Hausarbeit: Vorgehen und technische Umsetzung von Online-Banking Betrugsmaschen

Name: Kai Pistol
Matrikelnummer: 7347867, EY
s211298@student.dhbw-mannheim.de

Hausarbeit

Vorgehen und technische Umsetzung von Online-Banking Betrugsmaschen

Inhalt

1. Abstract

In den letzten Jahren hat sich das Online-Banking zu einer beliebten und bequemen Möglichkeit entwickelt, Finanzgeschäfte durchzuführen. Online-Banking ermöglicht es der Gesellschaft, von überall und jederzeit auf die eigenen Konten zuzugreifen und Transaktionen durchzuführen. Allerdings birgt das Online-Banking auch einige Risiken, insbesondere in Bezug auf Betrug. Cyberkriminelle nutzen immer fortgeschrittenere Techniken, um an sensible Finanzinformationen zu gelangen und Geld von Konten zu stehlen. In dieser Arbeit wird sich mit den verschiedenen Formen von Betrug im Online-Banking-Bereich auseinandergesetzt. Darüber hinaus wird tiefer auf die Historie der Sicherheits- und Authentifizierungsmethoden, sowie die Gesetzeslage und Strafaussichten eingegangen. Ebenso werden auf das Vorgehen und die technische Umsetzung der Betrüger eingegangen und untersucht, wie sich Personen davor schützen können.

2. Einleitung

2.1. Bedeutung der Banken in unserer Gesellschaft

Historisch waren Banken schon immer als Ort der Vermögensverwaltung, Kreditgeschäfte und des Zahlungsverkehrs bekannt. Über Jahrhunderte hinweg baute sich das Vertrauen der Menschen in Banken auf. Geld diente immer mehr als Sicherheit, jedoch wurde der Bedarf nach der Sicherung des Geldes auch immer größer. Im 11. Jahrhundert wurde die Gefahr durch Seeräuber in der Region Venedig immer größer, welcher auf offener See Bargeld in Form von Silber und Goldmünzen stahlen. Die Idee des bargeldlosen Zahlungsverkehrs wurde geboren. Das damalige Konzept sah vor, dass der Käufer dem Verkäufer eine Summe auf einem Brief notierte, welche der Verkäufer im Folgenden bei teilnehmenden Banken abholen konnte. Ebenfalls wurde dadurch auch die Möglichkeit auf Falschgeld bei einem Handel eliminiert, da die Bank das Geld bereits geprüft hatte. Somit etablierte sich schnell die Grundidee des Schecks. [1]

2.2. Entwicklung des Zahlungsverkehrs

Eine Studie des Zahlungsdienstes Klarna aus dem Jahr 2021 hat ergeben, dass Deutschland in Sachen bargeldloser Bezahlung im internationalen Vergleich mit 38% immer noch weit hinten liegt. Jedoch ändert sich das Zahlverhalten der Deutschen. [2] Dies zeigt eine Studie der Bundebank auf. Dafür wurden in den Jahren 2008, 2011, 2014, 2017, 2020 und 2021 5870 Personen befragt und ihnen 50 Fragen zu ihrem Zahlungsverhalten, sowie ihrer Einstellung bezüglich Themen wie Online-Banking oder dem Verhalten mit Bargeld gestellt. Die durch die Umfrage erhobenen Daten zeichnen einen repräsentativen Verlauf zur Akzeptanz zum Thema Online-Banking ab, geben Aufschluss, welche Gedanken die Befragten dazu haben und zeigen auf, wie sich die Akzeptanz von bargeldlosen Alternativen in den folgenden Jahren entwickeln könnte. So lässt sich zunächst aufzeigen, dass im Vergleich zu 2017 die Akzeptanz der Befragten zu Online-Banking deutlich gestiegen ist (Abbildung 1 Anstieg Akzeptanz von Online-Banking). [3, S. 15] Des Weiteren zeigt die Umfrage auch auf, dass im Jahre 2021 58% der Befragten das sogenannten Mobile-Banking[1] nutzten, was 10% mehr gegenüber dem Vorjahr waren (Abbildung 2 Nutzung Online-Banking/ Mobile-Banking) [3, S. 15] Auch zeigt sie, dass sich ein demografischer Wandel,

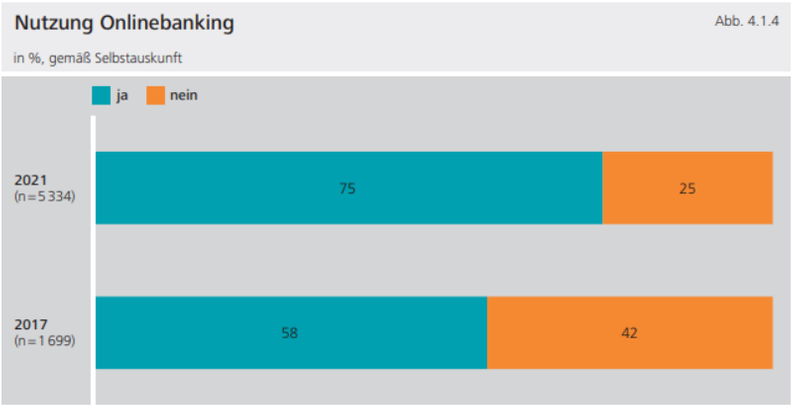

Abbildung 1 Anstieg Akzeptanz von Online-Banking

[1]Mobile-Banking beschreibt die Verwendung von Online-Banking durch eine von dem Finanzinstitut bereitgestellte App für das Smartphone.

hin zum Online-Banking ableiten lässt. Durchschnittlich 75% aller Befragten gaben an, Online-Banking regelmäßig zu nutzen. Dabei war die Gruppe der 18 bis 54-Jährigen über den Durchschnitt, was die regelmäßige Nutzung betraf.

