Best-Practice-Ansätze zur Umsetzung von technischen IT-Sicherheitsanforderungen an eine Bank in Österreich

Philipp Gigler, BSc MSc

MASTERARBEIT

eingereicht am
Fachhochschul-Masterstudiengang

Information Security Management

in Hagenberg

im Juli 2022

Betreuung:

FH-Prof. Dr. Harald Lampesberger, MSc

Erklärung

Ich erkläre eidesstattlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benutzt und die den benutzten Quellen entnommenen Stellen als solche gekennzeichnet habe. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt. Die vorliegende, gedruckte Arbeit ist mit dem elektronisch übermittelten Textdokument identisch.

Hagenberg, am 15. Juli 2022

Philipp Gigler, BSc MSc

Inhaltsverzeichnis

Kurzfassung

Aufgrund der steigender Bedrohung von Cyberangriffen auf IT-Systemen stellen Aufsichtsbehörden verstärkt Vorgaben an die IT-Sicherheit von Unternehmen. Ein Cyberangriff oder ein Ausfall von IT-Infrastrukturkomponenten kann einen erheblichen finanziellen und reputationstechnischen Schaden für Unternehmen darstellen. Vor allem die Sicherheit von Banken und anderer Finanzdienstleister stehen verstärkt im Fokus von Aufsichtsbehörden. Für Finanzinstitute gilt es einerseits die technische Sicherheit der eigenen IT-Umgebung zu erhöhen um Angriffe zu vereiteln und andererseits den unterschiedlichen Anforderungen von Aufsichtsbehörden nachzukommen. Die vorliegende Arbeit beschäftigt sich mit Anforderungen von Aufsichtsbehörden an die technische IT-Sicherheit von Banken in Österreich. Im Zuge dessen werden für die Ausarbeitung relevante Richtlinien erhoben und die Vollständigkeit der untersuchten Richtlinien mittels Peer Reviews sichergestellt. Die Richtlinien werden in weiterer Folge und auf technisch umzusetzende Sicherheitsanforderungen hin analysiert. Diese Sicherheitsanforderungen werden kategorisiert und mögliche technische Umsetzungen abgeleitet. Es wird der Frage nachgegangen, ob sich diese technischen Sicherheitsanforderungen auch mittels bereits etablierter Best-Practice-Ansätze umsetzen lassen. Ziel der vorliegenden Arbeit ist es einen Überblick über technische IT-Sicherheitsanforderungen an Banken in Österreich zu geben, die jeweilig adressierten Themenbereiche zu erörtern und mögliche Maßnahmen zur Umsetzung darzulegen.

Abstract

Due to the increasing threat of cyber attacks on IT systems, regulatory authorities are increasingly imposing requirements on companies' IT security. A cyber attack or a failure of IT infrastructure components can cause considerable financial and reputational damage to companies. In particular, the security of banks and other financial service providers is increasingly in the focus of supervisory authorities. On the one hand, financial institutions need to increase the technical security of their own IT environment in order to thwart attacks, and on the other hand, they need to meet the various requirements of supervisory authorities. This paper deals with the requirements of supervisory authorities for the technical IT security of banks in Austria. In the course of this work, relevant guidelines are collected and the completeness of the examined guidelines is ensured by means of peer reviews. The guidelines are then analyzed in terms of technical security requirements that need to be implemented. These security requirements are categorized and possible technical implementations are derived. The question of whether these technical security requirements can also be implemented using established best-practice approaches is investigated. The aim of this paper is to provide an overview of technical IT security requirements for banks in Austria, to discuss the respective topics addressed and to present possible measures for implementation.

Kapitel 1

Einleitung

Das Thema IT-Sicherheit wird für Unternehmen immer essentieller. Speziell der Banken-Sektor stellt ein lukratives Ziel für Angreifer dar, da Banken als als „Verteilzentren“ weltweiter Finanztransaktionen dienen. In den IT-Systemen von Banken werden Geldtransaktionen aus aller Welt gespeichert und Kundendaten verarbeitet. Laut einer Studie der „Boston Consulting Group“ (BCG[1]) treffen Cyberattacken Finanzdienstleister 300-Mal häufiger als Unternehmen aus anderen Sparten. Trotz dieser Tatsache sind viele Finanzdienstleister nicht genug auf Cyberangriffe und deren Folgen vorbereitet. Unterschiedliche Faktoren wie der steigende Konkurrenzdruck und die Etablierung von nicht-traditionellen Marktteilnehmern und Fintech-Unternehmen führen dazu, dass der Bereich der IT-Sicherheit bei Finanzdienstleistern oft von Einsparungen betroffen ist. [43]

Ein Cyberangriff oder ein Ausfall von IT-Infrastrukturkomponenten kann zu einem erheblichen finanziellen und reputationstechnischen Schaden für Finanzdienstleister und deren Partner führen. Ein weiterer möglicher Schaden eines Cyberangriffs ist der Verlust des Vertrauens der Kunden in das betroffene Finanzinstitut. Aus diesem Grund existieren für Finanzinstitute weitreichende Vorschriften betreffend der Sicherheit von IT-Systemen. [59]

Das Risiko eines Cyberangriffs, etwa auf die Infrastruktur eines Finanzdienstleisters, wird um einen weiteren Faktor verschärft. Es kann vorkommen, dass es Finanzdienstleistern nicht möglich ist, eine eigene IT-Infrastruktur zu betreiben. Aus diesem Grunde können unterschiedliche Aufgaben an Dritte ausgelagert werden um Kosten zu sparen und somit einen Wettbewerbsvorteil zu lukrieren. Anstatt beispielsweise die notwendige IT-Infrastruktur selbst zu betreiben, nötige Prozesse zu etablieren und Mitarbeiter zu beschäftigen, werden diese Aufgaben von spezialisierten Dienstleistern erbracht. Durch diese Auslagerung entsteht für den Finanzdienstleister eine neue Art von Risiko. Neben dem tatsächlichen Ausfall von Hard- oder Software oder einem Angriff auf die IT-Infrastruktur wird der gesamte Dienstleister zu einem Risiko. Dieses Risiko besteht, wenn der Dienstleister seine Leistungen nicht oder nicht ausreichend erbringt, oder selbst Opfer eines Cyberangriffs wird. [92]

[1] https://www.bcg.com

Aufgrund der steigenden Relevanz von IT-Sicherheit im Zuge von Auslagerungen hat die „Europäische Bankenaufsichtsbehörde“ (EBA[2]) im Jahr 2019 eine Leitlinie zum Umgang mit Auslagerungsrisiken veröffentlicht (EBA/GL/2019/02) [55]. Parallel dazu wird auf europäischer Ebene an einer Harmonisierung regulatorischer Anforderungen an die IT-Sicherheit von Finanzunternehmen in Europa gearbeitet. Die „Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung“ (EIOPA[3]) veröffentlichte gemeinsam mit der EBA und der „Europäischen Wertpapier- und Marktaufsichtsbehörde“ (ESMA[4]) eine Stellungnahme mit dem Titel „Joint Advice on the need for legislative improvements relating to Information and Communication Technoloy risk management requirements“ [58]. In dieser Stellungnahme werden konkreten Maßnahmen zur Harmonisierung und Konvergenz von Anforderungen an die Sicherheit der Informations- und Kommunikationstechnologie von Finanzunternehmen vorgeschlagen [44].

1.1 Problemstellung und Zielsetzung

Aufgrund der steigenden Gefahr von Cyber-Angriffen im Finanzdienstleistungssektor ist es äußerst wichtig allgemein geltende Anforderungen an IT-Sicherheit zu etablieren. Aufgrund der Komplexität des Themas IT-Sicherheit als solches und dem stetigen Wandel im Bereich Informationstechnik, stellen Aufsichtsbehörden nur Rahmenwerke zur Verfügung. Detaillierte technische und fachliche Anforderungen und damit einhergehende zu implementierende Maßnahmen werden in den Anforderungen häufig nicht oder nur oberflächlich vorgegeben. Aufsichtsbehörden fordern von Unternehmen etwa eine IT-Sicherheitsrichtlinie zu etablieren, diese umzusetzen und die Erfüllung der IT-Sicherheitsrichtlinie regelmäßig zu überprüfen. Die genauen Anforderungen an eine IT-Sicherheitsrichtlinie sind jedoch oft nicht im Detail spezifiziert, werden von den Finanzdienstleistern nach bestem Wissen und Gewissen subjektiv interpretiert und daraus entsprechende Erkenntnisse und Maßnahmen abgeleitet. Die tatsächliche technische und fachliche Umsetzung dieser Maßnahmen stellt viele Finanzdienstleister vor eine große Hürde. Eine weitere Herausforderung für Finanzdienstleister besteht darin den Überblick über aktuell geltende IT-Sicherheitsanforderungen an das eigene Unternehmen zu behalten. Je nach Standort und Tätigkeitsfeld des Unternehmens sind verschiedene Aufsichtsbehörden für ein Unternehmen zuständig und somit unterschiedliche regulatorische Anforderungen zu erfüllen. Es existiert beispielsweise kein allgemein gültiger Anforderungskatalog für IT-Sicherheit für Banken in Österreich. Welche Anforderungen im Bereich IT-Sicherheit zu erfüllen sind hängt von der jeweils prüfenden Aufsichtsbehörde ab.

Die vorliegende Masterarbeit dient als Überblick für regulatorische Anforderungen an die IT-Sicherheit von Banken in Österreich und als Basis für die Implementierung von technischen Maßnahmen zur Erfüllung dieser Anforderungen. Im Zuge der Ausarbeitung dieser Masterarbeit wird untersucht, welche technischen Anforderungen an die IT-Sicherheit einer Bank in Österreich bestehen und ob diese mit Hilfe von Best-Practice-

[2] https://www.eba.europa.eu
[3] https://www.eiopa.europa.eu
[4] https://www.esma.europa.eu

Ansätzen erfüllt werden können. Um dieser Frage nachgehen zu können werden im Zuge der Ausarbeitung aktuell geltende technische Anforderungen an IT-Sicherheit von Aufsichtsbehörden erhoben, in deren Zuständigkeit österreichische Bank-Institute fallen. Die erhobenen Anforderungen werden in weiterer Folge miteinander in Verbindung gebracht und kategorisiert. Im Anschluss daran werden mögliche technische Maßnahmen zur Umsetzung dieser Anforderungen abgeleitet. Schlussendlich wird untersucht welche Best-Practice-Ansätze sich für die Umsetzung der geforderten Maßnahmen eignen. Im Zuge der Ausarbeitung wird des Weiteren auf das Thema eingegangen, wie die Umsetzung der einzelnen Maßnahmen gemessen und auditiert werden kann. Abschließend wird analysiert ob Angriffsvektoren und Cyberbedrohungen bestehen, die mit den Anforderungen und abgeleiteten Maßnahmen nicht adressiert werden.

Fazit der Masterarbeit bildet eine Anforderungsmatrix mit aktuell gültigen Anforderungen, abgeleiteten technischen Maßnahmen, einer Übersicht über das jeweilig adressierte Risiko und einer Übersicht, mit welchen Best-Practice-Ansätzen diese Maßnahmen umgesetzt und deren Erfüllung gemessen werden kann.

1.2 Forschungsfrage und Methodik

Forschungsfrage: Können geltende technische IT-Sicherheitsanforderungen an eine Bank in Österreich auf Basis von Best-Practice-Ansätzen erfüllt werden?

Nebenfrage 1: Welche regulatorischen, technischen Anforderungen und Vorgaben im Bereich IT-Sicherheit bestehen für ein Bank-Institut in Österreich?
Nebenfrage 2: Welche technisch erforderlichen Maßnahmen können aus diesen technischen Anforderungen und Vorgaben abgeleitet werden?
Nebenfrage 3: Welche Best-Practice-Ansätze eignen sich für die Umsetzung der erforderlichen Maßnahmen?
Nebenfrage 4: Wie kann gemessen werden, ob die technischen Anforderungen und Vorgaben erfüllt werden?

Die Grundlage der Masterarbeit bildet eine Recherche über Aufsichtsbehörden mit Zuständigkeit im Finanzdienstleistungssektor. Der Fokus wurde im Zuge der Recherche noch nicht auf Bankunternehmen in Österreich gelegt um eine umfassende Sicht auf das Thema zu erhalten. So werden etwa auch Aufsichtsbehörden anderer Ausprägungen von Finanzdienstleistungsgesellschaften, wie etwa Versicherungen oder reinen Wertpapiergesellschaften, durchgeführt. Anschließend wird eine Literaturrecherche bezogen auf aktuell gültige technische IT-Sicherheitsanforderungen von Aufsichtsbehörden erhoben. Sowohl die Recherche nach relevanten Aufsichtsbehörden als auch die Literaturrecherche nach technischen IT-Sicherheitsanforderungen wird auf Basis allgemein zugänglicher Informationen im Internet und durch Befragung von Angestellten aus den Bereichen Governance und IT-Sicherheit eines österreichischen Finanzdienstleistungsunternehmen durchgeführt. Im nächsten Schritt werden die erhobenen technischen IT-Sicherheitsanforderungen in Bezug auf ihre Gültigkeit für eine Bank in Österreich geprüft. Dies dient dazu, die Zuständigkeit der analysierten Aufsichtsbehörden zu klären und damit die Relevanz der jeweiligen Anforderungen an Banken in Österreich abgren-

zen zu können. Um die Vollständigkeit der analysierten Aufsichtsbehörden und Anforderungen zu prüfen wird ein Peer Review mit drei Angestellten aus dem Bereich IT-Sicherheit und IT-Governance einer Bank in Österreich abgehalten. Das Ergebnis des Peer Reviews wird in Kapitel 3.3 behandelt.

Die öffentlich zugänglichen Dokumente der relevanten Aufsichtsbehörden werden in weiterer Folge analysiert und jeweils ein kurzer Überblick in Form eines Steckbriefs erstellt. Die Steckbriefe sind in Kapitel 3.4 ersichtlich. Auf Basis der gewonnenen Erkenntnisse wird eine Anforderungsmatrix aufgebaut und die technischen Anforderungen an IT-Sicherheit aus den Dokumenten darin festgehalten. Der Aufbau der Anforderungsmatrix wird in Kapitel 4 behandelt. Die analysierten Anforderungen werden im Anschluss auf Basis ihrer möglichen Umsetzbarkeit in „Technische Anforderungen“ und „Organisatorische Anforderungen“ aufgeteilt. Für die Technischen-Anforderungen werden mögliche Maßnahmen nach aktuellem Stand der Technik analysiert und Best-Practice-Ansätze recherchiert. Sowohl die Analyse möglicher Maßnahmen als auch die Recherche von Best-Practice-Ansätzen sind auf Basis frei zugänglicher Informationen im Internet und Gesprächen mit Angestellten aus dem Bereich IT-Infrastruktur und IT-Sicherheit eines Bank-Instituts in Österreich erhoben worden. Die Maßnahmen werden in weiterer Folge gruppiert und Best-Practice-Ansätze abgeleitet. Im Zuge der Analyse wird aufgezeigt, wie der Ansatz zur Umsetzung der technischen Maßnahme beitragen kann. Als Qualitätskontrolle der gewonnenen Erkenntnisse wird ein Abgleich mit der „Cyber Defense Matrix“ des „Open Web Application Security Project“ (OWASP[5]) durchgeführt [80]. Auf Basis diese Abgleichs kann erkannt werden, ob die Anforderungen der Aufsichtsbehörden alle gängigen Angriffsvektoren beziehungsweise Cyber-Bedrohungen abdecken und ob die analysierten Best-Practice-Ansätze legitim sind.

1.3 Abgrenzung

Im Zuge der Ausarbeitung dieser Masterarbeit werden nur Aufsichtsbehörden analysiert, in deren Zuständigkeitsbereich österreichische Bankinstitute fallen. Betrachtet werden nur Anforderungen die für die Gründung einer Bank in Österreich relevant und vorgeschrieben sind. Grundlegende IT-Sicherheitsanforderungen an Unternehmen, wie beispielsweise die Erfüllung der Datenschutzgrundverordnung (DSGVO), werden in der Anforderungsmatrix nicht beachtet [53]. Die erhobenen IT-Sicherheitsanforderungen können sich zum Teil mit allgemein gültigen IT-Sicherheitsanforderungen an Unternehmen außerhalb des Finanzdienstleistungssektors decken. Im Zuge der Ausarbeitung werden nur IT-Sicherheitsanforderungen analysiert, die technisch umgesetzt werden können. Die für die Ausarbeitung dieser Masterarbeit analysierten Aufsichtsbehörden und die verwendeten IT-Sicherheitsanforderungen sind in Kapitel 3.4 aufgelistet.

[5] https://owasp.org

Kapitel 2

Stand des Wissens

Ziel dieses Kapitels ist es, einen Überblick über die Begriffe „Governance“, „Compliance“ und „IT-Sicherheit“ zu geben, Unterschiede aufzuzeigen und so zu einem besseren Verständnis der weiteren Arbeit beizutragen. Im Zuge dessen wird auf die Relevanz von IT-Sicherheit im Banken-Sektor eingegangen und die möglichen Auswirkungen von IT-Sicherheitsvorfällen im Bankenumfeld aufgezeigt.

Der Begriff IT-Sicherheit beschreibt unterschiedliche Technologien, Prozesse und Praktiken, deren Zweck der Schutz von Assets in einem Unternehmen vor unberechtigten Zugriff oder unrechtmäßiger Verwendung ist. Unternehmen haben verschiedene Motivationsgründe und Ausprägungen zum Schutz ihrer Assets und Unternehmensdaten. Unabhängig vom jeweiligen Asset lassen sich drei Schutzziele ableiten, die in der Literatur als „CIA Triade“ bezeichnet werden [3]:

- (C) Confidentiality
  Das erste Schutzziel der CIA-Triade bildet die „Vertraulichkeit“ von Assets und Daten. Das Ziel ist der Schutz vor unberechtigtem Zugriff auf das zu schützende Asset. Vertrauliche Daten sollen nur von autorisierten Personen oder Systemen eingesehen werden können.
- (I) Integrity
  Das zweite Schutzziel bildet die „Integrität“ von Assets und Daten. Integrität verlangt, dass sowohl die Daten selbst als auch deren Funktionsweise zu jedem Zeitpunkt korrekt sind. Änderungen an Assets oder Daten müssen stets nachvollziehbar sein.
- (A) Availability
  Das dritte Schutzziel bildet die „Verfügbarkeit“ von Assets und Daten. Darunter ist zu verstehen, dass Assets und Daten zu jedem Zeitpunkt verfügbar sein müssen. Es ist zu vermeiden, dass Daten verloren gehen oder der Zugriff auf Assets nicht gegeben ist.

Angriffe auf IT-Systeme zielen auf die Verletzung eines oder mehrerer Schutzziele ab. Je nach Ausprägung eines Unternehmens kann die Verletzung eines Schutzziels unterschiedliche Auswirkungen haben. Vor allem im Bankensektor, dem Dreh- und Angelpunkt internationaler Geldtransaktionen steht der Schutz von Assets und Daten an erster Stelle.

Dagegen steht die steigende Anzahl an Angriffen auf Bankinstitute. Im Jahr 2019 liesen sich fast 50% aller untersuchten Phishing-Angriffe auf den Bankensektor zurückzuführen. Auch Ransomware-Attacken auf Banken sind im Jahr 2020 im Vergleich zum Jahr 2019 um 520% gestiegen. [51]

Auf Basis der stetig steigenden Bedrohungslage und als Reaktion auf verschiedene Unternehmenspleiten in den 1990er Jahren, wie beispielsweise der Bearing-Bank oder von Worldcom, sehen sich Unternehmen mittels regulatorischen Vorgaben zu einer transparenten Unternehmensführung verpflichtet [50] [49]. Die Einhaltung dieser Vorgaben wird seitens Gesetzgebern und relevanten Aufsichtsbehörden verstärkt in den Fokus genommen.

Die Erfüllung dieser regulatorischen Anforderungen wird mit dem Begriff „Compliance“ bezeichnet. Compliance leitet sich aus dem lateinischen Wort „complere“ ab. Übersetzt bedeutet es ausfüllen beziehungsweise ergänzen. Im wirtschaftlichen Bereich wird der Ausdruck im übertragenen Sinne für die Übereinstimmung mit etwas oder dem Einhalten von geltendem Recht verwendet. Das Ziel, compliant gegenüber unterschiedlichen Anforderungen zu sein, bezeichnet den Zustand der Anforderungskonformität gegenüber gesetzlichen oder aufsichtsrechtlichen Vorgaben. Das Erreichen des Ziels, compliant gegenüber Anforderungen zu sein, wird in Unternehmen mittels „Governance“ angestrebt. Der Begriff Governance leitet sich aus dem lateinischen Wort „gubernare“ ab. Übersetzt bedeutet es so viel wie leiten, lenken oder steuern. [4]

Johannsen [7] beschreibt den Begriff Governance mit der „verantwortlichen, transparenten und nachvollziehbaren Leitung und Überwachung von Organisationen und ihren Ausrichtungen an Regulierungen, Standards und ethischen Grundsätzen“. Im wirtschaftlichen Bereich wird der Ausdruck als Synonym für die Leitung und Überwachung von Unternehmen verwendet. Der Begriff Governance lässt sich in verschiedene Teilbereiche gliedern. Bezogen auf diese Arbeit sind die beiden Teilbereiche Corporate-Governance und IT-Governance relevant. Hauschka u. a. [6] beschreiben Corporate-Governance mit dem Begriff „Unternehmensverfassung“ und beziehen sich damit auf einen Ordungsrahmen für die Leitung und Überwachung in einem Unternehmen.

Mit Hilfe von Corporate-Governance können Managementsysteme geschaffen werden, die mittels internen Überwachungsmechanismen die Transparenz von Abläufen in Unternehmen erhöhen. Eine Möglichkeit für interne Überwachungsmechanismen sind „Interne Kontrollsysteme“ (IKS), welche die Unternehmensleitung bei der Erkennung von Risiken unterstützten. Ein IKS entspricht einer Ansammlung von Maßnahmen, sogenannten Controls, die in betriebliche Prozesse integriert werden können. Die Controls umfassen Richtlinien und Verfahren in Abläufen des Unternehmens und werden dafür verwendet, unerwünschten Ergebnissen vorzubeugen, Risiken zu erkennen und diese zu adressieren. Der Begriff „IT-Governance“ wird in der Praxis verwendet um Themen aus dem Bereich Governance im IT-Umfeld zu adressieren oder ein Regelwerk beziehungsweise Kontrollen für IT-Systeme zu etablieren. [4]

Kapitel 3

Regulatorische Anforderungen

Das folgende Kapitel zeigt auf, welche IT-Sicherheitsanforderungen für Banken in Österreich bestehen. Im Zuge der Ausarbeitung liefert das Kapitel einen Überblick über die im Zuge der Arbeit evaluierten Anforderungen an IT-Sicherheit von Aufsichtsbehörden. Zum Ende des Kapitels werden die Anforderungen, die für Banken in Österreich relevant sind, dargestellt.

3.1 Regulatorische Anforderungen

Betreibt ein Unternehmen konzessionspflichtige Geschäfte im Sinne des Bankwesengesetzes (BWG), wird eine Konzession der zuständigen Aufsichtsbehörde benötigt [88]. Für die Abwicklung von Konzessionsverfahren für Kreditinstituten ist die Europäische Zentralbank (EZB[1]) zuständig. Für österreichische Kreditinstitute, die nicht von der EZB beaufsichtigt werden, ist die Finanzmarktaufsichtsbehörde (FMA[2]) für die Erteilung der Konzession zuständig. Die FMA leitet in weiterer Folge den jeweiligen Antrag, zusammen mit einem Beschlussentwurf und den entsprechenden Unterlagen an die EZB zur Entscheidungsfindung weiter.

Eine Konzession wird erteilt, wenn unter anderem folgende Punkte erfüllt sind [72]:

- Das Unternehmen wird als Kreditinstitut geführt.
- Das Anfangskapital von 5 Millionen Euro steht zur Verfügung.
- Das Kreditinstitut hat mindestens zwei Geschäftsleiter.
- Der Sitz und die Hauptverwaltung liegen im Inland.

Eine Konzession für den Betrieb von Bankgeschäften kann mit Bedingungen und Auflagen verknüpft sein. Eine aufrechte Konzession ist die Voraussetzung für die Durchführung von Bankgeschäften in Österreich.

Eine Konzession kann gemäß BWG von der EZB oder der FMA widerrufen werden. Dies ist unter anderem erforderlich, wenn die Konzession durch unrichtige Angaben erschlichen wurde oder bestimmten Anforderungen von zuständigen Aufsichtsbehörden nicht

[1] https://www.ecb.europa.eu
[2] https://www.fma.gv.at

nachgekommen wird. Das bedeutet, dass auch das nicht einhalten der von Aufsichtsbehörden vorgeschriebenen Anforderungen zum Schutz der IT-Sicherheit, den Entzug einer aufrechten Konzession mit sich bringen kann.

Aus diesem Grund werden Banken in Österreich regelmäßig von der FMA überprüft. In der Pressemitteilung der FMA vom 04. Januar 2022, werden die Prüfungsschwerpunkte für das Jahr 2022 definiert [79]. Unter anderem wird der Schwerpunkt auf die Evaluierung der Cybersecurity in Unternehmen gesetzt. Es ist davon auszugehen, dass die Anforderungen aus dem „FMA Leitfaden IT-Sicherheit“ genauestens überprüft werden.

3.2 Evaluierte Aufsichtsbehörden und Anforderungen

Im Folgenden wird ein Überblick über die im Zuge der Masterarbeit analysierten Aufsichtsbehörden gegeben. Anschließend werden die von den Aufsichtsbehörden veröffentlichten Anforderungen an IT-Sicherheit einer Bank in Österreich aufgezeigt. Die Aufsichtsbehörden, die sich um Zuge der Recherche als relevant für eine Bank in Österreich herausgestellt haben, werden in diesem Kapitel dargestellt und in Form von Steckbriefen beschrieben. Eine Zusammenfassung über die Aufsichtsbehörden und die jeweils analysierten Anforderungen ist in Tabelle 3.1 ersichtlich. Die in 3.1 ersichtlichen Aufsichtsbehörden und Anforderungen wurden mittels Recherche im Internet und durch Befragung von Angestellten aus dem Bereich „IT-Governance“ einer Bank in Österreich analysiert. Die Vollständigkeit der Auflistung wird in Kapitel 3.3 überprüft.

Tabelle 3.1: Übersicht über die analysierte Aufsichtsbehörden und relevante Anforderungen.

