DuD - Datenschutz und Datensicherheit ,* 28 (2004), Nr. 11, S. 678–685

[Pohl06] POHLMANN, N.: *Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen?* In: *HMD - Praxis der Wirtschaftsinformatik* (2006), Nr. 248, S. 26–34

[Port98] PORTER, M. E.: *Competitive strategy.* New York, NY: Free Press, 1998

[PoWe93] POHL, H.; WECK, G.: *Stand und Zukunft der Informationssicherheit.* In: POHL, H.; WECK, G. (Hrsg.): *Einführung in die Informationssicherheit.* München: Oldenbourg, 1993, S. 9–31

[Pres01] PRESSMAN, R. S.: *Software engineering : Apractitioner's approach.* 5. ed. Boston, Mass: McGraw Hill, 2001

[Pri+05] PRIEBE, T.; DOBMEIER, W.; MUSCHALL, B.; PERNUL, G.: *ABAC - Ein Referenzmodell für attributbasierte Zugriffskontrolle.* In: FEDERRATH, H. (Hrsg.): *Sicherheit 2005.* Bonn: Ges. für Informatik, 2005, S. 285–296

[Pri+07] PRIEBE, T.; DOBMEIER, W.; SCHLÄGER, C.; KAMPRATH, N.: *Supporting Attribute-based Access Control in Authorization and Authentication Infrastructures with Ontologies.* In: *Journal of Software ,* 2 (2007), Nr. 1, S. 27–38

[PrMi04] PREUß, W.; MILLER, R.: *Integriertes Qualitäts- und Sicherheitsmanagement in der Kerntechnik: Auditierung und Zertifizierung unter Berücksichtigung der Sicherheitskultur.*
URL http://www.mensch-technik-organisation.de/pdf /sicherheitsmanagement-sicherheitskultur.pdf – Überprüfungsdatum 22.10.2008

[Proc+09] PROCTOR, R. W.; SCHULTZ, E. E.; VU, K. P. L.: *Human Factors in Information Security and Privacy.* In: GUPTA, J.; SHARMA, S. K. (Hrsg.): *Handbook of research on information security and assurance.* Hershey, Pa.: Information Science Reference, 2009, S. 402–414

[Püt+09] PÜTZ, C.; WAGNER, D.; FERSTL, O. K.; SINZ, E. J.: *Geschäftsprozesse in Medizinischen Versorgungszentren und ihre Flexibilitätsanforderungen - ein fallstudienbasiertes Szenario.* Arbeitsbericht forFLEX-2009-001, Otto-Friedrich-Universität Bamberg, 2009

[Püt+10] PÜTZ, C.; WAGNER, D.; FERSTL, O. K.; SINZ, E. J.: *Konzeption eines generischen Geschäftsprozessmodells für Medizinische Versorgungszentren.* In: SCHUMANN, M.; KOLBE, L. M.; BREITNER, M. H.; FRERICHS, A. (Hrsg.): *Multikonferenz Wirtschaftsinformatik 2010.* Göttingen: Universitätsverlag Göttingen, 2010, S. 143–154

[Qui+90] QUISQUATER, J. J.; GUILLOU, L. C.; BERSON, T. A.: *How to Explain Zero-Knowledge Protocols to Your Children.* In: BRASSARD, G. (Hrsg.): *Advances in cryptology : CRYPTO '89.* New York: Springer-Verlag, 1990, S. 628–631

[RaBr06] RAUSCH, A.; BROY, M.: *Das V-Modell XT : Grundlagen, Erfahrungen und Werkzeuge.* Heidelberg, Neckar: dpunkt Verlag, 2006

[Rams04] RAMSDELL, B.: *RFC 3851 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1.*
URL http://www.ietf.org/rfc/rfc3851.txt – Überprüfungsdatum 25.03.2009

[Rath09] RATH, M.: *Rechtliche Aspekte von IT-Compliance.* In: WECKER, G.; LAAK, H. (Hrsg.): *Compliance in der Unternehmerpraxis.* 2. Auflage. Wiesbaden: Gabler Verlag, 2009, S. 149–167

[Riv+78] RIVEST, R.; SHAMIR, A.; ADLEMAN, L.: *A method for obtaining digital signatures and public-key cryptosystems.* In: *Communications of the ACM ,* 21 (1978), S. 120–126

