universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Konzeptualisierung und Implementierung eines Security Layers für ArchiMate“

verfasst von / submitted by

Manuel Timotic, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Diplom-Ingenieur (Dipl.-Ing.)

Wien, 2017 / Vienna 2017

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 066 926
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Wirtschaftsinformatik
Betreut von / Supervisor:	Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

Danksagung

Diese Masterarbeit möchte ich meiner Mutter widmen, die mich während des gesamten Studiums bestmöglich unterstützt hat.

Ich möchte mich an dieser Stelle vor allem bei Herrn Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr für seine intensive Betreuung bei der Anfertigung meiner Masterarbeit bedanken.

Ein besonderes Dankeschön gebührt ebenfalls den Kolleginnen und Kollegen der BOC Information Technologies Consulting GmbH. Insbesondere möchte ich mich bei Christoph Moser und Michael Bültmann für die wertvollen fachlichen Diskussionen bedanken.

Eidesstattliche Erklärung

Ich erkläre eidesstattlich, dass ich die vorliegende Arbeit selbständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel verfasst habe und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Wien, am ....
(Unterschrift)

Abstract (Deutsch) In einer Zeit der immer stärker voranschreitenden Digitalisierung und komplexer werdenden IT-Landschaften setzen Unternehmen vermehrt Enterprise Architecture Management (EAM) ein. Trotz der zahlreichen Überlappungen von EAM und Security Management werden die beiden Managementdomänen oftmals separat voneinander organisiert, sodass sich ergebende Potenziale aus einer gesamtheitlichen Betrachtung nicht heben lassen. Umfassende Frameworks, wie beispielsweise TOGAF (The Open Group Architecture Frameworks), weisen zwar auf die Bedeutung sicherer Architekturen hin, bleiben aber oberflächlich und verweisen auf spezialisierte Frameworks, wie zum Beispiel SABSA. Diese Arbeit beschreibt die Implementierung eines Security Frameworks unter Verwendung der Modellierungssprache ArchiMate (Der Quellcode steht auf CD zur Verfügung). Es wird insbesondere der Bereich Grundschutz abgedeckt. Der Schutzbedarf fokussiert sich dabei auf die Bewertung von Unternehmensdaten und ermöglicht darauf basierend die Bewertung der wesentlichen Vermögenswerte (Assets) der Unternehmen. Für die Umsetzung eines ausreichenden IT-Grundschutzes wird der Grundschutzkatalog des BSI verwendet. Dieser bietet einen umfassenden Katalog an Maßnahmen und Gefährdungen, welche durch die beschriebene Methode einfach identifiziert und auf die unternehmenseigene Architektur angewendet werden können. Risiken lassen sich auf diese Weise strukturiert identifizieren und Maßnahmen zu deren Mitigation werden direkt ersichtlich. Die identifizierten Risiken werden auf Basis einer Likelihood-Impact-Analyse bewertet. Dabei orientiert sich der Konzeptualisierungsansatz an die Paper „Agile modeling method engineering“ (Karagiannis) und „Metamodelling Platforms“ (Karagiannis, Kühn). Auf Basis dieses Konzeptes wird die Methode mithilfe der Metamodellierungsplattform ADOxx implementiert. Final stellt diese Arbeit eine Case Study vor, die zur Evaluierung des umgesetzten Sicherheitskonzepts dient.

Abstract (English) In a time of ever-increasing digitalization and increasingly complex IT environments more and more companies are using enterprise architecture (EA). Despite the numerous overlaps of EA and Security Management, the two management domains are often organized separately from one another, so that the resulting potentials cannot be identified from a holistic point of view. Comprehensive frameworks, such as TOGAF (The Open Group Architecture Frameworks), point to the importance of secure architectures but remain superficial and refer to specialized frameworks such as SABSA. This work covers the area of basic protection and describes the implementation of a security framework using the modelling language ArchiMate (The source code is provided on CD). Basic protection is based on the valuation of company data and enables the valuation of the company's main assets. The IT-Grundschutz Catalogues of the BSI are used to implement adequate IT protection. This provides a comprehensive catalog of controls and threats, which can be easily identified by the described method and applied to the company's architecture. Risks can thus be identified in a structured manner and measures for their mitigation are immediately apparent. The identified risks are assessed on the basis of a likelihood impact analysis. The conceptualisation approach is based on the paper „Agile modeling method engineering“ (Karagiannis) and „Metamodelling Platforms“ (Karagiannis, Kühn). Based on this concept, the method is implemented using the ADOxx Metamodelling Platform. Finally, this thesis presents a case study to evaluate the implemented security concept.

Inhaltsverzeichnis

1 Motivation und Problemstellung

Die Bedeutung von Sicherheits- und Risikomanagement wird mit der zunehmenden Digitalisierung immer größer und wichtiger für Unternehmen. Größere Unternehmen bedienen sich dabei Standards und Frameworks, um das Sicherheitsmanagement erfolgreich zu etablieren. Diese Frameworks empfehlen in der Regel die integrierte Umsetzung von IT-Sicherheitsmanagement — d.h. Sicherheitsmanagement wird nicht als isolierter Management Ansatz betrachtet, sondern integrativ mit etablierten Managementpraktiken, wie ITIL und EAM, betrieben. EAM ermöglicht eine ganzheitliche Sicht auf das Unternehmen und bietet daher bereits in der Design-Phase ideale Andockpunkte für Sicherheitsmanagement, bevor Veränderungsprojekte überhaupt gestartet werden. Für die Implementierung eines Risikokonzepts stellen Frameworks wie TOGAF, SABSA, ITIL und der ISO-27000-Standard eine Empfehlung zur Verfügung. Ein nicht unbeachtliches Problem hierbei ist die Umsetzungskomplexität dieser Frameworks. Sie erfordern oftmals Ressourcen, die in kleineren und mittleren Unternehmen nicht zur Verfügung stehen. Aus dieser Problemstellung ergibt sich die Motivation in der vorliegenden Arbeit. Der Fokus liegt auf kleineren und mittleren Unternehmen, denen ein Werkzeug zur Verfügung stehen soll, um Risiko- und Sicherheitsmanagement erfolgreich aufzubauen. Das vorliegende Konzept stellt mit ArchiMate eine anerkannte Modellierungssprache zur Abbildung der wesentlichen Gestaltungselemente eines Unternehmens zur Verfügung. Die nahtlose Integration der zahlreichen Empfehlungen des Grundschutzkataloges soll es KMU's ermöglichen, wertvolle Ressourcen bei der Implementierung und beim späteren Betrieb des Sicherheitsmanagements zu sparen. Der Ansatz zielt somit vor allem auf die Etablierung der Mindestanforderungen in Hinblick auf den Grundschutz eines Unternehmens ab. Der Schutzbedarf wird durch die Identifikation und Bewertung unternehmenskritischer Daten ermittelt. Davon ausgehend werden alle unternehmenskritischen Assets und IT-Services ermittelt. Insbesondere die IT-Services werden den im Grundschutzkatalog empfohlenen Maßnahmen gegenübergestellt. Maßnahmen welche relevant erscheinen, jedoch nicht umgesetzt sind, werden unmittelbar ersichtlich. Der negative Einfluss nicht umgesetzter Maßnahmen auf die Risikosituation wird durch einen speziell für diesen Zweck konzipierten Bewertungsalgorithmus ermittelt. Sicherheitslücken werden direkt in den Modellen, welche zur Veranschaulichung der Architektur dienen, visualisiert und dadurch einfach kommunizierbar. Der Bewertungsalgorithmus kann darüber hinaus auch für What-If-Analysen verwendet werden. Dadurch wird ersichtlich, wie sich umgesetzte Maßnahmen auf die Risikobewertung auswirken, sodass die richtigen Stellhebel für eine sichere Unternehmensarchitektur identifiziert werden können. Damit können Investments in der Sicherheitsarchitektur zielgerichtet getätigt werden. Zur Bewertung des Schutzbedarfes werden die Sicherheitsattribute Vertraulichkeit, Integrität und Verfügbarkeit herangezogen. Der Grundschutz in diesem Framework verwendet den Grundschutzkatalogs des BSI als Basis. Dabei werden die Maßnahmen aus dem Katalog verwendet, um modellierte Architekturelemente zu bewerten. Durch diese beiden Best-Practice-Konzepte kann sichergestellt werden, dass die Risikobewertung effizient

abläuft. Zusätzlich wird die Bewertung ressourcenschonend (Zeit und Personal) vorgenommen. Zur Auswertung der vorgenommenen Bewertung dient eine vordefinierte Analyse, die einerseits den Impact, basierend auf den Schutzbedarf, und andererseits den Abdeckungsgrad der durchgeführten Grundschutzkatalog-Maßnahmen ausgibt. Sämtliche Aufgaben, die unter diese Risikobewertung fallen, können innerhalb des Systems (ADOxx) verteilt werden. So können z.B. auch Unternehmen, die keine Stelle „Security Architect“ definiert haben, eine Risiko- und Sicherheitsanalyse vornehmen.

2 State of the Art

2.1 Literature Review Methode und Literatursuche

Für die Literaturrecherche wurde nach folgenden Schlagwörtern gesucht:

- Enterprise Architecture Management + Security
- EAM Frameworks + Security
- EAM + Security Framework
- EAM Framework + Security Integration

Die Suchergebnisse lieferten jedoch keine konkreten Anhaltspunkte für eine werkzeuggestützte IT-Sicherheitsmethode, welche speziell auf die Bedürfnisse von KMU's ausgerichtet ist. Anhaltspunkte konkreter Methoden, welche die nahtlose Integration des Grundschutzhandbuches mit Architekturstandards, wie TOGAF und ArchiMate oder vergleichbarer Methoden, bieten, wurden nicht gefunden. Somit stützt sich die Arbeit vor allem auf weit verbreitete Standards und Frameworks aus den genannten Bereichen. In der Folge werden die wichtigsten dieser Ansätze kurz beschrieben und kritisch in Hinblick auf das Vorhaben der vorliegenden Arbeit bewertet.

2.2 TOGAF

2.2.1 Grundlagen The Open Group Architecture Framework (TOGAF) ist ein Enterprise Architecture Framework (EAF), welches Methoden und Tools für die Etablierung und den Betrieb von Unternehmensarchitekturmanagement beschreibt. TOGAF definiert den Begriff Architektur folgendermaßen [25]:

1. A formal description of a system, or a detailed plan of the system at component level to guide its implementation.
2. The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time.

TOGAF unterteilt Unternehmen in 4 Architekturdomänen [25] [19]:

- Die **Business Architecture** dient der Definition der Geschäftsstrategie, Governance, Organisation und Geschäftsprozesse. Sie stellt die Basis für die anderen Domänen dar. Der Output dieser Domäne dient dem Input der Daten- und Applikationsarchitektur.

– Die **Data Architecture** beschreibt die Struktur und Interaktion von logischen und physischen Daten. Diese können elektronisch, gedruckt, oder in anderen Formen vorliegen. Sie werden in IT-Systemen durch Hard- und Software verwendet.
– Die **Application Architecture** fokussiert sich auf die Architektur der Anwendungslandschaft des Unternehmens. Die Anwendungsarchitektur beschreibt die Applikationen und IT-Systeme, die für die Ausführung der Geschäftsprozesse erforderlich sind.
– Die **Technology Architecture** beschreibt die Struktur und Interaktion von logischen und physischen Technologie/-Infrastrukturelementen, welche eine unterstützende Funktion für die Applikations- und Datenebene bieten.

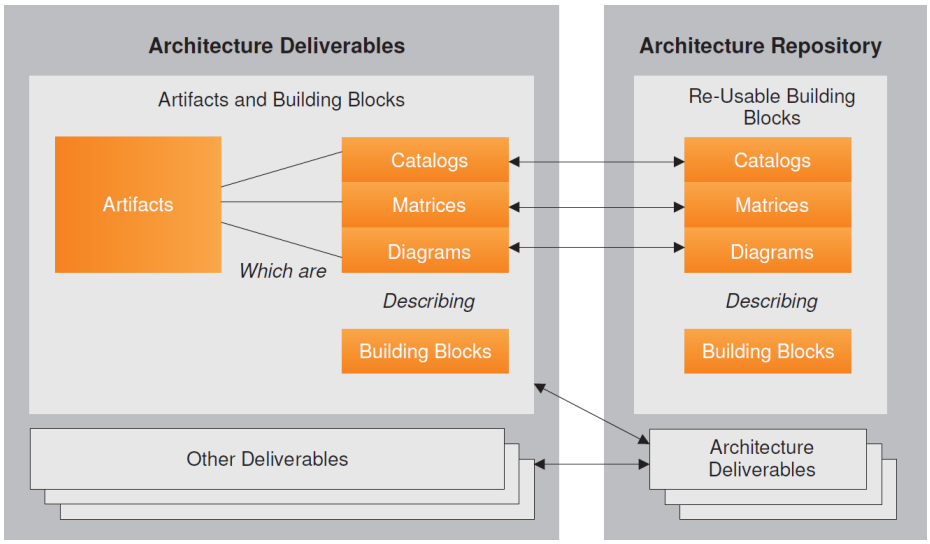

Abb. 1. Beziehungen zwischen Deliverables, Artifacts und Building Blocks [25]

Ein zentraler Bestandteil von TOGAF ist das TOGAF Content Metamodell. Es dient der standardisierten Beschreibung der Unternehmensarchitektur. Ergebnisse lassen sich wie folgt gliedern und beschreiben [25]:

– **Deliverables** werden vertraglich spezifiziert und stellen den Output von Projekten dar.
– **Artifacts** werden in Kataloge, Matrizen und Diagramme gegliedert. Sie dienen zur Beschreibung, Visualisierung und Kommunikation von Ausschnitten der Unternehmensarchitektur.
– **Building Blocks** können unterschiedliche Detaillierungsgrade haben und repräsentieren Komponenten aus der IT- bzw. Geschäftsdomäne. Sie sind

die Gestaltungsobjekte des Unternehmens. Architecture Building Blocks beschreiben die Gestaltungselemente auf einer abstrakten Ebene. Sie definieren die Anforderungen an die Architektur, ohne bereits konkrete Lösungen vorwegzunehmen. Beispiele für Building Blocks sind Geschäftsprozesse, Anwendungen, Datenelemente, und Organisationseinheiten. In späteren Phasen des Architekturdesigns werden die ABBs durch sogenannte Solution Building Blocks ausgestaltet. Wie der Name sagt, beschreiben Solution Building Blocks konkrete Lösungen. Beispiel: Als ABB wird ein CRM-System (Information System Layer) beschrieben. Die wesentlichen Funktionen und deren Nutzung im Kontext von Geschäftsprozessen (Business Layer) werden spezifiziert und in Form von grafischen Modellen (Artifacts) dokumentiert.
Auf Ebene der SBBs werden in nachgelagerten Phasen konkrete Lösungsbausteine erarbeitet. Z.B. werden die Geschäftsprozesse in Hinblick auf das neu einzuführende System (z.B. Salesforce) detailliert definiert.

2.2.2 Architecture Development Method Die Architecture Development Method (ADM) ist der Schlüsselbereich des TOGAF-Frameworks. ADM stellt einen Managementkreislauf, vergleichbar dem PDCA (Plan Do Check Act Cycle) [6], dar. Die ADM besteht aus zehn Phasen die Unternehmensarchitekten iterativ dabei unterstützen die Unternehmensarchitektur zu entwickeln. Jede Iteration steht für ein oder mehrere architekturrelevante Vorhaben. Insbesondere in den Phasen B-D entstehen Architektur Deliverables in Form von Architekturmodellen, welche im Idealfall in einem Architektur-Repository verwaltet werden. Die ADM stellt einen ganzheitlichen Ansatz zur Verfügung. Von der Architekturvision (dem initialen Vorhaben) bishin zur Umsetzung und Evaluierung der Umsetzung werden alle wesentlichen Schritte beschrieben. Ein Durchlauf durch den Kreislauf beschreibt somit die Transformation von Teilen des Unternehmens (Teilarchitektur). [25]

2.2.2.1 Preliminary Phase Initial werden Vorbereitungsarbeiten und Richtlinien für die Unternehmensarchitektur und das EAM festgelegt. Das Architektur-Framework wird auf die Bedürfnisse des Unternehmens angepasst. Die erforderlichen Architektur-Fähigkeiten werden identifiziert und in der Organisation etabliert. Dazu müssen folgende Schritte durchgeführt werden [25]:

- Festlegen des Scopes für die Durchführung der Unternehmensarchitekturarbeiten
- Identifikation der erforderlichen Fähigkeiten, um Architekturmanagement zu etablieren
- Identifikation der im Unternehmen etablierten Managementansätze, sodass EAM optimal integriert werden kann
- Definition des Organisationsmodells für das Betreiben von EAM
- Definition der detaillierten Prozesse für die Governance
- Auswahl/Implementierung von Tools
- Definition der Architekturprinzipien, welche später als Leitschiene für Architekturentscheidungen genutzt werden

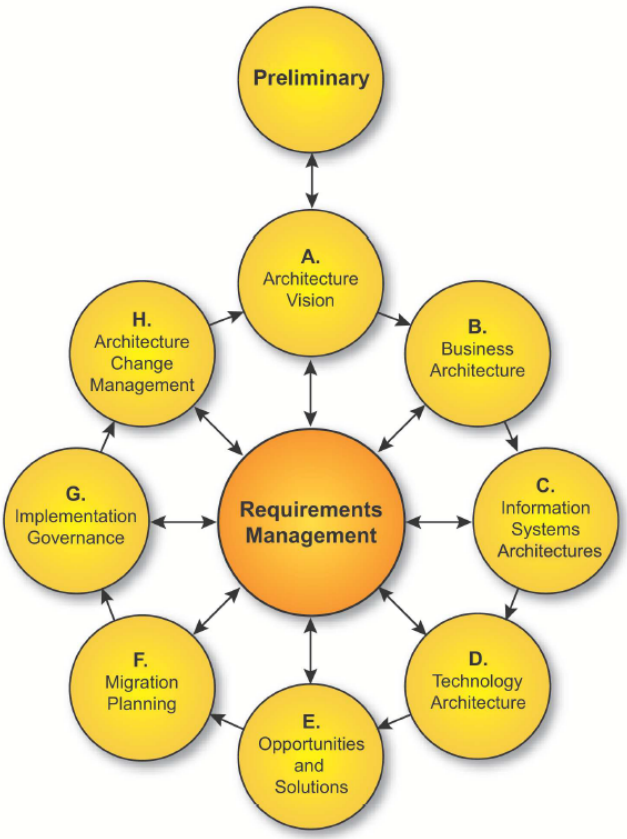

Abb. 2. Architecture Development Cycle [25]

2.2.2.2 Architecture Vision In dieser Phase wird der Scope des Architekturvorhabens festgelegt. Die relevanten Stakeholder werden identifiziert und deren Erwartungen abgeholt. Auf dieser Basis wird die Architekturvision — das Zielbild für die zukünftige Architektur — erstellt. [25]

2.2.2.3 Business Architecture In dieser Phase des Lifecycles wird die Geschäftsarchitektur beschrieben.
Durch die Gegenüberstellung von IST- und SOLL-Architektur werden die wesentlichen Unterschiede (sogenannte Gaps) ermittelt, die es in den weiteren Phasen und in den Umsetzungsprojekten zu schließen gilt. [25]

2.2.2.4 Information Systems Architectures Genauso wie in der Geschäftsarchitektur werden in dieser Phase sowohl IST- als auch SOLL-Architektur definiert und die sogenannten Architektur-Gaps ermittelt. Bei der Gestaltung der Architektur wird insbesondere auf jene Teile der Anwendungslandschaft fokussiert, welche die in der Geschäftsarchitektur identifizierten Geschäftsprozesse unterstützen. Das Gleiche gilt für die Datenarchitektur. Es werden jene Geschäftsobjekte ermittelt und ausgestaltet, die zur erfolgreichen Umsetzung der Architekturvision beitragen. [25]

2.2.2.5 Technology Architecture Ziel dieser Phase ist Technologiearchitektur zu entwickeln, die logische und physische Applikationen und Daten unterstützt. Auch in dieser Phase wird zwischen IST- und SOLL-Architektur unterschieden. [25]

2.2.2.6 Opportunities and Solutions Es werden die erforderlichen Projekte identifiziert, welche die Transformation der IST- in die SOLL-Architektur ermöglichen. Das zentrale Ergebnis dieser Phase ist eine erste Version des Projektportfolios. Die Projekte werden aneinander ausgerichtet. Sogenannte Transitionsarchitekturen (transition architectures) beschreiben grobe Meilensteine, die zeitlich geplant werden. Diese Planung erfolgt auf Basis der konkreten Lösungsarchitektur, welche ebenfalls in dieser Phase erarbeitet wird. [25]

2.2.2.7 Migration Planning In dieser Phase des Lifecycles wird ein Plan erstellt, in dem detailliert beschrieben wird, wie von der Ist-Architektur zur Soll-Architektur migriert werden soll. Das Ziel ist den Architektur-Projektplan fertigzustellen sowie sicherzustellen, dass der Implementations- und Migrationsplan korrekt ist und die Projekte in das Gesamtprojektportfolio des Unternehmens integriert sind. [25]

2.2.2.8 Implementation Governance Diese Phase ist für die Governance bzw. Überwachung der Implementierung zuständig. Das Ziel besteht darin, sicherzustellen, dass die Architekturvorgaben und das vereinbarte Architekturdesign in den Projekten berücksichtigt und umgesetzt werden. [25]

2.2.2.9 Architecture Change Management In dieser Phase werden die durchgeführten Änderungen im Unternehmen etabliert. Neue Anforderungen werden identifiziert und im Requirements Management verwaltet. Bei Bedarf wird eine neuerliche Iteration des ADM angestoßen. [25]

2.2.2.10 Requirements Management Im Zentrum des ADM steht das Anforderungsmanagement. Dieses Kernstück ist für die Einhaltung der Anforderungen an die einzelnen Phasen zuständig. In jeder Phase des ADM werden Anforderungen verwaltet und priorisiert, die beim Durchlaufen des ADMs eingemeldet werden. Anforderungen können in jeder Phase des ADM entstehen und eingereicht werden.
Das ADM verwaltet dabei nicht nur die Anforderungen, die sich beim Durchlauf eines ADM ergeben. Vielmehr kann der Kreislauf zu einem Zeitpunkt mehrfach für unterschiedlichste Architekturvorhaben im Unternehmen durchlaufen werden. Das Anforderungsmanagement prüft auf Konsistenz und Abhängigkeiten der Anforderungen innerhalb eines Kreislaufs und gleichzeitig über alle Instanzen an ADM-Kreisläufen hinweg. [25]

2.2.3 TOGAF-Security-Architecture Die Security Architecture beschreibt die konzeptuellen, logischen und physischen Komponenten, die miteinander interagieren, um Risiken effizient mitigieren zu können [29]. Security-Architecture-Elemente haben eine Beziehung zu allen Gestaltungsobjekten auf allen Architekturebenen. Für eine korrekte Security-Integration sollte ein System-Engineering-Ansatz gewählt werden. Gemäß TOGAF müssen Security-Aspekte in jeder Phase des ADM berücksichtigt werden [29]. TOGAF bietet in seiner Standardausführung ein Vorgehensmodell zur Etablierung von Security-Konzepten in die Architektur an. Als orthogonaler Layer, informiert die Security

Abb. 3. Security-Layer als orthogonaler Ansatz [29]

Architecture die Geschäfts-, Daten-, Applikations- und Technologiearchitektur [29].

Grundsätzlich hat die Security Architecture folgende Charakteristiken [25]:

- Eine Vorgehensweise mit konkreten Schritten,
- Eigene Views und Viewpoints auf die Architektur aus einem Security-Blickwinkel, welche ebenfalls in Form von Artifacts (Modellen) beschrieben werden, soweit diese nicht in die bestehenden Artefakte bereits integriert sind.

Die Security-Aktivitäten innerhalb der Phasen reichen dabei von einer High-Level-Governance bis hin zu detaillierten Security Checks. Da sämtliche Stakeholder eines Unternehmens individuelle Anforderungen an die Sicherheit stellen, empfiehlt der TOGAF-Standard die Zuhilfenahme eines Sicherheitsarchitekten. [25] Die Aufgaben des Sicherheitsarchitekten sind u.a. folgende [25]:

- Etablierung von Architekturlösungen für die Authentifizierung von Personen, die in irgendeiner Beziehung zum Unternehmen stehen.
- Sicherstellung der geregelten Zuweisung von Rechten an bereits autorisierten Personen.
- Audit-Management über die Systemnutzung.
- Audits über die Einhaltung der Security-Richtlinien im Zusammenhang mit der Unternehmensarchitektur.
- Die Wahrung der Serviceverfügbarkeit in der Organisation.
- Die Wahrung von Informationsressourcen.
- Die Weiterentwicklung der Security-Richtlinie und die Sicherstellung derer Einhaltung.
- Die Überwachung der Unternehmensrisiken.

Zudem ist die Identifizierung der Risiken und ihre Eintrittswahrscheinlichkeit sowie die Auswirkungen vom Sicherheitsarchitekten sicherzustellen [29]. Die Security Architecture ist in TOGAF jedoch nur sehr vage beschrieben. Neben der Security Architecture bietet TOGAF Verfahrensanweisungen für Risiko-Management an. Risiko wird in der ISO31000:2009 als 'effect of uncertainty on objectives' definiert [11]. Risiko-Management wird als „striking a balance between positive and negative outcomes resulting from the realization of either opportunities or threats“ beschrieben [29]. Die Risikomanagementprozesse in TOGAF bestehen aus einer Risikoklassifizierung, Risikoidentifikation, Risikobewertung, Minderung der Risiken, Restrisikobewertung und einem Risikomonitoring. TOGAF bietet ein Schema für die Durchführung dieser einzelnen Prozesse an. Jedoch fokussiert sich der Standard primär auf Architektur-Projektrisiken. Neben diesem einen Typ von Risiko sind noch Bereiche wie Business, Informationssysteme, Compliance, Datenschutz, Organisation und weitere von großer Bedeutung [29]. Da es sich bei TOGAF um ein generisches Framework mit einem flexiblen und erweiterbaren Content Framework handelt, bietet es sich an den Standard mit anderen Frameworks, wie ITIL, COBIT oder SABSA zu verwenden, die einen größeren Fokus auf Security und Risikomanagement legen.

[25]
Fazit: Für die vorliegende Arbeit wurde die AD-Methode als Grundgerüst für die Umsetzung des Security-Layers verwendet. Die Arbeit fokussiert sich auf die Phasen B (Geschäftsarchitektur), C (Informationssystemarchitektur) und D (Technologiearchitektur). Zudem werden diese Phasen, wie von TOGAF empfohlen, um Security-Aspekte angereichert. Jedoch wird nicht das TOGAF content metamodel verwendet, da die Open Group mit ArchiMate eine vollständige Modellierungssprache bietet (siehe Abschnitt 2.7). Das TOGAF content framework bietet ähnliche Konzepte. Jedoch bietet ArchiMate eine vollständige Modellierungssprache inklusive Notation der Konzepte und zahlreiche Sichten (Views) und Viewpoints inklusive Empfehlungen zu deren Einsatz an.

2.3 Sherwood Applied Business Security Architecture

2.3.1 SABSA-Modell SABSA ist ein Security Architecture Framework, bestehend aus einem sechsschichtigen Vorgehensmodell. Die horizontalen Layer in SABSA bilden kontextuelle, konzeptuelle, logische und physische Komponenten [19]. Der vertikale Layer beschreibt Verfahren zum Security Service Management. Jeder Layer im SABSA-Modell entspricht dabei einer View eines Stakeholders [23]. SABSA orientiert sich stark an dem Zachman Framework für Unternehmensarchitekturen, kann aber genauso im Zusammenhang mit TOGAF eingesetzt werden [22]. Daneben bietet SABSA Best-Practice-Modelle, -Methoden und -Prozesse, die risikofokussiert sind und die Identifikation und Entschärfung von Bedrohungen ermöglichen [4]. Um das SABSA-Modell anschaulicher zu gestalten, wird als nachfolgendes Beispiel das Thema Zugangskontrolle in Unternehmen herangezogen.