Nr	Aufsichtsbehörde	Literatur
1	BaFin	BAIT-Rundschreiben [47]
2	EBA	Leitlinien für das Management von IKT- und Sicherheitsrisiken [14]
3	EBA	Leitlinien zu Auslagerungen [15]
4	EBA	Leitlinien für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses [66]
5	EBA	Leitlinien zur zur Sicherheit von Internetzahlungen [16]
6	Eiopa	Leitlinien zu Sicherheit und Governance im Bereich der Informations und Kommunikationstechnologie [17]
7	ESMA	Leitlinien zur Auslagerung an Cloud-Anbieter [18]
8	FMA	Leitfaden IT-Sicherheit in Verwaltungsgesellschaften [19]
9	FMA	Leitfaden IT-Sicherheit in Wertpapierdienstleistungsunternehmen und Wertpapierfirmen [20]
10	EU	Richtlinie PSD2 [21]
11	EZB	Cyber resilience oversight expetcations for financial market infrastructures [60]
12	ENISA	Definition of Cybersecurity [22]

BaFin - BAIT Rundschreiben

- Institution: Bundesanstalt für Finanzienstleistungsaufsicht (BaFin[3])
- Titel: BAIT Rundschreiben [47]
- Version: 10/2017 – 16.08.2021
- Rahmenwerk: Vorgabe
- Inhalt:

[3] https://www.bafin.de

- IT-Strategie
- IT-Governance
- Informationsrisikomanagement
- Informationssicherheitsmanagement
- Operative Informationssicherheit
- Identitäts- und Rechtemanagement
- IT-Projekte und Anwendungsentwicklung
- IT-Betrieb
- Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen
- IT-Notfallmanagement
- Management der Beziehungen mit Zahlungsdienstnutzern
- Kritische Infrastruktur

Die Aufgabe der BaFin besteht in der Aufsicht von Banken, Finanzdienstleister, Versicherer und dem Wertpapierhandel in Deutschland. Die BaFin arbeitet im öffentlichen Interesse und verfolgt den Ansatz, ein funktionsfähiges, stabiles und integres deutsches Finanzsystem zu gewährleisten. Im Jahr 2021 beaufsichtigte die BaFin 1.555 Banken, 1.189 Finanz- und 51 Zahlungs-Institute. Das große Ziel ist es, das Vertrauen von Bankkunden, Versicherten und Anlegern in das deutsche Finanzsystem zu stärken. Aus diesem Grund sorgt die BaFin dafür, dass die von ihr beaufsichtigten Unternehmen etwa geltenden Vorgaben zur IT-Sicherheit oder der Prävention von Geldwäsche und Terrorismusfinanzierung einhalten. [46]

Auf Basis dieser Aufgaben hat die BaFin die „Bankaufsichtliche Anforderungen an die IT“ (BAIT), in der aktuell gültigen Fassung „10/2017“ veröffentlicht [47]. Im Zuge der BAIT hat die BaFin Vorgaben definiert, wie Auflagen aus dem Kapitalwesengesetz (KWG) von Finanzinstituten in Deutschland umzusetzen sind [65]. Das Rundschreiben gibt einen Rahmen für die technisch-organisatorische Ausstattung der betroffenen Institute bezogen auf IT-Ressourcen, Informationsrisikomanagement und das Informationssicherheitsmanagement vor. Bei der BAIT handelt es sich um eine Vorgabe beziehungsweise einen praxisnahen Rahmen für Anforderungen aus §25 des KWG, verweist jedoch auch auf die Verpflichtung zur Umsetzung gängiger Standards aus dem IT-Grundschutz und der ISO/IEC 27001 [70] [69] [46].

Vom KWG betroffen sind Kreditinstitute und Finanzdienstleister in der Bundesrepublik Deutschland und Finanzdienstleister der Bundesrepublik Deutschland mit Zweigniederlassungen im Ausland. Aufgrund der Nähe Deutschlands zu Österreich und den engen Wirtschaftsbeziehungen wurde die BAIT für die Analyse relevanter Anforderungen an Banken in Österreich herangezogen. [62]

EBA – Leitlinien für das Management von IKT- und Sicherheitsrisiken

- Institution: Europäische Bankenaufsichtsbehörde
- Titel: Leitlinien für das Management von IKT- und Sicherheitsrisiken [14]
- Version: EBA/GL/2019/04

- Rahmenwerk: Leitlinie
- Inhalt:
  - Proportionalität
  - Governance und Strategie
  - Rahmenwerk für das Management von IKT- und Sicherheitsrisiken
  - Informationssicherheit
  - Physische Sicherheit
  - IKT-Betriebsmanagement
  - IKT-Projekt- und Änderungsmanagement
  - Geschäftsfortführungsmanagement
  - Pflege der Kundenbeziehungen mit Zahlungsdienstnutzern

Die EBA ist eine unabhängige EU-Behörde für die Regulierung und Beaufsichtigung von Banken. Ihre Aufgabe ist die Wahrung der Finanzstabilität in der EU, der Schutz der Integrität und das ordnungsgemäße Funktionieren des Bankensektors. Die EBA ist für die Erarbeitung des einheitlichen Europäischen Regelwerks für den Finanzsektor zuständig und definiert verbindliche technische Standards und Leitlinien. Sie trägt damit zur Etablierung und zum Erhalt gleicher Wettbewerbsbedingungen, sowie dem Schutz von Einlegern, Anlegern und Verbrauchen bei. [48]

Die „Leitlinie für das Management von IKT- und Sicherheitsrisiken“ definiert Anforderungen an Kreditinstitute, Wertpapierfirmen und Zahlungsdienstleister, die sich auf das Management von Informations- und Kommunikationstechnologie (IKT) und Sicherheitsrisiken beziehen. Sie umfasst Erwartungen der EBA an die Informationssicherheit und Cybersicherheit für Informationen die auf IKT-Systemen bearbeitet werden. Die Leitlinie ist für alle Kreditinstitute, Wertpapierfirmen und Zahlungsdienstleister innerhalb der Europäischen Union gültig. Die Leitlinien wurden aufgrund der Relevanz für Banken in Österreich in die Anforderungsmatrix mit aufgenommen. [85]

EBA – Leitlinien zu Auslagerungen

- Institution: Europäische Bankenaufsichtsbehörde
- Titel: Leitlinien zu Auslagerungen [15]
- Version: EBA/GL/2019/02
- Rahmenwerk: Leitlinie
- Inhalt:
  - Verhältnismäßigkeit
  - Bewertung von Auslagerungsvereinbarungen
  - Rahmen für die Governance
  - Auslagerungsprozess
  - An die zuständigen Behörden gerichtete Leitlinien zu Auslagerungen

In der Leitlinie zur Auslagerung werden die internen Governance-Regelungen, einschließlich eines soliden Risikomanagements festgelegt, die im Falle einer Auslagerung von Funktionen beachtet werden müssen. Die Leitlinie ist für alle Zahlungsinstitute und E-Geld-Institute innerhalb der Europäischen Union gültig, wurde aber aufgrund des reinen Fokus auf das Thema Auslagerung nicht in die Anforderungsmatrix aufgenommen.

EBA – Leitlinien für die IKT-Risikobewertung

- Institution: Europäische Bankenaufsichtsbehörde
- Titel: Leitlinien für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfuungs- und Bewertungsprozesses [66]
- Version: EBA/GL/2017/05
- Rahmenwerk: Leitlinie
- Inhalt:
  - Anforderungen an die IKT-Risikobewertung
  - Bewertung der IKT-Risikopositionen und –kontrollen der Institute

Die Leitlinie zielt darauf ab, die Aufsichtspraktiken bei der Bewertung des Informations- und Kommunikationstechnologie-Risikos sicherzustellen. Die Leitlinie ist für alle Zahlungsinstitute innerhalb der Europäischen Union gültig, wurde aber aufgrund des Fokus auf die Risikobewertung nicht in die Anforderungsmatrix aufgenommen.

EBA – Leitlinien zur Sicherheit von Internetzahlungen

- Institution: Europäische Bankenaufsichtsbehörde
- Titel: Leitlinien zur Sicherheit von Internetzahlungen [16]
- Version: EBA/GL/2014/12
- Rahmenwerk: Leitlinie
- Inhalt:
  - Anwendungsbereich und Begriffsbestimmungen
  - Leitlinien zur Sicherheit von Internetzahlungen
  - Anhang 1: Beispiele für bewährte Vorgehensweisen

In dieser Leitlinie werden Mindestanforderungen im Bereich der Sicherheit von Internetzahlungen definiert, die für die Erbringung von angebotenen Zahlungsdiensten durch Zahlungsdienstleister über das Internet benötigt werden. Die Leitlinie ist für alle Zahlungsinstitute innerhalb der Europäischen Union gültig und wurde daher in die Anforderungsmatrix aufgenommen.

EIOPA – Leitlinien zur Sicherheit und Governance im Bereich der IKT

- Institution: Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung
- Titel: Leitlinien zur Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie [17]

- Version: EIOPA-BoS-20/600
- Rahmenwerk: Leitlinie
- Inhalt:
  - Verhältnismäßigkeit
  - IKT innerhalb des Governance-Systems
  - IKT-Strategie
  - IKT- und Sicherheitsrisiken innerhalb des Risikomanagementsystems
  - Revision
  - Informationssicherheitspolitik und -maßnahmen
  - Informationssicherheitsfunktion
  - Logische Sicherheit
  - Physische Sicherheit
  - Sicherheit des IKT-Betriebs
  - Überwachung der Sicherheit
  - Überprüfung, Bewertung und Testen der Informationssicherheit
  - Schulungen und Sensibilisierungsmaßnahmen zum Thema Informationssicherheit
  - Management des IKT-Betriebs
  - Management von IKT-Vorfällen und -Problemen
  - Management von IKT-Projekten
  - Erwerb und Entwicklung von IKT-Systemen
  - IKT-Änderungsmanagement
  - Betriebliches Kontinuitätsmanagement
  - Business-Impact-Analyse
  - Betriebskontinuitätsplanung
  - Reaktions- und Wiederherstellungspläne
  - Testen der Pläne
  - Krisenkommunikation
  - Outsourcing von IKT-Diensten und IKT-Systemen

Die EIOPA ist eine Agentur der Europäischen Union, mit Sitz in Frankfurt am Main. Als Teil des europäischen Systems der Finanzaufsicht berät sie die Europäische Kommission, das Europäische Parlament und den Rat der Europäischen Union, als unabhängiges Gremium. Auf diese Weise leistet die EIOPA einen wichtigen Beitrag zur Stabilität der Finanzprodukte, sorgt für Transparenz an den Finanzmärkten und schützt Versicherungsnehmer, Versorgungsanwärter und Leistungsempfänger. Da verstärkt die Notwendigkeit erkannt wird, dass Unternehmen für Cyberrisiken gerüstet sind und über einen soliden Cybersicherheitsrahmen verfügen, geht die Leitlinie ebenfalls auf die Cybersicherheit im Rahmen der Informationssicherheitsmaßnahmen eines Unternehmens ein. Die Leitlinie ist für Versicherungs- und Rückversicherungsunternehmen im Europäischen Wirtschaftsraum gültig. Die Anforderungen wurden aufgrund der fehlenden Relevanz für Bank-Institute nicht in die Anforderungsmatrix aufgenommen. [56]

ESMA – Leitlinien zur Auslagerung an Cloud Anbieter

- Institution: Europäische Wertpapier- und Marktaufsichtsbehörde
- Titel: Leitlinien zur Auslagerung an Cloud Anbieter [18]
- Version: 10/05/21 ESMA50-164-4285 DE
- Rahmenwerk: Leitlinie
- Inhalt:
  - Governance, Kontrolle und Dokumentation
  - Risikoanalyse der Auslagerung und Due-Diligence-Prüfung
  - Zentrale Bestandteile des Vertrags
  - Informationssicherheit
  - Ausstiegsstrategien
  - Zugangs- und Prüfungsrecht
  - Sub-Auslagerungen
  - Schriftliche Mitteilung an die zuständigen Behörden
  - Überwachung von Auslagerungsvereinbarungen mit Cloud-Anbietern

Die ESMA ist die Finanzmarktaufsichtsbehörde der Europäischen Union mit dem Auftrag, den Anlegerschutz zu verbessern und einen stabilen, geregelten und funktionierenden Finanzmarkt im Europäischen Wirtschaftsraum zu fördern. Sie ist eine unabhängige EU-Behörde mit Sitz in Paris und stellt sicher, dass die Bedürfnisse der Verbraucher umfassend berücksichtigt, deren Rechte gestärkt aber auch deren Verantwortlichkeit anerkannt werden. Die ESMA fördert die Integrität, Transparenz und Effizient der Finanzmärkte und trägt so zu einer stabilen Marktinfrastruktur bei. Eine weitere Aufgabe der ESMA ist die Koordination der Wertpapieraufsichtsbehörden und die Unterstützung bei Krisensituationen. Die Leitlinie zur Auslagerung an Cloud Anbieter etabliert eine effiziente und wirksame Aufsichtspraktik für die Sicherstellung der Anforderungen, bezogen auf Auslagerungen an Cloud-Anbieter und ist für alle Finanzunternehmen im Europäischen Wirtschaftsraum gültig. Aufgrund der Relevanz für Banken in Österreich wurden die Anforderungen der Leitlinien in die Anforderungsmatrix übernommen. [90]

FMA – Leitfaden IT-Sicherheit in Verwaltungsgesellschaften

- Institution: Finanzmarktaufsichtsbehörde Österreich
- Version: Nr. 02/2020 - 20.08.2020
- Rahmenwerk: Leitfaden
- Titel: Leitfaden IT-Sicherheit in Verwaltungsgesellschaften [19]
- Inhalt:
  - Rechtsgrundlagen und Grundlegendes
  - IT-Strategie
  - IT-Governance
  - Sicherheitsrichtlinien
  - Informationsrisikomanagement/Informationssicherheitsmanagement

  - Benutzerberechtigungsmanagement
  - Schwachstellenmanagement
  - IT-Projekte, Anwendungsentwicklung und zugekaufte Software
  - IT-Betrieb und Datenintegrität
  - IT-Auslagerungen
  - Verfügbarkeit und Kontinuität, Notfallmanagement
  - Besondere Aspekte bei VerwaltungsgesellschaftenLeitlinien zur Auslagerung an Cloud-Anbieter

Der Wertpapierhandel und die Finanzmarktinfrastruktur in Österreich unterliegen aufgrund des volkswirtschaftlichen Interesses einer besonderen staatlichen Aufsichtspflicht. Im Jahr 2002 hat sich die FMA in ihrer Rolle als unabhängige, weisungsfreie und integrierte Aufsichtsbehörde dieser Aufgabe angenommen. Sie vereint somit die Aufsicht über Kreditinstitute, Versicherungen, Pensionskassen und Wertpapiermärkte. Die FMA ist sich der immer bedeutender werdenden Möglichkeiten und Risiken, welche aus der IT resultieren bewusst. Aufgrund der gestiegenen Risikolage sieht die FMA die Notwendigkeit, den Verwaltungsgesellschaften einen Überblick über Ausgestaltung, Anforderungen und Vorkehrungen betreffend der IT-Sicherheit zur Verfügung zu stellen. Der Leitfaden stellt keine Verordnung dar, sondern soll vielmehr Know-How im Bereich IT-Sicherheit vermitteln und die Entwicklung eines gemeinsamen Verständnisses zum Thema IT-Sicherheit fördern. Aufgrund der Relevanz der FMA für Banken in Österreich, wurde der Leitfaden in die Anforderungsmatrix übernommen. [63]

FMA - Leitfaden IT-Sicherheit in Wertpapierdienstleistungsunternehmen und Wertpapierfirmen

- Institution: Finanzmarktaufsichtsbehörde Österreich
- Version: Nr. 04/2018 - 29.08.2018
- Rahmenwerk: Leitfaden
- Titel: Leitfaden IT-Sicherheit in Wertpapierdienstleistungsunternehmen und Wertpapierfirmen [20]
- Inhalt:
  - Rechtsgrundlagen und grundlegendes
  - IT-Strategie
  - IT-Governance
  - Sicherheitsrichtlinien
  - Informationsrisikomanagement/Informationssicherheitsmanagement
  - Benutzerberechtigungsmanagement
  - Schwachstellenmanagement
  - IT-Projekte, Anwendungsentwicklung und zugekaufte Software
  - IT-Betrieb und Datenintegrität
  - IT-Auslagerungen
  - Verfügbarkeit und Kontinuität, Notfallmanagement
  - Besondere Aspekte bei Wertpapierfirmen bzw. Wertpapierdienstleistungsunternehmen

Der Leitfaden deckt sich großteils mit dem „Leitfaden IT-Sicherheit in Verwaltungsgesellschaften“. Aufgrund der Relevanz der FMA für Banken in Österreich und gewisser Unterschiede zum bereits genannten Leitfaden, wurde der Leitfaden in die Anforderungsmatrix übernommen.

EU – PSD2

- Institution: Europäische Union
- Titel: Delegierte Verordnung zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation (PSD2) [21]
- Version: 2015/2366 auf Basis 2007/64/EG
- Rahmenwerk: Verordnung
- Inhalt:
  - Titel 1 - Gegestand, Anwendungsbereich und Begriffsbestimmungen
  - Titel 2 - Zahlungsdienstleister
  - Titel 3 - Transparenz der Vertragsbedingungen und Informationspflichten der Zahlungsdienste
  - Titel 4 - Rechte und Pflichten bei der Erbringung und Nutzung von Zahlungsdiensten
  - Titel 5 - Delegierte Rechtsakte und technische Regulierungsstandards
  - Titel 6 - Schlussbestimmungen

Die „Delegierte Verordnung zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation“ ist eine EU-Richtline zur Regulierung von Zahlungsdiensleistern und Zahlungsdiensten. Die Aufgabe der Richtlinie ist es die Sicherheit im Zahlungsverkehr zu erhöhen, den Verbraucherschutz zu stärken, Innovationen zu fördern und den Wettbewerb im Markt zu steigern. Die PSD2 ist für Zahlungen im Europäischen Wirtschaftsraum gültig und findet teilweise auch Anwendungen auf Zahlungen mit Nicht-EU-Währungen. Aufgrund der klaren Regelungen der PSD2 bei der Nutzung von Überweisungen im Onlinebanking oder für das Abfragen und Auswerten von Kontoinformationsdiensten ist sie speziell für Banken in Österreich relevant. Aus diesem Grund wurde die PSD2 in die Anforderungsmatrix aufgenommen.

EZB - Cyber resilience oversight expectations for finanzial market infrastructures

- Institution: Europäische Zentralbank
- Titel: Cyber resilience oversight expectations for finanzial market infrastructures (CROE) [60]
- Version: nicht vorhanden
- Rahmenwerk: Leitfaden
- Inhalt:

  - Governance
  - Identification
  - Protection
  - Detection
  - Response and recovery
  - Testing
  - Situational awareness
  - Learning and evolving

Die EZB ist als zentrale Einrichtung des Eurosystems für die Bankenaufsicht zuständig. Das Ziel der EZB ist die Gewährleistung der Preisstabilität im EWR und die Verwaltung der einheitlichen Währung der EU, dem Euro. Die EZB hat ihren Standort in Frankfurt am Main und tagt zweimal im Monat. Im Zuge dieser Tagungen werden wirtschaftliche und monetäre Entwicklungen bewertet. Zu den weiteren Aufgaben der EZB zählen unter anderem die Festlegung des Leitzinses, die Verwaltung von Währungsreserven und die Gewährleistung der Sicherheit und Stabilität im europäischen Bankensystem. [61]

Die Sicherheit und die Stabilität von Finanzinstituten ist essentiell für die Arbeit der EZB. Aus diesem Grund veröffentlichte die EZB im Jahr 2016 die CROE mit dem Ziel, Finanzunternehmen mit detaillierte Schritte für die Steigerung der eigenen Cyber-Resilienz zu unterstützen. Bei der Erstellung der CROE wurde von der EZB Bezug auf bereits bestehende internationale Richtlinien und Frameworks genommen. Auch wenn die EZB die Umsetzung von CROE nicht voraussetzt, stellt diese jedoch einen gewissen Standard für die Erwartungen nationaler Aufsichtsbehörden [60]. Da es sich bei CROE um keine zwingend umzusetzenden Vorgaben handelt und die Inhalte von CROE die Basis für Anforderungen von nationalen Aufsichtsbehörden stellt, wurde die CROE nicht in die Anforderungsmatrix mit aufgenommen.

Agentur der Europäischen Union für Cybersicherheit - Definition of Cybersecurity

- Institution: Agentur der Europäischen Union für Cybersicherheit
- Titel: Definition of Cybersecurity [22]
- Version: V1.0 - Dezember 2015
- Rahmenwerk: Empfehlung / Whitepaper
- Inhalt:
  - Introduction
  - Common understanding of Cybersecurity
  - Terminology of Cybersecurity in documentation
  - Standardisation work in Cybersecurity
  - Overlaps in standardisation efforts
  - Gaps in standardisation activities
  - Recommendations

Die Aufgabe der „Agentur der Europäischen Union für Cybersicherheit“ (ENISA[4]) besteht in der Gewährleistung und dem Schutz der Netz- und Informationssicherheit in der Europäischen Union. Sie unterstützt einzelstaatlichen Behörden und EU-Institionen in Bezug auf Netz- und Informationssicherheit. Des Weiteren fungiert die ENISA als zentrales Forum und unterstützt EU-Institutionen, staatliche Behörden und Unternehmen bei der Zusammenarbeit im Bereich Netz- und Informationssicherheit. Die ENISA verfolgt mit der Veröffentlichung der „Definition of Cybersecurity“ zum einen das Ziel ein gemeinsames Verständnis des Begriffs „Cybersecurity“ und zum anderen einen Überblick über Organisationen, die sich für die Standardisierung im Bereich der Cybersicherheit einsetzen, zu schaffen. Da das Dokument keine Anforderungen an technische IT-Sicherheit liefert, wurde das Dokument nicht in die Anforderungsmatrix aufgenommen. [57]

3.3 Peer Review

Um die Vollständigkeit der in Kapitel 3.2 analysierten Literatur zu überprüfen wurden Peer Reviews mit drei Personen, aus dem Bereich IT-Sicherheit und IT-Governance einer Bank in Österreich, durchgeführt:

- Peer 1: Chief Information Security Officer einer Bank in Österreich
- Peer 2: Informationssicherheits Beauftragter einer Bank in Österreich
- Peer 3: Angestellter im Bereich IT-Governance einer Bank in Österreich

Im Zuge des Reviews wurden die Peers gebeten folgende Fragen zu beantworten:

Fragestellung 1 - Aufsichtsbehörden

- Welchen Aufsichtsbehörden müssen Sie im Rahmen von regulatorischen Überprüfungen der Bank in Bezug auf IT-Sicherheit Rede und Antwort stehen?
- Welchen Aufsichtsbehörden gegenüber sind sie im Falle eines Security-Incidents innerhalb der Bank meldepflichtig?
- Sind die in Tabelle 3.1 aufgelisteten Aufsichtsbehörden Ihrer Meinung nach relevant für eine Bank in Österreich?
- Ist die Auflistung relevanter Aufsichtsbehörden für eine Bank in Österreich in Tabelle 3.1 vollständig?
- Falls nicht, welche relevanten Aufsichtsbehörden fehlen?

Fragestellung 2 - Richtlinien

- An welchen Richtlinien orientiert sich Ihr Unternehmen bei der Etablierung von IT-Sicherheitsanforderungen bzw. bei der Erstellung von Governance-Richtlinien?
- Sind die in Tabelle 3.1 aufgelisteten Richtlinien Ihrer Meinung nach relevant für eine Bank in Österreich?
- Ist die Auflistung relevanter Richtlinien in Tabelle 3.1 vollständig?

[4] https://www.enisa.europa.eu

- Falls nicht, welche relevanten Richtlinien fehlen?

Auswertung der Fragen

Die von den Peers beantworteten Fragebögen wurden ausgewertet. Auf Frage 1 antworteten die Peers, dass primär an die FMA zurückgemeldet werden muss. Im Falle von Großbanken werden die regulatorischen Überprüfungen direkt von der ÖNB durchgeführt. Im Falle eines Security-Incidents besteht eine Meldepflicht gegenüber der FMA. Im Falle von Großbanken besteht die Meldepflicht gegenüber der EZB. Die Peers sind sich darüber einig, dass die EIOPA nur für Versicherungen und nicht für Banken zuständig ist. Des Weiteren merken alle Peers an, dass die EU keine Aufsichtsbehörde in eigentlichen Sinne sei. Die EU gibt den Rahmen vor, der in weiterer Folge von den zuständigen Aufsichtsbehörden im Zuge von Überprüfungen adressiert wird. Auch die ENISA ist keine Aufsichtsbehörde sondern unterstützt öffentliche Institutionen und Behörden im Auftrag der EU. Die Peers sind sich darüber einig, dass die Auflistung relevanter Aufsichtsbehörden in Tabelle 3.1 für eine Bank in Österreich vollständig ist. Der Vollständigkeit halber können jedoch noch die ISO und die DSB erwähnt werden, auch wenn sich der Inhalt dieser in erster Linie nicht an IT-Sicherheit richtet. Die Transkription der Reviews ist in Anhang A ersichtlich.

Bezogen auf Frage 2 sind sich die Peer darüber einig, dass bei der Erstellung von IT-Sicherheitsanforderungen und Governance-Richtlinien die Richtlinien der EBA und der FMA betrachtet werden. Des Weiteren sind sich die Peers darüber einig, dass die aufgelisteten Richtlinien in Tabelle 3.1 vollständig sind.

3.4 Verwendete Richtlinien

Auf Basis der Analyse der Literatur in Kapitel 3.2 und des Ergebnisses der durchgeführten Peer Reviews in Kapitel 3.3, wurden nur die in Tabelle 3.2 enthaltenen Anforderungen an IT-Sicherheit in die Anforderungsmatrix aufgenommen. Die „Leitlinien zu Auslagerungen“ der EBA werden aufgrund des Fokus auf das Thema Auslagerungen nicht aufgenommen. Die „Leitlinien für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses“ der EZB beschäftigt sich einzig mit der Risikominimierung/-bewertung und enthalten keine technischen Anforderungen an die IT-Sicherheit für Banken in Österreich. Die „Cyber resilience oversight expetcations for financial market infrastructures“ der EZB stellt keine zwingend umzusetzende Vorgabe dar und wurde daher nicht aufgenommen. Des Weiteren bildet die CROE die Basis für Anforderungen von nationalen Aufsichtsbehörden, daher ist mit Überschneidungen in den analysierten Dokumenten zu rechnen. Die „Definition of Cybersecurity“ der ENISA beinhaltet keine technischen IT-Sicherheitsanforderungen und wurde deshalb nicht in die Anforderungsmatrix aufgenommen.