[Rive92] RIVEST, R.: *RFC 1321 - The MD5 Message-Digest Algorithm.* URL http://www.ietf.org/rfc/rfc1321.txt – Überprüfungsdatum 24.03.2009

[Rod+06] RODRÍGUEZ, A.; FERNÁNDEZ-MEDINA, E.; PIATTINI, M.: *Capturing Security Requirements in Business Processes Through a UML 2.0 Activity Diagrams Profile.* In: RODDICK, J. F. (Hrsg.): *Advances in conceptual modeling - theory and practice : ER 2006.* Berlin: Springer-Verlag, 2006, S. 32–42

[Rod+07] RODRÍGUEZ, A.; FERNÁNDEZ-MEDINA, E.; PIATTINI, M.: *A BPMN Extension for the Modeling of Security Requirements in Business Processes.* In: *IEICE Transactions on Information and Systems ,* E90-D (2007), Nr. 4, S. 745–752

[Röh+00] RÖHRIG, S.; KNORR, K.; NOSER, H.: *Sicherheit von E-Business-Anwendungen - Struktur und Quantifizierung.* In: *Wirtschaftsinformatik ,* 42 (2000), Nr. 6, S. 499–507

[Royc87] ROYCE, W. W.: *Managing the development of large software systems.* In: COMPUTER SOCIETY (HRSG.): *International Conference on Software Engineering : Proceedings of the 9th international conference on Software Engineering.* Washington, DC: IEEE Computer Society, 1987, S. 328–338

[Sac+04] SACHITANO, A.; CHAPMAN, R. O.; HAMILTON, J. A.: *Security in software architecture.* In: IEEE (HRSG.): *Fifth Annual IEEE SMC Information Assurance Workshop.* Piscataway, NJ: IEEE Computer Society, 2004, S. 370–376

[SaCa01] SAMARATI, P.; CAPITANI DE VIMERCATI, S.: *Access Control: Policies, Models, and Mechanisms.* In: FOCARDI, R. (Hrsg.): *Foundations of security analysis and design.* Berlin: Springer-Verlag, 2001, S. 138–196

[Sand90] SANDHU, R. S.: *Separation of Duties in Computerized Information Systems.* In: *Proceedings of the IFIP WG11.3 Workshop on Database Security,* 1990, S. 179–190

[Sch+05] SCHMALTZ, R.; GOOS, P.; HAGENHOFF, S.: *Sicherheitsmodelle in Kooperationen.* In: FERSTL, O. K.; ECKERT, S.; ISSELHORST, T.; SINZ, E. J. (Hrsg.): *Wirtschaftsinformatik 2005.* Heidelberg: Physica-Verlag, 2005, S. 1247–1266

[Scha06] SCHADT, D.: *Über die Ökonomie der IT-Sicherheit.* In: *HMD - Praxis der Wirtschaftsinformatik* (2006), Nr. 248, S. 16–25

[Schi99] SCHIER, K.: *Vertrauenswürdige Kommunikation im elektronischen Zahlungsverkehr.* Dissertation, Universität Hamburg, 1999

[Schl04] SCHLITT, M.: *Grundlagen und Methoden für Interpretation und Konstruktion von Informationssystemmodellen.* Dissertation, Otto-Friedrich-Universität Bamberg, 2004

[Schm01] SCHMITZ, K.: *Virtualisierung von wirtschaftswissenschaftlichen Lehr- und Lernsituationen : Konzeption eines Application Framework.* Wiesbaden: Deutscher Universitäts-Verlag, 2001

[Schm06] SCHMIDT, K.: *Der IT-Security-Manager.* München: Hanser, 2006

[Schn99] SCHNEIDER, E. A.: *Security Architecture-Based System Design.* In: ACM (HRSG.): *Proceedings of the 1999 Workshop on New Security Paradigms.* New York: ACM, 1999, S. 25–31

[Schö84] SCHÖNBERG, V.: *Organisatorische und softwaregestützte EDB-Sicherheit.* In: ZIMMERLI, E.; LIEBL, K. (Hrsg.): *Computermißbrauch, Computersicherheit.* Ingelheim: Hohl, 1984, S. 83–194

[Schu02] SCHUMACHER, M.: *Hacker Contest : Sicherheitsprobleme, Lösungen, Beispiele.* Berlin u.a.: Springer-Verlag, 2002

