Evaluierung von IT-Sicherheitsmaßnahmen an eine Bank in Österreich

Arbeitsbericht Masterprojekt

Autor: Philipp Gigler, BSc MSc

Vorgelegt am FH-Masterstudiengang Information Security Management, Fachhochschule Hagenberg

Betreuer: FH-Prof. Dr. Harald Lampesberger MSc

Salzburg, Österreich, 31.01.2022

Eidesstattliche Erklärung

Ich erkläre hiermit eidesstattlich, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, und keine anderen als die angegeben Quellen und Hilfsmittel benutzt habe. Weiter versichere ich hiermit, dass ich die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungskommission weder im In- noch im Ausland vorgelegt und auch nicht veröffentlicht.

Datum *Unterschrift*

Vorname *Nachname*

Inhaltsverzeichnis

Abkürzungsverzeichnis

BCG	Boston Consulting Group
EBA	Europäische Bankenaufsicht
IKT	Informations- und Kommunikationstechnik
FMA	Finanzmarktaufsicht Österreich
EIOPA	Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung
ESMA	Europäische Wertpapier- und Marktaufsichtsbehörde
IT	Informationstechnik
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
KWG	Kapitalwesengesetz
EU	Europäische Union

1 Einleitung

Das Thema IT-Sicherheit wird für Unternehmen immer essentieller. Speziell der Banken-Sektor stellt ein lukratives Ziel für Angreifer dar. Banken dienen als „Verteilzentren“ weltweiter Finanztransaktionen. 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 führt dazu, dass der Bereich der IT-Sicherheit oft von Einsparungen betroffen ist (Zakrzewski 2021).

Ein Cyberangriff oder Ausfall von IT-Infrastrukturkomponenten kann zu einem erheblichen finanziellen und reputationstechnischen Schaden für Finanzdienstleister und deren Partnern führen. Ein weiterer möglicher Schaden eines Cyberangriffs ist der Verlust des Vertrauens der Kunden in das betroffene Finanzinstitut. Aus diesem Grund existieren für Banken weitreichende Vorschriften betreffend die Sicherheit von IT-Systemen (Schmitt und Österreich 2021).

Die „Europäischen Bankenaufsichtsbehörde“ (EBA [2]) ist eine unabhängigen EU-Behörde mit der Aufgabe den europäischen Bankensektor zu regulieren und zu beaufsichtigen. Bezogen auf IT-Sicherheit veröffentlicht die EBA unter anderem die „Leitlinie für das Management von IKT- und Sicherheitsrisiken“ (EBA/GL/2019/04[3]).

Das Risiko eines Cyberangriffs, etwa auf die Infrastruktur eines Finanzdienstleisters, wird um einen weiteren Faktor verschärft. Vielen Finanzdienstleistern ist es nicht möglich eine eigene IT-Infrastruktur zu betreiben. Aus diesem Grunde werde häufig unterschiedliche Aufgaben an Dritte ausgelagert um Kosten zu sparen und somit einen Wettbewerbsvorteil zu lukrieren. Anstatt beispielsweise die notwendige IT-Infrastruktur selbst zu betreiben, Prozesse zu etablieren und Mitarbeiter zu beschäftigen, werden diese Aufgaben von spezialisierten Dienstleistern erbracht. Durch diese Auslagerung entsteht für das Unternehmen eine neue Art von Risiko. Neben dem tatsächlichen Ausfall von Hard- oder Software wird der gesamte Dienstleister zu einem Risiko. Dieses Risiko besteht, wenn der Dienstleister seine Leistungen nicht oder nur schlecht erbringt, oder selbst zum Einfallstor für Schadsoftware wird (Völkel 2019).

Aufgrund der steigenden Relevanz dieser Risiken hat die EBA hat im Jahr 2019 eine entsprechende Leitlinie zum Umgang mit Auslagerungs-Risiken erlassen (EBA/GL/2019/02[4]).