Tabelle 3.2: Übersicht über alle Richtlinien, die im Zuge der Erstellung der Anforderungsmatrix betrachtet werden

Nr	Aufsichtsbehörde	Literatur
1	BaFin	BAIT-Rundschreiben [47]
2	EBA	Leitlinien für das Management von IKT- und Sicherheitsrisiken [14]
3	EBA	Leitlinien zur zur Sicherheit von Internetzahlungen [16]
4	ESMA	Leitlinien zur Auslagerung an Cloud-Anbieter [18]
5	FMA	Leitfaden IT-Sicherheit in Verwaltungsgesellschaften [19]
6	FMA	Leitfaden IT-Sicherheit in Wertpapierdienstleistungsunternehmen und Wertpapierfirmen [20]
7	EU	Richtlinie PSD2 [21]

Kapitel 4

Anforderungsmatrix

4.1 Allgemeines

Die Analyse der in Kapitel 3.4 beschriebenen Richtlinien ergab insgesamt 417 Anforderungen an IT-Sicherheit (269 organisatorische, 148 technische), die von Banken in Österreich umzusetzen sind. Diese Anforderungen wurden zur besseren Übersicht und zur weiteren Bearbeitung in eine Anforderungsmatrix übernommen. In diesem Kapitel wird der Grundaufbau der Anforderungsmatrix und der Erstellungsprozess genauer beschrieben. Im Anschluss daran wird die Anforderungsmatrix ausgewertet.

4.2 Aufbau

Die Anforderungsmatrix gliedert sich in die 5 Bereichen „Allgemeines“, „Institution“, „Relevanz“, „Risiko“ und „Umsetzbarkeit“. Diese 5 Bereiche werden innerhalb von 23 Sub-Bereichen weiter untergliedert. Jede technische IT-Sicherheitsanforderung wird auf Basis der Bereiche und Sub-Bereiche näher definiert.

In folgendem Kapitel werden die Bereiche und die Sub-Bereiche der Anforderungsmatrix beschrieben.

Allgemeines

Dieser Bereich bietet allgemeine Informationen über die Anforderungen und beinhaltet folgende Elemente:

- #
  Diese Spalte stellt die fortlaufende Nummerierung der Anforderungen dar.
- **Kategorie**
  Jede Anforderungen ist einer Kategorien zugewiesen, welche die Anforderung bestmöglich beschreibt. Die Kategorien ermöglichen die Aufteilung der Anforderung in unterschiedliche Themengebiete, die sich im Laufe der Ausarbeitung der Anforderungsmatrix herauskristallisiert haben.

- **Titel der Anforderung**
  Der „Titel der Anforderung“ liefert Informationen zum Kapitel, unter dem die Anforderung in der jeweiligen Richtlinie angeführt ist. Der Titel dient gleichermaßen als umzusetzendes Themengebiet als auch als nähere Beschreibung der Kategorie.
- **Definition**
  Der Bereich „Definition“ definiert die tatsächlich umzusetzende Anforderung.
- **Beschreibung**
  In diesem Bereich wird die umzusetzende Anforderung, nach dem Schema „Wer“ hat „Wann“, „Was“ zu tun um die Anforderung zu erfüllen, beschrieben.
- **Referenz**
  Der Bereich „Referenz“ stellt eine Verbindung zum Dokument, in dem die Anforderung enthalten ist.

Institution

Dieser Bereich liefert Informationen über die jeweilige Richtlinie aus der die Anforderung abgeleitet wurde.

- **Institution**
  Dieses Feld definiert die Aufsichtsbehörde, welche die Richtlinie veröffentlicht hat.
- **Typ**
  Der „Typ“ gibt genauere Informationen über die Ausprägung der jeweiligen Richtlinie.
- **Dokument**
  Dieses Feld bietet eine Referenz auf die jeweilige Richtlinie.
- **Version / Fassung**
  Die Version / Fassung bietet weitere Informationen zur analysierten Ausgabe der Richtlinie.

Anforderung

Dieser Bereich liefert Informationen darüber, ob es sich bei der Anforderung um eine EU-weite Regelung handelt, die Anforderung speziell für Österreich gilt oder für andere Länder relevant ist. Aufgrund der wirtschaftlichen Nähe zwischen Österreich und Deutschland, können sich österreichische Prüfungsorgane auch an deutschen Richtlinien orientieren.

- **EU**
  Gibt an, dass es sich bei der Anforderung um eine EU-weite Richtlinie handelt.
- **AT**
  Gibt an, dass die Anforderung nur in Österreich Gültigkeit besitzt.
- **Andere**
  Definiert das Land für das die jeweilige Anforderung gilt, falls die Anforderung nicht EU-weit gültig oder ausschließlich für Österreich gültig ist.

Risiko

Der Bereich „Risiko“ beschreibt den der Anforderung zugrunde liegenden Risikofaktor.

- **Risikofaktor**
  Der „Risikofaktor“ unterteilt das durch die Anforderung adressierte Risiko in die Bereiche „Technisch“, „Organisatorisch“, „Menschlich“ und „Rechtlich“. Die unterschiedlichen Bereiche werden in Kapitel 4.3 genauer beschrieben.

Umsetzbarkeit

Im Zuge der Umsetzbarkeit wird analysiert, wie und durch welche Maßnahme die Anforderung umgesetzt werden kann. Auf Basis der Maßnahmen wird auf Best-Practice-Ansätze geschlossen.

- **Technisch**
  Die Anforderung kann mit Hilfe von technischen Mitteln umgesetzt werden.
- **Beschreibung**
  Beschreibung der technischen Umsetzbarkeit.
- **Organisatorisch**
  Die Anforderung kann organisatorisch umgesetzt werden.
- **Beschreibung**
  Beschreibung der organisatorischen Umsetzbarkeit.
- **Abgedeckt durch Maßnahme x**
  Dieser Sub-Bereich beschreibt die konkreten Maßnahmen für die Umsetzung. An Hand dieser Maßnahmen werden im Zuge der Ausarbeitung Best-Practice-Ansätze definiert.

4.3 Erstellung

Im ersten Schritt wurde der Inhalt der Richtlinien aus Kapitel 3.4 analysiert und die darin enthaltenen Anforderungen in den Bereichen „Allgemeines“, „Institution“ und „Anforderung“ niedergeschrieben. Im Zuge der Ausarbeitung wurden sämtliche evaluierten Anforderungen in die Matrix übernommen und der Fokus nicht nur auf technisch umsetzbare Anforderungen gelegt. Dies hat den Grund, dass auch auf den ersten Blick vermeintlich organisatorisch zu lösende Anforderungen unter Umständen technisch umgesetzt werden können und vice versa.

Im zweiten Schritt wurden die Anforderungen auf Basis ihres Inhalts gruppiert und in weiterer Folge entsprechend nach Themengebiet kategorisiert. Für die Kategorisierung, zu finden im Bereich „Allgemein“ - „Kategorie“ , wurden passende Themengebiete gewählt, welche die jeweiligen Anforderungen bestmöglich beschreiben.

Im dritten Schritt wurde festgelegt, ob die jeweilige Anforderung für Unternehmen in der Europäischen Union, Österreich oder anderen Ländern gültig ist.

Im vierten Schritt wurde den Anforderungen jeweils ein Risikofaktor zugewiesen. Im Zuge der Ausarbeitung haben sich folgende Risikofaktoren als passend erwiesen:

- Technischer Risikofaktor
- Organisatorischer Risikofaktor
- Menschlicher Risikofaktor
- Rechtlicher Risikofaktor

Technischer Risikofaktor

Dieser Risikofaktor bedeutet, dass die Anforderung auf den Schutz von Vertraulichkeit, Integrität oder Verfügbarkeit des zu schützenden Assets ausgelegt ist. Ein Beispiel dafür ist die Anforderung, dass Organisationen sich laufend über Bedrohungen und Schwachstellen des Informationsverbundes zu informieren, deren Relevanz zu prüfen, diese zu Bewertung und entsprechend Maßnahmen zu ergreifen haben. Ein nicht einhalten dieser Anforderung könnte in einem Angriff mittels Malware über eine Schwachstelle im System oder etwa einem Denial-of-Service Angriff resultieren. Beide Angriffe würden die Vertraulichkeit, Integrität oder Verfügbarkeit der Systeme und der darin enthaltenen Daten gefährden.

Organisatorischer Risikofaktor

Dieser Risikofaktor adressiert Anforderungen, die auf den Erhalt von Kontrolle, Kommunikation, Information oder Nachvollziehbarkeit von Prozessen und Abläufen innerhalb des Unternehmens ausgelegt sind. Ein Beispiel bietet die Anforderung an Unternehmen, die Rolle eines Informationssicherheitsbeauftragten zu etablieren. Wird dieser Anforderung nicht nachgekommen können diverse sicherheitsrelevante Prozesse nicht eingehalten und relevante Informationen gegebenenfalls nicht kommuniziert werden.

Menschlicher Risikofaktor

Anforderungen mit diesem Risikofaktor dienen dem Schutz von Mitarbeiter*innen und Kund*innen des Unternehmens. Ein Beispiel ist die Anforderung an Unternehmen, ein kontinuierliches und angemessenes Sensibilisierung- und Schulungsprogramm für Informationssicherheit festzulegen und den Erfolg der Maßnahmen regelmäßig zu überprüfen. Wird diese Anforderung nicht erfüllt fehlt den Mitarbeitern des Unternehmens Awareness im Bereich IT-Sicherheit. Eine mögliche Auswirkung könnte ein erfolgreicher Phishing-Angriff per Email sein. In diesem Fall könnte auch der Mitarbeiter zur Verantwortung gezogen werden.

Rechtlicher Risikofaktor

Anforderungen mit diesem Risikofaktor schützen Unternehmen vor Imageschäden, Strafgebühren, Strafverfolgung oder monetären Schäden. Ein Beispiel hierfür ist die Anforderung, dass Unternehmen sicherzustellen haben, dass Tests und Überprüfungen zur Informationssicherheit von unabhängigen Prüfern mit ausreichenden Kenntnissen, Fähigkeiten und Fachwissen durchgeführt werden. Eine Auswirkung der Nichteinhaltung

könnte eine Strafverfolgung aufgrund eines Angriffs sein, bei dem Kundendaten entwendet wurden. Kann das Unternehmen nicht nachweisen, dass der implementierte Schutz zur Informationssicherheit den geforderten Standards entspricht, könnte das Unternehmen hier haftbar gemacht werden.

Im letzten Schritt wurde Bezug auf die Umsetzbarkeit der einzelnen Anforderungen genommen. Hierbei wurde unterschieden, ob sich die Anforderung technisch und / oder organisatorisch umsetzen lässt. Im Zuge dessen wurde analysiert, mit welchen Maßnahmen sich die technischen Anforderung umsetzen lassen. Hierfür wurden pro Anforderung bis zu vier Maßnahmen definiert. Aus diesen Maßnahmen werden in weiterer Folge Best-Practice-Ansätze abgeleitet.

4.4 Auswertung und Erkenntnisgewinn

Im Zuge der Ausarbeitung der in Tabelle 3.2 ausgewählten Richtlinien konnten 417 IT-Sicherheitsanforderungen an eine Bank in Österreich abgeleitet werden. Diese Anforderungen unterteilen sich in 148 Anforderungen die technisch umzusetzen sind und 269 Anforderungen die organisatorisch umzusetzen sind, wie in Tabelle 4.1 ersichtlich. Interessant ist die Erkenntnis, dass zwei Drittel der Anforderungen an IT-Sicherheit für Banken in Österreich keinen technischen Hintergrund besitzen.

Tabelle 4.1: Übersicht technischer und organisatorischer Anforderungen.

Anforderung	Anzahl	Prozentanteil
Organisatorisch	269	64.5%
Technisch	148	32.5%
Gesamt	417	100 %

Im Zuge der Ausarbeitung der Anforderungsmatrix, konnten die Richtlinien folgenden Kategorien zugeordnet werden:

- Auslagerung und Fremdbezug IT-Dienstleistungen
- Business-Continuity Management
- Identity- und Access-Management
- Informationsrisikomanagement
- Informationssicherheitsmanagement
- IT-Betrieb
- IT-Projekte und Anwendungsentwicklung
- IT-Strategie
- Management Zahlungsdienstleister
- Management Zahlungsdienstnutzer
- Operative Informationssicherheit

Die Kategorie „Auslagerung und Fremdbezug IT-Dienstleistungen“ vereint alle Anforderungen die sich auf die Auslagerung von Funktionen, Tätigkeiten und Systemen beziehen. Des Weiteren wird in diesen Anforderungen festgelegt, wie mit Dienstleistungen umzugehen sind, die von Dritten bezogen werden. Ein Beispiel für eine Anforderung aus dieser Kategorie ist, dass für jeglichen Fremdbezug von IT-Dienstleistungen vorab eine Risikobewertung durchzuführen ist und die Organisation diese Bewertung laufend zu überwachen und aktuell zu halten hat. Im Bereich „Business-Continuity Management“ sind Anforderungen enthalten, die sich auf den stabilen Betrieb des Unternehmens beziehen. Ein Beispiel hierfür ist die Anforderung, dass für den Fall einer Störung oder einem Notfall wirksame Maßnahmen zur internen und externen Krisenkommunikation zu definieren sind.

Die Kategorie „Identity- und Access-Management“ vereint Anforderungen die sich auf das Management von Benutzeraccounts, die Vergabe von Berechtigungen und den Zugriff auf IT-Ressourcen beziehen. So besteht etwa die Anforderung, dass ein Prozess zur Regelung von Berechtigungsvergaben auf IT-Ressourcen zu definieren ist. Dies schützt Unternehmen vor einer missbräuchlichen Verwendung oder einer unautorisierten Manipulation von Daten und IT-Systemen. In der Kategorie „Informationsrisikomanagement“ sind Anforderungen rund um die Themen Risikoanalyse, Schutzbedarfsanalyse und Risikobewertung definiert. So haben Unternehmen beispielsweise der Forderung nachzukommen, dass IT-Assets, Geschäftsfunktionen und Unterstützungsprozesse in Hinblick auf deren Kritikalität entsprechend einzustufen sind.

Die Richtlinien in der Kategorie „Informationssicherheitsmanagement“ beschäftigen sich mit der Compliance und Governance von Unternehmen. So ist die Geschäftsleitung eines Unternehmens etwa verpflichtet die Funktion eines Informationssicherheitsbeauftragten zu etablieren und diesen zu stellen. Unter die Kategorie „IT-Betrieb“ fallen Anforderungen die sich um das Management, die Verfügbarkeit und den physischen Schutz von IT-Ressourcen drehen. Ein Unternehmen ist verpflichtet Konzepte zur Hochverfügbarkeit zu implementieren, diese anzuwenden und entsprechend zu überprüfen.

Der Bereich „IT-Projekte und Anwendungsentwicklung“ umfasst Anforderungen die sich mit der Steuerung von Projekten und der Entwicklung von eigenen Anwendungen beschäftigen. Ein Beispiel für eine Anforderung aus dieser Kategorie ist, dass ein Unternehmen für Projekte ausreichende personelle Ressourcen zur Verfügung zu stellen hat. Die Kategorie „IT-Strategie“ beinhaltet Anforderungen an die strategische Ausrichtung eines Unternehmens, die Aus- und Weiterbildung von Mitarbeitern und der Festlegung von Zuständigkeiten. So hat die Geschäftsleitung eines Unternehmens eine IT-Strategie zu erstellen die im Einklang mit Art, Umfang und Komplexität der Geschäftstätigkeit steht.

Die beiden Kategorien „Management Zahlungsdienstleister“ und „Management Zahlungsdienstnutzer“ behandeln Anforderungen zum Schutz von Kunden und Kundentransaktionen. So ist ein Unternehmen beispielsweise verpflichtet seine Kunden über mögliche neue Gefahren, Schwachstellen oder Änderungen in IT-Systemen zu informieren. In der letzten Kategorie „Operative Informationssicherheit“ sind Anforderungen

zusammengefasst, die sich mit dem Thema IT-Sicherheit und der technischen Implementierung von IT-Sicherheitsmaßnahmen beschäftigen. So ist ein Unternehmen beispielsweise verpflichtet, Daten bei der Speicherung und der Übertragung gemäß definiertem Schutzbedarf zu verschlüsseln.

Tabelle 4.2 zeigt die Aufteilung der Anforderungen auf die unterschiedlichen Kategorien.

Tabelle 4.2: Kategorien der Anforderungsmatrix und die Anzahl der zugeordneten Anforderungen.

Kategorie	Anzahl
Auslagerung und Fremdbezug IT-Dienstleistungen	53
Business-Continuity Management	14
Identity- und Access-Management	31
Informationsrisikomanagement	49
Informationssicherheitsmanagement	35
IT-Betrieb	47
IT-Projekte und Anwendungsentwicklung	40
IT-Strategie	38
Management Zahlungsdienstleister	12
Management Zahlungsdienstnutzer	46
Operative Informationssicherheit	52

Abbildung 4.1 zeigt die prozentuale Verteilung aller Anforderungen auf die unterschiedlichen Kategorien. Es sind keine Ausreißer zu erkennen, mit Ausnahme von „Management Zahlungsdienstnutzer“ und „Business-Continuity Management“ verteilen sich die Anforderungen gleich auf die unterschiedlichen Kategorien.

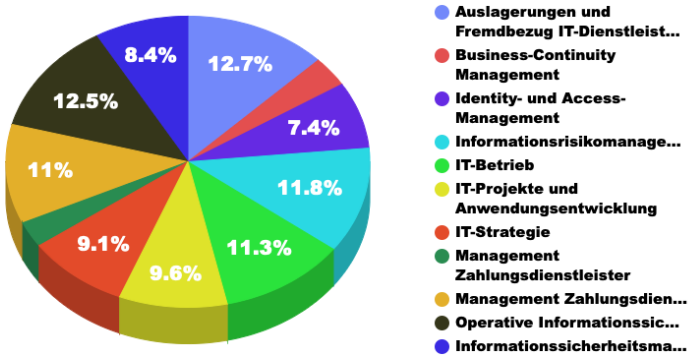

Abbildung 4.1: Visuelle Darstellung der Aufteilung aller Anforderungen auf die definierten Kategorien. Quelle: Eigene Darstellung, 2022

Betrachtet man in weiterer Folge nur jene Anforderungen die technisch umzusetzen sind, ergibt sich die in Tabelle 4.3 dargestellte Aufteilung. Es ist zu erkennen, dass die technisch umzusetzenden Anforderungen vorwiegend in den Kategorien „Identity- und Access-Management“, „IT-Betrieb“ und vor allem in der Kategorie „Operative Informationssicherheit“ zu finden sind. Abbildung 4.2 zeigt die prozentuale Verteilung der technischen Anforderungen auf die unterschiedlichen Kategorien.

Tabelle 4.3: Zeigt die Kategorien der Anforderungsmatrix und die Anzahl der zugeordneten, technischen Anforderungen.

Kategorie	Anzahl
Auslagerung und Fremdbezug IT-Dienstleistungen	1
Business-Continuity Management	1
Identity- und Access-Management	30
Informationsrisikomanagement	7
Informationssicherheitsmanagement	11
IT-Betrieb	31
IT-Projekte und Anwendungsentwicklung	2
IT-Strategie	1
Management Zahlungsdienstleister	0
Management Zahlungsdienstnutzer	18
Operative Informationssicherheit	46

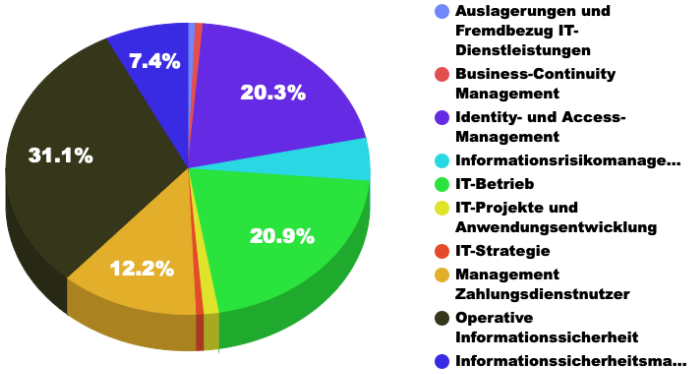

Abbildung 4.2: Visuelle Darstellung der Aufteilung von technischen Anforderungen auf die definierten Kategorien. Quelle: Eigene Darstellung, 2022

Zur besseren Veranschaulichung wurden die organisatorisch und technisch umzusetzenden Anforderungen in Tabelle 4.4 direkt gegenübergestellt. Es ist zu erkennen, dass es nur eine Anforderungen aus dem Bereich „Auslagerung und Fremdbezug IT-Dienstleistungen“ gibt, die sich technisch umsetzen lässt. Es handelt sich dabei um die Anforderung, dass Informationen die mit Drittanbietern ausgetauscht werden verschlüsselt übertragen werden müssen. Alle anderen Anforderungen liegen in der Durchführung bei dem jeweiligen Auslagerungspartner. Die technischen Anforderungen bestehen somit auf Seiten des Dritten. Auch im Bereich „Business-Continuity Management“ besteht nur eine technische Anforderung. Es handelt sich dabei um die Notwendigkeit für eine redundante Auslegung von kritischen IT-Komponenten.

Im Gegensatz zu den eben genannten Kategorien, sind 30 von 31 Anforderungen aus dem Bereich „Identity- und Access-Management“ technischer Natur. Bei einer organisatorischen Anforderungen handelt es sich um die Notwendigkeit die implementierten, technischen Zugangskontrollen zu überwachen. Interessant ist, dass nur 5% der Anforderungen aus dem Bereich „IT-Projekte und Anwendungsentwicklung“ technisch erfüllt werden können. Es geht dabei um die Vorgabe, dass eigens erstellte Anwendungen auf mögliche Abweichungen vom Regelbetrieb zu überwachen und die Integrität der Anwendung, insbesondere des Quellcodes, angemessen sicherzustellen ist.

Ein weiterer Ausreißer findet sich im Bereich „IT-Strategie“. Nur eine Anforderung kann technisch umgesetzt werden. Es geht dabei um die Notwendigkeit, dass die Geschäftsleitung imstande sein muss Aussagen zu selbst entwickelten oder selbst betriebenen IT-Systemen treffen zu können. Auch wenn für die Umsetzung der Anforderung nur Informationen nötig sind, kann die Effizienz durch ein Verwaltungssystem, wie beispielsweise einer Content-Management-Database (CMDB) gesteigert werden. Im Bereich „Opera-

tive Informationssicherheit“ bestehen 6 Anforderungen die organisatorisch umzusetzen sind. Diese Anforderungen wurden nicht als „Technische Anforderung“ deklariert, da die Umsetzung vorrangig organisatorisch zu definieren ist. Ein Beispiel hierfür ist die Vorgabe, dass ein Zahlungsdienstkunde eine Warnung erhält, bevor eine dauerhafte Sperre seines Accounts in Kraft tritt.

Tabelle 4.4: Zeigt alle Kategorien und die Anzahl der zugeordneten Anforderungen.

Kategorie	Gesamt	Organisatorisch	Technisch
Auslagerung und Fremdbezug IT-Dienstleistungen	53	52	1
Business-Continuity Management	14	13	1
Identity- und Access-Management	31	1	30
Informationsrisikomanagement	49	42	7
Informationssicherheitsmanagement	35	14	11
IT-Betrieb	47	16	31
IT-Projekte und Anwendungsentwicklung	40	38	2
IT-Strategie	38	37	1
Management Zahlungsdienstleister	12	12	0
Management Zahlungsdienstnutzer	46	28	18
Operative Informationssicherheit	52	6	46

Im Zuge der Auswertung der Anforderungsmatrix wurden auch die Risikofaktoren näher betrachtet. Abbildung 4.3 zeigt die Verteilung der Risikofaktoren bezogen auf die abgeleiteten Anforderungen. Es ist zu erkennen, dass sich je ein Drittel der Risiken auf die beiden Bereiche „Technisch“ und „Organisatorisch“ verteilen. Daraus lässt sich ableiten, dass zwei Drittel der Anforderungen auf den Schutz der Infrastruktur und der internen Abläufe und Prozesse des Unternehmens ausgelegt sind.

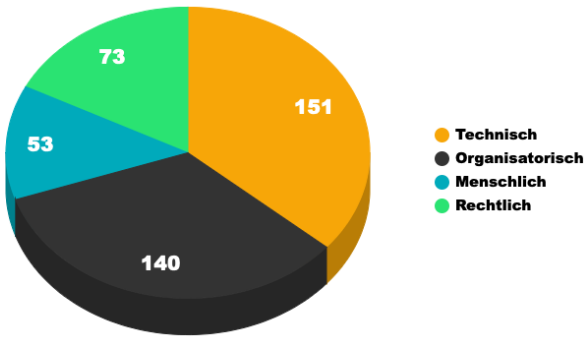

Abbildung 4.3: Visuelle Darstellung der Aufteilung der Risikofaktoren aller Anforderungen. Quelle: Eigene Darstellung, 2022

Abbildung 4.4 zeigt die Verteilung der technischen Anforderungen auf die unterschiedlichen Risikofaktoren. Wie zu erwarten war, adressieren ein Großteil der Anforderungen

den „Technischen Risikofaktor“. Interessant ist hierbei, dass 23 Anforderungen Bezug auf den „Menschlichen Risikofaktor“ nehmen. Es handelt sich dabei um die Anforderungen aus dem Bereich „Identity- und Access-Management“. Betrachtet man die technischen Anforderungen die den „Rechtlichen Risikofaktor“ adressieren, handelt es sich dabei um die Anforderungen zum Schutz von Transaktionsüberwachungen im Bereich Onlinebanking. Können betrügerische Zahlungen nicht erkannt oder etwa persönliche Sicherheitsmerkmale von Kunden nicht geschützt werden, kann dies rechtliche Konsequenzen für das Unternehmen mit sich ziehen. Bei den technischen Anforderungen die das „Organisatorische Risiko“ adressieren, handelt es sich großteils um Anforderungen zum Umgang und der Verwaltung von IT-Ressourcen. Eine fehlende Verwaltung oder ein nicht definierter Umgang mit IT-Ressourcen kann zu Problemen beim Ablauf interner Prozesse führen und so die Stabilität des Unternehmens gefährden. Anforderungen mit „Technischem Risikofaktor“ beziehen sich unter anderem auf die Implementierung von IT-Sicherheitsmaßnahmen und den Schutz von IT-Ressourcen und Daten. In Anbetracht der Tatsache, dass hierbei nur Anforderungen betrachtet wurden die technisch umgesetzt werden können, erscheint die Aufteilung legitim.

