Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Master-Thesis

Konzeption von IT-Sicherheitskriterien für vernetzte Endgeräte

Abschlussarbeit zur Erlangung des Grades eines

Master of Engineering

der Hochschule Wismar

Datum: 28.08.2019

von: Thomas Stemplewitz
geboren am 26.09.1980 in Rudolstadt

Betreuer: Prof. Dr. A. Raab-Düsterhöft
Zweitbetreuer: Prof. Dr. A. Ahrens

Aufgabenstellung

Das Ziel dieser Master-Thesis ist das Erstellen von allgemeinen IT-Sicherheitskriterien für vernetzte Endgeräte auf IP-Basis.
Mit allgemeinen IT-Sicherheitskriterien und einer Erstanalyse vernetzter Geräte, könnte sich die Komplexität bei Produktentwicklungen reduzieren und Vertrauen bzw. Gewissheit über den IT-Sicherheitszustand vorhandener Geräte geschaffen werden.
Die zu erstellenden IT-Sicherheitskriterien sollen auf ihre Funktionalität und ihre Qualität überprüft werden. Zudem soll es möglich sein, vernetzte Endgeräte mit Hilfe von IT-Sicherheitsmodellen, Schwachstellenscannern und Penetrationstests auf diese Sicherheitskriterien zu überprüfen.
Die zu erarbeitenden Sicherheitskriterien können als Basis für weitere und komplexere Test- und Analyseverfahren sowie für Zertifizierungen herangezogen werden.

Autoreferat

IT-Sicherheit wird oft als komplexe Thematik verstanden, deren Bewertung und zu ergreifende Maßnahmen zum Erreichen von IT-Sicherheit, nur durch Experten wahrgenommen werden kann. Mithilfe von wenigen und generellen IT-Sicherheitskriterien könnte ein schneller Einstieg in das Thema erfolgen.
Ziel dieser Arbeit ist das Erstellen von allgemeinen IT-Sicherheitskriterien für vernetzte Endgeräte. Die zu erstellenden IT-Sicherheitskriterien sollen auf ihre Funktionalität und ihre Qualität untersucht werden. Zudem soll es möglich sein, vernetzte Endgeräte mithilfe von Testverfahren auf diese Sicherheitskriterien zu überprüfen. Die Darstellung kann in vereinfachter Form als *ERFÜLLT* oder *NICHT ERFÜLLT* und mit den jeweiligen Handlungsempfehlungen dargestellt werden. Eine Systembewertung anhand der IT-Sicherheitskriterien soll allen Nutzern von Endgeräten Gewissheit über den IT-Sicherheitszustand ihrer Geräte geben.

Abstract

IT security is often understood as a complex topic whose evaluation and measures to be taken to achieve IT security can only be perceived by experts. With the help of a few and general IT security criteria, a quick introduction to the topic could take place.

The aim of this work is to create general IT security criteria for networked end devices. The functionality and quality of the IT security criteria to be created are to be examined. In addition, it should be possible to check networked end devices for these security criteria with the aid of test procedures. The representation can be represented in simplified form as *FULFILLED* or *NOT FULFILLED* and with the respective recommendations for action. A system evaluation based on the IT security criteria should give all users of terminal equipment certainty about the IT security status of their devices.

Inhaltsverzeichnis

1 Motivation und Einleitung

Digitalisierung und die damit verbundene Vernetzung von Geräten ist allgegenwärtig. Derzeit sind etwa 20 Milliarden verbundene Geräte im Einsatz, davon 7 Milliarden im Internet der Dinge (Internet of Things (IoT)). Bis zum Jahr 2025 wird ein jährliches Wachstum bis zu 10 Prozent erwartet [Jej18] [Lue18].
Viele der derzeit eingesetzten vernetzten Geräte sind unzureichend gesichert und verwenden Netzwerkprotokolle, bei denen keine Sicherheitsfunktionen integriert sind. Aus diesen Gründen ist der Einbruch in solche Geräte für Angreifer, wie Botnetzbetreiber sehr einfach. Das wurde am Beispiel des Botnetzes *Mirai* sehr deutlich. Die Übernahme der Geräte erfolgte durch einfaches Durchprobieren von wenigen Kombinationen aus Nutzernamen und Passwörtern, sowie dem Ausnutzen der fehlenden Sicherheitsimplementierungen des Netzwerkprotokolls *Telnet* [Kre17].
Die Tatsache der teils fehlenden und unzureichenden Sicherheitsfunktionen in den Geräten, sowie die Vielzahl der vorhandenen Geräte und das erwartete Wachstum, machen neue Sicherheitsansätze erforderlich.
Auch wenn mittlerweile die ersten ganzheitlichen Sicherheitskonzepte für die Industrie 4.0 veröffentlicht sind [WM16] und auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen und technische Richtlinien herausgibt, fehlen verbindliche Standards und Richtlinien für Hersteller und Betreiber, ausgenommen die Betreiber kritischer Infrastrukturen (KRITIS).
Vorhandene Frameworks und Standards, wie Control Objectives for Information and Related Technology (COBIT), die ISO-27000-Reihe, der IT-Grundschutz des BSI und die Regularien des National Institute of Standards and Technology (NIST), sowie deren Zertifizierungen zielen auf gesamtheitliche IT-Sicherheitsprozesse in Unternehmen ab. Die darin enthaltenen Test- und Prüfverfahren sind entsprechend umfangreich und haben für große Unternehmen und kritische Infrastrukturen ihre Daseinsberechtigung.
Für Hersteller vernetzter Endgeräte gibt es keine Vorgaben. Eine aktuelle Veröffentlichung fasst eine Reihe von IT-Sicherheitstests für IoT-Geräte zusammen [MBQA18]. Konkrete Handlungsanweisungen oder neue Produkte, in denen diese Verfahren vereint und angewendet werden, fehlen. Mit neuen Ansätzen könnte die

allgemeine Bedrohungsweite von Angriffsvektoren verkleinert werden, sowie Vertrauen, Sicherheit und Akzeptanz durch Betreiber und Benutzer erreicht werden. Zudem sollte ein einfacher Einstieg in die Themen IT-Sicherheitsüberprüfungen und IT-Sicherheitsimplementierungen möglich sein. Einfache IT-Sicherheitstests für vernetzte Endgeräte könnten das Interesse der Hersteller am Thema wecken.
Für Endnutzer gibt es Handlungsempfehlungen des BSI, die auf der Internetseite https://bsi-fuer-buerger.de zu finden sind. Damit möchte das Bundesamt alle Bürger erreichen. Auch Endnutzer könnten mit einfachen IT-Sicherheitstests ihrer verwendeten Geräte für das Thema sensibilisiert werden.
Ziel dieser Arbeit ist das Erstellen von allgemeinen IT-Sicherheitskriterien für vernetzte Endgeräte. Die zu erstellenden IT-Sicherheitskriterien sollen auf ihre Funktionalität und ihre Qualität überprüft werden. Zudem soll es möglich sein, vernetzte Endgeräte mithilfe einfacher Testverfahren auf diese Sicherheitskriterien zu überprüfen. Die Ergebnisse der Tests sollen in vereinfachter Form als *ERFÜLLT* oder *NICHT ERFÜLLT* und mit den jeweiligen Handlungsempfehlungen dargestellt werden.
Mit allgemeinen IT-Sicherheitskriterien und einer Erstanalyse vernetzter Endgeräte, könnte sich die Komplexität bei der Produktentwicklung reduzieren, sowie Vertrauen und Gewissheit über den IT-Sicherheitszustand vorhandener Geräte geschaffen werden. Weiterhin können die zu erstellenden IT-Sicherheitskriterien als Basis oder Baustein für weitere und komplexe Testverfahren und Zertifizierungen herangezogen werden.
Mit der Einleitung, Motivation und Zielsetzung in diesem Kapitel, folgen im 2. Kapitel Definitionen, Begriffe, Abgrenzungen, Klassifizierungen und allgemeine Grundwerte der Informationssicherheit. Im 3. Kapitel werden häufige Sicherheitsprobleme im Zusammenhang mit informationstechnischen Systemen zusammengefasst und daraus durch Cyber-Antipattern, allgemeine Sicherheitskriterien für vernetzte Endgeräte entwickelt. Modellhafte Nachweise, sowie organisatorische, als auch technische Nachweise der Sicherheitskriterien werden im 4. Kapitel geführt, gefolgt von Diskussionen und Bewertungen dieser Nachweise. Damit stellen die Kapitel 3 bis Kapitel 5 den zentralen Kern dieser Arbeit dar.

Einen Überblick über den Ablauf im Hauptteil dieser Thesis ist in Abbildung 1.1 dargestellt.

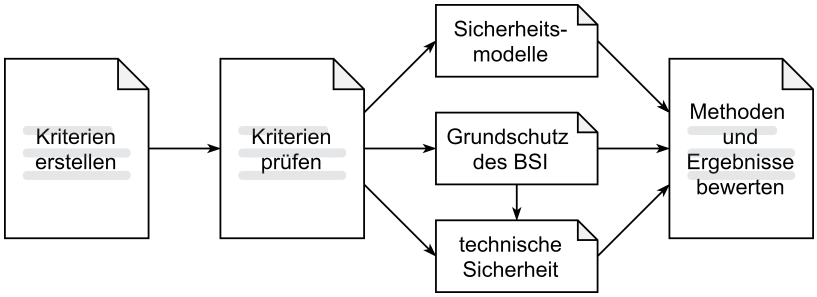

Abbildung 1.1: Ablauf im Hauptteil der Master Thesis (Eigene Darstellung)

Im abschließenden 6. Kapitel erfolgt eine Zusammenfassung und ein Ausblick.

2 Begriffsbestimmungen

Anhand verwendungsspezifischer Eigenschaften werden Endgeräte in diesem Kapitel von anderen Geräten und Diensten abgegrenzt, spezifiziert und somit bestimmt. Daraus wird eine mögliche Klassifizierung für vernetzte Endgeräte auf IP-Basis vorgestellt, sowie deren Schutzziele erläutert und Angriffsvektoren auf solche Geräte beschrieben. Diese Begriffsbestimmungen bilden Basis für weiterführende IT-sicherheitsrelevante Betrachtungen.

2.1 Vernetzte Endgeräte

Zunächst soll der Begriff *vernetztes Endgerät* bestimmt werden, der in der vorliegenden Thesis eine zentrale Rolle spielt. Der Begriff Endgerät wird allgemein verwendet, wenn von Geräten die Rede ist, die an Netzwerke angeschlossen sind und Dienste über das Netzwerk nutzen oder selbst anbieten. Das können Client-PCs, Server, Drucker etc. sein [Wü11]. Häufig findet die Bezeichnung Endgerät bei der Erläuterung des Aufbau, der Funktionsweise und der Sicherheit von Rechnernetzen Verwendung und wird als Endpunkt von Kommunikationsverbindungen beschrieben [Bau18] [Kap13] [Wen18].
Mit diesem grundsätzlichen Verständnis kann eine erste Abgrenzung zu allen netzwerkfähigen Geräten auf IP-Basis getroffen werden, die an der Bereitstellung, der Vermittlung, dem Transport oder der Sicherung von Netzwerken beteiligt sind. Somit werden Router, Switche oder Firewallsysteme in dieser Arbeit nicht betrachtet. Ein Großeteil der folgenden IT-Sicherheitsbetrachtungen wird sich auf TCP/IP-Netzwerke beziehen, so dass vernetzte Endgeräte wie folgt bestimmt werden können.
Als vernetzte Endgeräte werden alle physischen und virtuellen IT-Systeme aufgefasst, die einen TCP/IP-Stack implementiert haben und damit über ein Netzwerkinterface eine 2-Wege-Kommunikation ermöglichen. Die Verbindung zum Weitverkehrsnetz WAN (engl.: Wide Area Network) erfolgt über ein Gateway. Darunter fallen Systeme, die als Client oder Server eingesetzt werden.

2.1.1 Internet der Dinge

Auf Grund des hohen Anteils vernetzter Geräte im Internet der Dinge, vgl. Kapitel 1, erfolgt im vorliegenden Abschnitt eine zusammenfassende Beschreibung des IoT und der darin verwendeten vernetzten Geräte. Aus diesen Erkenntnissen soll festgelegt bzw. abgegrenzt werden, in wie weit Geräte im IoT für IT-sicherheitsrelevante Betrachtungen in dieser Thesis herangezogen werden können.
Mit der Entwicklung des Internet werden Aufgaben aus der realen Welt in einen imaginären Raum der virtuellen Welt überführt. Da nicht alle menschlichen Aktivitäten in diesem imaginären Raum abgebildet werden können, ist es das Ziel des Internet der Dinge IoT, durch neue Technologien den imaginären Raum und die reale Welt auf einer Plattform zu integrieren [KP14]. Im Internet der Dinge werden neben Computern und Menschen, auch Alltagsgegenstände mit dem Internet verbunden [AS14]. Dinge können dabei alle physischen, virtuellen, sowie lebende als auch leblose Objekte in allen Lebensbereichen darstellen. Es soll nicht einmal zwischen Mensch und Maschine unterschieden werden [Wen18]. Verallgemeinert besteht ist die Hauptfunktion von IoT-Geräten darin, Daten über das Internet zu senden, sowie Kommandos zu empfangen bzw. auszuführen [Kof18]. Dabei spielt die allgegenwärtige, zeit- und ortsabhängige Zugänglichkeit eine zentrale Rolle [KBD16]. Mit dieser Maßgabe bringen die Anforderungen an die Entwicklung und Vernetzung von IoT-Geräten zahlreiche technische Herausforderungen mit sich. Darunter fallen die Herstellung einer Vielzahl kleiner, stromsparender, kostengünstiger und intermittierend verbundener Sensoren und Geräte mit ressourcenschonenden Betriebssystemen, sowie die Entwicklung und der Einsatz von effizienten Routing- und IP-Protokollen [PD12].
IoT-Geräte können in direkt adressierbare und indirekt adressierbare Geräte unterteilt werden. Direkt adressierbare Geräte sind meist mit einer eigenen IP-Adresse an ein Netzwerk angeschlossen und können autark betrieben oder durch Systeme verwaltet werden, während indirekt adressierbare Geräte ausschließlich mit Steuereinheiten über Funknetze wie z.B. ZigBee, ZWave, Bluetooth kommunizieren [BSI17c]. Indirekt adressierbare Geräte wie Sensoren, Aktoren etc. sollen bei der weiteren Betrachtung keine Rolle spielen, ebens owenig spezielle Funkprotokolle.
Auf Grund dieser weitreichenden Durchdringung wird Sicherheit im IoT als umfassender Gegenstand betrachtet [Wen18]. Mit dem Internet der Dinge kommt für IT-sicherheitsrelevanten Betrachtungen der Umstand hinzu, dass vernetzte Endgeräte umfassendere Aufgaben für und in allen Lebensbereichen wahrnehmen können und demzufolge als Teil des Internet der Dinge aufgefasst werden können oder min-

destens mit dem IoT in Berührung kommen.

2.1.2 Klassifikation

Mit der allgemein bestimmten Verwendung, lassen sich vernetzte Endgeräte in drei Klassen unterteilen. Typische Vertreter sind zum einen solche Geräte, die ausschließlich selbst Dienste anbieten und Geräte, die ausschließlich Dienste nutzen. Eine weitere Klasse lässt sich aus Geräten bilden, die simultan verwendet werden. Ein allgemeines Klassifizierungsschema vernetzter Endgeräte ist in Abbildung 2.1 dargestellt.

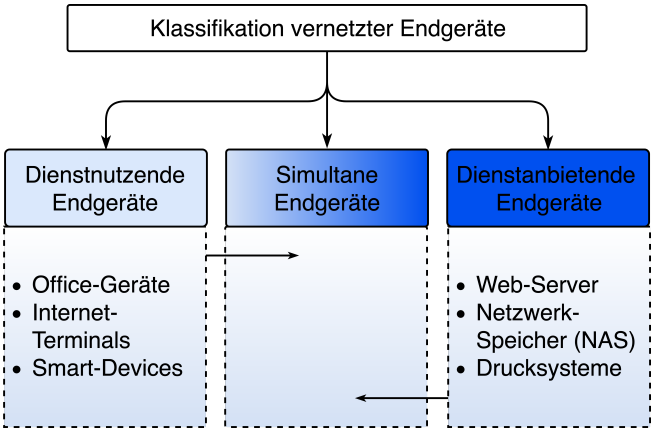

Abbildung 2.1: Klassifikation vernetzter Endgeräte (Eigene Darstellung)

Die Besonderheit simultan verwendeter Geräte liegt darin, zugleich Dienste anzubieten, als auch aktiv aus Sicht eines Endgerätes zu nutzen. So werden beispielsweise Desktop-PCs dazu verwendet Datenfreigaben über Netzwerke zu nutzen oder selbst anzubieten, oder einfache Webdienste anzubieten. Anders herum ist es möglich, das Betriebssystem eines Webservers auch für die Emailnutzung oder als Webbrowser zu verwenden. Die Nutzung solcher Anwendungsszenarien, bzw. die Anforderung daran, sollte kritisch hinterfragt und geprüft werden.

2.1.3 Komponenten

Um möglichst vollständige IT-Sicherheitsbetrachtungen auf vernetzten Endgeräten durchführen zu können, sind differenzierende Perspektiven auf die typische Verwendung der Geräte sinnvoll. Aus diesem Grund wird die Unterteilung einer allgemeinen

Verwendung vernetzter Endgeräte, in funktionale Komponenten vorgeschlagen. Abbildung 2.2 zeigt einen verallgemeinerten und typischen Anwendungsfall eines vernetzten Endgerätes mit der Darstellung der differenzierenden Komponenten, welche wie folgt erläutert werden.

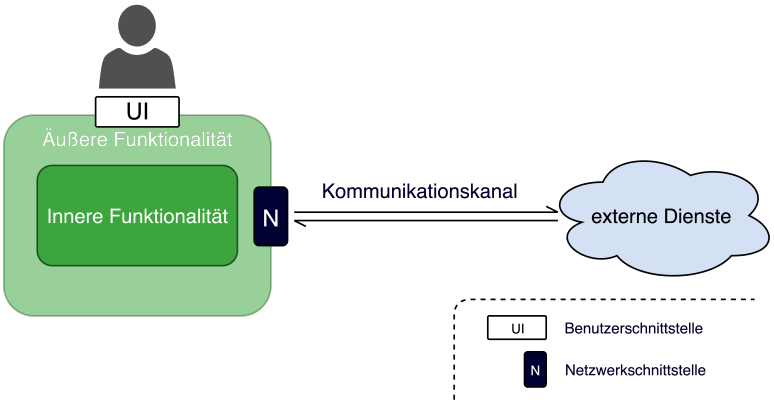

Abbildung 2.2: Komponenten vernetzter Endgeräte (Eigene Darstellung)

Zunächst sei der **Nutzer** als Komponente genannt, welcher durch seine Eingaben an der Komponente **Nutzerinterface**, maßgeblich an der IT-Sicherheit der Geräte beitragen kann. Der Komponente **Äußere Funktionalität** können alle Eigenschaften zugeordnet werden, welche mit der physischen Beschaffenheit des Gerätes direkt in Verbindung stehen. Die **Innere Funktionalität** behandelt den Betrieb und die Sicherheit der eingesetzten Betriebssysteme. Eine weitere wichtige Komponente stellt die **Netzwerkschnittstelle** dar. Diese kann in Form einer TCP/IP-Netzwerksverbindung verstanden werden und ist für den Aufbau, die Sicherstellung und die Sicherheit des **Kommunikationskanals** zu einem **externen Dienst** verantwortlich.

2.2 Informationssicherheit, Cyber-Sicherheit und IT-Sicherheit

Die **Informationssicherheit** behandelt den Schutz von Informationen jeglicher Art, unabhängig davon wo oder wie die Daten verarbeitet, transportiert oder gespeichert werden.
Die **Cyber-Sicherheit** beschäftigt sich dagegen mit dem Schutz von Informationen im gesamten virtuellen Raum. Das schließt IT-Systeme, die darauf aufbauende Kommunikation, deren Vernetzung, sowie Anwendungen mit ein [BSI17b].
Aufgabe der **IT-Sicherheit** ist es, Daten und Werte von informationsverarbeitenden Systemen in Unternehmen gegen Bedrohungen jeglicher Art zu schützen [Eck14]

[BSI17b]. In dem Zusammenhang sind in [Wen18] die Begriffe Werte und Unternehmen weiter gefasst, so dass auch die Privatsphäre von Organisationen und Individuen durch informationsverarbeitende Systeme geschützt werden soll und durch die IT-Sicherheit bedient wird.
Die Handlungsfelder können in eine mengentheoretische Beziehung gesetzt werden. Dafür erhalten sie eigens gewählte alphabetische Bezeichner, welche wie folgt gelistet sind:

- **A** IT-Sicherheit
- **B** Cyber-Sicherheit
- **C** Informationssicherheit

Die mengentheoretische Beziehung ist in Formel 2.1 dargestellt:

$$A \subset B \subset C \tag{2.1}$$

Bezogen auf alle schützenswerten Informationen **x** unterliegt die mengentheoretische Darstellung folgender Bedingung:

$$A \subset B \subset C :\Leftrightarrow \forall\ x \in C \tag{2.2}$$

Alle im Verlauf dieser Master-Thesis vorkommenden IT-Sicherheitsbetrachtungen werden sich auf die Teilmenge der IT-Sicherheit **A** beziehen.

2.2.1 Schutzziele

Im Zusammenhang mit dem Schutz von Informationen in der Informationssicherheit und der IT-Sicherheit als Teilmenge dieser, nehmen die drei klassischen Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit eine zentrale Rolle ein [BSI17a] [Wen18] [Kap13]. Mit der Einhaltung aller drei Grundwerte kann der Schutz von Informationen in informationstechnischen Systemen möglich sein. Im Folgenden soll die Bedeutung und Abhängigkeit der drei Grundwerte erläutert werden.
Um Informationen in Systemen schützen zu können ist der Zugang zu beschränken und zu kontrollieren. Der Zugang sollte nur durch gültige Authentizität, also durch

eindeutige Identifizierung eines Subjektes autorisiert werden. Kann dies sichergestellt werden, sind die Grundwerte Vertraulichkeit und Integrität erfüllt. Können authentifizierte und autorisierte Subjekte ihre Berechtigung uneingeschränkt wahrnehmen, entspricht das dem Grundwert der Verfügbarkeit [Eck14].
Die enge Beziehung der Schutzziele wird auch als CIA-Triade[1] bezeichnet und kann wie folgt dargestellt werden [CS19].

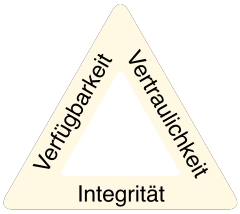

Abbildung 2.3: Schutzziel-Dreieck (Eigene Darstellung in Anlehnung an [CS19])

Angreifer und Penetrationstester verfolgen das Ziel, diese Grundwerte mit den entsprechenden Gegensätzen zu untergraben. Die Schutzziele und deren Gegensätze sind zur besseren Veranschaulichung sind in Abbildung 2.4 dargestellt.

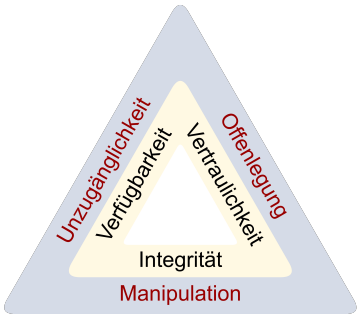

Abbildung 2.4: Bedrohungen der Schutzziele (Eigene Darstellung in Anlehnung an [CS19])

IT-Sicherheitskriterien müssen demnach so erstellt werden, dass mit der Anwendung dieser Kriterien, IT-Systeme und deren Daten vor ungewollter Unzugänglichkeit, illegitimer Manipulation, sowie der Offenlegung der Informationen wirksamen Schutz bieten.

[1] Der Begriff setzt sich aus den Anfangsbuchstaben der englischen Begriffe der Schutzwerte Confidentiality, Integrity, Availability zusammen

2.2.2 Schwachstellen, Verwundbarkeiten und Bedrohungen

Schwachstellen werden als Schwäche oder Punkt eines Systems beschrieben, an dem das System verwundbar bzw. angreifbar ist. Verwundbarkeiten sind wiederum Schwachstellen mit denen die Sicherheitsdienste des Systems umgangen, getäuscht oder manipuliert werden können [Eck14].
Diese und ähnliche Beschreibungen verleiten zu einer synonymen Verwendung der Begriffe Schwachstelle und Verwundbarkeit. Wendzel weist darauf hin, dass die Begriffe Schwachstelle und Verwundbarkeit nicht gleichzusetzen sind. Während Schwachstellen erst einmal keine Gefahr für das System darstellen, liegt der Unterschied bei der Verwundbarkeit darin, dass Schwachstellen durch einen Angreifer ausgenutzt werden können, um die Schutzziele des Systems zu gefährden. Dies stellt einen Vorteil für den Angreifer und einen Nachteil für das System dar. Die eigentliche Gefahr für die Kompromittierung der Schutzziele eines IT-Systems stellen Bedrohungen dar. Mit einer Bedrohung existiert ein Weg über den ein Angreifer eine Verwundbarkeit eines Systems ausnutzt, also einen Angriff durchführen kann [Wen18].
Bezogen auf die Betrachtung der Schutzziele, sowie deren Bedrohungen lässt sich IT-Sicherheit wie folgt bestimmen.
Ziel der IT-Sicherheit ist es somit, dass kein Weg mehr existiert, um die Schutzziele des Systems zu untergraben. Dieses Ziel lässt sich nach [Wen18] durch folgende aufeinander aufbauende Schritte erreichen:

- Prävention
- Angriffsdetektion
- Systemwiederherstellung

Weitere Betrachtungen in dieser Thesis fokussieren Präventionsmaßnahmen, sowie der Angriffsdetektion, welche überwiegend durch Prävention erzielt werden soll.

2.2.3 Angriffsvektoren vernetzter Endgeräte

Angriffsvektoren stellen typische Klassen von Angriffen auf informationstechnische Systeme dar. Dabei unterscheiden sich die Angriffsvektoren in Abhängigkeit von den Gerätetypen, sowie deren Anwendungsfokus. Biometrische Systeme sind beispielsweise anderen Angriffsvektoren ausgesetzt, als Groupware- und Email-Dienstleister,

oder Cloud-Anbieter. Auch wenn in den Komponenten vernetzter Endgeräte biometrische Authentifizierung implementiert sein könnten, oder Dienste von Cloud-Anbietern nutzen, werden nur die häufigsten und somit gängige Angriffsvektoren verallgemeinert betrachtet. Kofler et. al. beschreiben Angriffsvektoren als „sperrigen Begriff“ der Wege bezeichnet, die Angreifer (Hacker) beschreiten können, um in Computersysteme einzudringen [Kof18]. Dabei fassen die Autoren gängige Verfahren zusammen, um die Breite der Angriffsmöglichkeiten aufzuzeigen und verdeutlichen zugleich die Schwierigkeit, bzw. die Unmöglichkeit ganzheitlicher IT-Sicherheit zu erreichen [Kof18]. Als Basis für weitere Beschreibungen von Angriffsvektoren, werden die wichtigsten Verfahren nach Kofler et. al. herangezogen. Diese sind im Folgenden benannt und beschrieben:

- **Netzwerkangriffe**
  Dieser Angriffsvektor bezeichnet sehr allgemeine und klassische Angriffswege, welche über Netzwerke bzw. das Internet durchgeführt werden. Meist sind Serversysteme betroffen, bei denen Daten entwendet, manipuliert oder sonstiger Schaden angerichtet wird. Zu dieser Angriffsklasse können Angriffsarten wie DoS-Attacken (Deny of Service) und MitM-Attacken (Man in the Middle) gezählt werden.

- **Geräteinfizierung durch Schadsoftware**
  Mit der Geräteinfizierung durch Schadsoftware wie Malware, Viren oder mobilen Code, werden Angriffe beschrieben, bei denen die Infizierung meist über E-Mails, gefälschte Webseiten oder Malware-Apps erfolgt. Häufiges Ziel bei dieser Angriffsart ist es, die Kontrolle über IT-Systeme zu übernehmen, um Daten zu entwenden oder Geräteressourcen für Botnetze zu verwenden. Bei der Infizierung spielt der Nutzer eine maßgebliche Rolle.

- **Angriffe auf externe Dienste (Cloud)**
  Die Cloud ist ein attraktives Ziel für Angriffe, auch um Endgeräte zu manipulieren. Mit der Übernahme von Cloud-Konten durch Angreifer ist zudem das Einschleusen von Schadsoftware denkbar, wenn die Cloud-Konten auf Endgeräten eingebunden und aktiv sind. Am häufigsten aber zielen Angreifer bei dieser Angriffsart auf die Zugangsdaten der Nutzer ab.

- **Physischer Zugang**
  Haben Angreifer physischen Zugang zu einem Gerät, sind viele Angriffsmöglichkeiten denkbar, z.B. Hardwaremanipulationen, Mitschreiben von Nutzerdaten durch manipulierte USB-Sticks, Einschleusen von Schadsoftware oder

direkte Login-Versuche durch bspw. Brute-Force-Attacken, also dem systematischen oder unsystematischen Durchprobieren von Nutzerkennungen [Mü11].

- **Phishing**
  Password Phishing bezeichnet eine Angriffsart, bei dem der Angreifer den Anwender um die Eingabe seines Passwortes bewegt, meist per E-Mail in Form von Verifizierungen über gefälschte Online-Zugänge. Dieser Angriff kann auch durch Telefonate durchgeführt werden.

- **Social Engineering**
  Social Engineering zielt auf die rein menschliche Komponente ab, bei der versucht wird, alles über ein potenzielles Opfer herauszufinden und zwar mit allen möglichen Mitteln. Beispielhaft seinen das Durchsuchen des Internet, Befragen von Nachbaren, Mülldurchsuchungen etc. genannt.

Zusammengefasst können Angriffe in aktive Angriffe und passive Angriffe unterteilt werden, wobei aktive Angriffe zur Beeinflussung von Netzen und Systemen dienen. Passive Angriffe hingegen, werden ausschließlich zur Informationsgewinnung genutzt. Dabei können sowohl aktive Angriffe, als auch passive Angriffe mit technischen und sozialen Mitteln durchgeführt werden [Wen18].

2.2.4 Zusammenhang zwischen Schutzzielen und Gegenmaßnahmen

Erfolgreiche Angriffe durch Angriffsvektoren verletzen immer die Schutzziele der IT-Sicherheit, vgl. Abschnitt 2.2.1. Durch Gegenmaßnahmen wird versucht, die Schutzziele zu gewährleiten, vgl. Abschnitt 2.2.2. Es besteht ein Zusammenhang zwischen den Angriffen auf die Schutzziele und den allgemeinen Gegenmaßnahmen, vgl. Abbildung 2.5.