2.3.1.1 Contextual Security Architecture „Perspektive des Fachbereichs“: Bei der Contextual Security Architecture handelt es sich um die oberste Schicht im SABSA-Modell. Es wird der geschäftliche Kontext beschrieben, in welchem die Sicherheitssysteme entworfen und in Produktion gebracht werden. Die SABSA-Rolle, die in dieser Ebene operiert, ist der Geschäftsverantwortliche. Bezogen auf das Beispiel der Zugangskontrolle werden unter anderem Fragen über die Zugangskontrolle und Berechtigungen im Zusammenhang mit Geschäftsrisiken abgehandelt. [5][23]

2.3.1.2 Conceptual Security Architecture „Perspektive des Architekten“: Auf dieser Ebene identifiziert der Security Architect kritische Vermögenswerte. Bezogen auf das Beispiel des Zugangskontrollsystems sind typische Fragestellungen [5]:

- Woraus muss das Zugangskontrollsystem bestehen?
- Auf welchen Architektur-Layern wird das System betrieben?
- Wie werden User-Rollen zugewiesen?
- Wie wird es in den Achitekturdomänen integriert?

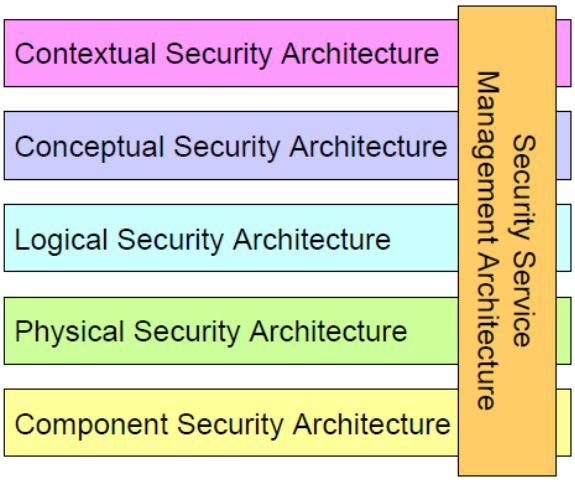

Abb. 4. Das SABSA-Modell für Security Architecture [23]

2.3.1.3 Logical Security Architecture „Perspektive des Designers“: Das erarbeitete Fachkonzept wird vom Designer entgegengenommen und verfeinert, sodass dieses eine ausreichende Grundlage für die Umsetzung bildet [23].

Bezogen auf das Beispiel der Zugangskontrolle spezifiziert der Designer detailliertere Eigenschaften des Zugangskontrollsystems, wie zum Beispiel Passwortmanagement, User-Registrierung, Rollenzuweisung, Überwachung und die Pflichtenaufteilung [5].

2.3.1.4 Physical Security Architecture „Perspektive des Umsetzungsverantwortlichen“: In dieser Ebene wird dem Konstrukteur die Vorarbeit des Designers übergeben. Es werden die erforderlichen sicherheitsrelevanten Datenstrukturen und Konfigurationen erarbeitet. [23]

In Bezug auf das Zugangskontrollsystem werden die erforderlichen Rollen, Berechtigungen und Regeln für den Zutritt spezifiziert [5].

2.3.1.5 Component Security Architecture „Perspektive des Facharbeiters“: In dieser Phase wird die Sicherheitslösung gemäß den Vorgaben implementiert. Das Umsetzungsteam wird zusammengestellt, um die ICT-Komponenten zu implementieren und in die Gesamtarchitektur zu integrieren. [23]

Bezogen auf das Zugangskontrollsystem wird die Lösung durch das zuständige Implementierungsteam umgesetzt. Dies bezieht sich sowohl auf bauliche Maßnahmen (z.B. Ausbringung der Kartenleser oder Integration in das physische

Netzwerk) als auch auf softwaretechnische Bereiche wie die Installation und Konfiguration des Serversystems. [5]

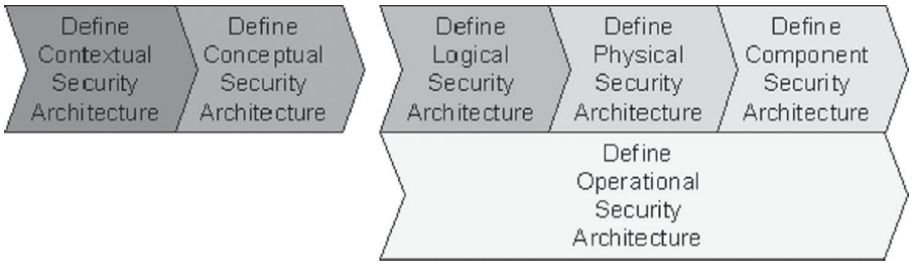

Abb. 5. Der SABSA-Prozess [4]

2.3.1.6 Operational Security Architecture „Perspektive des Betreibers“: Diese Phase fokussiert sich auf den laufenden Betrieb der Sicherheitslösung. Ein zuständiger Service Owner wird ernannt, welcher sich für das Service-Management der Lösung verantwortlich zeigt. Im Falle des Zutrittskontrollsystems kümmert sich der Serviceverantwortliche um die Einhaltung der vereinbarten Service-Levels und um die Weiterentwicklung des Systems. Er erstellt Service Level Reports zum Zutrittskontrollsystem, etc. [5][23]

2.3.2 SABSA Matrix Das zuvor beschriebene SABSA-Modell stellt die Basis für die SABSA-Matrix dar. Die sechs vertikalen Architekturelemente werden horizontal in eine Matrix eingebettet. SABSA orientiert sich stark am Zachman Framework [31]. Die oben beschriebenen Architektur-Layer werden horizontal nach folgenden Fragestellungen strukturiert [23]:

- Was wird in diesem Layer gemacht? — Das Vermögen, das geschützt werden soll, wird identifiziert.
- Wieso wird das gemacht? — Es wird die Motivation definiert, warum Sicherheit benötigt wird.
- Wie wird es umgesetzt? — Dies betrifft Prozesse und Funktionen, die benötigt werden, um die Sicherheitsziele zu erreichen.
- Wer ist involviert? — Dies betrifft die organisatorischen Aspekte von Sicherheit.
- Wo wird es gemacht? — Orte an denen Sicherheit angewendet wird.
- Wann wird es gemacht? — Die Definition von zeitspezifischen Angaben.

Das ergibt eine 6x6-Matrix, welche das gesamte Modell der Enterprise Security Architecture beinhaltet.

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Abb. 6. Die SABSA-Matrix [23]

2.3.3 SABSA Lifecycle Der SABSA-Prozess kann in einem Lifecycle zusammengefasst werden. Dabei sind die ersten beiden Prozesse (Definition einer kontextuellen bzw. konzeptuellen Security-Architektur) der Aktivität „Strategie und Planung“ zuzuordnen. Danach folgt die Aktivität „Design“, welche das Design für die logische und physische Architektur sowie die Komponentenarchitektur vorsieht. In der Aktivität „Implementierung“ wird auf die Implementierung der Security Achitecture Bezug genommen und abschließend werden während „Manage and Measure“ aktuelle Performances gegen Ziel-Performances gemessen und bewertet. Werden Ziele nicht erreicht, führt das zu Risiko-Events. [23]

2.3.4 SABSA Business Attributes Profile Das Business Attribute Profile stellt ein wichtiges Werkzeug für die Identifikation und Bewertung von Geschäftsanforderungen im Kontext von Sicherheitsmaßnahmen dar. Sie baut die Verbindung zwischen Geschäftsanforderungen und Technologie- und Prozessdesign auf. Das Business Attribute Profile ermöglicht es eine Menge an Geschäftsanforderungen in ein standardisiertes SABSA-Format zu transformieren. Die Liste besteht aus 85 Attributen, die sich aus der praktischen Erfahrung mit zahlreichen Unternehmen aus den unterschiedlichsten Industriesektoren entwickelt hat. [15][23]

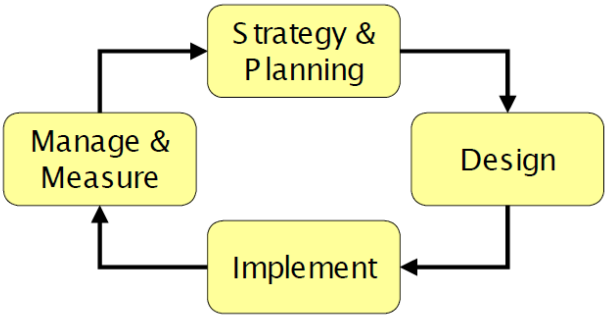

Abb. 7. Der SABSA-Lifecycle [23]

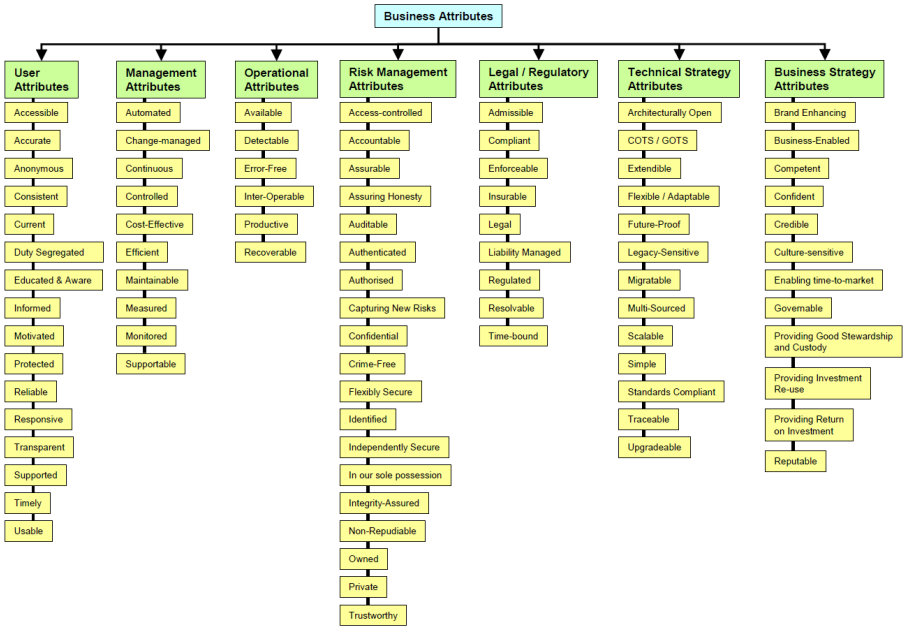

Abb. 8. SABSA Business Attributes [23]

2.3.5 SABSA Risikomanagement SABSA definiert operationales Risiko folgendermaßen:

> „Operational risk is the set of risks that includes the opportunities to attain business benefits through operational excellence in processes, people, and technology, and the threats of loss originating from inadequate or failed internal processes, people, and technology or from external events, or systemic failures. In all cases, although the threats are restricted to the operational domain, negative impacts may include both strategic failure and reputation damage“ [26].

2.4 SABSA-Integration

Um das SABSA-Framework in TOGAF zu integrieren, müssen drei Voraussetzungen beachtet werden [26]:

1. Risiken sollen minimiert werden.
2. Das Business Attribute Profile soll während der Requirements-Phase im TOGAF-Framework dabei unterstützen die „Architectural Requirements“ zu erfassen.
3. Ziel der Integration ist die Security-Architekturartefakte den richtigen Phasen in der ADM zuzuweisen, sodass die Security-Architektur ein fester Bestandteil des TOGAF-Vorgehensmodells wird.

Das Kernstück von TOGAF ist die ADM. Daher ist dies der optimale Ansatzpunkt, um Security-Architektur zu integrieren. Da die Vorgehensmodelle von TOGAF und SABSA beide geschäftsgesteuert sind, ist es sinnvoll diesen Aspekt als Integrationsschnittstelle zu verwenden. Das Pendant zur TOGAF-ADM ist der SABSA-Lifecycle. Diese beiden Kernstücke haben sowohl überlappende als auch unterschiedliche Elemente. Ein möglicher Ansatz zur Integration ist in Abb. 9 zu sehen.

Fazit: Durch die Ausrichtung am Architekturmanagement-Framework Zachman ist SABSA derart konzipiert, dass es Architekturmanagement-Frameworks wie TOGAF ideal ergänzt. Für die vorliegende Arbeit erscheint insbesondere das SABSA Business Attributes Profile und das SABSA-Vorgehensmodell von Bedeutung.
Im Zuge des Designs neuer Architekturen kann das Business Attributes Profile verwendet werden, um Sicherheitsanforderungen zu spezifizieren. Die erarbeitete Methode erlaubt es Security-Anforderungen direkt zu erfassen. ArchiMate bietet hierfür das Modellierungskonzept „Requirement“ (Anforderung). Aus dem Business Attributes Profile abgeleitete Anforderungen werden im Zuge der Design-Phasen direkt mit den betroffenen Architekturelementen (z.B. Geschäftsprozess, Anwendung etc.) verlinkt. Somit ermöglicht die vorliegende Implementierung eine integrierte Sicht auf Sicherheitsanforderungen auf allen Architekturebenen.

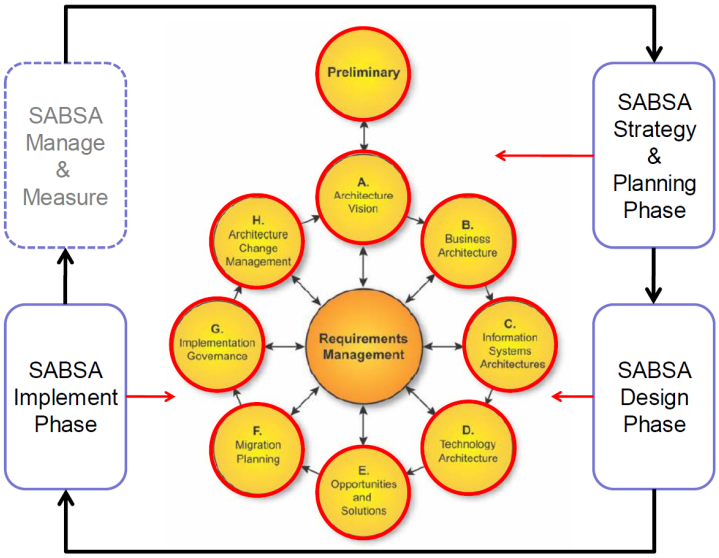

Abb. 9. Mapping der TOGAF-ADM und des SABSA-Lifecycles [26]

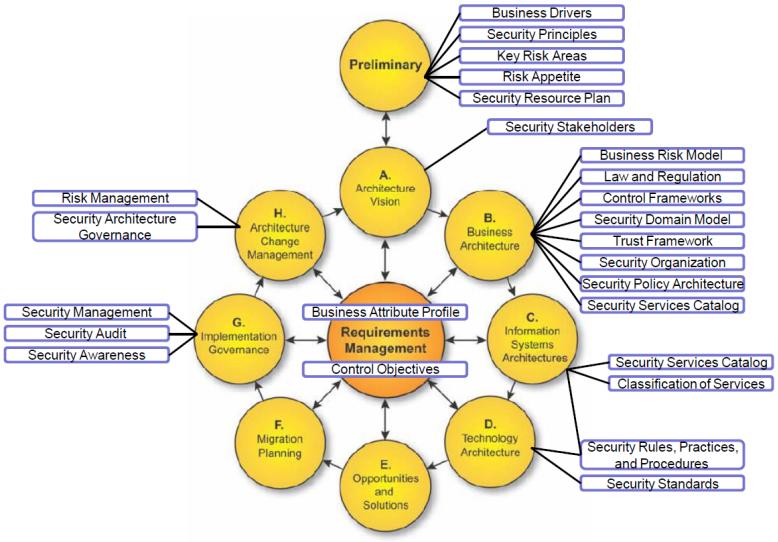

Abb. 10. SABSA Artifacts Mapping auf die ADM [26]

2.5 ITIL

2.5.1 Grundlagen Die IT Infrastructure Library (ITIL) ist eine Menge von Best Practices zur Umsetzung eines IT-Service-Managements (ITSM). Das Framework bietet eine einheitliche Sprache zur Umsetzung und Verwaltung von IT-Services, die Werte für das Business generieren und den Ansprüchen der Kunden genügen sollen. Services werden nach dem ITIL-Standard folgendermaßen definiert [21]:

> 'A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.' [21]

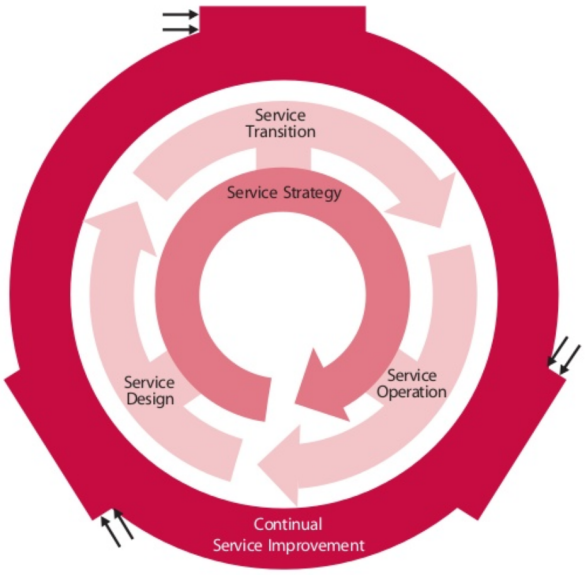

Abb. 11. ITIL-Lebenszyklus [21]

Der Kern von ITIL besteht aus fünf Hauptphasen, die gemeinsam den ITIL-Lebenszyklus bilden [21]:

- In dieser Phase gilt es die Strategie für die Bereitstellung von IT-Services zu erarbeiten. Auf Basis von Kundenbedürfnissen und Marktanforderungen wird festgelegt, welche Services die IT-Organisation anbietet. Die IT-Organisation richtet sich dabei konsequent an der Unternehmensstrategie aus.
- In dieser Phase werden neue Services entwickelt und bestehende Services optimiert. U.a. finden sich in dieser Phase auch die Prozesse „Risikomana-

gement“, „IT-Service Continuity Management“ und „Information Security Management.“
- Die Service-Transation-Phase stellt das Bindeglied zwischen der Design- und Operations-Phase dar. In dieser Phase geht es um die Produktivsetzung neuer Services bzw. um die Anpassung bestehender Services. Die Prozesse Change Management und Release Management spielen dabei eine zentrale Rolle.
- Die Service-Operation-Phase ist für das Management des täglichen Servicebetriebs zuständig. Es soll darüber hinaus die Lieferung von Services effizienter gestalten, um den Nutzenbeitrag für die Kunden zu verbessern.
- Das Continual Service Improvement ist ein kontinuierlicher Verbesserungsprozess, um die Design-, Transition- und Operations-Phase effektiver zu gestalten.

2.5.2 Information Security Management In der Service-Design-Phase wird die Erstellung von Security-Anforderungen berücksichtigt.

> 'The goal of the ISM process is to align IT security with business security and ensure that information security is effectively managed in all service and Service Management activities.' [20]

Information Security ist ein Prozessschritt innerhalb des Corporate Governance, welches die strategische Richtung für Security-Aktivitäten vorgibt. Weiters sorgt sie für das Management von Risiken und die korrekte Verwendung von Ressourcen. Mittels Information Security Management (ISM) soll dafür gesorgt werden, dass Informationen und Informationssysteme vor Schäden, resultierend aus Problemen in der Verfügbarkeit, Vertraulichkeit und Integrität, geschützt werden [20]. In den meisten Unternehmen ist das Sicherheitsziel erreicht sobald [20]:

- Informationen, sobald erforderlich, verfügbar sind und das betreffende System vor Angriffen geschützt ist bzw. vor möglichen Fehlern präventiv schützen kann (Verfügbarkeit),
- Informationen in geschlossenem Zustand nur für autorisierte Personen zugänglich sind (Vertraulichkeit),
- Informationen vollständig, exakt und geschützt sind vor unautorisierter Modifizierung (Integrität),
- Transaktionen jeglicher Art zwischen Unternehmen vertrauensvoll sind (Authentizität).

Die genauen Richtlinien, was in welchem Ausmaß geschützt werden soll, müssen geschäftsseitig vorgegeben werden. Zudem muss die Security alle Geschäftsprozesse abdecken. Alle Information-Security-Management-Aktivitäten müssen einer Information-Security-Richtlinie folgen. Diese Richtlinie sollte alle Sicherheitsbereiche einer Organisation abdecken und den Geschäftsanforderungen nachkommen. [20]
Das Information Security Management System (ISMS) bietet die Möglichkeit ein kosteneffektives Information-Security-Programm zu entwickeln. ISMS folgt

einem Framework, das auf dem ISO-27001-Standard aufbaut. Die fünf Elemente des Frameworks sind [20]:

- **Control:** Es soll ein Management-Framework geschaffen werden, das Information-Security innerhalb der Organisation verwaltet, Verantwortlichkeiten zuteilt, Security-Dokumentation pflegt und die Information-Security-Richtlinie implementiert.
- **Plan:** Das Ziel dieser Phase ist die Entwicklung von Sicherheitsmaßnahmen, basierend auf den Anforderungen der Organisation. Diese Anforderungen stammen von Quellen wie Geschäfts- und Service-Risiken, Plänen, Strategien sowie SLA's und OLA's.
- **Implement:** Hier sollen Prozeduren, Tools und Kontrollen die Information-Security-Richtlinie unterstützen. Es werden zudem die Verantwortlichkeit von Vermögen zugeteilt und Informationen klassifiziert.
- **Evaluation:** Die Ziele sind die Überwachung und Einhaltung der Security-Richtlinie und Security-Anforderungen in SLA's und OLA's, die Durchführung von Audits im technischen Security-Bereich und Informationsbereitstellung an externe Revisoren.
- **Maintain:** Ziele sind die Verbesserung von Security-Vereinbarungen und die Verbesserung der Implementierung von Sicherheitsmaßnahmen und Sicherheitskontrollen.

Zusätzlich sollen Security-Kontrollen zur Minimierung von identifizierten Bedrohungen eingeführt werden. Aus Kosten- und Effizienzgründen werden diese Kontrollen innerhalb jedes Service-Designs integriert. Dadurch kann sichergestellt werden, dass alle in Produktion gebrachten Services mit der Security-Richtlinie konform sind. Sicherheitsvorfälle entstehen nicht nur durch technische Bedrohungen, sondern vielmehr durch menschliche Fehlhandlungen. Zu Beginn steht ein Risiko, das von einer Bedrohung verwirklicht wird. Diese Bedrohung kann in ihrer Folge einen Geschäftsprozess unterbrechen oder sich anderweitig negativ auf das Geschäft auswirken. Je nach Bedrohung gibt es verschiedene Arten von Maßnahmen dagegen [20]:

- **Preventive:** Diese Sicherheitsmaßnahmen werden genutzt, um Sicherheitsvorfälle an ihrem Entstehen zu hindern. Als gängige Methode hierfür gelten die Zuweisung von Zugriffsrechten für eine bestimmte Gruppe von autorisierten Personen.
- **Reductive:** Bei dieser Methode sollen Maßnahmen dafür sorgen, dass Schadenauswirkungen reduziert werden, z.B. durch Backups nach einem Datenverlust.
- **Detective:** Bei Auftreten einer Sicherheitsbedrohung gilt es diese ausfindig zu machen.
- **Repressive:** Bei häufigerem Wiederholen von gleichen Sicherheitsvorfällen soll die Kontinuität unterbrochen werden. Z.B. bei häufigen Authentifizierungsversuchen.
- **Corrective:** Hierbei wird der aufgetretene Schaden behoben. Dies kann durch Wiederherstellung eines funktionierenden Systemzustands geschehen.

Fazit: Für das in dieser Arbeit beschriebene Konzept wurden einige Konzepte aus ITIL verwendet. Nach ITIL werden Security-Anforderungen bereits in der Service-Design-Phase berücksichtigt. Der in der vorliegenden Arbeit beschriebene Ansatz erlaubt es Services gemäß ITIL zu designen und zu beschreiben. Durch die Integration des Grundschutzhandbuches stehen eine Reihe konkreter Maßnahmen zur Auswahl, welche vor allem die ITIL-Bereiche „Service Design“ und „Service Operations“ unterstützen. Desweiteren lässt sich das hier implementierte Framework in die Maßnahme „Preventive“ einordnen, da mithilfe des implementierten Grundschutzkatalogs Sicherheitsvorfälle an ihrem Entstehen gehindert werden. Zudem wird der Schutzbedarf, genauso wie in ITIL empfohlen, nach den Kategorien Vertraulichkeit, Integrität und Verfügbarkeit bewertet.

2.6 ISO/IEC 27000 Familie

Die ISO/IEC 27000 Familie soll Organisationen bei der Umsetzung und Inbetriebnahme eines Managementsystems für Informationssicherheit (ISMS) unterstützen. In der „ISO 27000: Information security management systems - Overview and vocabulary“ [6] wird ein Überblick über die gesamte Serie gegeben. Eine kurze Einführung über die ISMS-Thematik und die Beschreibung des darin verwendeten Plan-Do-Check-Act (PDCA) Prozesses werden behandelt. Vor allem die beiden Standards ISO/IEC 27001 und ISO/IEC 27002 werden in der Praxis oft verwendet und auch entsprechend häufig als Grundlage für weitere Vorgehensmodelle im ISMS-Bereich verwendet. Daher werden diese nachfolgend genauer betrachtet. [6]

2.6.1 ISO/IEC 27001 ISO/IEC ist eine Norm zur Umsetzung und Verwaltung eines Informationssicherheits-Managementsystems (ISMS) [7] [5]. Das ISMS bestimmt angemessene Sicherheitsmaßnahmen, um Informationswerte in einer Organisation zu schützen. Dabei kann das ISMS unterschiedlich große Dimensionen einnehmen, da es stark von den Sicherheitsanforderungen der Organisation abhängt. Bei der Umsetzung hilft das „Plan-Do-Check-Act“-Modell (PDCA). Es nimmt als Input Informationssicherheitsanforderungen entgegen und erzielt nach einem Ablauf von Prozessen die gewünschte Informationssicherheit.

In der Plan-Phase wird das ISMS festgelegt — Dazu gehören die Leitlinie, Ziele, Prozesse und Verfahren für das Risikomanagement und die Informationssicherheit. Anschließend wird die Planung in der Do-Phase umgesetzt. Während der Prüfung werden die Prozesse an der ISMS-Leitlinie, den ISMS-Zielen und praktischen Erfahrungen gemessen. Aufgrund interner ISMS-Audits können final Korrekturmaßnahmen durchgeführt werden. [7]

2.6.1.1 Festlegung des ISMS In einem ersten Schritt wird der Anwendungsbereich des ISMS, unter Berücksichtigung der Eigenschaften und Anforderungen der Organisation, genau spezifiziert sowie aufbauend darauf das Entwerfen der

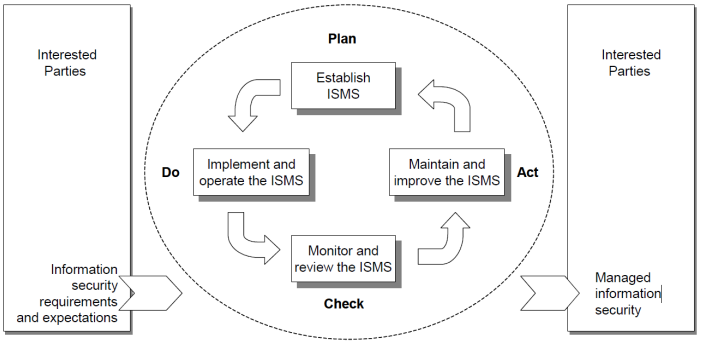

Abb. 12. Das PDCA-Modell [7]

Prinzipien. Anschließend kann eine Methode für die Risikoeinschätzung innerhalb der Organisation definiert werden — In diesem Zusammenhang wird auch eine Risikotoleranzgrenze festgelegt. Die Identifikation und Bewertung der Risiken setzt sich aus folgenden Schritten zusammen [7]:

- Identifizierung der Assets,
- Identifizierung der Bedrohungen für die Assets,
- Identifizierung der Schwachstellen, die durch diese Bedrohungen genutzt werden,
- Identifizierung der Auswirkungen bei einem Schadensfall und des möglichen Verlustes von Vertraulichkeit, Integrität und Verfügbarkeit auf die definierten Assets,
- Einschätzung des geschäftlichen Schadens bei einem Schadensfall,
- Einschätzung der Auftrittswahrscheinlichkeit,
- Beurteilung der Risikoakzeptanz.