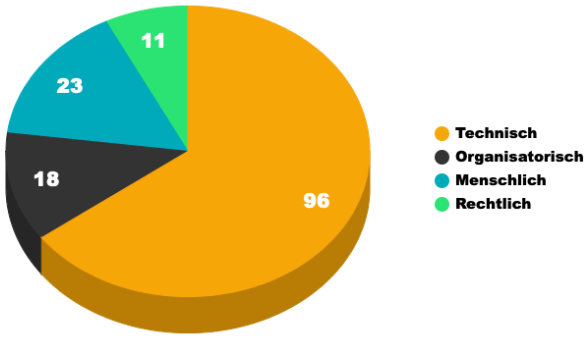

Abbildung 4.4: Visuelle Darstellung der Aufteilung der Risikofaktoren technischer Anforderungen. Quelle: Eigene Darstellung, 2022

4.5 Abgeleitete Maßnahmen

Dieses Kapitel gibt eine Übersicht über die aus den Anforderungen abgeleiteten Maßnahmen und zeigt, wie viele Anforderungen die einzelnen Maßnahmen abdecken. Auf Basis dieser Anforderungen wird in weiterer Folge versucht, Best-Practice-Ansätze für die Umsetzung der technischen IT-Sicherheitsvorgaben abzuleiten. Die nötigen Informationen für die Evaluierung der einzelnen Maßnahmen erfolgte auf Basis von Recherchen im Internet und Befragung von Mitarbeitern aus dem Bereichen „IT-Security“ und „IT-

Infrastruktur“ einer Bank in Österreich.

Im Zuge der Erstellung der Anforderungsmatrix wurde im Bereich „Umsetzbarkeit“ definiert, ob die jeweilige Anforderung technisch oder organisatorisch umgesetzt werden kann. Der Bereich „Beschreibung“ bietet eine Zusammenfassung für eine mögliche Umsetzung. Die Bereiche „Abgedeckt durch Maßnahme x“ geben eine Übersicht über mögliche technische Maßnahmen, mit denen die Anforderung umgesetzt werden kann. Für die Evaluierung der möglichen Maßnahmen wurden pro Anforderung folgende Schritte durchgeführt:

1. Recherche im Internet mit Hilfe der Informationen aus den Bereichen „Kategorie“, „Titel der Anforderung“ und „Definition“ der Anforderungsmatrix.
2. Recherche von möglichen Hardware-/Softwareprodukten zur Adressierung der jeweiligen Anforderung.
3. Befragung von Mitarbeitern aus den Bereichen „IT-Infrastruktur“, „IT-Technik“ und „Security-Operation-Center“ einer Bank in Österreich.

Tabelle 4.5 zeigt eine Auflistung der abgeleiteten Maßnahmen und die Anzahl der technischen Anforderungen, die mit der jeweiligen Maßnahme umgesetzt werden können. Bei dieser Auswertung ist zu beachten, dass Anforderungen auch mit mehr als einer Maßnahme umgesetzt werden können. Aus diesem Grund variieren die Anzahl der technischen Anforderungen und die Anzahl der in Tabelle 4.5 dargestellten Maßnahmen. Interessant ist hierbei, dass sich 15% der Anforderungen mittels der Adressierung von „Identity-Management“ umsetzen lassen. Das bedeutet, dass Aufsichtsbehörden großen Wert auf den korrekten Umgang mit Berechtigungen und Accounts legen. 10% der Anforderungen können durch die Betrachtung von „Vulnerability-Management“ und weitere 9% durch „Security Incident und Event Monitoring“ adressiert werden. Daraus resultiert die Tatsache, dass sich ein Drittel der technischen Anforderungen für IT-Sicherheit an eine Bank in Österreich mit der Implementierung von drei Maßnahmen umsetzen lassen.

Tabelle 4.5: Zeigt eine Übersicht über die analysierten Maßnahmen und die Anzahl der adressierten, technischen Anforderungen.

Maßnahme	Anzahl adressierter Anforderungen
Identity-Management	32
Vulnerability-Management	21
Security Incident und Event Monitoring	20
Kryptografie	17
Content-Management Database	15
Multifaktor-Authentifizierung	15
Patch-Management	15
Zentrales Log-Management	13
Netzwerksegmentierung	11
Monitoring	10
Single-Sign On	10
Backup and Restore	10
Endpoint-Detection and Response	7
Penetration-Testing	6
Baselining und Change-Management	4
Sourcecode Verwaltung	4
Native-Change Detection	3
Privileged-Access Management	3
Hochverfügbarkeit	3
Firewalls	2
Network-Access Control	1

Kapitel 5

Best-Practice-Ansätze

In diesem Kapitel wird versucht, die in Kapitel 4.5 abgeleiteten technischen Maßnahmen in Bereiche zu Gruppieren. Auf Basis dieser Gruppen werden die einzelnen Maßnahmen beschrieben und Best-Practice-Ansätze definiert um eine umfassende und effiziente Adressierung der Maßnahmen zu ermöglichen. Die Gruppierung hat sich im Zuge der Ausarbeitung als sinnvoll ergeben, da unterschiedliche Maßnahmen ineinander greifen und voneinander profitieren.

Unter einem Best-Practice-Ansatz kann eine bestmögliche, bereits erprobte Methode oder Maßnahme zur Umsetzung einer Problemstellung verstanden werden. Ein Best-Practice-Ansatz stellt allerdings im allgemeinen Sprachgebrauch nur eine unverbindliche Empfehlung dar und unterscheidet sich somit von einem etablierten Standard. Die Empfehlung kann aufgrund Erfahrungen der jeweiligen Community entstehen oder sich im Laufe der Zeit als die effizienteste Methode etabliert haben. [54]

Zur besseren Übersicht sind die Gruppen, die enthaltenen Maßnahmen und die abgeleiteten Best-Practice-Ansätze in Abbildung 5.1 dargestellt. In weiterer Folge werden die einzelnen Gruppen und Best-Practice-Ansätze näher beschrieben

Gruppierung	Enthaltene Maßnahmen	Abgeleitete Best-Practise Ansätze
Identity- und Access-Management	Identity-Management	Identity-Management
	Native-Change Detection	
	Multifaktor-Authentifizierung	Access-Management
	Single-Sign On	
	Privileged-Access Management	
Asset-Management	Content-Management Database	Content-Management Datanbase
	Source-Code Verwaltung	Everything as Code
	Baselining und Change-Management	
Infrastruktur-Betrieb	Monitoring	Ausfallsicherheit
	Hochverfügbarkeit	
	Patch-Management	
	Backup-Restore	Recovery-Management
Netzwerk-Management	Netzwerk-Segmentierung	Netzwerk-Segmentierung
	Network-Access Control	
	Firewalls	
	Kryptografie	Verschlüsselung
Cybersecurity-Management	Log-Management	Zentrales Log-Management
	Security Incident Event Monitoring	Schwachstellen-Management
	Vulnerability-Management	
	Penetration-Testing	
	Endpoint-Detection and Response	

Abbildung 5.1: Visuelle Darstellung der Gruppierungen, enthaltenen Maßnahmen und abgeleiteten Best-Practice-Ansätzen. Quelle: Eigene Darstellung, 2022

5.1 Identity- und Access-Management

Die Gruppe „Identity- und Access-Management“ (IAM) vereint die Maßnahmen „Identity-Management“, „Privileged-Access Management“ (PAM), „Multifaktor-Authentifizierung“ (MFA), „Single-Sign On“ (SSO) und „Native-Change Detection“ (NCD). Die Gruppe beschäftigt sich mit dem Lifecycle, der Authentifizierung und der Autorisierung von Identitäten und Benutzeraccounts.

Darran Rolls und Morey J. Haber beschreiben in ihrem Buch „Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution“ fünf Grundpfeiler des IAM, die fünf „A´s“ [11]:

- Administration
- Audit
- Analyse
- Authentifizierung
- Autorisierung

Die in der Gruppe IAM enthaltenen Maßnahmen decken jede für sich einen Teil der fünf A´s ab und tragen so zum Schutz von Identitäten und IT-Systemen bei.

Best-Practice-Ansatz: Identity-Management-System (IDM)

Um Identitäten eines Unternehmens und deren zugeordnete Accounts in den unterschiedlichen Systemen verwalten zu können, ist eine globale Administration von beteiligten Identitäten erforderlich. Die in Kapitel 4.5 abgeleitete Maßnahme „Identity-Management“ deckt die drei Bereiche „Administration“, „Audit“ und „Analyse“ ab. Eine globale Administration von Identitäten kann mit Hilfe eines „Identity-Management Systems“ (IDM) realisiert werden. Ein IDM verwaltet Identitäten und bildet den gesamten Lifecycle einer Identität auf Basis von Prozessen ab. Zu diesem Lifecycle zählen das Erstellen der Identität, das Erstellen von Accounts, die Vergabe, Änderung und der Entzug von Berechtigungen. Das Ausscheiden einer Identität aus dem Unternehmen und damit einhergehend das Löschen aller zugehörigen Accounts schließt den Lifecycle ab. Ein IDM bietet somit die Möglichkeit den gesamten Lifecycle einer Identität zu definieren, durchzuführen und zu auditieren. Um dies zu ermöglichen werden unterschiedliche IT-Systeme, in Form von „Applikationen“, an das IDM angebunden. Beispiele für angebundene Applikationen sind etwa Benutzerdatenbanken auf die von unterschiedlichen anderen IT-Systemen zugegriffen wird.

Aufgrund der Tatsache, dass ein IDM System den gesamten Lifecycle von Identität und Berechtigungen abbildet, muss die Integrität der Daten gewährleistet werden. Aus diesem Grund wird ein IDM System als „Single Source of Truth“ etabliert. Eine nicht autorisierte Änderung an einer Identität kann mittels NCD erkannt und behoben werden. Somit wird gewährleistet, dass ein IDM System bei einer direkten, nicht autorisierten Änderung in einem angebundenen System eingreifen kann. Eine mögliche Aktion des IDM wäre, dass die durchgeführte Änderung automatisch überschrieben und somit der vom IDM definierten Stand der Identität wieder herstellt wird. Mittels NCD können Unternehmen der Anforderung Nummer 317 laut Anforderungsmatrix nachkommen. In dieser Anforderung fordert die FMA, dass Unternehmen durch technisch-organisatorische Maßnahmen sicherzustellen haben, dass eine Manipulation der Berechtigungskonzepte verhindert wird.

Durch die Abbildung des Lifecycles von Identitäten und Berechtigungen innerhalb eines IDM wird auch weiteren Anforderungen von Aufsichtsbehörden nachgekommen. So ist laut Anforderung Nummer 315 aus der Anforderungsmatrix ein Unternehmen laut FMA verpflichtet, dass die Einräumung, Änderung, Deaktivierung und Löschung von Berechtigungen nachvollziehbar, zuordenbar und auswertbar dokumentiert wird. Diese Anforderung kann mit Hilfe eines IDM realisiert werden.

Eine weitere Anforderung der FMA besteht darin, dass die den Identitäten eingeräumten Berechtigungen jederzeit, auditierbar sein müssen. Die Anforderung ist in der Anforderungsmatrix unter der Nummer 45 ersichtlich und kann mittels einer Rezertifizierung von Berechtigungen erfüllt werden. Im Zuge einer Rezertifizierung wird überprüft, welche Identitäten ein zu auditierendes Recht besitzen. Somit kann die Zuordnung einer bestimmten Berechtigung im Zuge einer Rezertifizierung legitimiert oder auch sämtlichen Identitäten gesammelt entzogen werden. Auch eine „Separation of Duty“ (SoD) kann mittels eines IDM realisiert werden. Unter einer SoD versteht man eine Funktionstrennung von Identitäten. Mit Hilfe dieser Funktionstrennung soll beispielsweise

vermieden werden, dass eine Identität die Berechtigung für das Anfordern eines Darlehens und gleichzeitig die Berechtigung für die Genehmigung dieses Darlehens besitzt. Das Vorhandensein von solchen Konstellationen kann mittels einer Analyse durch ein IDM überprüft werden.

Ein Beispiel für ein IDM, das die beschriebenen Funktionen zur Verfügung stellt, ist „Sailpoint Identity-IQ“ [23].

Best-Practice-Ansatz: Access-Management

Die beiden nach Darran Rolls und Morey J. Haber noch verbleibenden Grundpfeiler „Authentifizierung“ und „Autorisierung“ zählen zum Bereich des Access-Managements.

Unter einer Authentifizierung wird ein Login in Verbindung mit einer Art von Geheimnis, meist in der Ausprägung eines Passworts, verstanden. Eine Authentifizierung (v. griechischen „authentikos“ für Urheber, der Echte, der Wirkliche), bezeichnet das Nachweisen einer Identität und den legitimen Zugang zu Privilegien, die der nachgewiesenen Identität zustehen. Alexander Tsolkas und Klaus Schmidt beschreiben in ihrer Arbeit „Rollen und Berechtigungskonzepte - Identity- und Access-Management im Unternehmen“ die Möglichkeit zur Durchführung einer Authentifizierung mittels drei unterschiedlichen Objekten [13]:

- Preisgabe von Wissen (Passwort, PIN-Code, ...)
- Benutzung eines Besitzes (Token, ...)
- Benutzung des eigenen Subjekts (Retinascan, Fingerabdruck, ...)

Die Authentifizierung einer Identität erfolgt im einfachsten Fall mittels Benutzername und Kennwort und wird von dem jeweiligen System durchgeführt, auf das die Identität zugreifen möchte. Das System nimmt hierfür den Benutzeraccount und das Passwort der Identität entgegen und verifiziert diese beiden Daten gegen eine Datenbank. Diese als „Basic-Authentication“ bekannte Methode hat den Nachteil, dass jedes System für sich eine Abbildung der im IDM verwalteten Identitäten besitzen oder Zugriff auf die zugrunde liegende Datenbank haben muss. Mit der Anzahl der Systeme die Zugriff auf sensible Daten, wie etwa der Datenbank mit Benutzeraccounts und Kennwörtern benötigen, steigt auf das Risiko bei einer Kompromittierung des Systems. Gerade bei Systemen die beispielsweise aus dem freien Internet erreichbar sind oder nicht in der Verantwortung eines Unternehmens stehen, ist ein direkter Zugriff auf Benutzerdaten kritisch zu sehen. [11]

Die EBA fordert in ihrer Leitlinie für das Management von IKT- und Sicherheitsrisiken, dass Authentifizierungsmethoden der Kritikalität der IKT-Systeme angemessen sein sollen. Diese Anforderung ist unter der Nummer 117 in der Anforderungsmatrix ersichtlich. Auf Basis dieser Anforderungen wurden Möglichkeiten etabliert, damit kritische Systeme nicht mit sensiblen Daten, wie etwa Passwörtern, in Berührung kommen. Eine Möglichkeit dafür bietet die Verwendung von Token-basierten Authentifizierungsmethoden, wie sie bei SSO-Systemen verwendet werden. Das „OAuth 2.0 Protokoll“ beziehungsweise die Verwendung des Layers „OpenID-Connect 1.0“ bietet Verfahren

für diese Art der Authentifizierung. OAuth 2.0 ist ein offenes und standardisiertes Protokoll für die Token-basierte Authentifizierung im Internet [24] [25].

Abbildung 5.2 zeigt den Ablauf einer Authentifizierung mittels Token. Im Zuge der Authentifizierung sind drei Komponenten beteiligt. Der „Browser“ symbolisiert die Identität, die Zugriff auf eine Ressource, die „Applikation“ erhalten möchte. Der „Authorization Server“ übernimmt die Rolle des SSO-Systems. Im ersten Schritt fordert der Browser Zugriff auf die Applikation. Innerhalb der Applikation wurde definiert, dass die Authentifizierung über den Authorization-Server stattfinden soll. Aus diesem Grund antwortet die Applikation mit einem Redirect zum Authorization-Server. Im Zuge des Redirects bietet der Authorization-Server eine Login-Seite, auf sich die Identität mittels Benutzername und Kennwort anmeldet. Der Authorization-Server validiert die von der Identität eingegeben Daten und antwortet mit einem Redirect zurück zur Applikation, gepaart mit einem zuvor generierten Authentication-Code. Im nächsten Schritt fordert die Applikation unter Verwendung des Authentication-Codes einen Token beim Authorization-Server an. Nach erfolgreicher Validierung des Authentication-Codes durch den Authorization-Server wird ein Token generiert und der Applikation übermittelt. Der Token stellt somit die Legitimation der Identität sicher. Aufgrund der Tatsache, dass die Applikation dem Authorization-Server vertraut, kann nun der Zugriff auf die Applikation gewährt werden.

Dieses Beispiel beschreibt die Möglichkeit einer Anmeldung an einem kritischen System. Der Vorteil liegt darin, dass das System selbst zu keinem Zeitpunkt der Anmeldung Kenntnis über die Logindaten der Identität erhält.

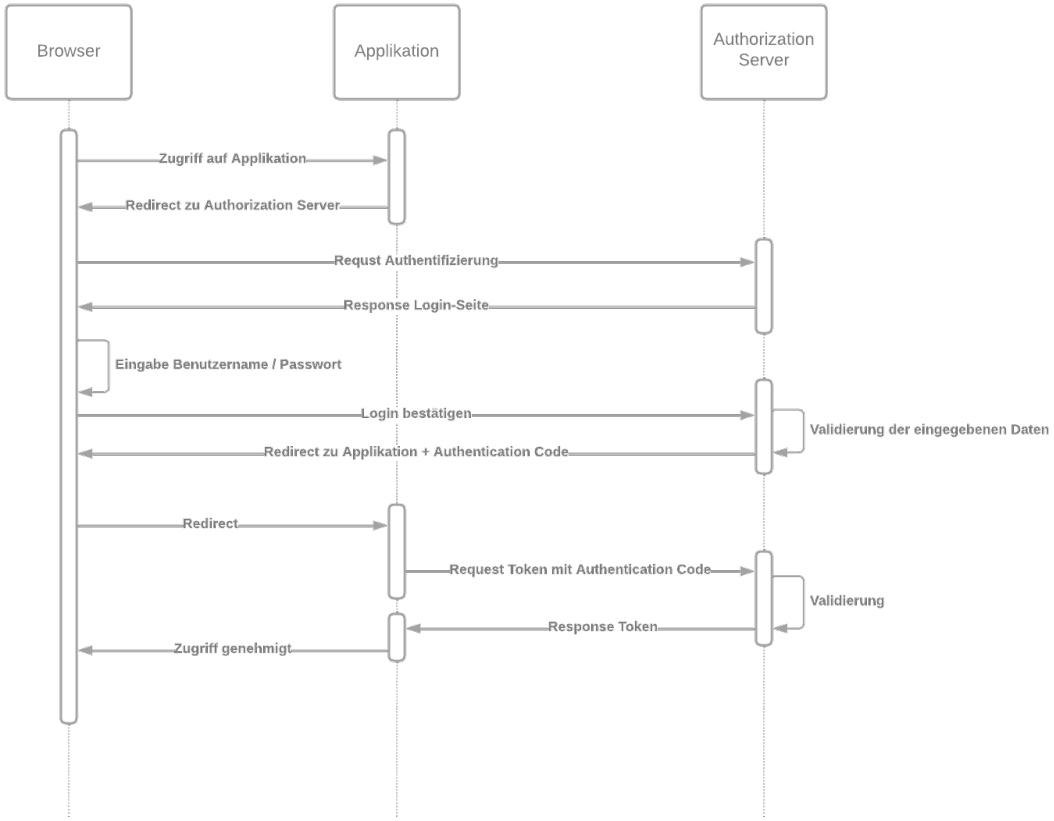

Abbildung 5.2: Visuelle Darstellung einer Authentifizierung mittels Token. Quelle: Eigene Darstellung, 2022

Die Authentifizierung über SSO kann hierbei noch um die Verwendung zusätzlicher Faktoren abgesichert werden. So benötigt eine Identität im Zuge der Authentifizierung neben dem Kennwort einen oder mehrere zusätzliche Faktoren, wie etwa einen zufällig generierten Code oder dem Vorhandensein einer Chip-Karte. MFA wird von vielen gängigen SSO-Frameworks, wie etwa „Redhat Single Sign-On“ unterstützt [26].

Das Thema Access-Management bietet unterschiedliche Ausprägungen mit denen sich der Schutz von Identitäten und IT-Systemen verbessern lässt. PAM ist eine Subdisziplin im Bereich des IAM und eine Methode um privilegierte Aktivitäten auf Ressourcen abzusichern, zu kontrollieren, zu Monitoren und zu Managen. Unter einem privilegierten Account versteht man Accounts, die über besondere Berechtigungen verfügen. Beispiele hierfür sind lokale Administratoren, Service-Accounts, Domänen-Administratoren, privilegierte User-Accounts und C-Level Accounts. Das Ziel von PAM ist eine Risikominimierung, in dem privilegierter Zugriff auf Ressourcen nur dann gewährt wird, wenn die Notwendigkeit dafür besteht. Auf diese Weise wird vermieden, dass privilegierte Accounts während der täglichen Arbeit verwendet werden oder diese von Angreifern ausgenutzt werden können. Letzteres wird dadurch gewährleistet, dass Kennwörter für privilegierte Accounts erst bei Anforderung generiert werden. Abbildung 5.3 zeigt einen

Möglichen Ablauf für den Zugriff auf eine Ressource durch einen Administrator unter der Verwendung von PAM. Es ist zu erkennen, dass der privilegierte Zugriff auf eine Ressource on-demand angefordert und von einem Dritten genehmigt werden muss. Der privilegierte Zugriff wird nach Beendigung des Task oder nach einem zuvor definierten Zeitraum automatisch entfernt. [11]

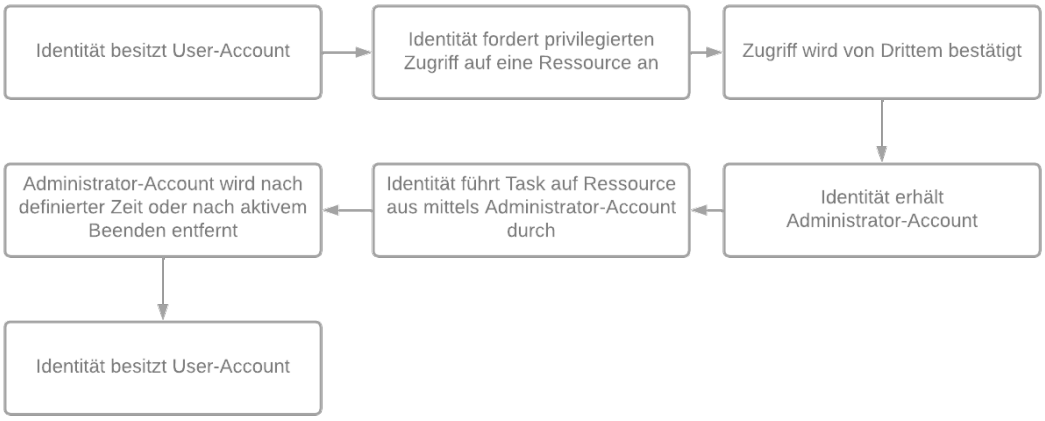

Abbildung 5.3: Visuelle Darstellung des Zugriffs auf eine Ressource mittels PAM. Quelle: Eigene Darstellung, 2022

Mit Hilfe von PAM kann das „Least-Privilege“ Modell, das Prinzip der minimalen Rechtevergabe realisiert werden. Dieses Prinzip wird sowohl von der EBA als auch von der BaFin gefordert. Die Anforderungen sind in der Anforderungsmatrix unter Nummer 41 und Nummer 111 hinterlegt.

Die beiden Best-Practice-Ansätze und die jeweiligen technischen Umsetzungen SSO, MFA, NCD und PAM adressieren die von Darran Rolls und Morey J. Haber beschriebenen Grundpfeiler der Authentifizierung und Autorisierung und decken die von Aufsichtsbehörden gesetzten Anforderungen aus dem Bereich IAM ab.

5.2 Asset-Management

Die Gruppe „Asset-Management“ vereint die Maßnahmen „Content-Management -Database“, „Source-Code-Verwaltung“ und „Baselining und Change-Management“. Die Gruppe beschäftigt sich mit der Dokumentation, Sicherung, Änderung und Bereitstellung von Asset-Daten.

Eine zentrale und konsistente Übersicht über den aktuellen Zustand der gesamten IT-Umgebung ist ein wesentlicher Grundstein für einen reibungslosen Betrieb und die Implementierung und Sicherstellung der IT-Sicherheit im Unternehmen. Aus diesem Grund fordert die EBA, dass Unternehmen eine Übersicht über eigene IT-Assets und IKT-Systeme besitzen und diese Übersicht stets aktuell zu halten haben. Des Weiteren sind Unternehmen verpflichtet ein aktuelles Verzeichnis über die eigenen IKT-Assets

zu führen und deren Verbindungen und Abhängigkeiten zueinander darzustellen. Diese beiden Anforderungen sind in der Anforderungsmatrix unter Nummer 97 und Nummer 136 ersichtlich. Die FMA fordert Abhängigkeiten von IT-Systeme abzubilden, das IT-Inventar zu verwalten und entsprechend zu steuern (Anforderungsmatrix Nummer 275). Die BaFin fordert, dass Unternehmen jederzeit einen aktuellen Überblick über die Bestandteile des festgelegten Informationsverbunds und deren Abhängigkeiten geben können. Außerdem muss die Geschäftsleitung imstande sein Aussagen zu selbst betriebenen IT-Systemen treffen zu können. Die Anforderungen der Bafin sind in der Anforderungsmatrix unter Nummer 5 und Nummer 7 ersichtlich.

Best-Practice-Ansatz: Configuration Management Database

Eine „Configuration Management Database“ (CMBD) ist eine Möglichkeit um den Anforderungen der Aufsichtsbehörden in diesem Bereich nachzukommen. Eine CMDB unterstützt Unternehmen dabei stets einen aktuellen Überblick über alle IT-Systeme, aktuelle Konfigurationen und betriebenen Services zu erhalten. Des Weiteren bildet eine CMDB die Grundlage für unterschiedliche IT-Sicherheitssysteme und nach gelagerte Automatisierungswerkzeuge, die auf Basis der von der CMDB bereit gestellten Daten arbeiten. Eine CMDB aggregiert die Datenbestände unterschiedlicher Systeme, korreliert diese und wertet sie aus.