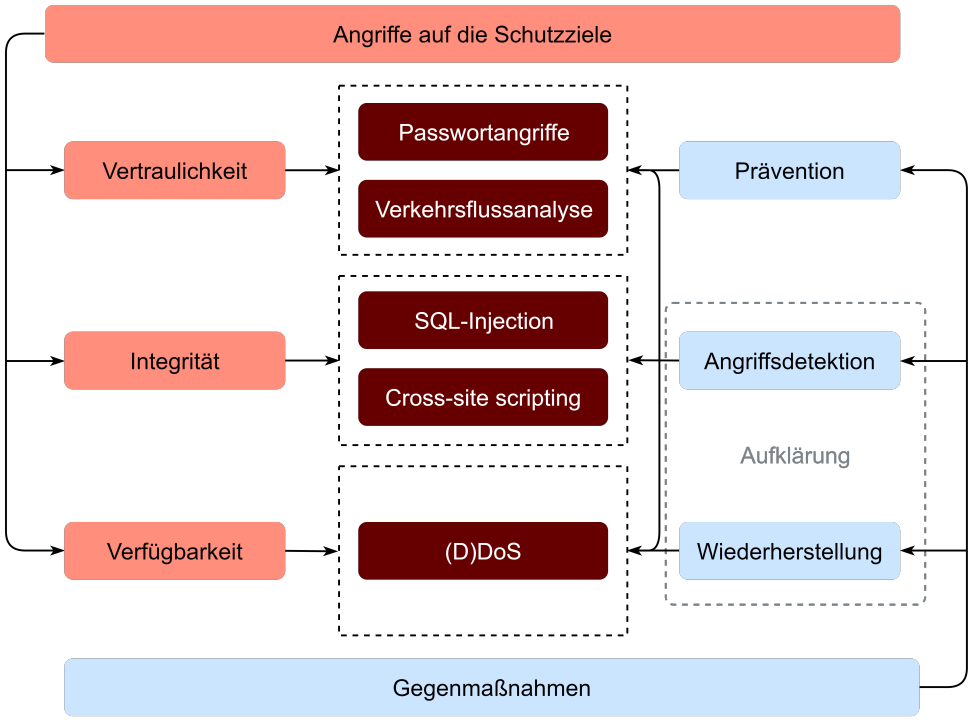

Abbildung 2.5: Zusammenhang zwischen Angriffen auf die Schutzziele und Gegenmaßnahmen (Eigene Darstellung)

Für die Darstellung wurden typische Vertreter von Angriffsvektoren ausgewählt. Diese Angriffsarten können eindeutig den Schutzzielen zugeordnet werden. Die Gegenmaßnahmen sollten möglichst so gewählt werden, dass geeignete Vorgehensweisen für alle Angriffsvektoren existieren. Am Beispiel von Präventionsmaßnahmen sind neben Sensibilisierungen für Nutzer, auch technische Systemhärtungen notwendig. Die Angriffsdetektion und die Wiederherstellung sollten geeignete Verfahren für alle Angriffsvektoren beinhalten. Dazu zählen auch Maßnahmen zur Erkennung von Verkehrsflussanalysen im WAN und die damit im Zusammenhang stehende Wiederherstellung einer nicht kompromittieren Netzwerkverbindung.

3 IT-Sicherheitskriterien

Auf Basis der Schutzziele informationstechnischer Systeme, sowie den entgegenstehenden Bedrohungen, sollen IT-Sicherheitskriterien konzeptioniert werden. Ziel ist eine universelle Anwendbarkeit auf vernetzte Endgeräte. Dafür werden häufige IT-Sicherheitsprobleme zusammengefasst und den Komponenten vernetzter Endgeräte zugeordnet, vgl. Kapitel 2.1.3. Mithilfe von Cyber-Antipattern werden die zusammengefassten Sicherheitsprobleme analysiert. Aus diesen Ergebnissen können die IT-Sicherheitskriterien abgeleitet werden.

3.1 Zusammenfassen häufiger IT-Sicherheitsprobleme

Um IT-Sicherheitskriterien für vernetzte Endgeräte konzeptionieren zu können, ist es zunächst notwendig, typische und häufig auftretende IT-Sicherheitsprobleme informationstechnischer Systeme zu kennen, sowie deren Relevanz für vernetzte Endgeräte zu prüfen. Als Auswertung soll eine Zuordnung von häufigen Sicherheitsproblemen zu den einzelnen Komponenten vernetzter Endgeräte erfolgen, vgl. Kapitel 2.1.3. Die Grundlage für generelle Sicherheitsprobleme bilden einschlägige Projekte der Open Web Application Security Project (OWASP)[1]. OWASP beschäftigt sich mit der Sicherheit von Diensten und Anwendungen im Internet. Deren Ziel ist es, mit Transparenz durch Veröffentlichung der Ergebnisse eine Verbesserung der Sicherheit der im Internet angebotenen Dienste zu erreichen. OWASP bewertet dabei mangelnde Anwendungssicherheit, welche aus personen-, prozess- und technologie-bezogenen Problemen entstehen. Die Häufigkeit von auftretenden Sicherheitsproblemen werden dann in Form von *TOP 10 - Listen* veröffentlicht [OWA18b].
Durch den rasanten Zuwachs an mobilen Geräten und Anwendungen, sowie IoT-Geräten in den vergangenen Jahren, widmet sich OWASP auch diesen Themen und hat speziell für mobile Geräte und IoT-Geräte *TOP 10 - Listen* der häufigsten Sicherheitsprobleme erstellt und veröffentlicht [OWA16] [OWA18a]. Weitere häufige Sicherheitsprobleme, wie sie in [Kof18] und [TB16] zu finden sind, wurden für eine

[1] OWASP™ Foundation: https://www.owasp.org (letzter Zugriff: 2019-08-28)

Zusammenfassung von Sicherheitsproblemen herangezogen und auf deren Relevanz für vernetzte Endgeräte geprüft.
Um die Gesamtsicherheit einen IT-Systems gewährleisten zu können, besteht für alle Komponenten vernetzter Endgeräte der Anspruch die Schutzziele zu erreichen, vgl. Kapitel 2.2.1. Auf Komponenten, wo dies beispielsweise nicht möglich ist, sind entsprechende Vorkehrungen auf anderen Komponenten zu erbringen. Als Beispiel sei hier der Kommunikationskanal angeführt. An diesen kann man die Forderung an die Verfügbarkeit stellen, jedoch nicht auf Vertraulichkeit setzen. Das liegt darin begründet, dass es grundsätzlich durch Dritte möglich sein kann, den Kommunikationskanal abzuhören. Damit einhergehend müssen auch ausreichend Schutzmechanismen gegen Datenmanipulationen implementiert sein.
Die in diesem Abschnitt zusammengefassten und häufigen Sicherheitsprobleme, sind in Tabelle 3.1 den einzelnen Komponenten vernetzter Endgeräte zugeordnet.

Sicherheitsproblem	Beschreibung	Komponente	Angriffsvektoren
Authentifizierungsschwächen	Betrifft schwache und leicht zu erratende Zugangsdaten aus bekannten, sowie einfachen Nutzernamen und Passwörtern, sowie fest hinterlegten Zugangsdaten	• Nutzer • Innere Funktionalität	• Netzwerkangriffe • Physischer Zugang
Authentifizierungsfehler	Fehlerhafte Implementierung der Authentifizierung	• Nutzerschnittstelle • Innere Funktionalität • Netzwerkschnittstelle	• Netzwerkangriffe • Physischer Zugang
Einsatz und Abhängigkeit von unsicheren und veralteten Komponenten und Diensten	Verwendung veralteter und unsicherer Hard- und Softwarekomponenten, sowie unsichere Dienste Dritter, wie Cloud-Lösungen, Restschnittstellen (API)	• Äußere Funktionalität • Innere Funktionalität • Netzwerkschnittstelle	• Netzwerkangriffe • Physischer Zugang
Sicherheitsrelevante Fehlfunktionen durch Standardauslieferungen	Auslieferung ohne Betrachtung von: Minimalkonfigurationen, Segmentierungen, Containering und sonstigen Systemhärtungen	• Nutzerschnittstelle • Äußere Funktionalität • Innere Funktionalität • Netzwerkschnittstelle	• Netzwerkangriffe • Physischer Zugang
Unsicherer Datentransfer und Datenspeicherung	Ursachen hierfür können z.B. der Einsatz veralteter Komponenten oder Fehlkonfigurationen sein	• Äußere Funktionalität • Innere Funktionalität • Netzwerkschnittstelle • Kommunikationskanal	• Netzwerkangriffe • Physischer Zugang
Fehlende oder eingeschränkte Geräteverwaltung	Fehlende Sicherheitsunterstützung für Geräte, einschließlich Asset Management, Update-Management, sichere Außerbetriebnahme	• Äußere Funktionalität • Innere Funktionalität	• Netzwerkangriffe • Physischer Zugang
Unzureichendes Logging und Monitoring	Betrifft alle Bereiche, von denen die Sicherheit der Geräte beeinträchtigt werden kann, z.B. Logging von Fehlfunktionen und Überwachung von Zutritten und Zugriffen auf das System, oder auf Daten des Systems	• Nutzerschnittstelle • Äußere Funktionalität • Innere Funktionalität • Netzwerkschnittstelle	• Netzwerkangriffe • Physischer Zugang
Menschliches Fehlverhalten	Umfasst alle bewussten und unbewussten Fehlhandlungen, welche maßgelblich zur Beeinträchtung der Gerätesicherheit beitragen	• Nutzer	• Social Engineering • Phishing

Tabelle 3.1: Zusammenfassung häufiger Sicherheitsprobleme von IT-Systemen

Es auch möglich sein, dass ein Sicherheitsproblem mehrere Komponenten betrifft. Den Sicherheitsproblemen sind typische Angriffsvektoren zugeordnet.

3.2 Konzeptionelle IT-Sicherheit durch Cyber-Antipattern

Die im vorangegangenen Abschnitt zusammengefassten und für vernetzte Endgeräte relevanten Sicherheitsprobleme, sollen für die konzeptionelle Erstellung von IT-Sicherheitskriterien herangezogen werden. Die Konzeptionierung wird mithilfe von Cyber-Antipattern vorgenommen.
Cyber-Antipattern dienen ähnlich der Entwurfsmuster beim Design von Software dazu, eine strukturierte Darstellung der Konstruktion zu erhalten. Der Unterschied bei Antipattern liegt darin, dass diese nicht auf die eigentliche Lösung abzielen. Vielmehr geht es beim Entwurf mit Antipattern darum, häufig wiederkehrende Probleme aufzugreifen und alternative Lösungsvorschläge zur Problembehebung vorzuschlagen [Mow14]. Als Motivation für den Einsatz von Antipattern greift Mowbray dabei die schwierige Lage in Bezug auf die Cyber-Sicherheit auf und sieht als Lösung von IT-Sicherheitsproblemen radikale neue Denkweisen und paradoxerweise auch die Rückkehr zu ursrpünglichen Prinzipien und vor allem der Einsatz gesunden Menschenverstands. Antipattern verwenden dabei psychologische Rahmenbedingungen zur Problemlösung, da die Ursachen von Fehlern meist in Gewohnheiten liegen. Zudem fordern sie einen Bewusstseinswandel, welcher sich von naturwissenschaftlichen Denkweisen hin zu einem wertenden Umfeld von Unternehmensarchitekturen und dem organisatorischen Wandel entwickelt. Antipattern sind die Art und Weise, wie man klar über gewöhnliche Ursachen, schwerwiegende Probleme und effektive Lösungen denkt.
Beim Entwurf mit Antipattern beeinflussen konkurrierende und technische Faktoren, sowie Priorisierungen mögliche Lösungen. Es wird zwischen der Antipattern-Lösung und der Erneuerungslösung unterschieden. Die Antipattern-Lösung stellt eine gewöhnliche Fehlfunktion oder Fehlkonfiguration dar, die die Lösung aus ursprünglichen Entscheidungen sein kann oder unabsichtlich entstanden ist. Damit kann diese Lösung Nutzen, aber auch Konsequenzen mit sich bringen. Die Erneuerungslösung ergibt sich aus einer Neubewertung des ursprünglichen Designs und einer Auswahl effektiver Lösungsvorschläge. Dabei kann es auch verwandte bzw. ähnliche Lösungen geben. Der Ablauf und die Zusammenhänge des Antipattern-Konzeptes sind in Abbildung 3.2 dargestellt.

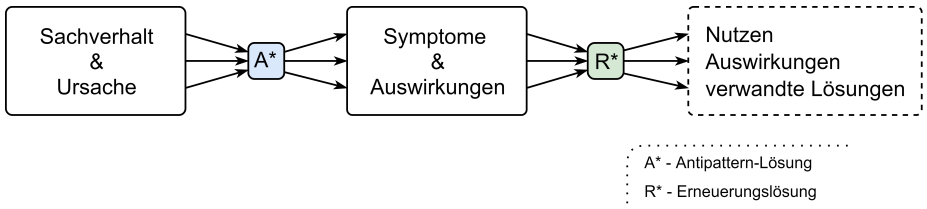

Tabelle 3.2: Antipattern-Konzept (Eigene Darstellung in Anlehnung an [Mow14])

Für den Entwurf schlägt Mowbray zwei Vorlagen vor, die Mikro-Antipattern-Vorlage und die vollständige Cyber-Antipattern-Vorlage. Zudem kann der Entwurf in drei unterschiedliche Richtungen ausgelegt werden. Hier wird zwischen dem grundsätzlichen Entwurf, sowie einem horizontalen und vertikalen Entwurf unterschieden werden. Der grundsätzliche bzw. elementare Entwurf zielt ausschließlich auf die drei Schutzziele ab, vgl. Kapitel 2.2.1, während der horizontal ausgerichtete Entwurf auf Betrachtungen über alle Bereiche an einer IT-infrastrukturellen Sicherheitsbetrachtung durchgeführt wird. Der vertikale Entwurf wird auf nur einen spezifischen Bereich, also ein IT-System oder eine separat zu betrachtende Domäne einer IT-Infrastruktur angewendet. Mowbay inkludiert in die elementaren Betrachtungen noch das Management der Funktionalität, gibt aber zu bedenken, dass dieses Themengebiet grundsätzlich bei der Entwicklung von Produkten abgedeckt ist. Somit wird der funktionelle Bereich als gegeben bzw. erfüllt betrachtet und beim Entwurf von IT-Sicherheitskriterien mit Antipattern in dieser Arbeit nicht berücksichtigt.
Die Verwendung eines Antipattern-Templates ist lt. Mowbay eine wichtige Ausgangssituation, um erfolgreiche Sicherheitsbetrachtungen mittels Antipattern durchzuführen. Im Verlauf dieser Thesis wird ein angepasstes, vollständiges Antipattern-Template verwendet, dass auf vertikale Betrachtungsweisen häufiger Sicherheitsprobleme vernetzter Endgeräte angewendet wird. Zudem behandelt das Template auch die primär angesprochene Komponente der vollständigen Kommunikation vernetzter Endgeräte, vgl. Kapitel 2.1.3. Das verwendete Template ist in Tabelle 3.3 abgebildet.

Antipattern	
Verwandte Bezeichnung(en)	
Gegenwärtige Lösung	
Titel der Erneuerungslösung	
Beeinträchtigte Schutzziele	
Betroffene Komponente(n)	
Antipattern-Lösung	
Symptome & Auswirkungen	
Erneuerungslösungen	

Tabelle 3.3: Antipattern-Template (Eigene Darstellung)

Im Anhang A sind die bearbeiteten Antipattern abgelegt. Aus den Ergebnissen in den Erneuerungslösungen der Antipattern werden die IT-Sicherheitskriterien für vernetzte Endgeräte abgeleitet. Folgende IT-Sicherheitskriterien konnten so ermittelt werden. Die IT-Sicherheitskriterien erhalten für die bessere Weiterverarbeitung im nächsten Abschnitt selbstgewählte und eindeutige Bezeichner in Form vom Großbuchstaben.

- **AA** Authentifizierung und Autorisierung
- **VZ** Komponentenzertifizierung und Verifizierung
- **V** Verschlüsselung des Datenverkehrs und der Datenablage
- **SL** Sicherheit durch Standardauslieferung
- **S** Überprüfbare Sensibilisierungsmethoden
- **MR** Monitoring und Reaktion

3.3 Komponentenzuordnung der IT-Sicherheitskriterien

Die im vorangegangenen Abschnitt erarbeiteten IT-Sicherheitskriterien werden nun den einzelnen Komponenten vernetzter Endgeräte zugeordnet werden, vgl. Abbildung 2.2 aus Abschnitt 2.1.3. Mit den Zuordnungen soll die Bedeutung der einzelnen Kriterien in der Gesamtheit des Endgerätes betrachtet werden, vgl. Abbildung 3.1.

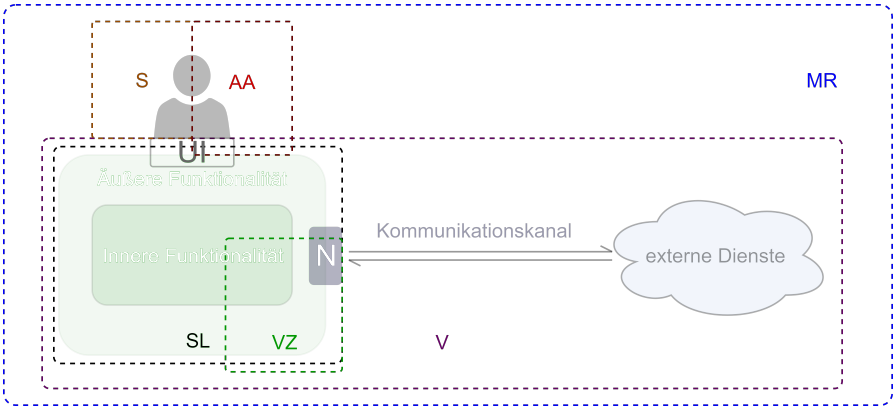

Abbildung 3.1: Zuordnen von IT-Sicherheitskriterien auf Endgeräte-Komponenten (Eigene Darstellung)

Aus dieser Abbildung kann abgeleitet werden, dass dem Kriterium *Monitoring und Reaktion (MR)* die größte Bedeutung zugeordnet werden kann, da es alle Komponenten direkt beeinflusst. Eine weitere große Bedeutung erfährt das Kriterium *Verschlüsselung des Datenverkehrs und der Datenablage (V)*, da dieses Kriterium an den Komponenten *Innere Funktionalität*, *Äußere Funktionalität*, der *Netzwerkschnittstelle* und dem *Kommunikationskanal* ansetzt und dadurch das Gesamtsystem zu großen Teilen beeinflussen kann. Eine geringere Bedeutung hingegen kommt den Kriterien *Authentifizierung und Autorisierung (AA)* und *Überprüfbare Sensibilisierungsmethoden (S)*, da diese entweder nur eine Komponente oder zwei Komponenten direkt berühren. Die Betrachtung der Kriterien an den Komponenten repräsentieren dabei ausschließlich die Breite der Angriffsfläche, keinesfalls jedoch die Auswirkungen bei der Verletzung eines der Schutzziele, vgl. Abschnitt 2.2.1. Verletzungen der Schutzziele betreffen immer das zu betrachtende Gesamtsystem.

4 Überprüfen von IT-Sicherheit

Im vorliegenden Kapitel werden die erstellten IT-Sicherheitskriterien auf ihre Anwendbarkeit überprüft. Dazu kommen neben formalen Prüfungen mithilfe von IT-Sicherheitsmodellen und dem Erstellen einer idealisierten IT-Sicherheitsrichtlinie an einem Beispiel, auch Testverfahren zum Einsatz, welche als Bestandteile für Penetrationstests und IT-Audits Verwendung finden könnten.

4.1 IT-Sicherheitsmodelle

Durch Hervorheben wichtiger Aspekte, sowie dem Weglassen unwichtiger Aspekte, liefern Modelle abstrakte Beschreibungen oder Darstellungen von Gegenständen aus der Realität. Das Abstrahieren wird dazu genutzt, die hervorgehobenen Aspekte vereinfacht dem Betrachter darzustellen oder durch andere Objekte zu ersetzen.
In der IT-Sicherheit beschreiben Modelle Systemzustände sowie ihre Übergänge und unterscheiden dabei zwischen sicheren und unsicheren Zuständen. Weiterhin liefern sie Erklärungen dafür, unter welchen Umständen sichere Zustände erreicht werden können [Gri08]. Somit können IT-Sicherheitsmodelle verwendet werden, um informationstechnische Systeme zu analysieren, zu bewerten oder nach diesen Modellen sichere Systeme und Anwendungen aufzubauen. Nach Grimm können IT-Sicherheitsmodelle nicht nur Sicherheitsanforderungen aufzeigen, sondern auch Hinweise dafür liefern, welche Arten von Sicherheitsmechanismen für die Erfüllung von Anforderungen geeignet sind [Gri08].
Auf Grund dieser weitreichenden Möglichkeiten werden IT-Sicherheitsmodelle in dieser Thesis herangezogen und bewertet, ob IT-Sicherheitsmodelle auf die im vorangegangenen Kapitel 3.2 erarbeiteten IT-Sicherheitskriterien angewendet werden können.
IT-Sicherheitsmodelle werden ausgehend von einem Kernmodell nach klassischen Sicherheitsaspekten in drei Klassen unterteilt, *Zugriffskontrollmodelle*, *Informationsflussmodelle* und *Transaktionsmodelle* [Kep13]. Grimm beschreibt Sicherheit als „Ausgleich von Interessenskonflikten von Menschen“ und betont damit die starke

Abhängigkeit vom Anwendungskontext. Als Beispiele führt er an, dass für die Sicherheit von Geldautomatenauszahlungen andere Regeln gelten, als für gesetzliche Aufbewahrungsfristen von Personalakten, bezogen auf die Anonymität der Daten. Verbunden mit der Abhängigkeit zu einem bestimmten Anwendungsbereich muss zunächst für jedes IT-Sicherheitsmodell ein ‚übergeordnetes Schutzziel' festgelegt werden. Alle essentiellen Beschreibungselemente für IT-Sicherheitsmodelle nach [Gri08] sind:

- Definition eines übergeordneten Sicherheitsziels
- Spezifikation sicherer Systemzustände
- Regelwerk für erlaubte Zustandsübergänge
- Sicherheitstheorem
- Vertrauensmodell

Im Sicherheitstheorem sind z.B. die Übergänge von sicheren Systemzuständen beschrieben. Das Vertrauensmodell beschreibt, unter welchen Annahmen das Sicherheitsziel durch sichere Systemzustände erreicht werden kann.
Nach Grimm ist die Aufgabe eines jeden IT-Sicherheitsmodells, drei Lücken zu schließen. Die Lücke zwischen

- dem Sicherheitsziel und seinen Anwendungen.
- sicheren Systemzuständen und dem Sicherheitsziel.
- erlaubten Zustandsübergängen und sicheren Systemzuständen.

Nach diesen allgemeinen Beschreibungen werden in den folgenden Abschnitten, die bekanntesten IT-Sicherheitsmodelle chronologisch nach ihrer Entstehung allgemein zusammengefasst vorgestellt und auf ihre Anwendbarkeit geprüft. Eine gesonderte Bewertung der Methoden wird in Kapitel 5.1.2 vorgenommen.

4.1.1 BellaPadula-Modell

Eines der bekanntesten Vertreter der Zugriffsmodelle ist das BellaPadula-Modell (1973). Streng formalisiert zielt es auf Sicherheitsanforderungen höchster Vertraulichkeit in hierarchischen Organisationsformen ab und regelt die allgemeine Zugriffskontrolle. Als Sicherheitsziel hat das Modell „die Verhinderung von vertraulichen

Informationsflüssen in unzuständige Bereiche“ definiert. Realisiert wird die allgemeine Zugriffskontrolle durch Zugriffskontrollmatrizen. Die Idee hinter dem Modell war die Ablösung von Einzelzugriffsrechten Discretionary Access Control (DAC), also diskreten Zugriffsrechten und die Einführung von generellen Zugriffsrechten Mandatory Access Control (MAC). Unter der Voraussetzung, das in festgelegten Hierarchien Informationsflüsse immer „von unten nach oben“, aber nie umgekehrt stattfinden, lässt sich MAC als Erweiterung von Einzelzugriffsrechten implementieren [Gri08]. Das bedeutet, dass Informationen immer von einer niedrigeren zu einer höheren Sicherheitsklasse fließen dürfen [Kap13].

4.1.2 Clark-Wilson-Modell

Integrität ist im BellaPadula-Modell nur implizit erreicht. Daher liegt im Modell von Clark-Wilson (1987) der Fokus auf handelnden Subjekten, mit ihrer Anfälligkeit zu Fehlern und Betrug. In diesem Modell werden Verifikationsprozeduren mit dem Ziel eingeführt, Fehler- und Betrugsvermeidung von handelnden Subjekten durch Aufgabenteilung zu erwirken. Das Sicherheitsziel in diesem Modell ist „der Schutz der Integrität der Anwendungsprozesse und ihrer Daten“ [Gri08].
Ausgehend von der Annahme, dass zwei Menschen seltener dieselben Fehler verursachen, spezifiziert das Modell in seinem Kern eine „Menge von Zertifizierungs- und Durchsetzungsregeln“. Grimm beschreibt, dass in diesen Verifikationsprozeduren Menschen Computerdaten mit der dargestellten Wirklichkeit vergleichen und wenn nötig Fehler korrigieren. Nach Grimm ist das Modell in diesem Kontext als Transaktionsmodell zu verstehen und zeigt die Grenzen der Automatisierung von Systemen auf.

4.1.3 Chinese-Wall-Modell

Mit der Veröffentlichung des Chinese-Wall-Modells im Jahr 1989, zielt das Modell auf den Konkurrentenschutz im Börsenumfeld ab. Unternehmensberatern verschiedener konkurrierender Firmen soll es nicht möglich sein, Firmengeheimnisse zu erfahren und zu verbreiten. Das Modell ist ein Zugriffskontrollmodell mit dem Sicherheitsziel der *Verhinderung von Insiderhandel*. Umgesetzt wird die Zugriffskontrolle in einer Zugriffskontrollmatrix, wie auch beim BellaPadula-Modell, sowie einer dynamisch wachsenden Protokollmatrix [Gri08].

4.1.4 Gleichgewichtsmodell

In offenen Netzen, wie dem Internet, kann man sich auf sich selbst verlassen, jedoch nicht auf das Verhalten von Kooperationspartnern. Mit dem Gleichgewichtsmodell (1993) nach Grimm war es erstmals möglich, einen sicheren und fairen Austausch von digitalen Gütern zwischen autonomen Partnern in offenen Netzen zu beschreiben. Das Sicherheitsziel dieses Transaktionsmodells ist die *Erfolgskopplung*. Diese Erfolgskopplung besagt, dass entweder beide Kooperationspartner ihr Ziel erreichen oder keiner von beiden. Umgesetzt wird das durch wechselseitige Verpflichtungen, sog. signierte Willenserklärungen und Empfangsbestätigungen an dazugehörigen Zeitpunkten. Das Modell kann dadurch auf zentral gesteuerte Kontrollmechanismen verzichten. Grimm definiert sichere Zustände indem Verpflichtungen und ihre Beweise im Gleichgewicht sind. Geregelte Abbrüche sind dabei auch akzeptabel. Im Gleichgewichtsmodell sind formale Ausdrücke zu Kooperationszielen, Verpflichtungen, sowie Regeln zur Lieferung von Beweisen definiert. Grimm setzt in diesem Modell zudem „ein funktionierendes juristisches Umfeld voraus, in dem digitale Signaturen akzeptiert werden“ [Gri08].

4.2 Prozessorientierte IT-Sicherheit

Eine Prozessorientierung ist immer dann gegeben, wenn IT-Sicherheit an Geschäftsprozessen oder Prozesszyklen, wie dem PCDA-Zyklus (Plan Do Check Act) ausrichtet wird. Die Prozessausrichtung ist Bestandteil bekannter Rahmenwerke und Standards wie COBIT und ITIL (Information Technology Infrastructure Library). In der ISO/IEC 27000-Reihe sind Prozesse wichtiger Bestandteil beim Aufbau eines ISMS (Information Security Management System). Auf Grund des hohen Umfang solcher Frameworks, Best Practices und Standards werden solche Verfahren und deren Prozesse nicht in dieser Thesis herangezogen. Einen möglichen Ansatz liefert die prozessorientierte Vorgehensweise für IT-Sicherheitsanalysen (ProSA) nach Simic [Sim17]. Diese Methode wird in folgenden beiden Abschnitten behandelt. Zunächst wird die Methode vorgestellt und beschrieben und anschließend exemplarisch auf ein IT-Sicherheitskriterium angewendet.

4.2.1 ProSA-Vorgehensweise

Die in diesem Abschnitt vorgestellten Beschreibungen für die Prozessorientierte Vorgehensweise für Sicherheitsanalysen (ProSA), stützen sich dabei im Wesentlichen auf die Literatur der Autorin D. Simic [Sim17].
Mit diesem prozessorientierten Vorgehensmodell soll vor allem der *Faktor Mensch* einen zentralen Charakter bei IT-Sicherheitsbewertungen spielen und in den Sicherheitsbegriff integriert werden. Die Vorgehensweise ist für die zielorientierte Kooperation in offenen Kommunikationsnetzen konzipiert und setzt auf dem Gleichgewichtsmodell von Grimm auf. Dabei sollen nach Simic fünf Perspektiven auf die IT-Sicherheit (technisch, organisatorisch, rechtlich, anwendungsorientiert, prozessorientiert) betrachtet werden. In der anwendungsorientierten Sicht sieht Simic den Faktor Mensch in folgenden drei Rollen:

- Sicherheitsträger
- Sicherheitsrisiko
- Kenntnisträger

Als **Sicherheitsträger** fungiert der Mensch ebenso in den Modellen von Clark-Wilson und dem Gleichgewichtsmodell von Grimm. Bei Clark-Wilson werden die „wohlgeformten Transaktionen“ durch Akteure nach festgelegten Regeln durchgeführt. Weiterhin ist der Mensch Akteur bei der Aufgabenteilung, wo auch Änderungen im Datenbestand durch handelnde Personen möglich sind, und den Integritätsprüfungen, bei denen Vorgänge nicht allein durch IT-Systeme geprüft werden dürfen. Auf Grund des heterogenen Teilnehmerkreises sind es vor allem die von den Teilnehmern zu erbringenden fälschungssicheren Beweise, die den Menschen aktiv als Sicherheitsträger in das Gleichgewichtsmodell einbinden.
Als **Risiko** ist der Mensch vor allem dann zu betrachten, wenn er als „böswilliger Insider“ Gefahren verursacht und als Angreifer im Angriffsvektor *Social Engineering* vorkommt, vgl. Kapitel 2.2.3. Die vom Menschen ausgehenden Risiken können nicht allen über technische Wege minimiert werden, sondern auch durch Sensibilisierungs- und Schulungsmaßnahmen. Weiter fasst Simic zusammen, dass der Mensch eine entscheidende Rolle bei der Entwicklung, Implementierung und der Nutzbarkeit von Sicherheitsmaßnahmen spielt und sollte daher bereits bei der Konzeptionierung und Analyse von Sicherheit einbezogen werden. Simic begründet sicherheitseinträchtigendes Verhalten von Menschen durch fehlende Akzeptanz, sowie komplexe Verwendungsmöglichkeiten von IT-Sicherheitsmaßnahmen. Es muss von den Akteuren

verstanden werden, warum so gehandelt wird und sollte dabei einfach anzuwenden sein.
Als **Wissens- bzw. Kenntnisträger** fungiert der Mensch dann, wenn er in Analysevorgänge einbezogen wird. Durch das Einbinden als Kenntnisträger findet wiederum die Integration als Sicherheitsträger statt.
Die ProSA-Vorgehensweise für prozessorientierte Sicherheitsanalysen gliedert sich in sechs Arbeitsschritte, welche in Abbildung 4.1 dargestellt sind und wie folgt erläutert werden.