[ScSh04] SCHNEIER, B.; SHAFIR, A.: *Secrets & lies : IT-Sicherheit in einer vernetzten Welt.* Weinheim: dpunkt Verlag, 2004

[ScTe06] SCHLIENGER, T.; TEUFEL, S.: *Informationssicherheit braucht eine Kultur.* In: *BSI Forum* (2006), Nr. 6, S. 63–66

[Shan48] SHANNON, C. E.: *A Mathematical Theory of Communication.* In: *The Bell System Technical Journal ,* 27 (1948), S. 379–423

[ShGa96] SHAW, M.; GARLAN, D.: *Software architecture : Perspectives on an emerging discipline.* Upper Saddle River, NJ: Prentice Hall, 1996

[Shir07] SHIREY, R.: *RFC 4949 - Internet Security Glossary.* Version 2. URL http://www.ietf.org/rfc/rfc4949.txt – Überprüfungsdatum 28.02.2008

[Sinz01] SINZ, E. J.: *Modellierung.* In: MERTENS, P.; BACK, A. (Hrsg.): *Lexikon der Wirtschaftsinformatik.* 4. Aufl. Berlin: Springer-Verlag, 2001, S. 312–313

[Sinz93] SINZ, E. J.: *Datenmodellierung im Strukturierten Entity-Relationship-Modell (SERM).* In: MÜLLER-ETTRICH, G. (Hrsg.): *Fachliche Modellierung von Informationssystemen : Methoden, Vorgehen, Werkzeuge.* Bonn: Addison-Wesley, 1993, S. 61–126

[Sinz96] SINZ, E. J.: *Ansätze zur fachlichen Modellierung betrieblicher Informationssysteme. Entwicklung, aktueller Stand und Trends.* In: HEILMANN, H. (Hrsg.): *Information Engineering : Wirtschaftsinformatik im Schnittpunkt von Wirtschafts-, Sozial- und Ingenieurwissenschaften.* München: Oldenbourg, 1996

[Sinz99a] SINZ, E. J.: *Architektur von Informationssystemen.* In: RECHENBERG, P.; POMBERGER, G. (Hrsg.): *Informatik-Handbuch.* 2., aktualisierte und erw. Aufl. München: Hanser, 1999, S. 1035–1047

[Sinz99b] SINZ, E. J.: *Konstruktion von Informationssystemen.* In: RECHENBERG, P.; POMBERGER, G. (Hrsg.): *Informatik-Handbuch.* 2., aktualisierte und erw. Aufl. München: Hanser, 1999, S. 1049–1064

[Somm07] SOMMERVILLE, I.: *Software engineering.* 8. Aufl. Harlow: Addison-Wesley, 2007

[Spei07] SPEICHERT, H.: *Praxis des IT-Rechts.* 2., aktual. und erw. Aufl. Wiesbaden: Vieweg, 2007

[Stam06] STAMP, M.: *Information security : Principles and practice.* Hoboken, NJ: Wiley & Sons, 2006

[Stau06] STAUD, J.: *Geschäftsprozessanalyse.* Dritte Auflage. Berlin, Heidelberg: Springer-Verlag, 2006

[StBe07] STAHL, T.; BETTIN, J.: *Modellgetriebene Softwareentwicklung : Techniken, Engineering, Management.* 2., akt. und erw. Aufl. Heidelberg: dpunkt Verlag, 2007

[Stel94] STELZER, D.: *Risikoanalyse : Konzepte, Methoden und Werkzeuge.* In: BAUKNECHT, K.; TEUFEL, S. (Hrsg.): *Sicherheit in Informationssystemen : SIS '94,* 1994, S. 185–200

[StHu06] STAMP, M.; HUSHYAR, A.: *Multilevel Security Models.* In: BIDGOLI, H. (Hrsg.): *Handbook of information security.* Hoboken NJ: Wiley & Sons, 2006, S. 987–997

[Stra91] STRAUß, C.: *Informatik-Sicherheitsmanagement.* Stuttgart: Teubner, 1991

[SüGi03] SÜßMILCH-WALTHER, I.; GILLEßEN, S.: *Ein Bezugsrahmen für Rollen in Unternehmungen : Teil 1: Grundlagen, Abgrenzung und Methodik.* Arbeitspapier 1/2003, Universität Erlangen-Nürnberg, 2003