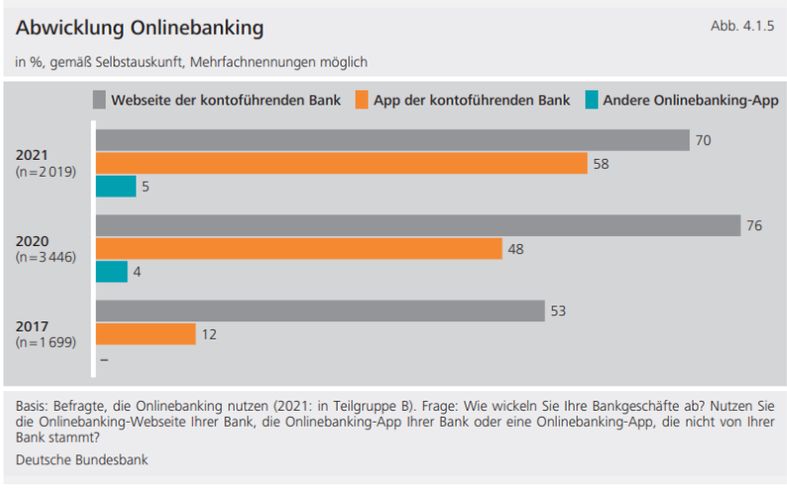

Abbildung 2 Nutzung Online-Banking/ Mobile-Banking

Darüber hinaus zeigt die Statistik auch auf, dass sich ein Verweis zwischen regelmäßiger Online-Banking Nutzung und der Höhe des Einkommens aufzeigen lässt. So befassen sich besonders die Personen häufiger mit Online-Banking, welche ein Einkommen ab 3000€ netto pro Monat haben (Abbildung 3 Nutzung Online-Banking nach Alter & Gehalt). [3, S. 44]

Bargeld wird mit einem Durchschnitt von 30% zwar immer noch als bevorzugtes Zahlungsmittel verwendet, allerdings findet dies nur bei der Bevölkerungsgruppe der 55-Jährigen und steigend noch überdurchschnittlichen Anklang. [3, S. 12]

Insgesamt zeigt die Datenerhebung der Bundesbank also auf, dass der Trend immer weiter hin zum digitalen Bezahlen geht, sei es in Form von Online-Banking oder Kartenzahlung. Ein Umdenken der Gesellschaft findet bereits statt und wurde gerade durch die notwendigen Umstellungen im Rahmen der COVID-19 Pandemie in den vergangenen Jahren bestärkt. Die Akzeptanz von bargeldlosen Transaktionen in Geschäften des täglichen Bedarfs, wie Bäcker und Fleischer, ist seitdem fortan gestiegen.