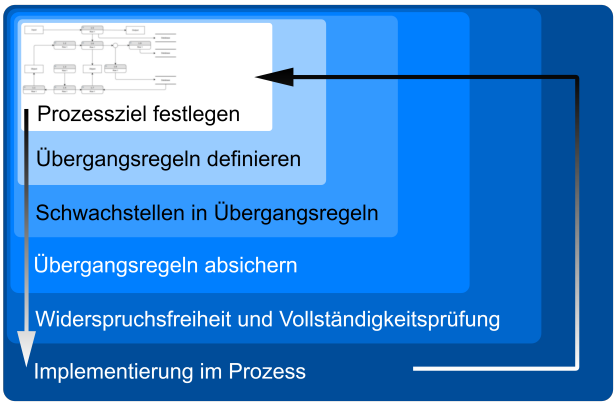

Abbildung 4.1: Schrittweise Durchführung von Sicherheitsanalysen nach ProSA (Eigene Darstellung)

Nach der Modellierung des zu untersuchenden Prozesses wird das **Prozessziel** im 1. Schritt festgelegt. Im 2. Schritt werden bereits die Wechselwirkungen zwischen Akteuren und Ressourcen in den **Übergangsregeln** beschrieben, da Aktivitäten Ereignisse auslösen. Die Übergangsregeln werden u.a. durch Akteure in Ihrer Funktion als Wissensträger mitgestaltet. Die Übergangsregeln als Ergebnisse aus diesem Schritt dienen als Grundlage für die **Bedrohungsanalyse** im 3. Schritt. Hier werden neben den technischen Schwachstellen, auch Interessenskonflikte der Akteure berücksichtigt, welche aus berechtigten und ungeberechtigten Interessen resultieren. Eine Bedrohung besteht dann, wenn ein Akteur in einem Interessenskonflikt technische Schwachstellen ausnutzt. Im 4. Schritt werden für jede untersuchte Übergangsregel **Sicherheitsanforderungen** abgeleitet und im 5. Schritt auf ihre **Vollständigkeit und Widerspruchsfreiheit** geprüft. „Die Vollständigkeit der Anforderungen wird in Bezug auf die Bedrohungen (verursacht durch Interessenskonflikte in Verbindung mit Schwachstellen) sichergestellt“. Im letzten Schritt erfolgt die **Implementierung** der Sicherheitsmaßnahmen in den untersuchten Prozess. Um eine stetige Verbesserung des Prozesses zu erwirken, sollten die Schritte kontinuierlich wiederholt werden.

4.2.2 Vorgehen der ProSA am Beispiel

Am Beispiel des IT-Sicherheitskriterium *Authentifizierung und Autorisierung* soll eine Sicherheitsanalyse nach der ProSA-Vorgehensweise durchgeführt werden. Als Grundlage für die Analyse wird das IT-Sicherheitskriterium in einem verallgemeinerten Geschäftsprozess in der Business Process Management Notation (BPMN) der Version 2.0 erstellt, vgl. Abbildung 4.2. Mit der Modellierungssprache BPMN ist es u.a. möglich, aus den Abgrenzungen der Abstraktionsebenen ‚fachlich' und ‚technisch' ganzheitliche Ansätze in ausführbare Modelle zu verfeinern [Gad17].

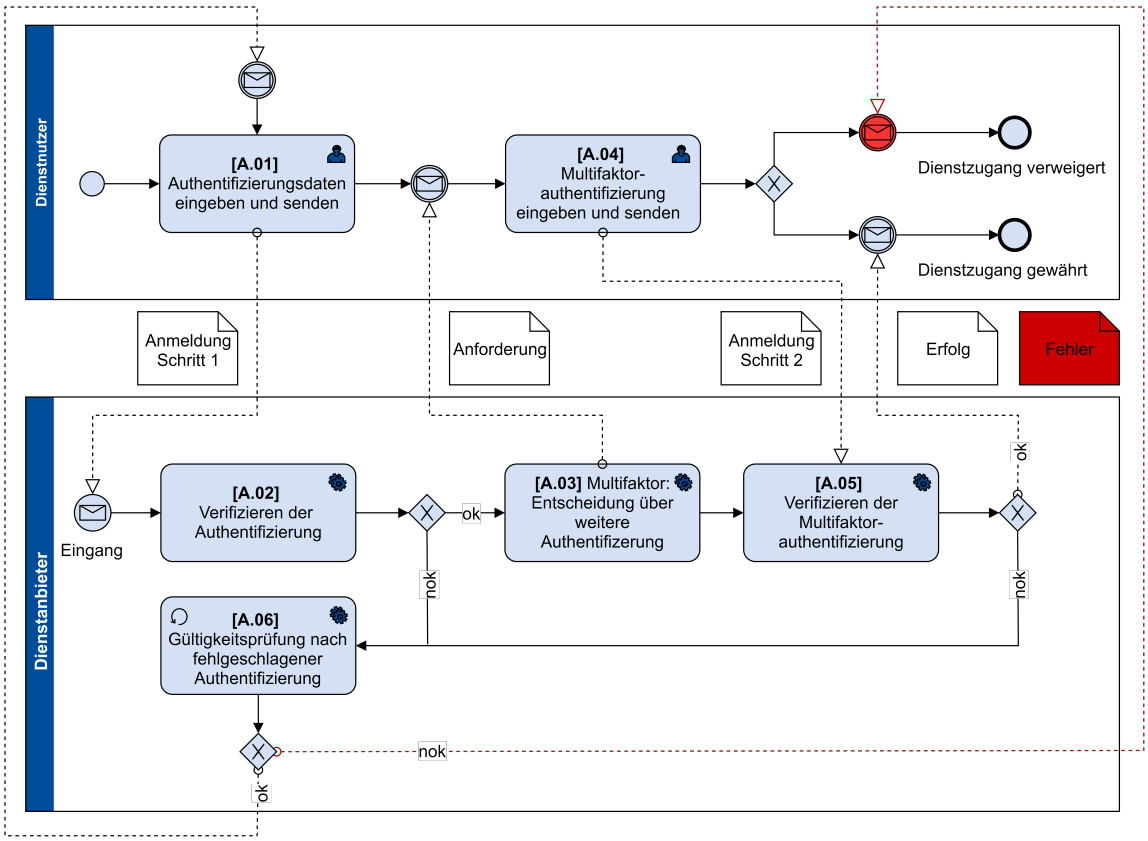

Abbildung 4.2: allgemeiner Prozess der *Authentifizierung und Autorisierung* (Eigene Darstellung)

Aufbauend auf diesen Geschäftsprozess werden die sechs Schritte der ProSA-Vorgehensweise angewendet, vgl. Abschnitt 4.2.1.
Beginnend mit dem **1. Schritt** wird aus dem Prozess ein Prozessziel definiert:

Zugang zu einem Dienst eines informationstechnischen Systems

Aus dem Prozess können zwei Akteure ermittelt werden, deren Interessen es zu bewerten gilt:

- Dienstnutzer:
  Interesse des Dienstnutzers, die Dienstleistung nach den für ihn zugesicherten Berechtigungen zu nutzen
- Dienstanbieter:
  Interesse zufriedener Kunden, indem der Dienst störungs- und stressfrei nutzbar ist

Auch wenn nach dem Geschäftsprozess aus Abbildung 4.2 der Akteur Dienstnutzer ausschließlich mit einem technischen System interagiert, wird der Akteur Dienstanbieter stellvertretend für das technische System benannt. Auf Grund der besseren Lesbarkeit werden anstelle der formalen Bezeichnung Dienstenutzer auch die Begriffe Nutzer oder Kunde geführt.
Den Akteuren werden nun subjektive Interessen unterstellt, die den Prozess unter Ausnutzen von Schwachstellen gefährden können:

- Dienstnutzer:
  Mögliche Motivationen könnten das Ausweiten der Rechte sein, um höherwertigere Dienste in Anspruch zu nehmen
- Dienstanbieter:
  Für Dienstanbieter könnte die Motivation dahingehend bestehen, die Daten seiner Kunden zu verkaufen

Simic teilt den Motivationsgrad in niedrige, mittlere und hohe Motivation ein. Für die beiden Akteure wird eine mittlere Motivation angenommen, was in einem Bereich von 30 Prozent bis 60 Prozent einer Wahrscheinlichkeit zum Regelbruch entsprechen soll. Externe Angreifer als Akteure sind hier nicht zu berücksichtigen, da diese am Prozess nicht beteiligt sind. Die visualisierte Darstellung dieser Motivationen und Beteiligungen lässt sich angelehnt an Simic folgendermaßen abbilden:

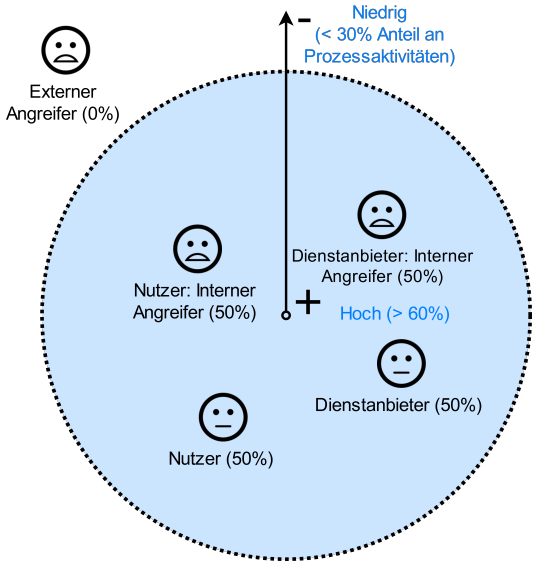

Abbildung 4.3: Beteiligung und Motivation der Akteure in der ProSA-Vorgehensweise (Eigene Darstellung in Anlehnung an [Sim17])

Im **nächsten Schritt** werden die Übergangsregeln in den Aktivitäten bestimmt. Diese werden formal beschrieben und stützen sich auf den Prozess aus Abbildung 4.2. Dabei werden in den Übergangsregeln die Akteure und deren Handlungen in Bezug auf die Objekte beschrieben. In jeder Übergangsregel wird mindestens ein Akteur beschrieben, wobei Akteure auch Komponenten technischer Systeme darstellen können. Damit werden auch automatisierte Vorgänge beschrieben.
Als Notation für die formalisierte Beschreibung wird eine von Simic angepasste Form der ECAA-Regeln (**E**vent of **C**ondition do **A**ction else do **A**lternative Action) verwendet. Die gewählte Syntax besteht aus formalisierten Geschäftsprozessregeln mit SQL-ähnlichen Sprachkonstrukten, die nach Simic „eine gute Balance zwischen ausreichendem Formalisierungsgrad und einer auch für technischen Laien guten Verständlichkeit gegeben ist.“ [Sim17]. In der Syntax werden folgende Elemente verwendet:

- Aktivität (engl. Activity): *[A.m]*
- Schwachstelle (engl. Vulnerability): *V [A.m_Rn.a].Bezeichner.Schwachstelle*
- Bedrohung (engl. Threat): *T [A.m_Rn.a].Bezeichner.Bedrohung*

[A.01] Authentifizierungsdaten eingeben und senden: Aus der Entscheidung heraus, einen Dienst eines informationstechnischen Systems Nutzen zu wollen, wird zunächst der Dienst aufgerufen. Nach der Eingabe und Bestätigung der Authentifizierungsdaten wird an das IT-System des Dienstanbieters eine Nachricht, mit der Anforderung zum Dienstzugang, gesendet. Das lässt sich wie folgt formalisieren:

```
ActivityID [A.01] Authentifizierungsdaten eingeben und senden
ON Event IT-Dienst nutzen
IF Condition <Akteur: Nutzer> hat entschieden einen Dienst eines informationstechnischen
    Systems <Ressource: IT-Dienst> eines bestimmten Anbieters <Akteur: Dienstanbieter>
    zu nutzen

    THEN DO Action
        {(
        [A.01_R1] <IT-System: allgemeiner Dienst> zeigt <Datenobjekt:
        ITDienst.Anmeldeformular>,
        [A.01_R2] <Akteur: Nutzer> gibt <Datenobjekt: AuthDaten.Nutzer> in <Datenobjekt:
        ITDienst.Anmeldeformular> ein,
        [A.01.R3] <Akteur: Nutzer> bestätigt <Datenobjekt:
        ITDienst.Anmeldeformular.Button="Anmelden">,
        [A.01.R4] <IT-System: allgemeiner Dienst> sendet <Datenobjekt:
        Anmeldedaten.Nutzer> an <IT-System: allgemeiner Dienst.Verifizierungsmodul>
        )}
    FOR Event Authentifizierungsdaten eingegeben und senden

    ELSE DO Alternative Action
        [A.01_R5] <Akteur: Nutzer> bricht [A.01] ab
    FOR Alternative Event Vorgang abgebrochen
```

Listing 4.1: Übergangsregeln der Aktivität [A.01]

[A.02] Verifizieren der Authentifizierung: Nachdem der Dienstanbieter die Anfrage zur Nutzung des Dienstes in Form der Zugangsdaten erhalten hat, können diese nun mittels eines Authentifizierungsmoduls verifiziert werden. Wurden die Daten erfolgreich verifiziert und auf ihre Gültigkeit geprüft, sendet das Authentifizierungsmodul eine Erfolgsmeldung an das Multifaktormodul. Anderenfalls wird eine Nachricht über eine erfolglose Authentifizierung an ein Modul gesendet, dass für Entscheidungen über Abbruch oder Wiederholung der Authentifizierung verantwortlich ist.

Formalisiert augedrückt bedeutet das:

```
ActivityID [A.02] Verifizieren der Authentifizierung
ON Event Authentifizierungsdaten erhalten
IF Condition -

    THEN DO Action
        {(
        [A.02_R1] <IT-System: allgemeiner Dienst.Verifizierungsmodul> prüft
        <Datenobjekt: Anmeldedaten.Nutzer>
        IF Condition <Datenobjekt: Anmeldedaten.Nutzer.true>
        THEN DO Action
```

```
            (
            [A.02_R2] <IT-System: allgemeiner Dienst.Verifizierungsmodul> sendet
            Nachricht <Datenobjekt: Anmeldedaten.Nutzer.true> an
            <IT-System: allgemeiner Dienst.Multifaktormodul>
            )
        IF Condition <Datenobjekt: Anmeldedaten.Nutzer.false>
        THEN DO Action
            (
            [A.02_R3] <IT-System: allgemeiner Dienst.Verifizierungsmodul> sendet
            Nachricht <Datenobjekt: Anmeldedaten.Nutzer.false> an
            <IT-System: allgemeiner Dienst.Authentifizierung_Wdh.>
            )
        )}
    FOR Event Validität der Anmeldedaten

    ELSE DO Alternative Action
        [A.02_R4] <IT-System: allgemeiner Dienst bricht [A.02] ab
    FOR Alternative Event Vorgang abgebrochen
```

Listing 4.2: Übergangsregeln der Aktivität [A.02]

[A.03] Multifaktor: Entscheidung über weitere Authentifizierung: Nachdem das Verifizierungsmodul eine Nachricht über die positive Validität der Nutzerauthentifizierung an das Multifaktormodul gesendet hat, entscheidet dieses auf Basis von Algorithmen und Pseudozufallsprinzipien, die in Form einer weiteren Authentifizierung durch den Nutzer zu erbringen ist. Das Ergebnis schickt das Multifaktormodul an den Nutzer.
Formalisiert wird das wie folgt beschrieben:

```
ActivityID [A.03] Entscheidung über weitere Authentifizierung
ON Event Multifaktormodul empfängt Nachricht = ok vom Verifizierungsmodul
IF Condition -

    THEN DO Action
        {(
        [A.03_R1] <IT-System: allgemeiner Dienst.Multifaktormodul> entscheidet über
        weitere Authentifizierungsmethode,
        [A.03_R2] <IT-System: allgemeiner Dienst.Multifaktormodul> sendet Nachricht
        <Datenobjekt: Multifaktorauthentifizierung.Form> an <Akteur: Nutzer>
        )}
    FOR Event Wahl der Multifaktorauthentifizierung

    ELSE DO Alternative Action
        [A.03_R3] <IT-System: allgemeiner Dienst bricht [A.03] ab
    FOR Alternative Event Vorgang abgebrochen
```

Listing 4.3: Übergangsregeln der Aktivität [A.03]

[A.04] Multifaktorauthentifizierung eingeben und senden: Der Nutzer hat vom Multifaktormodul eine Nachricht erhalten nach welcher Methode er eine Multifaktorauthentifizierung durchführen soll. Als Beispiele können hier Verfahren für

Transaktionsnummer (TAN) oder Technologien wie Zertifikate genutzt werden. Formalisiert lässt sich der allgemeine Ablauf, ähnlich zur Aktivität [A.01] beschreiben:

```
ActivityID [A.04] Multifaktor-Authentifizierungsdaten eingeben und senden
ON Event IT-Dienst nutzen
IF Condition <Akteur: Nutzer> erhält vom System <IT-System: allgemeiner Dienst.
    Multifaktormodul> die Aufforderung zu einer weiteren bestimmten
    Authentifizierungsmethode

    THEN DO Action
        {(
        [A.04_R1] <IT-System: allgemeiner Dienst> zeigt <Datenobjekt:
        ITDienst.Multifaktor-Anmeldeformular>,
       [A.04_R2] <Akteur: Nutzer> gibt <Datenobjekt: AuthDatenMF.Nutzer>
        in <Datenobjekt: ITDienst.Multifaktor-Anmeldeformular> ein,
        [A.04.R3] <Akteur: Nutzer> bestätigt <Datenobjekt:
        ITDienst.Multifaktor-Anmeldeformular.Button="Anmelden">,
        [A.04.R4] <IT-System: allgemeiner Dienst> sendet <Datenobjekt:
        AnmeldedatenMF.Nutzer> an <IT-System: allgemeiner
        Dienst.Verifizierungsmodul_MF>
        )}
    FOR Event weitere Authentifizierungsdaten eingegeben und senden

    ELSE DO Alternative Action
        [A.04_R5] <Akteur: Nutzer> bricht [A.04] ab
    FOR Alternative Event Vorgang abgebrochen
```

Listing 4.4: Übergangsregeln der Aktivität [A.04]

[A.05] Verifizieren der Multifaktor-Authentifizierung: Nachdem der Dienstanbieter die Zugangsdaten für die Multifaktorauthentifizierung erhalten hat, können diese nun mittels eines Multifaktor-Authentifizierungsmoduls verifiziert werden. Wurden die Daten erfolgreich verifiziert, so erhält der Nutzer eine Nachricht und den Zugang zum angeforderten IT-Dienst. Im Fall einer fehlerhaften Authentifizierung wird die Information an die Gültigkeitsprüfung weitergegeben.
Die Übergänge in der Aktivität sind ähnlich denen in [A.02] und lassen sich formalisiert wie folgt darstellen:

```
ActivityID [A.05] Verifizieren der Multifaktor-Authentifizierung
ON Event Multifaktor-Authentifizierungsdaten erhalten
IF Condition -

    THEN DO Action
        {(
        [A.05_R1] <IT-System: allgemeiner Dienst.Verifizierungsmodul_MF> prüft
        <Datenobjekt: Anmeldedaten_MF.Nutzer>
        IF Condition <Datenobjekt: Anmeldedaten_MF.Nutzer.true>
        THEN DO Action
            (
            [A.05_R2] <IT-System: allgemeiner Dienst.Verifizierungsmodul_MF> sendet
            Nachricht <Datenobjekt: Anmeldedaten_MF.Nutzer.true> an
```

```
            <IT-System: allgemeiner Dienst.Multifaktormodul>
            )
        IF Condition <Datenobjekt: Anmeldedaten_MF.Nutzer.false>
        THEN DO Action
            (
            [A.05_R3] <IT-System: allgemeiner Dienst.Verifizierungsmodul_MF> sendet
            Nachricht <Datenobjekt: Anmeldedaten_MF.Nutzer.false> an
            <IT-System: allgemeiner Dienst.Authentifizierung_Wdh.>
            )
        )}
    FOR Event Validität der Multifaktor-Anmeldedaten

    ELSE DO Alternative Action
        [A.05_R4] <IT-System: allgemeiner Dienst bricht [A.05] ab
    FOR Alternative Event Vorgang abgebrochen
```

Listing 4.5: Übergangsregeln der Aktivität [A.05]

[A.06] Gültigkeitsprüfung nach fehlgeschlagener Authentifizierung: Ist die Authentifizierung fehlgeschlagen, sollen Algorithmen anhand verschiedener Faktoren, wie der Häufigkeit von Fehlschlägen, den Zeitabständen zwischen den Fehlschlägen, der Herkunft, Validität und Konsistenz von Quell-IP-Adressen, prüfen, ob der Nutzer die Zugangsdaten erneut eingeben darf. Als Fehlschläge gelten nicht nur Systemfehler. Vor allem sind diese anhand fehlerhaft eingegebener Nutzerdaten zu bewerten.

Im Fall einer Positiventscheidung des Moduls wird der Nutzer erneut aufgefordert seine Zugangsdaten einzugeben, beginnend mit der ersten Zugangsmethode. Bei einer Negativentscheidung wird der Nutzer entsprechend auf alternativ hinterlegten Benachrichtigungsmethoden über das Fehlschlagen informiert. Zudem wird der Zugang zunächst für einen temporären Zeitraum gesperrt.

Die Formalisierung dieser Übergangsregel ist wie folgt beschrieben:

```
ActivityID [A.06] Gültigkeitsprüfung nach fehlgeschlagener Authentifizierung
ON Event Authentifizierung fehlgeschlagen
IF Condition Nachricht <Datenobjekt: Anmeldedaten.Nutzer.false> || <Datenobjekt:
    Anmeldedaten_MF.Nutzer.false>

    THEN DO Action
        {(
        [A.06_R1] <IT-System: allgemeiner Dienst.Gültigkeitsprüfung> ermittelt
        Ergebnis
        IF Condition <IT-System: allgemeiner Dienst.Gültigkeitsprüfung.ok>
        THEN DO Action
            (
            [A.06_R2] <IT-System: allgemeiner Dienst.Gültigkeitsprüfung> sendet
            Nachricht <Datenobjekt: Authentifizierung.Form>
            an <Akteur: Nutzer>
            )
        IF Condition <IT-System: allgemeiner Dienst.Gültigkeitsprüfung.false>
        THEN DO Action
```

```
            (
            [A.06_R3] <IT-System: allgemeiner Dienst.Gültigkeitsprüfung>
            sperrt Zugang für <Akteur: Nutzer>,
            [A.06_R4] <IT-System: allgemeiner Dienst.Gültigkeitsprüfung>
            sendet Nachricht <Datenobjekt: Authentifizierung.Fehlerinformation>
            an <Akteur: Nutzer.Fallback>
            )
        )}
    FOR Event Gültigkeitsprüfung nach fehlgeschlagener Authentifizierung

    ELSE DO Alternative Action
        [A.06_R5] <IT-System: allgemeiner Dienst bricht [A.06] ab
    FOR Alternative Event Vorgang abgebrochen
```

Listing 4.6: Übergangsregeln der Aktivität [A.06]

Aus diesen Übergangsregeln kann nun im **3. Schritt** die Untersuchung auf Schwachstellen erfolgen. Diese Untersuchung wird nach Simic zunächst verbal beschrieben. Auch wenn der externe Angreifer im Geschäftsprozess keine Beteiligung hat, wird er für die Ermittlung der Schwachstellen hinzugezogen [Sim17]. Dieser Umstand wird im Kapitel 5.1.3 herangezogen und fließt somit in die Bewertung dieser Methode ein.

Simic nutzt die verbale Beschreibung für die zu ermittelnden Schwachstellen und deren Bedrohung zur Diskussion. Auf Grund des großen Umfangs der verbalen Beschreibungen und der Redundanzen der gleichartigen Übergangsregeln der Aktivitäten [A.01] und [A.04], sowie [A.02] und [A.05], wird an dieser Stelle auf die verbale Beschreibung verzichtet. Zwar wird jede einzelne Übergangsregel auf ihre Schwachstellen untersucht, jedoch für eine bessere Übersichtlichkeit gruppiert in der folgenden Tabelle 4.1 dargestellt:

Schwachstelle [V.o].Bezeichner	Bedrohung [T.p].Bezeichner	Aktivität [A.q].Bezeichner
[V.01].KonfigITDienst	[T.01].DoS	[A.01_R1].ITDienst_Anmeldeformular [A.04_R1].ITDienst_Anmeldeformular
[V.02].Nutzereingabe	[T.02].SQL-Injection	[A.01_R2].Dateneingabe [A.01_R3].Anmelden_ausführen [A.01_R4].Datenobjekt_senden [A.04_R2].Dateneingabe [A.04_R3].Anmelden_ausführen [A.04_R4].Datenobjekt_senden
[V.03].Datenübertragung	[T.03].Man_In_the_Middle	[A.01_R4].Datenobjekt_senden [A.03_R2].Datenobjekt_senden [A.04_R4].Datenobjekt_senden [A.06_R2].Datenobjekt_senden [A.06_R4].Datenobjekt_senden
[V.04].NutzerSensibilisierung	[T.04].Phishing	[A.01_R1].ITDienst_Anmeldeformular [A.01_R2].Dateneingabe [A.01_R3].Anmelden_ausführen [A.04_R1].ITDienst_Anmeldeformular [A.04_R2].Dateneingabe [A.04_R3].Anmelden_ausführen
[V.05].Verifizierung	[T.05].Kompromittierungen	[A.02_R1].Anmeldedaten_prüfen [A.02_R2].Intern_senden_true [A.02_R3].Intern_senden_false [A.03_R1].Intern_Algorithmus [A.05_R1].Anmeldedaten_prüfen [A.05_R2].Intern_senden_true [A.05_R3].Intern_senden_false [A.06_R1].Intern_Algorithmus [A.06_R3].Zugang_sperren
[V.06].Entwicklung	[T.06].Softwarefehler	[A.02_R1].Anmeldedaten_prüfen [A.02_R2].Intern_senden_true [A.02_R3].Intern_senden_false [A.03_R1].Intern_Algorithmus [A.05_R1].Anmeldedaten_prüfen [A.05_R2].Intern_senden_true [A.05_R3].Intern_senden_false [A.06_R1].Intern_Algorithmus

Tabelle 4.1: Schwachstellen und Bedrohungen am ProSA-Beispiel

Die in diesem Schritt ermittelten Schwachstellen und Bedrohungen können grundlegend in zwei Bereiche unterteilt werden, einen Bereich für die *inneren Sicherheitsanforderungen* und einen Bereich für die *äußeren Sicherheitsanforderungen*. Der Bereich der *inneren Sicherheitsanforderungen* umfasst alle Komponenten, die ein geschlossenes IT-System betreffen. Als Beispiele seien hier interne Prozesskommunikationen oder der Betrieb von Hard- und Softwarekomponenten innerhalb des Betriebssystems benannt. Der Bereich der *äußeren Sicherheitsanforderungen* behandelt Anforderungen an eine offene Kommunikation in unsicheren Netzen, sowie menschliche Interaktionen mit IT-Systemen. Beispiele hierfür sind, das Eingeben und Übermitteln von Nutzerdaten zur Authentifizierung an das System oder Benachrichtigungen aus dem System an die Benutzer.

Im **4. Schritt** werden die Sicherheitsanforderungen spezifiziert und Maßnahmen

für deren Erfüllung vorgeschlagen. In ihren Beispielen beschreibt Simic die Sicherheitsanforderungen und Maßnahmen elementar für jede Übergangsregel. Von diesem Detailgrad wird an der Stelle abgewichen. Zudem behandelt Simic auch Maßnahmen die bereits umgesetzt sind. An einem Beispiel bezieht sie sich auf die Maßnahme der Zugriffskontrolle des Systems auf die Sicherheitsanforderung. Es ist ein Berechtigungsnachweis durch die Benutzer beim Anmelden zu erbringen. Im Folgenden werden nur solche Sicherheitsanforderungen und Maßnahmen behandelt, welche sich direkt auf die im vorangegangen Schritt ermittelten Schwachstellen und deren Bedrohungen beziehen. Die Ergebnisse sind in Tabelle 4.2 dargestellt.

Anforderung [Req.n].Bezeichner	Schwachstelle [V.o].Bezeichner	Bedrohung [T.p].Bezeichner	Maßnahmen [M.r].Bezeichner
[Req.01].VerfügbarkeitIT-Dienst	[V.01].KonfigITDienst	[T.01].DoS	[M.01].Redundanz
[Req.01].VerfügbarkeitIT-Dienst [Req.02].VertraulichkeitIT-Dienst [Req.03].IntegritätIT-Dienst	[V.02].Nutzereingabe	[T.02].SQL-Injection	[M.02].Eingabeprüfung [M.03].Limitierung
[Req.02].VertraulichkeitIT-Dienst [Req.03].IntegritätIT-Dienst	[V.03].Datenübertragung	[T.03].Man_In_the_Middle	[M.04].Transportverschlüsselung
[Req.02].VertraulichkeitIT-Dienst [Req.03].IntegritätIT-Dienst	[V.04].NutzerSensibilisierung	[T.04].Phishing	[M.05].NutzerSenibilisierung
[Req.03].IntegritätIT-Dienst	[V.05].Verifizierung	[T.05].Kompromittierungen	[M.06].SichereSoftwareentwicklung
[Req.03].IntegritätIT-Dienst	[V.06].Entwicklung	[T.06].Softwarefehler	[M.06].SichereSoftwareentwicklung

Tabelle 4.2: Anforderungen und Maßnahmen am ProSA-Beispiel

Resultierend aus diesem Schritt kann festgestellt werden, dass sich in diesem Beispiel alle Sicherheitsanforderungen mit den allgemeinen Schutzzielen der IT-Sicherheit beschreiben lassen, vgl. Kapitel 2.2.1. Entscheidend sind allerdings die Maßnahmen, die sich typischerweise aus den Bedrohungen ergeben.