[Swo+08] SWOBODA, J.; SPITZ, S.; PRAMATEFTAKIS, M.: *Kryptographie und IT-Sicherheit.* Wiesbaden: Vieweg+Teubner Verlag, 2008

[TeFe08] TEUBNER, A.; FELLER, T.: *Informationstechnologie, Governance und Compliance.* In: *Wirtschaftsinformatik ,* 50 (2008), Nr. 5, S. 400–407

[Tele06] TELETRUST DEUTSCHLAND E.V.: *Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren.*
URL http://www.teletrust.de/uploads/media/KritKat-3_final.pdf – Überprüfungsdatum 11.10.2009

[TeSc00] TEUFEL, S.; SCHLIENGER, T.: *Informationssicherheit - Wege zur kontrollierten Unsicherheit.* In: *HMD - Praxis der Wirtschaftsinformatik* (2000), Nr. 216, S. 18–31

[TeTe05] TEUBNER, R. A.; TERWEY, J.: *IT-Risikomanagement im Spiegel aktueller Normen und Standards.* In: *HMD - Praxis der Wirtschaftsinformatik* (2005), Nr. 244, S. 95–107

[TeTe07] TESCHL, G.; TESCHL, S.: *Mathematik für Informatiker.* 2. Auflage. Berlin, Heidelberg: Springer-Verlag, 2007

[ThAc06] THOMMEN, J. P.; ACHLEITNER, A. K.: *Allgemeine Betriebswirtschaftslehre : Umfassende Einführung aus managementorientierter Sicht.* 5., überarb. und erw. Aufl. Wiesbaden: Gabler Verlag, 2006

[Thom06] THOMAS, O.: *Das Referenzmodellverständnis in der Wirtschaftsinformatik: Historie, Literaturanalyse und Begriffsexplikation.* In: *IWi - Veröffentlichungen des Instituts für Wirtschaftsinformatik im Deutschen Forschungszentrum für Künstliche Intelligenz* (2006), Nr. 187, S. 1–32

[Vacc07] VACCA, J. R.: *Practical Internet Security.* Boston, MA: Springer Science+Business Media LLC, 2007

[Vei+07] DA VEIGA, A.; MARTINS, N.; ELOFF, J. H. P.: *Information security culture - validation of an assessment instrument.* In: *SA Business Review ,* 11 (2007), Nr. 1, S. 147–166

[ViMc08] VIEGA, J.; MCGRAW, G.: *Building secure software : How to avoid security problems the right way.* 9. Aufl. Boston: Addison-Wesley, 2008

[Voig08] VOIGT, K. I.: *Industrielles Management : Industriebetriebslehre aus prozessorientierter Sicht.* Berlin, Heidelberg: Springer-Verlag, 2008

[vzMü95] VON ZUR MÜHLEN, R.A.H: *Planung sicherer Rechenzentren.* In: POHL, H.; WECK, G. (Hrsg.): *Managementaufgaben im Bereich der Informationssicherheit.* München: Oldenbourg, 1995, S. 179–210

[WaDe88] WALTON, M.; DEMING, W. E.: *The Deming management method.* New York, N.Y.: Putnam Publ. Co., 1988

[WaWa03] WANG, H.; WANG, C.: *Taxonomy of security considerations and software quality.* In: *Communications of the ACM ,* 46 (2003), Nr. 6, S. 75–78

[Weck93] WECK, G.: *Realisierung der Schutzfunktionen.* In: POHL, H.; WECK, G. (Hrsg.): *Einführung in die Informationssicherheit.* München: Oldenbourg, 1993, S. 123–190

[Witt06] WITT, B. C.: *IT-Sicherheit kompakt und verständlich : Eine praxisorientierte Einführung.* Wiesbaden: Vieweg, 2006

[Wol+08] WOLTER, C.; MENZEL, M.; MEINEL, C.: *Modelling Security Goals in Business Processes.* In: KÜHNE, T.; REISIG, W. (Hrsg.): *Modellierung 2008.* Bonn: Ges. für Informatik, 2008, S. 197–212

[Wol+09] WOLTER, C.; MENZEL, M.; SCHAAD, A.; MISELDINE, P.; MEINEL, C.: *Model-driven business process security requirement specification.* In: *Journal of Systems Architecture ,* 55 (2009), Nr. 4, S. 211–233