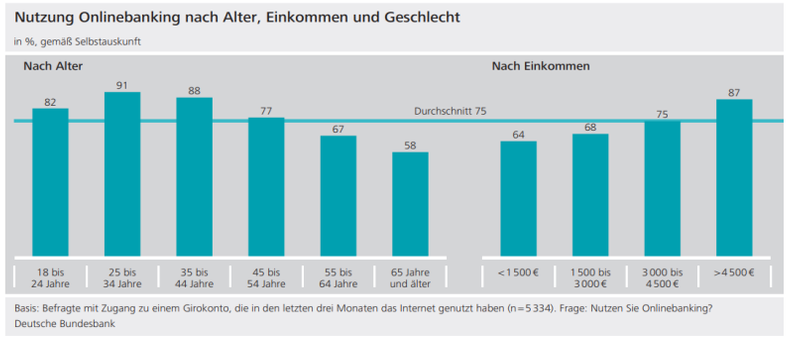

Abbildung 3 Nutzung Online-Banking nach Alter & Gehalt

2.3. Aktuelle Bedrohungslage

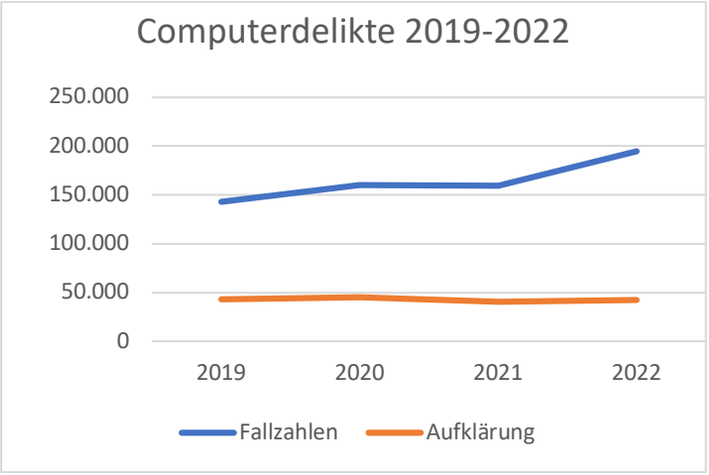

Abbildung 4 PKS Auswertung Computerbetrug 2019 - 2022

Dass die Onlinebetrugsdelikte ein immer größeres Gefahrenpotenzial darstellen, war durch die breite Digitalisierung in unserer Gesellschaft bereits anzunehmen. Diese These wurde aber noch zusätzlich durch die Fallzahlen in den vergangenen Jahren untermauert. Dies lässt sich mit Unter auch auf COVID-19 Pandemie zurückführen, wodurch die Onlinegeschäfte zusätzlich florierten. Die polizeiliche Kriminalstatistik (PKS) gibt darüber einen besseren Aufschluss. Diese wird jährlich vom Bundeskriminalamt veröffentlicht und gibt Auskunft unteranderem über Fallzahlen, Aufklärungszahlen und Ort des Verbrechens auf In- sowie Ausland oder Bundesland. In Rahmen dieser Arbeit, wurden die Jahre 2019 bis 2022 ausgewertet und die Fallzahlen aller Online-Straftaten analysiert und in ein Verhältnis zu den Vor- beziehungsweise den Folgejahren gestellt. Dabei konnte nicht nur ein Anstieg der Fallzahlen von 142.951 aus 2019 auf 194.768 im Jahr 2022 festgestellt werden, sondern auch dass die Aufklärungsrate in Prozent der Polizei sogar leicht sinkt (Abbildung 4 PKS Auswertung Computerbetrug 2019 – 2022). Die Masse der Taten und die Anonymität der Täter im Internet und die Möglichkeit, länderübergreifend zu agieren, erschwert die Aufklärungsarbeit der Polizei zusätzlich. Besonders der Anstieg von Onlinekäufen und demnach auch das elektronische Bezahlen von Rechnungen, macht für den Kunden besonders attraktiv das Online-Banking zu nutzen. Jedoch öffnet es auch Spielraum für Kriminelle, welche dieses System ausnutzen wollen. Diese Entwicklung war schon 2020 absehbar.[4]–[7] So gab am 02.04.2020 das Bundesamt für Sicherheit in der Informationstechnologie (BSI) bereits eine Warnung heraus, dass es aufgrund der COVID-19 Pandemie verstärkt zu Online-Banking Betrug kommt.[8] Ein ähnliches Bild wird ebenfalls von einer Analyse der Firma Fico gezeichnet. Diese erhob für die Jahre 2005 bis 2021 Daten zu verschiedenen Arten des Kreditkartenbetrugs. Dabei wurden auf Basis einzelner europäischer Länder Daten erhoben, durch das Marktforschungsinstitut Euromonitor International. In der Gesamtauswertung geht klar hervor, dass Deutschland 2021 eine Summe von 119,4 Mio. Euro Schadenshöhe in Kreditkartenbetrug zu verzeichnen hatte.

Darüber hinaus zeigt die Auswertung ebenfalls auf, dass dies das größte Einfallstor für Kriminelle auf diesem Gebiet darstellt.[9]

International gesehen ist Deutschland allerdings kein Einzelfall. Dadurch, dass Täter global agieren, werden folglich auch global Banken angegriffen. So gab es in Großbritannien 2019 bereits einen Anstieg von 64% im Bereich Online-Banking Betrug. Es wird davon ausgegangen, dass die Schadenssumme bei ca. 600 Mio. £ in diesem Zeitraum lag. Nur ein Jahr später, 2020 wurden 2,3 Millionen Straffälle polizeilich gemeldet. Dabei ist die Gesamtschadenssumme der Überweisungen durch autorisierte App (konkreter in Kapitel 5.3 TAN-Verfahren erläutert) allein auf 479.000.000£ zu schätzen. Dies verdeutlicht, wie viel Potenzial und Geld in dieser Form von Cyber-Kriminalität stecken.[10]

Richtet man den Blick auf die USA so wurden im Jahr 2021 1.686.121 Fälle von Identitätsdiebstahl in Verbindung mit einer finanziellen Bereicherung gemeldet wovon sich 389.845 auf Kreditkartenbetrug und 124.497 Bankenbetrug zurückführen ließen. Während der Kreditkartenbetrug aufgrund von stetig verbesserten Sicherheitsmechanismen, wie das Geo-Blocking[2] und besseren Authentifizierungsmaßnahmen, um 1% zurück ging, wuchs der Bankenbetrug um 39% zum Vorjahr an. Hochrechnungen gehen davon aus, dass sich allein der Schaden in den USA im Bereich des Bankenbetrugs aus dem Jahr 2020 auf ca. 1.67 Milliarden Dollar belief.[10], [11]

Zusammenfassend lässt sich nach Auswertung der Daten schließen, dass die Gefahr von Online-Banking Betrugsmaschen und damit verbunden auch des Identitätsdiebstahls unweigerlich steigen werden, dies ist mitunter auch der COVID-19 Pandemie geschuldet. Es sowohl den Banken als auch an den Kunden daran gelegen, für mehr Sicherheit im Umgang mit digitalen Transaktionen sorgen. Wie dies erreicht wird, wird im folgenden Kapitel 4 Absicherung des Kundengeschäfts durch die Banken beschrieben.

[2] Überprüfen der geographischen Lage der IP-Adresse bei einer Transaktion zur Erkennung von ungewöhnlichen Bestellverhalten.

3. Anforderungen an die IT - Informationssicherheit der Banken

Um zu verstehen, weshalb Banken weniger Opfer von Cyberkriminalität als ihre Kunden werden, muss zunächst erläutert werden, welchen Auflagen Finanzunternehmen unterliegen und wie diese zur Härtung der IT-Systeme beitragen. Kreditinstitute sowie Finanzunternehmen im Allgemeinen, sind durch ihre Arbeit als KRITIS[3]-Unternehmen[12] eingestuft und somit an eine Vielzahl von Rechtsvorschriften gebunden, um den Schutz Dieser sicherzustellen. Im Rahmen dieser Arbeit werden die Auflagen nun herausgearbeitet, welche Auswirkungen diese auf die Unternehmen haben und welcher Zweck damit verfolgt wird. Ziel dessen ist es aufzuzeigen, dass Banken durch ihre Rolle als KRITIS Unternehmen als besonders schützenwert gelten und diese somit hohen gesetzlichen und regulatorischen Anforderungen unterliegen, was ein hohes Maß an Sicherheit der IT-Infrastruktur mit sich führen muss.