Der **5. Prozessschritt** behandelt die Vollständigkeit und Widerspruchsfreiheit, siehe das Vorgehen nach der ProSA-Methode aus Abschnitt 4.2.1. Sicherheitsanforderungen sind nicht losgelöst von den zugrundeliegenden Aktivitäten zu betrachten. Vollständigkeit ist dann gegeben, wenn jede abgeleitete Bedrohung mindestens durch eine Sicherheitsanforderung abgefangen wird, d.h. die Vollständigkeit ergibt sich aus der Bedrohungsmenge [Sim17]. Diese Beziehung kann in Tabelle 4.2 aus dem vorangegangenen Schritt gezeigt werden. Bei der Widerspruchsfreiheit prüft Simic Anforderungen, die sich gegenseitig ausschließen. Ein Widerspruch kann sich bereits in den Anforderungen ergeben, da dort keine Prüfung auf Widerspruchsfreiheit durchgeführt wird. Ein Beispiel für einen Widerspruch ist die Anforderung an eine anonyme und nachvollziehbare Kommunikation. Weitere Untersuchungen dieses Schrittes werden im Beispiel nicht durchgeführt, da bereits im 3. Schritt eine geänderte Vorgehensweise nach der ProSA-Methode verfolgt wurde.

Der **6. Schritt** der ProSA-Vorgehensweise sieht die Implementierung vor. Auf Grund des abstrahierten Beispiels kann an der Stelle keine Implementierung in den Prozess gezeigt werden. Das Beispiel sollte die Vorgehensweise an einem IT-Sicherheitskriterium veranschaulichen. Eine Bewertung dieser Methode wird im Kapitel 5.1.3 behandelt.

4.3 IT-Sicherheit nach dem IT-Grundschutz des BSI

Mit dem BSI-Standard 200-2 bietet das BSI eine Methodik die dabei unterstützt, effektives Management von Informationssicherheit herzustellen. Dabei richtet sich dieser Standard an alle Institutionen, unabhängig von deren Art oder Größe. Um Informationssicherheit herstellen zu können, werden nach diesem Vorgehen Prozesse durchlaufen, welche Aktivitäten auf organisatorischen und technischen Ebenen erfordern. Nachdem die organisatorischen Prozessphasen *Initiierung des Sicherheitsprozesses*, *Erstellen der Leitlinie zur Informationssicherheit* und *Organisation des Sicherheitsprozesses* durch die Leitungsebene durchgeführt wurden, folgen die Prozessphasen *Erstellen einer Sicherheitskonzeption*, *Umsetzung einer Sicherheitskonzeption*, sowie die *Aufrechterhaltung und Verbesserung* auf operativer Ebene. Während dieser Prozessphasen entstehen eine Vielzahl von Dokumenten, wie Berichte, Konzepte, Richtlinien und Meldungen über sicherheitsrelevante Ereignisse. Diese Aufgabe sollte neben anderen Aufgaben, wie der Steuerung des Informationssicherheitsprozesses, der Initiierung und Überprüfung von Sicherheitsmaßnahmen oder der Berichterstattung an die Leitungsebene, durch Informationssicherheitsbeauftragte (ISB) wahrgenommen werden [BSI17b].
In den folgenden Absätzen wird die Prozessphase *Erstellen einer Sicherheitskonzeption* beschrieben, da dieser Phase für das Überprüfen der konzeptionierten IT-Sicherheitskriterien aus Kapitel 3.2 angewendet wird.
Die Erarbeitung von IT-Sicherheitsrichtlinien auf operativer Ebene erfolgt in Kombination mit dem IT-Grundschutz-Kompendium, welches beim Erstellen dieser Arbeit in Version 7.0 - 2019 vorliegt [BSI19b]. Um Sicherheitsanforderungen des typischerweise heterogenen Vorkommens der in den verschiedensten Institutionen eingesetzten IT-Systeme und Anwendungen auf einheitliche Art abbilden zu können, ist das IT-Grundschutz-Kompendium nach einem Baukastenprinzip strukturiert. Dabei bilden sogenannte Bausteine das Fundament und beinhalten typische Bereiche und Bedürfnisse der Informationssicherheit von Institutionen. Das umfasst sowohl übergeordnete Themen wie das IS-Management, die Datensicherung und die Notfallvorsorge, aber auch spezifische Anforderungen an ICS-Umgebungen. Die Bau-

steine werden dabei in prozessorientierte und systemorientierte Bausteine unterteilt. Im BSI Standard 200-2 heißt es: „Das IT-Grundschutz-Kompendium beschreibt die spezifische Gefährdungslage und die Sicherheitsanforderungen für verschiedene Komponenten, Vorgehensweisen und Systeme, die jeweils in einem Baustein zusammengefasst sind.“ [BSI17b].

Um IT-Sicherheitsrichtlinien zu erstellen, ist es zunächst notwendig ein anzustrebendes Sicherheitsniveau festzulegen. Das Sicherheitsniveau ergibt sich aus dem Schutzbedarf der schützenswerten Daten informationsverarbeitender Systeme. Die Methodik BSI-Standard 200-2 unterscheidet die Sicherheitsniveaus in das Niveau der Basis-Absicherung, der Standard-Absicherung und der Kern-Absicherung. Das Sicherheitsniveau der Basis-Absicherung stellt dabei einen Einstieg dar und bildet die Grundlage für die anderen beiden Sicherheitsniveaus. Mit dem Sicherheitsniveau der Standard-Absicherung wird ein nach dem IT-Grundschutz vorgesehener ganzheitlicher Ansatz verfolgt, indem das Niveau durch geeignete Umsetzung von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen erreicht werden kann. Die Kern-Absicherung zielt auf besonders schützenswerte Daten und den Schutz kritischer Geschäftsprozesse ab, die damit vorrangig geschützt werden sollen [BSI17b]. Die Beschreibung für die Kern-Absicherung lässt den Schluss zu, dass es sich dabei immer um Daten mit einem höheren Schutzbedarf handelt.

Die Vorgehensweisen für das Erstellen von Sicherheitsrichtlinien für unterschiedliche Sicherheitsniveaus unterscheiden sich kaum. Einige Schritte sind bei allen drei Sicherheitsniveaus gleich. Es sind Zusammenhänge und Abhängigkeiten erkennbar, die in einer Gegenüberstellung in Abbildung 4.4 dargestellt sind.

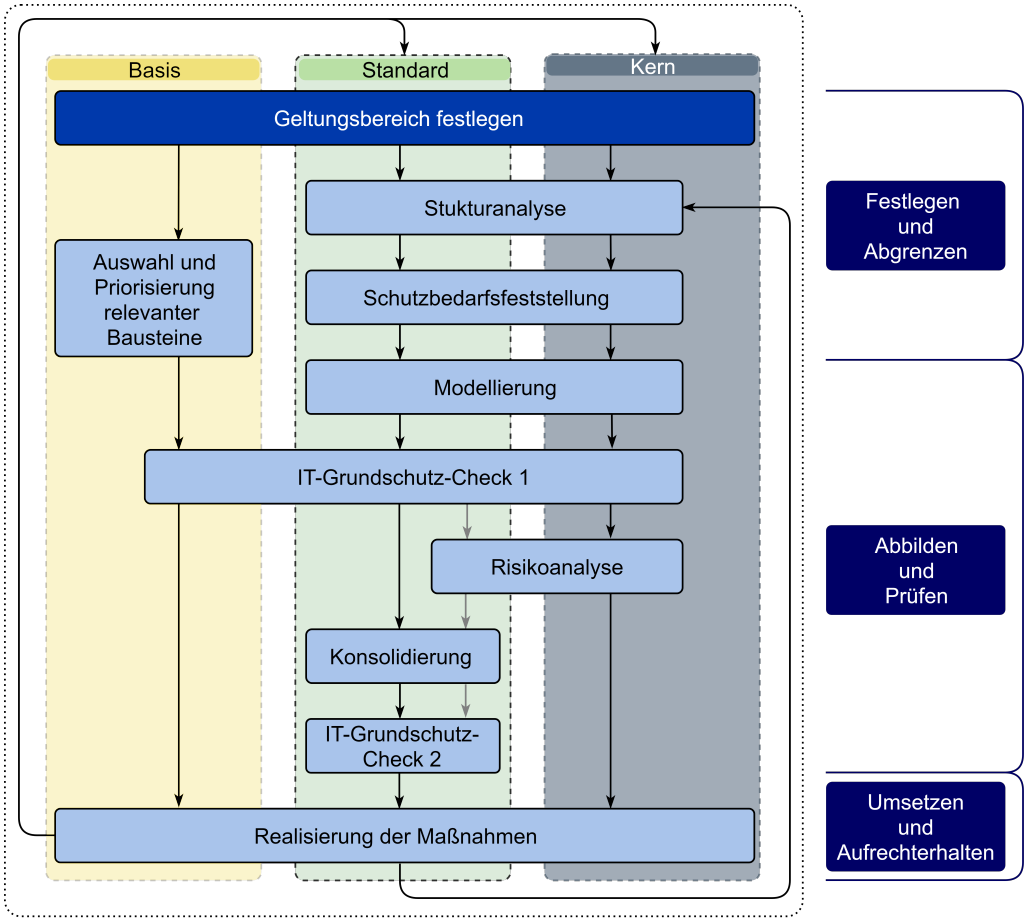

Abbildung 4.4: operatives Vorgehen nach IT-Grundschutz (Eigene Darstellung)

Aus den Zusammenhängen können allgemeine Arbeitsschritte zusammengefasst werden, welche immer durchlaufen werden müssen und sich nur in ihren Ausprägungen unterscheiden. Unabhängig vom anzustrebenden Sicherheitsniveau müssen immer die Phasen *Festlegen und Abgrenzen*, *Abbilden und Prüfen*, sowie *Umsetzen und Aufrechterhalten* bearbeitet werden.

4.3.1 Erstellen einer IT-Sicherheitsrichtlinie am Beispiel

Neben der Sicherheitsleitlinie als zentrales Element, gehören IT-Sicherheitskonzepte und IT-Sicherheitsrichtlinien zu den wichtigen Dokumenten in einem Informationssicherheitsprozess. An diesen Dokumenten kann Informationssicherheit aufgebaut und umgesetzt werden. IT-Sicherheitskonzepte und IT-Sicherheitsrichtlinien unterscheiden sich dadurch, dass in den Richtlinien die Grundzüge der organisationsweiten IT-Nutzung zielgruppenorientiert zusammengefasst sind und erforderliche Maßnahmen eines Sicherheitskonzeptes allgemeinverständlich und ohne technische Details

beschrieben werden. Die vom BSI angebotenen Praxisbeispiele für Sicherheitskonzepte und Sicherheitsrichtlinien unterscheiden sich allerdings nicht in ihrer Ausprägung auf den technischen Detaillierungsgrad [BSI08].
Um die Sicherheit einer spezifischen Anwendung oder eines bestimmtes IT-Systems zu verbessern, behandeln Sicherheitsrichtlinien die Maßnahmen für konkrete Produkte wie Tablets mit dem Betriebssystem *Windows 10*[1]. Ist zudem der Einsatz von *MacBooks*[2] mit dem Betriebssystem *macOS*[3] gefordert, so wird dafür jeweils eine separate Sicherheitsrichtlinie erstellt.
Durch eine allgemeine Sicherheitsrichtlinie, die mit verschiedenen wählbaren Optionen konkrete Einsatzszenarien und Produkte ähnlichen Typs abdeckt, könnte diesem Problem entgegengewirkt werden. Am folgenden Beispiel soll eine solche Richtlinie erstellt werden. Die Richtlinie wird dabei in einen *Allgemeinen Teil* und in einen *Modularen Teil* untergliedert. Der *allgemeine Teil* umfasst dabei ermittelte Gefährdungen, organisatorische Maßnahmen und verallgemeinerte technische Maßnahmen. Im *modularen Teil* werden Umsetzungshinweise der wählbaren Optionen mit technischen Sicherheitsmaßnahmen für bestimmte Einsatzszenarien und Produkte behandelt. Wählbare Optionen könnten am genannten Beispiel der Einsatz verschiedener Betriebssysteme sein. Würde eine modulare IT-Sicherheitsrichtlinie Netzwerkkomponenten behandeln, dann könnten die wählbaren Optionen, Geräte wie Router und Switches unterschiedlicher Hersteller mit unterschiedlichen Betriebssystemen sein. Der schematische Aufbau einer solchen Sicherheitsrichtlinie ist in Abbildung 4.5 dargestellt.

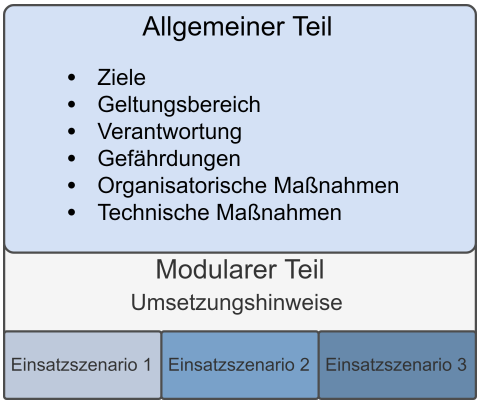

Abbildung 4.5: Aufbau einer modularen IT-Sicherheitsrichtlinie (Eigene Darstellung)

[1]https://www.microsoft.com/de-de/windows (letzter Zugriff: 2019-08-28)
[2]https://www.apple.com/de/mac/ (letzter Zugriff: 2019-08-28)
[3]https://www.apple.com/de/macos/mojave/ (letzter Zugriff: 2019-08-28)

Am folgenden Beispiel wird eine modulare IT-Sicherheitsrichtlinie nach dem IT-Grundschutz aufgebaut, welche die IT-Sicherheit der Sicherheitskriterien aus Kapitel 3 behandelt. Dafür wird eine angepasste Vorgehensweise für das Erstellen eines Sicherheitskonzeptes nach BSI-Standard 200-2 verwendet, welche das Ziel einer Standard-Absicherung verfolgt. Die im vorangegangenen Abschnitt 4.3 vorgeschlagenen allgemeinen Phasen für das Erstellen einer IT-Sicherheitsrichtlinie, werden mit folgenden operativen Arbeitsschritten der Basis-Absicherung und der Standard-Absicherung angewandt:

- Festlegen und Abgrenzen
  - Geltungsbereich festlegen
  - Schutzbedarf bestimmen
  - Auswahl und Priorisierung relevanter Bausteine
- Abbilden und Prüfen
  - Modellierung
  - angepasster IT-Grundschutz-Check
- Umsetzen und Aufrechterhalten
  - Zuordnen von technischen Maßnahmen

4.3.1.1 Festlegen und Abgrenzen

Zunächst wird der **Geltungsbereich** festgelegt. Der Geltungsbereich wird nach der Vorgehensweise des BSI auch als Informationsverbund bezeichnet und umfasst dabei die Gesamtheit aller beteiligten Komponenten, die zur Erfüllung der Aufgaben in einem festgelegten Anwendungsbereich der Informationsverarbeitung benötigt werden. Neben technischen Komponenten werden auch infrastrukturelle, organisatorische und personelle Komponenten in einem Informationsverbund eingebunden und zur Betrachtung hinzugezogen [BSI17b].
Der Informationsverbund wird idealisiert betrachtet und umfasst alle Definitionen und Beschreibungen von vernetzten Endgeräten, vgl. Kapitel 2.1. Die gewählte Bezeichnung des Informationsverbundes ist *Endgeräte*.
Ein weiterer Schritt in der 1. Phase ist die **Feststellung des Schutzbedarfs**. Die Feststellung des Schutzbedarfs verfolgt das Ziel, für die in den Geschäftsprozessen

verarbeiteten Informationen ausreichenden, sowie angemessenen Schutz zu gewährleisten. Dabei wird der bei Beeinträchtigung der Schutzziele, vgl. Kapitel 2.2.1, zu erwartende Schaden, der im Informationsverbund festgelegten Anwendungen, möglichst realistisch eingeschätzt. Der Schutzbedarf wird in drei Schutzbedarfskategorien unterteilt. In der Schutzbedarfskategorie *normal*, müssen definierte schutzbedürftige Daten intern bleiben, kleinere Fehler können toleriert werden und größere bzw. erhebliche Fehler müssen erkannt und vermieden werden können. Daten mit dem Schutzbedarf *hoch* beinhalten vertrauliche Informationen und Personendaten. Sind die Schutzziele dieser Daten beeinträchtigt, so ist die gesellschaftliche Stellung der Betroffenen gefährdet oder deren wirtschaftliche Verhältnisse erheblich beeinträchtigt. Bei der dritten und höchsten Schutzbedarfskategorie *sehr hoch*, handelt es sich um Daten bei deren Kompromittierung Leib und Leben der Betroffenen in Gefahr ist [BSI17b]. Dieser Fall könnte schnell zutreffen, wenn man bedenkt das vernetzte Herzschrittmacher zum Einsatz kommen [Han18].
Unabhängig vom Schutzbedarf ist die Verarbeitung personenbezogener Daten immer nach der Datenschutz-Grundverordnung (DSGVO)[4] zu prüfen.
Für das Erstellen von IT-Sicherheitsrichtlinien vernetzter Endgeräte wird von einem normalen Schutzbedarf ausgegangen und somit für weitere Bearbeitungsschritte festgelegt.
Der letzte Arbeitsschritt in der 1. Phase ist die **Auswahl und die Priorisierung relevanter Bausteine** aus dem IT-Grundschutz-Kompendium. Für diese Auswahl werden alle Bausteine betrachtet, welche auf den Geltungsbereich *Endgeräte* angewendet werden können. Dazu wird das vom BSI erstellte Mindmap ausgewertet und daraus eine angepasste Übersicht relevanter Bausteine erstellt. In Abbildung 4.6 sind alle in Frage kommenden Bausteine dargestellt, inklusive einer Priorisierung der Bearbeitung, wie sie in der Methodik des BSI vorgeschlagen wird [BSI19b]. Ausgewählte Bausteine wurden markiert.

[4] https://dsgvo-gesetz.de/ (letzter Zugriff: 2019-08-28)

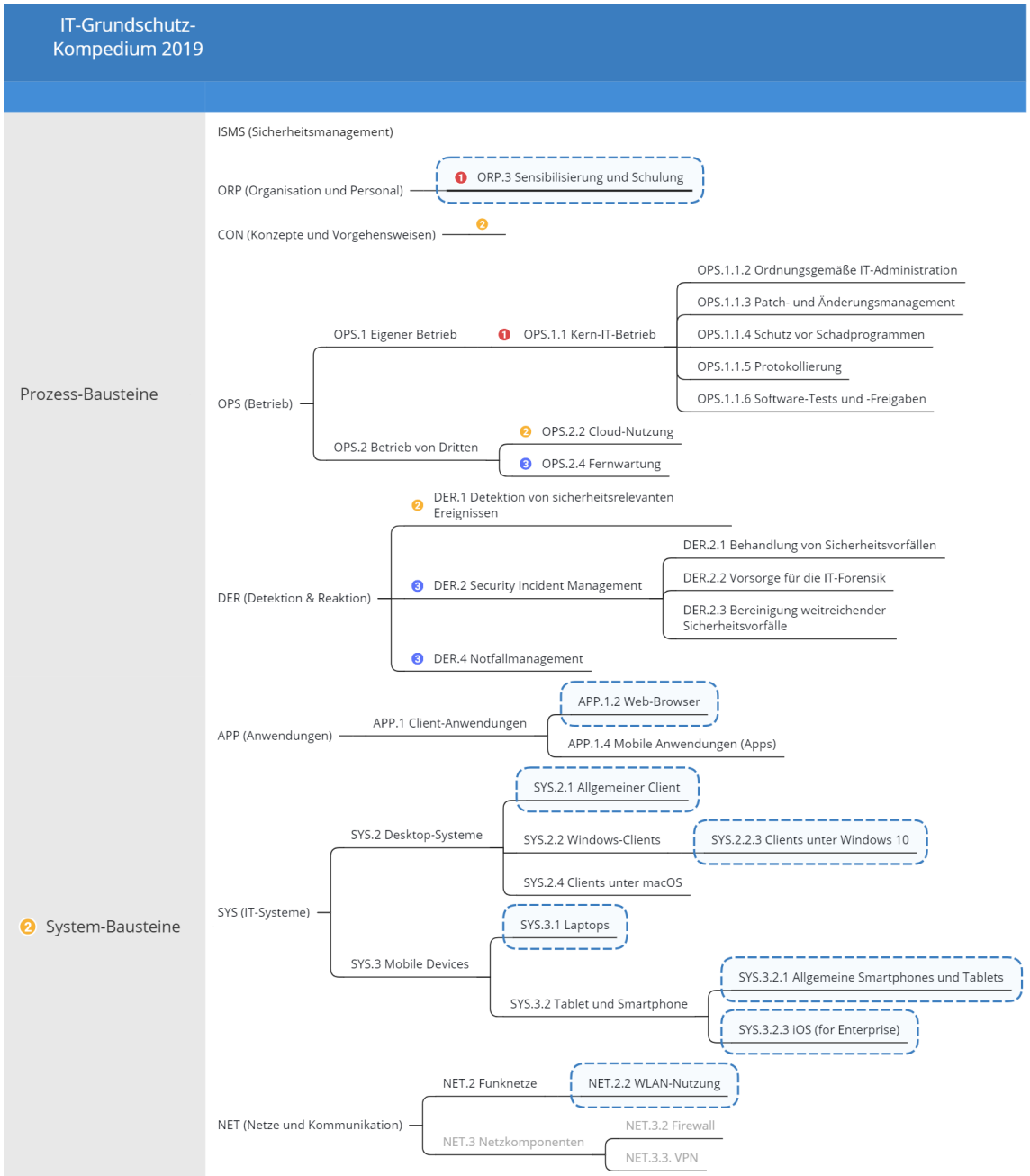

Abbildung 4.6: ausgewählte Bausteine aus dem IT-Grundschutz-Kompendium (Eigene Darstellung in Anlehnung an [BSI19b])

4.3.1.2 Abbilden und Prüfen

Nachdem die grundlegenden Rahmenbedingungen für eine Modellierung im vorangegangenen Schritt festgelegt wurden, kann mit dem **Abbilden** begonnen werden. Das Abbilden erfolgt mithilfe der auf *Eclipse*[5] basierenden Software *verinice.PRO*.

[5] https://www.eclipse.org/ (letzter Zugriff: 2019-08-28)

Verinice hat die Grundschutzkataloge des BSI lizenziert und Bausteine, sowie Gefährdungs- und Maßnahmenkataloge integriert und ist damit ein Werkzeug, mit dem IT-Sicherheitsrichtlinien nach der IT-Grundschutz-Methodik des BSI erstellt werden können [ver19].
In *verinice* wird zunächst ein Informationsverbund erstellt und als *Endgeräte* bezeichnet. In diesem angelegten Informationsverbund werden hierarchisch zu betrachtende Objekte angelegt und miteinander verknüpft. Am Beispiel werden Verallgemeinerungen der Objekte mit der Annahme durchgeführt, dass eine Authentifizierung an einer beliebigen Anwendung durch einen Endnutzer unter Verwendung von IT-Systemen mit Internetverbindung durchgeführt werden kann, vgl. Abbildung 4.7. Diese Annahme entspricht einem typischen Anwendungsfall eines vernetzten Endgerätes, vgl. Kapitel 2.1.3.

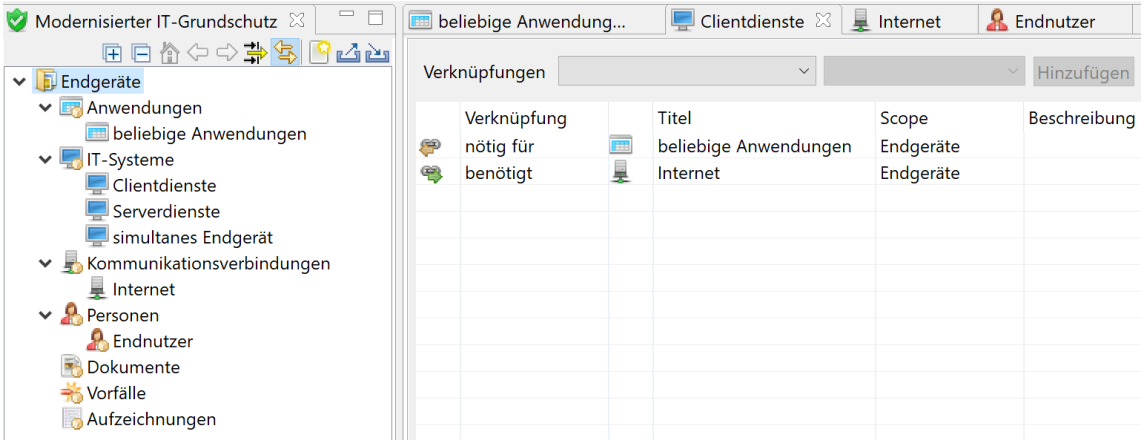

Abbildung 4.7: Allgemeine und verknüpfte Objekte im Informationsverbund (Eigener Screenshot)

Durch die Verknüpfung der Objekte wird das *Maximumprinzip* für den Schutzbedarf wirksam, welches in *verinice* die Standardoption ist [ver18]. Unter dem *Maximumprinzip* wird das Übertragen des Schutzbedarfs von Objekten mit hohem Schutzbedarf auf Objekte mit geringerem Schutzbedarf verstanden, nicht umgekehrt. Wird für eine Anwendung ein hoher Schutzbedarf ermittelt, so müssen alle hierarchisch untergeordneten Objekte, wie IT-Systeme, Netzkomponenten als hochschutzbedürftig behandelt werden [BSI17b].
Beginnend mit den Prozess-Bausteinen werden im nächsten Schritt die Zuordnungen von infrage kommenden Bausteinen zu den angelegten Objekten durchgeführt. Da Prozess-Bausteine typischerweise Themen beinhalten, die den gesamten Informationsverbund betreffen, werden diese nicht auf einzelne Objekte, sondern der obersten

Ebene des Informationsverbundes zugeordnet. Aus Sicht von Herstellern, Dienstleistern und Betreibern sollten für jede Sicherheitsrichtlinie alle organisatorischen Bausteine auf Ihre Anwendbarkeit geprüft werden. Am Beispiel wurden nur essenzielle organisatorische Bausteine ausgewählt oder auf solche verwiesen, um ein vollständiges Bild einer Sicherheitsrichtlinie zu erhalten.
Nach der Zuordnung der ausgewählten Prozess-Bausteine zum Informationsverbund, folgt die Zuordnung allgemeiner Systembausteine wie *SYS.2.1 Allgemeiner Client* und *SYS.3.2.1 Allgemeine Smartphones und Tablets* auf die dazu passenden Objekte des Informationsverbundes. Für den *Modularen Teil* der Richtlinie, vgl. Abschnitt 4.3.1, werden den jeweiligen Objekten noch verschiedene produktspezifische Bausteine wie *SYS.2.2.3 Clients unter Windows 10* und *SYS.2.4 Clients unter macOS* zugeordnet. In Abbildung 4.8 ist der Informationsverbund mit seinen Objekte und den ausgewählten und zugeordneten Bausteinen dargestellt.

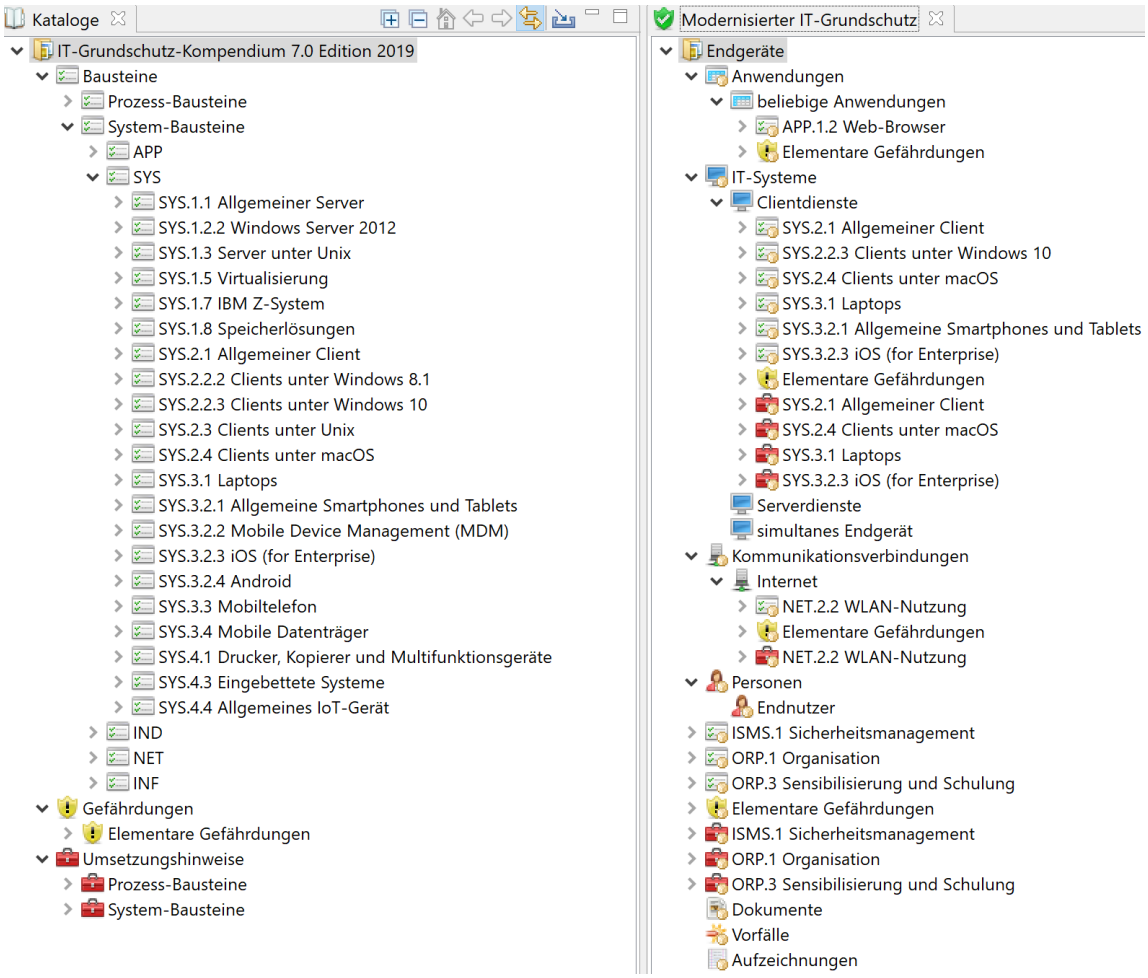

Abbildung 4.8: Zugeordnete Bausteine im Informationsverbund (Eigener Screenshot)

Nachdem die Verknüpfungen der angelegten Objekte und die Zuordnungen von in Frage kommenden Bausteinen zu den Objekten erstellt wurden, sieht die Methodik nach dem BSI-Grundschutz den IT-Grundschutz-Check vor. Dieser gibt einen Erfüllungsstatus wieder. Dabei sollen alle Anforderungen, die noch nicht erfüllt sind, als NICHT umgesetzt gekennzeichnet werden. Anforderungen, welche bereits erfüllt sind, werden durch ein JA bestätigt. Nicht relevante Anforderungen werden auf ENTBEHRLICH gesetzt und Anforderungen die noch nicht vollständig umgesetzt sind, erhalten die Kennzeichnung TEILWEISE [BSI17b]. Der Erfüllungsgrad der Anforderungen kann bei der Umsetzung hilfreich sein. Als Grundlage für die zusammengefassten Maßnahmen der zu erstellenden Richtlinie werden nicht relevante und entbehrliche Anforderungen entfernt.
Der abschließende Schritt ist das Erarbeiten und **Zuordnen von Umsetzungshinweisen** für den *Modularen Teil* der Richtlinie. Das Grundschutz-Kompendium des BSI bietet Umsetzungshinweise für die meisten Maßnahmen der Anforderungen aus den Bausteinen an. Das kann bei allgemeinen Bausteinen hilfreich sein. Bei produktspezifischen Bausteinen gibt es Hinweise, dass bestimmte Funktionalitäten vorhanden sind und deaktiviert oder aktiviert werden sollten. Als Beispiel sei die Anforderung *SYS.2.4.A7 Zwei-Faktor-Authentisierung für Apple-ID* aus dem Baustein *YS.2.4 Clients unter macOS* genannt, in der es heißt: „Die Zwei-Faktor-Authentisierung für die Verwendung des Apple-ID-Kontos SOLLTE aktiviert werden.“ [BSI19b]. Dieser Umsetzungshinweis lässt den Schluss zu, dass eine Zwei-Faktor-Authentifizierung mit einer Apple-ID möglich ist. An der Stelle fehlt der konkrete Hinweis, wie sich die Aktivierung durchführen lässt. Mit fundiertem Fachwissen, einschlägiger Literatur und technischen Anleitungen kann eine Umsetzung erfolgreich sein.
Für die technischen Umsetzungshinweise der Richtlinie werden die Benchmarks des Center of Security (CIS)[6] verwendet. Das CIS ist eine gemeinnützige Organisation, die in Zusammenarbeit mit einer IT-Community private und öffentliche Unternehmen vor Cyberbedrohungen schützen möchte. Dafür stellt das CIS sogenannte CIS Benchmarks™ zur freien Verfügung. Diese Benchmarks sind anerkannte Best Practices zur Sicherung von IT-Systemen gegen bekannte Angriffe und werden von einer freiwilligen, globalen Gemeinschaft erfahrener IT-Experten kontinuierlich weiterentwickelt und verifiziert [IS19]. Die Benchmarks sind jeweils produktspezifisch und als PDF-Dateien erhältlich. Der *Modulare Teil* der Richtlinie soll die Maßnahmen für die Anforderungen folgender Produkte liefern:

[6] https://www.cisecurity.org (letzter Zugriff: 2019-08-28)

- Betriebssystem: Windows 10
- Betriebssystem: macOS 10.13
- Betriebssystem: iOS 12
- Browser: Mozilla Firefox 38
- Browser: Google Chrome

Für diese Produkte wurden die Benchmarks ausgewertet und im *Modulare Teil* der Richtlinie auf die Seitenzahlen des jeweiligen Benchmark-PDFs verwiesen [CIS15] [CIS18a] [CIS18b] [CIS18c] [CIS18d]. Eine auf die technischen Maßnahmen referenzierende Übersicht ist im *modularen Teil* der IT-Sicherheitsrichtlinie abgebildet und als Anhang B beigefügt.