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[5]) veröffentlichte gemeinsam mit der EBA und der „Europäischen Wertpapier- und Mark-

1. https://www.bcg.com/de-at/
2. https://www.eba.europa.eu
3. https://www.fma.gv.at/eu/eba-leitlinien-und-andere-konvergenzinstrumente
4. https://www.fma.gv.at/eu/eba-leitlinien-und-andere-konvergenzinstrumente
5. https://www.eiopa.europa.eu

taufsichtsbehörde“ (ESMA[6]) eine Stellungnahme mit dem Titel „Joint Advice on the need for legislative improvements relating to Information and Communication Technoloy risk management requirements“ [7]. In dieser Stellungnahme werden konkreten Maßnahmen zur Harmonisierung und Konvergenz von Anforderungen an die Sicherheit der Informations- und Kommunikationstechnologie von Finanzunternehmen vorgeschlagen (*Beiträge aus den Bafinperspektiven*).

2 Problemstellung und Zielsetzung der Masterarbeit

Aufgrund der steigenden Gefahr von Cyber-Angriffen im Banken-Sektor scheint es umso wichtiger, allgemein gültige Anforderungen im Bereich IT-Sicherheit zu etablieren. Aufgrund der Komplexität des Themas IT-Sicherheit als solches ist es vielen Aufsichtsbehörden lediglich möglich ein gewisses Rahmenwerk zur Verfügung zu stellen. Genaue technische und fachliche Anforderungen und damit einhergehende Maßnahmen werden in den Anforderungen häufig nicht oder nur oberflächlich thematisiert.

Ein weiteres Problem für Finanzdienstleister besteht darin den Überblick über aktuell geltende Anforderungen und Vorgaben zu behalten. Behörden fordern von den jeweiligen Finanzdienstleistern eine IT-Sicherheitsrichtlinie zu etablieren, umzusetzen und regelmäßig zu auditieren. Die genauen Anforderungen an diese IT-Sicherheitsrichtlinie sind jedoch oft nicht spezifiziert, werden 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 weitere Hürde.

Die Masterarbeit soll als Überblick und Basis für die Implementierung einer IT-Sicherheitsrichtlinie im Banken-Sektor dienen. Es wird untersucht ob notwendige IT-Sicherheitsanforderungen mit Hilfe von Best-Practice-Ansätzen erfüllt werden können.

Im Zuge der Masterarbeit wird der Frage nachgegangen, welche Anforderungen und Vorgaben aus dem Bereich IT-Sicherheit für ein Bank-Institut in Österreich bestehen.

Im Anschluss daran werden die erhobenen Anforderungen und Vorgaben miteinander in Verbindung gebracht und kategorisiert. Daraus folgend werden mögliche fachliche und technische Maßnahmen zur Erfüllung dieser Anforderungen und Vorgaben abgeleitet.

Es 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 Erfüllung der Anforderungen und Vorgaben gemessen und auditiert werden kann.

Fazit der Masterarbeit bildet eine Matrix mit gültigen Anforderungen und Vorgaben, abgeleiteten technischen und fachlichen Maßnahmen, einer Übersicht über das jeweilig adressierte Risiko und eine Übersicht, mit welchen Best-Practice-Ansätzen diese Maßnahmen umgesetzt und auditiert werden können.

6. https://www.esma.europa.eu
7. https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf

3 Ziel des Masterprojekts

Grundlage für die Masterarbeit bietet eine Übersicht über regulatorische Anforderungen und Vorgaben für IT-Sicherheit im Banken-Sektor. Im Zuge des Masterprojekts werden die Vorarbeiten und Voraussetzungen für die Masterarbeit erarbeitet. Die Erkenntnisse aus dem Masterprojekt bilden somit einen Teil der Masterarbeit ab und werden direkt in die Masterarbeit übernommen.

Im Zuge des Masterprojekts werden die Vorgaben an IT-Sicherheit im Banken-Sektor recherchiert und miteinander in Bezug gesetzt. Um in weiterer Folge Maßnahmen zur Steigerung der IT-Sicherheit abzuleiten, findet eine Kategorisierung und Risikobewertung der Anforderungen und Vorgaben statt.

Das Fazit des Masterprojekts bildet eine Übersichtsmatrix über aktuelle Anforderungen auf Basis einer zuvor durchgeführten Kategorisierung und entsprechender Risikobewertung der adressierten Bedrohung.