Für eine optimale Darstellung der IT-Landschaft ist die zugrunde liegende Datenqualität von höchster Priorität. Die benötigten Konfigurationsdaten der einzelnen IT-Systeme manuell zu erheben gestaltet sich mit steigender Komplexität der IT-Infrastruktur unwirtschaftlich bis hin zu unmöglich. Für die Aggregation der Daten können automatische Discovery-Tools unterstützen. Ein Beispiel hierfür sind „Endpoint-Detection and Response Systeme“ (EDR) wie Tanium[1], die auf allen IT-Assets installiert werden. Mit Hilfe von Tanium können Echtzeitdaten der IT-Assets ausgelesen und an die CMDB übermittelt werden. Ein weiterer Vorteil von Tanium besteht darin, dass auch IT-Assets auf denen Tanium nicht installiert werden kann, erkannt werden können. Beispiele hierfür sind Netzwerk-Komponenten oder Appliance-Lösungen. Tanium erkennt und analysiert diese Systeme auf Basis der Verbindungen zu Systemen auf denen Tanium bereits installiert wurde.

Trotz der Verwendung von Tools wie Tanium können physikalische Komponenten in Unternehmen betrieben werden, nicht nicht automatisch erkannt werden können. Hier ist die Einbindung in Prozesse wie dem Change-Management relevant um einen stets aktuellen und konsistenten Datenbestand zu erhalten. Eine CMDB kann neben der technischen Daten eines IT-Assets noch weitere Informationen enthalten. So kann die Beschreibung eines IT-Assets aus folgenden Komponenten bestehen:

- Technische Daten
  - IP-Adresse
  - MAC-Adresse
  - CPU, RAM, ...

[1] https://www.tanium.com

- Geografischer Standort
- Betriebssystem
  - Version
  - Lizenzkey
  - Lizenzvertrag
- Seriennummer
- Inventarnummer
- Servicevertrag
- SLA-Level
- Applikationen
- Sonstige Dokumente

Anhand dieser Informationen lässt sich auf Basis unterschiedlicher Informationsquellen ein Gesamtbild der IT-Infrastruktur erstellen und den Anforderungen von Aufsichtsbehörden nachkommen.

Best-Practice-Ansatz: Everything as Code (EaC)

Auch in Bezug auf die Nachvollziehbarkeit von Änderungen an Assets werden Anforderungen gestellt. Die EBA und die BaFin fordern, dass Organisationen die Integrität der Anwendungen und Systeme angemessen sicherzustellen haben. Des Weiteren müssen Vorkehrungen getroffen werden um versehentliche Änderungen oder absichtliche Manipulationen erkennen zu können. Diese Anforderungen sind in der Anforderungsmatrix unter den Nummern 54 und 125 ersichtlich. Unternehmen sind laut BaFin außerdem dazu verpflichtet, Änderungen an IT-Systemen in geordneter Art und Weise aufzunehmen, zu dokumentieren, zu bewerten, zu genehmigen und zu koordinieren (Anforderungsmatrix Nummer 63). Laut EBA sind Konfigurationsbaselinies für alle Netzwerkkomponenten zu implementieren.

EaC ist eine Technik, in der sämtliche Teile eines Systems als Code behandelt werden. Dieses Prinzip wird bereits verstärkt im Bereich der Softwareentwicklung verwendet, wo sämtlicher Source-Code in Repositories wie etwa Apache-SVN[2] oder Github[3] verwaltet wird, um eine SoT zu definieren. SoT beschreibt ein Konzept, in dem Daten von unterschiedlichen Systemen eines Unternehmens in einem bestimmten Platz aggregiert werden um Datensilos zu vermeiden. So wird sichergestellt, dass Systeme Daten von nur einer Quelle beziehen, welche stets den aktuellen Stand widerspiegelt. Ein „Code-Repository“ (CR) ist der erste Schritt in der Deployment-Pipeline vom Source-Code hin zum fertigen Produkt oder System. Im Zuge des Deployment-Prozesses werden unterschiedliche Schritte, wie etwa automatische Tests oder automatische Freigabeprozesse in der Pipeline durchgeführt. Ein CR bildet somit einen Baustein für die von den Aufsichtsbehörden definierten Anforderungen. [74]

[2] https://subversion.apache.org
[3] https://github.com

Gerade mit der Etablierung der DevOps Bewegung, in der sich die Bereiche „Software-Development“ und „IT-Operations“ zusammenschließen, um einen sicheren, effizienteren und vor allem automatisierten System-Lifecycle zu definieren, nimmt die Vorgehensweise der Behandlung von Komponenten als Code, neben der Softwareentwicklung auch verstärkt Einzug in anderen Bereiche der IT. [8]

Einer dieser Bereiche ist die IT-Infrastruktur, in der sich der Grad der Automation häufig auf wieder ausführbare Skripte oder speziell angepasste Betriebssystem-Images begrenzt. Darüber hinausgehende Konfigurationen werden manuell oder mit Skripten, welche eigens für den jeweiligen Server angepasst werden, durchgeführt. „Infrastructure as Code“ (IaC) übernimmt die Bereitstellung und die Konfiguration der gesamten Infrastruktur im Quellcode und ermöglicht das Schaffen von konsistenten und wiederholbaren Routinen. [82]

Unterschiedliche Anbieter von Container Virtualisierungslösungen, wie etwa Docker[4] oder Redhat-Openshift[5], arbeiten bereits mit einheitlichen Konfigurationen, welche Server oder Applikationen auf Basis von Templates beschreibend definieren, um diese so vom jeweiligen Framework plattformunabhängig provisionieren zu lassen. Weitere wichtige Themen, die eng mit dem Provisioning von Servern oder Applikationen verbunden sind werden häufig separat in anderen Tools behandelt oder gar nicht berücksichtigt. Zu diesen Themen zählen unter anderem das Erstellen von Dokumentationen, dem Berücksichtigen und Auditieren von Berechtigungsfreigaben oder dem Einpflegen und Berücksichtigen von IT- Sicherheitsrichtlinien.

Einen weiteren Bereich, der von der Behandlung von Komponenten als Code profitieren kann, bildet der Compliance-Bereich, die Einhaltung von Governance-Richtlinien. Mit Hilfe von „Policy as Code“ (PaC) wird versucht bei der Überprüfung auf Richtlinien weg von einem manuellen Ansatz der von Menschen durchgeführt wird, hin zu einem konsistenten, effizienten und wiederholbaren Ansatz der Überprüfung von Richtlinien, auf Basis von Code zu kommen. [67]

Der Zusatz „as Code“ weist auf die der jeweiligen Technologie hinzugefügten Attribute Effizienz, Sicherheit, Transparenz und Automatisierung hin und versucht diese Themen ebenso im Zuge des Provisionings zu berücksichtigen. Spricht man von „codification“ bedeutet dies den Erhalt von automatisierten Tests, einer einheitlichen Sprache, welche sowohl von IT-affinen als auch Mitarbeiter aus dem organisatorischem Umfeld verstanden werden kann, und einer automatisierter Deployment-Pipeline, welche sich modular um diverse Komponenten erweitern lässt. Eine Deployment-Pipeline beschreibt den automatisierten Prozess von der Erstellung des Quellcodes bis hin zum Provisioning des fertigen Produkts. Mit Hilfe unterschiedlicher Schritte ermöglicht eine Deployment-Pipeline die automatisierte Ausführung von Arbeitsschritten. Zu diesen Arbeitsschritten zählen unter anderem eine Versionierung des Quellcodes, eine automatisierte Freigabe von Änderungen, die Ausführung von Tests, das Deployment in eine Test-Umgebung und das anschließenden Deployment in die produktive Umgebung. [8]

[4] https://www.docker.com
[5] https://www.openshift.com

Auf Basis der Vorteile der Definition von Komponenten als Code, gliedert sich der Bereich EaC unter anderem in folgende Teilbereiche:

- Infrastructure as Code
- Security as Code
- Policy as Code

Infrastructure as Code
Mit Hilfe von IaC können die Anforderungen der BaFin und der EBA in Bezug auf Änderungen an Assets unter Einbezug eines Genehmigungsprozesses und der Etablierung von Konfigurationsbaselines nachgekommen werden. IaC versucht die Vorteile von EaC bezogen auf Infrastrukturkomponenten zu behandeln und abzudecken. Sämtliche Teile eines Systems, wie etwa die Konfiguration der virtuellen Umgebung, die Konfiguration des Betriebssystems, Einstellungen betreffend installierter Programme oder auch die Dokumentation dieser, werden in Repositories gespeichert. Dies bringt unter anderem folgende Vorteile mit sich [78]:

- Nachvollziehbarkeit
  Änderungen an Systemen können jederzeit detailliert nachvollzogen oder rückgängig gemacht werden. Backups und Restores von Infrastrukturkomponenten sind großteils überflüssig, da die Komponenten ad-hoc neu provisioniert werden können.
- Wiederholbarkeit
  Systeme können jederzeit auf unterschiedliche Plattformen provisioniert werden (Ready for Cloud). Somit bietet IaC die Möglichkeit einer „On Demand Infrastruktur“.
- Testing
  Durch ein Testing Verfahren können Änderungen am System getestet und bei erfolgreichem Test automatisiert in der Produktionsumgebung provisioniert werden.
- Schutz vor Server- und Configuration Drift
  Es existiert nur mehr eine SoT. Änderungen, welche direkt am Zielsystem vorgenommen und somit nicht in der SoT aufzufinden sind, werden automatisch überschrieben. Dies dient zum einen dem Erkennen von unautorisierten Änderungen von Einstellungen am System, zum anderen beugt es Configuration-Drifts vor. Darunter versteht man das Abweichen einer Konfiguration von einem definierten und gewünschten Zustand. Configuration-Drifts können etwa entstehen, wenn unterschiedliche Server von verschiedenen Mitarbeitern erstellt und konfiguriert werden. Obwohl alle Mitarbeiter nach denselben Vorgaben arbeiten, können sich Unterschiede in der Konfiguration ergeben. [73]
- Dokumentation und Geteiltes Wissen
  Sämtliche Komponenten eines Systems werden an einer gesammelten Stelle dokumentiert und sind dort einsehbar. Arbeiten mehrere Personen, oder sogar unterschiedliche Teams, an ein und demselben System, kann das Wissen durch eine einheitliche Definitionssprache leichter vermittelt und die verwalteten Systeme schneller erfasst werden. Auch personellen Ausfällen kann so vorgebeugt werden. Bei Standalone-Lösungen kann es Mitarbeitern ohne einer vorhandenen Dokumentation Probleme bereiten, die ursprüngliche Intention des Erstellers oder manuelle

Änderungen an einem System nachzuvollziehen.

- Freigabe und Audit
  Änderungen am System, ohne vorheriger Freigabe durch das Management, werden technisch unterbunden. Durch die zentrale Speicherung sämtlicher Komponenten eines Systems, werden etwaige Audit-Anfragen und Feedback-Schleifen signifikant beschleunigt.

Der Vollständigkeit halber wird auch noch auf die beiden anderen Teilbereiche von EaC eingegangen. Obwohl die Anwendungsgebiete von „Security as Code“ (SaC) und „Policy as Code“ (PaC) nicht explizit von den Aufsichtsbehörden gefordert sind, tragen sie dennoch stark zu einer sicheren und stabilen IT-Infrastruktur bei.

Security as Code
SaC beschreibt Techniken um Sicherheit bei der Entwicklung mittels einer Deployment-Pipeline zu gewährleisten. Im Zuge des jeweiligen Deployment-Prozesses werden automatisiert Sicherheitsüberprüfungen durchgeführt und nach Schwachstellen gesucht. Folgende Überprüfungen können als Teil einer zusätzlichen Sicherheitsschicht integriert werden [78]:

- Automatische Vulnerarbility-Scans
- Ausführung von Skript-Tests
- Überprüfung auf Default-Konfigurationen
- Implementierung von Monitoring Funktionalitäten

Diese Ansätze bringen unter anderem folgende Vorteile mit sich [78]:

- Schnellere Reaktion auf Änderungen und Sicherheitsanforderungen
- Bessere Zusammenarbeit zwischen den einzelnen Teams
- Vulnerabilities können in einem frühen Stadium erkannt und behoben werden
- Entwicklungskosten können durch das automatisierte und frühzeitige Erkennen von Schwachstellen und Fehlern verringert werden
- Die Möglichkeit für automatisierte Sicherheitsüberprüfungen wird geschaffen

Policy as Code
PaC beschreibt die Möglichkeit Richtlinien in einem Weg zu definieren, dass diese sowohl von Mensch als auch Maschine gelesen, interpretiert und validiert werden können. Das Ziel von PaC ist es organisatorische Richtlinien des Unternehmens automatisch zu implementieren, verifizieren, monitoren und zu reporten. Ein großer Vorteil besteht darin, dass Richtlinien bereits im Zuge des Deployment-Prozesses behandelt werden können. So wird gewährleistet, dass bereits während der Entwicklung frühzeitig und nachvollziehbar auf potentielle Policy-Verletzung reagiert werden kann.
Um PaC zu ermöglichen können die jeweiligen Richtlinien auf Basis von Code abgebildet und in Form von Tests in den Deployment-Prozess integriert werden. Ein weiterer Weg ist, Richtlinien mit der Konfiguration der Deployment-Pipeline durchzusetzen. Auf diesem Weg können etwa unterschiedliche Aktionen oder Abläufe unterbunden werden. PaC baut somit automatisierte Compliance sowohl in der Entwicklung als auch im Betrieb auf. Der Begriff „Policy“ ist in der Literatur nicht klar definiert und umfasst mehrere Bereiche [52]:

- Compliance Policies
  Diese Richtlinien schaffen Compliance unter Einbezug externer Standards wie dem „Payment Card Industry Security Standard“ (PCI-DSS5) oder der „General Data Protection Regulation“ (GDPR6) [27] [28].
- Security Policies
  Diese Richtlinien definieren interne Datenschutz- und Datensicherheits-Vorgaben eines Unternehmens um die Sicherheit und die Integrität von Daten zu schützen. Die Definition von Applikationen, welche vom freien Internet aus erreichbar sind, stellen ein Beispiel für eine Security Policy.
- Operational Excellence
  Diese Art von Policy verhindert Service-Ausfälle oder Service-Verschlechterungen zu Lasten des Unternehmens oder des Kunden. Beispiele hierfür sind die Validierung von neuen Konfigurationseinstellungen oder die Sicherstellung einer redundant ausgelegten Anbindung von Systemen.

Die Definition von Richtlinien mittels PaC bietet unter anderem folgende Vorteile [78]:

- Routineberichte optimieren die Auditierung von Systemen
  Berichte, die während des gesamten DevOps-Lebenszyklus generiert werden liefern Dokumentation und Nachweis, mit deren Hilfe viele internen und behördlichen Prüfungsverfahren nachverfolgt und rationalisiert werden können.
- Compliance Transparenz
- Zeitersparnis
- Kontinuierliche Auditierbarkeit

5.3 Infrastruktur-Betrieb

Die Gruppe „Infrastruktur-Betrieb“ vereint die Maßnahmen „Monitoring“, „Hochverfügbarkeit“, „Backup-Restore“ und „Patch-Management“. Die Gruppe beschäftigt sich mit der Aufrechterhaltung und der Absicherung von IT-Systemen um einen sicheren und stabilen Betrieb zu gewährleisten. Aufsichtsbehörden stellen unterschiedliche Anforderungen an den Betrieb und die Verfügbarkeit von IT-Systemen von Banken. Die BaFin fordert, dass Konzepte zur Hochverfügbarkeit implementiert, angewendet und entsprechend überprüft werden (Anforderungsmatrix Nummer 82). Die EBA fordert, dass Unternehmen Leistungs-. Kapazitätsplanungs- und Kapazitätsüberwachungs-Prozesse einführen um bedeutende Leistungsprobleme von IKT-Systemen und Engpässe bei IKT-Kapazitäten rechtzeitig zu erkennen und darauf reagieren zu können (Anforderungsmatrix Nummer 139). Die FMA setzt des Weiteren voraus, dass die Kontinuität und Ausfallsicherheit der IT-Systeme laufend überprüft und eine rechtzeitige Wiederherstellung von IT-Systemen nach Betriebsausfällen gewährleistet wird (Anforderungsmatrix Nummer 340). Außerdem werden Anforderungen an Update-Prozesse von Systemen gestellt. Die BaFin setzt voraus, dass Unternehmen IT-Systeme regelmäßig aktualisieren und die Stabilität der Systeme im Falle einer Änderung entsprechend testen (Anforderungsmatrix Nummer 61). Im Falle eines Ausfalls oder eines Datenverlustes setzt die EBA voraus, dass Unternehmen Verfahren zur Sicherung und Wiederherstellung von

Daten und IKT-Systemen festlegen und umsetzen, um sicherzustellen, dass diese bei Bedarf wiederhergestellt werden können (Anforderungsmatrix Nummer 140).

Betrachtet man die Anforderungen der Aufsichtsbehörden, ergeben sich zwei Bereiche die von Banken in Österreich adressiert werden müssen [71]:

- Gewährleistung des stabilen Betriebs der IT-Infrastruktur (Ausfallsicherheit)
  - Hochverfügbarkeit
  - Monitoring
  - Patch-Management
- Reaktion auf Ereignisse betreffend IT-Infrastrukturkomponenten (Recovery Management)
  - Backup-Restore

Best-Practice-Ansatz: Ausfallsicherheit

Ist ein System „hochverfügbar“ bedeutet das, dass das System lange Zeit ohne Unterbrechung stabil läuft. Die Verfügbarkeit eines Systems wird in Prozent gemessen. Besitzt ein System eine Verfügbarkeit von 100%, ist keine Ausfallzeit zu erwarten. In der Realität kann eine Verfügbarkeit von 100% nahezu ausgeschlossen werden.

Eine hochverfügbare Infrastruktur charakterisiert sich unter anderem durch folgende Eigenschaften:

- Vermeidung von Single Points of Failure (SPoF)
- Redundanz / Load-Balancing
- Auto-Skalierbarkeit
- Monitoring

SPoFs können in unterschiedlicher Ausprägung bestehen und stellen ein Bottleneck in der Ausfallsicherheit dar. Egal ob es sich bei der Instanz um einen einzelnen Server oder um ein ganzes Rechenzentrum handelt, fällt ein SPoF aus, hat dies Auswirkungen auf alle angebundenen IT-Systeme.

Hardware Redundanz wird erzielt in dem zwei oder mehr Instanzen einer Hardware Komponente bereitgestellt werden. Wird zusätzlich ein Load-Balancer implementiert, kann dieser die Last gleichmäßig auf die redundanten Hardware Komponenten verteilen, Lastspitzen abgefangen und die Systemstabilität gewährleisten. Eine weitere Möglichkeit um Lastspitzen abzufangen und auf steigende Auslastung zu reagieren ist die Skalierung von Systemen. Unter einer Auto-Skalierbarkeit versteht man die Fähigkeit von Systemen sich wachsenden oder schrumpfenden Anforderungen hinsichtlich der Leistungsfähigkeit automatisch anzupassen. Es wird zwischen der vertikalen Skalierung (scale up) und der horizontalen Skalierung (scale out) unterschieden. Bei der vertikalen Skalierung wird Leistung innerhalb des IT-Systems hinzugefügt oder entfernt. Die Leistungssteigerung entsteht somit durch das Hinzufügen zusätzlicher Komponenten wie etwa Speicherplatz, CPUs oder zusätzlicher Grafikkarten. Bei der horizontalen Skalierung wird die Leistungssteigerung eines IT-Systems durch das Hinzufügen zusätzlicher Systeme erbracht.

Die vom IT-System durchzuführenden Arbeiten wird auf unterschiedlichen Instanzen verteilt. So kann gewährleistet werden, dass steigender Workload mit gleichbleibender Performance abgearbeitet werden kann. [64]

Um die Stabilität von IT-Systemen gewährleisten und auf etwaige Störungen oder Lastspitzen entsprechend reagieren zu können, ist eine Überwachung der IT-Infrastruktur unumgänglich.
Bevor eine Überwachung implementiert wird, sollten folgende Punkte geklärt sein [45]:

- Grund für das Monitoring
  Je nach Anwendungsfall kommen unterschiedliche Lösungen für ein Logging und ein Monitoring in Frage. Mögliche Gründe für ein Monitoring sind Compliance-Anforderungen, Gesetzliche Anforderungen oder Incident-Response-Anforderungen.
- Daten, die für das Monitoring benötigt werden
  Für das Monitoring von Finanztransaktionen sind beispielsweise andere Daten sinnvoll und nötig, als für das Monitoring von Netzwerk-Komponenten. Unabhängig vom Anwendungsfall sollten Logeinträge folgende Informationen enthalten:
  - Durchführender (Wer: Accountname oder IP-Adresse)
  - Aktion (Was: Lesen/schreiben auf welcher Ressource)
  - Zeitpunkt (Wann: Timestamp)
  - Lokation (Wo: Geolocation, Browser, Skript-Name, ...)
- Zu überwachende Assets
  Um zu verhindern, dass Logdaten die für das Monitoring nötig sind zu viel Speicherplatz in Anspruch nehmen, sollte im Vorfeld geklärt werden welche Assets zu überwachen sind. Basierend auf den jeweiligen Assets ist zu definieren, welche Software-Komponente überwacht werden soll und welcher Daten-Klassifizierung die gesammelten Daten entsprechen.
- Sicherheitsaspekt betrachten
  Basierend auf der Daten-Klassifizierung sind entsprechende Sicherheitsvorkehrungen zu treffen. Personenbezogene Daten sollten maskiert oder anonymisiert werden. Die Übertragung von Log-Daten sollte verschlüsselt stattfinden und der Zugriff auf den Zustand eines Systems oder einer Applikation einem rollenbasierten Berechtigungskonzept unterliegen.
- Automatisierung und Standardisierung
  Soweit möglich sollte ein Monitoring automatisiert stattfinden und das System im Fehlerfall automatisch die zuständige Person benachrichtigen. Um Monitoring-Alarme weiterverarbeiten zu können, sollten diese in einem standardisierten Format, etwa im Format „JSON“ übergeben werden [29].

Dies Überwachung von IT-Systemen kann mit unterschiedlichen Software-Produkten umgesetzt werden. Die Implementierung einer Monitoring-Software gestaltet sich vergleichsweise einfach. Eine viel größere Herausforderung bietet die Frage, welche Daten im speziellen betrachtet werden müssen um die Instabilität oder Auslastung von IT-Systemen zu erkennen. Um den Gesundheitsstatus eines Systems zu messen werden unterschiedliche Metriken definiert und auf den Systemen gemessen. Unter einer Metrik wird ein Datensatz verstanden, der die Performance und Verfügbarkeit von Ressourcen

widerspiegelt. Mit Hilfe von Metriken kann der Status eines Systems zu einer bestimmten Zeit gemessen und entsprechend interpretiert werden. [64]

Datadog[6], ein Betreiber von Software-as-a-Service Monitoring Diensten teilt Metriken in die zwei Kategorien „Work-Metrics“ (WM) und „Ressource-Metrics“ (RM). WM geben den Top-Level Status eines IT-Systems an, in dem die Leistung des Systems, bezogen auf die durchzuführende Tätigkeit gemessen wird.

WM lassen sich in vier Typen einteilen [83]:

- Throughput
  Gibt die Menge an Tasks an, die das System pro Zeiteinheit absolviert.
- Success
  Repräsentiert die Anzahl erfolgreich durchgeführter Tasks in Prozent.
- Error
  Repräsentiert die Anzahl an Fehlern, die ein System während der Durchführung von Tasks produziert.
- Performance
  Gibt die Effizienz des Systems im Zuge der Durchführung von Tasks an.

WM können dabei unterstützen eine generelle Aussage zum Status und der Performance eines Systems zu treffen. So können WM beispielsweise Antwort auf folgende Fragen liefern:

- Ist das System aktiv?
- Wie gut performed das System?
- Wie ist die Qualität der durchgeführten Tasks?

Tabelle 5.1 zeigt ein Beispiel für mögliche WM eines Webservers bezogen auf die Anzahl von Requests und die Qualität der Reponses.
So werden im Schnitt 32 Requests pro Sekunde mit einer durchschnittlichen Antwort-Zeit von 0.4 Sekunden vom Webserver abgearbeitet. 99.1% der Requests sind erfolgreich, 0.1% der Requests bewirken einen Fehler vom Typ 5xx auf Serverseite.

Tabelle 5.1: Beispiel für Work-Metrics: Webserver, Quelle Le-Quoc [83], 2022

Type	Beschreibung	Wert
Throughput	Requests pro Sekunde	32
Success	Prozentualer Anteil von Web-Responses vom Typ 2xx seit der letzten Messung	99.1
Error	Prozentualer Anteil von Web-Responses vom Typ 5xx seit der letzten Messung	0.1
Performance	Durchschnittliche Response-Zeit in Sekunden	0.4

Im Gegensatz zu WM liefern RM keine Auskunft über den Status der durchgeführten Tasks, sondern über den Status des überwachten Systems selbst. Am Beispiel des genannten Webservers sind etwa Ressourcen wie die Auslastung der CPU, des Arbeitsspeichers, der Festplatte und des Netzwerk-Interfaces relevant um den Status des Systems zu beschreiben.

[6] https://www.datadoghq.com

Für jede zu überwachende Ressource des Systems sind folgende vier Werte relevant [83]:

- Utilization
  Repräsentiert die anteilsmäßige Auslastung der Ressource in Prozent.
- Saturation
  Gibt die Anzahl an anstehenden Tasks an, die zum Messzeitpunkt noch nicht abgearbeitet wurden (Anzahl Elemente in Queue).
- Errors
  Repräsentiert die Anzahl an Fehlern, welche die Ressource während der Durchführung eines Tasks produziert.
- Availability
  Gibt die Zeit an in der die Ressource tatsächlich Tasks abgearbeitet hat.

Tabelle 5.2 zeigt ein Beispiel für mögliche RM unterschiedlicher Komponenten eines Webservers.

Tabelle 5.2: Beispiel für Ressource-Metrics: Webserver, Quelle Le-Quoc [83], 2022

Ressource	Utilization	Saturation	Errors	Availability
Disk Input/Output	Gesamtauslastung in %	Länge der Queue	<#Error>	Verfügbare Zeit in %
Speicher	Gesamtauslastung in %	Größe der Auslagerung	<#Error>	N/A
Webservice	Mittlere Antwortzeit pro Request in %	#Elemente in Queue	<#Error>	Verfügbare Zeit in %
Datenbank	Mittlere Antwortzeit pro Request in %	#Elemente in Queue	<#Error>	Verfügbare Zeit in %

Neben Metriken bestehen noch weitere Indikatoren für den Zustand eines IT-Systems. Monitoringlösungen können „Events“ auf Basis von Vorkommnissen am IT-System entgegennehmen und unterschiedliche Aktionen durchführen. Beispiele für Events sind „Alarme“ die von Applikationen am IT-System oder vom IT-System selbst abgegeben werden oder „Scaling-Events“ die Hinweis auf eine durchgeführte Skalierung des Systems geben.