3.1. KWG

Das Kreditwesengesetz (KWG) definiert ebenfalls Anforderungen an deutsche Banken. Zu dessen wichtigsten Aufgaben gehört unter anderem:

- Banken zu verpflichten Risiko-Strategie zu erstellen
- Banken zur Einhaltung aufsichtsrechtlicher Regelungen zu aufzufordern
- Definieren von aufsichtsrechtlichen KPIs
- Mindestanforderungen an das Risikomanagement der Bank zu stellen.

Diese Anforderungen des KWG bilden dabei die Grundlage der MaRisk und der BAIT, sowie deren Erweiterungen wie etwa KAIT und ZAIT, welche die Anforderungen deutlich mehr konkretisieren.[13], [14]

[3] Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

3.2. MaRisk

Die MaRisk[4] ist ein Rundschreiben der BaFin[5] zur Durchsetzung von Mindeststandards an die IT von Finanzinstituten. Dies ist bindend für alle nationalen Bankinstitute und kann bei nicht einhalten von der BaFin mit Bußgeldern oder im äußersten Fall mit der Handelsaussetzung geahndet werden.
Im Rahmen der MaRisk sind besonders die Kapitel AT 7 Ressourcen, sowie AT 9 Auslagerung relevant für den Umgang der Bank mit ihrer IT-Infrastruktur und den benötigten Diensten.

AT 7 Ressourcen lässt sich in 3 Unterpunkte unterteilen:

- AT 7.1 Personal – setzt sich mit der quantitativen Personalausstattung der Finanzunternehmen auseinander und mit den qualitativen Kenntnissen der Mitarbeiter. Demnach sollten die IT-Organisationen, welche sich mit risikobehafteten Bereichen der Bank beschäftigen, entsprechend personell bestückt und geschult sein, um Sicherheitskonzepte korrekt umzusetzen und im Krisenfall schnell reagieren zu können.

- AT 7.2 Technisch-organisatorische Ausstattung – Die technische Ausstattung der Bank muss den reibungslosen Ablauf der notwendigen Prozesse, die zur Aufrechterhaltung des Geschäftsbetriebs notwendig sind, gewährleisten. Des Weiteren ist sicherzustellen, dass Informationen den drei Prinzipien, Integrität, Verfügbarkeit und Authentizität, unterliegen. Dafür sollte ein entsprechendes Rollenkonzept erarbeitet werden, welches den Mitarbeitern nur die Daten zur Verfügung stellt, welche sie für ihre Arbeit benötigen. Um die Funktionalität und Sicherheit von Soft- sowie Hardware zu gewährleisten, ist das Etablieren einer Testumgebung für diese notwendig, welche von der Produktivumgebung klar abgetrennt ist. Darüber hinaus muss ein Freigabeprozess definiert sein, welcher eine Vertestung, sowie die Behebung von Fehlern vorsieht. Um die IT abzusichern, müssten besonders schützenswerte Daten, sowie Hardware definiert werden und Konzepte zum Schutze dieser erarbeitet

[4] MaRisk - Mindestanforderungen an das Risikomanagement

[5] Bundesanstalt für Finanzdienstleistungsaufsicht

werden. Eine Bewertung des Risikos muss angemessen nach herausgestellten Kriterien erfolgen.

- AT 7.3 Notfallmanagement – Die Finanzunternehmen sind dazu veranlasst konkrete Notfallpläne zu verschiedenen Szenarien zu konzipieren. Diese können vom Eintreffen von Naturkatastrophen bis hin zu Cyberattacken reichen. Zusätzlich dazu, müssen die Banken ebenfalls über Geschäftsfortführungs- und Wiederherstellungspläne verfügen, welche die Zurückführung in das normale Tagesgeschäft sicherstellen sollen. Um die Wirksamkeit der Konzepte zu bestätigen ist es notwendig, dass die Pläne auf ihre Wirksamkeit überprüft und gegebenenfalls angepasst werden.

AT 9 Auslagerung befasst sich mit den Voraussetzungen für das Auslagern von Dienstleistungen und definiert die Anforderungen an die Finanzunternehmen und ihre Dritt-Dienstleister. So wird im Punkt AT 9.1 klar definiert, wann eine Auslagerung vorliegt:

> „Eine Auslagerung liegt vor, wenn ein anderes Unternehmen mit der Wahrnehmung solcher Aktivitäten und Prozesse im Zusammenhang mit der Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen beauftragt wird, die ansonsten vom Institut selbst erbracht würden. Zivilrechtliche Gestaltungen und Vereinbarungen können dabei das Vorliegen einer Auslagerung nicht von vornherein ausschließen.“ - Rundschreiben 10/2021 (BA) - Mindestanforderungen an das Risikomanagement – MaRisk[15]

Darüber hinaus ist das Finanzunternehmen verpflichtet, die zu outsourcenden Prozesse einer Risikoanalyse zu unterziehen und eine entsprechende Bewertung der Prozesse vorzunehmen, um festzustellen, ob es sich dabei um eine wesentliche bzw. nicht wesentliche Auslagerung handelt. In diesem Prozess ist die interne Revision zwingend mit einzubeziehen. Sollte es sich dabei um eine nicht wesentliche Auslagerung handeln, so ist der Prozess trotzdem in die Festlegung der Strategien und in die nachhaltige Entwicklung des Instituts mit einzubinden nach §25a Abs.1 KWG[6].[14], [15] Grundsätzlich sind Prozesse und Aktivitäten auslagerbar, jedoch ist das Finanzunternehmen trotzdem weiterhin für die Einhaltung, die