4.3.1.3 Umsetzen und Aufrechterhalten

Dieser Schritt sieht die organisatorische und technische Umsetzung der organisatorischen und technischen Maßnahmen und die Aufrechterhaltung der IT-Sicherheit durch regelmäßige Kontrollmechanismen vor. Idealerweise sollten die meisten Kontrollmechanismen automatisiert implementiert sein. Das kann durch Monitoringsysteme, wie *Nagios*[7] oder *Zabbix*[8] und Loganalyse-Systeme wie dem *ELK-Stack*[9] umgesetzt werden.
Umsetzungshinweise sind dem *modularen Teil* der IT-Sicherheitsrichtlinie aus Anhang B zu entnehmen.

4.3.2 Handlungsempfehlungen des BSI für Bürger am Beispiel

Eine weitere Aufgabe aus Sicht des BSI ist es, auch private IT-Anwender in Bezug auf die IT-Sicherheit zu informieren und zu sensibilisieren. Diese Aufgabe startete als Service bereits im Jahr 2002 mit einer CD-ROM-Version, zunächst unter dem Namen „Ins Internet - mit Sicherheit!“. Die Angebote für diese Zielgruppe sind derzeit auf Informationsportalen wie dem BSI für Bürger, dem Bürger-CERT, BSI Service Centern, sowie auf einschlägigen Kanälen sozialer Netzwerke zu finden [BSI16]. Die Informationsportale bieten Handlungsempfehlungen zum Schutz vor Risiken aus

[7] https://www.nagios.org (letzter Zugriff: 2019-08-28)
[8] https://www.zabbix.com (letzter Zugriff: 2019-08-28)
[9] https://www.elastic.co/de/elk-stack (letzter Zugriff: 2019-08-28)

dem Internet, im Umgang mit Endgeräten und Hilfestellungen zu Themen wie sicheres Online-Banking, oder der Absicherung des smarten Zuhauses [Kat17]. Es besteht auch die Möglichkeit eine derzeit kostenfreie telefonische Hotline oder eine Emailadresse für Fragen in Anspruch zu nehmen.
Damit ergibt sich ein vielschichtiges Angebot. Im Folgenden soll gezielt nach Handlungsempfehlungen auf den Internetseiten des BSI für Bürger gesucht, ausgewertet und zusammengefasst werden, welche in Zusammenhang des IT-Sicherheitskriteriums *Authentifizierung und Autorisierung* stehen könnten. Aus Sicht eines Endnutzers scheinen die Empfehlungskategorien *Basisschutz für Computer & Smartphone*, *Passwörter*, *Benutzerkonten & Heimnetzwerke* und *Gesunder Menschenverstand* einen Bezug zu dem IT-Sicherheitskriterium herzustellen.

Basisschutz für Computer & Smartphone: Mit dem Basisschutz soll durch gezielte Gerätekonfiguration eine solide Grundlage der Gerätesicherheit geschaffen werden. Der Leser kann sich beim Einstieg zwischen *Computern* oder *mobilen Geräten* entscheiden. Für das Beispiel wurde die Option *Computer* mit dem Betriebssystem *Windows 10* gewählt. Mit dieser Wahl wird der Nutzer auf das PDF-Dokument *Sichere Nutzung von Geräten unter Microsoft Windows 10 - Empfehlungen für Privatanwender* verwiesen. Unter Betrachtung des Lebenszyklus eines Endgerätes, kann sich der Nutzer in diesem 11-seitigen Dokument über die sichere Basiskonfiguration von Windows10-PCs informieren. Bezugnehmend auf die Anwendung am Beispiel des IT-Sicherheitskriteriums erhält man aus dem Dokument unter der Überschrift *Gebrauch von Passwörtern* folgende Handlungsempfehlungen [BSI17d]:

- Für verschiedene Online-Dienste, sollten jeweils unterschiedliche und angemessene Passwörter verwendet werden.
- Das Notieren von Passwörtern und Passworthilfen wird mit räumlich getrennter Aufbewahrung zum Endgerät empfohlen.
- Bei der Verwendung von Master-Passwörtern sollte der Zugriff vor unbefugtem Auslesen geschützt werden, z.B. durch die Verwendung von Passwort-Managern.
- Ergänzende Hilfestellungen zum Passwortgebrauch sind u.a. auf den Internetseiten des Bundesamtes *BSI für Bürger* zu finden.

Passwörter: Authentifizierungen unter der Verwendung von Wissen, sind nach wie vor das zentrale Element bei den meisten Zugangskontrollsystemen und werden

durch die Eingabe von Benutzernamen und Passwörtern realisiert. Hier reichen die Handlungsempfehlungen des BSI von der Wahl bis zur Verwendung der Passwörter und können folgendermaßen zusammengefasst werden [BSI19c]:

- Passwörter sollte man sich gut merken können. Das kann z.B. unter Zuhilfenahme von Merksätzen aus denen die jeweils ersten Buchstaben der Wörter extrahiert werden und zusätzlich Ersetzungen durch Zahlen und Sonderzeichen durchgeführt werden.
- Die Passwortlänge ist möglichst hoch gestaltet werden, mindestens jedoch acht Zeichen lang. Bei Offlinediensten werden 20 Zeichen empfohlen.
- Empfohlen wird die Verwendung des gesamten Zeichenraumes, sofern keine technischen Beschränkungen der angebotenen IT-Dienste vorgegeben sind.
- Es sollen keine Wörter verwendet werden, die in Wörterbüchern vorkommen, ebenso wenig wie Wiederholungs- und Tastaturmuster. Beispiele zu vermeidender Passwörter sind: *123456, qwertz, abc123abc123*.
- Die Komplexizität von Passwörtern kann nicht durch Anhängen oder Voranstellen von Zahlen oder Sonderzeichen an, oder vor Wörtern erreicht werden.
- Regelmäßige Änderungen von Passwörtern sind anzustreben.
- Die Verwendung verschiedener Kennwörter für verschiedene Dienste.
- Voreingestellte Passwörter sind zu ändern.
- Bildschirmschoner sollten mit Passwörtern geschützt werden.
- Passwörter sollten nie an Dritte weitergegeben werden.
- Bei Verwendung von z.B. Passwort-Verwaltungsprogrammen sind starke Masterkennwörter zu verwenden.

Benutzerkonten & Heimnetzwerke: Diese Kategorie zielt auf die Problematik ab, dass in einem Netzwerk mehrere Endgeräte vorhanden sind, sowie auf die Verwendung eines Endgerätes durch mehrere Nutzer. Die Verbreitung von Schadsoftware hat in diesem Kontext eine breite Angriffsfläche. Die Empfehlungen sind in einem Kurzvideo dargestellt und Erklären die Trennung der Nutzerkonten in Konten mit Administrationsrechten zur Installation und Aktualisierung von Programmen und Konten, die für das Surfen im Internet oder den Emailverkehr verwendet werden.

Gesunder Menschenverstand: Ein weiteres Thema, dass im Zusammenhang der Authentifizierung stehen kann, ist der gesunde Menschenverstand. Hier wird vom

BSI die Achtsamkeit der Nutzer adressiert, so dass Meldungen, Nachrichten und Aufforderungen nicht blind vertraut werden darf. Bei Zweifel an der Integrität z.B. von Webseiten, sollten Nutzer das Impressum von Webseiten genauer betrachten und sich telefonisch erkundigen oder die Situation durch Dritte einschätzen lassen. „Denn auch im Internet gibt es nichts umsonst.“ [BSI19a].

4.4 Technische Überprüfung von IT-Sicherheit

Die Überprüfung von IT-Sicherheit mit technischen Hilfsmitteln zielt vorwiegend auf Sicherheitsbewertungen der eingesetzten IT-Systeme und Produkte ab. Die Überprüfungen können entweder außerhalb der zu testenden Systeme durchgeführt werden, oder innerhalb der Systeme. Die Ausgangspunkte für Tests, die außerhalb eines Systems ansetzen, sind die Netzwerkkommunikation und das physische Gerät. Bei Tests innerhalb des Systems, werden überwiegend produktspezifische Sicherheitseinstellungen der eingesetzten Betriebssysteme und Anwendungen überprüft.

4.4.1 Angriffsablauf und Aufklärung

Um verschiedene Möglichkeiten der Sicherheitstests mit technischen Hilfsmitteln zu bewerten, ist die Kenntnis über einen vollständigen Angriffsablauf hilfreich. Abbildung zeigt 4.9 einen allgemeinen Angriffsverlauf mit seinen typischen Phasen. Diese Phasen werden im Folgenden kurz erläutert.

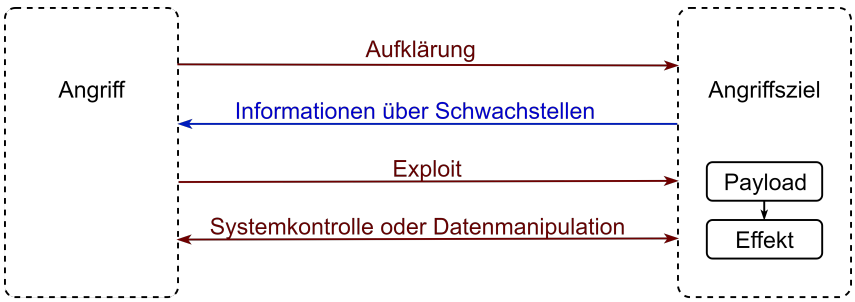

Abbildung 4.9: Angriffsphasen (Eigene Darstellung in Anlehnung an [DGP+18])

Zunächst leiten Derby at al. den Begriff Cyber-Angriff den Begriff *Angriff* aus allgemeinen Definitionen her, wie er in Lexika verwendet wird und projizieren ihn auf IT-Systeme. Sie bezeichnen Cyber-Angriffe als offensive Maßnahme gegen Cyber-Infrastrukturen, zu der nicht nur IT-Systeme, sondern auch Anwendungen, Personen und Verfahren gehören. Solche Angriffe beginnen meist mit einer Aufklärung,

indem Informationen über die Ziele gesammelt werden [DGP+18]. Das kann auch in einem nicht auf die virtuelle Welt bezogenen Kontext geschehen, wie es beim Angriffsvektor *Social Engineering* angewendet wird, vgl. Angriffsvektoren aus Kapitel 2.2.3. Mit der Aufklärung können Angreifer Informationen über Schwachstellen in den Infrastrukturen und IT-Systemen der Betreiber erhalten. Die eigentlichen Bedrohungen sind durch Exploits gegeben, vgl. Kapitel 2.2.2. *Payloads (Nutzlasten)* stellen bösartige Funktionen zur Verfügung, wenn der *Exploit* auf dem Zielsystem platziert ist. Daraus entsteht ein Effekt über den Angreifer das System kontrollieren oder Daten kopieren und manipulieren könnten. In diesem Zusammenhang ist noch Begriff *Threat Intelligence* zu nennen, da hiermit das Sammeln von Informationen beschrieben wird [Wen18].
Mit der Annahme des Handelns unachtsamer Nutzer und der Verwendung schwacher und leicht zu erratender Passwörter, ist es für potenzielle Angreifer bzw. Penetrationstester einfach in Systeme einzudringen [Kes13]. Daher wird im weiteren Verlauf auf die Schritte des Auffindens und Ausnutzen von Schwachstellen verzichtet. Vielmehr soll mithilfe von technischen Hilfsmitteln die Systemsicherheit aus dem System selbst bewertet werden. In den technischen Maßnahmen der IT-Sicherheitsrichtlinie konnte gezeigt werden, dass die IT-Sicherheitskriterien überwiegend innerhalb vernetzter Endgeräte anzuwenden sind. Aus diesen Gründen werden die folgenden Betrachtungen und Systemtests innerhalb eines IT-Systems durchgeführt.

4.4.2 IT-Audits und Penetrationstests

Mit dem festgelegten Fokus auf die technische Bewertung von IT-Sicherheit innerhalb eines vernetzten Endgerätes, können IT-Audits und Penetrationstests eine sinnvolle Grundlage bilden.
Die nachfolgenden Betrachtungen zu IT-Audits stützen sich im Wesentlichen auf [Bei14].
In Unternehmen werden Audits allgemein als Prozess verstanden, mit denen Überprüfungen der verschiedensten Themenbereiche durchgeführt werden können. Ungeachtet des zu überprüfenden Themenbereiches, verfolgen alle Audits das Ziel der unabhängigen und nachvollziehbaren Überprüfung, sowie angemessenen Nachweisen der Ergebnisse. Wichtig dabei ist das Sicherstellen der Unabhängigkeit, dass die Auditoren keinen Interessenskonflikten unterliegen und im höchsten Maße objektiv bewerten.
Bezogen auf das Themenfeld der IT, definiert Beißel IT-Audits als „unabhängige Überprüfung der Einhaltung von Vorgaben und der Funktionalität von Kontroll-

maßnahmen innerhalb der IT eines Unternehmens“ [Bei14].
Wie allgemeine Audits, werden auch IT-Audits durch interne und externe Vorgaben bestimmt. Interne Unternehmensvorgaben können Richtlinien und Arbeitsanweisungen sein. Externe Vorgaben bilden sich aus verpflichtenden Gesetzen und optionalen Standards, wie der ISO 27000-Reihe oder Cobit und Best Practices wie ITIL. Sie können auch technische Empfehlungen beinhalten, wie die in Abschnitt 4.3.1.2 verwendeten Benchmarks des CIS.
Für das Erarbeiten von IT-Audits werden nach Beißel zunächst Kontrollziele definiert, aus denen ein Prüfungskatalog mit Kontrollfragen erstellt wird. Dabei werden nicht nur die Schutzziele aus der IT behandelt, sondern auch auf Wirtschaftlichkeit geachtet, wie Effizienz und Effektivität. In dieser Thesis werden ausschließlich die Schutzziele der IT-Sicherheit betrachtet, vgl. Kapitel 2.2.1.
Penetrationstests sind autorisierte und rechtlich abgesicherte Vorgehensweisen, welche die Sicherheitsvorkehrungen von IT-Systemen in Unternehmen umgehen, um unbefugte Aktivitäten durchführen zu können. Auch wenn Penetrationstests teuer und aufwändig sind, gelten sie effektives Mittel, um ein möglichst vollständiges Bild der Schwachstellen von IT-Systemen aufzuzeigen [CS19]. Dabei kommen Verfahren, Werkzeuge und Applikationen zum Einsatz, wie sie auch Angreifer verwenden. Es werden aber dabei keine Daten entwendet, manipuliert oder zerstört. Das Ziel von Penetrationstests ist einzig das Aufzeigen und Melden von Sicherheitslücken auf der Grundlage von expliziten Aufträgen [Kof18].
Penetrationstests können als Bestandteil von IT-Audits verstanden werden, da diese einen Teil des Fragenkataloges repräsentieren.
In dieser Thesis wird die Umsetzungsüberprüfung der technischen Maßnahmen der Sicherheitsrichtlinie aus Abschnitt 4.3.1 und Anhang B mithilfe von technischen Tests durchgeführt. Resultierend aus diesen technischen Maßnahmen werden folgende Prüfkriterien berücksichtigt:

- Kontorichtlinien
- Rollentrennung
- Firewall
- Update-Einstellungen
- Datenverschlüsselung
- Protokollierung und Systemüberwachung

Für die Prüfkriterien besteht die Möglichkeit der manuellen Überprüfung. Das kann über die grafische Oberfläche des Betriebssystems und über Kommandozeilenbefehle durchzuführt werden. Am Beispiel des Prüfpunktes *Kontorichtlinien* wird das für die Betriebssysteme *Windows 10* und *macOS* demonstriert.
Auf einem *Windows 10*-System können mithilfe des Gruppenrichlinieneditors, die aktiven Kennwortrichtlinien und Kennwortsperrungsrichtlinien eingesehen und geändert werden. Abbildung 4.10 zeigt die Standardeinstellungen, wie sie bei der Installation von *Windows 10* konfiguriert werden.

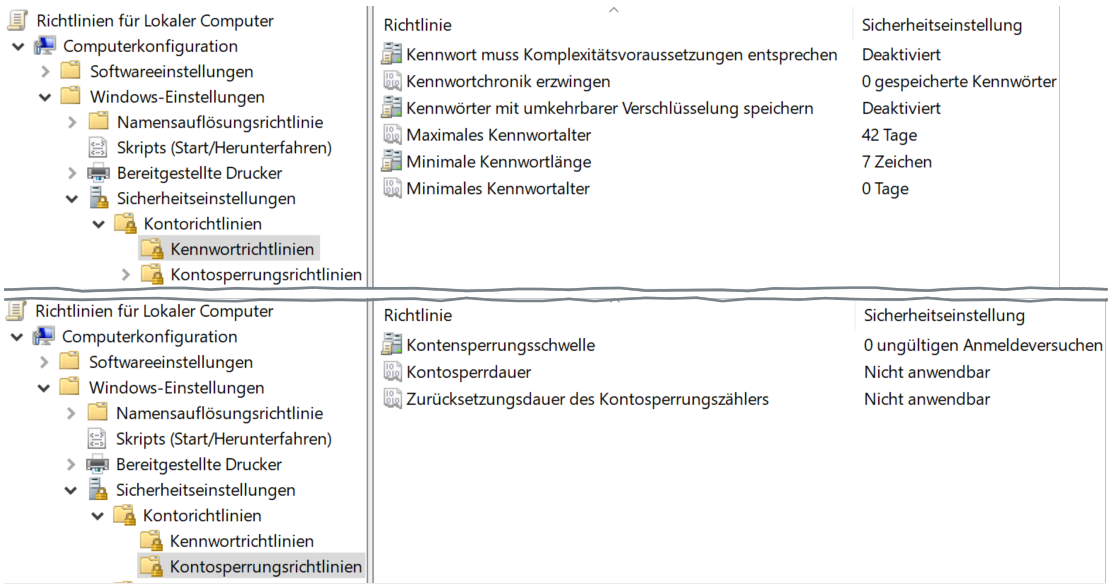

Abbildung 4.10: Windows 10 - Kennwortrichtlinien und Kontosperrungsrichtlinien (Eigener Screenshot)

Alternativ kann diese Überprüfung auf einem *Windows 10* betriebenen System mit dem Kommandozeilenbefehl `net accounts` durchgeführt werden. Die Ausgabe des Befehls ist in Abbildung 4.11 dargestellt und zeigt ebenfalls die von Windows bei der Installation gesetzten Standardeinstellungen.

```
O:\>net accounts
Abmelden erzwingen nach:                                   Nie
Minimales Kennwortalter (Tage):                            0
Maximales Kennwortalter (Tage):                            42
Minimale Kennwortlänge:                                    7
Länge der Kennwortchronik:                                 Keine
Sperrschwelle:                                             Nie
Sperrdauer (Minuten):                                      30
Sperrüberprüfungsfenster (Minuten):                        30
Rolle des Computers:                                       WORKSTATION
```

Abbildung 4.11: Windows 10 - Kontenrichtlinie auf der Kommandozeile (Eigener Screenshot)

Darüber hinaus kann bei Windows-Systemen noch die Möglichkeit verwendet werden, die *Kontorichtlinien* über interne Registrierungsdatenbank abzurufen und zu manipulieren.
Am Beispiel des Prüfpunktes *Kontorichtlinien* eines unter *macOS* betriebenen Systems, lässt sich keine Möglichkeit einer grafikgestützten Überprüfung ermitteln. Stattdessen kommt der Kommandozeilenbefehl `pwpolicy -getaccountpolicies` zum Einsatz. Die Bildschirmausgabe zeigt eine XML-Datei, welche die globalen Konteneinstellungen wiedergibt [CIS18b]. Die Ausgabe der Konteneinstellungen auf einem *macOS*-System ist in Abbildung 4.12 dargestellt.

```
Getting global account policies
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>policyCategoryPasswordContent</key>
        <array>
                <dict>
                        <key>policyContent</key>
                        <string>policyAttributePassword matches '^$|.{4,}+'</string>
                        <key>policyContentDescription</key>
                        <dict>
                                <key>Dutch</key>
                                <string>Voer een wachtwoord van vier of meer tekens in of laat het wachtwoordveld leeg.</string>
                                <key>English</key>
                                <string>Enter a password that is four characters or more or leave the password field blank.</string>
```

Abbildung 4.12: macOS - Kontenrichtlinie (Eigener Screenshot)

Für eine möglichst automatisierte Auswertung aller Prüfkriterien, werden in den folgenden beiden Abschnitten Testskripte für die beiden Systeme *Windows 10* und *macOS* erarbeitet. Diese Skripte prüfen die technischen Einstellungen der Systeme und geben als Ergebnisse des jeweiligen Prüfpunktes ein *ERFÜLLT*, *NICHT ERFÜLLT* oder *TEILWEISE ERFÜLLT* wieder.
Für das mobile Betriebssystem *iOS* wird kein Skript erstellt, da skriptbasierende Sicherheitsanalysen für dieses Betriebssystem nur mit einem manipulierten Betriebssystemabbild und einem alternativen App-Store möglich sind [Spr17].

4.4.2.1 Sicherheitsskript für Windows-10-Systeme

Das Erstellen des Testskriptes für Windows-Systeme erfolgt in der Windows PowerShell (WPS). Die Windows-PowerShell ist eine Skriptsprache, die unter Verwendung des .NET Frameworks und der Anbindung an die Windows Management Instrumentation (WMI) arbeitet [Sch18]. Sie ist auf jedem *Windows 10* betriebenen System integriert und liegt derzeit in der Version 5.1 vor.
Die Prüfkriterien sind im Skript jeweils als Funktionen mit den einzelnen Prüfpunkten und einer integrierten Auswertung abgebildet. Die Ergebnisse der Prüfpunkte

werden am Bildschirm ausgegeben und die Auswertung erfolgt in einer separaten Protokolldatei.
Das vollständige Skript ist dem Anhang C.1 beigefügt. Die Ergebnisse werden in Kapitel 5.1.6 bewertet.
Abbildung 4.13 zeigt die Bildschirmausgabe nach einem vollständigen Durchlauf des Skriptes. Die Bildschirmausgabe besteht aus einem *Kopf*, welcher grundlegende Informationen, wie die vorliegende Windows-Version und das Datum des Testlaufes wiedergibt und einem *Prüfteil*, der eine farblich markierte und numerische Wertung der einzelnen Prüfpunkte ausgibt. Abschließend kennzeichnet der *Schlussteil* des Skriptes das Ende eines Testlaufes.

```
-------------------------------------------------------
Test von allgemeinen Sicherheitseinstellungen
-------------------------------------------------------
-------------------------------------------------------
eingesetzte Version: Microsoft Windows 10 Enterprise
Datum:  2019-08-21 15:28:12 Uhr
-------------------------------------------------------
Beginn: Testlauf
-------------------------------------------------------

Rollentrennung
----------------------------
  Administrationsrechte: [1]

Kontorichtlinien
----------------------------
  Kennwortlaenge:        [0]
  Kennwortchronik:       [0]
  Sperrschwelle:         [0]
  Sperrdauer:            [1]
  Kontensperrung Reset:  [1]

Updateverhalten
----------------------------
  Windows Version:       [1]
  Updatedienst:          [0]

Firewall
----------------------------
  Firewall:              [1]
  Defender:              [0]

Verschluesselung
----------------------------
  Bitlocker:             [0]

Protokollierung
----------------------------
  Event-Log:             [1]

----------------------------
Ende: Testlauf
-------------------------------------------------------
-------------------------------------------------------
```

Abbildung 4.13: Windows - Skriptteil: Prüfdurchlauf (Eigener Screenshot)

Die Auswertung der Prüfpunkte zu dem vorangegangenen Testlauf ist in Abbildung 4.14 dargestellt. Sie besteht, wie auch die Ausgabe des *Prüfteils*, aus einem *Kopfteil*, einem *Hauptteil* und einem *Schlussteil*.

```
-------------------------------------------------------
Auswertung der Sicherheitstests
eingesetzte Version: Microsoft Windows 10 Enterprise
Datum:  2019-08-22 12:07:29 Uhr
---------------------------------------
Beginn: Auswertung
---------------------------------------

 Administrationsrechte:       [ERFÜLLT]
---------------------------------------

 Kontorichtlinien:      [NICHT ERFÜLLT]
---------------------------------------
  Handlungsempfehlung:
   - Einstellungen im Gruppenrichtlinieneditor 'gpedit':
     Computerconfiguration -> Windows-Einstellungen ->
     Sicherheitseinstellungen -> Kontorichtlinien
   - Aktuelle Empfehlungen können dem
     IT-Grundschutz-Kompendium entnommen werden.

 Updateverhalten:   [TEILWEISE ERFÜLLT]
---------------------------------------
  Handlungsempfehlung:
   - Automatische Updates einstellen.

 Firewall:          [TEILWEISE ERFÜLLT]
---------------------------------------
  Handlungsempfehlung:
   - Prüfen, ob alternativer Virenscanner
     installiert und aktuell ist.

 Bitlocker Status:         [UNBESTIMMT]
---------------------------------------
  Handlungsempfehlung:
   - Erneute Prüfung mit administrativen Rechten.

 Eventlog:          [TEILWEISE ERFÜLLT]
---------------------------------------
  - Zu Überprüfen ist, welche Nutzer- und -gruppen
    die Log-Daten auswerten dürfen.

Weiterführende Literatur
CIS Microsoft Windows 10 Enterprise Benchmark
https://learn.cisecurity.org/benchmarks
letzter Zugriff: 2019-08-19
---------------------------------------
---------------------------------------
Ende: Auswertung
-------------------------------------------------------
-------------------------------------------------------
```

Abbildung 4.14: Windows - Skriptteil: Protokoll mit Auswertung (Eigener Screenshot)

Der *Hauptteil* gibt den ausgewerteten Erfüllungsgrad der Prüfkriterien und daraus abgeleitete Handlungsempfehlungen wieder. Handlungsbedarf und Empfehlungen werden dann ausgegeben, wenn Prüfpunkte als *NICHT ERFÜLLT* oder *TEILWEISE ERFÜLLT* gewertet wurden.