Bei der Auswahl der Maßnahmen und Maßnahmenziele zur Bewältigung der Risiken kann der Maßnahmenkatalog des ISO 27001 herangezogen werden [7].

2.6.1.2 Umsetzen und Durchführen des ISMS In dieser Phase wird ein Risikobehandlungsplan erstellt und umgesetzt, der Ressourcen, Verantwortlichkeiten und Prioritäten der Risiken festlegt. Zusätzlich werden das ISMS und Ressourcen für das ISMS verwaltet sowie Maßnahmen umgesetzt, die Security-Events schnell erkennen und darauf entsprechend reagieren können. [7]

2.6.1.3 Überwachen und Überprüfen des ISMS In dieser Phase sollen Fehler in Verarbeitungsergebnissen und Sicherheitsverstöße erkannt werden. Daraus folgend ist zu beurteilen, ob die Maßnahmen gegen Sicherheitsverstöße effizient wirken — In diesem Zusammenhang sollen die Wirksamkeit des ISMS und der Maßnahmen kontinuierlich überprüft werden. Weitere Punkte, die einer Kontrolle unterzogen werden müssen, sind [7]:

– Überprüfung der Risikoeinschätzung der Unternehmens-Assets,
– Durchführung von internen ISMS-Audits,
– Ausführung einer Managementbewertung des ISMS,
– Aktualisierung der Sicherheitspläne bei Auffälligkeiten in den Überwachungsaktivitäten.

2.6.1.4 Instandhalten und Verbessern des ISMS Es werden die evaluierten Verbesserungen der vorherigen Phase umgesetzt — Lessons Learned aus der eigenen bzw. externen Organisation werden dabei berücksichtigt [7].

2.6.1.5 Dokumentation Die Dokumentationsfunktion der ISO 27001 soll Aufzeichnungen über den gesamten ISMS-Prozess liefern. Dabei sollen auch ausgewählte Maßnahmen derart dokumentiert sein, dass sich die darauf basierenden Risikoeinschätzungen zurückverfolgen lassen, um so zu einem späteren Zeitpunkt Schlussfolgerungen möglich zu machen. In der Dokumentation müssen im Kern der Anwendungsbereich der ISMS-Prinzipien, die gewählten Verfahren und Maßnahmen, die Methode, der Bericht zur Risikoeinschätzung sowie der Risikobehandlungsplan enthalten sein. [7]

2.6.1.6 Verbesserung des ISMS Final soll das ISMS einer ständigen Verbesserung unterzogen werden, Korrekturmaßnahmen im Zusammenhang mit der Nichtkonformität der ISMS-Anforderungen vornehmen und auch in diesem Zusammenhang Vorbeugungsmaßnahmen treffen, um mögliche Nichtkonformitäten zu vermeiden [7].

2.6.2 ISO/IEC 27002 Dieser Standard stellt Richtlinien und Prinzipien zum Initiieren, Implementieren, Warten und Verbessern der ISMS in Unternehmen zur Verfügung. Die hier beschriebenen Ziele sind für die meisten Unternehmen geeignet und bieten eine solide Grundlage, um identifizierte Risiken zu behandeln. Der Standard enthält 11 Abschnitte zu Security-Maßnahmen, die gesamt aus 39 Hauptsicherheitskategorien bestehen. Um einen Themenüberblick zu gewährleisten, sind nachfolgend die elf Sicherheitsabschnitte angeführt [8]:

– Sicherheitsleitlinie
– Organisation der Informationssicherheit
– Management der Organisationswerte
– Personalsicherheit
– Physische und umgebungsbezogene Sicherheit
– Betriebs- und Kommunikationsmanagement
– Zugangskontrolle
– Beschaffung, Entwicklung und Wartung von Informationssystemen
– Umgang mit Informationssicherheitsvorfällen
– Sicherstellung des Geschäftsbetriebs
– Einhaltung von Vorgaben

Jede Sicherheitskategorie enthält ein Kontrollziel sowie darunterliegende Kontrollen, um die Kontrollziele zu erreichen. Kontrollen werden wiederum in Kontrollen, Implementierungsrichtlinien und zusätzliche Informationen gegliedert. Die Kontrolle enthält die spezifischen Anweisungen, um das Kontrollziel zu erreichen. Die Implementierungsrichtlinie unterstützt bei der Implementierung der Kontrolle unter Berücksichtigung des Kontrollziels. Referenzen zu anderen Standards und rechtliche Vorgaben sind unter zusätzliche Informationen zu finden. [8]
Fazit: Der im ISO Standard 27000 empfohlene PDCA-Cycle wird in der vorliegenden Methode durch die TOGAF ADM repräsentiert. Neben prozessualen Vorgaben beschreibt ISO 27000 auch eine Reihe an Maßnahmen, z.B. zum Schutz vor Schadsoftware, zur Implementierung von Backups und zum Management von Netzwerksicherheit. Vergleichbare Maßnahmen werden allerdings auch im Grundschutzkatalog in detaillierterer Form beschrieben und finden in der vorliegenden Arbeit daher keine weitere Berücksichtigung.

2.7 ArchiMate

2.7.1 Einleitung Mit der ArchiMate-Spezifikation hat die Open Group eine grafische Notation zur Abbildung von Unternehmensarchitekturen publiziert. Der Standard enthält eine Menge an Entitäten und Relationen, inklusive eigener grafischer Repräsentationen, zur Abbildung von Architekturen entlang des gesamten ADM. Zudem besteht der Standard aus interrelated Architectures, rollenspezifischen Viewpoints und Mechanismen zum Customizing diverser ArchiMate-Elemente. Die Top-Level-Struktur des ArchiMate-Standards besteht auf oberster Ebene aus einem Modell, welches wiederum aus Konzepten besteht. Ein Konzept kann entweder ein Element oder eine Relation sein. Die Sub-Klassen von Elementen sind Behaviour Element, Structure Element, Motivation Element und Composite Element. [28]

2.7.2 ArchiMate Layer und Core Framework Der ArchiMate Core besteht aus drei Layern, die Klassen zur Beschreibung der Architekturschichten enthalten [28]:

- Der Business Layer deckt Geschäftsservices ab, die von Geschäftsprozessen realisiert werden. Prozesse werden wiederum von Business Actors ausgeführt.
- Der Application Layer beinhaltet Applikationen, die Services nach außen hin realisieren, um das Geschäft zu unterstützen.
- Der Technology Layer beinhaltet Technologie Services, die zur Unterstützung des Application Layers dienen. Diese Services können von Technologiekomponenten, wie Devices oder System Software, bereitgestellt werden.

Da jeder Layer aus Passive Structure Elements, Behaviour Elements und Active Structure Elements besteht, kann aus dieser Erkenntnis, der Matrix, bestehend aus 9 Zellen, jedes Architekturelement zugeordnet werden. Das Framework erlaubt es Unternehmensarchitekturen aus verschiedenen Viewpoints zu

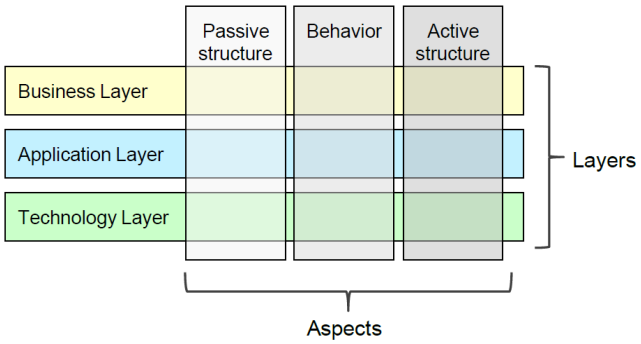

Abb. 13. ArchiMate Core Framework [28]

betrachten, da jede Zelle in dem Raster unterschiedliche Stakeholder-Interessen anspricht. Neben den Layern besteht das Framework aus drei Aspekten [28]:

- Active Structure Aspect, welcher aus Elementen wie z.B. Business Actors oder Application Components besteht und Behaviour Elemente ausführen kann.
- Behaviour Aspect, welcher Verhaltenselemente wie z.B. Prozesse, Funktionen oder Events beinhaltet, die von Active Structure Elements ausgeführt werden.
- Passive Structure Aspect, welcher aus Objekten besteht, die von Behaviour Elements getriggered werden.

Dieses Konzept lässt sich auf Real World Entities übertragen: Ein Satz besteht dabei aus einem Subjekt (Active Structure), einem Verb (Behaviour) und einem Objekt (Passive Structure). Unter ArchiMate 3.0 kann das Core Framework um weitere Layer erweitert werden. Dadurch kann die Modellierungssprache nach individuellen Bedürfnissen getailored werden. Weitere Layer sind:

- Strategy Layer
- Physical Layer
- Implementation and Migration Layer

Details zum Full Framework können im ArchiMate 3.0 Standard nachgelesen werden.

2.7.3 ArchiMate und TOGAF Während TOGAF schwerpunktmäßig ein Vorgehensmodell zur Umsetzung einer Unternehmensarchitektur darstellt, bietet die ArchiMate-Sprache die passende Notation dazu an. Die Struktur des ArchiMate Kernmodells leitet sich aus den drei Hauptarchitekturdomänen der TOGAF ADM ab (siehe Abb. 15). Die Strategy-, Motivation-, Implementation- und Migration- Elements lassen sich auf die restlichen Phasen der ADM mappen. Obwohl jedoch einige der in TOGAF definierten Viewpoints schlecht mit

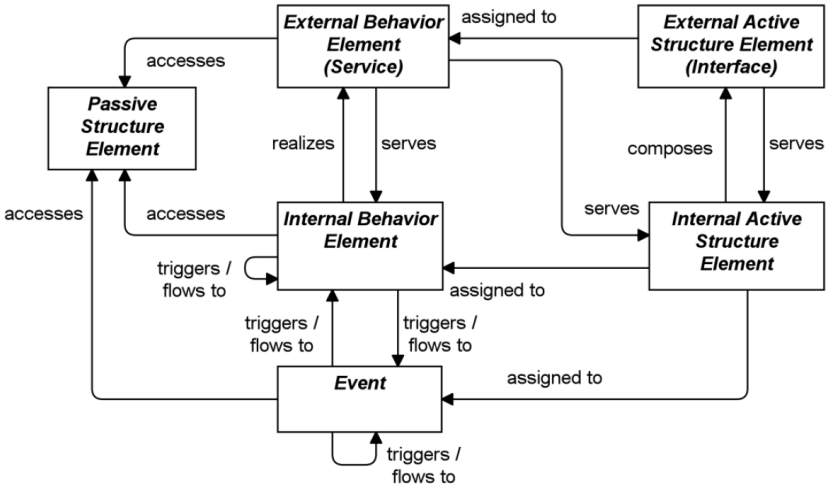

Abb. 14. ArchiMate Generic Metamodel [28]

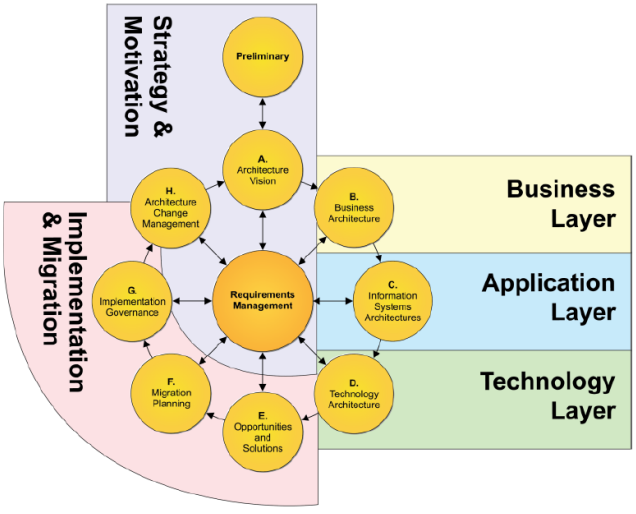

Abb. 15. ArchiMate und TOGAF Mapping [28]

jenen in ArchiMate übereinstimmen, unterstützt der ArchiMate-Standard die Konzepte, die in diesen Viewpoints adressiert werden. Im Gegensatz zu TOGAF handelt es sich bei ArchiMate nicht um ein Framework, sondern um eine Modellierungssprache — Daher spricht man von ArchiMate als Komplementersprache im Zusammenhang mit TOGAF. [28]

2.7.4 ArchiMate Metamodel Jeder ArchiMate-Layer hat sein eigenes Metamodell, welches aus dem generischen Metamodell abgeleitet ist. Nachfolgend wird auf die drei Core Metamodels eingegangen. Das Business Layer Metamo-

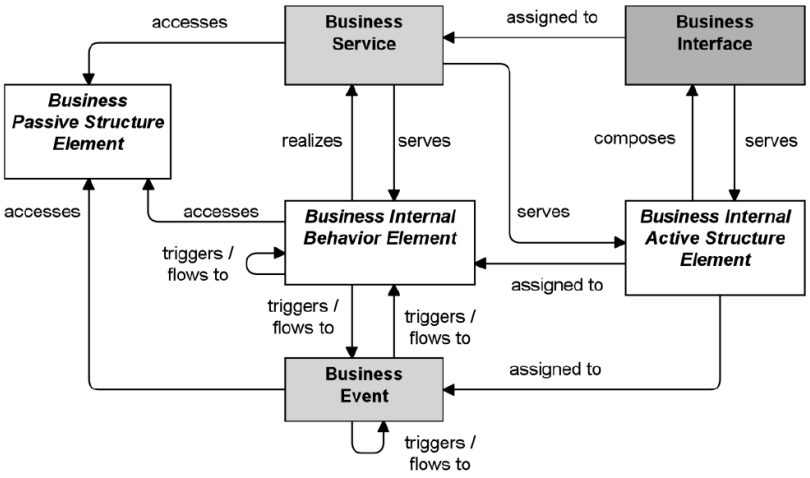

Abb. 16. ArchiMate Business Layer Metamodel [28]

del wird üblicherweise für die Modellierung der Geschäftsarchitektur verwendet. Die aktiven Entitäten sind die Subjekte, z.B. Business Actor oder Business Role, welche Behaviour Elemente, wie Geschäftsprozesse oder Funktionen, ausführen. Business Actors können dabei individuelle Personen aber auch Organisationseinheiten sein. Business Services bieten ihre Funktionalität über Business Interfaces nach außen hin an.

2.7.4.1 Geschäftsakteur Ein Geschäftsakteur ist eine Geschäftsentität, der es möglich ist Verhalten auszuüben. Er kann Geschäftsentitäten auf verschiedenen Detaillierungsebenen darstellen und kann dabei entweder als Akteur oder Organisationseinheit fungieren. Beispiele für Business Actors sind Personen, Abteilungen und Organisationseinheiten. [28]

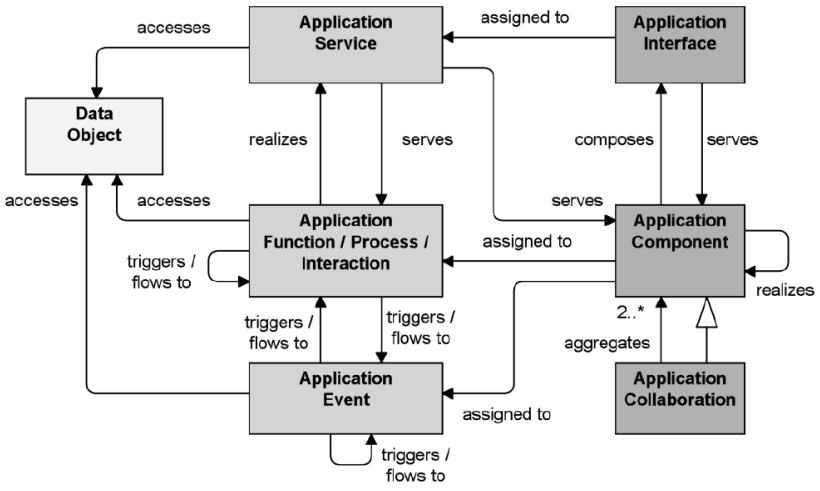

Abb. 17. ArchiMate Application Layer Metamodel [28]

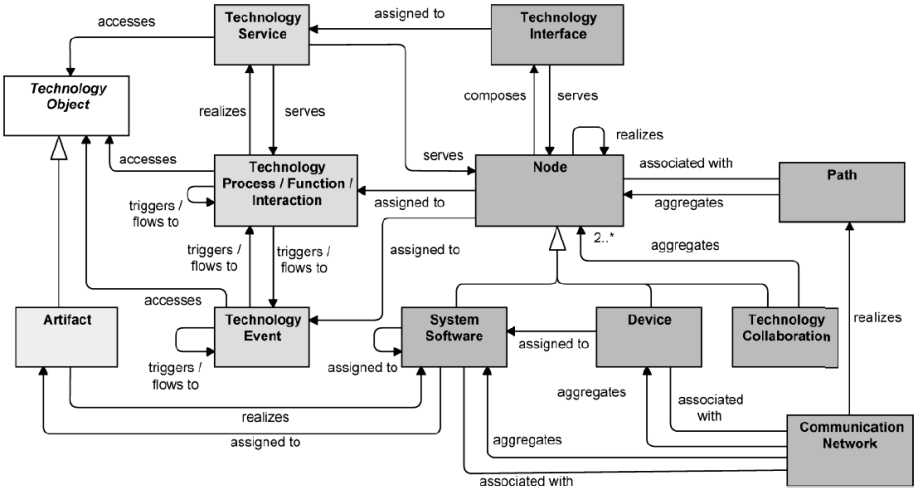

Abb. 18. ArchiMate Technology Layer Metamodel [28]

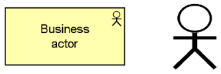

Abb. 19. Geschäftsakteur [28]

2.7.4.2 Geschäftsrolle Eine Geschäftsrolle ist verantwortlich dafür bestimmtes Verhalten auszuüben. Sie kann Geschäftsakteuren zugewiesen werden. Der Geschäftsrolle werden Geschäftsprozesse oder Geschäftsfunktionen zugewiesen. Zudem kann eine Geschäftsrolle eine unterstützende Rolle in Organisationsstrukturen einnehmen, z.B. für die Arbeitsteilung in einer Organisation. [28]

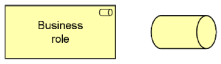

Abb. 20. Geschäftsrolle [28]

2.7.4.3 Geschäftskollaboration Eine Geschäftskollaboration ist eine Aggregation von zwei oder mehreren Internal Active Structure Elements, die zusammenarbeiten können, um gemeinsam Verhalten auszuüben. Einzelne Geschäftsrollen werden verwendet, um Verhaltenselemente wie z.B. Geschäftsprozesse auszuführen. Kollaborationen von zwei oder mehreren Geschäftsrollen führen wiederum ein Kollektiv an Verhaltenselementen aus. Dieses Kollektiv wird Geschäftsinteraktion genannt. [28]

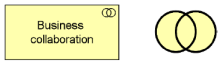

Abb. 21. Geschäftskollaboration [28]

2.7.4.4 Geschäftsschnittstelle Eine Geschäftsschnittstelle ist ein Zugangspunkt, durch welchen ein Geschäftsservice der „Außenwelt“ zur Verfügung gestellt wird. Dasselbe Geschäftsservice kann mehreren Geschäftsschnittstellen zugewiesen werden. [28]

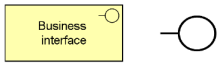

Abb. 22. Geschäftsschnittstelle [28]

2.7.4.5 Geschäftsprozess Ein Geschäftsprozess repräsentiert eine Abfolge von Geschäftsverhalten. Er wird von der Geschäftsrolle ausgeführt, um eine Menge an Produkten bzw. Services zu produzieren und stellt internes Verhalten dar. Geschäftsprozesse können zu weiteren Prozessen zusammengefasst werden. [28]

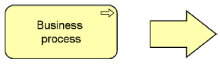

Abb. 23. Geschäftsprozess [28]

2.7.4.6 Geschäftsfunktion Eine Geschäftsfunktion ist eine Sammlung von Geschäftsverhalten basierend auf einer Menge von Kriterien. Ähnlich wie Geschäftsprozesse stellen Geschäftsfunktionen auch internes Verhalten dar und werden von Geschäftsrollen ausgeführt. Sie gruppieren Verhalten basierend auf Ressourcen, Fähigkeiten, Kompetenzen, Wissen, etc. [28]

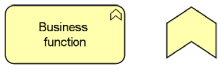

Abb. 24. Geschäftsfunktion [28]

2.7.4.7 Geschäftsinteraktion Geschäftsinteraktionen sind eine Menge von Geschäftsverhalten, welche von einer Geschäftskollaboration, bestehend aus zwei oder mehreren Geschäftsrollen, ausgeführt werden. [28]

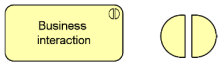

Abb. 25. Geschäftsinteraktion [28]

2.7.4.8 Geschäftsereignis Geschäftsereignisse stellen Geschäftsverhalten dar und werden für Zustandsänderungen in der Organisation verwendet. Andere Geschäftsverhaltenselemente, wie z.B. Geschäftsprozesse, werden von Geschäftsereignisse angestoßen. Sie sind unmittelbar und haben daher keine Dauer. Geschäftsereignisse können Zeitattribute enthalten, die nach einem bestimmten Zeitpunkt Verhaltenselemente anstoßen können. [28]

Abb. 26. Geschäftsereignis [28]

2.7.4.9 Geschäftsservice Ein Geschäftsservice ist ein nach außen hin sichtbares Geschäftsverhalten. Konkret wird dabei die Funktionalität von Geschäftsrollen bzw. Geschäftskollaborationen nach außen getragen. Auf diese Funktionalität kann über Geschäftsschnittstellen zugegriffen werden. Die Realisierung solcher Geschäftsservices erfolgt durch Geschäftsprozesse, Geschäftsfunktionen oder Geschäftsinteraktionen. [28]

Abb. 27. Geschäftsservice [28]

2.7.4.10 Geschäftsobjekt Ein Geschäftsobjekt repräsentiert ein Konzept innerhalb einer bestimmten Geschäftsdomäne. Geschäftsobjekte stellen typischerweise Objekttypen bzw. Klassen dar, aus denen Instanzen erstellt werden können. Sie werden zur Darstellung von Informationen verwendet, die für das Geschäft relevant sind. [28]

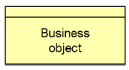

Abb. 28. Geschäftsobjekt [28]

2.7.4.11 Vertrag Ein Vertrag ist eine formale bzw. informale Vereinbarung zwischen einem Anbieter und einem Konsumenten. Er spezifiziert die Rechte und Verpflichtungen betreffend eines Produkts. Er kann auch für Service Level Agreements (SLA's) verwendet werden. [28]

Abb. 29. Vertrag [28]

2.7.4.12 Darstellung Eine Darstellung bzw. Repräsentation ist eine wahrnehmbare Form von Informationen und ist eine spezielle Art von Geschäftsobjekten. Es handelt sich um Informationsträger, welche elektronisch bzw. auf Papier bestehen können. Mögliche Formate sind z.B. HTML, ASCII, PDF, RTF, etc. [28]

Abb. 30. Darstellung [28]

2.7.4.13 Produkt Ein Produkt ist eine Menge von Services und Passive Structure Elements auf Basis von Verträgen. Produkte repräsentieren sowohl immaterielle Güter, als auch Services bzw. physische Produkte. [28]

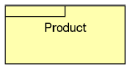

Abb. 31. Produkt [28]

Das Application Layer Metamodel wird verwendet, um die Informationssystemarchitektur des Unternehmens zu modellieren. Wie in TOGAF beschrieben wird in dieser Domäne die Struktur und Interaktion der Applikationen behandelt. Das wichtigste Active Structure Element im Application Layer ist die Application Component. Diese Klasse kann zur Modellierung ganzer Applikationen, Applikationskomponenten oder Informationssysteme verwendet werden. Das Application Interface ist der logische Kanal über den ein Application Service angesprochen werden kann. Services werden wiederum von Applicaton Components realisiert. [28]

2.7.4.14 Applikationskomponente Eine Applikationskomponente enthält modulare Anwendungsfunktionalitäten und ist eine eigenständige Einheit. Sie ist unabhängig einsetzbar, wiederverwendbar und ersetzbar. Als Active Structure Element ist die Applikationskomponente dafür zuständig Verhaltenselemente auszuführen. Die Funktionalität einer Applikationskomponente ist nur über Applikationsschnittstellen erreichbar. [28]

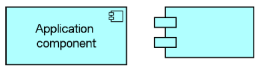

Abb. 32. Applikationskomponente [28]

2.7.4.15 Applikationskollaboration Eine Applikationskollaboration ist eine Aggregation von zwei oder mehreren Applikationskomponenten, die zusammenarbeiten, um als Kollektiv Anwendungsverhalten auszuüben. Sie bildet logische bzw. temporäre Kollaborationen von Applikationskomponenten ab und existiert nicht als eigenständige Entität. [28]

Abb. 33. Applikationskollaboration [28]

2.7.4.16 Applikationsschnittstelle Eine Applikationsschnittstelle stellt einen Zugangspunkt dar, durch den auf Applikationsservices zugegriffen werden kann. Die Schnittstelle spezifiziert wie die Applikationsfunktionalität durch andere Elemente erreicht werden kann. [28]

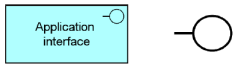

Abb. 34. Applikationsschnittstelle [28]

2.7.4.17 Applikationsfunktion Eine Applikationsfunktion repräsentiert automatisiertes Verhalten, welches durch eine Applikationskomponente ausgeführt werden kann. Sie beschreibt das interne Verhalten einer Applikationskomponente. Der Zugriff von außen auf die Applikationsfunktion erfolgt durch die Verwendung von Applikationsservices. [28]

Abb. 35. Applikationsfunktion [28]

2.7.4.18 Applikationsinteraktion Eine Applikationsinteraktion ist eine Menge aus Anwendungsverhalten und wird durch eine Applikationskollaboration, bestehend aus mehreren Applikationskomponenten, ausgeführt. [28]

Abb. 36. Applikationsinteraktion [28]

2.7.4.19 Applikationsprozess Ein Applikationsprozess ist eine Abfolge von Anwendungsverhalten, um ein bestimmtes Ergebnis zu erzielen. Er wird von der Applikationskomponente ausgeführt und beschreibt internes Verhalten. Mittels Applikationsservices kann das Verhalten nach außen publik gemacht werden. [28]

Abb. 37. Applikationsprozess [28]

2.7.4.20 Applikationsereignis Applikationsereignisse werden für Zustandsänderungen in der Organisation verwendet und stellen Anwendungsverhalten dar. Sie triggern Verhaltenselemente, wie z.B. Applikationsfunktionen, und haben keine Dauer. Sie können Zeitattribute enthalten, die verwalten, wann Verhaltenselemente angestoßen werden sollen. [28]

Abb. 38. Applikationsereignis [28]

2.7.4.21 Applikationsservice Ein Applikationsservice ist ein nach außen hin sichtbares Anwendungsverhalten. Auf die Funktionalität kann über ein oder mehrere Applikationsschnittstellen zugegriffen werden. Realisiert werden diese Artefakte von Applikationsfunktionen. [28]

Abb. 39. Applikationsservice [28]