[6] KWG - Kreditwesengesetz

Risikobewertung, sowie für die Überwachung verantwortlich. Sollten Auslagerungen vorgenommen werden, so ist ein Auslagerungsbeauftragter zu benennen, welcher sich um Kontroll- und Überwachungsprozesse, Dokumentation sowie Vertragserstellung, Unterstützung der Fachbereiche, Koordination und Durchführung der Risikoanalyse kümmert. Zum Zwecke der Kontrolle und der Übersichtlichkeit, muss die Bank ein Auslagerungsregister erstellen, welches die ausgelagerten Prozesse, Firmen und die dazugehörigen Auslagerungsvereinbarungen enthalten.[15]

3.3. BAIT

Die BAIT[7] richtet sich an die Geschäftsleitung von Finanzunternehmen und spiegelt die Erwartungshaltung der BaFin in Bezug auf die Sicherheit der IT-Systeme der Bank [16]wider. Die BAIT vertieft dabei die in der MaRisk regulatorischen Anforderungen und geht weiter auf das KWG ein. Dabei wird besonders die Organisation und Handhabung der Hard-/ bzw. Software konkretisiert, aber auch die Anforderungen an das Risikomanagement der Bank. Im Folgenden werden primär die Kapitel, Informationsrisikomanagement, Informationssicherheitsmanagement und IT-Notfallmanagement der BAIT befasst, da sich diese inhaltlich mit den Themen Schutz und die Wiederherstellung von IT-Systemen befassen.

- **Informationsrisikomanagement** – Befasst sich mit der Verarbeitung und der Weitergabe von Informationen. Im Vordergrund stehen dabei die Verfügbarkeit, Vertraulichkeit und die Authentizität der Daten, zu jedem Zeitpunkt der Prozesse. Im Rahmen der Verarbeitung der Daten sind die Aufgaben und Kompetenzen der Mitarbeiter der für das Aufgabengebiet verantwortlichen Abteilung zu bestimmen, sowie Überwachungs- und Steuerungsprozesse einzurichten. Das Finanzinstitut muss jederzeit über einen Überblick der IT-Systeme und -Prozesse, sowie über die Netzinfrastruktur und die Geschäfts- und Unterstützungsprozesse verfügen. Dies beinhaltet auch die an andere Dienstleister abgegebenen Prozesse sowie die Schnittstellen zu diesen. Um für die Systeme einen Schutzbedarf zu definieren ist es notwendig, dass regelmäßig anlassbezogene Risikoanalysen der Systeme und Prozesse vollzogen werden. Die dazugehörigen Dokumentationen sind ebenfalls in die Schutzbedarfsanalyse mit einzubeziehen. Dies dient der Wahrung der Sicherheitsziele:

[7] Bankenaufsichtliche Anforderungen an die IT

Verfügbarkeit, Vertraulichkeit und Integrität, da durch die Analysen und Dokumentation gegebenenfalls Konfigurations-/ Entwicklungsfehler aufgezeigt werden können, wodurch Schaden präventiv vorgebeugt werden kann. Sollten bei der Risikoanalyse Beanstandungen auftreten, sind für diese entsprechende Maßnahmen zu definieren, sodass das Schadenspotenzial gesenkt wird. Infolgedessen müssen die definierten Maßnahmen auch durch die verantwortlichen Fachbereiche umgesetzt werden. Das Risikomanagement des Instituts ist verpflichtet, sich ein aktuelles Bild über das Bedrohungspotenzial der Bank zu verschaffen, ausschlaggebend hierfür können koordinierte Cyberangriffe, Statistiken von Angriffen und Angriffsversuche der vergangenen Monate oder auch aktuelle Exploits[8] sein. Das Risikomanagement hat aus seinen Erkenntnissen konkrete Soll-Maßnahmen zu generieren, die zur Minderung der Eintrittswahrscheinlichkeit, der Auswirkungen im Eintrittsfall und der Schadenshöhe führen sollen. Die Geschäftsführung ist in regelmäßigen Abständen (mindestens alle 3 Monate) über die Ergebnisse der Risikoanalyse und die Bedrohungslage zu informieren und hat darüber hinaus auch die Befugnis, ein Risiko als hinnehmbar zu deklarieren, was zur Folge hat, dass keine Sollmaßnahmen für dieses ergriffen werden müssen. [16, S. 6–8]

- **Informationssicherheitsmanagement** – Befasst sich mit dem Erstellen von Vorgaben für die Informationssicherheit, definieren von Prozessen und der Steuerung der Umsetzung. Wie das Informationsrisikomanagement auch, ist das Informationssicherheitsmanagement zur regelmäßigen Berichtserstattung an die Geschäftsführung verpflichtet. Die Ziele in der Übersicht:
    - Verfügbarkeit → Daten sollen zu jedem Moment abrufbar sein
    - Vertraulichkeit → Daten sollen nur von den Personen einsehbar sein, die sie für Ihre Arbeit benötigen, demnach soll unautorisierter Zugriff untersagt werden
    - Integrität → Daten sollen nicht unbemerkt und unautorisiert manipuliert werden
    - Authentizität → Daten müssen eindeutig identifizierbar sein und können dabei charakteristische Eigenschaften aufweisen, welche überprüfbar sind. [17]

[8] Sicherheitslücke oder Schadprogramm, welches auf eine Sicherheitslücke zurückgreift