Neben dem Monitoring von IT-Systemen besteht noch ein weiterer Aspekt, der zur Stabilität und damit zur Ausfallsicherheit von IT-Systemen beiträgt. Unter „Patch-Management“ wird die Identifizierung von Systemfunktionen verstanden, die verbessert oder korrigiert werden müssen. Patches, Hotfixes oder Mitigations, einem Weg zur Minderung des bestehenden Problems, werden meist vom Hersteller zur Verfügung gestellt. Es handelt sich dabei um neue oder aktualisierte Codezeilen, die das Verhalten von Software-Anwendungen oder Hardware-Systemen beeinflussen. Sie werden veröffentlicht um Fehler im bestehenden Code zu beheben oder neue Features hinzuzufügen. Der Vorteil in der Verteilung von Patches besteht darin, dass sie meist nur bestimmte Features adressieren und somit nicht bei jeder Änderung am IT-System ein neues Software-Release veröffentlicht werden muss. Patch-Management steht in direktem Zusammenhang mit dem „Vulnerability-Management“, das in Kapitel 5.5 beschrieben wird. Oft erfolgt die Veröffentlichung eines Patches auf Basis von gefundenen Vulnerabilities in IT-Systemen. [86]

Da IT-Umgebungen in Unternehmen meist eine Vielzahl von Systemen enthalten, die von unterschiedlichen Teams betreut werden, erweist sich ein Patching ohne Plan als

ineffizient. Patch-Management-Tools geben eine Übersicht über den aktuellen Patch-Stand von Systemen und helfen bei der Identifizierung von nötigen, durchzuführenden Patches. Unabhängig davon wie Patches in den IT-Systemen eingespielt werden, sollten folgende Punkte beachtet werden [86]:

- Identifikation von Systemen
  Ein funktionierendes Patch-Management erfordert eine regelmäßige Identifikation von Systemen, die nicht konform, fehleranfällig oder nicht gepatched sind.
- Evaluierung / Bewertung des Patches
  Im Zuge der Evaluierung des Patches sollte eine Einschätzung auf etwaige negative Auswirkungen durchgeführt werden. Es ist zu klären, ob die Behebung der potentiellen Sicherheitslücke über einem möglichen Ausfall beziehungsweise Stillstand des Systems steht.
- Etablierung von Patch-Zyklen
  Die Bereitstellung von Patches durch Hersteller erfolgt im Regelfall in fest abgestimmten Zeitabständen. Diese Zyklen sollten im Betrieb übernommen werden um ein Überschneiden von Patches zu vermeiden.
- Verteilung und Reporting
  Für ein funktionierendes Patch-Management werden die Patches mit Hilfe einer zentralen Plattform im gesamten Unternehmen verteilt, installiert und überwacht. Eine erfolgreiche Installation eines Patches kann auf Basis von Reports überprüft und fehlerhafte Patches erneut verteilt werden.

Best-Practice-Ansatz: Recovery-Management

Trotz der Tatsache, dass IT-Systeme ausfallsicher gestaltet werden können, besteht immer ein Restrisiko für Datenverlust. Aus diesem Grund sind Sicherungen von relevanten IT-Systemen, Datenbanken und Komponenten unumgänglich. Auch eine ausfallsicheres IT-System kann beispielsweise Opfer einer Ransomware-Attacke werden die zur Folge hat, dass sämtliche auf dem IT-System befindlichen Daten unbrauchbar werden. Doch nicht nur böswillige Angriffe sondern auch versehentliches Löschen oder ein Hardware-Defekt können zu Datenverlust führen. Bei einem Systemausfall mit Datenverlust sind alle Daten seit der letzten Sicherung verloren. Aus diesem Grund ist es wichtig die für das Unternehmen und das IT-System korrekte Backup-Strategie zu wählen, welche den Datenverlust im Rahmen der technischen Möglichkeiten und des verfügbaren Speicherplatzes so gering wie möglich hält.

Bei der Datensicherung wird zwischen folgenden Strategien unterschieden [2]:

- Voll-Backup
  Bei dieser Backup-Strategie wird stets der gesamte Stand des IT-Systems auf ein entsprechendes Medium gesichert. Das Backup hat aus diesem Grund die selbe Größe wie die Originaldaten, allerdings können die Daten im Zuge des Backups komprimiert werden. Der Vorteil besteht darin, dass immer eine 1:1 Kopie der produktiven Daten besteht. Die Nachteile sind der benötigte Speicherplatz und der benötigte Zeitaufwand im Zuge des Backups und des Restores.
- Inkrementelles-Backup
  Das Inkrementelle-Backup setzt ein Vollbackup voraus, ergänzt dieses aber um

nützliche Funktionen. Bei einer inkrementellen Sicherung werden nur jede Daten gesichert, die sich seit der letzten Sicherung verändert haben oder hinzugefügt wurden. Ein großer Vorteil von inkrementellen Backups ist, dass die einzelnen Backup-Stände weniger Speicherplatz in Anspruch nehmen und sich die Inkremente effizient erzeugen lassen. Aufgrund dieser Tatsache ist es möglich, die Inkremente in kurzen Zeitabständen zu sichern und die Datenmenge bei einem Datenverlust klein zu halten. Im Zuge eines Restores werden erst das Voll-Backup und dann die einzelnen Inkremente der Reihe nach eingespielt. Dies resultiert in einer längeren Restore-Zeit als beim Voll-Backup.

- Differenzielles-Backup
  Auch das differenzielle Backup benötigt als Grundlage ein Voll-Backup. Im Unterschied zu einem inkrementellen Backup werden beim Restore eines differenziellen Backup nur das Voll-Backup und das letzte differenzielle Backup eingespielt. Das differenzielle Backup enthält alle Änderungen seit dem letzten Voll-Backup und kann daher, je nach Backup-Zyklus, auch das Voll-Backup in der Größe übertreffen.

5.4 Netzwerk-Management

Die Gruppe „Netzwerk-Management“ vereint die Maßnahmen „Netzwerk-Segmentierung“, „Kryptografie“, „Firewalls“ und das Thema „Network-Access Control“ (NAC). Die Gruppe beschäftigt sich mit den von Aufsichtsbehörden geforderten Maßnahmen zur Definition, Gestaltung und Absicherung von IT-Netzwerken in Banken.

Sowohl die BaFin als auch die EBA und die FMA fordern von Banken die Implementierung einer Netzwerksegmentierung und die Verschlüsselung des Netzverkehrs entsprechend Datenklassifizierung. Diese Anforderungen sind in der Anforderungsmatrix unter den Nummern 32, 35, 123, 218, 221, 259 und 320 ersichtlich.

Best-Practice-Ansatz: Netzwerksegmentierung

Unter einer Netzwerksegmentierung versteht man die Aufteilung vernetzter Komponenten innerhalb eines physischen Netzwerks in unterschiedliche Subnetze. Diese Aufteilung kann entweder auf Basis von physisch getrennter Netzwerken realisiert oder mittels „Virtual Local Area Networks“ (VLANs) umgesetzt werden. Mit Hilfe von VLANs können IT-Systeme aus unterschiedlichen physikalischen Netzwerken zusammengeschlossen werden und miteinander kommunizieren. Ahmed [1] erklärt die Funktionsweise von VLANs am Beispiel eines Sales-Department, das auf zwei Stockwerke im Unternehmen aufgeteilt ist. Anstatt alle Mitarbeiter des Sales-Departments auf dem selben Stockwerk unterzubringen, können VLANs definiert werden, um die Zusammenarbeit der Sales-Mitarbeiter zu gewährleisten. Abbildung 5.4 veranschaulicht das Beispiel.

Abbildung 5.4: Visuelle Darstellung der Aufteilung des Sales-Department, verbunden mittels VLAN. Quelle: Ahmed [1]

VLANs können mittels „Managed-Switches“ auf Basis von Port-Zuweisung oder „Tagging“ realisiert werden. Bei Managed-Switches handelt es sich um Switches mit erweiterter Konfigurationsmöglichkeit wie etwa der gezielte Vergabe von IP-Adressen oder dem Filtering von MAC-Adressen [75]. Beim portbasierten VLAN wird jedem VLAN ein spezifischer Port auf einem Switch zugewiesen, was in einem statischen VLAN resultiert. Im Gegensatz dazu wird beim tagged VLAN die Zuweisung dynamisch durchgeführt. Die Zuweisung zu einem VLAN erfolgt über eine Markierung (Tag) im Frame des Nachrichtenpakets. Auf Basis des Tags kann ein Switch erkennen in welchem Segment die Kommunikation stattfindet und das Paket entsprechend weiterleiten. Jedes VLAN besitzt seine eigene Broadcast-Domäne. [91]

Die Verwendung von VLANs bringt unterschiedliche Vorteile mit sich [91]:

- Flexibilität
  Änderungen an Teilnehmern des LANs können on-demand realisiert werden.
- Performance
  Durch die Reduzierung der Broadcast-Domäne wird unnötiger Traffic vermieden und die Bandbreite minimiert.
- Kostenersparnis
  Die Verwendung von VLANs ersetzt die Installation von parallelen physischen Netzen.

Der größte Vorteil liegt allerdings am Sicherheitsgewinn, wenn große Netzwerke in kleine Gruppen segmentiert werden um damit den Zugang zu beschränken. Netzwerke können so auf Basis von VLANs nach belieben strukturiert und segmentiert werden. Nur Komponenten, die sich im selben VLAN befinden, können miteinander kommunizieren, ohne an Routern oder Firewalls vorbei zu müssen. Eine Kommunikation über Netzsegemente hinweg unterliegt der Kontrolle von Firewalls. [91]

Firewalls kontrollieren eingehende und ausgehende Datenpakete und regulieren den Zugriff auf Komponenten innerhalb eines Netzwerksegments auf Basis von definierten Regeln. Es wird zwischen „Packet-Filtering“, „Stateful Packet-Filtering“ und „Deep Packet-Inspection“ unterschieden. In der einfachsten Ausführung überprüft eine Fire-

wall ein- und ausgehende Datenpakete und entscheidet auf Basis von Regeln ob die Pakete die Firewall passieren dürfen. Stateful Packet-Filtering ist eine Weiterentwicklung dieser Überprüfung und bieten ein dynamisches Paketfiltering. So kann beispielsweise der gesamten Datenverkehr blockiert werden, wenn es sich nicht Responses zu ausgehenden Requests handelt. Deep Packet-Inspection bietet eine weitere Ausbaustufe und erlaubt der Firewall den Inhalt von Paketen zu analysieren und entsprechend auf diese Inhalte zu reagieren. [1]

Mit Hilfe von VLANs und Firewalls lassen sich Unternehmens-Netzwerke in unterschiedliche Zonen unterteilen. Die Unterteilung kann auf Basis unterschiedlicher Ansätze erfolgen [76]:

- Trennung auf Basis pauschaler Sicherheitszonen
- Trennung nach Funktion oder Schutzbedarf
- Trennung nach Gerätetyp
- Trennung nach Entwicklungs- und Produktionsumgebung

Bei der Trennung auf Basis pauschaler Sicherheitszonen erfolgt eine erste grobe Segmentierung des Netzwerks. Mögliche Ausprägungen sind hierbei die Trennung in „Vertrauenswürdige Zonen“, „Demilitarisierte Zonen (DMZ)“ und „Management-Zonen“. In vertrauenswürdigen Zonen befinden sich ausschließliche IT-Systeme mit bekannter Konfiguration und bekanntem Gesundheitsstatus. DMZ sind Zonen die den Austausch mit dem Interner in kontrolliert Art und Weise sicherstellen. IT-Komponenten innerhalb von DMZ exponieren sich im Internet. Auf diese Weise können Dienste wie E-Mail, Collaboration-Tools für Externe oder Webserver für Webseiten betrieben und aus dem Internet zugänglich gemacht werden. In der Regel werden DMZ zusätzlich über Perimeter-Firewalls, die den Zugriff auf nötige IP-Adressen und Ports beschränken, nach außen hin geschützt. Managed-Zonen sind Bereiche die ausschließlich Systeme zur Bereitstellung und Verwaltung der IT-Infrastruktur beheimaten. Ein Beispiel hierfür wäre ein zentraler Active-Directory Server [68].

Zusätzlich zu den pauschalen Sicherheitszonen können IT-Komponenten nach Geräteart oder auszuführender Funktion etabliert werden. So bietet sich eigene Segmente für Clients, Server oder etwa IP-Telefone an. Auf Basis der Trennung nach Funktion können zusätzliche Sicherheitsmechanismen, wie beispielsweise NAC etabliert werden. Mittels NAC kann einem Client zum Beispiel der Zugang zum Client-Segment verwehrt werden, wenn der Client nicht bestimmten Anforderungen entspricht. Mit Hilfe von NAC ist es somit möglich Clients mit einem veralteten Virenschutz automatisch in ein Quarantänenetz zu stellen.

NAC bietet des Weiteren folgende Funktionen [89]:

- Lokalisierung und Identifizierung neuer Geräte im Netzwerk
- Authentifizierung der Geräte
- Zuweisung von Rollen und Berechtigungen
- Prüfung der Einhaltung festgelegter Sicherheitsrichtlinien
- Quarantäne-Zuweisung nicht-konformer Geräte
- Überwachung des Verhaltens der Endgeräte im Netzwerksegment

Sowohl bei der Realisierung von Netzwerksegmentierung als auch bei Verwendung von NAC ist der Schutz von Vertraulichkeit und damit einhergehend die Absicherung der übertragenen Daten und des Netzwerkverkehrs unerlässlich. Diese Tatsache wird auch von Aufsichtsbehörden erkannt. Die EBA fordert, dass beim Austausch sensibler Zahlungsdaten über das Internet eine sichere Ende-zu-Ende-Verschlüsselung zwischen den kommunizierenden Parteien eingesetzt wird (Anforderungsmatrix Nummer 218). Zu diesem Zweck soll eine starke und weithin anerkannte Verschlüsselungstechnik verwendet werden. Auch die ESMA fordert, dass Daten bei der Übertragung verschlüsselt sein müssen (Anforderungsmatrix Nummer 415). Gerade für Banken ist die sichere Übertragung von Daten, nicht nur im Bereich des Online-Banking, unumgänglich um vertrauenswürdige Daten wie Passwörter oder Kreditkarten-Informationen zu schützen. Der vorherrschende Ansatz für die Verschlüsselung von Daten auf Transportebene ist die Verwendung von „Transport Layer Security (TLS)“ beziehungsweise „Secure Socket Layer (SSL)“. [12]

Best-Practice-Ansatz: Verschlüsselung mittels SSL/TLS

Kryptographie unterstützt bei der Wahrung der drei Sicherheitsziele „Vertraulichkeit“, „Integrität“ und „Authentizität“. Schwenk [12] beschreibt die Erreichung der Sicherheitsziele durch Kryptografie wie folgt:

- Vertraulichkeit
  Mit Hilfe von Verschlüsselungsalgorithmen ist es möglich, die Vertraulichkeit von Daten zu bewahren, damit nur die Besitzer eines bestimmten kryptographischen Schlüssels diese lesen können.
- Integrität
  Mit Hilfe eines gültigen „Message Authentication Code“ (MAC) kann sichergestellt werden, dass Daten nicht verändert wurden [87].
- Authentizität
  Die mit einer gültigen digitalen Signatur gesicherten Nachrichten können nur von der Person stammen, die den erforderlichen Schlüssel besitzt. Auf diesem Weg kann die Authentizität eines Teilnehmers gewährleistet werden.

Um die Sicherheitsziele zu gewährleisten besteht die Grundidee von SSL/TLS darin, einen verschlüsselten, transparenten und authentifizierten Kanal zur Verfügung zu stellen, über den Daten zwischen zwei Systemen zuverlässig übertragen werden können.

SSL in den Versionen 1.0 und 2.0 wurde 1994 von der Firma „Netscape[7]“, zur Absicherung der Kommunikation über den Webbrowser „Netscape Navigator“, entwickelt. Aufgrund einiger Schwächen in Version 2.0 wurde die weitere Verwendung durch „RFC 6176“ verboten [30]. SSL 3.0 wurde im Jahr 1996 veröffentlicht aufgrund einer Sicherheitslücke und des daraus resultierenden „POODLE-Angriffs“ 2015 mittels „RFC 7568“ verboten [31] [32]. Im Jahr 1999 wurde SSL 3.1, als Upgrade auf SSL 3.0, unter der Bezeichnung TLS 1.0 veröffentlicht. TLS 1.0 wurde im Laufe der folgenden Jahre weiterentwickelt und neue Versionen im Jahr 2008 (TLS 1.2) und im Jahr 2018 (TLS 1.3)

[7] https://isp.netscape.com

veröffentlicht. TLS 1.3 brachte große Änderungen, wie einen schnelleren Austausch von Nutzdaten und einem verkürzten Handshake mit sich. [12]

Folgende Funktionen werden von SSL/TLS angeboten [10]:

- Authentifikation von Server und Client auf Basis der Verwendung von Verschlüsselungsverfahren und elektronischen Zertifikaten.
- Vertrauliche Client-to-Server Datenübertragung unter Verwendung eines gemeinsamen Sitzungsschlüssel.
- Sicherstellung der Integrität der transportierten Daten unter Verwendung des HMAC-Verfahrens [33].
- Komprimierung von Daten

Eine SSL/TLS-Implementierung besteht auf Client- und Serverseite aus unterschiedlichen Komponenten [12]:

- Record-Layer
  Dieser bildet die grundlegende Komponente über die ein sicherer Kanal realisiert wird. Der Record-Layer empfängt einen Bytestrom, den er in „Records“ aufteilt. Diese werden einzeln verschlüsselt, authentifiziert und mittels einer Sequenznummer miteinander verknüpft.
- Handshake-Protokoll
  Mit Hilfe dieses Protokolls werden kryptographische Algorithmen und Schlüssel zwischen Client und Server ausgehandelt. Die Nachrichten des Handshake-Protokolls werden über den Record-Layer sowohl verschlüsselt als auch unverschlüsselt übertragen.
- Change-Cipher
  „Change-CipherSpec-Nachrichten“ signalisieren dem Record Layer den Wechsel vom unverschlüsselten in den verschlüsselten Modus.
- Alert-Protokoll
  Über das Alert-Protokoll werden Fehlermeldungen zwischen Client und Server ausgetauscht.

Der TLS-Handshake, in dem der Schlüsselaustausch zwischen Client und Server stattfindet, bildet das Herzstück von TLS. Mit Hilfe des Schlüsselaustausches ist es den beteiligten IT-Systemen möglich verschlüsselt zu kommunizieren. Der TLS-Handshake baut nach „RFC 5246“ auf der „Diffie-Hellman-Schlüsselvereinbarung“ oder dem „RSA-basierten Schlüsseltransport“ auf [34] [35].

Der Schlüsselaustausch wird durch die beiden Nachrichten „Certificate“ und „ClientKeyExchange“ im Zuge des TLS-Handshake realisiert. Hierbei sendet der Server seinen öffentlichen RSA-Schlüssel mit einem X.509-Zertifikat, in der „Certificate“-Nachricht an den Client [36]. Der Client verschlüsselt daraufhin einen zufällig generierten 46-Byte-Wert zusammen mit der vom Client höchstmöglich unterstützten TLS-Version. Diese beiden Informationen bilden zusammen das „Premaster Secret“. Daraufhin verschlüsselt der Server das Premaster Secret mit dem öffentlichen Schlüssel des Servers und dem RSA-PKCS-Algorithmus und sendet den daraus resultierenden Chiffretext in der „ClientKeyExchange“-Nachricht zum Server [37]. Der Server wiederum kann den

Chiffretext mit seinem privaten Schlüssel entschlüsseln [38]. Dieser Austausch wird von anderen beteiligten Nachrichten, wie in Abbildung 5.5 ersichtlich, begleitet. [12]

Der weitere Ablauf gestaltet sich wie folgt [12]:

- ClientHello
  Im Zuge der ClientHello-Nachricht werden die höchstmöglich unterstützte TLS-Version, eine Zufallszahl und eine Liste von möglichen kryptographischen Verfahren übergeben.
- ServerHello, Certificate, ServerHelloDone
  Nach Erhalt der ClientHello-Nachricht antwortet der Server mit einer Folge von Nachrichten (Entscheidung über gewähltes kryptographisches Verfahren, öffentlicher Schlüssel in Form eines X.509-Zertifikats) und schließt den Schritt mit ServerHelloDone ab.
- ClientKeyExchange
  Der Client generiert einen zufällig Wert (PremasterSecret), verschlüsselt diesen mit dem öffentlichen Schlüssel des Servers und sendet diese Informationen an den Server.
- ChangeCipherSpec, Finished
  Der Server leitet aus dem PremasterSecret das MasterSecret ab, das als Ausgangspunkt für die Berechnung der kryptographischen Schlüssel dient. Nach Ableitung der Schlüssel kann der Client die vereinbarten Algorithmen aktivieren und den Handshake mittels ClientKeyExchange beenden. Der Server entschlüsselt die Nachricht ClientKeyExchange und leitet ebenfalls die Ableitung der Schlüssel durch. Im Anschluss daran aktiviert der Server die vereinbarten Algorithmen und beendet den Handshake mit der Nachricht ServerFinished.

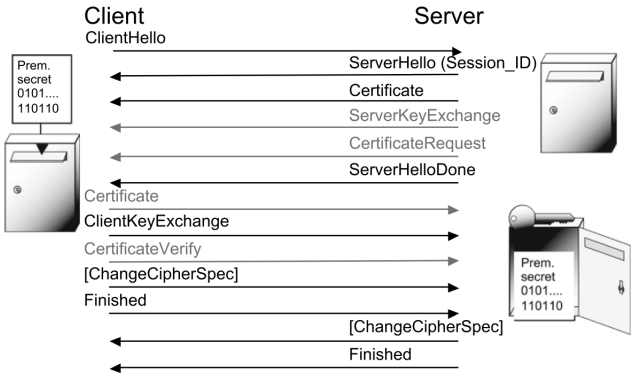

Abbildung 5.5: Schematische Darstellung eines TLS-Handshake mit RSA-basiertem Schlüsselaustausch. Quelle: Schwenk [12]

Nach erfolgreichem Handshake sind dem Server und dem Client untereinander jeweils folgende Informationen bekannt [12]:

- Die höchste vom Server und Client unterstützte TLS-Versionsnummer.
- Eine Ciphersuite mit einem Public-Key-Algorithmus zur Aushandlung des Premaster Secrets.

- Das definierte Master-Secret.
- Eine Session-ID.
- Der Verschlüsselungsschlüssel für den Datenverkehr zwischen Client und Server.
- Ein Schlüssel zur Generierung des MAC von Nachrichten für beide Übertragungsrichtungen.

SSL/TLS wird von einer Vielzahl von Anwendungsprotokollen unterstützt und trägt somit zum Schutz der übertragenen Daten bei. Mit Hilfe von SSL/TLS kann beispielsweise eine verschlüsselte und integritätsgesicherte Verbindung für die Protokolle „HTTP“, „SMTP“, „IMAP“, „FTP“ und „Telnet“ realisiert und so den Anforderungen von Aufsichtsbehörden nachgekommen werden. [10]

5.5 Cybersecurity-Management

Die Gruppe „Cyersecurity-Management“ vereint die Maßnahmen „Security Incident Event Monitoring“ (SIEM), „Log-Management“, „Vulnerability-Management“, „Penetration-Testing“ und „Endpoint-Detection and Response“. Die Gruppe beschäftigt sich mit der Erkennung von Angriffen auf IT-Systeme und dem aktiven Schutz dieser Komponenten.

Der Bereich „Cybersecurity“ deckt einen breiten Bereich an Bedrohungen und Maßnahmen ab, dem sich Banken in Österreich stellen müssen. Aufgrund der Relevanz stellen Aufsichtsbehörden unterschiedliche Anforderungen an die Cybersecurity von Banken. Die BaFin, die EBA und die FMA setzen voraus, dass Systeme für die automatische Erkennung von Anomalien und sicherheitsrelevanten Ereignissen eingeführt werden. Des Weiteren wird erwartet, dass sich Unternehmen ständig über laufende Bedrohungen und Schwachstellen des eigenen Informationsverbundes informieren, deren Relevanz prüfen und entsprechende Maßnahmen ergreifen. Aus diesem Grund haben Unternehmen ein Schwachstellenmanagement zur Erkennung, Bewertung und Behandlung von Schwachstellen zu implementieren (Anforderungsmatrix Nummer 19 und Nummer 31). Die FMA fordert des Weiteren, dass Unternehmen Maßnahmen zur Schwachstellenbeseitigung umsetzen. Unternehmen haben die Wirksamkeit der umgesetzten Maßnahmen laufend zu Überprüfung. Dies kann mittels Penetrationstests oder der Kontrolle von Logdaten durchgeführt werden (Anforderungsmatrix Nummer 265).

Best-Practice-Ansatz: Aufbau Datenbasis - zentrales Logmanagement

Ein erfolgreiches Cybersecurity-Management erfordert Kenntnisse über relevante Prozesse und Ereignisse innerhalb der IT-Struktur. Ein zur Verfügung stehendes Mittel, um Bedrohungen und Schwachstellen zu Identifizieren sind Logeinträge der im Netzwerk betriebenen IT-Systeme. Eine zentrale Forderung aus dem Bereich Cybersecurity der FMA an Unternehmen, ist die regelmäßige Erfassung und Auswertung von Logdaten der im Unternehmen verwendeten IT-Systeme (Anforderungsmatrix Nummer 261). Ein zentrales Logmanagement stellt geeignete Funktionen zur Übertragung, Speicherung, Analyse und Löschung von Logdaten zur Verfügung.

In folgendem Kapitel werden die grundlegenden Bestandteile eines zentralen Logmanagements erörtert und eine mögliche Implementierung, anhand des „Elastic-Stacks“ (ELK-Stack), vorgestellt. „ELK“ ist ein Akronym der im Framework enthaltenen Komponenten „Elastic“, „Logstash“ und „Kibana“ [39].