4.4.2.2 Sicherheitsskript für macOS-Systeme

Das Testskript für *macOS*-Systeme ist für *bash*-Umgebungen des *macOS*-Terminals ausgerichtet. *Bash*-Umgebungen sind auch auf Linux-Systemen zu finden. Das Skript ist analog zu dem Skript für *Windows*-Systeme aufgebaut, vgl. vorangegangen Abschnitt 4.4.2.1. In Abbildung 4.15 ist der Testlauf des Skriptes mit den farblich und numerisch gewerteten Prüfpunkten dargestellt.

```
Überprüfung von allgemeinen Sicherheitseinstellungen
Prüfdatum: 2019-08-19 # 17:22:33 Uhr
Betriebssystemversion: macOS Mojave
Beginn: Prüfdurchlauf
.....................

Rollentrennung:
Administrationsrechte: [0]
Kontorichtlinien:
Passwortlänge          [0]
Passwortkomplexität    [1]
Kontosperrung          [0]
Firewall:
Firewall               [1]
Gatekeeper             [1]
Datenverschlüsselung:
Verschlüsselung        [0]
Updateverhalten:
Systemupdates          [0]
Applikations-Updates   [0]
Protokollierung:
Log-Dienst             [1]

...................
Ende: Prüfdurchlauf
```

Abbildung 4.15: macOS - Skriptteil: Prüfdurchlauf (Eigener Screenshot)

Abbildung 4.16 zeigt die Auswertung des Skriptes mit den jeweiligen Handlungsempfehlungen.

```
Auswertung der Sicherheitsüberprüfung
Datum: 2019-08-19 # 17:30:16 Uhr
Betriebssystemversion:
.....................................

Rollentrennung:
Test der Rollentrennung [NICHT ERFÜLLT]
Handlungsempfehlung:
Für administrative Zwecke einen separaten Benutzer erstellen.
Den aktuellen Benutzer aus der Gruppe 'root' entfernen.

Kontorichtlinien:
Kontoeinstellungen [teilweise ERFÜLLT]
Handlungsempfehlung:
Konteneinstellung mit folgendem Befehl setzen:
 $ pwpolicy -setaccountpolicies
Kernpunkte der Einstellungen:
 - mindestens 8 Zeichen
 - alphanumerisch
 - Kontensperrung nach 10 Fehlversuchen

Firewalleinstellungen:
Firewall und Gatekeeper [ERFÜLLT]

Verschlüsselung:
Festplattenverschlüsselung [NICHT ERFÜLLT]
Handlungsempfehlung:
FileVault aktivieren
 Systemeinstellungen -> Sicherheit -> FileVault -> FileFault aktivieren

Updateverhalten:
Automatische Updateeinstellungen [NICHT ERFÜLLT]
Handlungsempfehlung:

Logging:
Protokollierung [ERFÜLLT]
Handlungsempfehlung:
Einstellungen des Protokollierungsdienstes sind zu überprüfen.
Weiterführende Empfehlungen sind der Quelle zu entnehmen.

.....................................

Quelle:
CIS Apple macOS 10.13 Benchmark
https://learn.cisecurity.org/benchmarks
letzter Zugriff: 2019-08-19
.....................................
Auswertung beendet
.....................................
```

Abbildung 4.16: macOS - Skriptteil: Auswertung der Prüfpunkte (Eigener Screenshot)

Die Auswertung wurde anhand der numerischen Wertung der Prüfpunkte vorgenommen und gibt den entsprechenden Erfüllungsgrad wieder. Die Bewertung der Ergebnisse erfolgt in Kapitel 5.1.6.

5 Methodenbewertung und Ergebnisauswertung

In diesem Kapitel werden die verwendeten Methoden und die daraus resultierenden Ergebnisse aus den Implementierungen des vorangegangenen Kapitel 4 bewertet. Zudem werden aus den Ergebnissen, Handlungsempfehlungen für Hersteller und Endnutzer abgeleitet.

5.1 Methodenbewertung

Beginnend mit dem Vorgehen der Cyber-Antipattern, werden in den folgenden Abschnitten die verwendeten Methoden auf ihre allgemeine Anwendbarkeit bewertet. Die Ergebnisse der angewendeten Methoden werden innerhalb der jeweiligen Methodenbewertung geführt. Im abschließenden Abschnitt werden die Methoden anhand allgemeiner Bewertungspunkte verglichen.

5.1.1 Bewertung der Cyber-Antipattern

Das kritische Hinterfragen von Gewohnheiten im Umgang mit IT-Systemen und bekannten Sicherheitsfunktionalitäten steht im Mittelpunkt der Analyse durch Cyber-Antipattern. In Kapitel 3 konnte gezeigt werden, wie mithilfe zusammengefasster und häufiger Sicherheitsprobleme eine solche Auseinandersetzung möglich ist. Aus den Ergebnissen wurden wichtige IT-Sicherheitskriterien für vernetzte Endgeräte abgeleitet. Durch fehlende alternative Verfahren sind die Ergebnisse kritisch zu betrachten. Zudem nimmt die Subjektivität der Bearbeiter Einfluss auf Ergebnisse. Mit der Bearbeitung derselben Problematiken durch viele Akteure, kann diesen Einflüssen entgegengewirkt werden. Eine anwendungsgestützte Bearbeitung mit IT-Systemen, könnte zudem die Effizienz erhöhen und die Ergebnisqualität verbessern.

5.1.2 Anwendbarkeit von IT-Sicherheitsmodellen

IT-Sicherheitsmodelle zeigen hinsichtlich ihrer chronologischen Einführung, eine Entwicklung von reinen Zugriffsmodellen in geschlossenen Systemen, hin zu Modellen, die in offenen Systemen Transaktionen überwachen und absichern, vgl. Abbildung 5.1. Zudem erhalten anwendungsbezogene Sichtweisen, sowie Subjekte, bzw. Akteure im Verlauf der Entwicklung von IT-Sicherheitsmodellen immer größere Bedeutung. Mit zunehmender Komplexität und steigendem Vernetzungsgrad von IT-Systemen ist die Entwicklung zu umfassenderen IT-Sicherheitsmodellen zu erwarten [Sim17].

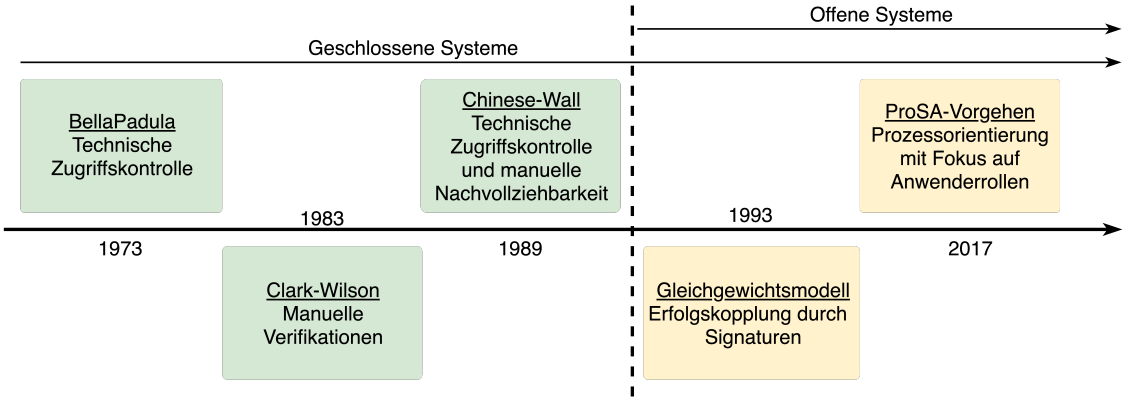

Abbildung 5.1: Historische Entwicklung von IT-Sicherheitsmodellen (Eigene Darstellung)

Die ersten IT-Sicherheitsmodelle sind nur eingeschränkt oder mit Erweiterungen auf die Anforderungen heutiger Systeme anwendbar. So zeigt das BellaPadula-Modell deutliche Grenzen hinsichtlich einer beschränkten Ausdrucksfähigkeit auf, d.h. es lassen sich einige Klassen von Anwendungsszenarien nicht modellieren, obwohl sie informell die Sicherheitsanforderungen erfüllen würden. Weiterhin besteht die Problematik des blinden Schreibens. So könnte auf Objekte geschrieben werden, die durch Schreibberechtigte aber nicht gelesen werden darf. Für Integritätsanforderungen ist das problematisch. Fehlende Granularität für Objekte und Subjekte, sowie Anforderungen an hohe Datenintegrität können auf Grund der im Modell festgelegten universellen Rechte und der einfachen Zugriffsbeschränkungsregeln nicht abgebildet werden. Auch die Befehlskommunikationen ist in diesem Modell nicht implementiert [Eck14].
Beim IT-Sicherheitsmodell nach Clark-Wilson könnten mehrere Nutzer zusammen einen Betrug gemeinsam ausführen oder trotz erhöhter Aufmerksamkeit einen Fehler

machen. Daher ist der Erfolg dieses Modells nicht rein mathematisch zu beweisen und ist selbst bei formaler Auslegung als semi-formales Modell zu verstehen.
Das Chinese-Wall-Modell nach Nash-Brewer nutzt in der Praxis nur die Leseregel und nimmt die Möglichkeit von indirekten Informationsflüssen in Kauf. Ausschließlich durch das nachträgliche Prüfen der Zugriffsprotokollmatrix sind Zugriffsverletzungen erkennbar. Grenzen auf Grund fehlender Dynamik sind in dem Modell erkennbar, da mit zunehmender Dauer die *Mauer* immer größer wird und mit neu aufgenommenen Tätigkeiten auch andere Tätigkeiten verboten werden. Die Mauer sollte an den Stellen wieder abbaut werden, wo Tätigkeiten aufgegeben werden oder Sperrfristen ablaufen. Praktisch ist das aber nur durch manuelle Bereinigung der Protokollmatrix möglich. Weiterhin erfordert das Modell eine zentrale Kontrolle, in der alle beteiligten Firmen gemeinsam an Regeln für die Zugriffskontrolle erarbeiten und überwachen.
Das Gleichgewichtsmodell steht vor der Problematik des hohen Implementierungsaufwandes. Auf den jeweiligen IT-Systemen der Kooperationspartner müssen lokale Speicher vorgehalten werden, sowie einheitliche Infrastrukturen zur digitalen Schlüsselverwaltung Public-Key-Infrastruktur (PKI). Am Beispiel von Ebay wird auf derartige Implementierungen verzichtet. Hier erweist sich der durch Fehlhandlungen drohende Reputationsverlust bis hin zum Ausschluss der Mitglieder, als wirkungsvolle Sanktionsmethode [Gri08].
Die ProSA-Vorgehensweise betrachtet auch aktuelle Aspekte der IT-Sicherheit und setzt einen Fokus auf menschliche Interaktionen. Dadurch lassen sich Prozesse hinsichtlich ihrer IT-Sicherheit bewerten und geeignete Maßnahmen anwenden. Simic fasst in ihrem Fazit zusammen, dass die Zerlegung der einzelnen Prozessaktivitäten in atomare Bestandteile der Übergangsregeln einen klar abgegrenzten und spezifischen Überblick in das Zusammenwirken von Akteuren und IT-Systemen erlaubt. Sie sieht darin aber auch den Nachteil, dass abhängig von den zu betrachteten Prozessen die Analysen komplex und unüberschaubar werden könnten [Sim17].
Insgesamt scheinen damit die klassischen Sicherheitsmodelle ohne Erweiterungen keine praktische Anwendung zu finden, sodass bei der Betrachtung von Sicherheitskriterien mit diesen Modellen erhebliche Einschränkungen zu erwarten sind. Auf Grund aktueller Anforderungen, welche in die ProSA-Vorgehensweise einfließen, scheint mit diesem Prozessmodell eine vollständige Sicherheitsbetrachtung möglich zu sein. Daher wurde in Kapitel 4.2.2 versucht, eine eben solche vollständige Sicherheitsanalyse eines IT-Sicherheitskriteriums durchzuführen. Die Ergebnisse sind im folgenden Abschnitt separat beertet.

5.1.3 Bewertung der ProSA-Vorgehensweise

Am Beispiel des IT-Sicherheitskriteriums *Authentifizierung und Autorisierung* wurde die ProSA-Vorgehensweise für IT-Sicherheitsanalysen angewendet. Hierfür wurde das IT-Sicherheitskriterium als allgemeiner Geschäftsprozess abgebildet, vgl. Abbildung 4.2 aus Kapitel 4.2.2. Anhand dieses Geschäftsprozesses konnten Aktivitäten festgelegt werden, die dann auf Schwachstellen und Bedrohungen untersucht wurden. Diese Arbeitsschritte bildeten die Grundlage für das systematische Herleiten von Sicherheitsanforderungen und dem Festlegen von erforderlichen Maßnahmen.
Am Beispiel wurde nicht nur die strukturierte Durchführung der Methode gezeigt, sondern auch die Komplexität dieser Vorgehensweise. Der interessante Ansatz, den Faktor Mensch in den Fokus zu stellen und ihm drei Rollen innerhalb der Untersuchung zuzuordnen, bringt Einblick in neue Perspektiven für IT-Sicherheitsanalysen.
Unstimmigkeiten entstanden beim Ermitteln der Schwachstellen und Bedrohungen. In isolierten Geschäftsprozessen und den daraus entwickelten Übergangsregeln sind keine externen Angreifer berücksichtigt, vgl. Abbildung 4.3. Externe Angreifer müssen aber beim Ermitteln von Schwachstellen und Bedrohungen einbezogen werden, da sonst viele Schwachstellen nicht ermittelt werden können.
Problematisch sind die teilweise subjektiven Herangehensweisen, wie das Herleiten von Schwachstellen oder das Festlegen von Maßnahmen. Dies betreffend sieht Simic durch fehlende Systematiken entsprechenden Forschungsbedarf und bewertet selbst, dass der Erfolg beim Herleiten von Schwachstellen maßgeblich vom durchführenden Analysten abhängt [Sim17]. Weiter ist anzunehmen, dass beim erneuten Vorgehen nach ProSA andere Ergebnisse erzielt werden.
Mit entsprechenden Lösungen für diese Problematiken und systemgestützten Durchführungen, kann diese Methode bei Analysen und Bewertungen von IT-Sicherheit Verwendung finden. Insgesamt bietet diese Vorgehensweise ein breites Anwendungsspektrum, da sie auch auf Prozesse angewendet werden kann, die nur teilweise oder gar nicht mit IT-Systemen in Berührung kommen.

5.1.4 Bewertung der IT-Grundschutz Methodik

In Kapitel 4.3 wurde der Standard 200-2 der IT-Grundschutz-Methodik des BSI vorgestellt und deren Arbeitsschritte beim Erreichen verschiedener Sicherheitsniveaus miteinander verglichen. Aus dieser Gegenüberstellung wurden verallgemeinerte Arbeitsschritte der Grundschutz-Methodik vorgeschlagen, vgl. Kapitel 4.3.1. Unter

Verwendung der so angepassten Arbeitsschritte, wurden mithilfe der Software *verinice.PRO*, relevante Bausteine aus dem Grundschutz-Kompendium modelliert und bewertet. Das Ergebnis ist eine allgemein anwendbare Sicherheitsrichtlinie, die aus zwei Teilen besteht, vgl. Anhang B. Im *Allgemeinen Teil* der Sicherheitsrichtlinie, konnten die IT-Sicherheitskriterien Anwendung finden. Der Nachweis für den *Modularen Teil* der Richtlinie wird unter Verwendung von Skripten für Sicherheitsaudits im Kapitel 4.4.2 geführt.
Eine große Herausforderung beim Erstellen der Richtlinie, war das Festlegen von technischen Maßnahmen für die einzelnen Systeme im *Modularen Teil*. Hierfür bietet das BSI Umsetzungshinweise im IT-Grundschutz-Kompendium an, welche in vielen Fällen aber ohne technologischen Bezug sind, vgl. Abschnitt B. Die Grundschutz-Methodik des BSI ist auf die Absicherung von Unternehmen ausrichtet und an Sicherheitsverantwortliche, -experten, -berater etc. adressiert [BSI17b]. Der Übergang von abgeleiteten allgemeinen technischen Maßnahmen zu den technischen Maßnahmen spezifischer Systeme, erfordert fundiertes Wissen und Erfahrung mit den eingesetzten und abzusichernden Systemen und ist daher nicht für private Endnutzer geeignet. Für vernetzte Endgeräte entsteht somit die Forderung der Absicherung und des Nachweises durch den Dienstanbieter. Eine mögliche Anlaufstelle für private Endnutzer stellt das *BSI für Bürger* dar. Dieses Angebot wird im folgenden Abschnitt auf seine Anwendbarkeit überprüft und bewertet.

5.1.5 Bewertung des BSI für Bürger

Mit dem Angebot des *BSI für Bürger* bietet das Bundesamt eine Vielzahl von allgemein verständlichen und aktuellen Risiken und Empfehlungen im Zusammenhang mit der Verwendung von digitalen Medien an. Interessierte Leser können sich in zusammengefassten Anleitungen und Kurzvideos über die verschiedensten Themenfelder der Informationssicherheit informieren. Dabei wird in den Themenfeldern oft auf weitere Informationsquellen und Anleitungen bestimmter Systeme, wie der Einsatz von Geräten mit *Windows 10*, verwiesen.
Bei der Auswertung und Zusammenfassung einzelner Themenfelder in Kapitel 4.3.2, konnte die allgemeine Anwendbarkeit auf das Sicherheitskriterium *Authentifizierung und Autorisierung* gezeigt werden. Bei den Empfehlungen zur Passwortsicherheit fehlen teils Konkretisierungen, wie häufig Passwörter zu ändern sind.
Grundsätzlich stehen dem Erfolg des Angebotes des BSI zwei Sachverhalte entgegen. Zum einen werden vor allem interessierte und auch versierte Leser erreicht. Zum anderen scheint der Bekanntheitsgrad in der Bevölkerung nicht sehr hoch. Mit

ausgewählten Marketingstrategien könnte der Bekanntheitsgrad erhöht und mit Untersuchungen nachgewiesen werden.

5.1.6 Bewertung der Testskripte

Mithilfe der in Kapitel 4.4.2 erstellten, systemspezifischen Testskripte konnte gezeigt werden, dass eine Erstanalyse der IT-Sicherheitseinstellungen auf *Windows*- und *macOS*-Systemen möglich ist. Die Ergebnisse spiegeln dabei überwiegend die Standardeinstellungen wieder, welche nach typischen Systeminstallationen eingestellt sind. Die Ergebnisse zeigen damit auch, dass keine der aktuellen und gängigen Betriebssysteme die grundlegenden IT-Sicherheitskriterien erfüllen, vgl. Kapitel 3.
Die Skripte können als Einstieg für die technische Bewertung von IT-Sicherheit auf vernetzten Endgeräten eingesetzt werden und dabei unterstützen, grundlegende Sicherheitseinstellungen an den jeweiligen Betriebssystemen der IT-Systeme durchzuführen. Somit ist die Verwendung der Skripte als Bestandteile von IT-Audits und Penetrationstests möglich, vgl. Kapitel 4.4.2.
Für weiterführende technische IT-Sicherheitsanalysen sind detailliertere Prüfverfahren notwendig. Am Beispiel des Prüfkriteriums *Firewall*, sollten detaillierte Tests auf einzelne Firewallregeln, sowie dem ein- und ausgehenden Netzwerkverkehr erfolgen. Um die Skripte vor Manipulationen zu schützen, ist das Überführen der offenen Quellcodes hin zu geschlossenen und signierten Programmen notwendig. Mit entsprechenden Erweiterungen in den Sicherheitsskripten, sollte es den Nutzern möglich sein, wichtige Sicherheitseinstellungen bereits während der Skriptausführung durchführen zu können.

5.1.7 Zusammenfassende Methodenbewertung

Zusammenfassend werden die verwendeten Methoden für das Erstellen und Überprüfen der IT-Sicherheitskriterien, anhand allgemeiner und für die Nutzbarkeit und Ergebnisqualität ausschlaggebenden Eigenschaften miteinander verglichen. Die so zusammengefasste Methodenbewertung ist in Tabelle 5.1 dargestellt. Dieser Übersicht kann eine allgemeine Anwendbarkeit der verwendeten Methoden entnommen werden, ausgenommen die klassischen IT-Sicherheitsmodelle. Auf Grund ihrer historischen Betrachtungsweisen können klassische IT-Sicherheitsmodelle ohne Erweiterungen nicht auf aktuelle IT-Sicherheitsbetrachtungen angewendet werden, vgl. Kapitel 4.1 und Abschnitt 5.1.2. Eine Generalisierung von und mit den IT-Sicherheitskriterien konnte mit den Methoden der Cyber-Antipattern, der ProSA-Vorgehensweise und

den Methoden des BSI nachgewiesen werden. Die technische Umsetzung von IT-Sicherheit kann nicht verallgemeinert werden, diese produktspezifisch angewendet werden. Die Wiederholbarkeit bei gleichen Ergebnissen kann nur mit den Methoden des BSI erzielt werden, auf Grund festgelegter Abläufe beim Zugriff auf eine Quelle (IT-Grundschutz-Kompendium). Aus demselben Grund ist mit den Methoden des BSI die Nachhaltigkeit nur bedingt möglich. Eine Toolunterstützung ist bis auf die IT-Grundschutz-Methodik 200-2 nicht gegeben. Mit einer Toolunterstützung für alle anderen Methoden, kann auch die Wiederholbarkeit bei gleichen Ergebnissen erzielt werden.

	Erstellen und	Bewerten von IT-Sicherheitskriterien				
		IT-Sicherheitsmodelle		IT-Grundschutz		technische IT-Sicherheit
	Cyber-Antipattern	klassisch	ProSA	BSI 200-2	BSI für Bürger	Sicherheitsskripte
allgemeine Anwendbarkeit	✓	×	✓	✓	✓	✓
Generalisierung	✓	×	✓	✓	✓	×
Wiederholbarkeit	○	×	○	✓	✓	✓
Nachhaltigkeit	✓	×	✓	○	○	×
Toolunterstützung	×	×	×	✓	×	×

Tabelle 5.1: allgemeine Methodenbewertung

5.2 Handlungsempfehlungen

Aus den Ergebnissen dieser Thesis und den daraus gezogenen Schlussfolgerungen, ergeben sich wichtige allgemeine Handlungsempfehlungen für Hersteller von vernetzten Endgeräten und Betreibern von allgemeinen IT-Diensten. Weiterhin lassen sich auch für Endnutzer allgemeine Empfehlungen im Umgang mit IT-Systemen ableiten, die dazu beitragen können die IT-Sicherheit dieser Geräte zu verbessern.

5.2.1 Empfehlungen für Hersteller

IT-Sicherheit beginnt mit der Konzeptionierung. Daher richten sich zunächst die Handlungsempfehlungen an die Hersteller vernetzter Endgeräte. Die Handlungsempfehlungen sind wie folgt aufgelistet:

- IT-Sicherheitsbetrachtungen im Produktlebenszyklus berücksichtigen
- IT-Systeme so einfach wie möglich halten
- IT-Sicherheitskriterien als Standards implementieren

- Mitarbeiter, Kunden und sonstige Benutzer sensibilisieren
- Vorbild sein

5.2.2 Empfehlungen für Endnutzer

Im Umgang mit IT-Systemen ergeben sich für Endnutzer folgende zusammenfassende Empfehlungen:

- Sensibler Umgang mit persönlichen und fremden Daten
- Achtsam sein und Auffälligkeiten in der virtuellen Welt kritisch hinterfragen
- Unterstützung und Hilfe suchen
- Szenarien der virtuellen Welt auf die reale Welt projizieren
- Vorbild sein

6 Zusammenfassung und Ausblick

Die rasante Zunahme vernetzter und mit dem Internet verbundener Geräte, sowie der Anstieg an IT-Sicherheitsverletzungen, galten als Motivationsgrundlage dieser Thesis. Ziel war es, bestimmende IT-Sicherheitskriterien für vernetzte Endgeräte zu konzeptionieren und deren Relevanz und Anwendbarkeit nachzuweisen.
Als Grundlage für die Konzeptionierung der IT-Sicherheitskriterien, wurden im 2. Kapitel vernetzte Endgeräte anhand ihrer Hauptaufgaben klassifiziert und von anderen Geräten abgegrenzt. Das Resultat waren allgemeine Endgeräte, die eine 2-Wege-Kommunikation in TCP/IP-Netzwerken aufbauen können. Systeme die für den Datentransport eingesetzt werden und passive Geräte des Internet der Dinge, wurden nicht betrachtet. Im nächsten Schritt wurde eine typische Verwendung eines vernetzten Endgerätes dargestellt und in Komponenten unterteilt. Mit dieser Aufteilung wurde die Grundlage für differenzierende IT-Sicherheitsbetrachtungen gelegt.
Im 3. Kapitel erfolgte das Auswerten häufiger und bekannter Sicherheitsprobleme aus anerkannten Projekten, wie OWASP und einschlägiger Literatur. Diese Auswertungen wurden zusammengefasst und den zuvor definierten Komponenten mit typischen Angriffsvektoren zugeordnet. Die so erstellte Zusammenfassung diente als Grundlage für die Konzeptionierung der Sicherheitskriterien. Hierfür wurde eine Analyse mittels Cyber-Antipattern vorgenommen. Mithilfe eines angepassten Cyber-Antipattern Template, wurden die zusammengefassten IT-Sicherheitsprobleme behandelt und Lösungsmöglichkeiten vorgeschlagen, vgl. Kapitel 5.1.1 und Anhang A. Aus diesen so entstandenen Lösungen, konnten allgemeine IT-Sicherheitskriterien abgeleitet werden.
Der weitere Verlauf dieser Arbeit galt dem Nachweis der IT-Sicherheitskriterien. So wurden im 4. Kapitel verschiedene auf Modelle basierende, prozessorientierte und technische Ansätze auf ihre Anwendbarkeit untersucht. Beginnend mit der Untersuchung von klassischen IT-Sicherheitsmodellen konnte festgestellt werden, dass diese nicht ohne Erweiterungen auf die aktuellen Anforderungen der IT-Sicherheit angewendet werden können. Einen Ansatz der Anwendbarkeit für aktuelle IT-Sicherheitsanalysen, konnte mit der ProSA-Vorgehensweise gefunden werden. Daraufhin wurde am Beispiel des IT-Sicherheitskriteriums *Authentifizierung und Autorisierung* eine

angepasste Vorgehensweise nach der ProSA durchgeführt, vgl. Kapitel 4.2.2. Die Ergebnisse zeigten eine allgemeine Anwendbarkeit der Methode und konnten zudem einen Nachweis für die Anwendbarkeit des IT-Sicherheitskriteriums liefern.
Eine weitere Methode ist die Anwendung des IT-Grundschutz 200-2 des BSI. Mithilfe der Grundschutz-Methodik wurde eine modulare IT-Sicherheitsrichtlinie erstellt, deren Anwendungsspektrum Endgeräte mit verschiedenen Betriebssystemen (*macOS, iOS, Windows 10* und Browsern (*Firefox, Chrome*) abdeckt, vgl. Kapitel 4.3.1 und Anhang B.
Die technische Nachweisbarkeit wurde durch selbst erstellte Sicherheitsskripte realisiert. Die Sicherheitsskripte sind auf die IT-Sicherheitskriterien und die technischen Maßnahmen der IT-Sicherheitsrichtlinie ausgerichtet. Mithilfe dieser Skripte wurden die Sicherheitseinstellungen der Betriebsysteme (*macOS, Windows 10* untersucht. Die Ergebnisse zeigten zum einen die Anwendbarkeit der IT-Sicherheitskriterien und zum anderen, die teils unsicheren Standardeinstellungen der zwei überprüften Betriebssysteme, vgl. Anhang C und Kapitel 4.4.2.
Eine Bewertung der verwendeten Methoden und eine Ergebnisauswertung erfolgten im 5. Kapitel. Es wurden die verwendeten Methoden anhand allgemeiner Merkmale, wie Anwendbarkeit und Wiederholbarkeit miteinander verglichen. Zudem wurden allgemeine und nicht technische Handlungsempfehlungen für Hersteller und Anwender abgeleitet.
In dieser Thesis wurden neue Methoden verwendet, wie die Analyse mittels Cyber-Antipattern und die ProSA-Vorgehensweise für IT-Sicherheitsanalysen, vgl. Kapitel 3.2 und Kapitel 4.2.1. Diese Methoden zeigten vielversprechende Ansätze und könnten mit entsprechenden softwaregestützten Hilfsmitteln, Akzeptanz bei IT-Sicherheitsexperten und Nutzern erlangen. Die erstellten systemspezifischen Sicherheitsskripte aus Kapitel 4.4.2, können als Basis für eine Erstanalyse des IT-Sicherheitszustandes der verwendeten Systeme herangezogen und modular erweitert werden. Eine weitere Einsatzmöglichkeit sieht die Sicherheitsskripte als Bestandteile von Penetrationstests und IT-Audits vor.