2.7.4.22 Datenobjekt Datenobjekte sind strukturierte Informationen für automatisierte Verarbeitung. Typische Beispiele sind Kundenaufzeichnungen, Kun-

dendatenbanken oder Versicherungsansprüche. Datenobjekte haben neben der Anwendungsebene auch einen starken Bezug zur Geschäftsarchitektur. Genau wie Geschäftsobjekte stellen Datenobjekte Objekttypen dar, auf deren Basis Instanzen erstellt werden können. [28]

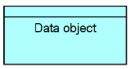

Abb. 40. Datenobjekt [28]

Das Technology Layer Metamodel wird für die Modellierung der Technologiearchitektur verwendet. Laut TOGAF wird die Technologiearchitektur als Struktur und Interaktion von Plattform Services sowie logischen und physischen Technologiekomponenten definiert. Die Hauptkomponente in diesem Metamodell ist der Node und wird zur Modellierung von strukturellen Aspekten im System verwendet. Bei einem Node kann es sich einerseits um Devices oder System Software handeln. Während Devices berechnende Ressourcen darstellen, handelt es sich bei System Software um Softwarekomponenten die auf Devices laufen. Wie in den Layern zuvor, bietet dieses Metamodell ebenfalls Interfaces und Services an, wodurch unter anderem Application Components die Funktionalitäten des Technology Layers nutzen können. [28]

2.7.4.23 Knoten Ein Knoten ist eine rechenfähige physische Ressource, die mit anderen rechenfähigen oder physischen Ressourcen in Verbindung steht. Sie führen Technologieverhalten aus und gehören daher zu den Active Structure Elements. Zudem sind Knoten dafür zuständig Artefakte zu verarbeiten. Der primäre Fokus liegt mit dem Knoten in der Unterstützung der Anwendungsebene — So kann er als Deploymentumgebung für Applikationskomponenten dienen. [28]

Abb. 41. Knoten [28]

2.7.4.24 Gerät Ein Gerät ist eine physische IT-Ressource und wird als Deploymentumgebung für System Software und Artefakte verwendet. Es handelt sich beim Gerät um eine Spezialisierung der Knoten-Klasse und wird typischerweise zur Modellierung von Hardware Systemen, wie PC's oder Router, verwendet. [28]

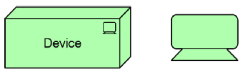

Abb. 42. Gerät [28]

2.7.4.25 System Software Bei System Software handelt sich um das Gegenstück zum Gerät. Sie stellt die Softwareumgebung für das Hosten von Software zur Verfügung. Beispiele sind Betriebssysteme, JEE Anwendungsserver, Datenbanksysteme oder Workflow Engines. System Software ist ebenfalls eine Spezialisierung des Knotens und bildet mit dem Gerät gemeinsam einen Knoten. [28]

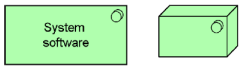

Abb. 43. System Software [28]

2.7.4.26 Technologiekollaboration Eine Technologiekollaboration ist eine Aggregation von zwei oder mehreren Knoten, um gemeinsam Technologieverhalten auszuüben. Sie bildet logische oder temporäre Kollaborationen von Knoten ab und existiert nicht als eigenständige Entität. [28]

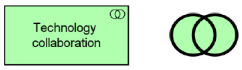

Abb. 44. Technologiekollaboration [28]

2.7.4.27 Technologieschnittstelle Eine Technologieschnittstelle repräsentiert einen Zugangspunkt, über die nach außen hin auf Technologieservices zugegriffen werden kann. Sie spezifiziert, wie auf die Funktionalität von Komponenten durch andere Elementen zugegriffen werden kann. [28]

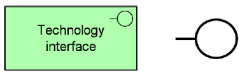

Abb. 45. Technologieschnittstelle [28]

2.7.4.28 Pfad Ein Pfad stellt die Verbindung zwischen zwei oder mehreren Knoten her, über den Daten gesendet werden können. Er ist für die logische Kommunikation zuständig und wird vom Netzwerk-Element, das für die physische Kommunikation zuständig ist, realisiert. [28]

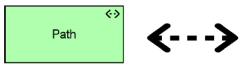

Abb. 46. Pfad [28]

2.7.4.29 Kommunikationsnetzwerk Ein Kommunikationsnetzwerk repräsentiert eine Menge an Strukturen und Verhalten, um Computersysteme für die Datenübertragung zu verbinden. Es werden zumindest zwei Geräte miteinander verbunden. Das Kommunikationsnetzwerk stellt die physische Realisierung dar und realisiert einen oder mehrere Pfade (logische Realisierung). [28]

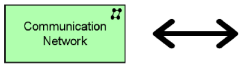

Abb. 47. Kommunikationsnetzwerk [28]

2.7.4.30 Technologiefunktion Eine Technologiefunktion stellt Technologieverhalten dar und wird von Knoten ausgeführt. Das Verhalten von Technologiefunktionen kann nach außen hin mittels Services zur Verfügung gestellt werden. [28]

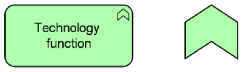

Abb. 48. Technologiefunktion [28]

2.7.4.31 Technologieprozess Ein Technologieprozess ist ein Ablauf von Technologieverhalten, das ein spezielles Ergebnis erzielt. Er kann Technologieobjekte als Input verwenden und diese weiter verarbeiten und weitere Technologieobjekte als Ergebnis erzeugen. Das Verhalten von Technologieprozessen kann nach außen hin mittels Services zur Verfügung gestellt werden. [28]

Abb. 49. Technologieprozess [28]

2.7.4.32 Technologieinteraktion Eine Technologieinteraktion ist eine Menge von Technologieverhalten, die von Technologiekollaborationen, bestehend aus mehreren Knoten, ausgeführt werden kann. [28]

Abb. 50. Technologieinteraktion [28]

2.7.4.33 Technologieereignis Technologieereignisse werden für Zustandsänderungen in der Organisation verwendet und stellen Technologieverhalten dar. Sie triggern Verhaltenselemente, wie z.B. Technologiefunktionen, und haben keine Dauer. Sie können Zeitattribute enthalten, die managen, wann Verhaltenselemente angestoßen werden sollen. [28]

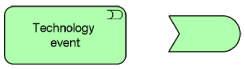

Abb. 51. Technologieereignis [28]

2.7.4.34 Technologieservice Technologieservices repräsentieren nach außen hin zur Verfügung gestelltes Technologieverhalten. Typischerweise kann das Verhalten eines Knotens durch Technologieservices zur Verfügung gestellt werden. Auf das Service kann mittels Technologieschnittstellen zugegriffen werden. [28]

Abb. 52. Technologieservice [28]

2.7.4.35 Technologieobjekt Technologieobjekte sind Passive Structure Elements und werden durch Technologieverhalten genutzt bzw. produziert. Sie sind phy-

sische Objekte und werden von der Infrastruktur im Unternehmen manipuliert. [28]

2.7.4.36 Artefakt Artefakte sind Datenelemente, welche im Softwareentwicklungsprozess verwendet oder produziert werden. Es handelt sich um eine Spezialisierung des Technologieobjekts und wird zur Darstellung von Quellcode, Skripts, Datenbanktabellen, Nachrichten oder Dokumenten verwendet. [28]

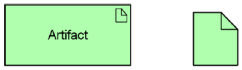

Abb. 53. Artefakt [28]

In ArchiMate wird eine Menge an Beziehungen zur Verfügung gestellt, die eine vordefinierte Menge an Quell- und Zielobjekten haben. Sie werden grundsätzlich in folgende Arten gegliedert [28]:

- Strukturelle Beziehungen — Diese Art von Beziehungen modellieren die Konstruktion oder Komposition von Konzepten. Diese Beziehungen können neben der Verwendung von Kanten auch durch Gruppierung bestimmter Objekte modelliert werden.
- Abhängigkeitsbeziehungen — Diese Beziehungen werden verwendet, um darzustellen wie Elemente von anderen Elementen unterstützt werden.
- Dynamische Beziehungen — Diese werden verwendet, um Abhängigkeiten zwischen Verhaltenselementen darzustellen.
- Andere Beziehungen — Diese Beziehungen fallen nicht in eine der oben genannten Kategorien.

2.7.4.37 Komposition Die Komposition vermittelt, dass ein Element aus einem oder mehreren anderen Elementen besteht. Sie wurde aus UML abgeleitet und das verbundene Element kann im Gegensatz zur Aggregation immer nur Teil derselben Komposition sein. Mehrere Kompositionen eines Objekts sind daher nicht möglich. Eine Kompositionsbeziehung zwischen zwei Objekten derselben Klasse ist immer möglich. Zusätzlich werden noch im Metamodell weitere zulässige Quell- und Zielobjekte genannt. [28]

Abb. 54. Komposition [28]

2.7.4.38 Aggregation Die Aggregation ermöglicht die Gruppierung von mehreren Objekten durch ein Objekt. Im Gegensatz zur Komposition kann dasselbe Objekt Teil mehrerer Aggregationen sein. Eine Aggregationsbeziehung zwischen zwei Objekten derselben Klasse ist immer möglich. Zusätzlich werden noch im Metamodell weitere zulässige Quell- und Zielobjekte genannt. [28]

Abb. 55. Aggregation [28]

2.7.4.39 Zuweisung Diese Beziehung wird für Zuweisungen von Verantwortlichkeiten und Verhaltensausführungen verwendet. Sie verbindet Active Structure Elements mit Verhaltenselementen. So kann z.B. eine Schnittstelle (Active Structure) mit einem Service (Behaviour) per Zuweisungsrelation verbunden werden. [28]

Abb. 56. Zuweisung [28]

2.7.4.40 Realisierung Die Realisierung bildet die Erstellung von Entitäten zur Laufzeit ab. Z.B. kann ein Geschäftsprozess ein Geschäftsservice realisieren oder ein Artefakt eine Applikationskomponente. [28]

Abb. 57. Realisierung [28]

2.7.4.41 Servierung Diese Beziehung wird verwendet, wenn ein Element seine Funktionalität anderen Elementen zur Verfügung stellen will. Konkret beschreibt die Beziehung, wie Services und Schnittstellen die Funktionalität von Active Structure Elements anderen Entitäten anbieten. [28]

Abb. 58. Servierung [28]

2.7.4.42 Zugang Die Zugangsbeziehung gibt Active Structure und Behaviour Elements die Möglichkeit auf Passive Structure Elements zuzugreifen, um diese zu lesen oder zu adaptieren. Konkret können z.B. Prozesse oder Funktionen Objekte anlegen, Daten aus Objekten lesen bzw. diese bearbeiten. [28]

Abb. 59. Zugang [28]

2.7.4.43 Einfluss Mit dieser Beziehung können Einflüsse auf Motivationselemente modelliert werden. Sie ist für das Verständnis dieser Arbeit nicht von Bedeutung und wird hier nur der Vollständigkeit halber erwähnt. [28]

Abb. 60. Einfluss [28]

2.7.4.44 Auslöser Diese Relation beschreibt kausale Beziehungen zwischen Verhaltenselementen. So können z.B. mehrere Prozesse miteinander kausal verbunden werden. [28]

Abb. 61. Auslöser [28]

2.7.4.45 Fluss Diese Beziehung repräsentiert Transfers von einem Verhaltenselement zum anderen. Solche Transfers können z.B. Informationen, Güter oder Geld sein. [28]

Abb. 62. Fluss [28]

2.7.4.46 Spezialisierung Die Spezialisierungsrelation beschreibt, dass ein Element ein Teil eines anderen Elements ist. Das Konzept entspricht jenem aus

UML, jedoch wird die Beziehung in ArchiMate weitläufiger gefasst. Sie kann zumindest zwischen zwei Instanzen desselben Typs verwendet werden. [28]

Abb. 63. Spezialisierung [28]

2.7.4.47 Assoziation Diese Beziehung wird verwendet, sobald es keine spezifischere Relation zur Abbildung gibt. Diese Beziehung darf für alle Elemente des ArchiMate-Metamodells verwendet werden. [28]

Abb. 64. Assoziation [28]

2.7.4.48 Knotenpunkt Beim Knotenpunkt handelt es sich um einen Relationskonnektor. So können Beziehungen desselben Typs miteinander verbunden werden. Der Konnektor kann in UND- und ODER-Knotenpunkte geteilt werden. Bei Ersterem müssen alle eingehenden Beziehungen erfüllt sein und bei Letzterem reicht eine. Der Knotenpunkt kann mehrere eingehende und eine ausgehende, eine eingehende und mehrere ausgehende oder mehrere eingehende und mehrere ausgehende Beziehungen haben. [28]

Abb. 65. Knotenpunkt [28]

2.7.5 Security Integration in ArchiMate Grundsätzlich geht die ArchiMate 3.0 Spezifikation nur sehr gering auf den Risiko- und Sicherheitsaspekt ein [2]. Ähnlich wie beim TOGAF-Framework kann auch die ArchiMate-Modellierungssprache erweitert werden, um Unternehmensarchitekten zu helfen Risiken und Sicherheit zu adressieren.
Es gibt zahlreiche Risiko- und Sicherheits-Frameworks, wobei sich einige besser in ArchiMate integrieren lassen als andere. Nachfolgend werden vier Security Frameworks analysiert und abschließend wird beispielhaft anhand des ISSRM Metamodells die Vorgehensweise des Mappings zwischen den Security- und ArchiMate-Entitäten erläutert. Bei den analysierten Frameworks handelt es

sich um Casualty Actuary Society (CAS), Committee of Sponsoring Organizations of the Treadway Commission framework (COSO) und Factor Analysis of Information Risk (Open FAIR). [2]

2.8 Committee of Sponsoring Organizations of the Treadway Commission framework

COSO wurde entwickelt, um Organisationen bei der Bewertung und Verbesserung ihrer internen Kontrollsysteme zu unterstützen. Später wurde dem Risikoaspekt immer mehr Bedeutung zugesprochen Das COSO Enterprise Risk Management (ERM) Framework enthält Prinzipien, ein Vokabular und einen Leitfaden, um ERM zu implementieren. EAM wird nach dem COSO-Standard folgendermaßen definiert:

> „... a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.“ [2]

Unsicherheiten umfassen sowohl Risiken und Chancen. Risikomanagement soll an dieser Stelle mit diesen Risiken und Chancen richtig umgehen. Die zentralen Elemente von COSO ERM sind [24]:

- Internes Umfeld — Die Unternehmenskultur wird beschrieben und in weiterer Folge, wie Mitarbeiter Risiken wahrnehmen und handhaben.
- Zielfestlegung — Das Risikomanagement ist ein essentieller Teil der Zielsetzung in einem Unternehmen.
- Ereignisidentifikation — Ereignisse werden in Form von Risiken und Chancen identifiziert.
- Risikobeurteilung — Risiken werden prinzipiell auf Ihre Auswirkung und Eintrittswahrscheinlichkeit untersucht. Unter Berücksichtigung der Fehlermöglichkeits- und -einflussanalyse wird auch die Erkennbarkeit bei der Bewertung berücksichtigt.
- Risikosteuerung — Mögliche Instrumente zur Steuerung von Risiken sind: Vermeiden, Annehmen, Verringern, Teilen.
- Kontrollaktivitäten — Verfahren, die kontrollieren, ob Maßnahmen zur Risikomitigation (Counter-Measures) ausgeführt werden.
- Information und Kommunikation — Risiken und mögliche Maßnahmen zur Risikomitigation müssen im Unternehmen kommuniziert werden.
- Überwachung — In der Phase wird das unternehmensweite Risikomanagement inklusive erforderlicher Anpassungen überwacht.

2.9 Factor Analysis of Information Risk (Open FAIR)

Dieser Open Group Standard bietet eine Definition und Taxonomie für Information Security Risk und eine Vorgehensweise zur Verwendung dieses Standards.

Grundsätzlich beschreibt es die Hauptursachen von Risiken sowie deren Definitionen und Beziehungen zueinander. Darauf basierend wird ein Vorgehensmodell zur Verfügung gestellt, welches Grundlagen anbietet, um Risiken mittels eines taxonomischen Frameworks zu messen. In der Taxonomie ist „Risiko“ abhängig von zwei Faktoren [27]:

- Loss Event Frequency (LEF)
- Loss Magnitude (LM)

Die Loss Event Frequency misst die Eintrittswahrscheinlichkeit eines Vermögensschadens innerhalb einer bestimmten Zeitspanne. Dieser Faktor lässt sich einerseits in „Threat Event Frequency“ (TEF) und andererseits in Verwundbarkeit gliedern. Während TEF die Wahrscheinlichkeit misst, dass ein Vermögensgegenstand angegriffen wird, soll die Verwundbarkeit festhalten, ob der Schaden abgewehrt werden kann. Sie misst daher, ob eine Bedrohung zu einem Loss-Event werden kann. TEF wird detaillierter in Contact Frequency (CF) und Probability of Action gegliedert. Wie in der Ebene zuvor wird hier auch die Wahrscheinlichkeit gemessen, ob ein Event tatsächlich auftritt (CF) und ob die Bedrohung den Vermögensgegenstand auch nach erfolgtem Kontakt angreift. Die Verwundbarkeit misst einerseits die Stärke, die von der Bedrohung ausgeht (Threat Capability), und anderseits die Resistenzstärke des Systems. Basierend darauf misst die LM die Wahrscheinlichkeit der Auswirkungen nach einem Loss Event. Dabei können Schäden primäre (als unmittelbare Folge), bzw. sekundäre (als Folge der primären Phase) Auswirkungen auf Vermögensgegenstände haben. [27]
Basierend auf diesen Regeln kann diese Taxonomie auch individuell weiter in die Tiefe gebaut werden.

2.10 CAS ERM

Während die Open FAIR Taxonomie verwendet wird, um ein einzelnes Risiko zu analysieren, beschäftigt sich die Taxonomie von CAS ERM mit der Klassifizierung von Risiken innerhalb einer bestimmten Domäne. CAS unterscheidet vier Arten von Unternehmensrisiken [2]:

- Zufällige Risiken: Beinhalten Risiken wie Höhere Gewalt.
- Finanzielle Risiken: Beinhalten Liquidität, Preise, Kredite, Inflationen, usw.
- Operationale Risiken: Diese entsprechen Risiken, die aus dem Betrieb hervorgehen. Z.B. Zuständigkeiten, Verfügbarkeit von Informationstechnologien, usw.
- Strategische Risiken: Dazu gehören Rufschädigung, Wettbewerb, demographische, soziale und kulturelle Trends, usw.

2.11 ISSRM Domain Model

Es existieren viele Information System Security Risk Management Ansätze. Das Tudor Centre hat die verschiedenen Ansätze und Konzepte von ISSRM mittels eines Domain-Metamodells formalisiert. Das Domain Model wurde unter

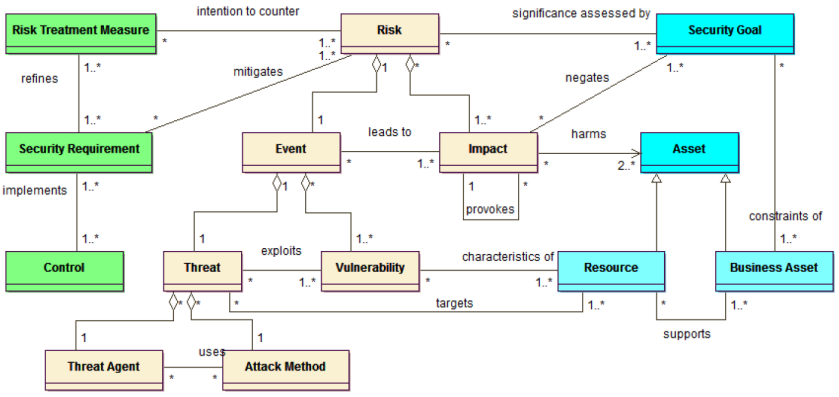

Abb. 66. ISSRM Domain Model [16]

Verwendung von Risikomanagement-Standards, sicherheitsbezogene Standards, Security Risk Management Standards und Security Requirements Engineering Frameworks erstellt. [16] Das Ziel von ISSRM ist Vermögensgegenstände einer Organisation vor Bedrohungen zu schützen. Nachfolgend wird auf diese Kernkonzepte des ISSRM Domain Models eingegangen [16]:

- Asset-related concepts
- Risk-related concepts
- Risk treatment-related concepts

Mittels sogenannter Asset-related concepts wird beschrieben, welche Vermögensgegenstände geschützt werden müssen und welche Maßnahmen es braucht, um dies zu gewährleisten. Risiken stellen eine Kombination aus Bedrohungen dar, mit jeweils einer oder mehreren Schwachstellen, welche negative Auswirkungen auf Vermögenswerte eines Unternehmens haben. Risk treatment-related concepts beschreiben welche Maßnahmen und Kontrollen implementiert werden müssen, um Risiken zu mindern. [16]
Im Folgenden werden die ISSRM-Konzepte, wie sie im Metmodell zu finden sind, beschrieben [16]:

- Vermögen — Assets in einer Organisation generieren Werte und werden zur Erreichung von Unternehmenszielen benötigt.
- Geschäftsvermögen — Business Assets stellen einen Wert für die Organisation dar und beschreiben unter anderem Informationen, Prozesse und Geschäftsfähigkeiten.
- IS-Vermögen — Informationssystem-Vermögen stellen Komponenten aus der IS-Domäne dar und unterstützen Geschäftsvermögen, wie z.B. Technologien oder Datenbanken.
- Sicherheitsziel — Sicherheitskriterien werden definiert und für das Geschäftsvermögen angewendet. Die Kriterien sind zumeist Vertraulichkeit, Verfügbarkeit und Integrität.

– Risiko — Ein Risiko ist die Kombination einer Bedrohung inklusive einer oder mehrerer Schwächen für das System der Organisation. Risiken haben negative Auswirkungen auf das Vermögen des Unternehmens.
– Auswirkung — Ist die negative Konsequenz eines Risikos.
– Schwäche — Ist eine Charakteristik eines IS-Assets, das Schwächen für einen Angriff enthält.
– Bedrohung — Hier handelt es sich um einen Vorfall, welcher ein oder mehrere IS-Assets betrifft und Schaden verursacht.
– Risikobehandlung — Das ist die Entscheidung identifizierte Risiken zu behandeln.
– Sicherheitsanforderung — Dies sind Anforderungen, die getroffen werden, um mögliche Risiken zu mildern.
– Kontrolle — Kontrollen werden auf Basis von Sicherheitsanforderungen entworfen und sollen die Sicherheit verbessern.

2.12 Mapping zwischen ArchiMate und ISSRM Domain Model

Tabelle 1. ISSRM-ArchiMate Mapping [16]

ISSRM Konzept	**EAM Konzept**	**Mapping**
Business Asset	Business Process	Generalisation
Business Asset	Business Object	Generalisation
Business Asset	Business Actor	Generalisation
Business Asset	Business Role	Generalisation
IS Asset	Application Component	Generalisation
IS Asset	System Software	Generalisation
IS Asset	Node	Generalisation
IS Asset	Device	Generalisation
IS Asset	Network	Generalisation
Security Objective	Driver	Specialisation
Risk	Assessment	Specialisation
Event	Assessment	Specialisation
Impact	Assessment	Specialisation
Threat	Assessment	Specialisation
Vulnerability	Assessment	Specialisation
Risk Treatment	Goal	Specialisation
Security Requirement	Requirement	Specialisation
Control	Core Element	Specialisation

ISSRM unterscheidet grundsätzlich zwischen Geschäfts- und IS-Assets. Die ArchiMate-Elemente Business Process, Business Object, Business Actor und Business Role sind Spezialisierungen von Geschäftsvermögen im Kontext von Risikomanagement. In ISSRM unterstützen IS-Assets jene Komponenten aus dem Geschäftsvermögen. Das entspricht etwa dem Konzept in ArchiMate — Elemente aus dem Application Layer unterstützen Business Layer Elemente.

Daher können Elemente aus dem Technology und Application Layer auf IS Assets in Form von Spezialisierungen gemapped werden. [16] Sicherheitsziele sehen es vor Geschäftsvermögen zu sichern. Diese können auf Driver und Risiken von Assessments gemapped werden. Das Mapping zwischen Sicherheitszielen und Geschäftsvermögen erfordert noch zusätzliche Konzepte, da ArchiMate keine direkte Beziehung zwischen Driver (Sicherheitsziel) und den Elementen aus dem Business Layer unterstützt. Jedoch hat ein Driver Einfluss auf den Wert von Geschäftsservices. Die Risikokomponenten (Event und Impact) sowie Bedrohungen und Schwächen werden auf Assessment gemapped. Die Risikobehandlung — Beibehaltung, Reduktion, Weiterleitung, Vermeidung — wird auf die Klasse „Goal“ (Ziel) in ArchiMate gemapped. Das ISSRM-Element Sicherheitsanforderung kann auf die ArchiMate-Klasse Requirement gemapped werden. Eine Übersicht über die ISSRM- und ArchiMate-Konzepte ist in der Tabelle 1 zu sehen. [16] Im Vordergrund des Mappings steht die Lösung der semantischen Heterogenität durch konzeptuelles mappen mittels Integrationsregeln [32]. Das konzeptuelle Mappen erfordert eine Übereinstimmung zwischen zumindest einem Konzept jedes Metamodells. Die Übereinstimmung kann klassifiziert werden in: Äquivalenz, Relation und Nicht-Relation. Bei der Relation zwischen zwei Konzepten kann es sich um Generalisierung, Spezialisierung, Komposition, Aggregation, Assoziation und Klassifikation handeln. Äquivalente Konzepte werden durch Angleichungsregeln (Verschmelzen, Mapping und Abstraktion) integriert.
Fazit: ArchiMate bildet eine ideale Grundlage für die Dokumentation der Unternehmensarchitektur. Die Security Frameworks CAS ERM, Open FAIR und COSO beinhalten Verfahrensanweisungen zur Identifikation und Handhabung von Risiken. In der vorliegenden Arbeit werden insbesondere Anleihen aus dem ISSRM-Metamodell genommen, da dieses bereits ein Mapping auf ArchiMate beinhaltet. Insbesondere das Mapping der sicherheitsspezifischen Konzepte (Risk, Event, Impact, ...) des ISSRM bleibt vage. Genau hier setzt die vorliegende Arbeit an. Das ArchiMate Metamodell wird um vergleichbare Konzepte aus dem BSI-Grundschutzkatalog erweitert. Dabei wird starke Anleihe an dem ISSRM-Metamodell genommen.
Der Grundschutzkatalog wird im nachstehenden Kapitel detailliert vorgestellt.

2.13 IT-Grundschutz des BSI

Mit den IT-Grundschutzkatalogen hat das BSI ein Vorgehensmodell entwickelt, um Unternehmen mit Sicherheitsmechanismen auszustatten. Durch den ständigen Einsatz neuer Technologien zur Gewährleistung von Effizienzsteigerungen in betrieblichen Prozessen, steigt ebenfalls die Komplexität der IT-Infrastruktur. Diese stetige Steigerung erfordert eine kontinuierliche Anpassung der Sicherheitsmechanismen.

Der IT-Grundschutz bietet eine einfache Methode, um Informationen in einem Unternehmen zu schützen. Er bietet sowohl eine IT-Grundschutz-Vorgehensweise als auch diverse IT-Grundschutz-Kataloge, die eine Reihe konkreter Sicherheitsmaßnahmen auflisten sowie eine Methodik zur Auswahl und Anpassung geeigneter Maßnahmen, an. Durch die Anfälligkeit der IT auf

Schäden und Datenverlust besteht ein großes Interesse sämtliche Daten, die elektronisch verarbeitet werden, zu schützen. Potentielle Schäden lassen sich im Verlust der Verfügbarkeit, Integrität und Vertraulichkeit kategorisieren.