Für die Realisierung eines zentralen Logmanagements sind vorab unterschiedliche Überlegungen nötig:

- Welche Systeme sollen angebunden werden?
  Basierend auf den Betriebssystemen der jeweiligen Komponenten werden Programme zur Interpretation und Weiterleitung von Logeinträgen benötigt.
- Welche Logdaten sollen übertragen werden?
  Werden sämtliche Logdaten eines Systems oder nur die Logdaten von bestimmten auf den Systemen betriebenen Applikationen benötigt?
- Wie lange sollen die Logdaten im zentralen Logmanagement gespeichert werden?
  Die Speicherung und Analyse von großen Mengen an Logdaten kann in einer erheblichen finanzielle Belastung resultieren.

Auf Basis der genannten Überlegungen kommen unterschiedliche Komponenten für die Implementierung zum Einsatz. Am Beginn der Logmanagement-Pipeline stehen die einzelnen IT-Systeme, deren Logdaten gesammelt werden sollen. Abhängig vom Betriebssystem können die Logdaten beispielsweise mittels RSyslog[8], für UNIX-Systeme, oder dem „Windows-Event-Collector“ (WEC), für Windows Systeme, übertragen werden [40]. Die Logdaten werden in weiterer Folge an einen zentralen Logkollektor weitergeleitet. Für die Konstellation aus UNIX- und Windows-Systemen bietet sich Syslog-NG[9] an, da dieser mit unterschiedlichen Betriebssystemen und Anwendungen kompatibel ist. Die Logdaten werden von Syslog-NG entgegengenommen und auf Basis der Quellen zwischengespeichert. Mittels einer Analysesoftware für Logdaten, wie beispielsweise „Filebeat“, Bestandteil des ELK-Stacks, werden die von Syslog-NG empfangenen Logeinträge in weiterer Folge ausgelesen und weiterbearbeitet. Im Anschluss daran werden die Logdaten mittels Logstash geparsed, gefiltert, normalisiert und an Elasticsearch weitergeleitet. Elasticsearch dient der Speicherung, Indexierung, Suche und Analyse von Logeinträgen. Mittels der Weboberfläche Kibana können die gespeicherten Logdaten grafisch dargestellt werden. Abbildung 5.6 zeigt die Schematische Darstellung einer mögliche Implementierung unter Verwendung des ELK-Stacks.

[8] https://www.rsyslog.com
[9] https://www.syslog-ng.com

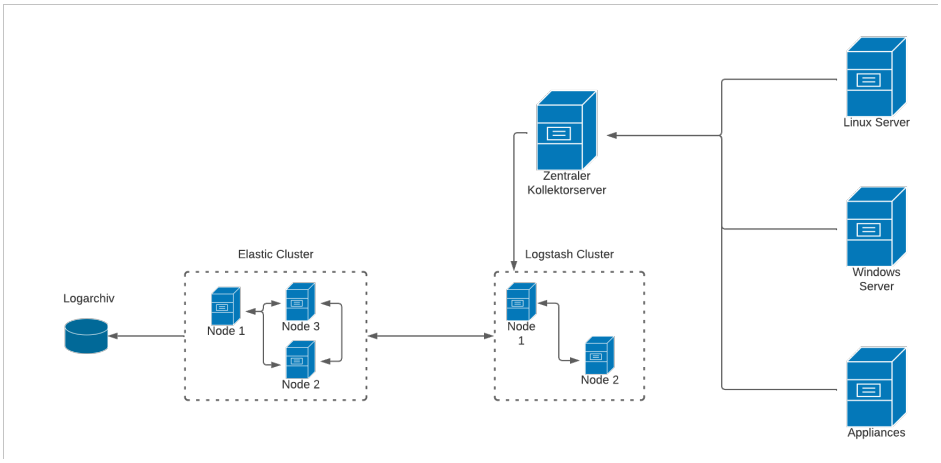

Abbildung 5.6: Schematische Darstellung eines zentralen Logmanagementsystems. Quelle: Eigene Darstellung, 2022

Die Implementierung eines zentralen Logmanagementsystems kann folgende Vorteile mit sich bringen:

- Erfüllung von Vorgaben der Aufsichtsbehörden.
- Etablierung eines zentralen Sammelpunktes für Logdaten.
- Möglichkeit zur zentralen Analyse sämtlicher Logdaten.
- Wahrung der Integrität der Logdaten (Logdaten auf den Systemen können von Angreifern gelöscht oder bearbeitet werden).
- Anbindung eines SIEM-Systems zur sicherheitstechnischen Analyse und Erkennung von Anomalien und Angriffsmustern.

Best-Practice-Ansatz: Schwachstellen-Management

Ein zentrales Logmanagement bietet die grundlegende Datenbasis für die Erkennung von Anomalien und Schwachstellen im IT-Netzwerk. Ein „Security Information and Event Management“ System zentralisiert, korreliert und analysiert Daten im gesamten IT-Netzwerk in Echtzeit um etwaige Sicherheitsprobleme zu erkennen. Effizientes Log-Management ist für ein funktionierendes SIEM-System unerlässlich. Obwohl viele SIEM-Systeme aus diesem Grund auch die Funktionen eines zentralen Logmanagement-Systems bieten, wird diese Funktion aus Kostengründen häufig ausgelagert. Häufig werden SIEM-Systeme auf Basis der Menge an übertragenen Daten lizenziert und daher nur sicherheitsrelevante Logdaten vom zentralen Logmanagement in das SIEM-System importiert. Die Aufgabe eines SIEM-Systems ist es, schädliches Verhalten auf Basis vorliegender Logdaten zu identifizieren und Warnungen an die zuständigen Mitarbeiter zu senden.

Des Weiteren bieten führende SIEM-Systeme, wie etwa Splunk[10], folgende Möglichkeiten [9]:

[10] https://www.splunk.com

- Überblick über relevante Events.
- Details zu relevanten Events.
- Möglichkeit zur Risikoanalyse von Systemen.
- Informationen über etwaige Bedrohungen.
- Informationen über beteiligte Prozesse bei einem Event.
- Definition von Usecases.

SIEM-Systeme bieten die Möglichkeit eigene Usecases auf Basis von definierten Pattern zu erstellen. So besteht etwa die Möglichkeit der Implementierung einer „Out-of-worktime Detection“ die alarmiert, falls Aktivitäten von privilegierten Accounts, außerhalb der üblichen Arbeitszeit, in den Logdaten gefunden werden. [9]

Die Implementierung eines SIEM-Systems setzt die von der EBA geforderten Maßnahmen an Banken zur Überwachung, Erkennung und Reaktion auf Sicherheitsvorfälle um. Häufig bieten SIEM-Systeme auch die Möglichkeit einer direkten Anbindung von Drittapplikationen, wie beispielsweise EDR-Systemen, an. EDR-Systeme bieten ähnlich wie SIEM-Systeme die Möglichkeit zur Überwachung auf Anomalien und sicherheitsrelevante Ereignisse in Echtzeit, basieren jedoch auf einem anderen Ansatz. Während ein SIEM-System auf Basis von erhaltenen Logdaten überwacht, wird bei der Überwachung mittels EDR meist ein Agent auf dem zu überwachenden IT-System installiert.

Der Agent bietet folgende Möglichkeiten:

- Monitoring des zu überwachenden IT-Systems in Echtzeit.
- Sammeln relevanter Daten über das IT-System.
- Analyse der gesammelt Daten um Angriffsmuster oder Anomalien zu erkennen.
- Möglichkeit zur automatischen Quarantäne eines IT-Systems bei einem Sicherheits-Event.
- Möglichkeit zur forensischen Analyse im Zuge eines Sicherheits-Events.

Ähnlich wie bei einem SIEM-System arbeiten EDR-Systeme auf Basis von Usecases. Ein bekannter Vertreter von EDR-Systemen ist Tanium.

Eine weitere Möglichkeit zur Erkennung von Schwachstellen bietet das „Vulnerability-Management“ (VuMa). Mit Hilfe von VuMa ist es möglich Sicherheitslücken in IT-Systemen und in den auf diesen Systemen laufenden Softwareprodukten zu erkennen, zu bewerten und diese zu melden.

Ein VuMa-Prozess kann in vier Schritte unterteilt werden [84]:

1. Schwachstellen erkennen
2. Schwachstellen bewerten
3. Schwachstellen behandeln
4. Schwachstellen melden

Für die Erkennung von Schwachstellen auf IT-Systemen mittels VuMa, werden die IT-Systeme mit Hilfe eines Schwachstellenscanners überprüft. Hierfür wird das IT-Netzwerk nach zugänglichen Systemen untersucht und offene Ports oder Dienste auf den einzelnen IT-Systemen identifiziert. Es wird zwischen aktiven und passivem Scannen unterschieden. Beim aktiven Scannen interagiert der Scanner mit dem jeweiligen IT-System und bietet somit die Möglichkeit simulierte Angriffe auf das IT-System zu starten und Schwachstellen aktiv auszunutzen. Beim passiven Scannen werden detailliertere Systeminformationen gesammelt und die erhaltenen Systeminformationen in weiterer Folge mit bekannten Schwachstellen abgeglichen. Da sich das Scannen eines gesamten Netzwerkes zeitintensiv gestalten kann, können die erforderlichen Daten auch von EDR-Agents gesammelt und VuMa-Systemen zur Verfügung gestellt werden. [5]

Werden auf einem IT-System Schwachstellen erkannt, müssen diese bewertet werden um das Risiko entsprechend behandeln zu können. VuMa-Systeme bieten meist unterschiedliche Risikobewertungen und Scores für gefundene Schwachstellen an. In der Praxis wird häufig nach dem „Common Vulnerability Scoring System“ (CVSS) bewertet [41]. Das tatsächliche Risiko einer Schwachstelle ist jedoch auch von weiteren Faktoren abhängig.

So sind folgende Punkte relevant [84]:

- Ist das betroffene IT-System aus dem Internet aus erreichbar?
- Welche Auswirkungen hat das Ausnützen der Schwachstelle auf den Betrieb?
- Handelt es sich um eine Schwachstelle oder ein False-Positive Ergebnis?
- Sind noch weitere Sicherheitsmaßnahmen vorhanden die ein Ausnützen der Schwachstelle verhindern könnten?

Die Behandlung einer Schwachstelle erfolgt im besten Fall durch das Einspielen eines Patches mittels Patch-Management, wie in Kapitel 5.3 beschrieben. Existiert noch kein Patch oder ist das System bereits aus der Wartung, können unter Umständen mitigierende Maßnahmen zur Schadensbegrenzung gesetzt werden. Ziel ist es hierbei die Wahrscheinlichkeit eines Incidents, beziehungsweise möglichen resultierenden Auswirkungen zu reduzieren. Auch die Akzeptanz eine Schwachstelle und damit einhergehend dem ausbleibenden Setzen einer Maßnahme kann einer Behandlung entsprechen. Dies kann der Fall sein, wenn die Kosten der Behebung der Schwachstelle wesentlich höher sind als die Kosten, die einem Unternehmen entstehen wenn die Schwachstelle ausgenutzt wird. [84]

VuMa-Systeme bieten häufig die Möglichkeit automatisierte Scans durchzuführen und im Falle einer Schwachstelle zu alarmieren. Mittels eigens konfigurierbarer Dashboards kann der aktuelle Status der IT-Systeme auch grafisch dargestellt werden.

Prävention gegenüber Angriffen

Präventive Maßnahmen zur Steigerung der Sicherheit von IT-Systemen schließen das Kapitel 5.5 ab. Die FMA fordert, dass umgesetzte Maßnahmen zur Schwachstellenbeseitigung regelmäßig mittels Penetration-Tests überprüft werden. Obwohl sich die beiden Themen VuMa und Penetration-Testing in gewissen Bereichen überschneiden, bestehen

grundlegende Unterschiede. Im Zuge des VuMa wird überprüft, ob eine Schwachstelle auf einem IT-System existiert oder nicht. Die Detektion kann auf Basis von einem fehlenden Update oder beispielsweise einem nicht gesetzten Windows Registry-Key geschehen. In den meisten Fällen kann im Zuge des VuMas nicht definiert werden ob andere mitigierende Maßnahmen implementiert sind, oder nicht. Im Gegensatz dazu wird bei einem Penetration-Test versucht die Sicherheitslücke aktiv auszunutzen um zu beweisen, dass eine Schwachstelle vorhanden ist und diese ausgenutzt werden kann. [5]

Es existieren unterschiedliche Ansätze und Ausprägungen von Penetration-Tests:

- Black-Box Test
  Der Tester besitzt keinerlei Informationen über die zu testende IT-Infrastruktur.
- White-Box Test
  Der Test besitzt Informationen über die IT-Infrastruktur, vorhandene Server, Betriebssysteme, offene Ports oder verwendete Dienste. Der Sinn eines White-Box Tests liegt in der gesteigerten Effizienz und wird verwendet, wenn ein bestimmtes System oder Verfahren getestet werden soll.
- Grey-Box Test
  Hierbei handelt es sich um eine Mischung aus Black-Box Test und White-Box Test. Dem Tester sind gewisse Informationen über das zu testende System, wie beispielsweise IP-Adressen Ranges, bekannt.

Kapitel 6

Qualitätsüberprüfung

6.1 Validierung der umgesetzten Maßnahmen

In den vorangegangenen Kapitel wurden Maßnahmen zur Umsetzung von technischen IT-Sicherheitsanforderungen an eine Bank in Österreich untersucht. Die Frage die sich stellt ist, wie eine erfolgreiche Umsetzung dieser Maßnahmen gemessen und in weiterer Folge auditiert werden kann.

Im Zuge der Ausarbeitung haben sich folgende Möglichkeiten für die Überprüfung einer korrekten Umsetzung ergeben:

- Technische Überprüfung
  - Überprüfung durch interne Mechanismen
    Einige Produkte, mit denen Maßnahmen umgesetzt werden, bieten die Möglichkeit interner Kontrollmechanismen um die ordnungsgemäße Funktionalität des Produktes sicherzustellen. So bieten Identity-Management Systeme etwa die Möglichkeit zur Rezertifizierung von Berechtigungen oder zur Analyse ob nicht korrelierte Accounts bestehen. Auf Basis dieser Mechanismen können regelmäßige Kontrollen etabliert und auditiert werden.
  - Überprüfung mittels Penetration-Test
    Umgesetzte IT-Sicherheitsanforderungen lassen sich häufig mittels Penetration-Test überprüfen. Auf Basis unterschiedlicher Penetration-Tests, wie in Kapitel 5.5 beschrieben, können Angriffe simuliert und die Funktionalität der IT-Sicherheitsmaßnahme überprüft werden.
  - Überprüfung mittels Katastrophentest oder „Business-Continuity Management“ (BCM)
    Ähnlich wie bei Penetration-Tests lassen sich umgesetzte Maßnahmen im Zuge eines Katastrophentests überprüfen. Häufig decken Bereiche aus dem BCM auch IT-Sicherheitsmaßnahmen ab. Im Zuge eines Katastrophentests können die Ausfallsicherheit von Systemen oder die einwandfreie Funktionalität von Backup-Prozessen überprüft werden.
- Organisatorische Überprüfung
  - Überprüfung mittels Audits

Interne und externe Audits sind das erste Mittel der Wahl um die Umsetzung von technischen IT-Sicherheitsmaßnahmen und deren korrekte Arbeitsweise sicherzustellen.

– Überprüfung mittels internem Kontrollsystem (IKS)
  Auch mittels eines IKS kann die Umsetzung von Maßnahmen überprüft werden. Im Falle von Firewall-Änderungen etwa können beispielsweise periodisch Stichproben genommen und die Legitimität der Änderungen überprüft werden.
– Überprüfung mittels Service-Level Agreement (SLA)
  Mittels vereinbarter SLAs lässt sich nicht nur die Funktionalität sondern auch die Effizienz von umgesetzten Maßnahmen überprüfen. So können SLAs Auskunft darüber geben ob kritische System-Patchens eingespielt werden und wie viel Zeit das Update in Anspruch nimmt.

Abbildung 6.1 zeigt die in Kapitel 4.5 abgeleiteten IT-Sicherheitsmaßnahmen und passende Überprüfungsmethoden.

Gruppierung	Enthaltene Maßnahmen	Überprüfungsart	Überprüfungsmethode
Identity- und Access-Management	Identity-Management	Technisch / Organisatorisch	Rezertifizierungen, Audit / IKS
	Native-Change Detection	Technisch	Penetration-Test
	Multifaktor-Authentifizierung	Technisch / Organisatorisch	Penetration-Test, Audit / IKS
	Single-Sign On		
	Privileged-Access Management		
Asset-Management	Content-Management Database	Organisatorisch	Audit / IKS
	Source-Code Verwaltung		
	Baselining und Change-Management		
Infrastruktur-Betrieb	Monitoring	Technisch	Katastrophentest / BCM
	Hochverfügbarkeit		
	Patch-Management	Organisatorisch	Audit / IKS
	Backup-Restore	Technisch	Katastrophentest / BCM / Standardisierung
Netzwerk-Management	Netzwerk-Segmentierung	Technisch	Penetration-Test
	Network-Access Control		
	Firewalls	Technisch / Organisatorisch	Penetration-Test, Audit / IKS
	Kryptografie	Technisch	Penetration-Test
Cybersecurity-Management	Log-Management	Organisatorisch	Audit / IKS
	Security Incident Event Monitoring	Technisch / Organisatorisch	Penetration-Test, Audit / IKS
	Vulnerability-Management	Organisatorisch	SLAs / Audit / IKS
	Penetration-Testing	Organisatorisch	Audit / IKS
	Endpoint-Detection and Response	Technisch	Penetration-Test

Abbildung 6.1: Visuelle Darstellung der Gruppierung, enthaltenen Maßnahmen und Möglichkeit zur Überprüfung der Umsetzung. Quelle: Eigene Darstellung, 2022

6.2 Vollständigkeit der Maßnahmen

In Kapitel 5 wurden Maßnahmen und Best-Practice-Ansätze zur Umsetzung von technischen IT-Sicherheitsanforderungen an eine Bank in Österreich definiert und beschrieben. Zur Überprüfung, ob diese geeignet sind die Anforderungen der Aufsichtsbehörden zu

erfüllen, werden die Maßnahmen und Best-Practice-Ansätze auf die „OWASP Cyber Defense Matrix“ (CDM) angewandt [80].

Die CDM ist ein Open-Source-Community-Projekt unter der Leitung der OWASP[1] und in Abbildung 6.2 dargestellt. Es handelt sich um eine zweidimensionale Matrix mit den fünf Kernfunktionen des „NIST Cybersecurity Frameworks“ auf der X-Achse und fünf unterschiedlichen Asset-Ausprägungen auf der Y-Achse [42]. Das „Nation Institute of Standards and Technology“ (NIST[2]) definiert fünf grundlegende Kernfunktionen zur Behandlung von- und zum Schutz vor Cyberangriffen, zu sehen in Abbildung 6.3.

Die fünf Kernfunktionen beziehen sich auf die Zeit vor und nach einem erfolgreichen Angriff [77]:

- Pre-incident:
  - Identify
    Identifizierung der im Unternehmen befindlichen Assets.
  - Protect
    Schutz aller im Unternehmen befindlichen Assets und/oder die Etablierung von mitigierenden Maßnahmen.
- Post-incident:
  - Detect
    Erkennen von schadhaften Aktivität auf den Assets.
  - Respond
    Reaktion auf schadhafte Aktivitäten auf den Assets.
  - Recover
    Wiederherstellung der jeweiligen Assets.

Die Y-Achse der CDM beschreibt fünf schützenswerte Ausprägungen von IT-Assets:

- Devices
  Clients, Server, Storage, ...
- Applications
  Software Interaktion auf den Devices.
- Networks
  Client/Server Interaktionen, Daten die über das Netzwerk übertragen werden.
- Data
  Daten die auf den Devices gespeichert oder von diesen verarbeitet werden.
- Users
  Anwender der jeweiligen Assets.

Der untere Bereich der Matrix zeigt eine Kombination aus benötigter Technologie, Menschen und relevanter Prozesse für die Adressierung der fünf Kernfunktionen. Es ist erkennbar, dass die Funktionen im linken Bereich der Matrix stark automatisiert mittels

[1] https://owasp.org
[2] https://www.nist.gov

Technologie durchgeführt werden können. Die Funktionen im rechten Bereich der Matrix benötigen die Unterstützung durch Mitarbeiter und manuelles Doing. Etablierte und funktionierende Prozesse sind für alle fünf Kernfunktionen nötig.

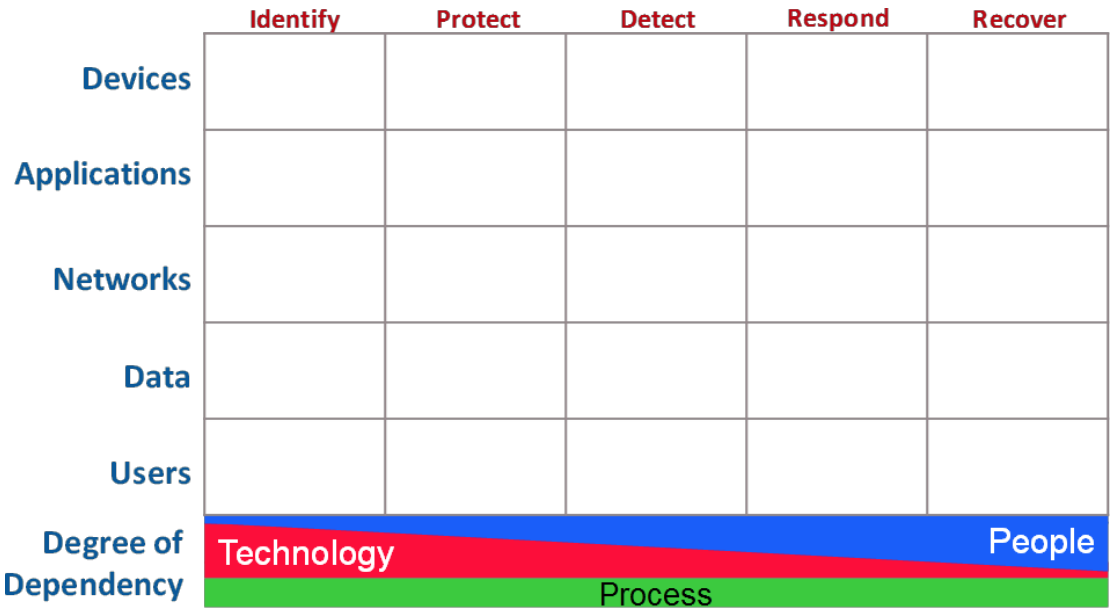

Abbildung 6.2: Darstellung der CDM. Quelle: *Owasp Cyber Defense Matrix* [81], 2022

Abbildung 6.3: Darstellung der fünf Kernfunktionen des NIST Cybersecurity Frameworks. Quelle: Nicole.keller@nist.gov [77], 2022

Im Zuge der Qualitätsüberprüfung werden die in Kapitel 5 definierten IT-Sicherheitsmaßnahmen und Best-Practice-Ansätze in die CDM eingetragen. Hierfür ist relevant in welcher Angriffsphase, welche Ausprägung von IT-Asset, mit Hilfe der jeweiligen Maßnahme geschützt werden. Dieser Vorgang lässt sich am Beispiel IAM verdeutlichen. Mit Hilfe von IAM können Anwender im Unternehmen eindeutig identifiziert werden. Des Weiteren bietet IAM Mechanismen zum Schutz der Anwender, etwa vor unerlaubter Verwendung von Benutzerdaten. Auch eine unerlaubte Verwendung von Benutzerdaten kann mittels

IAM erkannt werden. Aus diesem Grund ist die Maßnahme IAM in der CDM in den Bereichen „Users - Identify“, „Users - Protect“ und „Users - Detect“ zu finden.

Es ist zu erkennen, dass die abgeleiteten Maßnahmen und Best-Practice-Ansätze einen Großteil der fünf Kernfunktionen der Matrix adressieren. Im Zuge der Ausarbeitung hat sich herausgestellt, dass die Punkte „Identify Data“, „Respond Users“ und „Recover Users“ technisch nicht realisierbar sind. Eine Identifizierung und Klassifizierung der in einem Unternehmen verwendeten Daten benötigen eine manuelle Betrachtung und kann nicht technisch realisiert werden. Die Punkte „Detect Data“ und „Respond Data“ wurden in den Anforderungen in Kapitel 3 und daher auch in den umzusetzenden Maßnahmen in Kapitel 4.5 nicht betrachtet. Eine mögliche Maßnahme für „Detect Data“ bietet die Recherche nach unternehmensrelevanten Daten im Darknet. Ein Beispiel für den Bereich „Respond Data“ liefert die Implementierung von „Digital Rights Management“, der Kontrolle und dem Management von urheberrechtlich geschützten Daten.

Abbildung 6.4 zeigt die CDM, mit den in Kapitel 4.5 abgeleiteten Maßnahmen und den in Kapitel 5 definierten Best-Practice-Ansätzen.

	Identify	Protect	Detect	Respond	Recover
Devices	CMDB, EDR, VuMa	EDR, VuMa, Netzwerksegmentierung, IAM Verschlüsselung, PAM, MFA, SSO, Baselining, Pentesting, Patch-Management, Firewalls, Hochverfügbarkeit	EDR, SIEM, Native-Change-Detection, Monitoring, NAC	Zentrales-Logmanagement	EaC, Backup-Restore
Applications	CMDB, EDR, VuMa	EDR, VuMa, Netzwerksegmentierung, IAM Verschlüsselung, PAM, MFA, SSO, Baselining, Pentesting, Patch-Management, Firewalls, Hochverfügbarkeit	EDR, SIEM	Zentrales-Logmanagement	Backup-Restore
Networks	CMDB, EDR, VuMa	EDR, VuMa, Netzwerksegmentierung, IAM Verschlüsselung, PAM, MFA, SSO, Baselining, Pentesting, Patch-Management, Firewalls, Hochverfügbarkeit	EDR, SIEM	Zentrales-Logmanagement	EaC, Backup-Restore
Data	<technisch nicht realisierbar>	Verschlüsselung	<nicht adressiert>	<nicht adressiert>	Backup-Restore
Users	IAM	IAM, PAM, MFA, SSO	EDR, SIEM, IAM, Native-Change-Detection	<technisch nicht realisierbar>	<technisch nicht realisierbar>

Abbildung 6.4: Darstellung der CDM mit den definierten Best-Practice-Ansätzen und damit einhergehenden Maßnahmen. Quelle: Eigene Darstellung, 2022

Kapitel 7

Fazit und Zusammenfassung

Die vorliegende Arbeit gibt einen Überblick über geltende IT-Sicherheitsanforderungen an eine Bank in Österreich. Im Zuge der Ausarbeitung wurden unterschiedliche regulatorische Anforderungen von Aufsichtsbehörden in einer Anforderungsmatrix dargestellt und gegliedert. In weiterer Folge wurden die relevanten Anforderungen an IT-Sicherheit untersucht und auf Basis ihrer technischen und organisatorischen Umsetzbarkeit aufgeteilt. Für die technisch umsetzbaren Anforderungen an IT-Sicherheit wurden Maßnahmen abgleitet und diese nach passenden Themengebieten gruppiert. Die einzelnen Maßnahmen jedes Themengebietes wurden beschrieben und deren Relevanz aufgezeigt. Im Zuge der Beschreibung der Maßnahmen wurden Best-Practice-Ansätze nach aktuellem Stand der Technik abgeleitet und beschrieben. Eine Qualitätsüberprüfung der abgeleiteten Best-Practice-Ansätze mittels der CDM rundet die Arbeit ab.