Das Informationssicherheitsmanagement hat für sein Vorgehen eine Richtlinie zu definieren, welches einerseits die Gesamtverantwortung der Abteilung definiert und andererseits die Frequenz und den Umfang des Berichtswesens festlegt. Ebenfalls müssen in der Richtlinie die Kompetenzen im Umgang mit den Informationsrisiken festgelegt werden, sowie die Anforderungen an das Personal sowie Auftragnehmer, Prozesse, System-/Sicherheitstests und Technologien der Abteilung bzw. des Unternehmens bestimmt werden. Die Aufgabe des Informationssicherheitsmanagements besteht ebenfalls darin, Vorgaben zu Themen wie Kryptografie, Rechtemanagement oder der Netzwerksicherheit zu machen. Ziel dessen ist, dass präventive Vorgehen, gegen Informationssicherheitsvorfälle.
Um die Umsetzung der getroffenen Maßnahmen zu koordinieren ist ein Informationssicherheitsbeauftragter durch das Unternehmen zu bestimmen. Dieser ist unteranderem auch für die Erstellung und Pflege der Richtline und für die Sensibilisierung der Mitarbeiter in Themen der IT-Sicherheit verantwortlich. Im Falle eines Informationssicherheitsvorfall ist es die Aufgabe des Informationssicherheitsmanagements, den Vorfall im Nachhinein zu untersuchen und entsprechende Vorkehrungen zu treffen, sodass sich eine solche Störung nicht wiederholen kann.[16, S. 9–13]

- **Operative Informationssicherheit** – setzt die Anforderungen des Informationssicherheitsmanagements um und sorgt ebenfalls für die Einhaltung deren Sicherheitsziele. Der Bereich sorgt für die Überwachung und Steuerung der IT-Risiken, sowie der Festlegung des Schutzbedarfs und daraus abzuleitende Maßnahmen. Die Aufgaben und Ziele der Informationssicherheitsmaßnahmen und Prozesse sind durch Abbildung 5 „Aufgaben der Operativen Informationssicherheit“ anschaulich verdeutlicht.

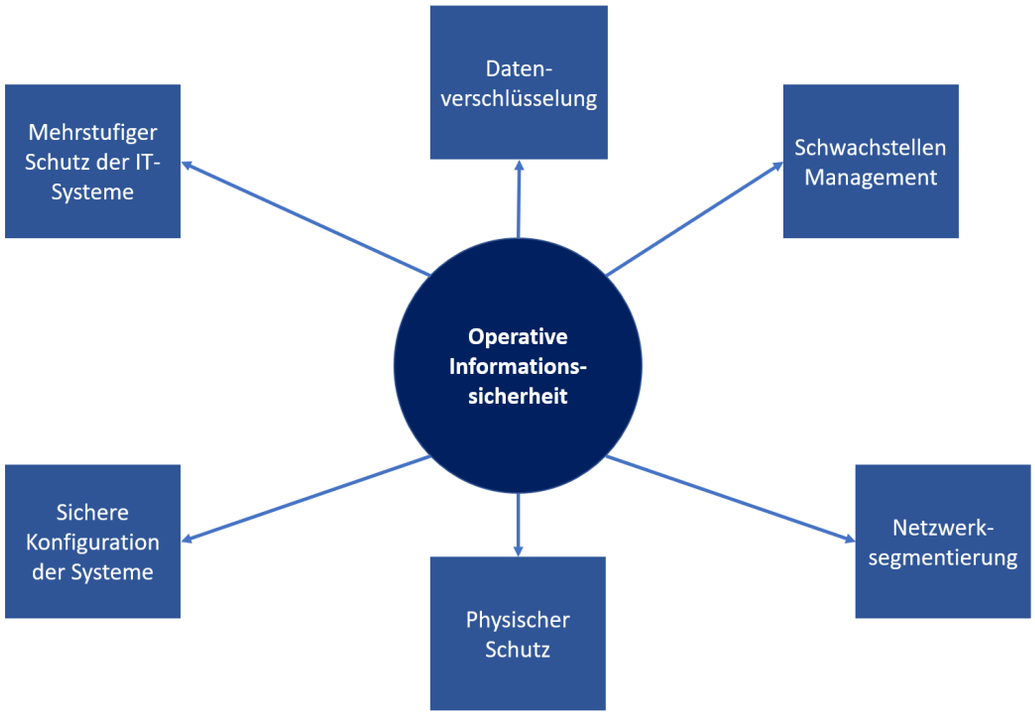

Abbildung 5 Aufgaben der Operativen Informationssicherheit

- Sollten Gefährdungen des Informationsverbundes auftreten, so ist es die Aufgabe der operativen Informationssicherheit diese zeitnah zu identifizieren und die Informationen der entsprechenden Schwachstelle frühzeitig zu analysieren und entsprechend auszuwerten. Schwachstellen bzw. sicherheitsrelevante Informationen können in Form von Störungen oder Meldungen auftreten. Zur Evaluierung der Systeme sollten beispielsweise regelbasierte Auswertungen gefahren werden, jedoch können ebenfalls IT forensische Mittel herangezogen werden, um weitere Kenntnisse über eine mögliche Bedrohungslage zu erlangen. Das Finanzunternehmen hat entsprechende Regeln an die IT-Systeme aufzustellen, um einen entsprechenden Soll-Stand zu etablieren. Hierbei können Ergebnisse, die außerhalb der Regel sind, analysiert werden und gegebenenfalls Verstöße festgestellt werden. Weitere Mittel der operativen Informationssicherheit für den Schutz der eigenen IT-Infrastruktur können

die Analyse von Abweichungen innerhalb der Systeme, das Scannen auf Schachstellen, Pentests [9]sowie die Verwendung von Audits zur Zertifizierung der ISO 27001[10] sein. [16, S. 14–16]