Literaturverzeichnis

[AS14] Alqassem, I. ; Sventionovic, D.: A Taxonomy of Security and Privacy Requirements for the Internet of Things (IoT). In: *IEEE IEEM* (2014), S. 1244–1248

[Bau18] Baun, C.: *Computernetze kompakt*. 4. Auflage. Springer, 2018

[Bei14] Beissel, S.: *IT-Audit: Grundlagen Prüfungsprozess Best Practice*. 1. Auflage. ESV Erich Schmidt Verlag, 2014

[BSI08] BSI: *Hilfsmittel - Musterrichtlinien und Beispielkonzepte*. 2008. – https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/hilfmi/muster/musterrichtlinien/musterrichtlinien.html, letzter Zugriff: 2019-08-28

[BSI16] BSI: *Mit Sicherheit - BSI-Magazin 2016/01*. 2016. – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2016_01.pdf, letzter Zugriff: 2019-08-28

[BSI17a] BSI: *BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)*. 2017. – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_1.pdf, letzter Zugriff: 2019-08-28

[BSI17b] BSI: *BSI-Standard 200-2: IT-Grundschutz-Methodik*. 2017. – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf, letzter Zugriff: 2019-08-28

[BSI17c] BSI: *IT-Grundschutz: SYS.4.4 Allgemeines IoT-Gerät*. 2017. – https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_4_4_Allgemeines_IoT-Ger%C3%A4t.html, letzter Zugriff: 2019-08-28

[BSI17d] BSI: *Sichere Nutzung von Geräten unter Microsoft Windows 10 - Empfehlungen für Privatanwender*. 2017. – https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSIFB/Publikationen/BSI_CS_019.pdf, letzter Zugriff: 2019-08-28

[BSI19a] BSI: *Gesunder Menschenverstand - Surfen Sie mit gesundem Menschenverstand*. 2019. – https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Menschenverstand/menschenverstand_node.html, letzter Zugriff: 2019-08-28

[BSI19b] BSI: *IT-Grundschutz-Kompendium - Edition 2019*. 2019. – https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html, letzter Zugriff: 2019-08-28

[BSI19c] BSI: *Passwörter*. 2019. – https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html, letzter Zugriff: 2019-08-28

[CIS15] CIS: *CIS Mozilla Firefox 38 ESR Benchmark*. 2015. – https://learn.cisecurity.org/benchmarks, letzter Zugriff: 2019-08-28

[CIS18a] CIS: *CIS Apple iOS 12 Benchmark*. 2018. – https://learn.cisecurity.org/benchmarks, letzter Zugriff: 2019-08-28

[CIS18b] CIS: *CIS Apple macOS 10.13 Benchmark*. 2018. – https://learn.cisecurity.org/benchmarks, letzter Zugriff: 2019-08-28

[CIS18c] CIS: *CIS Google Chrome Benchmark*. 2018. – https://learn.cisecurity.org/benchmarks, letzter Zugriff: 2019-08-28

[CIS18d] CIS: *CIS Microsoft Windows 10 Enterprise (Release 1709) Benchmark*. 2018. – https://learn.cisecurity.org/benchmarks, letzter Zugriff: 2019-08-28

[CS19] Chapple, M. ; Seidl, D.: *PenTest+ Study Guide*. Wiley, 2019

[DGP+18] Derbyshire, R. ; Green, B. ; Prince, D. ; Mauthe, A. ; Hutchison, D.: An Analysis of Cyber Security Attack Taxonomies. In: *IEEE European Symposium on Security and Privacy Workshops* (2018), S. 153–161

[Eck14] Eckert, C.: *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. Oldenbourg, 2014

[Gad17] Gadatsch, A.: *Grundkurs Geschäftsprozess-Management*. 8. Auflage. Springer, 2017

[Gri08] Grimm, R.: IT-Sicherheitsmodelle. In: *Arbeitsberichte aus dem Fachbereich Informatik* Nr.3 (2008)

[Han18] Handelsblatt: *Wenn der Herzschrittmacher gehackt wird*. 2018. – https://www.handelsblatt.com/technik/medizin/medizintechnik-wenn-der-herzschrittmacher-gehackt-wird/21122168.html, letzter Zugriff: 2019-08-28

[IS19] Internet Security, Center for: *Center for Internet Security - About us*. 2019. – https://www.cisecurity.org/about-us/, letzter Zugriff: 2019-08-28

[Jej18] Jejdling, F.: *Ericsson Mobility Report November 2018*. 2018. – https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-november-2018.pdf, letzter Zugriff: 2019-08-28

[Kap13] Kappes, M.: *Netzwerk- und Datensicherheit*. 2. Auflage. Springer, 2013

[Kat17] Katthöfer, Ursula: *Interview mit Arne Schönborn - Die Wirtschaft Oktober 2017*. 2017. – https://www.ihk-bonn.de/fileadmin/dokumente/News/Die_Wirtschaft/Die_Wirtschaft_2017/10/Dokumente/Interview_mit_Arne_Schoenbohm.pdf, letzter Zugriff: 2019-08-28

[KBD16] Khodadadi, F. ; Buyya, R. ; Dastjerdi, A.V.: *Internet of Things: Principles and Paradigms*. Elsevier Inc., 2016

[Kep13] Keppel, V.: *Klassifikation und Analyse von IT-Sicherheitsmodellen*. 2013

[Kes13] Keszthelyi, A.: About Passwords. In: *Acta Polytechnica Hungarica* 10 (2013), Nr. 6, S. 99–118

[Kof18] Kofler, M.: *Hacking & Security - Das umfassende Handbuch*. Rheinwerk Computing, 2018

[KP14] Kumar, J. ; Patel, R.: A Survey on Internet of Things: Security and Privacy Issues. In: *International Journal of Computer Applications* 90 (2014), Nr. 11

[Kre17] Krebs, B.: *Who is Anna-Senpai, the Mirai Worm Author?* 2017. – https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/, letzter Zugriff: 2019-08-28

[Lue18] Lueth, K.: *State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating.* 2018. – https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/, letzter Zugriff: 2019-08-28

[MBQA18] Murad, G. ; Badarneh, A. ; Qusef, A. ; Almasalha, F.: Software Testing Techniques in IoT. In: *IEEE 2018 8th International Conference on Computer Science and Information Technology (CSIT)* (2018), S. 17–21

[Mow14] Mowbray, T.J.: *Cybersecurity: Managing Systems, Conducting Testing, and Investigating Instructions.* Wiley, 2014

[Mü11] Müller, K.-R.: *IT-Sicherheit mit System.* 4. Auflage. Vieweg+Teubner, 2011

[OWA16] OWASP: *Mobile Top 10 2016-Top 10.* 2016. – https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10, letzter Zugriff: 2019-08-28

[OWA18a] OWASP: *OWASP IoT Top 10 - 2018.* 2018. – https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf, letzter Zugriff: 2019-08-28

[OWA18b] OWASP: *OWASP Top 10 - 2017: Die 10 kritischsten Sicherheitsrisiken für Webanwendungen.* 2018. – https://www.owasp.org/images/9/90/OWASP_Top_10-2017_de_V1.0.pdf, letzter Zugriff: 2019-08-28

[PD12] Peterson, L.L. ; Davie, B.S.: *Computer networks : a systems approach.* Elsevier Inc., 2012

[Sch18] Schwichtenberg, H.: *Windows Powershell und Powershell Core - Der schnelle Einstieg.* Hanser Verlag, 2018

[Sim17] Simic, D.: *IT-Sicherheitsanalysen: Ein prozessorientiertes Vorgehensmodell.* DeGruyter, 2017

[Spr17] Spreitzenbarth, M.: *Mobile Hacking.* 1. Auflage. dpunkt.verlag, 2017

[TB16] Tanenbaum, A. S. ; Bos, H.: *Moderne Betriebssysteme.* 4. Auflage. Pearson, 2016

[ver18] VERINICE.: Benutzerhandbuch 1.17. In: *SerNet GmbH* (2018)

[ver19] VERINICE: *Verinice Produkt*. 2019. – https://verinice.com/produkt/, letzter Zugriff: 2019-08-28

[Wen18] WENDZEL, S.: *IT-Sicherheit für TCP/IP- und IoT-Netzwerke - Grundlagen, Konzepte, Protokolle, Härtung*. 1. Auflage. Springer, 2018

[WM16] WALLNER, S. ; MAYER, K.: Ein ganzheitliches IT-Sicherheitskonzept für Industrie 4.0 Infrastrukturen. In: *Datenschutz und Datensicherheit - DuD* 40 (2016), Jan, Nr. 1, 43–46. http://dx.doi.org/10.1007/s11623-016-0541-x. – DOI 10.1007/s11623–016–0541–x. – ISSN 1862–2607

[Wü11] WÜNSCHE, M.: *Prüfungsvorbereitung für IT-Berufe*. 5. Auflage. Springer, 2011

Abbildungsverzeichnis

Listings

Tabellenverzeichnis

Abkürzungsverzeichnis

BPMN Business Process Management Notation

BSI Bundesamt für Sicherheit in der Informationstechnik

CIS Center of Security

COBIT Control Objectives for Information and Related Technology

DAC Discretionary Access Control

DoS Deny of Service

DSGVO Datenschutz-Grundverordnung

ECAA Event of Condition do Action else do Alternative Action

ICS Industrial Control System

IEC International Electrotechnical Commission

IoT Internet of Things

IP Internetprotokoll

IS Informationssicherheit

ISB Informationssicherheitsbeauftragte

ISMS Information Security Management System

ISO International Organization for Standardization

IT Informationstechnologie

ITIL Information Technology Infrastructure Library

MAC Mandatory Access Control

MitM Man in the Middle

NIST National Institute of Standards and Technology

OWASP Open Web Application Security Project

PDCA Plan Do Check Act

PKI Public-Key-Infrastruktur

ProSA Prozessorientierte Vorgehensweise für Sicherheitsanalysen

SQL Structured Query Language

TAN Transaktionsnummer

TCP Tranmission Control Protocol

WAN Wide Area Network

WMI Windows Management Instrumentation

WPS Windows PowerShell

XML Extensible Markup Language

A Cyber-Antipattern

Antipattern	Authentifizierung- & Autorisierungsprobleme und -schwächen
Verwandte Bezeichnung(en)	Passwörter, Credentials, Zugangsdaten, Identitäten
Gegenwärtige Lösung	Verwendung und Verwahrung sicherer und komplexer Passwörter
Titel der Erneuerungslösung	Mehrstufige Authentifizierung und Autorisierung und die Entwicklung neuer Authentifizierungstechnologien
Beeinträchtigte Schutzziele	Integrität, Vertraulichkeit
Betroffene Komponente(n)	Nutzer, Nutzerschnittstelle Äußere und Innere Funktionalität

Antipattern-Lösung
Passwörter müssen so gestaltet sein, das sie dem aktuellen technischen Stand als *sicher* entsprechen. Dabei umfassen die meisten Empfehlungen und technischen Implementierungen eine Mindestlänge von 8 Zeichen, welche Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten sollen, keinesfalls jedoch Wörterbucheinträge. Weiterhin ist der zyklische Austausch von Passwörtern unter Verwendung neuer Passwörter gefordert. Alle diese Eigenschaften werden als Komplexizitätsanforderungen bezeichnet.

Symptome & Auswirkungen
Komplexizitätsanforderungen an Passwörter provozieren das unsichere Ablegen und transportieren von Nutzerdaten, bis hin zur Aushändigung an Dritte. Außerdem kann nicht gewehrleistet sein, das die Passwörter beim einem Dienstanbieter sicher sind.

Erneuerungslösungen
Die Mehrstufige Authenifizierungs und Autorisierung ist gefordert. Nutzerfreundliche Verfahren sind dabei anzustreben. Um die Akzeptanz der Nutzer zu erhöhen, sollten passwortfreie Authentifizierungsverfahren entwickelt und implementiert werden.

Tabelle A.1: Antipattern - Authentifizierung und Autorisierung

Antipattern	Sicherheitsrelevante Fehlfunktionen durch Standardauslieferungen
Verwandte Bezeichnung(en)	Nicht benötigte Funktionen und Komponenten
Gegenwärtige Lösung	Funktionalität und Kompatibilität gilt als Maß für Produktqualität
Titel der Erneuerungslösung	*"Security by default and design"*
Beeinträchtigte Schutzziele	Integrität, Vertraulichkeit
Betroffene Komponente(n)	Alle Komponenten betreffend

Antipattern-Lösung
Nach der Auslieferung sind eine Reihe von Funktionen und Komponenten anzupassen bzw. zu deaktivieren um die Sicherheit von Systemen oder den Datenschutz zu erhöhen. Dies erfolgt meist im Rahmen einer Erstkonfiguration bei Inbetriebnahme von Geräten.

Symptome & Auswirkungen
Endnutzer besitzen selten das technische Wissen um Systemanpassungen und Härtungen durchführen zu können. Weiterhin ist die Informationsbeschaffung nicht immer einfach. Herstellerbedingt sind viele Systemhärtungen nicht möglich. Mit der Installation von Updates, werden viele Betriebssystemkomponenten auf Standardeinstellungen zurückgesetzt.

Erneuerungslösungen
Die Funktionsweise sollte angelehnt der Arbeitsweise von Firewalls sein, die nach dem Prinzip *"Es ist alles verboten, was nicht explizit erlaubt ist."* , arbeiten. So können beispielsweise nach standardisierten Anwendungsfällen und Sicherheitsanforderungen, benötigte Funktionen und Komponenten aktiviert werden.

Tabelle A.2: Antipattern - Standardkomponenten und Standardauslieferungen

Antipattern	Einsatz und Abhängigkeit von unsicheren und veralteten Komponenten und Diensten
Verwandte Bezeichnung(en)	Produktlebenszyklus, Kompatibilität
Gegenwärtige Lösung	Zertifizierung von Hard- und Softwarekomponenten
Titel der Erneuerungslösung	Verpflichtende Zulassungs- und Betriebsverfahren
Beeinträchtigte Schutzziele	Integrität, Verfügbarkeit, Vertraulichkeit
Betroffene Komponente(n)	Äußere und Innere Funktionalität

Antipattern-Lösung
Hard- und Softwarekomponenten können für den Einsatz zertifiziert werden.

Symptome & Auswirkungen
Hard- und Softwarezertifizierungen sind freiwillig und nicht standardisiert. Mit dem Zulassen von nicht zertifizierten Drittanbieterprodukten, soll die Kompatibilität erhöht werden. Zertifizierungsverfahren zu durchlaufen ist mit zusätzlichem Aufwand und Kosten verbunden.

Erneuerungslösungen
Eine Komponentenzulassung und der Betrieb eines Produktes, sollte nur mit standardisierten und allgemein anerkannten Zertifizierungen möglich sein.

Tabelle A.3: Antipattern - Verpflichtende Komponentenzertifizierung

Antipattern	Unsicherer und unzureichend verschlüsselter Datentransfer und Datenspeicherung
Verwandte Bezeichnung(en)	Funktionalität vor Sicherheit
Gegenwärtige Lösung	Verschlüsselungsmethoden für den Netzwerkverkehr und Endgeräte
Titel der Erneuerungslösung	Standardisierung und Verpflichtung von Verschlüsselungsmethoden für Daten- und verkehr
Beeinträchtigte Schutzziele	Integrität, Verfügbarkeit, Vertraulichkeit
Betroffene Komponente(n)	Äußere und Innere Funktionalität Netzwerkschnittstelle und Kommunikation Externe Dienste

Antipattern-Lösung
Der Einsatz verschiedener Hard- und Softwareprodukte für die Verschlüsselung der Daten und des Datenverkehrs soll wirksamen Schutz vor Kompromittierungen bieten.

Symptome & Auswirkungen
Es existieren keine verpflichtenden Standards für die Verschlüsselung der Kommunikation und der Datenablage. Die Implementierung verursacht zusätzliche Kosten und Zeitaufwand.

Erneuerungslösungen
Die Verschlüsselung des Datenverkehrs und der Datenablage sollte standardisiert und verplichtend sein.

Tabelle A.4: Antipattern - Zertifiziert zugelassener Datentransfer

Antipattern	Menschliches Fehlverhalten
Andere Bezeichnung(en)	Phishing, Social Engineering
Gegenwärtige Lösung	Schulungen und Sensibilisierungen
Titel der Erneuerungslösung	Einschlägige und häufige Kampanien zur Sensibilisierung
Beeinträchtigte Schutzziele	Integrität, Vertraulichkeit
Betroffene Komponente(n)	Nutzer

Antipattern-Lösung
Durch gezielte Schulungs- und Sensibilisierungsprogramme können Gefahren durch menschliches Fehlverhalten reduziert werden. Oft werden solche Kampanien von Unternehmen durchgeführt, um ihre Mitarbeiter zu sensibilisieren.

Symptome & Auswirkungen
Schulungs- und Sensibilisierungsprogramme finden selten statt und sind somit nicht auf die aktuellen Gefährdungen der IT angepasst. Es fehlen zudem oft wirksame Überprüfungen über den erzielten Erfolg solcher Kampanien. Mit der oft fehlenden Einsicht in eigene Handlungsweisen steigen die Risiken durch menschliches Fehlverhalten. Im privaten Bereich gibt es keine Sensibilisierungsmaßnahmen.

Erneuerungslösungen
Häufige und einschlägige Kampanien sind notwendig. Diese sollten sich an den ständig verändernden Methoden der Angreifer orientieren und die Nutzer in unbequeme Situationen bringen. So könnten Kampanien von Banken darauf abzielen die Nutzer durch Maßnahmen aktiv zu täuschen. Damit könnte die Vorgehensweise der Angriffe und deren Auswirkungen verdeutlicht werden.

Tabelle A.5: Antipattern - Menschliches Fehlverhalten

Antipattern	Unzureichendes Logging und Monitoring
Andere Bezeichnung(en)	Protokollierung, Loganalyse
Gegenwärtige Lösung	Integrierte System- und Sicherheitscenter
Titel der Erneuerungslösung	Erweiterte Loganalyse mit Reaktionen
Beeinträchtigte Schutzziele	Integrität, Verfügbarkeit, Vertraulichkeit
Betroffene Komponente(n)	Äußere und Innere Funktionalität Netzwerkschnittstelle und Kommunikation Externe Dienste

Antipattern-Lösung
In Unternehmen werden meist je nach Größe Netzwerk-Operating-Center (NOC) eingesetzt, bei denen sich Mitarbeiter mit Logfileanalysen, Logserver und Erkennungssystemen auseinandersetzen.

Symptome & Auswirkungen
Es gibt keine Meldungen, ob dass Logging selbst funktioniert. Die Verantwortung für Konfiguration, Auswertung und Reaktion von Ereignissen ist weitgehend ungeklärt. Es gibt keine Alarmfunktionalitäten für Konfigurationsdaten von Betriebssystemkomponenten und Software.

Erneuerungslösungen
Für vernetzte Endgeräte ist es notwendig, auch nach eingetretenen Ereignissen die Nutzer in verständlicher Form zu informieren und Handlungsempfehlungen vorschlagen. Technologien der künstlichen Intelligenz könnten bei der Erkennung und Reaktion unterstützen.

Tabelle A.6: Antipattern - Monitoring und Reaktion

B Modulare IT-Sicherheitsrichtlinie

IT-Sicherheitsrichtlinie	
Vernetzte Endgeräte	
Zielsetzung & Geltungsbereich	
Durch die Möglichkeit der sicheren und für die Nutzer transparenten Verwendung informationstechnischer Systeme und Dienste, soll der Schutz von Vertraulichkeit, Verfügbarkeit und Integrität gewährleitet werden. Die Richtlinie ist für Anwendungsfälle konzipiert, bei denen Benutzer mittels persönlicher Endgeräte, verschiedene Dienste im Internet durch Webbrowser sicher verwenden können.	
Abgrenzung	
Diese Richtlinie behandelt keine Maßnahmen der sicheren Verwendung von öffentlichen Terminals oder offenen Netzwerken.	
Gefährdungen	
Nachfolgend werden die wichtigsten Gefährdungen im Zusammenhang mit der Sicherheit vernetzter Endgeräte nach dem Grundschutz-Kompendium 7.0 zusammengefasst.	
[G0.14] [G0.15] [G.036] [G0.42]	Ausspähen und Abhören von Informationen, Gesprächen, Kommunikationskanälen, sowie Identitätsdiebstahl; auch unter Verwendung von Social Engineering
[G0.16] [G0.17] [G0.24] [G0.25] [G0.26]	Diebstahl, Verlust Zerstörung, Fehlfunktionen oder Ausfall von Geräten und Datenträgern
[G0.20] [G0.21] [G0.22]	Manipulationen von Hardware, Software und Informationen, auch aus unzuverlässigen Quellen
[G0.30] [G0.31]	Unberechtigte oder fehlerhafte Nutzung oder Administration von Geräten und Systemen
[G0.19] [G0.29] [G0.38]	Offenlegung schützenswerter Information unter Verstoß von Gesetzen und Regelungen
[G0.18] [G0.28]	Fehlplanung oder fehlerhafte Anpassung, sowie Software-Schwachstellen oder Softwarefehler
[G0.40] [G0.45]	Verhinderung von Diensten (Deny of Service) und Datenverlust
Verantwortungen	
Die Bereitstellung von sicheren Systemen und Diensten wird durch die Hersteller oder Dienstleister verantwortet. Möglichkeiten zur Wirksamkeitsüberprüfungen werden den Nutzern verständlich zur Verfügung gestellt. Die Dienstanbieter und die Dienstnutzer haben eine Sorgfaltspflicht im Umgang mit Nutzerdaten.	
Organisatorische Maßnahmen	
Folgende übergreifende organisatorische Maßnahmen sind vorgesehen.	
[ISMS.1.M16]	Erstellung von zielgruppengerechten Sicherheitsrichtlinien
[ISMS.1.M14] [ORP.3.M4] [ORP.3.M6] [ORP.3.M8]	Sensibilisierung von Informationssicherheit durch Konzepte von Schulungsprogrammen, sowie die Planung und Durchführung von Sensibilisierungs- und Schulungsmaßnahmen mit Wirksamkeitsprüfungen

Technische Maßnahmen	
Das Erreichen der IT-Sicherheit von Endgeräten, kann durch allgemeine technische Maßnahmen erfolgen, unabhängig vom eingesetzten System oder der eingesetzten Anwendung.	
[SYS.2.1.A1] [SYS.2.1.A5] [SYS.3.1.A2] [SYS.3.2.1.A4] [SYS.2.1.A2]	Das Entsperren eines obligatorischen Gerätezugriffsschutzes oder einer Bildschirmsperre soll durch eine Benutzerauthentifizierung erfolgen. Die Auswahl aufgabenspezifischer Nutzer setzt eine Rollentrennung voraus.
[SYS.2.1.A31] [SYS.3.1.A3] [SYS.3.1.A4] [APP.1.2.A11]	Verwendete Geräte sind mit einer aktivierten und konfigurierten Firewall oder einem Paketfilter, sowie einem Antivirenprogramm ausgestattet.
[SYS.2.1.A3] [SYS.2.1.A14] [SYS.3.2.1.A5] [APP.1.2.A4]	Eingesetzte Hard- und Softwarekomponenten sind möglichst automatisiert mit aktuellen Updates , Patches und Firmware zu versorgen.
[SYS.2.1.A28] [SYS.3.1.A13] [SYS.3.2.1.A11]	Die Geräte und Speicher sollten bei Auslieferung oder spätestens bei Inbetriebnahme verschlüsselt werden.
[SYS.2.1.A15] [SYS.3.2.1.A3] [SYS.3.2.1.A9] [SYS.3.2.1.A16] [APP.1.2.A5]	Bei der Inbetriebnahme ist eine sichere Grundkonfiguration einzustellen und abhängig vom geplanten Einsatzzweck sind unsichere und nicht benötigte Programme zu deinstallieren. Weiter sind überflüssige Funktionalitäten zu entfernen oder zu deaktivieren.
[APP.1.2.A1]	Anwendungen, Browser und Browsertabs sind jeweils in isolierten Umgebungen innerhalb des Betriebssystems zu betreiben.
[SYS.2.1.A18] [APP.1.2.A2] [APP.1.2.A3]	Alle Kommunikationsverbindungen über Netzwerke sind nach aktuellem Stand der Technik zu verschlüsseln.
[SYS.3.2.1.A8]	Die Installation von Applikationen und Erweiterungen sollte nur aus vertrauenswürden und zertifizierten Quellen erfolgen.
[SYS.2.1.A27] [SYS.3.1.A1]	Sicheres Löschen von Geräteeinstellungen und Nutzerdaten bei Rücknahme, Weitergabe und Außerbetriebnahme der Geräte.
[SYS.2.1.A7] [SYS.2.1.A29]	Alle im Zusammenhang mit dieser Richtlinie relevanten Sicherheitsmaßnahmen sind durch technische Hilfsmittel zu überwachen und zu protokollieren.
Anhang	
Der Anhang dieser Richtlinie sieht die Umsetzung der Maßnahmen vor. Dabei können je nach Einsatzszenario verschiedene Optionen gewählt werden.	

Tabelle B.1: Modulare IT-Sicherheitsrichtlinie

Anforderung	Kurzbezeichnung	Windows 10 [CIS18d]	MacOS 10.13 [CIS18b]	iOS 12 [CIS18a]*	Firefox [CIS15]*	Chrome [CIS18c]*
[SYS.2.1.A1]	Benutzerauthentifizierung	S. 37 - S. 55	S. 117 - S. 174	S. 46 - S. 55	n.v.*	S. 14 - S. 15 S. 24 - S. 25 S. 36 - S. 37
[SYS.2.1.A5] [SYS.3.1.A2] [SYS.3.2.1.A4]	Bildschirmsperre Zugriffsschutz	S. 1112 - S. 1120 Bildschirmschoner*			n.v.*	n.v.*
[SYS.2.1.A2]	Rollentrennung	S. 56 - S. 273		n.v.*	n.v.*	n.v.*
[SYS.2.1.A31] [SYS.3.1.A3]	lokaler Paketfilter, Firewall	S. 367 - S. 418 Firewall*	S. 62 - S. 69	n.v.*	n.v.*	n.v.*
[SYS.3.1.A4]	Antivirus	S. 508 - S. 509 Defender*	S. 61 Gatekeeper*	n.v.*	S. 27 S. 65 - 70	-
[APP.1.2.A11]	Schädliche Inhalte Überprüfen			S. 40 - S. 41 Fraud Warning*		
[SYS.2.1.A3] [SYS.2.1.A14] [SYS.3.2.1.A5]	(Auto)Update und Patches	-	S. 14 - S. 21	S. 139	S. 15 - S. 22	-
[APP.1.2.A4]	Browseraktualisierung	-	-	-		
[SYS.2.1.A28] [SYS.3.1.A13] [SYS.3.2.1.A11]	Geräte- und Speicherverschlüsselung	Bitlocker* TPM*	S. 53 - S. 60	S.22 Backups*	n.v.*	n.v.*
[SYS.2.1.A15] [SYS.3.2.1.A3]	Installation und Grundkonfiguration	-	-	-	-	-
[SYS.3.2.1.A9]	Funktionale Erweiterungen	-	S. 186 - S.187	-	S. 56 - S. 64	S. 56 - S. 64
[SYS.3.2.1.A16]	Nicht benötigte Komponenten	-	S. 38 - S. 49 S. 102 - S. 110	S. 64 - S. 109	S. 23 - S. 31 S. 41 - S. 47	S. 12 - S. 15
[APP.1.2.A5]	Grundkonfiguation	-	-	-	-	-
[APP.1.2.A1]	Sandboxing	-	-	-	-	S. 42 - S. 43
[SYS.2.1.A18]	Verschlüsselung (TLS)	-	-	S. 24 - S. 25	S. 32 - S. 40	Erweiterung*
[APP.1.2.A2]	Kommunikations-verschlüsselung	-	-			
[APP.1.2.A3]	Zertifikate	-	-	-		-
[SYS.3.2.1.A8]	Vertrauenswürdige und zertifizierte Quellen	-	-	-	-	-
[SYS.2.1.A27] [SYS.3.1.A7]	Außerbetriebnahme, Rücknahme, Weitergabe	-	-	S. 80 - S. 81	n.v.*	n.v.*
[SYS.2.1.A7] [SYS.2.1.A29]	Protokollierung und Systemüberwachung	S. 367 - S. 418 Firewall*	S. 94 - S. 101	-	n.v.*	n.v.*

[CIS15]*	Kenntnisse mit tieferen Konfigurationesmöglichkeiten wie about:config werden vorausgesetzt
[CIS18a]*	setzt größtenteils den Einsatz von Profilen über MDM-Lösungen und Apple Configurator voraus
[CIS18c]*	Die Dokumentation setzt Umgang mit Windows Registry voraus.
Backups*	beschränkt auf diese Funktionalität
Bildschirmschoner*	Für weitere Konfigurationen sind diese Suchbegriffe im MDSN-Netzwerk unter https://msdn.microsoft.com/de-de/ hilfreich.
Bitlocker* TPM*	Für weitere Konfigurationen sind diese Suchbegriffe im MDSN-Netzwerk unter https://msdn.microsoft.com/de-de/ hilfreich.
Erweiterung*	Mit Erweiterungen wie "HTTPS Everywhere" möglich.
Firewall* Defender*	Für weitere Konfigurationen sind diese Suchbegriffe im MDSN-Netzwerk unter https://msdn.microsoft.com/de-de/ hilfreich.
Fraud Warning*	Beschränkt auf diese Funktionalität.
n.v.*	Funktion in der eingesetzten Technologie nicht vorhanden.