[Wölf06] WÖLFL, T.: *Formale Modellierung von Authentifizierungs- und Authorisierungsinfrastrukturen.* Wiesbaden: Deutscher Universitäts-Verlag, 2006

[Wolt06] WOLTHUSEN, S. D.: *Revisionssichere Protokollierung in Standardbetriebssystemen.* In: *DuD - Datenschutz und Datensicherheit ,* 30 (2006), Nr. 5, S. 281–284

[Wolt07] WOLTHUSEN, S. D.: *Vertrauenswürdige Protokollierung : Protokollierung mittels nicht-deterministischer nebenläufiger wechselseitiger Überwachung ,* 31 (2007), Nr. 10, S. 740–743

[WoPf00] WOLF, G.; PFITZMANN, A.: *Charakteristika von Schutzzielen und Konsequenzen für Benutzungsschnittstellen.* In: *Informatik Spektrum ,* 23 (2000), S. 173–191

[WoPf99] WOLF, G.; PFITZMANN, A.: *Empowering users to set their protection goals.* In: MÜLLER, G.; RANNENBERG, K. (Hrsg.): *Multilateral Security in Communications : Technology, infrastructure, economy.* München: Addison-Wesley, 1999, S. 113–135

[Wörn03] WÖRNDL, W.: *Privatheit bei dezentraler Verwaltung von Benutzerprofilen.* Dissertation, Technische Universität München, 2003

[WoWi07] WORTMANN, F.; WINTER, R.: *Vorgehensmodelle für die rollenbasierte Autorisierung in heterogenen Systemlandschaften.* In: *Wirtschaftsinformatik ,* 49 (2007), Nr. 6, S. 439–447

[Zimm95] ZIMMERMANN, P. R.: *PGP source code and internals.* Cambridge, Mass: MIT Press, 1995

Anhang

Anhang A: Objektzerlegung im Szenario MVZ

MVZ
- Annahme
  - D: Kurzanamnese
- Orthopädie
  - D: Arztzuweisung
    - V: Arztanfrage
    - D: Arztbestätigung
  - D: Leistungsdaten
- Buchhaltung

KV

Patient

Anhang B: Transaktionszerlegung im Szenario MVZ

D: Vergütung
- V: Abrechnungsdaten
- D: Zahlung

D: Behandlung
- A: Leistungsangebot
- V: Terminvereinbarung
  - V.seq1: Ersterminanfrage
  - V.seq2: Ersterminbestätigung
  - V.seq3: Patienteninformation
- D: Med. Leistung
  - D.par1: Anamnese
  - D.par2: Diagnose
  - D.par3: Orth. Behandlung

Danksagung

Als Autor kann man den Zeitpunkt nur schwerlich vorhersehen, an dem man wirklich am Ende einer Arbeit angelangt ist und „nur“ noch Kleinigkeiten, wie zum Beispiel eine Danksagung, zu ergänzen sind. Hat man diesen erreicht, so ist das durchaus ein angenehmes Gefühl.

Bedanken dafür möchte ich mich in erster Linie bei meinem Doktorvater, Herrn Prof. Dr. Otto K. Ferstl, der mir das Verfassen dieser Dissertation ermöglicht und mich während des Erstellungsprozesses fachlich begleitet hat. Mein Dank gilt außerdem den weiteren Mitgliedern der Promotionskommission, Herrn Prof. Dr. Elmar J. Sinz und Herrn Univ.-Prof. Dr. Dr. habil. Wolfgang Becker, für ihre konstruktiven Anregungen im Rahmen der Kolloquien. Schließlich möchte ich noch Herrn Dipl.-Wirtsch.-Inf. Michael Fischer-Dederra für seine Lektüre der Arbeit und den damit verbundenen Verbesserungsvorschlägen danken.

Für ihr Verständnis und ihre konstante Ermutigung möchte ich Frau Dr. Julia Eiche danken, ohne die ich diese Arbeit nicht hätte fertigstellen können. Weiterhin danke ich meinen Eltern für ihre großartige Unterstützung. Nicht zuletzt möchte ich auch meinem Sohn Felix, der während der Endphase dieser Arbeit zur Welt kam, dafür danken, dass er mir trotz verbesserungswürdiger Schlafgewohnheiten noch genügend Ressourcen zur Fertigstellung ließ.