- **IT-Notfallmanagement** – knüpft eng an das Notfallmanagement der MaRisk an, wobei die BAIT diesen Punkt deutlich konkretisiert. So wird hierbei tiefer auf Details der Wiederanlauf, Notbetriebs- und Wiederherstellungspläne eingegangen. Pläne müssen dabei Parameter und Abhängigkeiten aufführen, um die Effektivität dieser messbar zu machen. Diese sind beispielsweise:

Parameter	**Abhängigkeiten**
Wiederanlaufzeit eines Systems	Eingesetzte IT-Systeme
Maximal tolerierbare Zeit eines Datenverlusts	Wiederherstellungspriorisierung
Konfiguration für den Notbetrieb	Externe Faktoren (Gesetzgeber, Anteilseigner, Öffentlichkeit, etc.)

Die Effektivität der Pläne ist durch regelmäßige Tests (mind. 1x jährlich) zu prüfen und zu bewerten. Sollte dabei die angedachte Vorgehensweise nicht einzuhalten sein oder sich als ineffektiv rausstellen, so sind die Pläne entsprechend anzupassen. Darüber sind für die System- und Prozesstests ein entsprechendes Testkonzept zu erstellen. [16, S. 27–29]

3.4. ZAIT

ZAIT steht für „Zahlungsdiensteaufsichtliche Anforderungen an die IT“ und deckt sich in weiten Teilen mit den Vorgaben der BAIT. Jedoch lieferte die BaFin als Herausgeber einige Anforderungen nach, welche die Zahlungsdienstleister berücksichtigen müssen. Dabei ergänzt das Rundschreiben unter anderem den Punkt IT-Notfallmanagement. So schreibt die ZAIT die Zeitkritikalität bei der Auswirkung der Risiko- und Auswirkungsanalyse vor. Dabei sollen speziell vertieft die Auswirkungen eines Ausfalls auf den Geschäftsbetrieb untersucht werden.

[9] Pentest - Penetrationstests unter Verwendung von offensiven Hacking Praktiken zur Prüfung und Härtung der eigenen Systeme.

[10] ISO 27001 – Ist eine international Industrie Norm, welche das Informationssicherheit-Management zertifizieren soll.

Des Weiteren werden die Unternehmen in die Pflicht genommen, dass Notfall- und Wiederherstellungspläne bestimmte Szenarien beinhalten müssen. Hierzu gehören unteranderem der Ausfall von Dienstleistern, eines Standorts oder der IT-Systeme.

Ebenfalls wird die Wirksamkeit der Konzepte durch die ZAIT in den Fokus gerückt, sodass die Banken ihre Maßnahmen und Prozesse jährlich prüfen müssen. Teil dieser Prüfungen sind unter anderem die Alarmierungs-, Ernstfall-Übung und die technische Vorsorge. [18], [19]

3.5. KAIT

Die KAIT (Kapitalverwaltungsaufsichtliche Anforderungen an die IT) definiert Anforderungen ähnlich zur BAIT und dient dabei der Ausgestaltung der IT-Maßnahmen für Kapitalverwaltungsgesellschaften. Inhaltlich ist die KAIT nahezu identisch zur BAIT beinhaltet jedoch nicht die Definition zur kritischen Infrastruktur.

Ergänzt wurde im Rundschreiben allerdings sowohl die Rolle des Informationssicherheitsbeauftragten (ISB), als auch neue Anforderungen für die Auslagerungen an IT-Dienstleister. Die KAIT definiert die Aufgaben des Informationssicherheitsbeauftragten wie folgt: „

- die Geschäftsleitung beim Festlegen und Anpassen der Informationssicherheitsleitlinie zu unterstützen und in allen Fragen der Informationssicherheit zu beraten; dies umfasst auch Hilfestellungen bei der Lösung von Zielkonflikten (z. B. Wirtschaftlichkeit kontra Informationssicherheit),
- Erstellung von Informationssicherheitsrichtlinien und ggf. weiteren einschlägigen Regelungen sowie die Kontrolle ihrer Einhaltung,
- den Informationssicherheitsprozess in der KVG zu steuern und zu koordinieren sowie diesen gegenüber IT-Dienstleistern zu überwachen und bei allen damit zusammenhängenden Aufgaben mitzuwirken,
- Beteiligung bei der Erstellung und Fortschreibung des Notfallkonzepts bzgl. der IT-Belange,
- die Realisierung von Informationssicherheitsmaßnahmen zu initiieren und zu überwachen,
- Beteiligung bei Projekten mit IT-Relevanz,
- als Ansprechpartner für Fragen der Informationssicherheit innerhalb der KVG und für Dritte bereitzustehen,

- Informationssicherheitsvorfälle zu untersuchen und diesbezüglich an die Geschäftsleitung zu berichten,
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und zu koordinieren.“ – BaFin Rundschreiben 11/2019 (WA) in der Fassung vom 01.10.2019 [20, S. 12–13]

Der ISB ist folglich maßgeblich an der IT-Sicherheit der Kapitalverwaltungsgesellschaften mit beteiligt und dient auch nach außen als Ansprechpartner für Sicherheitsbelange und Ermittler für Sicherheitsbelange im eigenen Unternehmen.