Ziel des IT-Grundschutzes ist es sämtliche in einer Organisation befindlichen Informationen zu schützen. Eine angemessene Kombination aus organisatorischen, personellen, infrastrukturellen und technischen Standardsicherheitsmaßnahmen tragen zu einem ausreichenden Schutzbedarf bei. [34]

Der BSI besteht, aufbauend auf der Entwicklung eines ISMS, aus folgenden Komponenten:

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
- BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
- BSI-Standard 100-4: Notfallmanagement
- Bausteine
- Gefährdungskataloge
- Maßnahmenkataloge

Der BSI-Grundschutz liefert eine Reihe an Standards, die Organisationen heranziehen können, um sich die darin enthaltenen Empfehlungen zu Methoden, Prozessen und Verfahren zu Informationssicherheit zunutze machen zu können. [34]

2.13.1 BSI-Standard 100-1 Dieser Standard beschreibt Anforderungen, die ein ISMS gewährleisten muss. Er ist kompatibel mit dem ISO-Standard 27001. Die dort beschriebenen Anforderungen werden im BSI-Standard 100-1 konkretisiert und praxisbezogen beschrieben.

2.13.2 BSI-Standard 100-2 In der IT-Grundschutz-Vorgehensweise wird beschrieben, wie ein ISMS aufgebaut und umgesetzt wird, basierend auf den spezifizierten Anforderungen der vorherigen Phase. Für die Umsetzung können die IT-Grundschutz-Kataloge herangezogen werden, die fester Bestandteil der IT-Grundschutz-Vorgehensweise sind.

2.13.3 BSI-Standard 100-3 Die Standard-Sicherheitsmaßnahmen, welche die Grundschutz-Kataloge behandeln, sind in den meisten Anwendungsfällen ausreichend. In Fällen von Sicherheitsanforderungen, die über das normale Maß hinausgehen, z.B. bei einem erhöhten Schutzbedarf, muss eine detaillierte Risikoanalyse in einem vorausgehenden Schritt durchgeführt werden. Für dieses Szenario bietet der BSI-Standard 100-3 ein Vorgehensmodell.

2.13.4 BSI-Standard 100-4 Der BSI-Standard 100-4 behandelt das Business Continuity Management und soll ein Notfallmanagement in einem Unternehmen aufbauen. Das Ziel ist Schäden zu minimieren und die Ausfallsicherheit zu erhöhen.

2.13.5 Baustein-Kataloge Kern des IT-Grundschutzes stellen die Baustein-Kataloge dar. Diese bestehen aus zahlreichen IT-Komponenten, wie sie in Unternehmen zu finden sind. Zu jeder Komponente werden die Gefährdungslage sowie passende Maßnahmen beschrieben. Gefährdungen werden prinzipiell nach den Bereichen Höhere Gewalt, Organisatorische Mängel, Menschliche Fehlhandlungen, Technisches Versagen und Vorsätzliche Handlungen kategorisiert. Sie werden in folgende Kataloge gruppiert [34]:

- B 1: Übergreifende Aspekte der Informationssicherheit
- B 2: Sicherheit der Infrastruktur
- B 3: Sicherheit der IT-Systeme
- B 4: Sicherheit im Netz
- B 5: Sicherheit in Anwendungen

2.13.6 Gefährdungskataloge In diesen Katalogen werden Beschreibungen zu den potentiell möglichen Gefährdungen aufgeführt. Die Gefährdungen sind in folgende Kataloge gruppiert [34]:

- G 0: Elementare Gefährdungen
- G 1: Höhere Gewalt
- G 2: Organisatorische Mängel
- G 3: Menschliche Fehlhandlungen
- G 4: Technisches Versagen
- G 5: Vorsätzliche Handlungen

2.13.7 Maßnahmenkataloge In diesen Katalogen werden Maßnahmen zur Bewältigung von Gefährdungen im Unternehmen behandelt. Die Maßnahmen sind in folgende Maßnahmenkataloge gegliedert [34]:

- M 1: Infrastruktur
- M 2: Organisation
- M 3: Personal
- M 4: Hard- und Software
- M 5: Kommunikation
- M 6: Notfallvorsorge

Fazit: Im Gegensatz zu allen anderen Security Frameworks bietet der BSI-Grundschutz neben einem Vorgehensmodell, die Grundschutzkataloge als Referenzmodell für Maßnahmen, Bausteine und Gefährdungen. Unternehmen können damit auf einfache Art und Weise relevante Maßnahmen, bezogen auf die jeweiligen Vermögenswerte, ableiten. Aufgrund der Annahme, dass die Nutzung des Referenzmodells Zeit und Ressourcen bei der Implementierung und beim Betrieb von Security-Management spart und somit insbesondere für KMU's möglich wird Security-Management effizient zu betreiben, wird der Katalog in die vorliegende Lösung integriert. Andockpunkte zu ArchiMate werden, wie in Abschnitt 2.11 beschrieben, ausgestaltet.

3 Vorgehensweise zur Konzeption der Modellierungsmethode

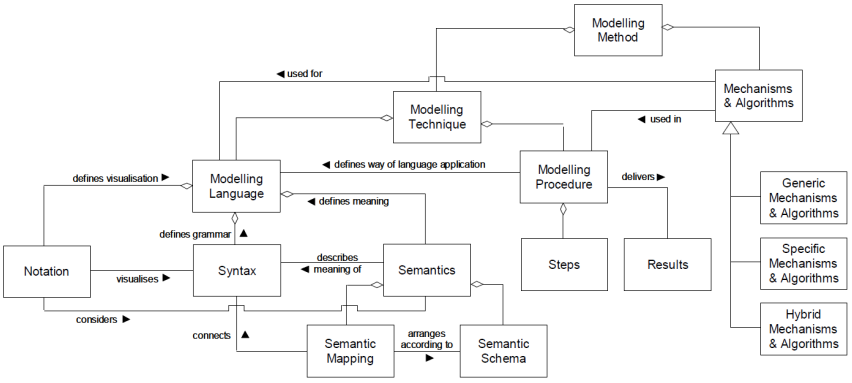

Abb. 67. Komponenten von Modellierungsmethoden [13]

Der OMI Lifecycle ist ein iterativer Prozess, um eine Modellierungsmethode zu konzeptualisieren und zu entwickeln. Dieser Prozess besteht dabei aus fünf Phasen [12][14]:

- Create — In dieser Phase wird die Idee ausgearbeitet. Es werden die Anforderungen der Modellierungsmethode definiert. Dazu bedient man sich verschiedenster Hilfsmittel und greift auf textuelle Beschreibungen bzw. Grafiken zurück.
- Design — Es werden das Metamodell, die Sprache, Grammatik, Notation und Funktionalität spezifiziert.
- Formalize — Das Ergebnis der vorherigen Phase wird in eine formale Schreibweise gebracht, um die Methode publizierfähig zu machen.
- Develop — In dieser Phase wird die Modellierungsmethode, basierend auf der Planung in der Design-Phase, entwickelt.
- Deploy/Validate — Hier wird die Software deployed und Stakeholder werden in Kontakt mit der Methode gebracht. Die Erfahrungen werden an die erste Phase zurückgegeben.

3.1 Create

Das Ziel der hier entwickelten Modellierungsmethode ist die Integration eines Sicherheits- und Risikokonzepts in die bestehende ArchiMate-Modellierungsmethode. Dazu soll neben den in ArchiMate vorhandenen Core-Layern, Business, Application und Technology, eine Extension, „Security“, hinzugefügt werden. Es ist gefordert, dass die beiden Bereiche Grundschutz und Schutzbedarf abgedeckt sind, um ein solides Security-Konzept entwerfen zu können. Um einen praktischen Use Case zu schaffen, soll ebenfalls eine grafische Auswertung in Form einer Likelihood-Impact-Analyse basierend auf den bewerteten Elementen, möglich sein. ArchiMate wird somit um Modellierungskonstrukte (als Teil der Modellierungssprache) aber auch um Algorithmen, zur Bewertung der Architekturen, erweitert.
Initial wird die Modellierung der Architektur vorgenommen. Der Schutzbedarf sieht anschließend eine Bewertung der Datenelemente im Modell vor. Datenelemente werden nach den klassischen Sicherheitsattributen „Vertraulichkeit“, „Verfügbarkeit“ und „Integrität“ bewertet. Dadurch, dass solche Datenelemente zumeist mit anderen Architekturelementen, wie Server, Applikationen, Schnittstellen, Services, usw. verbunden sind, ist auch eine entsprechende Bewertung dieser Elemente vorzunehmen. Die hier vorgestellte Methode geht davon aus, dass der Schutzbedarf eines Servers eng mit dem Schutzbedarf eines IT-Assets, welches diese Daten verwaltet, korreliert. Der Schutzbedarf kann somit vom Schutzbedarf der Daten abgeleitet werden. Genauso verhält es sich mit einer Applikation, die entsprechende Daten liest bzw. weiterverarbeitet. Handelt es sich etwa um hoch vertrauliche Daten, so ist die Applikation ebenfalls entsprechend einzustufen. Basierend auf dieser Annahme können Netzwerke von Architekturelementen, auf Grundlage der Bewertung von Datenobjekten, automatisiert bewertet werden. Steht ein Architekturelement mit mehreren Daten in Verbindung, welche jeweils unterschiedliche Security-Anforderungen besitzen, so ist das Architekturelement so zu bewerten, wie das am kritischsten bewertete Datenelement. So kann mittels einer Maximum-Funktion über einen Baum von Architekturelementen traversiert werden. In [18] wird beschrieben, wie der Analyseansatz zur Bewertung anhand von Verfügbarkeit, Genauigkeit, Vertraulichkeit und Integrität verwendet wird. Neben des Schutzbedarfs stellt der Grundschutz einen weiteren wichtigen Aspekt in der Bewertung von Sicherheit in Architekturen dar. Grundsätzlich besteht der Grundschutzkatalog des BSI aus den Konzepten Baustein, Maßnahme und Bedrohung [34]. Um eine Grundschutzbewertung vornehmen zu können, ist eine Metamodellerweiterung von ArchiMate um diese 3 Konzepte vorzunehmen. Konkret wird ein Mapping der Bausteine des Grundschutzkatalogs mit den Objektinstanzen in ArchiMate vorgenommen. Das Ziel ist somit eine Bewertung der Maßnahmen aus dem Grundschutzkatalog im Zusammenhang mit den Architekturelementen. Durch die Zuordnung der Bausteine mit den ArchiMate-Elementen können die jeweiligen Maßnahmen aus den Bausteinen geladen und den ArchiMate-Elementen zugeordnet werden. In einem nächsten Schritt werden die Maßnahmen pro Asset bewertet.
Nach der Bewertung des Schutzbedarfs und des Grundschutzes, auf Basis des

Grundschutzkatalogs des BSI, ist eine Auswertung in Form einer Likelihood-Impact-Analyse möglich. Diese besteht aus den zwei Ausprägungen „Impact“ und „Likelihood“. Da es einen direkten Zusammenhang mit Schutzbedarf und Grundschutz auf diese beiden Ausprägungen gibt, kann daraus eine zusammenhängende Analyse erstellt werden. Sie stellt die Wahrscheinlichkeit eines Risikoauftretens der Risikoauswirkung in einer Organisation gegenüber.

3.2 Design

In dieser Phase soll die Spezifikation aus der Create-Phase formal spezifiziert werden. Um die Modellierungsmethode zu erstellen, wird das Framework von [13] bzw. [12] verwendet. Modellierungsmethoden bestehen dabei aus einer Modellierungstechnik, bestehend aus Modellierungssprache und Modellierungsprozedur, sowie Mechanismen und Algorithmen. Die Modellierungssprache enthält Elemente, mit denen sie beschrieben wird: Syntax, Semantik und Notation. Das Vorgehensmodell enthält konkrete Schritte, um Ergebnisse aus der Modellierungssprache zu erzielen.

3.2.1 Metamodell In der nachfolgenden Tabelle (siehe Tabelle 2) ist eine formale Beschreibung des Metamodells gegeben. Die grafische Repräsentation (GRAPHREP) ist in der Abb. 68 zu sehen. Die Syntax des Metamodellierungs-Frameworks wurde mithilfe eines Klassendiagramms dargestellt (siehe Abb. 69).

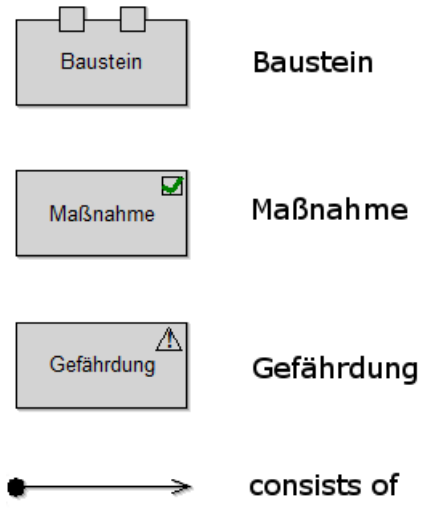

Abb. 68. Notation

Tabelle 2. Metamodell

Klassen	**Beschreibung**
Baustein	Dieses Element entspricht jenem aus dem Grundschutzkatalog des BSI. Jeder Baustein besteht aus Maßnahmenempfehlungen und Gefährdungslage. Der Baustein wird Objekten des ArchiMate-Metamodells passend zugeordnet.
Maßnahme	Maßnahmen sind Bausteinen untergeordnet und entsprechen Empfehlungen, um das Risikoauftreten gering zu halten.
Gefährdung	Gefährdungen sind Bausteinen untegeordnet und beschreiben die Gefährdungslage pro Baustein.
besteht aus	Repräsentiert die Relation von Bausteinen zu Maßnahmen bzw. Gefährdungen.
Analyse	Die Analyseklasse entnimmt Informationen aus den nach dem Grundschutz und Schutzbedarf bewerteten Elementen und generiert daraus eine Likelihood-Impact-Grafik.
Attribute	
Name	Der Name des Elements.
Icon	Feld zur Auswahl einer alternativen grafischen Notation zur Darstellung des Objekts.
Confidentiality	Bewertung der Vertraulichkeit des jeweiligen Datenobjekts. Ausprägungen sind: Kein Eintrag, 1 - Very Low, 2 - Low, 3 - Average, 4 - High, 5 - Very High
Integrity	Bewertung der Datenintegrität. Ausprägungen sind: Kein Eintrag, 1 - Very Low, 2 - Low, 3 - Average, 4 - High, 5 - Very High
Availability	Bewertung der Verfügbarkeit von Daten. Ausprägungen sind: Kein Eintrag, 1 - Very Low, 2 - Low, 3 - Average, 4 - High, 5 - Very High
Measures	Dient der Verbindung von ArchiMate-Architekturelementen und konkreten Maßnahmen aus dem Grundschutzkatalog des BSI.
Grundschutz-Score	Eine Kennzahl deren Wert dem Quotienten der erfüllten Maßnahmen in Relation mit allen Maßnahmen entspricht.
Impact	Der Wert wird für die grafische Analyse des Likelihood-Impacts benötigt. Ausprägungen sind: Kein Eintrag, 1 - Very Low, 2 - Low, 3 - Average, 4 - High, 5 - Very High
Likelihood	Der Wert wird für die grafische Analyse des Likelihood-Impacts benötigt.,Ausprägungen sind: Kein Eintrag, 1 - Very Low, 2 - Low, 3 - Average, 4 -,High, 5 - Very High
Risk Appetite	Gibt den Risikoappetit der ausgewerteten Analyse an.

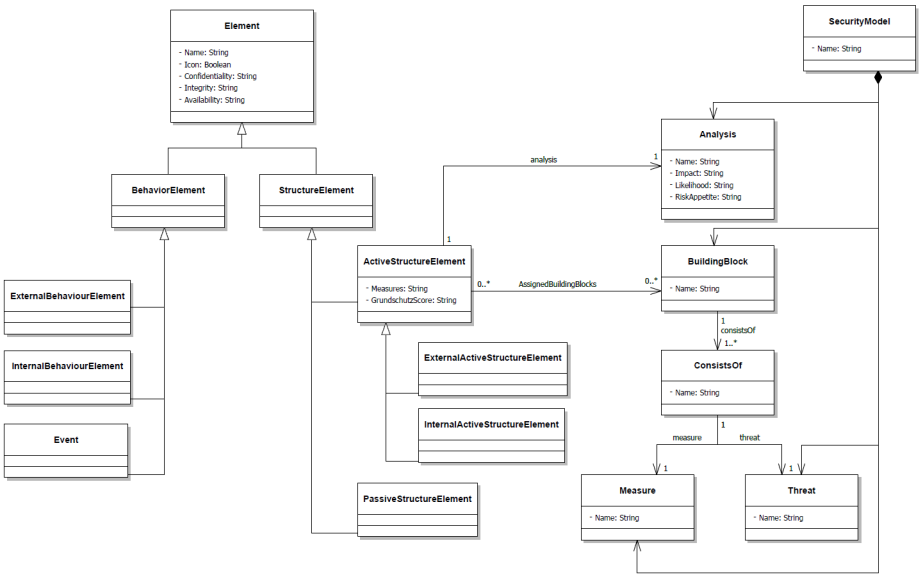

Abb. 69. Syntax

3.2.2 Vorgehensmodell (Modellierungsprozedur) Zu Beginn der Prozedur steht die Modellierung im Vordergrund. Es können Business-Layer-, Application-Layer- und Technology-Layer-Modelle oder layer-übergreifende Modelle erstellt werden. Anschließend können beliebige Architekturen modelliert werden. Unter der Voraussetzung, dass Datenobjekte modelliert wurden, können diese anschließend nacheinander bewertet werden. Die Bewertungsausprägungen sind „Confidentiality“, „Integrity“ und „Availability“ (siehe Tabelle 2). Fehlen Informationen zu diesen drei Attributen, wird das Attributfeld mit „No Entry“ bewertet. Je schlechter die Vertraulichkeit/Verfügbarkeit/Integrität, desto höher ist der Impact bei Auftreten eines Risikos. Nach erfolgter Bewertung kann der Algorithmus zur Bewertung des Schutzbedarfs angestoßen werden. Anschließend wird das gesamte Architekturnetzwerk automatisch bewertet. Nach der Schutzbedarfsbewertung erfolgt die Bewertung des Grundschutzes. Dazu ist es erforderlich den Grundschutzkatalog in Form von Modellen zur Verfügung zu haben — Es müssen daher Bausteine, Maßnahmen und Gefährdungen in Form von Modellierungselementen zur Verfügung stehen. Anschließend können Bausteine mit den passenden Architekturelementen verbunden werden. Sind alle Elemente korrekt gemapped, kann der Algorithmus zur Bewertung des Grundschutzes angestoßen werden. Dieser Algorithmus erzeugt eine Maßnahmentabelle in den Notebooks der ArchiMate-Architekturelemente, sofern diese mit den Bausteinen verbunden sind. Anschließend kann jede Maßnahme in den einzelnen Tabellen mit erfüllt bzw. nicht erfüllt bewertet werden (siehe Abb. 70). Sind alle Maßnahmen erfüllt, ist der Grundschutz sehr hoch, wodurch die Eintrittswahrscheinlichkeit eines Risikos sehr gering gehalten wird. Bei wenig erfüllten

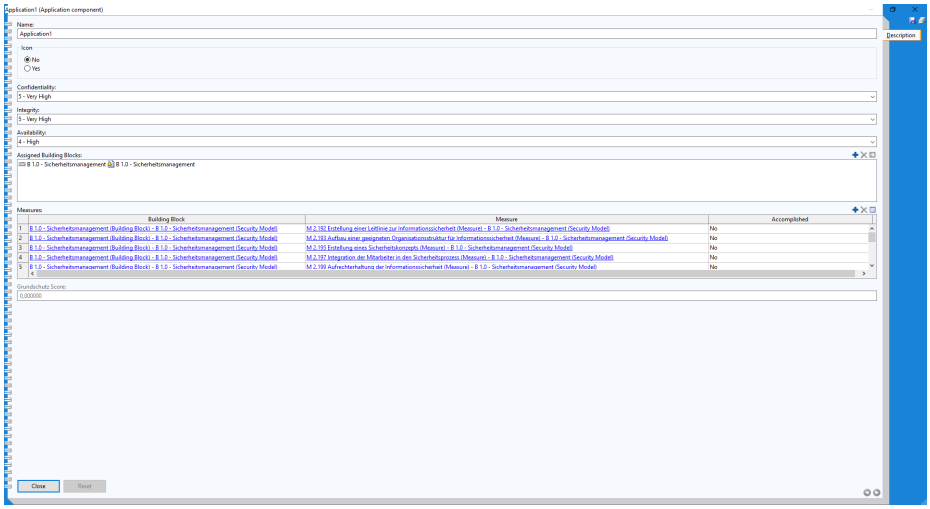

Abb. 70. Maßnahmenbewertung

Sicherheitsmaßnahmen steigt die Eintrittswahrscheinlichkeit. Nach erfolgreicher Bewertung in Bezug auf Grundschutz und Schutzbedarf, kann der Algorithmus zur Generierung einer Likelihood-Impact-Analyse gestartet werden.

3.2.3 Mechanismen und Algorithmen Nach [13] können Mechanismen entweder generisch, hybrid oder spezifisch sein. [10] Die hier beschriebenen Algorithmen sind alle spezifisch gehalten. Sie sind daher nicht metamodellunabhängig und nur für die in dieser Arbeit beschriebene Modellierungsmethode geeignet. Der Algorithmus zur Bewertung des Schutzbedarfs berechnet anhand einer Maximum-Funktion den jeweils höchsten Wert von Verfügbarkeit, Vertraulichkeit und Integrität und aggregiert die Werte zum nächst verbundenen Element. Das Element übernimmt diese Werte und kann sie anschließend ebenfalls über das nächst verbundene Element übertragen. So kann über alle übergeordneten Objekte traversiert werden. Für die Richtung der Bewertung sind die Kanten in ArchiMate ausschlaggebend. In ArchiMate muss zwischen ein- und ausgehenden Kanten unterschieden werden, um die Richtungsweisung des Algorithmus korrekt zu haben. So kann es sein, dass der Pfad zwischen ein- und ausgehenden Beziehungen differenziert werden muss. Problematisch wird es bei Elementen, die ein- und ausgehende Beziehungen vom selben Typ zulassen. Hier besteht die Gefahr, dass der Zyklus nicht terminiert. Das gilt z.B. für die Klasse „Data Object“, die sowohl mit eingehenden als auch ausgehenden „Access“-Kanten verbunden werden kann. Eine Möglichkeit ist zunächst den Baum mit einer Traversierungs-Strategie, z.B. breadth-first, zu durchlaufen und sämtliche Informationen über Objekte und Kanten zu speichern (siehe Abb. 71). Nun kann bei der nächsten Iteration des Baumes überprüft werden, welche Elemente bereits zur Gänze bewertet wurden und somit der Zyklus auch termi-

nieren.
Bei der Bewertung des Grundschutzes muss der Algorithmus über sämtliche den

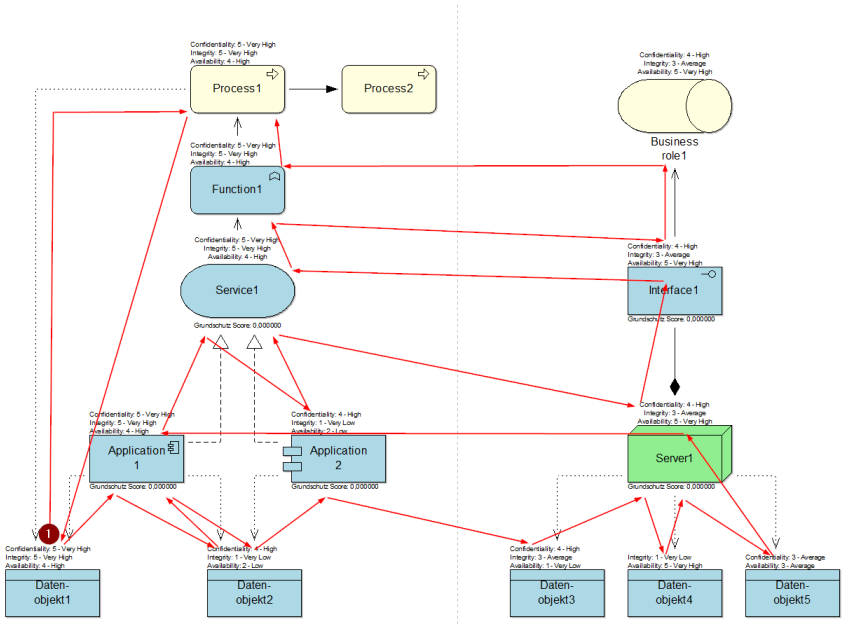

Abb. 71. Breitensuche

ArchiMate-Objekten zugewiesenen Bausteinen iterieren. Dadurch, dass Bausteine direkt mit Maßnahmen und Gefährdungen in Verbindung stehen, ist auch eine Relation zwischen den ArchiMate-Elementen und Gefährdungen bzw. Maßnahmen gegeben. Voraussetzung hierfür ist, dass der Grundschutzkatalog des BSI im Modellierungswerkzeug zur Verfügung steht. Hat man Zugriff auf diese Objekte und Relationen, kann über diese Objekte iteriert werden. Durch die Verbindung von Maßnahmen und ArchiMate-Elementen kann eine Bewertung dieser Maßnahmen in den jeweiligen Objekten erfolgen. Es steht eine Tabelle pro ArchiMate-Element mit den jeweiligen Maßnahmen zur Verfügung, in der man Zeile für Zeile bewerten kann, ob die Maßnahmen erfüllt sind. Sind wenige Maßnahmen erfüllt, ist der Grundschutz-Score entsprechend gering. Er berechnet sich mit Anzahl erfüllter Maßnahmen geteilt durch Anzahl der Gesamtmaßnahmen. Nun soll, ähnlich wie beim Algorithmus für den Schutzbedarf, der Grundschutz-Score anhand einer Minimum-Funktion über den Baum traversieren. Sind also zwei Elemente miteinander verbunden mit unterschiedlichem Score, wird das Element mit dem höheren Wert ebenfalls entsprechend niedrig bewertet. Sollte z.B. ein Server alle Sicherheitsmaßnahmen erfüllen, die Applikationen, die auf diesem laufen jedoch nicht, ist der Server ebenfalls stark von Risikoeintritten betroffen und dementsprechend zu bewerten.

Zur grafischen Auswertung eignet sich eine Portfolio-Analyse, die auf der x-Achse die Eintrittswahrscheinlichkeit und auf der y-Achse die Auswirkung von Risiken angibt. Die Ausprägungen auf den jeweiligen beiden Achsen entsprechen idealerweise den Ausprägungen von den Attributen Verfügbarkeit, Vertraulichkeit und Integrität: 1 - Very Low, 2 - Low, 3 - Average, 4 - High, 5 - Very High. Hier wird ebenfalls wieder eine Maximum-Funktion verwendet, um zu entscheiden welcher Wert der drei Attribute Vertraulichkeit, Integrität und Verfügbarkeit für das Mapping verwendet wird. Ist also die Verfügbarkeit und Integrität sehr niedrig bewertet und die Vertraulichkeit jedoch hoch, ist das Mapping mit hoch einzustufen, da die Risikoauswirkung auf das Unternehmen hoch ist.
In diesem Fall ist ein Mapping auf die Werte der Impact-Achse in der Portfolio-Analyse einfach zu machen, da diese die gleichen Ausprägungen hat. Konkret betrifft das hier den Schutzbedarf. Für den Grundschutz ist lediglich ein Score gegeben. Hier ist das Mapping etwas schwieriger auf die Ausprägungen 1 - 5 vorzunehmen. Es empfiehlt sich das Heranziehen der Delphi-Methode. Mittels Expertenbefragung kann der Score, der zwischen 0 und 1 reicht, auf die Attributausprägungen 1 - Very Low, 2 - Low, 3 - Average, 4 - High und 5 - Very High gemapped werden. Für diese Arbeit gehen wir von der Annahme in Tabelle 3 aus.