Im Zuge der Ausarbeitung der relevanten Richtlinien hat sich gezeigt, dass 417 technische und organisatorische Anforderungen an IT-Sicherheit einer Bank in Österreich bestehen. Von diesen Anforderungen lassen sich 269 Anforderungen organisatorisch und 148 Anforderungen technisch umsetzen. Diese Aufteilung zeigt, dass das Thema IT-Sicherheit zu einem großen Teil organisatorische Maßnahmen erfordert. Die 148 technischen Anforderungen lassen sich mit Hilfe von 21 Maßnahmen umsetzen. Bei der Ableitung der Maßnahmen hat sich herausgestellt, dass sich ein Drittel der technischen Anforderungen mit der Behandlung der drei Themengebiete „Identity-Management“, „Vulnerability-Management“ und „Security Incident und Event Monitoring“ umsetzen lassen. Die technisch erforderlichen Maßnahmen sind in Tabelle 4.5 aufgelistet. Im Zuge der weiteren Ausarbeitung konnten 10 Best-Practice-Ansätze definiert werden, mit deren sich die 21 erforderlichen Maßnahmen umsetzen lassen. Die Best-Practice-Ansätze und die darin enthaltenen Maßnahmen sind in Abbildung 5.1 dargestellt. Abbildung 6.1 zeigt, dass eine erfolgreiche Umsetzung der Maßnahmen und damit einhergehend eine Erfüllung der technischen Anforderungen mittels technischer und organisatorischer Mittel gemessen werden kann.

Die Arbeit zeigt, dass geltende technische IT-Sicherheitsanforderungen an eine Bank in Österreich auf Basis von Best-Practice-Ansätzen erfüllt werden können. Es ist darauf zu achten, dass man sich bei der Implementierung von technischen IT-Sicherheitsmaßnahmen nicht nur auf die von Aufsichtsbehörden vorgeschrieben Anforderungen beschränken

sollte. Aufsichtsbehörden geben nur ein Rahmenwerk vor, die Vollständigkeit der durch die Richtlinien abgeleiteten Maßnahmen darf nicht als gegeben angenommen werden. Schlussendlich geht es nicht darum die Anforderungen von Aufsichtsbehörden zu erfüllen, sondern die IT-Sicherheit des Unternehmens sicherstellen zu können und so gegen bösartige Angriffe gewappnet zu sein.

Anhang A

Peer Review

A.1 Peer 1

Fragestellung 1 - Aufsichtsbehörden

- Welchen Aufsichtsbehörden müssen Sie im Rahmen von regulatorischen Überprüfungen der Bank in Bezug auf IT-Sicherheit Rede und Antwort stehen?
  Antwort: Im Lead, wenn es um Prüfungen geht ist die FMA.

- Welchen Aufsichtsbehörden gegenüber sind sie im Falle eines Security-Incidents innerhalb der Bank meldepflichtig?
  Antwort: Security-Incidents gehen zentral an die FMA, es gibt jedoch auch EZB Meldepflichten, meines Wissens aber nur für Unternehmen, welche auch direkt von der ETB überwacht werden (Großbanken).

- Sind die in Tabelle 3.1 aufgelisteten Aufsichtsbehörden Ihrer Meinung nach relevant für eine Bank in Österreich?
  Antwort: EIOPA gilt nur für Versicherungen, nicht für Banken und bildet das Pendant zu den EBA-Guidelines. Die EU ist in diesem Sinne keine Aufsichtsbehörde. Die Überwachung wird von beauftraten Behörden durchgeführt (EZB oder FMA), von der EU wird nur der Rahmen vereinbart bzw. vorgegeben. Die ENISA ist in diesem Sinne auch keine Behörde sondern eine Agentur, die im Auftrag der EU öffentliche Institutionen sowie Behörden unterstützt.

- Ist die Auflistung relevanter Aufsichtsbehörden für eine Bank in Österreich in Tabelle 3.1 vollständig?
  Antwort: Ja, die Auflistung ist vollständig.

Fragestellung 2 - Richtlinien

- An welchen Richtlinien orientiert sich Ihr Unternehmen bei der Etablierung von IT-Sicherheitsanforderungen bzw. bei der Erstellung von Governance-Richtlinien?
  Antwort: Primär an Hand der Vorgaben der FMA

- Sind die in Tabelle 3.1 aufgelisteten Richtlinien Ihrer Meinung nach relevant für eine Bank in Österreich?
  Antwort: Ja, die Richtlinien und Vorgaben sind relevant.

- Ist die Auflistung relevanter Richtlinien in Tabelle 3.1 vollständig?
  Antwort: Ja, die Auflistung ist vollständig.

A.2 Peer 2

Fragestellung 1 - Aufsichtsbehörden

- Welchen Aufsichtsbehörden müssen Sie im Rahmen von regulatorischen Überprüfungen der Bank in Bezug auf IT-Sicherheit Rede und Antwort stehen?
  Antwort: FMA

- Welchen Aufsichtsbehörden gegenüber sind sie im Falle eines Security-Incidents innerhalb der Bank meldepflichtig?
  Antwort: FMA

- Sind die in Tabelle 3.1 aufgelisteten Aufsichtsbehörden Ihrer Meinung nach relevant für eine Bank in Österreich?
  Antwort: Ja, ggf. ist die DSGVO zu ergänzen. EIOPA ist für Versicherungen relevant (Hier stellt sich die Frage, welche Produkte von der Bank angeboten werden).

- Ist die Auflistung relevanter Aufsichtsbehörden für eine Bank in Österreich in Tabelle 3.1 vollständig?
  Antwort: Ja

Fragestellung 2 - Richtlinien

- An welchen Richtlinien orientiert sich Ihr Unternehmen bei der Etablierung von IT-Sicherheitsanforderungen bzw. bei der Erstellung von Governance-Richtlinien?
  Antwort: FMA

- Sind die in Tabelle 3.1 aufgelisteten Richtlinien Ihrer Meinung nach relevant für eine Bank in Österreich?
  Antwort: Das BAIT-Rundschreiben ist für Österreich nicht relevant, alle anderen sehe ich als relevant an.

- Ist die Auflistung relevanter Richtlinien in Tabelle 3.1 vollständig?
  Antwort: Ja

A.3 Peer 3

Fragestellung 1 - Aufsichtsbehörden

- Welchen Aufsichtsbehörden müssen Sie im Rahmen von regulatorischen Überprüfungen der Bank in Bezug auf IT-Sicherheit Rede und Antwort stehen?
  Antwort: Wir werden von der FMA auditiert und melden auch Security-Incidents an die FMA.

- Welchen Aufsichtsbehörden gegenüber sind sie im Falle eines Security-Incidents innerhalb der Bank meldepflichtig?
  Antwort: Security-Incidents werden in erster Instanz an die FMA gemeldet.

- Sind die in Tabelle 3.1 aufgelisteten Aufsichtsbehörden Ihrer Meinung nach relevant für eine Bank in Österreich?
  Antwort: Für eine nationale Bank in Österreich ist die BaFin nicht relevant. Die Inhalte der BaFin werden häufig von der FMA übernommen. Die EIOPA ist für eine Bank nicht relevant. Die ENISA ist keine Aufsichtsbehörde aber natürlich relevant für Banken in Österreich.

- Ist die Auflistung relevanter Aufsichtsbehörden für eine Bank in Österreich in Tabelle 3.1 vollständig?
  Antwort: Ja, ich habe nichts zu ergänzen.

Fragestellung 2 - Richtlinien

- An welchen Richtlinien orientiert sich Ihr Unternehmen bei der Etablierung von IT-Sicherheitsanforderungen bzw. bei der Erstellung von Governance-Richtlinien?
  Antwort: Wir orientieren uns hauptsächlich an den Vorgaben der FMA.

- Sind die in Tabelle 3.1 aufgelisteten Richtlinien Ihrer Meinung nach relevant für eine Bank in Österreich?
  Antwort: BAIT-Rundschreiben ist nicht relevant, kann aber als Quelle herangezogen werden. Die Inhalte decken sich mit den Inhalten der FMA.

- Ist die Auflistung relevanter Richtlinien in Tabelle 3.1 vollständig?
  Antwort: Aus meiner Sicht, ja.

Anhang B

Anforderungsmatrix / Git-Repository

In diesem Git-Repository sind folgende Inhalte hinterlegt:

- Latex-Source Code als .zip inklusive aller verwendeten Abbildungen und Listings
- Masterarbeit in PDF-Form
- Anforderungsmatrix in Form einer Excel-Datei
- Archivierte Webseiten, die als Referenz verwendet wurden

Link zum Repository: https://github.com/sikoqdos/MasterThesisISM2022:

Quellenverzeichnis

Literatur

[1] Sheikh Ahmed. *CompTIA Security+ Certification Study Guide : Network Security Essentials*. 2020 (siehe S. 51–53).

[2] Bradley Beard. *Beginning Backup and Restore for SQL Server - Data Loss Management and Prevention Techniques*. 2018 (siehe S. 50).

[3] Nitul Dutta. *Cyber Security*. eng. Studies in Computational Intelligence Ser. ; 2021 (siehe S. 5).

[4] Michael Falk. *IT-Compliance in der Corporate Governance : Anforderungen und Umsetzung*. ger. 2012 (siehe S. 6).

[5] Morey J Haber. *Asset Attack Vectors : Building Effective Vulnerability Management Strategies to Protect Organizations*. 2018 (siehe S. 61, 62).

[6] Christoph E. Hauschka u. a. *Corporate compliance handbuch der haftungsvermeidung im Unternehmen*. C.H. Beck, 2016 (siehe S. 6).

[7] Wolfgang Johannsen. *Referenzmodelle für IT-Governance : methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL und Co*. ger. 2., aktualisierte und erw. Aufl.. 2011 (siehe S. 6).

[8] Georgia König und René Kugel. „DevOps—Welcome to the Jungle“. *HMD Praxis der Wirtschaftsinformatik* 56.2 (2019), S. 289–300 (siehe S. 42).

[9] Deep Mehta. *Splunk Certified Study Guide : Prepare for the User, Power User, and Enterprise Admin Certifications*. 2021 (siehe S. 59, 60).

[10] Norbert Pohlmann. *Cyber-Sicherheit*. Springer Fachmedien Wiesbaden, 2022 (siehe S. 55, 57).

[11] Darran Rolls und Morey J. Haber. *Identity attack vectors: Implementing an effective identity and Access Management Solution*. Apress, 2020 (siehe S. 34, 36, 39).

[12] Jörg Schwenk. *Sicherheit und Kryptographie im Internet : Theorie und Praxis*. 2020 (siehe S. 54–56).

[13] Alexander Tsolkas. *Rollen und Berechtigungskonzepte : Ansätze für das Identity- und Access-Management im Unternehmen*. 2010 (siehe S. 36).

Online-Quellen

[14] URL: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2522896/32a28233-12f5-49c8-9bb5-f8744ccb4e92/Final%5C%20Guidelines%5C%20on%5C%20ICT%5C%20and%5C%20security%5C%20risk%5C%20management.pdf (besucht am 28. 02. 2022) (siehe S. 8, 9, 19).

[15] URL: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%5C%20revised%5C%20Guidelines%5C%20on%5C%20outsourcing%5C%20arrangements.pdf?retry=1 (besucht am 28. 02. 2022) (siehe S. 8, 10).

[16] URL: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/934179/f27bf266-580a-4ad0-aaec-59ce52286af0/EBA-GL-2014-12%5C%20%5C%28Guidelines%5C%20on%5C%20the%5C%20security%5C%20of%5C%20internet%5C%20payments%5C%29_Rev1.pdf (besucht am 28. 02. 2022) (siehe S. 8, 11, 19).

[17] URL: https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/eiopa-bos-20-600-guidelines-ict-security-and-governance.pdf (besucht am 28. 02. 2022) (siehe S. 8, 11).

[18] URL: https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines_de.pdf (besucht am 28. 02. 2022) (siehe S. 8, 13, 19).

[19] URL: https://www.fma.gv.at/download.php?d=3597 (besucht am 28. 02. 2022) (siehe S. 8, 13, 19).

[20] URL: https://www.fma.gv.at%5C%2Ffma-veroeffentlicht-leitfaeden-zur-it-sicherheit-bei-fonds-verwaltern-und-wertpapierdienstleistern%5C%2F&usg=AOvVaw31yulqq9Q13K5cv6mtGdCb (besucht am 28. 02. 2022) (siehe S. 8, 14, 19).

[21] URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32018R0389 (besucht am 28. 02. 2022) (siehe S. 8, 15, 19).

[22] URL: https://www.enisa.europa.eu/publications/definition-of-cybersecurity (besucht am 28. 02. 2022) (siehe S. 8, 16).

[23] URL: https://www.sailpoint.com/solutions/identityiq (besucht am 28. 02. 2022) (siehe S. 36).

[24] URL: https://oauth.net/2 (besucht am 28. 02. 2022) (siehe S. 37).

[25] URL: https://openid.net/connect (besucht am 28. 02. 2022) (siehe S. 37).

[26] URL: https://access.redhat.com/products/red-hat-single-sign-on (besucht am 28. 02. 2022) (siehe S. 38).

[27] URL: https://www.pcisecuritystandards.org (besucht am 28. 02. 2022) (siehe S. 45).

[28] URL: https://gdpr.eu (besucht am 28. 02. 2022) (siehe S. 45).

[29] URL: https://www.json.org/json-de.html (besucht am 28. 02. 2022) (siehe S. 47).

[30] URL: https://datatracker.ietf.org/doc/html/rfc6176 (besucht am 05. 06. 2022) (siehe S. 54).

[31] URL: https://datatracker.ietf.org/doc/html/rfc7568 (besucht am 05. 06. 2022) (siehe S. 54).

[32] URL: https://www.cisa.gov/uscert/ncas/alerts/TA14-290A (besucht am 05. 06. 2022) (siehe S. 54).

[33] URL: https://datatracker.ietf.org/doc/html/rfc2104 (besucht am 05. 06. 2022) (siehe S. 55).

[34] URL: https://datatracker.ietf.org/doc/html/rfc5246 (besucht am 05. 06. 2022) (siehe S. 55).

[35] URL: https://datatracker.ietf.org/doc/html/rfc5990 (besucht am 05. 06. 2022) (siehe S. 55).

[36] URL: https://datatracker.ietf.org/doc/html/rfc2459 (besucht am 05. 06. 2022) (siehe S. 55).

[37] URL: https://datatracker.ietf.org/doc/html/rfc8017 (besucht am 05. 06. 2022) (siehe S. 55).

[38] URL: https://datatracker.ietf.org/doc/html/rfc3447 (besucht am 05. 06. 2022) (siehe S. 56).

[39] URL: https://www.elastic.co/de/elastic-stack (besucht am 05. 06. 2022) (siehe S. 58).

[40] URL: https://docs.microsoft.com/en-us/windows/win32/wec/windows-event-collector (besucht am 05. 06. 2022) (siehe S. 58).

[41] URL: https://nvd.nist.gov/vuln-metrics/cvss (besucht am 05. 06. 2022) (siehe S. 61).

[42] URL: https://www.nist.gov/cyberframework (besucht am 05. 06. 2022) (siehe S. 65).

[43] Anna Zakrzewski et al. *Global Wealth 2019: Reigniting Radical Growth*. 2019. URL: https://www.bcg.com/publications/2019/global-wealth-reigniting-radical-growth (besucht am 28. 02. 2022) (siehe S. 1).

[44] Silke Brüggemann et al. *Aufsicht über Informationssicherheit und Cloud-Computing verlangt europaweite Harmonisierung*. URL: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/BaFinPerspektiven/2020/bp_20_1_Bruggemann_Kocatepe.html (besucht am 28. 02. 2022) (siehe S. 2).

[45] Rana Ashutosh und Murthy Nivedita. *Top seven logging and monitoring best practices: Synopsys*. URL: https://www.synopsys.com/blogs/software-security/logging-and-monitoring-best-practices/ (besucht am 28. 02. 2022) (siehe S. 47).

[46] BaFin. *Die BaFin*. URL: https://www.bafin.de/DE/DieBaFin/diebafin_node.html (besucht am 28. 02. 2022) (siehe S. 9).

[47] BaFin. *Rundschreiben 10/2017 (BA) Bankaufsichtliche Anforderungen an die it (bait)*. URL: https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.html (besucht am 28. 02. 2022) (siehe S. 8, 9, 19).

[48] Europäische Bankenaufsicht. *EBA*. URL: https://www.eba.europa.eu/languages/home_de (besucht am 28. 02. 2022) (siehe S. 10).

[49] Capital. *Der Untergang von Worldcom-chef Bernie Ebbers*. Jan. 2022. URL: https://www.capital.de/wirtschaft-politik/der-untergang-von-worldcom-chef-bernie-ebbers (besucht am 05. 06. 2022) (siehe S. 6).

[50] Capital. *WIE Nick Leeson die barings bank in die pleite ritt*. Jan. 2022. URL: https://www.capital.de/wirtschaft-politik/financial-crimes-die-grossen-betrueger-nick-leeson-barings-bank (besucht am 05. 06. 2022) (siehe S. 6).

[51] Penny Crosman. *5 ransomware trends that should alarm banks*. Okt. 2020. URL: https://www.americanbanker.com/news/5-ransomware-trends-that-should-alarm-banks (besucht am 05. 06. 2022) (siehe S. 6).

[52] Armon Dadgar. *Why policy as code?* URL: https://www.hashicorp.com/blog/why-policy-as-code (besucht am 28. 02. 2022) (siehe S. 44).

[53] *Datenschutzrecht in österreich*. URL: https://www.dsb.gv.at/recht-entscheidungen/gesetze-in-oesterreich.html (besucht am 28. 02. 2022) (siehe S. 4).

[54] Duden. *Best practice*. URL: https://www.duden.de/rechtschreibung/Best_Practice (besucht am 28. 02. 2022) (siehe S. 33).

[55] *Eba-Leitlinien und Andere Konvergenzinstrumente*. Jan. 2021. URL: https://www.fma.gv.at/eu/eba-leitlinien-und-andere-konvergenzinstrumente (siehe S. 2).

[56] EIOPA. *Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA)*. URL: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/eiopa_de (besucht am 28. 02. 2022) (siehe S. 12).

[57] ENISA. *ENISA*. URL: https://www.enisa.europa.eu (besucht am 28. 02. 2022) (siehe S. 17).

[58] *ESAS publish joint advice on information and Communication Technology Risk Management and Cybersecurity*. URL: https://www.eba.europa.eu/esas-publish-joint-advice-on-information-and-communication-technology-risk-management-and-cybersecurity (besucht am 28. 02. 2022) (siehe S. 2).

[59] Armin Schmitt EY Österreich. *Was macht Banken für Datendiebstahl und Cyberangriffe besonders interessant?* 2021. URL: https://www.ey.com/de_at/cybersecurity/was-macht-banken-fuer-datendiebstahl-und-cyberangriffe-besonders-interessant (besucht am 28. 02. 2022) (siehe S. 1).

[60] EZB. *CROE*. URL: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf (besucht am 28. 02. 2022) (siehe S. 8, 15, 16).

[61] EZB. *EZB*. URL: https://www.europaimunterricht.de/eu-ezb (besucht am 28. 02. 2022) (siehe S. 16).

[62] Bundesanstalt für Finanzdienstleistungsaufsicht. *MaRisk*. URL: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2021/rs_1021_MaRisk_BA.html;jsessionid=4B2D490B277228F280297A24CA1A1BD1.2_cid501?nn=9450904#doc16502162bodyText3 (besucht am 28. 02. 2022) (siehe S. 9).

[63] FMA. *Finanzmarktaufsicht*. URL: https://www.bmf.gv.at/themen/finanzmarkt/finanzmarktaufsicht.html (besucht am 28. 02. 2022) (siehe S. 14).

[64] Otto Geißler. *Was Ist Skalierbarkeit?* URL: https://www.datacenter-insider.de/was-ist-skalierbarkeit-a-852037/ (besucht am 28. 02. 2022) (siehe S. 47, 48).

[65] *Gesetz über das Kreditwesen (kreditwesengesetz - KWG).* URL: https://www.gesetze-im-internet.de/kredwg/BJNR008810961.html (besucht am 28. 02. 2022) (siehe S. 9).

[66] *Guidelines on ICT risk assessment under the SREP.* URL: https://www.eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-on-ict-risk-assessment-under-the-srep (besucht am 28. 02. 2022) (siehe S. 8, 11).

[67] HashiCorp. *Why Policy as Code?* URL: https://www.hashicorp.com/blog/why-policy-as-code (besucht am 28. 02. 2022) (siehe S. 42).

[68] Iainfoulds. *Active directory domain services overview.* URL: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (besucht am 28. 02. 2022) (siehe S. 53).

[69] *Informationssicherheits-Zertifizierung: ISO 27001.* URL: https://www.tuv.at/iso27001 (besucht am 28. 02. 2022) (siehe S. 9).

[70] *It-grundschutz.* URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (besucht am 28. 02. 2022) (siehe S. 9).

[71] Savan Kharod. *7 best practices for creating a high availability infrastructure.* 2021. URL: https://blogs.sap.com/2021/10/05/7-best-practices-for-creating-a-high-availability-infrastructure/ (besucht am 28. 02. 2022) (siehe S. 46).

[72] *Konzession.* URL: https://www.fma.gv.at/banken/konzessionierung (besucht am 28. 02. 2022) (siehe S. 7).

[73] Kief Morris. *Infrastructure as code.* URL: https://www.oreilly.com/library/view/infrastructure-as-code/9781491924334/ch01.html (besucht am 28. 02. 2022) (siehe S. 43).

[74] mulesoft.com. *What is a Single Source of Truth (SSOT).* URL: https://www.mulesoft.com/resources/esb/what-is-single-source-of-truth-ssot (besucht am 28. 02. 2022) (siehe S. 41).

[75] Netgear. *Fully managed switches, switches, business und Netgear.* URL: https://www.netgear.com/at/business/wired/switches/fully-managed (besucht am 28. 02. 2022) (siehe S. 52).

[76] *Netzwerksegmentierung - Ein UNTERSCHÄTZTES instrument in der it-sicherheit teil 2.* URL: https://www.bristol.de/netzwerksegmentierung-ein-unterschaetztes-instrument-in-der-it-sicherheit-teil-2/ (besucht am 28. 02. 2022) (siehe S. 53).

[77] Nicole.keller@nist.gov. *Cybersecurity framework.* URL: https://www.nist.gov/cyberframework (besucht am 28. 02. 2022) (siehe S. 65, 66).

[78] Hacker Noon. *What is Everything-as-Code? Examining the Explosion of „as Code" Buzzwords.* URL: https://hackernoon.com/everything-as-code-explained-0ibg32a3 (besucht am 28. 02. 2022) (siehe S. 43–45).

[79] FMA Österreich. *Oenb und FMA haben ihre gemeinsamen schwerpunkte in der Bankenaufsicht für das jahr 2022 definiert.* URL: https://www.fma.gv.at/oenb-und-fma-haben-ihre-gemeinsamen-schwerpunkte-in-der-bankenaufsicht-fuer-das-jahr-2022-definiert/ (besucht am 28. 02. 2022) (siehe S. 8).

[80] *Owasp Cyber Defense Matrix.* URL: https://owasp.org/www-project-cyber-defense-matrix/ (besucht am 28. 02. 2022) (siehe S. 4, 65).

[81] *Owasp Cyber Defense Matrix.* URL: https://owasp.org/www-project-cyber-defense-matrix/ (besucht am 28. 02. 2022) (siehe S. 66).

[82] Abdullah Özel, Tobias Pautz und Nikolaus Schmidt. *Infrastructure as code.* URL: https://link.springer.com/article/10.1365/s40702-020-00657-0 (besucht am 28. 02. 2022) (siehe S. 42).

[83] Alexis Le-Quoc. *Datadog.* URL: https://www.datadoghq.com/blog/monitoring-101-collecting-data/ (besucht am 28. 02. 2022) (siehe S. 48, 49).

[84] Rapid7. *Schwachstellenmanagement-Prozesse und systeme.* URL: https://www.rapid7.com/de/cybersecurity-grundlagen/vulnerability-management-and-scanning/ (besucht am 28. 02. 2022) (siehe S. 60, 61).

[85] PFR Rechtsanwälte. *PFR.* URL: https://www.pfr.at/de/news-medien/news/finanzmarktrecht/eba-leitlinien-zum-management-von-ikt-und-sicherheitsrisiken (besucht am 28. 02. 2022) (siehe S. 10).

[86] RedHat. *Was ist patch-management und Automatisierung.* URL: https://www.redhat.com/de/topics/management/what-patch-management-and-automation (besucht am 28. 02. 2022) (siehe S. 49, 50).

[87] *RFC 8573 - message authentication code for the network time protocol.* URL: https://datatracker.ietf.org/doc/html/rfc8573 (besucht am 28. 02. 2022) (siehe S. 54).

[88] RIS. *Bundesrecht Konsolidiert: Gesamte Rechtsvorschrift für Bankwesengesetz, Fassung vom 19.06.2022.* URL: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004827 (besucht am 28. 02. 2022) (siehe S. 7).

[89] SanData. *Was IST Network Access Control (NAC)?* URL: https://www.sandata.net/main.asp?VID=1&Kat1=123&Kat2=807&Kat3=727 (besucht am 28. 02. 2022) (siehe S. 53).

[90] European Securities und Markets Authority. *ESMA.* URL: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/esma_de (besucht am 28. 02. 2022) (siehe S. 13).

[91] *VLAN - was ist ein virtual local area network?* URL: https://www.ionos.at/digitalguide/server/knowhow/vlan-grundlagen/ (besucht am 28. 02. 2022) (siehe S. 52).

[92] Oliver Völkel. *Neue Vorgaben für IT-Sicherheit in Banken.* URL: https://www.diepresse.com/5690299/neue-vorgaben-fuer-it-sicherheit-in-banken (besucht am 28. 02. 2022) (siehe S. 1).