Tabelle B.2: Anhang zur IT-Sicherheitsrichtlinie

C Sicherheitsskripte

C.1 Sicherheitsskript für Windows10-Systeme

```
###
# Überprüfen von Client-Sicherheitseinstellungen nach dem BSI Grundschutz-Kompendium
# Betrifft: Allgemeine IT-Sicherheitsrichtlinie für vernetzte Endgeräte
# PowerShell für Windowsgeräte
###
# Autor: T. Stemplewitz
# Änderungsdatum: 2019-08-28
###

# Variablen und Einstellungen

$datetime_cstm = $((get-date).ToLocalTime()).ToString("yyyy-MM-dd HH:mm:ss")
$date_cstm = $((get-date).ToLocalTime()).ToString("yyyyMMdd")
$winver = (Get-WmiObject -class Win32_OperatingSystem).Caption
$curr_user = $env:UserName
$protokoll_dat = "$date_cstm-protokoll-win.txt"

# Allgemeine Funktionen

function Write-Color([String[]]$Text, [ConsoleColor[]]$Color) {
# Funktion Konsolenfarben

  for ($i = 0; $i -lt $Text.Length; $i++) {
  Write-Host $Text[$i] -Foreground $Color[$i] -NoNewLine
  }
  Write-Host
}

function lauf_beginn_f {
# Funktion Kopf_Lauf

write-host "‘t                                                        "
write-host "‘t -------------------------------------------------------"
write-host "‘t Test von allgemeinen Sicherheitseinstellungen"
write-host "‘t -------------------------------------------------------"
write-host "‘t -------------------------------------------------------"
write-host "‘t eingesetzte Version:" $winver
write-host "‘t Datum: " $datetime_cstm "Uhr"
write-host "‘t -------------------------------------------------------"
write-host "‘t Beginn: Testlauf                                       "
write-host "‘t -------------------------------------------------------"
}
```

```
function protokoll_beginn_f {
# Funktion Kopf_Datei Auswertung

"`t                                    "        | set-content $protokoll_dat
"`t -------------------------------------------------------" | add-content
    $protokoll_dat
"`t Auswertung der Sicherheitstests"          | add-content $protokoll_dat
"`t eingesetzte Version: $winver"             | add-content $protokoll_dat
"`t Datum:  $datetime_cstm Uhr"               | add-content $protokoll_dat
"`t ---------------------------------------" | add-content $protokoll_dat
"`t Beginn: Auswertung                "        | add-content $protokoll_dat
"`t ---------------------------------------" | add-content $protokoll_dat
}

#Testfunktionen

function kontosec_lauf_f {
#Funktionslauf: Kontorichtlinien

  write-host "`t                              "
  write-host "`t Kontorichtlinien"
  write-host "`t ----------------------------"

  $Konto = net accounts
  foreach($i in $Konto)
  {
    if ($i -like "*Sperrschwelle*")
    {
      if ($i -like "*3*")
      {
        write-Color -Text "`t   Sperrschwelle:", "`t [1]" -Color White, green
        $kennw_sperrschw_check = 1
      }
      else
      {
        write-Color -Text "`t   Sperrschwelle:", "`t [0]" -Color White, red
        $kennw_sperrschw_check = 0
      }
    }

  if ($i -like "*Sperrdauer*")
  {
    if ($i -like "*30*")
    {
      write-Color -Text "`t   Sperrdauer:", "`t`t [1]" -Color White, green
      $kennw_sperrd_check = 1
    }
    else
    {
      write-Color -Text "`t   Sperrdauer:", "`t`t [0]" -Color White, red
      $kennw_sperrd_check = 0
    }
    }

  if ($i -like "*fenster*")
  {
```

```
  if ($i -like "*30*")
  {
    write-Color -Text "`t   Kontensperrung Reset:", " [1]" -Color White, green
    $kennw_sperrf_check = 1
  }
  else
  {
    write-Color -Text "`t   Kontensperrung Reset:", " [0]" -Color White, red
    $kennw_sperrf_check = 0
  }
}

if ($i -like "*Minimale Kennwortl*")
{
  if ($i -like "*8*")
  {
    write-Color -Text "`t   Kennwortlaenge:", "`t [1]" -Color White, green
    $kennw_laenge_check = 1
  }
  else
  {
    write-Color -Text "`t   Kennwortlaenge:", "`t [0]" -Color White, red
    $kennw_laenge_check = 0
  }
}

if ($i -like "*Kennwortchron*")
{
  if ($i -notlike "*Kein*")
  {
    Write-Color -Text "`t   Kennwortchronik:", "`t [1]" -Color White, green
    $kennw_chronik_check = 1
  }
  else
  {
    Write-Color -Text "`t   Kennwortchronik:", "`t [0]" -Color White, red
    $kennw_chronik_check = 0
  }
}
}

# Auswertung
if ($kennw_sperrschw_check -eq 1 -and $kennw_sperrd_check -eq 1 -and
  $kennw_sperrf_check-eq 1 -and $kennw_laenge_check -eq 1 -and $kennw_laenge_check -eq
   1 -and  $kennw_chronik_check -eq 1)
{
  "`t                                          " | add-content $protokoll_dat
  "`t  Kontorichtlinien:            [ERFÜLLT] " | add-content $protokoll_dat
  "`t ----------------------------------------" | add-content $protokoll_dat
}
else
{
  "`t                                          " | add-content $protokoll_dat
  "`t  Kontorichtlinien:      [NICHT ERFÜLLT] " | add-content $protokoll_dat
  "`t ----------------------------------------" | add-content $protokoll_dat
  "`t   Handlungsempfehlung:"                   | add-content $protokoll_dat
```

```
    "`t    - Einstellungen im Gruppenrichtlinieneditor 'gpedit': " | add-content
    $protokoll_dat
    "`t      Computerconfiguration -> Windows-Einstellungen ->" | add-content
    $protokoll_dat
    "`t      Sicherheitseinstellungen -> Kontorichtlinien"      | add-content
    $protokoll_dat
    "`t    - Aktuelle Empfehlungen können dem "                 | add-content
    $protokoll_dat
    "`t      IT-Grundschutz-Kompendium entnommen werden."       | add-content
    $protokoll_dat
  }
}

 function admin_lauf_f {
  #Prüfung, ob angemeldeter Benutzer über Administrationsrechte verfügt

  write-host "`t                              "
  write-host "`t Rollentrennung"
  write-host "`t ----------------------------"

  $admingroup = net localgroup Administratoren
  if ($admingroup | Select-String -Pattern "$curr_user")
  {
    Write-Color -Text "`t   Administrationsrechte:", "[0]" -Color White, red
    $admin_check = 0

    # Auswertung
    "`t                                          " | add-content $protokoll_dat
    "`t   Administrationsrechte:[NICHT ERFÜLLT] " | add-content $protokoll_dat
    "`t ----------------------------------------"         | add-content $protokoll_dat
    "`t   Benutzer ist in der Gruppe der Administratoren."| add-content $protokoll_dat
    "`t   Handlungsempfehlung:"                           | add-content $protokoll_dat
    "`t    - Nutzer aus der Gruppe der Administratoren entfernen."    | add-content
    $protokoll_dat
    "`t    - Separaten Nuter für administrative Tätigkeiten anlegen." | add-content
    $protokoll_dat
  }
  else
  {
    Write-Color -Text "`t   Administrationsrechte:", "[1]" -Color White, green
    $admin_check = 1

    # Auswertung
    "`t                                          " | add-content $protokoll_dat
    "`t  Administrationsrechte:       [ERFÜLLT] " | add-content $protokoll_dat
    "`t ----------------------------------------" | add-content $protokoll_dat
  }
}

function update_lauf_f {
  # Windows Version

  write-host "`t                              "
  write-host "`t Updateverhalten"
  write-host "`t ----------------------------"
```

```
if ((Get-WmiObject -class Win32_OperatingSystem).Caption -like "*Windows 10*")
{
  Write-Color -Text "`t   Windows Version:", "`t [1]"-Color White, green
  $winver_check = 1
}
else
{
  Write-Color -Text "`t   Windows Version:", "`t [0]"-Color White, red
  $winver_check = 0
}

# Windows Updatedienst

if ((Get-Service wuauserv | Where-Object {$_.Status -eq "Running"}))
{
  Write-Color -Text "`t   Updatedienst:", "`t [1]"-Color White, green
  $update_check = 1
}
else
{
Write-Color -Text "`t   Updatedienst:", "`t [0]"-Color White, yellow
$update_check = 0
}

# Auswertung
if ($winver_check -eq 1 -and $update_check -eq 1)
{
  "`t                                          "| add-content $protokoll_dat
  "`t  Updateverhalten:             [ERFÜLLT] "| add-content $protokoll_dat
  "`t ----------------------------------------"| add-content $protokoll_dat
}
elseif  ($winver_check -eq 0)
{
  "`t                                         " | add-content $protokoll_dat
  "`t  Updateverhalten:   [TEILWEISE ERFÜLLT]" | add-content $protokoll_dat
  "`t ----------------------------------------"| add-content $protokoll_dat
  "`t   Handlungsempfehlung:"                  | add-content $protokoll_dat
  "`t    - Upgrade auf Windows 10 durchführen."| add-content $protokoll_dat
}
elseif  ($update_check -eq 0)
{
  "`t                                          " | add-content $protokoll_dat
  "`t  Updateverhalten:   [TEILWEISE ERFÜLLT] " | add-content $protokoll_dat
  "`t ----------------------------------------" | add-content $protokoll_dat
  "`t   Handlungsempfehlung:" | add-content $protokoll_dat
  "`t    - Automatische Updates einstellen."  | add-content $protokoll_dat
}
else
{
  "`t                                          " | add-content $protokoll_dat
  "`t  Updateverhalten:       [NICHT ERFÜLLT] " | add-content $protokoll_dat
  "`t ----------------------------------------" | add-content $protokoll_dat
  "`t   Handlungsempfehlung:"                   | add-content $protokoll_dat
  "`t    - Upgrade auf Windows 10 durchführen." | add-content $protokoll_dat
  "`t    - Automatische Updates einstellen."    | add-content $protokoll_dat
}
```

```
}

function firewall_lauf_f {
  # Firewall

  write-host "`t                                "
  write-host "`t Firewall"
  write-host "`t ----------------------------    "

  $Firewall_check = Get-ItemProperty -Path 'Registry::HKEY_LOCAL_MACHINE\SOFTWARE\
    Policies\Microsoft\WindowsFirewall\DomainProfile' -Name EnableFirewall
  if ($Firewall_check.EnableFirewall -eq 1)
  {
    Write-Color -Text "`t   Firewall:", "`t`t [1]" -Color White, green
    $firew_check = 1
  }
  else
  {
    Write-Color -Text "`t   Firewall:", "`t`t [0]" -Color White, red
    $firew_check = 0
  }

  # Defender
  if ((Get-Service Windefend | Where-Object {$_.Status -eq "Running"}))
  {
    Write-Color -Text "`t   Defender:", "`t`t [1]"-Color White, green
    $defend_check = 1
  }
  else
  {
    Write-Color -Text "`t   Defender:", "`t`t [0]"-Color White, yellow
    $defend_check = 0
  }

  # Auswertung
  if ($firew_check -eq 1 -and $defend_check -eq 1)
  {
    "`t                                          " | add-content $protokoll_dat
    "`t  Firewall:                    [ERFÜLLT] " | add-content $protokoll_dat
    "`t ----------------------------------------" | add-content $protokoll_dat
  }
  elseif  ($firew_check -eq 0)
  {
    "`t                                          " | add-content $protokoll_dat
    "`t  Firewall:          [TEILWEISE ERFÜLLT] " | add-content $protokoll_dat
    "`t ----------------------------------------" | add-content $protokoll_dat
    "`t   Handlungsempfehlung:" | add-content $protokoll_dat
    "`t    - Prüfen, ob bei aktivierter Firewall der eingehende Netzwerkverkehr geblockt
     wird."  | add-content $protokoll_dat
  }
  elseif  ($defend_check -eq 0)
  {
    "`t                                           "  | add-content $protokoll_dat
    "`t  Firewall:          [TEILWEISE ERFÜLLT] " | add-content $protokoll_dat
    "`t ----------------------------------------" | add-content $protokoll_dat
    "`t   Handlungsempfehlung:" | add-content $protokoll_dat
```

```
    "`t    - Prüfen, ob alternativer Virenscanner "  | add-content $protokoll_dat
    "`t      installiert und aktuell ist."  | add-content $protokoll_dat
  }
  else
  {
    "`t                                          "  | add-content $protokoll_dat
    "`t  Firewall:              [NICHT ERFÜLLT] " | add-content $protokoll_dat
    "`t ----------------------------------------" | add-content $protokoll_dat
    "`t   Handlungsempfehlung:" | add-content $protokoll_dat
    "`t    - Firewall aktivieren und eingehenden Netzwerkverkehr blockieren."  | add-
    content $protokoll_dat
    "`t    - Prüfen, ob alternativer Virenscanner installiert und aktuell ist."  | add-
    content $protokoll_dat
  }
}

function verschl_lauf_f {
  # Check von Bitlocker auf Laufwerke aktiviert ist

  write-host "`t                              "
  write-host "`t Verschluesselung"
  write-host "`t ----------------------------"

  $bitlck = manage-bde -status c:

  if ($bitlck -like "*Der Schutz ist aktiviert*")
  {
    Write-Color -Text "`t   Bitlocker:", "`t`t [1]" -Color White, green
     $bitl_check = 1

    # Auswertung
    "`t                                          " | add-content $protokoll_dat
    "`t  Verschluesselung:            [ERFÜLLT] " | add-content $protokoll_dat
    "`t ----------------------------------------" | add-content $protokoll_dat
    "`t   - Laufwerk c:\ ist verschluesselt"      | add-content $protokoll_dat

  }
  elseif ($bitlck -like "*Administratorrechte*")
  {
    Write-Color -Text "`t   Bitlocker: ", "`t`t [0]" -Color White, yellow
    $bitl_check = 0

    # Auswertung
    "`t                                          " | add-content $protokoll_dat
    "`t  Bitlocker Status:         [UNBESTIMMT] " | add-content $protokoll_dat
    "`t ----------------------------------------" | add-content $protokoll_dat
    "`t   Handlungsempfehlung:" | add-content $protokoll_dat
    "`t    - Erneute Prüfung mit administrativen Rechten." | add-content $protokoll_dat

  }
  else
  {
    Write-Color -Text "`t   Bitlocker:", "`t`t [0]" -Color White, red
    $bitl_check = 0

    # Auswertung
```

```
    "`t                                          " | add-content $protokoll_dat
    "`t  Bitlocker Status:      [NICHT ERFÜLLT] " | add-content $protokoll_dat
    "`t ----------------------------------------" | add-content $protokoll_dat
    "`t   Handlungsempfehlung:" | add-content $protokoll_dat
    "`t    - Mit administrativen Rechten den Befehl 'manage-bde -on c:' ausführen" | add
    -content $protokoll_dat
    "`t    - Weiterführende Literatur beachten"   | add-content $protokoll_dat
  }
}

function log_lauf_f {
  # Pruefen, ob Protokollierung von allen eingesehen werden darf

  write-host "`t                                 "
  write-host "`t Protokollierung"
  write-host "`t ----------------------------   "

  if ((Get-Service Eventlog | Where-Object {$_.Status -eq "Running"}))
  {
    Write-Color -Text "`t   Event-Log:", "`t`t [1]"-Color White, green
    $log_check = 1

  #Auswertung
    "`t                                          " | add-content $protokoll_dat
    "`t  Eventlog:          [TEILWEISE ERFÜLLT] " | add-content $protokoll_dat
    "`t ----------------------------------------" | add-content $protokoll_dat
    "`t   - Zu Überprüfen ist, welche Nutzer- und -gruppen " | add-content
    $protokoll_dat
    "`t     die Log-Daten auswerten dürfen."      | add-content $protokoll_dat
  }
  else
  {
  Write-Color -Text "`t   Event-Log:", "`t`t [0]"-Color White, red
  $log_check = 0

  #Auswertung
    "`t                                          "  | add-content $protokoll_dat
    "`t  Eventlog:              [NICHT ERFÜLLT] " | add-content $protokoll_dat
    "`t ----------------------------------------" | add-content $protokoll_dat
    "`t   - Eventlog-Dienst aktivieren und starten mit dem Befehl: 'Start-Service
    Eventlog'." | add-content $protokoll_dat
    "`t   - Überprüfen , welche Nutzergruppen die Log-Daten auswerten dürfen." | add-
    content $protokoll_dat
  }
}

function lauf_ende_f {
  # Ende Testlauf

write-host "`t                                                          "
write-host "`t ----------------------------                            "
write-host "`t Ende: Testlauf                                            "
write-host "`t ----------------------------------------------------------"
write-host "`t ----------------------------------------------------------"
}
```

```
function protokoll_ende_f {
  # Funktion Kopf_Datei Auswertung

  "`t                                    "             | add-content $protokoll_dat
  "`t Weiterführende Literatur           "             | add-content $protokoll_dat
  "`t CIS Microsoft Windows 10 Enterprise Benchmark" | add-content $protokoll_dat
  "`t https://learn.cisecurity.org/benchmarks"       | add-content $protokoll_dat
  "`t letzter Zugriff: 2019-08-19          "         | add-content $protokoll_dat
  "`t ----------------------------------------"      | add-content $protokoll_dat
  "`t ----------------------------------------"      | add-content $protokoll_dat
  "`t Ende: Auswertung                   "             | add-content $protokoll_dat
  "`t ---------------------------------------------------------" | add-content
    $protokoll_dat
  "`t ---------------------------------------------------------" | add-content
    $protokoll_dat
  "`t                                    "             | add-content $protokoll_dat
}

#Funktionsaufrufe

lauf_beginn_f
protokoll_beginn_f
admin_lauf_f
kontosec_lauf_f
update_lauf_f
firewall_lauf_f
verschl_lauf_f
log_lauf_f
lauf_ende_f
protokoll_ende_f

# Skriptende
#################
```

Listing C.1: Sicherheitsskript für Windows10-Systeme

C.2 Sicherheitsskript für macOS-Systeme

```
#!/usr/bin/env bash

###
# Überprüfen von Client-Sicherheitseinstellungen nach dem BSI Grundschutz-Kompendium
# Betrifft: Modulare IT-Sicherheitsrichtlinie für vernetzte Endgeräte
###
# Autor: T. Stemplewitz
# Änderungsdatum: 2019-08-28
###

# Allgemeine Funktionen

function sudo_prmpt_f {
  # Eingabe des Administrationskennwortes für tiefere Systemanalysen
  sudo --prompt="Bitte Passwort eingeben um Überprüfungen mit 'sudo' durchzuführen: " -v
}

function red_msg() {
  # Textfarbe: rot
  echo -e "${1} \\033[31;1m${2}\033[0m"
}

function green_msg() {
  # Textfarbe: grün
  echo -e "${1} \\033[32;1m${2}\033[0m"
}

function blue_msg() {
  # Textfarbe: blau
  echo -e "\\033[34;1m${@}\033[0m"
}

function y_msg() {
  # Textfarbe: gelb
  echo -e "${1} \\033[33;1m${2}\033[0m"
}

function u_msg() {
  # Text: unterstrichen, normal und kursiv
  echo -e "\\033[30;4m${1}\033[0m ${2} \\033[30;3m${3}\033[0m"
}

function b_msg() {
  # Text: fett
  echo -e "\\033[30;1m${1}\033[0m"
}

function k_msg() {
  # Text: kursiv
  echo -e "\\033[30;3m${1}\033[0m"
}

function os_ver_f {
  # Betriebssystemversion abfragen
```

```
  os_ver=${1-$(sw_vers -productVersion)}

  if [[ "$os_ver" == 10.14.* ]]; then
    os_ver="macOS Mojave"
  elif [[ "$os_ver" == 10.13.* ]]; then
    os_ver= "macOS High Sierra"
  elif [[ "$os_ver" == 10.12.* ]]; then
    os_ver= "macOS Sierra"
  else
    os_ver= "(Mac) OS X unbestimmt"
fi
}

function ausw_dat_f() {
  #Bildschirmausgabe vorbereiten
  clear
  b_msg "Überprüfung von allgemeinen Sicherheitseinstellungen"
  echo "Prüfdatum:" $(date +'%Y-%m-%d # %T') "Uhr"
  echo "Betriebssystemversion:" $os_ver
  echo "Beginn: Prüfdurchlauf"
  echo "....................."
  echo "                     "

  #Protokolldatei vorbereiten
  protokoll_dat=$(date +'%Y%m%d')"-protokolldatei.txt"
  touch $protokoll_dat
  echo "                                      "  >$protokoll_dat
  b_msg "Auswertung der Sicherheitsüberprüfung" >>$protokoll_dat
  echo "Datum:" $(date +'%Y-%m-%d # %T') "Uhr"  >>$protokoll_dat
  echo "Betriebssystemversion:" $ov_ver         >>$protokoll_dat
  echo "....................................." >>$protokoll_dat
  echo "                                      " >>$protokoll_dat
}

###
# Funktionen für Sicherheitsüberprüfungen

function check_user_f {
  # Prüfung, ob der angemeldete Benutzer über Adminrechte verfügen kann

  blue_msg "Rollentrennung:"

  if $(groups|grep -q 'admin'); then
    red_msg "Administrationsrechte:" "[0]"
    admin_check="0"
  else
    green_msg "Administrationsrechte: " "[1]"
    admin_check="1"
  fi
}

function check_pw_pol_f {
  # Prüfung, ob Kontoeinstellungen vom Standard abweichen

  blue_msg "Kontorichtlinien: "
```

```
  if $(pwpolicy -getaccountpolicies | grep -q 'four'); then
    red_msg "Passwortlänge " "        [0]"
    pw_laeng="0"
  else
    y_msg "Passwortlänge " "        [1]"
    pw_laeng="1"
  fi

  if $(pwpolicy -getaccountpolicies | grep -q 'alpha'); then
    red_msg "Passwortkomplexität " "   [0]"
    pw_kompl="0"
  else
    y_msg "Passwortkomplexität" "   [1]"
    pw_kompl="1"
  fi

  if $(pwpolicy -getaccountpolicies | grep -q '
    policyAttributeMaximumFailedAuthentications'); then
    green_msg "Kontosperrung " "        [1]"
    k_sperr="1"
  else
    red_msg "Kontosperrung " "        [0]"
    k_sperr="0"
  fi
}

function check_firewall_f {
  # Funktion prüft, ob die Firewall aktiviert ist (Default ist [nein]).

  blue_msg "Firewall:"

  if $(sudo /usr/libexec/ApplicationFirewall/socketfilterfw  --getglobalstate | grep -q
    'enabled'); then
    green_msg "Firewall" "              [1]"
    firew_check="1"
  else
    red_msg "Firewall" "              [0]"
    firew_check="0"
  fi
}

function check_gatekeeper_f {
  #Funktion prüft, ob Gatekeeper aktiviert ist (Default ist [ja]).

  if $(spctl --status|grep -q 'assessments enabled'); then
    green_msg "Gatekeeper" "            [1]"
    gk_check="1"
  else
    red_msg "Gatekeeper" "              [0]"
    gk_check="0"
  fi
}

function check_encrypt_f {
  #Prüfen, ob die Dateisystemverschlüsselung (FileVault) aktiviert ist.
```

```
  blue_msg "Datenverschlüsselung:"

  if $(fdesetup status|grep -q 'On'); then
    green_msg "Verschlüsselung" "     [1]"
    verschl_check="1"
  else
    red_msg "Verschlüsselung" "       [0]"
    verschl_check="0"
  fi
}

function check_updates_f {
  # Einstellungen des Updateverhaltens von Systemupdates und Updates für Apps aus dem
    AppStore werden geprüft

  blue_msg "Updateverhalten:"

  if $(if ! defaults read "/Library/Preferences/com.apple.SoftwareUpdate.plist" "
    AutomaticallyInstallMacOSUpdates" >/dev/null 2>&1; then exit 1; fi; defaults read "/
    Library/Preferences/com.apple.SoftwareUpdate.plist" AutomaticallyInstallMacOSUpdates
     | grep -q "1") ; then
    green_msg "Systemupdates" "         [1]"
    sysup_check="1"
  else
    red_msg "Systemupdates" "         [0]"
    sysup_check="0"
  fi

  if $(if ! defaults read "/Library/Preferences/com.apple.commerce.plist" "AutoUpdate"
    >/dev/null 2>&1; then exit 1; fi; defaults read "/Library/Preferences/com.apple.
    commerce.plist" "AutoUpdate" | grep -q "1") ; then
    green_msg "Applikations-Updates" "  [1]"
    appup_check="1"
  else
    red_msg "Applikations-Updates" "  [0]"
    appup_check="0"
  fi
}

function check_audit_f {
  #Prüft, ob der Log-Dienst ausgeführt wird

  blue_msg "Protokollierung:"

  if $(sudo launchctl list | grep -q auditd); then
    y_msg "Log-Dienst" "            [1]"
    log_check="1"
  else
    red_msg "Log-Dienst" "          [0]"
    log_check="0"
  fi
}

function check_end_f {
  # Abschlussausgabe
```

```
  echo "                    "
  echo "..................."
  echo "Ende: Prüfdurchlauf"
}

function ausgabe_auswertung_f {
  #Auswerten der Ergebnisse

  #Auswertung: Rollentrennung
  blue_msg "Rollentrennung:">>$protokoll_dat
  if [ "$admin_check" = "1" ]; then
    green_msg "Test der Rollentrennung" "[ERFÜLLT]" >>$protokoll_dat
  else
    red_msg "Test der Rollentrennung" "[NICHT ERFÜLLT]">>$protokoll_dat
    u_msg "Handlungsempfehlung:" >>$protokoll_dat
    echo "Für administrative Zwecke einen separaten Benutzer erstellen." >>
    $protokoll_dat
    echo "Den aktuellen Benutzer aus der Gruppe 'root' entfernen." >>$protokoll_dat
  fi

  #Auswertung: Kontoeinstellungen
  echo -e ""><>$protokoll_dat && blue_msg "Kontorichtlinien:" >>$protokoll_dat
  if [ "$pw_laeng" = "1" ] && [ "$pw_kompl" = "1" ] && [ "$k_sperr" = "1" ]; then
    green_msg "Kontoeinstellungen" "[ERFÜLLT]" >>$protokoll_dat
  elif [ "$pw_laeng" = "1" ] || [ "$pw_kompl" = "1" ] || [ "$k_sperr" = "1" ]; then
    y_msg "Kontoeinstellungen" "[teilweise ERFÜLLT]" >>$protokoll_dat
    u_msg "Handlungsempfehlung:" >>$protokoll_dat
    echo "Konteneinstellung mit folgendem Befehl setzen:" >>$protokoll_dat
    k_msg " $ pwpolicy -setaccountpolicies" >>$protokoll_dat
    echo "Kernpunkte der Einstellungen:" >>$protokoll_dat
    echo " - mindestens 8 Zeichen" >>$protokoll_dat
    echo " - alphanumerisch" >>$protokoll_dat
    echo " - Kontensperrung nach 10 Fehlversuchen" >>$protokoll_dat
  else
    red_msg "Kontoeinstellungen" "[NICHT ERFÜLLT]" >>$protokoll_dat
    u_msg "Handlungsempfehlung:" >>$protokoll_dat
    echo "Konteneinstellung mit folgendem Befehl setzen:" >>$protokoll_dat
    k_msg " $ pwpolicy -setaccountpolicies" >>$protokoll_dat
    echo "Kernpunkte der Einstellungen:" >>$protokoll_dat
    echo " - mindestens 8 Zeichen" >>$protokoll_dat
    echo " - alphanumerisch" >>$protokoll_dat
    echo " - Kontensperrung nach 10 Fehlversuchen" >>$protokoll_dat
  fi

  #Auswertung: Firewalleinstellungen
  echo -e ""><>$protokoll_dat && blue_msg "Firewalleinstellungen:" >>$protokoll_dat
  if [ "$firew_check" = "1" ] && [ "$gk_check" = "1" ] ; then
    green_msg "Firewall und Gatekeeper" "[ERFÜLLT]" >>$protokoll_dat
  elif [ "$firew_check" = "0" ] ; then
    red_msg "Firewall" "[NICHT ERFÜLLT]" >>$protokoll_dat
    u_msg "Handlungsempfehlung:" >>$protokoll_dat
    echo "Firewall aktivieren" >>$protokoll_dat
    k_msg " Systemeinstellungen -> Sicherheit -> Firewall aktivieren" >>$protokoll_dat
    echo "alternativ" >>$protokoll_dat
    k_msg " $ sudo defaults write /Library/Preferences/com.apple.alf globalstate - int
```

```
  1|2" >>$protokoll_dat
  echo " Wert 1 (spezifisch) oder 2 (essenziell)" >>$protokoll_dat
else
  red_msg "Gatekeeper" "[NICHT ERFÜLLT]" >>$protokoll_dat
  u_msg "Handlungsempfehlung:" >>$protokoll_dat
  echo "Gatekeeper aktivieren" >>$protokoll_dat
  k_msg " Systemeinstellungen -> Sicherheit -> Allgemein -> App-Download erlauben von:
   'App Store'" >>$protokoll_dat
  echo "alternativ" >>$protokoll_dat
  k_msg " $ sudo spctl --master-enable" >>$protokoll_dat
fi

#Auswertung: Festplattenverschlüsselung
echo -e ""><>$protokoll_dat && blue_msg "Verschlüsselung:" >>$protokoll_dat
if [ "$verschl_check" = "1" ]; then
  green_msg "Festplattenverschlüsselung" "[ERFÜLLT]" >>$protokoll_dat
else
  red_msg "Festplattenverschlüsselung" "[NICHT ERFÜLLT]" >>$protokoll_dat
  u_msg "Handlungsempfehlung:" >>$protokoll_dat
  echo "FileVault aktivieren" >>$protokoll_dat
  k_msg " Systemeinstellungen -> Sicherheit -> FileVault -> FileFault aktivieren" >>
  $protokoll_dat
fi

#Auswertung: Updateeinstellungen
echo -e ""><>$protokoll_dat && blue_msg "Updateverhalten:" >>$protokoll_dat
if [ "$sysup_check" = "1" ] && [ "$appup_check" = "1" ] ; then
  green_msg "Automatische Updateeinstellungen" "[ERFÜLLT]" >>$protokoll_dat
elif [ "$sysup_check" = "0" ] && [ "$appup_check" = "0" ] ; then
  red_msg "Automatische Updateeinstellungen" "[NICHT ERFÜLLT]" >>$protokoll_dat
  u_msg "Handlungsempfehlung:" >>$protokoll_dat
elif [ "$sysup_check" = "0" ] ; then
  red_msg "Automatische Systemupdates" "[NICHT ERFÜLLT]" >>$protokoll_dat
  u_msg "Handlungsempfehlung:" >>$protokoll_dat
  echo " Automatische Updates aktivieren" >>$protokoll_dat
  k_msg " Systemeinstellungen -> Softwareupdate -> 'Alle Haken setzen'" >>
  $protokoll_dat
elif [ "$appup_check" = "0" ] ; then
  red_msg "Automatische Updates von Apps" "[NICHT ERFÜLLT]" >>$protokoll_dat
  u_msg "Handlungsempfehlung:" >>$protokoll_dat
  echo " Automatische Updates aktivieren" >>$protokoll_dat
  k_msg " Systemeinstellungen -> Softwareupdate -> 'Alle Haken setzen'" >>
  $protokoll_dat
else
  red_msg "Automatische Systemupdates und App-Updates" "[NICHT ERFÜLLT]"
  u_msg "Handlungsempfehlung:" >>$protokoll_dat
  echo " Automatische Updates aktivieren" >>$protokoll_dat
  k_msg " Systemeinstellungen -> Softwareupdate -> 'Alle Haken setzen'" >>
  $protokoll_dat
fi

#Auswertung: Log-Dienst
echo -e ""><>$protokoll_dat && blue_msg "Logging:"><>$protokoll_dat
if [ "$log_check" = "1" ]; then
  y_msg "Protokollierung" "[ERFÜLLT]" >>$protokoll_dat
  u_msg "Handlungsempfehlung:" >>$protokoll_dat
```

```
    echo "Einstellungen des Protokollierungsdienstes sind zu überprüfen." >>
    $protokoll_dat
    echo "Weiterführende Empfehlungen sind der Quelle zu entnehmen." >>$protokoll_dat
  else
    red_msg "Protokollierungsdienst" "[NICHT ERFÜLLT]" >>$protokoll_dat
    u_msg "Handlungsempfehlung:" >>$protokoll_dat
    echo "Protokollierungsdienst aktivieren mit" >>$protokoll_dat
    k_msg " $ sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.auditd.
    plist" >>$protokoll_dat
  fi

  # Dateiende
  echo "                                        " >>$protokoll_dat
  echo "........................................" >>$protokoll_dat
  echo "                                        " >>$protokoll_dat
  echo "Quelle:                                 " >>$protokoll_dat
  k_msg "CIS Apple macOS 10.13 Benchmark        " >>$protokoll_dat
  u_msg "https://learn.cisecurity.org/benchmarks" >>$protokoll_dat
  echo "letzter Zugriff: 2019-08-19             " >>$protokoll_dat
  echo "........................................" >>$protokoll_dat
  echo "Auswertung beendet"                       >>$protokoll_dat
  echo "........................................" >>$protokoll_dat
  echo "                                        " >>$protokoll_dat
}

# Main-Funktion
function main {

# Funktionsaufrufe
os_ver_f
sudo_prmpt_f
ausw_dat_f
check_user_f
check_pw_pol_f
check_firewall_f
check_gatekeeper_f
check_encrypt_f
check_updates_f
check_audit_f
check_end_f
ausgabe_auswertung_f

#Ausgabe der Auswertung
cat $protokoll_dat
}

#Aufruf der Main-Funktion
main "$@"

####
# Skriptende
###
```

Listing C.2: Sicherheitsskript für macOS-Systeme

Thesen

- Das Zerlegen einer typischen Verwendung vernetzter Endgeräte in einzelne Komponenten, lässt abgrenzende und detaillierte IT-Sicherheitsbetrachtungen an diesen Komponenten zu.
- Durch Cyber-Antipattern ist die Bewertung von IT-Sicherheit möglich, da diese Methode mit alternativen Denkansätzen, sowie dem kritischen Hinterfragen von Gewohnheiten, neue Lösungswege aufzeigen kann.
- IT-Sicherheit kann anhand weniger bestimmender Kriterien für vernetzte Endgeräte ganzheitlich beschrieben werden.
- IT-Sicherheitskriterien können als allgemeine Geschäftsprozesse abgebildet werden.
- Atomare Beschreibungen der Prozessaktivitäten eines IT-Sicherheitskriteriums ergeben Vorteile bei der Sicherheitsanalyse und Maßnahmenerstellung.
- Mit einer modular aufgebauten IT-Sicherheitsrichtlinie ist die Ausrichtung von IT-Sicherheit auf verschiedene Betriebssysteme und Anwendungen möglich.
- Durch systemspezifische Skripte ist eine schnelle Erstanalyse des IT-Sicherheitszustandes eines Endgerätes möglich.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die hier vorliegende Arbeit selbstständig, ohne unerlaubte fremde Hilfe und nur unter Verwendung der aufgeführten Hilfsmittel angefertigt habe.

Ort, Datum Unterschrift

Thomas Stemplewitz

Digital unterschrieben von Thomas Stemplewitz
Datum: 2019.08.30 13:03:31 +02'00'