Im Zuge der Masterarbeit soll Grundlagenwissen zu regulatorischen Anforderungen aus dem Bereich IT-Sicherheit für den Banken-Sektor gewonnen werden. Es werden wesentliche Anforderungen an IT-Sicherheit untersucht und notwendige Maßnahmen abgeleitet. Eines der Ziele ist eine übersichtliche und kategorisierte Darstellung der wesentlichen Anforderungen an IT-Sicherheit im Banken-Sektor, der entsprechend adressierten Risiken und der technischen bzw. fachlichen Maßnahmen.

Auf Basis dieser Übersicht kann ein Handlungsleitfaden für die Etablierung und Steigerung von IT-Sicherheit im Banken-Sektor gewonnen werden. Im Anschluss an die Ausarbeitung wird untersucht, ob sich ein allgemein gültiges Konzept ableiten lässt.

1. Muss-Ziel: Literaturrecherche zum Thema IT-Sicherheit im Banken-Sektor
2. Muss-Ziel: Literaturrecherche unterschiedlicher Normen, regulatorischer Richtlinien und Vorgaben zum Thema IT-Sicherheit im Banken-Sektor
3. Muss-Ziel: Evaluierung und Kategorisierung von Anforderungen und Vorgaben aus den Normen und Richtlinien
4. Muss-Ziel: Erstellung der Übersichtsmatrix
5. Kann-Ziel: Evaluierung adressierter Risiken

4 Übersicht über die Literatur

4.1 Bundesanstalt für Finanzdienstleistungsaufsicht – BAIT Rundschreiben

- Urheber: Bundesanstalt für Finanzienstleistungsaufsicht (BaFin[8])
- Version: 10/2017 – 16.08.2021
- Rahmenwerk: Vorgabe
- Quelle: https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.pdf?__blob=publicationFile&v=6
- Inhalt:
  - 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 über 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. Ziel ist das Vertrauen von Bankkunden, Versicherten und Anlegern in das deutsche Finanzsystem. 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 (*Beiträge aus den Bafinperspektiven*).

Auf Basis dieser Aufgaben hat die BaFin die „Bankaufsichtliche Anforderungen an die IT“ (BAIT) veröffentlicht. Diese ist aktuell in der Fassung „10/2017“ veröffentlicht. Im Zuge der

8. https://www.bafin.de/DE/Startseite/startseite_node.html

BAIT hat die BaFin Vorgaben definiert, wie Auflagen aus dem Kapitalwesengesetz (KWG[9]) von Banken und Kreditinstituten umzusetzen sind. Das Rundschreiben gibt einen Rahmen für die technisch-organisatorische Ausstattung der betroffenen Institute auf IT-Ressourcen, Informationsrisikomanagement und das Informationssicherheitsmanagement vor. Es handelt sich um eine Vorgabe bzw. einen praxisnahmen 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 270xx (*Die bafin*).

Vom KWG betroffen sind Kreditinstitute und Finanzdienstleister in der Bundesrepublik Deutschland. Aufgrund der Nähe Deutschlands zu Österreich wurde das BAIT für die Evaluierung herangezogen.

4.2 EBA – Leitlinie für das Management von IKT-Sicherheitsrisiken

- Urheber: Europäische Bankenaufsicht (EBA[10])
- Version: EBA/GL/2019/04
- Rahmenwerk: Leitlinie
- Quelle: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880810/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_DE.pdf
- 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 „Europäische Bankenaufsicht“ (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

9. https://www.gesetze-im-internet.de/kredwg/BJNR008810961.html
10. https://www.eba.europa.eu

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.

Die „Leitlinie für das Management von Informations- und Kommunikationstechnik“ Systemen legt Maßnahmen für das Management und die Verwaltung von Informations- und Kommunikationstechnik (IKT) und Sicherheitsrisiken fest. Sie umfasst Anforderungen an die Informationssicherheit und Cybersicherheit für Informationen die auf IKT-Systemen bearbeitet werden. Die Leitlinie ist für alle Zahlungsdienstleister, Kreditinstitute und Wertpapierfirmen innerhalb der Europäischen Union gültig.