Tabelle 3. Mapping Grundschutz-Score und Eintrittswahrscheinlichkeit

Grundschutz-Score	**Eintrittswahrscheinlichkeit**
>=0 AND <0.2	5 - Very High
>=0.2 AND <0.4	4 - High
>=0.4 AND <0.6	3 - Average
>=0.6 AND <0.8	2 - Low
>=0.8 AND <= 1	1 - Very Low

3.3 Develop

Für die Entwicklung der spezifizierten Modellierungsmethode, wird die Metamodellierungsplattform ADOxx [33] herangezogen. Sie kann sowohl für die Implementierung von Modellierungssprachen als auch für die Modellierungsprozedur sowie Mechanismen und Algorithmen verwendet werden.

> 'The Open Models (OMi) Laboratory is a dedicated research and experimentation space for the conceptualization, development, and deployment of modelling methods and the models designed with them. Both a physical and virtual place, it is equipped with tools to explore method creation and design, experiment with method engineering and deploy software tools for modelling.' [35]

Im ersten Teil steht die Erstellung der

– Klassenhierarchie,
– Klassen,
– Relationsklassen,
– grafische Notationen,
– und Syntax

im Vordergrund. Anschließend kann mit der Entwicklung von Algorithmen und Mechanismen fortgesetzt werden. Da es sich bei dem Security-Konzept um eine Erweiterung des ArchiMate-Metamodells handelt, müssen zuerst das Metamodell von ArchiMate 3.0 in der ADOxx-Plattform erstellt werden. Da auch Vererbung unterstützt wird, kann eine Superklasse erstellt werden, die alle sich wiederholenden Konzepte nach unten vererbt. So kann die zuvor erstellte Syntax in dieser Form abgebildet werden. Ähnlich der objektorientierten Programmierung besteht eine Klasse aus Attributen, die wiederum unterschiedliche Attributtypen zulassen. Jede Klasse hat Standardattribute, die enthalten sein müssen. Ein Beispiel ist das Attribut „GRAPHREP“, welches die grafische Notation einer Klasse enthält. Zudem können auch Attribute ergänzt werden, die für die Modellierungsmethode benötigt werden.
Ähnlich dem Klassenkonzept können auch Relationsklassen erstellt werden. Diese haben einen ähnlichen Aufbau, da sie ebenfalls aus Attributen bestehen. Relationsklassen enthalten auch grafische Repräsentationen, die bestimmen wie die Notation für die Modellierung auszusehen hat.
Nach der Erstellung der Klassen und Attribute kann mit der Implementierung der Notation fortgesetzt werden. Hierzu stellt ADOxx eine Domain-specific Language (DSL) zur Verfügung, die ermöglicht die Notation von Klassen und Beziehungen dynamisch auf Basis von Attributwerten zu steuern. Sie kann dazu verwendet werden die grafische Repräsentation in beliebiger Weise zu erstellen und zudem auch die Notation während der Laufzeit des Programms zu ändern. Abbildung 73 zeigt ein Beispiel.

Mechanismen und Algorithmen für die Modellierungslogik werden mit der Skriptsprache AdoScript geschrieben. Diese Programmiersprache wird im Standard von ADOxx mitgeliefert. AdoScript basiert auf dem sogenannten „Message-Core-Konzept“ [33]. So werden Nachrichten an verschieden Ports gesendet und erhalten wiederum Result-Messages. Daher ist AdoScript extern gekoppelt und führt über eine API Funktionsaufrufe aus.

Es werden in der Implementierung die Bereiche Schutzbedarf, Grundschutz und Likelihood-Impact abgedeckt. Wie im Abschnitt 3.2.3 beschrieben, kann der Schutzbedarf, nach erfolgter Bewertung der Datenobjekte, automatisch auf alle direkt und indirekt verbundenen Objekte erfolgen.

Anschließend kann der Grundschutz anhand des Grundschutzkatalogs des BSI bewertet werden.

Wie in Abb. 76 zu sehen, sind die Maßnahmen, welche dem Baustein unter „Assigned Building Blocks“ zugewiesen sind, in der Tabelle „Measures“ zu sehen. Die dort erfolgte Bewertung hat Auswirkungen auf den Grundschutz-Score. Wie im Abschnitt 3.2 beschrieben, kann resultierend auf dem Grundschutz-Score und den Attributen Confidentiality, Integrity und Availability eine Likelihood-

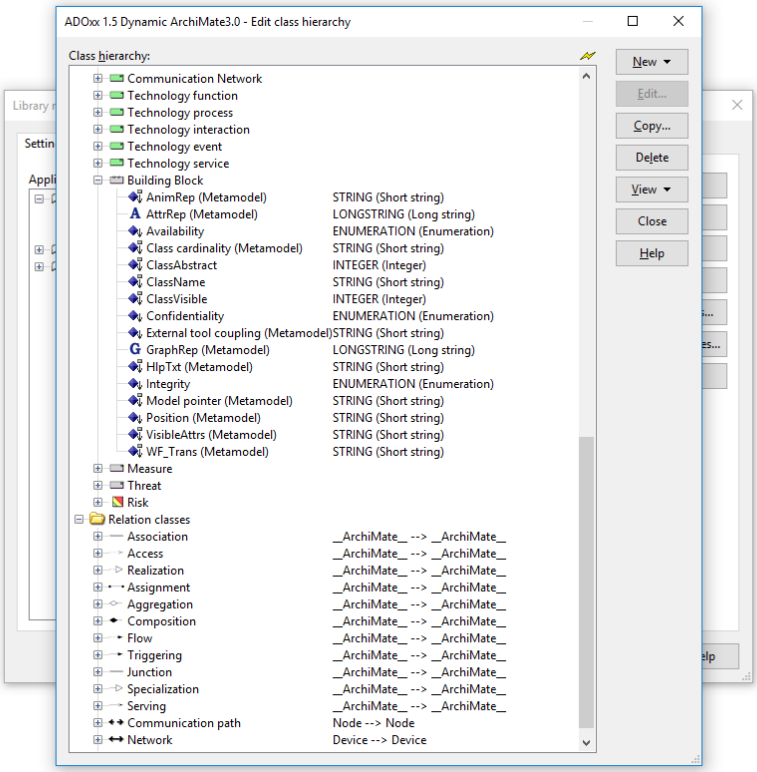

Abb. 72. Klassenhierarchie in ADOxx

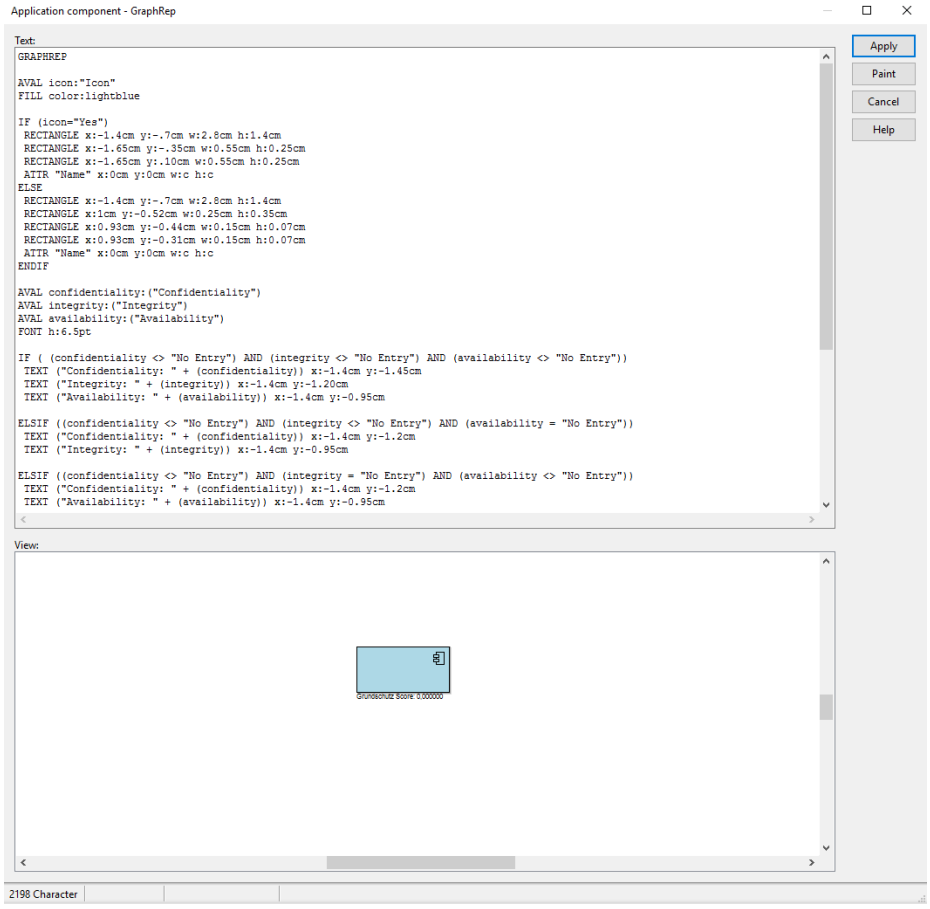

Abb. 73. Beispiel einer grafischen Repräsentation

```
    #Alle Objekte in einer Liste sortieren, sodass sie nach der richtigen Reihenfolge bewertet werden.
    PROCEDURE OBJ_FILLER
    {
        FOR currobjid in:(sReturnObjIds)
        {
            CC "Core" GET_CONNECTORS objid:(VAL (currobjid))
            CC "Core" GET_CLASS_ID objid:(VAL (token(objids,0)))
            CC "Core" GET_CLASS_NAME classid:(classid)

            FOR sconnectorId in:(objids)
            {
                CC "Core" GET_CONNECTOR_ENDPOINTS objid:(VAL(sconnectorId))

                SET iContains: (search(sReturnObjIds,STR(toobjid),0))

                IF (iContains = -1)
                {
                    SET sReturnObjIds: (sReturnObjIds + " " + STR(toobjid))
                }
                SET iContains: (search(sReturnObjIds,STR(fromobjid),0))
                IF (iContains = -1 AND classname = "Access")
                {
                    SET sReturnObjIds: (sReturnObjIds + " " + STR(fromobjid))
                }
            }
        }
        SET index:(tokcnt(sReturnObjIds))
        IF (index < counter)
        {
            OBJ_FILLER
        }
    }
}
```

Abb. 74. Beispiel einer AdoScript Procedure

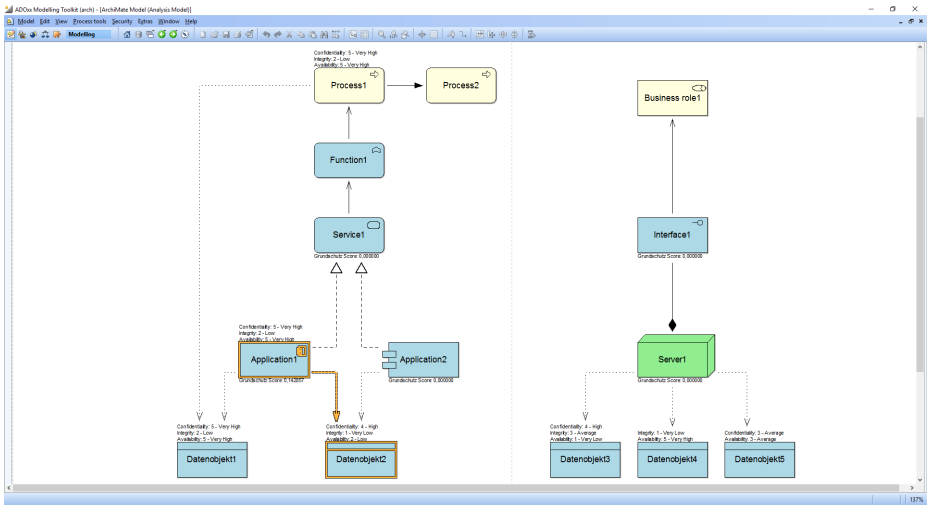

Abb. 75. Beispiel zur Bewertung des Schutzbedarfes

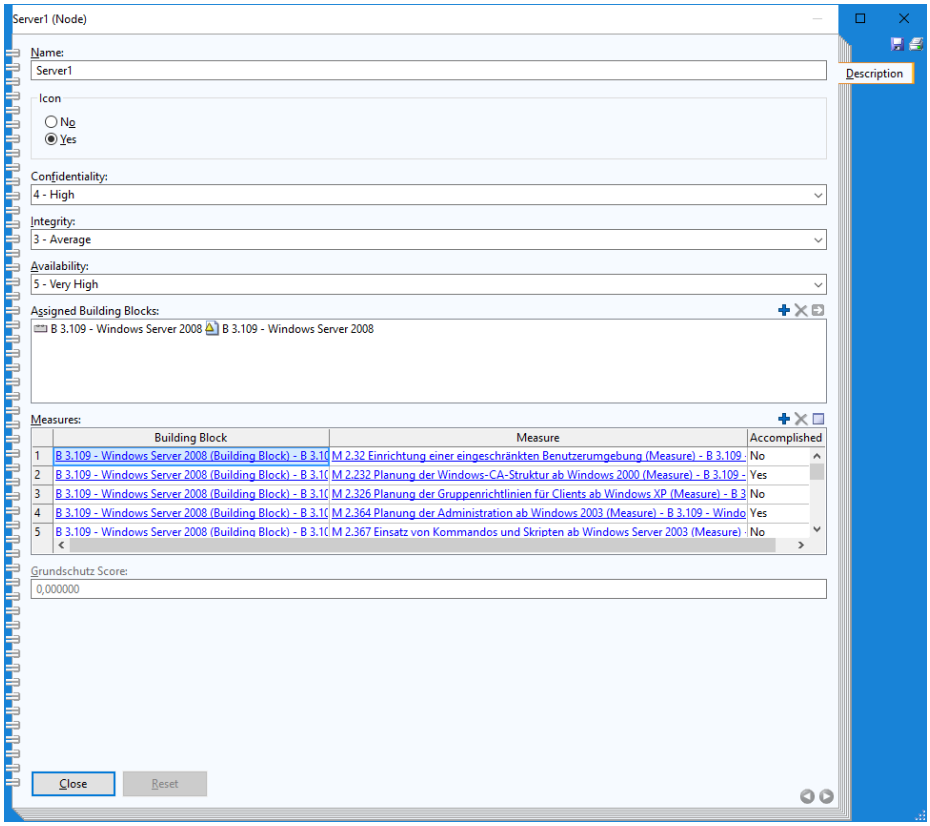

Abb. 76. Beispiel eines Notebooks mit zugewiesenem Grundschutz-Baustein

Impact-Analyse abgeleitet werden, da diese direkte Auswirkungen auf die Analyse, die Eintrittswahrscheinlichkeit und den Impact haben.

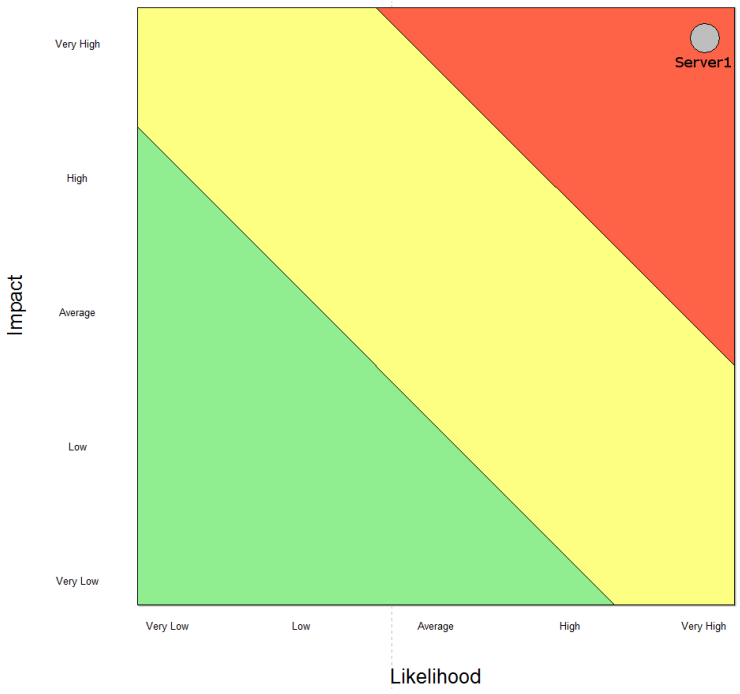

Abb. 77. Likelihood-Impact

3.4 Zusammenfassung des Konzepts

Zur Erstellung der Modellierungsmethode wurde der OMI Lifecycle [12] als Vorgehensmodell verwendet. Er besteht aus folgenden fünf Phasen:

- Create
- Design
- Formalize
- Develop
- Deploy/Validate

Während die Create-Phase dazu dient die Modellierungsmethode grob zu planen und die Idee auszuarbeiten, geht es in der Design-Phase bereits um die Konzeptualisierung des Metamodells, der Sprache, der Grammatik, der Notation und der Funktionalität. Für diese Phase wurde das Framework von „Metamodelling Platforms“ [13] verwendet. Das Ergebnis nach dieser Phase ist ein

fertiges Konzept, bestehend aus einem Metamodell mit 5 Klassen und 10 Attributen (siehe Tabelle 2). Zur Darstellung der spezifizierten Klassen dient eine Notation (siehe Abb. 68) und zur Abbildung der Syntax wurde ein Klassendiagramm erstellt (siehe Abb. 69). Anschließend beschreibt die Modellierungsprozedur in der Phase die einzelnen Schritte und Ergebnisse auf Basis des spezifizierten Metamodells und der Funktionalität. Das sind konkret die Erstellung von Architekturmodellen, Bewertung von Daten und anderen Architekturelementen anhand von CIA, Zuweisung der Bausteine des Grundschutzkatalogs und eine Auswertung mithilfe einer Likelihood-Impact-Analyse (siehe Abschnitt 3.2.2). Final ist in der Design-Phase die Implementierung von Mechanismen und Algorithmen relevant (siehe Abschnitt 3.2.3). Hierbei wurden die automatische Architekturelement-Bewertung auf Basis der bewerteten Daten, die korrekte Zuweisung der Maßnahmen des Grundschutzkatalogs mit den Architekturelementen und die Generierung der Likelihood-Impact-Analyse konzeptualisiert. Die anschließende Develop-Phase, in der es um die Entwicklung und Umsetzung der Design-Phase geht, wurde mit der ADOxx-Plattform [33] realisiert (siehe Abschnitt 3.3). Die Plattform bringt sämtliche Funktionalitäten mit, die benötigt werden, um eine Modellierungsmethode zu entwickeln. Für die Umsetzung wurden zuerst die Klassen und Attribute mithilfe der Klassenhierarchie-Funktionalität in ADOxx erstellt und anschließend die Relationen zwischen den Klassen (siehe Abb. 72). Für die Darstellung bzw. Notation der Klassen und Relationsklassen bedient sich ADOxx einer eigenen DSL (siehe. Abb. 73). Für die Umsetzung der in der Design-Phase spezifizierten „Mechanismen und Algorithmen“ wurde die Skriptsprache „AdoScript“ verwendet (siehe Abb. 74). Das Resultat nach der Develop-Phase ist die Umsetzung der konzipierten Modellierungsmethode. Die letzte Phase „Deploy/Validate“ behandelt das Deployment der umgesetzten Modellierungsmethode.

4 Case Study

In der folgenden Case Study dient das fiktive Unternehmen „CoolBox“ zur Illustration des Security-Konzepts. Das Unternehmen und die Idee entstanden im Rahmen einer Universitäts-Lehrveranstaltung. [17]
Das Produkt stellt einen intelligenten Behälter dar, der den Zustand verderblicher Lebensmittel über die gesamte Lieferkette überwacht und Informationen über den Zustand des Inhalts aufzeichnet. Hauptfokus sind die Sensoren, die sich im inneren der CoolBox-Container befinden und die zugrundeliegende Kommunikationsplattform.
So kann mittels der Sensoren der Zustand der Lebensmittel während des Transports jederzeit abgefragt werden. In der Version 1.0 der CoolBox werden folgende Daten ausgelesen:

- Daten zur Temperatur
- Daten zur Luftfeuchtigkeit
- Daten zu auftretenden Vibrationen und Erschütterungen

In der vorliegenden Case Study werden basierend auf der Unternehmensarchitektur, welche die Geschäfts, Informations- und System- und die Technologieebene detailliert beschreibt, eine Risiko- und Sicherheitsanalyse des Unternehmens vorgenommen.
Ein Beispiel im Zusammenhang eines Restaurants könnte so aussehen: Es werden Lebensmittel auf Vorrat bei einem Lieferanten bestellt, welche leicht verderblich sind und daher durchgehend bei -2 Grad Celsius gekühlt werden müssen. Der Spediteur verpackt die Lebensmittel in den CoolBox-Containern, welche unter anderem mit einem Temperatursensor versehen sind. Während die Lebensmittel transportiert werden, gewährleistet die CoolBox ein Monitoring über den Zustand ihrer Inhalts. Dabei werden folgende Daten überwacht:

- Daten zur Temperatur
- Daten zur Luftfeuchtigkeit
- Daten zu auftretenden Vibrationen und Erschütterungen

Die CoolBox ist mit einem kleinen internen Speicher ausgestattet auf welchem unter anderem Fakten wie Gewicht, Inhalt und Mindesthaltbarkeitsdatum gespeichert sind. Bei Unterbrechung der Kühlkette oder stärkerer Erschütterung, sodass die Möglichkeit einer Beschädigung besteht, werden diese Informationen an den Lieferanten übermittelt — Anschließend kann schnell eine Ersatzlieferung angefordert werden. Daher bekommt das Restaurant schneller die gewünschte Bestellung.

4.1 Das Technologische Konzept

Basis für diese Technologie sind miteinander verbundene Mikrocontroller in den Containern. In der Standardversion einer CoolBox sind Controller mit drei verschiedenen Sensoren (Temperatur, Feuchtigkeit, Erschütterungen) und einer SD-Karte für den internen Speicher ausgestattet. Das System ist modular erweiterbar. Daher können gegebenenfalls weitere Sensoren in die CoolBox eingebaut werden. Die intelligenten Behälter haben mit einer kleinen Li-Po Batterie einen Akku eingebaut, welcher die Steuerungselektronik mit Strom versorgt. Nach der Lieferung können die Boxen entweder komfortabel mittels Strominduktion oder per Kabel aufgeladen werden.
Die CoolBox-Controller senden und empfangen Daten über eine verschlüsselte Wi-Fi Verbindung. Für die permanente Überwachung der CoolBox-Container ist der CoolBox-Hub, welcher in Transportfahrzeugen eingebaut ist, über ein mobiles Datennetzwerk verbunden und soll als Schnittstelle zwischen den CoolBox-Servern und Boxen fungieren. Nach Erhalt der Lieferung kann der Kunde auch per Wi-Fi auf die Daten in den Containern mittels der CoolBox-App zugreifen. Die CoolBox-Server im Hintergrund tracken die gesamte Lieferung, empfangen Daten der Sensoren und reagieren unmittelbar bei Meldungen dieser Sensoren oder Überschreitungen der voreingestellten Grenzwerte.

4.2 Die Gesamtarchitektur

Für die Modellierung der Systemarchitektur wurden unterschiedliche Viewpoints in der Modellierungssprache ArchiMate erstellt, welche verschiedene Sichten auf die Architektur erlauben. Im folgenden Abschnitt wird der zuvor beschriebene Sachverhalt modelliert. Auf Basis dieser Architektur soll anschließend eine Risiko- und Sicherheitsanalyse vorgenommen werden.

4.2.1 Motivation View Im Motivation Viewpoint werden die Ziele und Anforderungen des Systems betrachtet. Im Fokus steht die ständige Online-Überwachung unserer Boxen. Während des Supply Chains soll der Informationsstatus des CoolBox-Inhalts aufgezeichnet werden. Bei Auffälligkeiten hinsichtlich der Werte reagiert der eingebaute Controller und entsprechende Maßnahmen werden in weiterer Folge ergriffen.

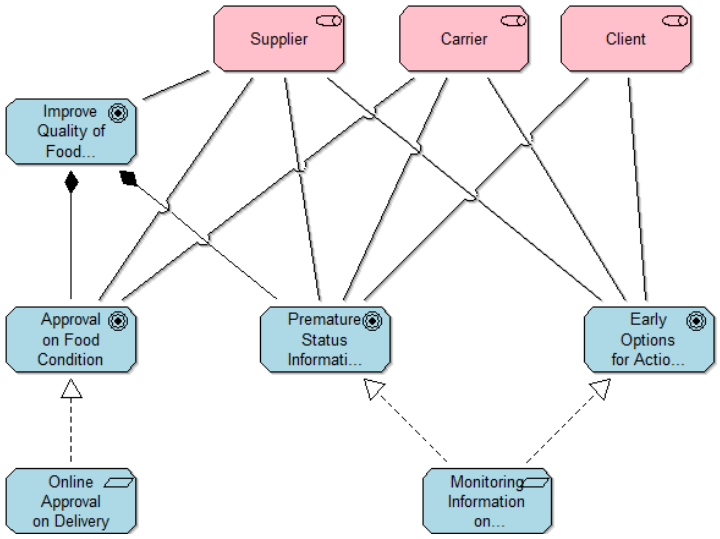

Abb. 78. Motivation View [17]

4.2.2 Product Configuration View Da jede Lieferung unterschiedliche Konfigurationsoptionen der CoolBox erfordert, sollen in dieser View produktspezifische Merkmale für die Einstellung der CoolBox erfasst werden. Die Werte sind frei konfigurierbar. Ähnliche Produkte sollen klassifiziert werden und dementsprechend den CoolBox-Containern zugeteilt werden.

4.2.3 Fleet Management View Nach erfolgter Lieferung kommt die CoolBox wieder zurück zum Lieferanten, der anschließend für die Überprüfung der

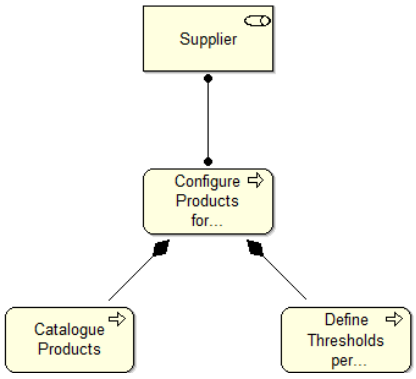

Abb. 79. Product Configuration View [17]

technischen Konditionen zuständig ist. Für diese Funktion ist die Komponente CoolBox App zuständig, die über eine Schnittstelle mit dem Server kommuniziert. Bei etwaigen Problemen mit der Kontrolleinheit (Sensoren, Wi-Fi Modul, ...) können die Einstellungen der CoolBox zurückgesetzt oder für eine Neukalibrierung und Wartung der Sensoren abgeholt werden.

4.2.4 Delivery View In der Delivery-View wird die gesamte Supply Chain inklusive Überwachung der CoolBox beschrieben. Im ersten Schritt wird der Kunde durch ein Service, welches die Komponente „Client ERP System“ zur Verfügung stellt, registriert. Anschließend wird die CoolBox vom Lieferanten mit den Lebensmitteln befüllt. Dieser Prozess beinhaltet auch die Registrierung der Boxen und die Aktivierung der Überwachungsfunktion. Dem Server werden die Tracking-Informationen jederzeit von der „CoolBox Controller Unit“ zur Verfügung gestellt. Dadurch haben die Stakeholder Zugriff auf die Informationen. Geht die CoolBox an den Lieferanten oder Kunden über, wird diese Information ebenfalls elektronisch an den Server übermittelt.

4.2.5 Infrastructure Usage View Der Kern in dieser View beschreibt die Kommunikation von Servern und Applikationsebene. Für die Kommunikation zwischen den Servern wird das ArchiMate-Element „Communication Path“ eingesetzt, das auf ein sicheres Nachrichtenprotokoll zurückgreifen kann. Die Kommunikation zwischen CoolBox-Applikation und Server erfolgt mittels Low-Power Wi-Fi inklusive Cryptochip, der einen sicheren Datenaustausch gewährleisten soll. Als Technologie für die Server wird das OS „Red Hat Enterprise Linux“ verwendet.