4.3 EBA – Leitlinie zur Auslagerung

- Urheber: Europäische Bankenaufsicht (EBA[11])
- Version: EBA/GL/2019/02
- Rahmenwerk: Leitlinie
- Quelle: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2761380/5546a705-bff2-43eb-b382-e5c7bed3a2bc/EBA%20revised%20Guidelines%20on%20outsourcing_DE.pdf?retry=1
- Inhalt:
  - Verhältnismäßigkeit
  - Bewertung von Auslagerungsvereinbarungen
  - Rahmen für die Governance

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.

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 innerhalb der Europäischen Union gültig, wurde aber aufgrund des Fokus auf die Auslagerungsthematik nicht in die Anforderungsmatrix mit aufgenommen.

11. https://www.eba.europa.eu

4.4 EBA – Leitlinie für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses

- Urheber: Europäische Bankenaufsicht (EBA[12])
- Version: EBA/GL/2017/05
- Rahmenwerk: Leitlinie
- Quelle: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1954038/d1f46d49-6b93-4fc0-b789-839edcaafb9a/Guidelines%20on%20ICT%20Risk%20Assessment%20under%20SREP%20%28EBA-GL-2017-05%29_DE.pdf?retry=1
- Inhalt:
  - Anforderungen an die IKT-Risikobewertung
  - Bewertung der IKT-Risikopositionen und –kontrollen der Institute

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.

Die Leitlinie zielt darauf ab, die Aufsichtspraktiken bei der Bewertung des informations- und Kommunikationstechnolgie-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 mit aufgenommen.

4.5 EBA – Leitlinie zur Sicherheit von Internetzahlungen

- Urheber: Europäische Bankenaufsicht (EBA[13])
- Version: EBA/GL/2014/12
- Rahmenwerk: Leitlinie
- Quelle: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1004450/eff847ff-f1ed-4589-8efc-900cd78e2707/EBA-GL-2014-12_DE_rev1%20GL%20on%20Internet%20Payments.pdf?retry=1
- Inhalt:

12. https://www.eba.europa.eu
13. https://www.eba.europa.eu

  - Anwendungsbereich und Begriffsbestimmungen
  - Leitlinien zur Sicherheit von Internetzahlungen
  - Anhang 1: Beispiele für bewährte Vorgehensweisen

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.

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.

4.6 EIOPA – Leitlinie zur Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie

- Urheber: Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA[14])
- Version: EIOPA-BoS-20/600
- Rahmenwerk: Leitlinie
- Quelle: https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/eiopa-gls-ict-secu pdf
- Inhalt:
  - 1 – Verhältnismäßigkeit
  - 2 – IKT innerhalb des Governance-Systems
  - 3 – IKT-Strategie
  - 4 – IKT- und Sicherheitsrisiken innerhalb des Risikomanagementsystems
  - 5 – Revision
  - 6 – Informationssicherheitspolitik und -maßnahmen
  - 7 – Informationssicherheitsfunktion
  - 8 – Logische Sicherheit
  - 9 – Physische Sicherheit

14. https://www.eiopa.europa.eu

- 10 – Sicherheit des IKT-Betriebs
- 11 – Überwachung der Sicherheit
- 12 – Überprüfung, Bewertung und Testen der Informationssicherheit
- 13 – Schulungen und Sensibilisierungsmaßnahmen zum Thema Informationssicherheit
- 14 – Management des IKT-Betriebs
- 15 – Management von IKT-Vorfällen und -Problemen
- 16 – Management von IKT-Projekten
- 17 – Erwerb und Entwicklung von IKT-Systemen
- 18 – IKT-Änderungsmanagement
- 19 – Betriebliches Kontinuitätsmanagement
- 20 – Business-Impact-Analyse
- 21 –Betriebskontinuitätsplanung
- 22 – Reaktions- und Wiederherstellungspläne
- 23 –Testen der Pläne
- 24 – Krisenkommunikation
- 25 – Outsourcing von IKT-Diensten und IKT-Systemen

Die EIOPA ist die „Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung“, 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 (*Eiopa*).

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 alle Finanzunternehmen im Europäischen Wirtschaftsraum gültig. Die Anforderungen wurden jedoch aufgrund des Fokus auf Versicherungsunternehmen nicht in die Anforderungsmatrix mit aufgenommen (*Eiopa*).

4.7 ESMA – Leitlinie zur Auslagerung an Cloud Anbieter

- Urheber: Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA[15])

15. https://www.esma.europa.eu

- Version: Nicht verfügbar
- Rahmenwerk: Leitlinie
- Quelle: https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines_de.pdf
- Inhalt:
  - Geltungsbereich
  - Rechtsrahmen, Abkürzungen und Begriffsbestimmungen
  - Zweck
  - Einhaltung der Vorschriften und Berichtspflichten
  - Leitlinien zur Auslagerung an Cloud-Anbieter

Die „Europäische Wertpapier- und Marktaufsichtsbehörde“ (ESMA) verbessert den Anlegerschutz und fördert stabile, geregelt funktionierende Finanzmärkte im Europäischen Wirtschaftsraum. Sie ist eine unabhängige EU-Behörde mit Sitz in Paris. Die ESMA stellt sicher, dass die Bedürfnisse der Verbraucher umfassend berücksichtigt, deren Rechte gestärkt aber auch deren Verantwortlichkeit anerkannt werden. Sie 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. Da die Auslagerung von Diensten und Services, für Banken in Österreich, nicht unbedingt erforderlich ist, wurde die Leitlinie nicht in die Anforderungsmatrix übernommen.

4.8 FMA – Leitfaden IT-Sicherheit in Verwaltungsgesellschaften

- Urheber: Finanzmarktaufsicht Österreich (FMA[16])
- Version: Nr. 02/2020
- Rahmenwerk: Leitfaden
- Quelle: https://www.fma.gv.at/download.php?d=3597
- Inhalt:
  - Rechtsgrundlagen und grundlegendes
  - IT-Strategie

16. https://www.fma.gv.at

  - 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 unter einer Aufsicht (*Finanzmarktaufsicht*).

Die FMA ist sich der immer bedeutender werdenden Möglichkeiten und Risiken, welche aus der IT resultieren, bewusst und sieht aufgrund der gestiegenen Risikolage die Notwendigkeit gegeben den Verwaltungsgesellschaften einen Überblick über Ausgestaltung, Anforderungen und Vorkehrungen betreffend die IT-Sicherheit als Orientierungshilfe 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 fördern (*Finanzmarktaufsicht*).

4.9 FMA - Leitfaden IT-Sicherheit in Wertpapierdienstleistungsunternehmen und Wertpapierfirmen

- Urheber: Finanzmarktaufsicht Österreich (FMA[17])
- Version: Nr. 04/2018
- Rahmenwerk: Leitfaden
- Quelle: https://www.fma.gv.at/download.php?d=3597
- Inhalt:
  - Rechtsgrundlagen und grundlegendes

17. https://www.fma.gv.at

- 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 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 unter einer Aufsicht (*Finanzmarktaufsicht*).

Die FMA ist sich der immer bedeutender werdenden Möglichkeiten und Risiken, welche aus der IT resultieren, bewusst und sieht aufgrund der gestiegenen Risikolage die Notwendigkeit gegeben den Verwaltungsgesellschaften einen Überblick über Ausgestaltung, Anforderungen und Vorkehrungen betreffend die IT-Sicherheit als Orientierungshilfe 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 fördern (*Finanzmarktaufsicht*).

4.10 EU – 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)

- Urheber: Europäische Union
- Version: 2015/2366 auf Basis 2007/64/EG
- Rahmenwerk: Verordnung
- Quelle: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32015L2366&from=DE

- Inhalt:
  - Nicht verfügbar

Die Verordnung legt Anforderungen für Zahlungsdienstleister für die Umsetzung von Sicherheitsmaßnahmen fest. Definiert wird, wie das Verfahren zur starken Kundenauthentifizierung anzuwenden ist und unter welchen Voraussetzungen von einer starken Kundenauthentifizierung abzusehen ist. Des Weiteren wird definiert wie die Vertraulichkeit und die Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer geschützt werden müssen. Die Verordnung ist für alle Zahlungsdienstleister im Europäischen Wirtschaftsraum gültig.