4.3 Risiko- und Sicherheitsanalyse

Das Internet und die Digitalisierung ermöglichen Unternehmen eigene Produkte zu gestalten und anzubieten. Die immer weiter voranschreitende Digitalisierung

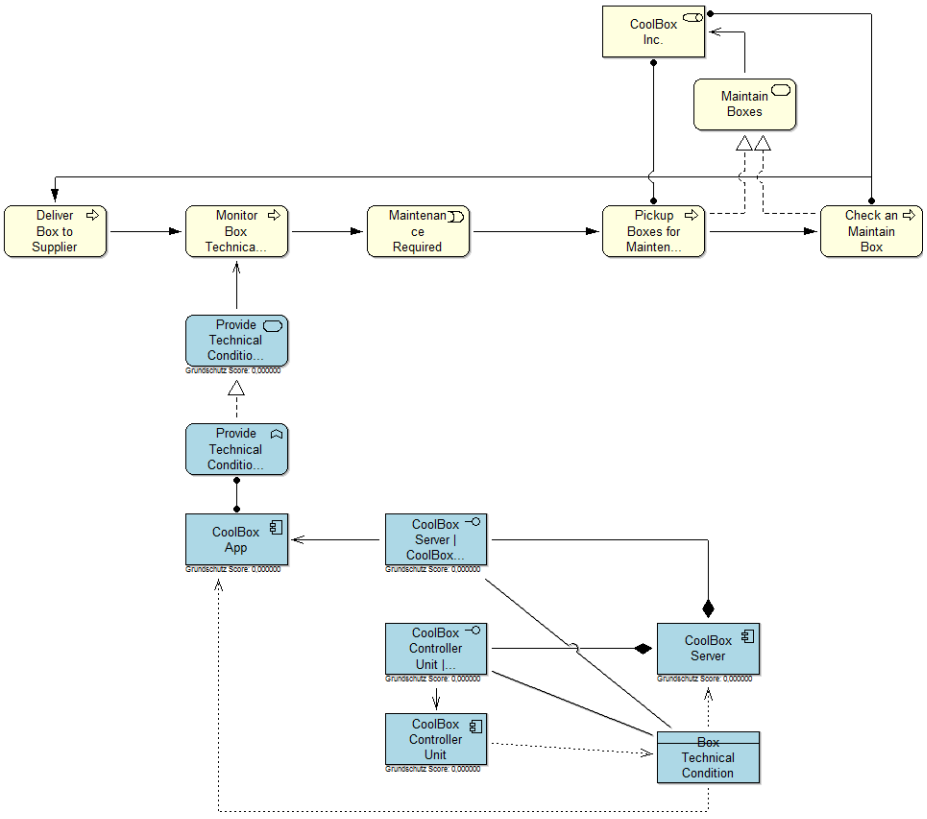

Abb. 80. Fleet Management View [17]

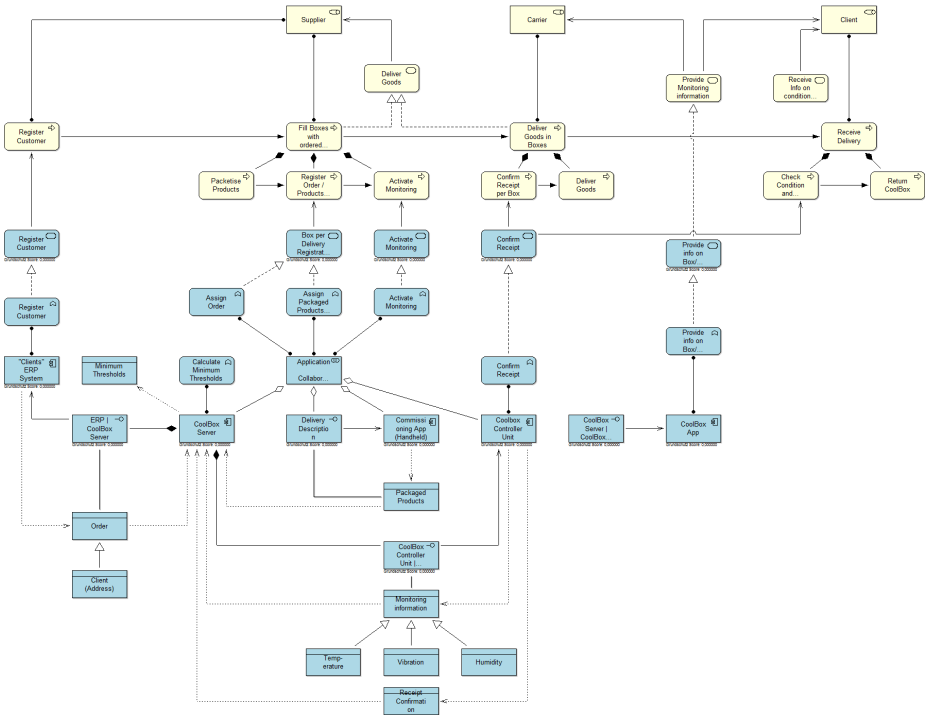

Abb. 81. Delivery View [17]

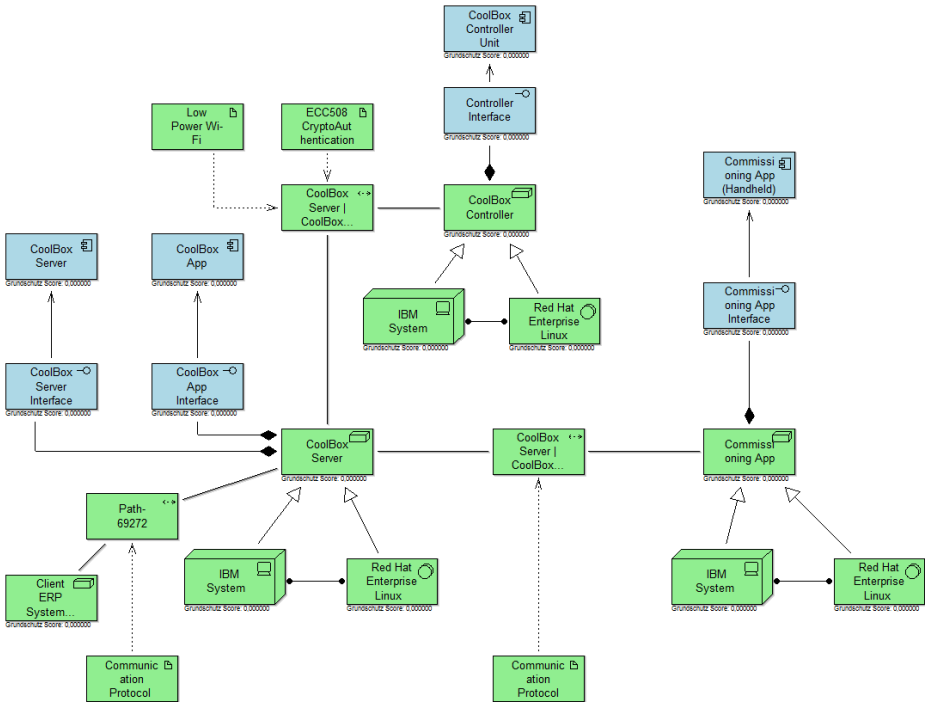

Abb. 82. Infrastructure Usage View [17]

sieht auch ein konkretes Bewusstsein für Risiken und Sicherheit vor, um potentielle Angriffe abwehren zu können. Speziell mit dem Internet of Things (IOT) werden aufgrund der großen Einsatzvielfalt große Anforderungen an die IT-Sicherheit gestellt. Insbesondere ist es wichtig für Unternehmen die IT-Landschaft der Organisation vor potentiellen Bedrohungen zu schützen, da sich die Schadenauswirkung durch den Wert an angebundenen Geräten erhöht. IT-Risiken lassen sich grundsätzlich in zwei primäre und zusätzliche sekundäre Kategorien einteilen, um die Möglichkeit zu bieten, die Typen der Gefahren zu beschreiben und daraus resultierend mögliche Gefährdungen ableiten zu können. Für die CoolBox werden die Kategorien Elektronische und Physische Angriffe sowie Höhere Gewalt und Personal herangezogen. Die Eintrittswahrscheinlichkeit und die Auswirkung je Angriff sind unterschiedlich für diese vier Kategorien, daher werden unterschiedlich spezifische Risikostrategien benötigt.

Elektronische Angriffe: Diese Art von Risiken sind unterschiedlich komplex, da die Vielzahl der unterschiedlichen Angriffe stark variiert. Hier wird ein gutes Verständnis der Bedrohungen durch elektronische Angriffe benötigt. Die Ziele dieser Angriffe unterscheiden sich ebenfalls stark. Beispiele für solche Angriffe sind: Denial of Service, Viren, Spam, Phishing, etc.

Physische Angriffe: Physische Angriffe setzen eine physische Anwesenheit voraus. So verschaffen sich Personen körperlich Zugang zu Systemen, um sie zu manipulieren, zu stehlen oder zu zerstören. Solche Angriffe sind zum Beispiel Einbruch, Beschädigung, Diebstahl etc.

Höhere Gewalt: Diese Art von Angriffen sind zum Beispiel Erdbeben, Hochwasser und Blitzschlag. Diese Risiken stehen nicht unmittelbar mit Personen in Verbindung und sind finanziell höher einzustufen in der Risikominimierung. Beispiel: Die Absicherung eines Gebäudes gegen Erdbeben.

Personal: Die Kategorie bezieht sich auf das interne und externe Personal. Eine Gefahrenquelle ist zum Beispiel die unzureichende Einschulung von Mitarbeitern, fehlende Sicherheitsrichtlinien und fehlende Sicherheitskontrollen. Ein Beispiel ist der leichtfertige Umgang mit Kennwörtern.

Die CoolBox Inc. wird als kleines und mittleres Unternehmen eingestuft. Dies hat nicht zuletzt Auswirkungen auf die gewählte Risikostrategie. Das ist vor allem auf die personellen Ressourcen zurückzuführen und weniger auf die eingesetzte IT-Infrastruktur, da speziell dieses Unternehmen stark auf moderne Technologien und IT-Services setzt, um Prozesse effizienter zu gestalten. Es wird auf eine eigene Serverlandschaft gesetzt mit der Verwendung großer Datenbanken. Weiters entsprechen die verwendeten Technologien stark jenen, die ebenfalls in großen Unternehmen verwendet werden. Daher ist auch hier ein großes Risiko- und Sicherheitsbewusstsein essentiell. IT-Abteilungen mit fundiertem Fachwissen sind in KMU's oftmals nicht anzutreffen. Auch die

geringe Bereitschaft des Managements die IT-Abteilung mit Geld zu versorgen, führen nicht selten dazu, dass IT-Sicherheitsstrategie nur aus der Durchführung von monatlichen Backups auf Festplatten besteht. [3] Große Sicherheitslücken und fehlendes Risikobewusstsein in vielen KMU's führten zu vielen Studien (siehe u.a. [3], [34] und [38]) in Europa. Frameworks und Vorgehensmodelle sollen diesem Trend entgegenwirken und KMU's helfen geeignete Sicherheits- und Risikomodelle aufzubauen und generell das Risikobewusstsein zu steigern.
Um eine Sicherheitsstrategie zu entwickeln ist fundiertes Wissen über die IT-Landschaft essentiell. Daher ist die zuvor modellierte Systemarchitektur wichtig für das Verständnis der IT-Sicherheit und bildet daher die Grundlage für die Erstellung der Sicherheitsstrategie. Details zur Systemarchitektur befinden sich im Abschnitt 4.2. Die Gesamtarchitektur, welche den Business, Application und Technology Layer abdeckt, wird auf mögliche Gefährdungen und Verwundbarkeiten analysiert. Initial wird eine Checkliste der existierenden Bedrohungen sowie eine Checkliste möglicher Verwundbarkeiten des Systems erstellt. Sobald eine Bedrohung ein möglich verwundbares Element ausnutzt, entsteht ein Schaden — Dies entspricht einem Risiko. Die Bedrohungs- und Verwundbarkeitsanalyse entspricht einer qualitativen Risikoanalyse und ist eine Vorbereitung für die sogenannte quantitative Risikoanalyse. Die Bedrohungsprofile und Verwundbarkeiten werden in weiterer Folge strukturiert, gegenübergestellt und bewertet. Daraus folgt ein Ergebnis, welches sämtliche Risiken und deren Risikopotential, bestehend aus Schadenshöhe und Eintrittswahrscheinlichkeit, auflistet. Nachdem die Systemanalyse auf mögliche Risiken abgeschlossen und die Aufstellung und Bewertung der IT-Risiken erfolgt ist, folgt schließlich die Entwicklung einer langfristigen IT-Sicherheitsstrategie. Ausgehend vom Risikopotential werden Maßnahmen bestimmt, die den Risiken entgegenwirken sollen. Dazu gehören insbesondere Schutzmechanismen, die langfristig Risiken vorbeugen bzw. minimieren sollen und nicht nur zum gegebenen Zeitpunkt eine Verwundbarkeit reduzieren. Bei der Risikobewältigung werden folgende Maßnahmen unterschieden: Risikovermeidung, Risikoverminderung, Risikoübertragung, Risikoübernahme. Als strategisch wichtig wird die Systemüberwachung angesehen. Eine ständige Systemüberwachung und kontinuierliche und tiefgehende Behandlung der Risikopotenziale (z.B. Risiko steigt durch Einsatz neuer Cloud-Lösungen) sind ausschlaggebend für den Erfolg.

4.4 Erstellung der Sicherheitsstrategie

Im IT-Bereich gibt es viele Frameworks, die Vorgehensweisen zum Erstellen einer Sicherheitsstrategie bereitstellen. In den meisten Fällen erfordert die Entwicklung einer Sicherheitsstrategie viel Know-how und Zeit und stellt eine aufwändige Prozedur dar. Für KMU's sind laut des Risk Management Teams von ENISA (European Network and Information Security Agency) folgende Risikomethoden geeignet [9]:

- OCTAVE-S von CERT/CC

- Österreichisches Informationssicherheitshandbuch vom Bundeskanzleramt
- IT-Grundschutz vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Mehari von CLUSIF

In dieser Arbeit wird die Sicherheitsstrategie anhand der OCTAVE-Methode (Operationally Critical Threat, Asset, and Vulnerability Evaluation) durchgeführt. Für die Analyse werden noch Empfehlungen aus dem Informationssicherheitshandbuch [30] und aus den IT-Grundschutzkatalogen des BSI [34] entnommen. Die OCTAVE Methode [37] [1] wurde an der Carnegie Mellon University und dem CERT/CC entwickelt. Im Fokus ist eine wertbezogene Analyse der Risiken und Sicherheitsprozesse im Unternehmen. Das erste Framework, welches Methoden, Tools und Techniken zur Erstellung einer IT-Sicherheitsstrategie enthält, wurde für große Unternehmen entwickelt. OCTAVE-S ist etwas kompakter gestaltet und speziell für kleinere und mittlere Unternehmen angepasst. Das Vorgehen kann grundsätzlich von wenigen Personen durchgeführt werden. Die Vorgangsweise umfasst in der Vorbereitung drei zentrale Phasen [36]:

- Phase 1: Ermittlung von Bedrohungsprofilen für Werte, die an Informationsverarbeitung und IT festzumachen sind.
- Phase 2: Identifizierung von Schwachstellen in der IT-Infrastruktur.
- Phase 3: Erstellung der Sicherheitsstrategie und deren Umsetzung.

Die wichtigsten Merkmale im Überblick [17]:

- Alle Verantwortlichen sind in den Prozess zu involvieren.
- Maßnahmenkataloge, welche auch von KMU's zur Maßnahmenbewertung herangezogen werden.
- Identifizierung und Bewertung von Vermögensgegenständen.
- Überprüfung der bereits vorliegenden Sicherheitsmaßnahmen und Analyse von potentiellen Schwachstellen.
- Bestimmung von Schutzmaßnahmen und Priorisierung.

In einem ersten Schritt werden sämtliche Vermögenswerte identifiziert. Werte können die IT-Infrastruktur, Datenbanken, Anwendungen oder Mitarbeiter sein. Diesen Vermögenswerten werden Bedrohungsprofile zugeordnet und daraus resultierend kritische Werte identifiziert.
Bei der Zuordnung der Bedrohungsprofile ergeben sich einige Fragestellungen: Was passiert bei Zerstörung, Verlust, geringer Verfügbarkeit und Modifikation ohne Berechtigung von Vermögenswerten durch nicht berechtigte Personen?

Die eingesetzten Vermögenswerte wurden aus der modellierten Gesamtarchitektur (siehe Abschnitt 4.2) entnommen. Die Datenobjekte (siehe Abschnitt 4.4.1) werden nach den Kriterien Vertraulichkeit, Integrität und Verfügbarkeit bewertet. Es wurde ebenfalls eine Bewertung der Elemente vorgenommen, die direkten bzw. indirekten Zugriff auf die Datenobjekte haben. So werden Elemente (Anwendungen, Server, ...), die diese Daten erstellen, aktualisieren, lesen oder löschen ebenfalls bewertet.

4.4.1 Datenobjekte

4.4.1.1 Kundendaten Kundendaten müssen streng geschützt werden. Für den laufenden Betrieb können Kundendaten vernachlässigt werden. Daher werden sie nicht von der CoolBox direkt gespeichert.

- Vertraulichkeit: sehr hoch
- Integrität: sehr hoch
- Verfügbarkeit: mittel

4.4.1.2 Produktkonfiguration Die Produktkonfiguration wird direkt auf den Servern gespeichert. Supplier verwalten eine Liste Ihrer Produkte und die dazugehörigen Grenzwerte (Thresholds). Diese werden im laufenden Betrieb benötigt, damit auf die korrekten Grenzwerte für die Lebensmittel per Box zugegriffen werden kann.

- Vertraulichkeit: hoch
- Integrität: sehr hoch
- Verfügbarkeit: hoch

4.4.1.3 Daten der CoolBox Control Units (Grenzwerte der Produkte, Tracking Daten der Sensoren, Technischer Zustand) Die CoolBox verwaltet Daten zu Messwerten und technische Daten. Aus Sicherheitsgründen werden keine Produkt- oder Kundendaten innerhalb der CoolBox verwendet. Die Daten liegen rein über technische Kunden- und Produkt-ID's vor.

- Vertraulichkeit: mittel
- Integrität: hoch
- Verfügbarkeit: hoch

4.4.1.4 Order Das Datenobjekt "Order" enthält Kundendaten. Der Handheld, zur Konfiguration einer Box, wird die technische Order-ID übermittelt, die anschließend dort verarbeitet wird. Die ID wird für die initiale Aktivierung der CoolBox und vor allem für das Monitoring einzelner Boxen verwendet.

- Vertraulichkeit: sehr hoch
- Integrität: sehr hoch
- Verfügbarkeit: hoch

Die Bestellungen werden am Server verwaltet. Daher ist der Schutzbedarf auf Server und CoolBox-Anwendungen zu übertragen.

4.4.1.5 Packaged Products Hier werden ebenfalls nur ID's verwendet. Die Produktdaten selbst werden auf den CoolBox-Servern verwaltet. Die Zuordnung von Produkten zu einer Box ist maßgeblich für die Berechnung der Thresholds auf dem CoolBox-Server.

- Vertraulichkeit: gering
- Integrität:mittel
- Verfügbarkeit: gering

4.4.2 Nodes (Infrastrukturbausteine)

4.4.2.1 CoolBox Server Auf dem Server werden unter anderem Kunden- und Produktdaten gespeichert. Daher werden mögliche Gefährdungen nun im Detail analysiert. Für den Grundschutz eines Servers werden folgende typische Gefährdungen gemäß IT-Grundschutzkatalog des BSI [34] angenommen:
Vererbter Schutzbedarf auf Basis der Datenobjekte:

- Vertraulichkeit: sehr hoch
- Integrität: sehr hoch
- Verfügbarkeit: hoch

Höhere Gewalt

- G 1.1 Personalausfall
- G 1.2 Ausfall von IT-Systemen

Organisatorische Mängel

- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.36 Ungeeignete Einschränkung der Benutzerumgebung

Menschliche Fehlhandlungen

- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von Sicherheitsmaßnahmen
- G 3.5 Unbeabsichtigte Leitungsbeschädigung
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung von IT-Systemen
- G 3.9 Fehlerhafte Administration von IT-Systemen

Technisches Versagen

- G 4.1 Ausfall der Stromversorgung
- G 4.6 Spannungsschwankungen/Überspannung/Unterspannung
- G 4.7 Defekte Datenträger
- G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
- G 4.13 Verlust gespeicherter Daten
- G 4.20 Überlastung von Informationssystemen
- G 4.22 Software-Schwachstellen oder -Fehler
- G 4.39 Software-Konzeptionsfehler

Vorsätzliche Handlungen

- G 5.1 Manipulation oder Zerstörung von Geräten oder Zubehör
- G 5.2 Manipulation an Informationen oder Software
- G 5.7 Abhören von Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.18 Systematisches Ausprobieren von Passwörtern

4.4.2.2 CoolBox Control Unit (Box) Hier liegen keine kritischen Daten vor. Liegt ein Ausfall bei einer CoolBox vor, ist lediglich ein Use Case unterbrochen. Solche Störungen werden mittels Service Level Agreements mit dem Kunden vereinbart. Daher ist keine detailliertere Bedrohungsanalyse nötig.

4.4.2.3 Handheld Bei Ausfall ist lediglich ein Use Case unterbrochen. Der Handheld ist speziell für die Kommissionierung zuständig. Bei einem Ausfall ist es sinnvoll ein Ersatzgerät zu verwenden. Weiters liegen hier keine kritischen Daten vor und es werden auch keine solche an den Server gesendet. Daher ist keine detailliertere Bedrohungsanalyse nötig.

4.4.3 Anwendungskomponenten

4.4.3.1 CoolBox Application Die Applikation läuft direkt auf dem Server und stellt das Kernstück in der Architektur dar. Für den Grundschutz werden folgende typische Gefährdungen für Webanwendungen auf Basis des Grundschutzkataloges des BSI [34] als üblich betrachtet:
Vererbter Schutzbedarf auf Basis der Server:

- Vertraulichkeit: sehr hoch
- Integrität: sehr hoch
- Verfügbarkeit: hoch

Organisatorische Mängel

- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.4 Unzureichende Kontrolle der Sicherheitsmaßnahmen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.22 Fehlende oder unzureichende Auswertung von Protokolldaten
- G 2.27 Fehlende oder unzureichende Dokumentation
- G 2.67 Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten
- G 2.87 Verwendung unsicherer Protokolle in öffentlichen Netzen
- G 2.103 Unzureichende Schulung der Mitarbeiter
- G 2.157 Mangelhafte Auswahl oder Konzeption von Webanwendungen
- G 2.158 Mängel bei der Entwicklung und der Erweiterung von Webanwendungen und Web-Services
- G 2.159 Unzureichender Schutz personenbezogener Daten bei Webanwendungen und Web-Services

Menschliche Fehlhandlungen

- G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten
- G 3.38 Konfigurations- und Bedienungsfehler
- G 3.43 Ungeeigneter Umgang mit Passwörtern

Technisches Versagen

- G 4.22 Software-Schwachstellen oder -Fehler

- G 4.33 Schlechte oder fehlende Authentifizierung
- G 4.35 Unsichere kryptographische Algorithmen
- G 4.84 Unzureichende Validierung von Ein- und Ausgabedaten bei Webanwendungen und Web-Services
- G 4.85 Fehlende oder mangelhafte Fehlerbehandlung durch Webanwendungen und Web-Services
- G 4.86 Unzureichende Nachvollziehbarkeit von sicherheitsrelevanten Ereignissen bei Webanwendungen
- G 4.87 Offenlegung vertraulicher Informationen bei Webanwendungen und Web-Services

Vorsätzliche Handlungen

- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.19 Missbrauch von Benutzerrechten
- G 5.20 Missbrauch von Administratorrechten
- G 5.28 Verhinderung von Diensten
- G 5.87 Web-Spoofing
- G 5.88 Missbrauch aktiver Inhalte
- G 5.131 SQL-Injection
- G 5.165 Unberechtigter Zugriff auf oder Manipulation von Daten bei Webanwendungen und Web-Services
- G 5.166 Missbrauch einer Webanwendung durch automatisierte Nutzung
- G 5.167 Fehler in der Logik von Webanwendungen und Web-Services
- G 5.168 Umgehung clientseitig umgesetzter Sicherheitsfunktionen von Webanwendungen und Web-Services
- G 5.169 Unzureichendes Session-Management von Webanwendungen und Web-Services
- G 5.170 Cross-Site Scripting (XSS)
- G 5.171 Cross-Site Request Forgery (CSRF, XSRF, Session Riding)
- G 5.172 Umgehung der Autorisierung bei Webanwendungen und Web-Services
- G 5.173 Einbindung von fremden Daten und Schadcode bei Webanwendungen und Web-Services
- G 5.174 Injection-Angriffe
- G 5.175 Clickjacking

4.4.3.2 Commissioning Application Diese Applikation verwendet keine sensiblen Daten. Daher wird auf eine detaillierte Bedrohungsanalyse verzichtet.

4.4.3.3 CoolBox-Controller-Unit Diese Applikation verwendet keine sensiblen Daten. Daher wird auf eine detaillierte Bedrohungsanalyse verzichtet.

4.4.4 Maßnahmen

4.4.4.1 CoolBox Application Für die CoolBox-Application sind folgende Maßnahmen für Webanwendungen des IT-Grundschutzkataloges zur Absicherung von Gefährdungen empfehlenswert [34]:

Tabelle 4. Maßnahmenbewertung für die CoolBox Application

Maßnahme	**Erfüllt**
M 2.1 (A) Festlegung von Verantwortlichkeiten und Regelungen	ja
M 2.11 (A) Regelung des Passwortgebrauchs	ja
M 2.63 (A) Einrichten der Zugriffsrechte	nein
M 2.363 (B) Schutz gegen SQL-Injection	ja
M 2.488 (W) Web-Tracking	nein
M 4.176 (B) Auswahl einer Authentifizierungsmethode für Webangebote	ja
M 5.168 (A) Sichere Anbindung von Hintergrundsystemen an Webanwendungen und Web-Services	ja
M 4.392 (A) Authentisierung bei Webanwendungen	nein
M 4.394 (A) Session-Management bei Webanwendungen und Web-Services	nein
M 4.395 (B) Fehlerbehandlung durch Webanwendungen und Web-Services	ja
M 4.396 (B) Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen	nein
M 4.398 (B) Sichere Konfiguration von Webanwendungen	ja
M 4.399 (A) Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen	nein
M 4.400 (B) Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services	ja
M 4.401 (B) Schutz vertraulicher Daten bei Webanwendungen	ja
M 4.402 (A) Zugriffskontrolle bei Webanwendungen	nein
M 2.8 (A) Vergabe von Zugriffsrechten	nein
M 2.31 (A) Dokumentation der zugelassenen Benutzer und Rechteprofile	nein
M 2.34 (A) Dokumentation der Veränderungen an einem bestehenden System	ja
M 2.64 (A) Kontrolle der Protokolldateien	nein
M 2.110 (A) Datenschutzaspekte bei der Protokollierung	ja
M 2.273 (A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	ja
M 4.78 (A) Sorgfältige Durchführung von Konfigurationsänderungen	nein

4.4.4.2 CoolBox Server (PaaS) Für die Verwendung von Platform as a Service für den Betrieb eines Servers werden Maßnahmen nach Tabelle 5 angenommen. Die hier verwendeten Maßnahmen stützen sich alle auf die Empfehlung des

Tabelle 5. Maßnahmenbewertung für den CoolBox Server (PaaS)

Maßnahmen	**Erfüllt**
M 2.250 Festlegung einer Outsourcing-Strategie,	ja
M 2.252 Wahl eines geeigneten Outsourcing-Dienstleisters,	ja
M 2.253 Vertragsgestaltung mit dem Outsourcing-Dienstleister,	ja
M 2.254 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben) und	ja
M 6.83 Notfallvorsorge beim Outsourcing	ja

Grundschutzkataloges des BSI [34].
Zur näheren Betrachtung wird die CoolBox Application herangezogen, da Sie vererbend die Risiken vom CoolBox Server und dieser wiederum von den Datenobjekten übernimmt. Die Applikation hat folgenden Schutzbedarf:
Vererbter Schutzbedarf auf Basis der Datenobjekte:

- Vertraulichkeit: sehr hoch
- Integrität: sehr hoch
- Verfügbarkeit: hoch

Der Grundschutz-Score beträgt **0,52**, da 12 der 23 vorgegebenen Maßnahmen erfüllt sind.
Dadurch ergibt sich eine Likelihood-Impact-Analyse wie in Abb. 83 zu sehen.

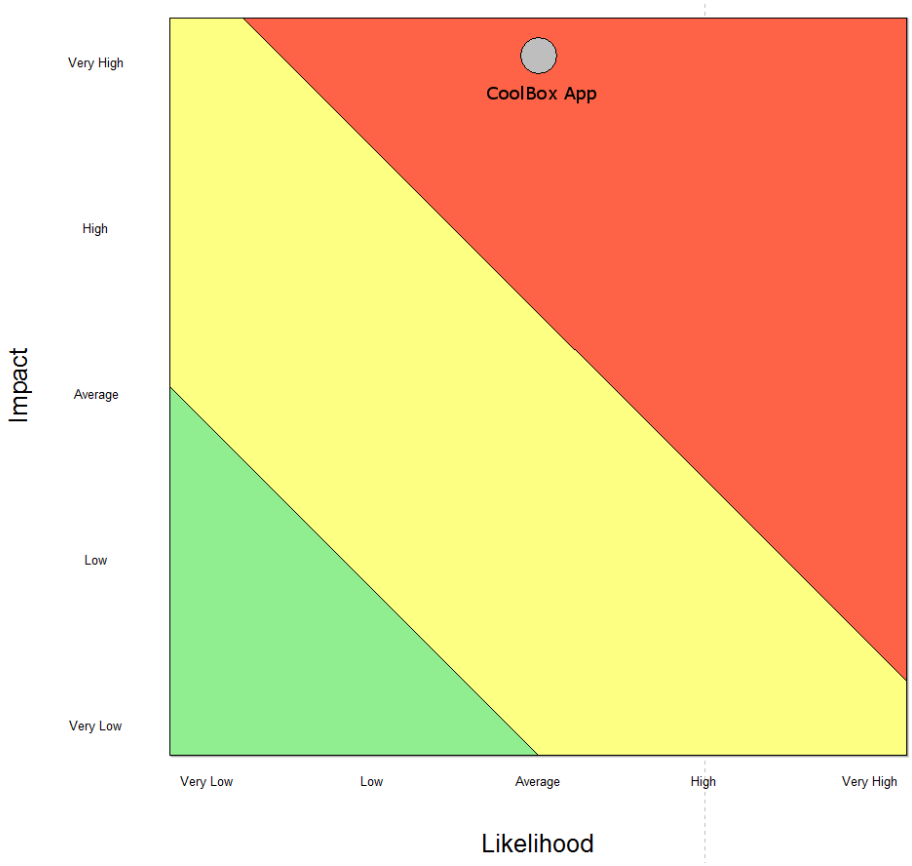

Abb. 83. Likelihood-Impact-Analyse für die CoolBox Application

5 Conclusio

In dieser Arbeit wurden Security-Konzepte von Standards wie TOGAF, ITIL, SABSA, ISO 27000 evaluiert. Vor allem die Tauglichkeit Sicherheitsmanagement für kleinere und mittlere Unternehmen aufzubauen, wurde bei der Evaluierung berücksichtigt. Aufgrund der schwierigen Verwendbarkeit solcher Frameworks, speziell für kleinere Unternehmen, beschreibt der Hauptteil dieser Arbeit ein Framework zur Konzeptualisierung und Implementierung eines Security Layers in der Modellierungssprache ArchiMate. Es eignet sich aufgrund der Einfachheit besonders für KMU's. Im Kern besteht dieses Framework aus einem Vorgehensmodell inklusive Modellierungssprache und Funktionen. Zur Validierung dieses Frameworks wurde das fiktive Unternehmen CoolBox Inc. herangezogen. Hier konnte zunächst mittels der Modellierungssprache ArchiMate die gesamte Unternehmensarchitektur aufgebaut werden. Anschließend erfolgte die Bewertung des Schutzbedarfs und Grundschutzes der Vermögenswerte. Im Fokus steht die einfache Bedienbarkeit sowie Effizienz. Daher wurden der Grundschutzkatalog des BSI und das CIA-Konzept (Vertraulichkeit, Verfügbarkeit und Integrität) verwendet. Die Umsetzung des in dieser Arbeit vorgestellten Konzepts erfolgte mit der ADOxx-Plattform. Generell ist die Erstellung einer Unternehmensarchitektur mit genügend Know-how verbunden. Selbiges gilt für die Bewertung der Datenobjekte zur Abdeckung des Schutzbedarfes. Hierbei wird es in den meisten Fällen notwendig sein, Informationen über die Vertraulichkeit, Verfügbarkeit und Integrität solcher Daten ausfindig zu machen. Der Rest des Frameworks, wie die Bewertung des Grundschutzes und Auswertung der Ergebnisse, kann mittels automatisierter Algorithmen erfolgen. Das Konzept schafft es eine Sprache, wie ArchiMate, mit Sicherheitskonzepten wie dem Grundschutzkatalog des BSI und dem CIA-Konzept, welches ebenfalls im ISO Standard 27000 bzw. ITIL verwendet wird, auszustatten.

Literatur

1. Alberts, C.e.a.: Introduction to the OCTAVE Approach. Software Engineering Institute (2003)
2. Band, I., et al.: Modeling Enterprise Risk Management and Security with the ArchiMate® Language. The Open Group, U.S (2015)
3. Büllingen, F., Hillebrand, A.: IT-Sicherheitsniveau in kleinen und mittleren Unternehmen. Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie. Paderborn (2012)
4. Burkett, J.S.: Business security architecture: Weaving information security into your organization's enterprise architecture through sabsa. Information Security Journal: A Global Perspective 21, 47–54 (2012)
5. Coetzee, M.: Enterprise information security, a review of architectures and frameworks from interoperability perspective. Availability, Reliability and Security (ARES) pp. 155–160 (2012)
6. Deutsches Institut für Normung: ISO/IEC 27000. DIN, 10787 Berlin (2007)
7. Deutsches Institut für Normung: ISO/IEC 27001. DIN, 10787 Berlin (2007)
8. Deutsches Institut für Normung: ISO/IEC 27002. DIN, 10787 Berlin (2007)
9. European Network and Information Security Agency: Risk Management - Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools (2006)
10. Fill, H.G., Karagiannis, D.: On the conceptualisation of modelling methods using the adoxx meta modelling platform. Enterprise Modelling and Information Systems Architectures - An International Journal 8, 5–10 (2013)
11. ISO: ISO 31000:2009: Risk Management – Principles and Guidelines. ISO (2009)
12. Karagiannis, D.: Agile modeling method engineering. Proceedings of the 19th Panhellenic Conference on Informatics pp. 5–10 (2015)
13. Karagiannis, D., Kühn, H.: Metamodelling platforms. 3rd International Conference EC-Web 2002 – Dexa 2002 Bauknecht K., Min Tjoa A., Quirchmayr G. (eds.) p. 182 (2002)
14. Karagiannis, D., Mayr, H., Mylopoulos, J.: Domain-Specific Conceptual Modeling. Springer International Publishing, Schweiz (2016)
15. Maketas, D., Zisopoulos, I.: Integration of TOGAF and SABSA on the Increased Effectiveness and Security of a Software Development Life Cycle, in the Context of a Spinoff Company. The Open Group (2013)
16. Mayer, N., Dubois, E., Matulevicius, R., Heymans, P.: Conceptual integration of enterprise architecture management and security risk management. Conference Paper (2013)
17. Moser, C., Stückler, K., Puhr, C., Timotic, M., Oppermann, M.: CoolBox Secure E-Commerce - Intelligente Kühlkette (2016)
18. Närman, P.e.a.: Using enterprise architecture models for system quality analysis. Enterprise Distributed Object Computing Conference, 2008. EDOC '08. 12th International IEEE (2008)
19. Oda, S., Fu, H., Zhu, Y.: Enterprise information security architecture a review of frameworks, methodology, and case studies. Computer Science and Information Technology, 2009. ICCSIT 2009 pp. 333–337 (2009)
20. Office of Government Commerce: Service Design. TSO, UK (2007)
21. Office of Government Commerce: ITIL The Official Introduction to the ITIL Service Lifecycle. TSO, U.K. (2007/08)

22. Shariati, M., Bahmani, F., Shams, F.: Enterprise information security, a review of architectures and frameworks from interoperability perspective. Procedia Computer Science 3, 537–543 (2011)
23. Sherwood, J., Clark, A., Lynas, D.: SABSA: Enterprise Security Architecture (White Paper). The Open Group, U.S (2009)
24. The Committee of Sponsoring Organization: Unternehmensweites Risikomanagement - Übergreifendes Rahmenwerk - Zusammenfassung. The Committee of Sponsoring Organization, Frankfurt/Main (2004)
25. The Open Group: TOGAF ® Version 9.1. The Open Group, U.S (2011)
26. The Open Group: TOGAF and SABSA Integration: How SABSA and TOGAF complement each other to create better architectures (White Paper). The Open Group, U.S (2011)
27. The Open Group: Risk Taxonomy (O-RT). The Open Group, U.K. (2013)
28. The Open Group: ArchiMate® 3.0 Specification. The Open Group, U.K. (2016)
29. The Open Group: Integrating Risk and Security within a TOGAF Enterprise Architecture. The Open Group, U.S (2016)
30. Wirtschaftskammer Österreich: IT Sicherheitshandbuch für kleine und mittlere Unternehmen (2016)
31. Zachman, J.: Enterprise architecture: The issue of the century. issue of Database Programming and Design magazine (1997)
32. Zivkovic, S., Kühn, H., Karagiannis, D.: Facilitate modelling using method integration: An approach using mappings and integration rules. Paper 122 (2007)

Web

33. BOC Asset Management GmbH: ADOxx. Website (2016), online erhältlich unter https://www.adoxx.org; abgerufen am 07. Dezember 2017.
34. BSI: IT-Grundschutz-Kataloge. Website (2016), online erhältlich unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html; abgerufen am 07. Oktober 2016.
35. Department Knowledge Engineering: OMiLAB. Website (2016), online erhältlich unter http://austria.omilab.org; abgerufen am 07. Dezember 2016.
36. Deutsches Forschungsnetz: CERT: Ablauf einer OCTAVE-Analyse. Website (2016), online erhältlich unter http://www.dfn-cert.de/leistungen/octave/octavephasen.html; abgerufen am 07. Dezember 2016.
37. Deutsches Forschungsnetz: CERT: OCTAVE - Operational Critical Threat Asset and Vulnerability Evaluation. Website (2016), online erhältlich unter https://www.dfn-cert.de/leistungen/octave.html; abgerufen am 07. Dezember 2016.
38. WKO: Bundessparte Information und Consulting der WKO. Website (2016), online erhältlich unter http://www.it-safe.at; abgerufen am 07. Dezember 2016.

A Benutzerhandbuch

A.1 Einleitung

Das vorliegende Handbuch soll einen Einstieg in die Verwendung des in dieser Arbeit implementierten Security-Konzepts ermöglichen. Als EAM-Sprache steht ArchiMate zur Verfügung sowie alle Elemente und Funktionalitäten, die in dieser Arbeit beschrieben wurden.
Über dieses Handbuch: Das folgende Handbuch dient als Anleitung zur Erstellung von Architekturmodellen und deren Sicherheitsbewertung auf Grundlage der Konzepte in dieser Arbeit. Es gliedert sich in folgende Bereiche:

- Erstellung eines Architekturmodells.
- Bewertung des Schutzbedarfs von Daten und anderen Architekturelementen.
- Bewertung von Maßnahmen des BSI Grundschutzkataloges.
- Auswertung der bewerteten Architekturelemente.

A.2 Erstellung eines Architekturmodells

Um ein Architekturmodell zu erstellen, können Sie zwischen folgenden Modelltypen wählen:

- Business Layer
- Application Layer
- Technology Layer
- Analysis Model (Dieser Modelltyp enthält alle Elemente des Metamodells)

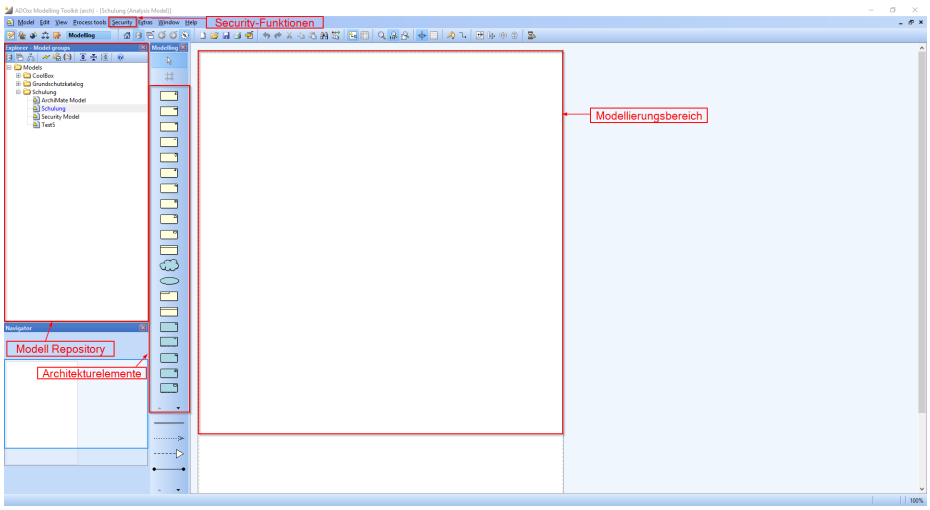

Abb. 84. Leeres Architekturmodell

Ist das Modell geöffnet, kann aus verschiedenen Architekturelementen des ArchiMate-Standards gewählt werden (siehe Abb. 84).

A.3 Bewertung des Schutzbedarfs von Daten und anderen Architekturelementen

Ist das Architekturmodell fertig, kann mit der Bewertung der Datenobjekte, sofern modelliert, begonnen werden. Dazu öffnen Sie das Notebook eines Datenobjekts und bewerten dessen Vertraulichkeit, Integrität und Verfügbarkeit (siehe Abb. 85). Gibt es Datenobjekte ohne konkrete Informationen zu Vertraulichkeit, Integrität oder Verfügbarkeit, kann der Wert „No Entry“ selektiert werden. Sind alle Datenelemente des Modells bewertet, kann die Funktion „Schutzbedarf bewerten“ gewählt werden, welche auf Basis der vorgenommenen Datenbewertung sämtliche Architekturelemente, welche direkt bzw. indirekt mit den Datenelementen verbunden sind, vererbend bewertet. Nach der Auswahl des zu bewer-

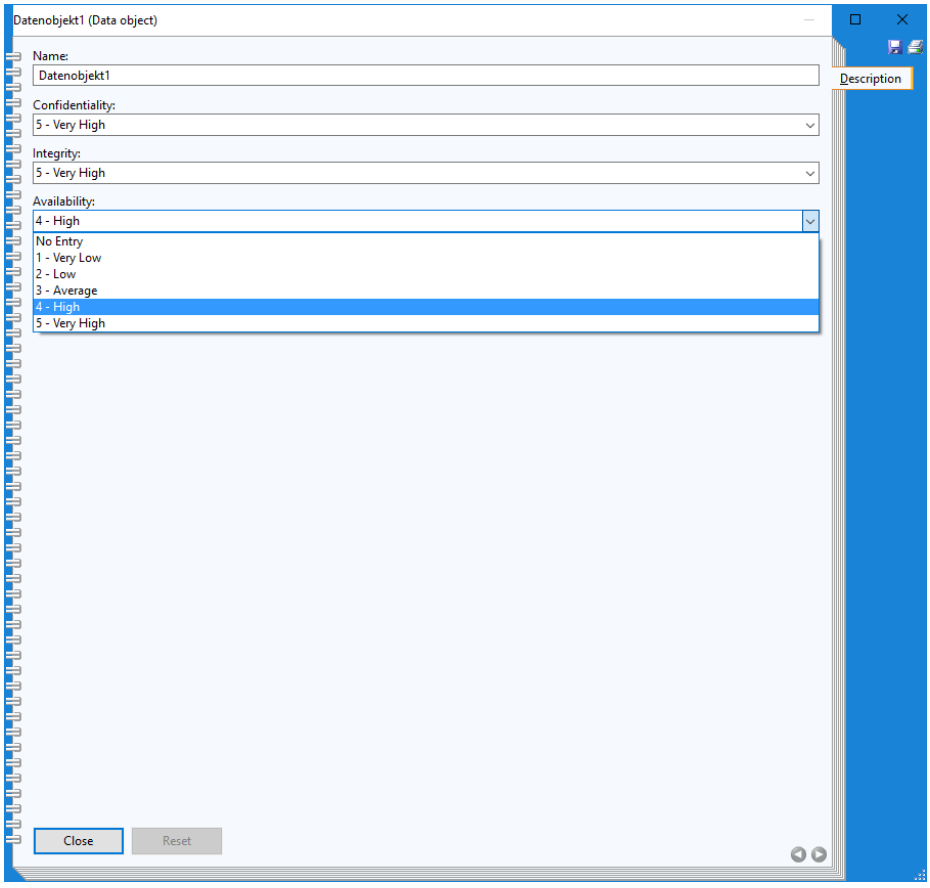

Abb. 85. Datenbewertung

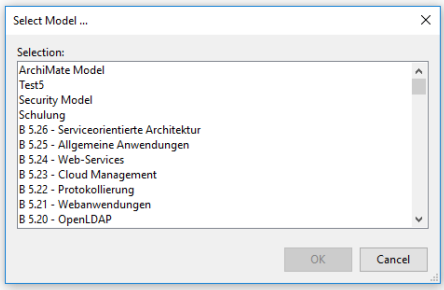

Abb. 86. Modellselektion

tenden Modells (siehe Abb. 86) werden alle Architekturelemente einzeln bewertet (siehe Abb. 87)

A.4 Bewertung von Maßnahmen des BSI Grundschutzkataloges

Anschließend kann mit der Bewertung des Grundschutzes begonnen werden. Dazu wird vorausgesetzt, dass der Grundschutzkatalog des BSI in der ADOxx-Plattform in Form von Modellen zur Verfügung steht. Soll eine Applikation bewertet werden, muss zunächst ihr Notebook geöffnet und anschließend der passende Baustein zugewiesen werden (siehe Abb. 88). Bausteine können einem Architekturelement auch mehrfach zugewiesen werden.

Nachdem alle gewünschten Bausteine zugewiesen wurden, kann die Funktion „Grundschutz bewerten“ gewählt werden. Dadurch werden alle dem Baustein zugewiesenen Maßnahmen automatisch dem entsprechenden Architekturelement zugewiesen (siehe Abb. 89). Diese Maßnahmen können dann auf ihre Erfüllung hin mit „Ja“ für erfüllt und „Nein“ für nicht erfüllt bewertet werden .

A.5 Auswertung der bewerteten Architekturelemente

Sind der Grundschutz und der Schutzbedarf für die Elemente bewertet, kann mit der implementierten Funktion „Likelihood-Impact-Analyse“ eine Auswertung gestartet werden. Nach der Selektion des zu analysierenden Modells und des Architekturelements wird eine grafische Auswertung generiert (siehe Abb. 90). Die Auswertung stellt einerseits die Eintrittswahrscheinlichkeit, auf Basis der zuvor selektierten Maßnahmen, und andererseits die Auswirkung, auf Basis der zuvor selektierten Ausprägung der CIA-Attribute, gegenüber.

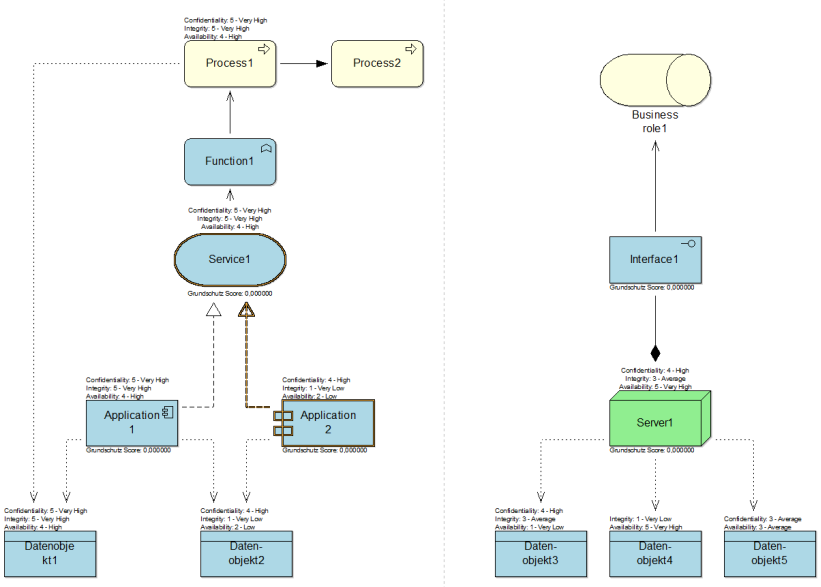

Abb. 87. Bewertung der Architekturelemente

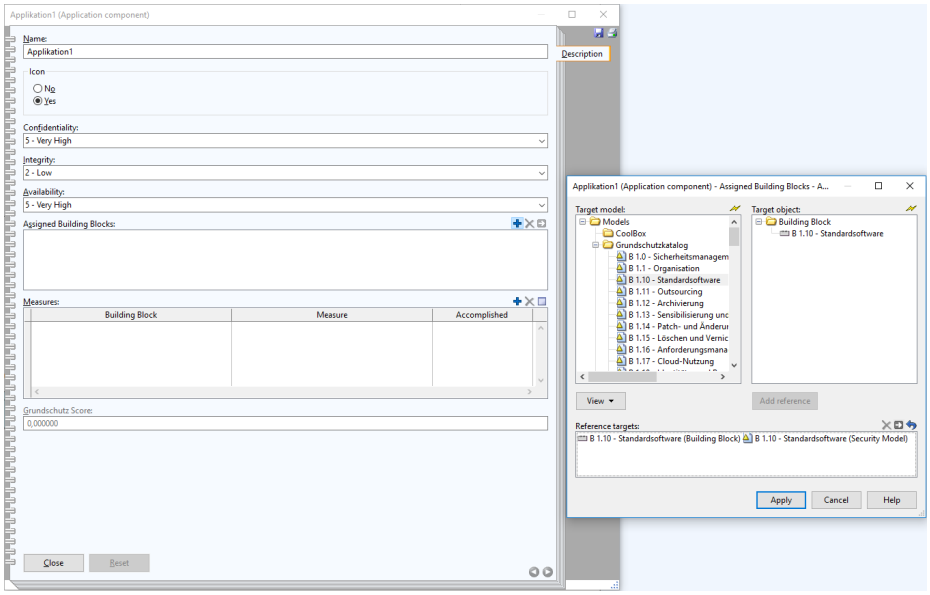

Abb. 88. Zuweisung eines Grundschutz-Bausteins

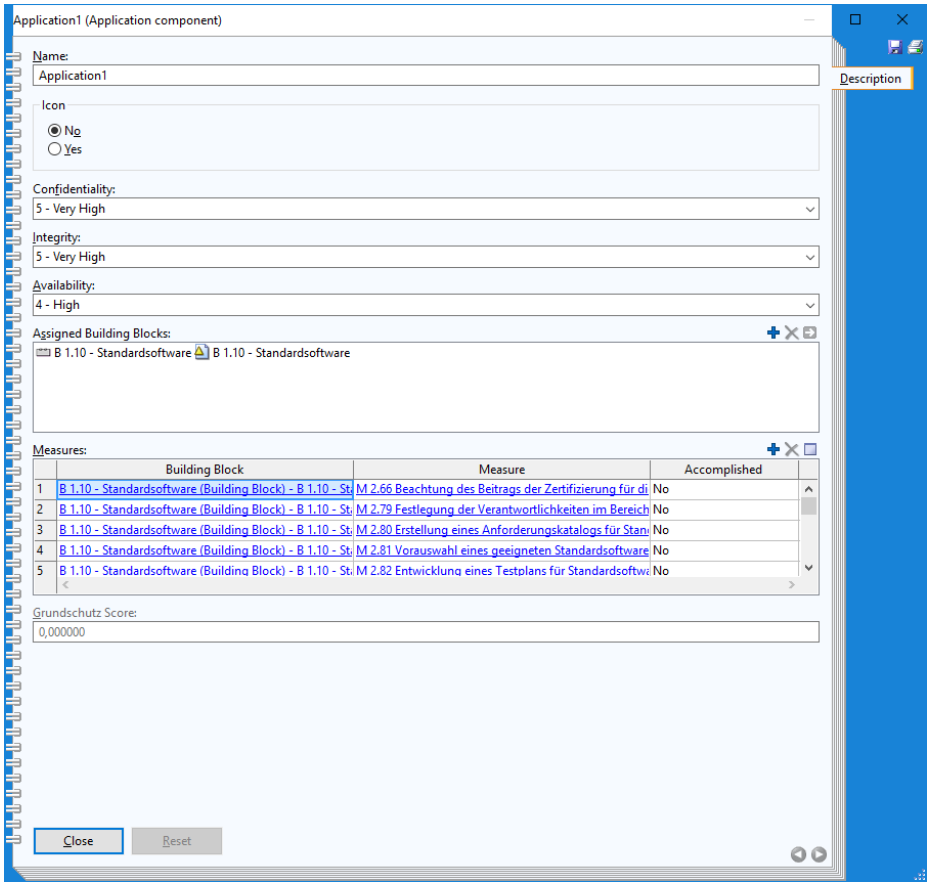

Abb. 89. Zuweisung der Grundschutz-Maßnahmen

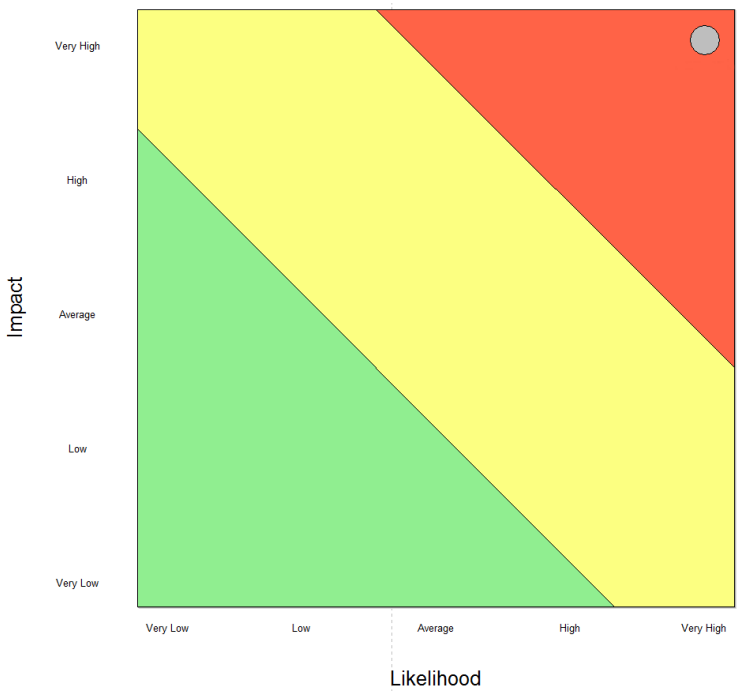

Abb. 90. Likelihood-Impact Analyse

B Source Code

Source Code auf CD