5 Anforderungsmatrix

5.1 Vorgehen

Für die Erstellung der Anforderungsmatrix wurden in erster Instanz alle Richtlinien aus Kapitel 4 evaluiert und niedergeschrieben. Aus Gründen der Vollständigkeit wurden sämtliche Anforderungen in die Matrix übernommen und der Fokus nicht nur auf technisch-umsetzbare Anforderungen gelegt. Im zweiten Schritt wurden die Anforderungen entsprechend nach Themen gruppiert und kategorisiert. Für die Kategorisierung wurde ein passendes Themengebiet gewählt, das alle enthaltenen Anforderungen bestmöglich umschreibt.

Im nächsten Schritt wurde festgelegt, ob es sich bei der Anforderung um eine allgemeine oder eine Banken-spezifische Anforderung handelt. Diese Einteilung verfolgt den Zweck, dass die Anforderungen, die speziell an eine Bank gerichtet sind, im Nachgang eindeutig erkennbar sind. Im Zuge der Evaluierung der Richtlinien hat sich gezeigt, dass viele Anforderungen allgemeiner Natur sind und auch von Unternehmen umgesetzt werden sollten, die keine Bank etablieren möchten. Des Weiteren wurde hinterlegt, ob die Anforderung für Unternehmen in der Europäischen Union, Österreich oder anderen Ländern gilt.

Im vierten Schritt wurde jede Anforderung ein Risikofaktor zugewiesen. Im Zuge der Evaluierung haben sich folgende Risikofaktoren herauskristallisiert:

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

5.1.1 Technischer Risikofaktor

Dieser Risikofaktor wurde vergeben, wenn die Anforderung auf den Schutz von Vertraulichkeit, Integrität und Verfügbarkeit des zu schützenden Assets ausgelegt ist.

5.1.2 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.

5.1.3 Menschlicher Risikofaktor

Anforderungen mit diesem Risikofaktor dienen dem Schutz von Mitarbeitern und Kunden des Unternehmens.

5.1.4 Rechtlicher Risikofaktor

Anforderungen mit diesem Risikofaktor schützen vor Imageverlust, Strafgebühren, Strafverfolgung oder monetären Schäden.

Im letzten Schritt wurde Bezug auf die Umsetzbarkeit der einzelnen Anforderungen genommen. Unterschieden wird hierbei, ob sich die Anforderung organisatorisch und / oder technisch realisieren lässt. Im Zuge dessen wurde eine erste grobe Evaluierung unternommen, mit welchen Maßnahmen sich die Anforderung umsetzen lassen kann.

5.2 Beschreibung der Anforderungsmatrix

In folgendem Kapitel werden die Bestandteile der Anforderungsmatrix näher beschrieben.

- Allgemeines
  - # - Fortlaufende Nummerierung der Anforderungen
  - Kategorie - Evaluierte Kategorie der Anforderung
  - Titel der Anforderung - Kapitel / Titel der Anforderung
  - Definition - Nähere Beschreibung der Anforderung
  - Beschreibung - Genaue Beschreibung, Wer, Wann, Was zu tun hat um der Anforderung gerecht zu werden
  - Referenz - Kapitel / Referenz in Richtlinie
- Institution
  - Institut - Herausgeber der Richtlinie
  - Typ - Art der Richtlinie
  - Dokument - Referenz auf Richtlinie
  - Version / Fassung - Verwendet Version der Richtlinie

- Anforderung
  - Allgemein - Es handelt sich um eine allgemeine Anforderung
  - Bank - Es handelt sich um eine Banken-spezifische Anforderung
  - EU - Anforderung ist für die Europäische Union
  - AT - Anforderung ist für Österreich gültig
  - Andere - Anforderung ist für andere Länder gültig
- Risiko
  - Risikofaktor - Beschreibt den adressierten Risikofaktor der Anforderung
- Umsetzbarkeit
  - Technisch - Die Anforderung ist technisch umsetzbar
  - Beschreibung - Beschreibung der technischen Umsetzbarkeit
  - Organisatorisch - Die Anforderung ist organisatorisch umsetzbar
  - Beschreibung - Beschreibung der organisatorischen Umsetzbarkeit
  - Abgedeckt durch Maßnahme - Konkrete Best-Practice-Maßnahme für die Umsetzung (wird im Zuge der Masterarbeit evaluiert)

6 Fazit Masterarbeit

6.1 Zielerfüllung

Im Zuge des Masterprojekts wurde eine umfassende Literaturrecherche zum Thema IT-Sicherheit im Banken-Sektor durchgeführt. Auf Basis von gewonnenen Erkenntnissen wurde nach Normen, regulatorische Richtlinien und Vorgaben zum Thema IT-Sicherheit im Banken-Sektor recherchiert, diese evaluiert und auf Basis der enthaltenen Informationen die Anforderungsmatrix generiert. Die in den Normen, Richtlinien und Vorgaben enthaltenen Anforderungen wurden in weiterer Folge in die Anforderungsmatrix übernommen. Die Anforderungen wurden kategorisiert und mit weiteren Informationen vervollständigt. Auf Basis der gewonnenen Erkenntnisse wurden adressierte Risiken evaluiert und entsprechend den Anforderungen zugewiesen.

Die Anforderungsmatrix bietet somit die erforderliche Grundlage für die Masterarbeit.

6.2 Persönlicher Erkenntnisgewinn

Zu Beginn des Masterprojekts war ich mir nicht sicher in welchem Umfang sich die Matrix bewegen wird. Aus eigener Erfahrung aus meinem beruflichen Umfeld wusste ich, wie unstrukturiert Anforderungen an eine Bank in Österreich gestellt werden. Mit steigendem Umfang der

Anforderungsmatrix hat sich jedoch ein Muster herauskristallisiert. Die Anforderungen der unterschiedlichen Normen, regulatorischen Richtlinien und Vorgaben sind in den einzelnen Richtlinien sehr ähnlich formuliert und abgebildet. Auch ist zu erkennen, dass sich die Anforderungen sehr gut durch die zwölf gefundenen Kategorien beschreiben lassen. Dadurch lässt sich die Komplexität erheblich reduzieren. Eine interessante Erkenntnis war, dass sich der Großteil der Anforderungen im organisatorischen bzw. Governance-Bereich bewegen. Nur ein Bruchteil ist per se technischer Natur. In wie weit und zu welchem Prozentsatz sich auch die organisatorischen Maßnahmen technisch abbilden lassen, werde ich im Zuge der Masterarbeit evaluieren.

Literaturverzeichnis

Beiträge aus den Bafinperspektiven. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/BaFinPerspektiven/2020/bp_20_1_Brueggemann_Kocatepe.html.

Die bafin. https://www.bafin.de/DE/DieBaFin/diebafin_node.html.

Eiopa. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/eiopa_de.

Finanzmarktaufsicht. https://www.bmf.gv.at/themen/finanzmarkt/finanzmarktaufsicht.html.

Schmitt, Armin, und EY Österreich. 2021. *Was Macht Banken für datendiebstahl und cyberangriffe besonders interessant?*, Mai. https://www.ey.com/de_at/cybersecurity/was-macht-banken-fuer-datendiebstahl-und-cyberangriffe-besonders-interessant.

Völkel, Oliver. 2019. *Neue Vorgaben für it-sicherheit in Banken*, September. https://www.diepresse.com/5690299/neue-vorgaben-fuer-it-sicherheit-in-banken.

Zakrzewski. 2021. *Global wealth 2019: Reigniting Radical Growth*, Januar. https://www.bcg.com/publications/2019/global-wealth-reigniting-radical-growth.

Appendices

A git-Repository

In diesem Git-Repository sind folgende Inhalte hinterlegt:

- Latex-Source Code als .zip
- Arbeitsbericht in PDF-Form
- Zeiterfassung in PDF-Form
- Anforderungsmatrix

Link zum Repository: https://github.com/sikoqdos/masterprojekt_ISM2.git