Zum einem werden die IT-Dienstleister näher definiert, wodurch nun auch Cloud-Dienstleister unter die Mindestanforderungen an das Risikomanagement von Kapitalverwaltungsgesellschaften, welche das Äquivalent zur MaRisk für Kapitalverwaltungsgesellschaften darstellt und somit stärkeren Regulatorien unterliegen. Zum anderen wird ein stärkerer Fokus auf Standard-Software gelegt, welche in das Unternehmen eingekauft wird. So ist eine Risikobewertung durchzuführen, wenn es sich bei der Software um Customizing in Form von Patches, Updates oder sonstigen wesentliche Anpassungen handelt. Ebenfalls zur Regelung zählen Unterstützungsdienstleistungen wie die Wartung, Fehlerbehebung im Auftrag der Kapitalverwaltungsgesellschaft oder das Testmanagement und der Freigabe bzw. Implementierung der Änderungen. Sollten sich dabei keine kritischen Auswirkungen ergeben, so wird in dem Fall zu Gunsten der Gesellschaften entschieden. Es handelt sich in der Folge dessen nicht um eine Auslagerung, sondern um einen „sonstiger Fremdbezug von Leistungen”, welcher weniger stark kontrolliert wird.[20]–[22]

3.6. DORA

Der „Digital Operational Resilience Act“ (Dora) wurde Ende 2022 von der EBA[11] beschlossen und tritt ab dem 16.01.2023 in Kraft. Ziel der Dora ist es die „Digital Finance Strategy“ der EU auszubauen und dabei Finanzunternehmen gegen die verschiedenen IT-Risiken von innen und außen abzusichern. DORA trifft allerdings nicht nur die Finanzunternehmen der EU, sondern auch die IT-Drittanbieter, welche beispielsweise Software und Services für Banken und Versicherungen zur Verfügung stellen. 2023 und 2024 sollen von den Europäischen Aufsichtsbehörden technische Regulierungs- und

[11] European Banking Authority

Durchführungsstandards herausgegeben werden, um die DORA weiter zu spezifizieren, wobei die Anforderungen ab 2025 für alle verpflichtend werden sollen. Inhaltlich stützt sich die DORA auf die folgenden Eckpunkte:[23]–[26]

- **Risiko Management der IKT**[12]
  Dazu gehören unter anderem der Aufbau und die Pflege einer belastbaren IT-Infrastruktur. Ebenfalls ist es notwendig kritische Funktionen/ Dienste in dieser zu identifizieren und zu kategorisieren, da diese als besonders schützenswert gelten. Eine Überwachung, wie sie in der BAIT vorgesehen ist, findet sich ebenfalls auch in den DORA-Richtlinien wieder, so ist die eigene IKT kontinuierlich zu Überwachen und entsprechende Schutz- sowie Präventionsmaßnahmen vorzusehen. Dieses Vorgehen soll im Optimalfall eine sofortige Erkennung von Anomalien innerhalb der Systeme mit sich führen.

- **Meldung IKT-Vorfälle**
  Durch die DORA sind Finanzunternehmen nun verpflichtet IKT-Vorfälle zu Protokollieren und zu Melden. Im Falle eines meldepflichtigen Ereignisses, ist Meldung an die EBA, EIOPA[13] und die ESMA[14] zu erstatten. Dafür sind die Standardvorlagen der ESA zu verwenden und Anfangs-, Zwischen- und Abschlussberichte des IKT-Vorfalls einzureichen. Meldepflichtig sind schwerwiegenden nicht geplanten Vorkommnisse, welche sich negativ auf die Authentizität, Integrität oder Verfügbarkeit von Daten des Finanzdienstleisters auswirken. [26, S. 5] Punkt 21

- **Resilienz Tests**
  Es ist vorgesehen, dass Finanzunternehmen jährlich Cyber-Security Audits durchführen, um Schwachstellen, Lücken und Mängel in den IKT-Systemen und Diensten zu identifizieren. Dies soll zur Folge haben, dass die Unternehmen die Fehler entsprechend bewerten und gegebenenfalls Vorkehrungen treffen, die die Feststellungen entweder abmildern oder gar beheben, sollten diese nicht als

[12] IKT - Informations- Kommunikationstechnik

[13] European Insurance and Occupational Pensions Authority

[14] European Securities and Markets Authority

hinnehmbares Risiko betrachtet werden. Darüber hinaus sind auch die Drittanbieter, welche ihre Dienste den Finanzunternehmen zur Verfügung stellen, verpflichtet an den Audits teilzunehmen, da sich sonst kein umfassendes Bild über den Sicherheitsstand der IKT-Systeme gebildet werden kann. Zur Auditdurchführung sind hierbei TLPT[15] vorgesehen. Red Teaming Methodiken, welche sich an echten Angriffsszenarien orientieren und sich gezielt gegen Menschen, Prozesse und die IT des Finanzunternehmens richtet, mit nur minimalen Vorkenntnissen (Black/ Grey Box Testing).

- **Risiken durch IKT-Drittanbieter**
  Um eine vollumfassende Überwachung der Risiken für Finanzunternehmen zu gewährleisten, ist es unabdinglich auch die Anbieter der ausgelagerten IKT-Dienstleistungen mit in die Verantwortung zu ziehen und mitzuüberwachen. Bereits in der MaRisk und der BAIT wird eine Führsorgepflicht der Dienstleister mit verankert, welche durch DORA nun auch auf EU-Ebene etabliert wird. Die Finanzunternehmen sind nun gegenüber der EBA verpflichtet, alle kritischen IKT-Dienste zu melden, welche an Drittanbieter ausgelagert wurden. Ebenfalls muss darüber ein Verzeichnis geführt werden, welcher Dienstleister, welche Leistung erbringt und welche Änderungen der unterstützenden Dienstleister sich hierbei ergeben haben. Dies soll zum einen sicherstellen, dass Verträge alle notwendigen Leistungen, Standorte und die Daten, welche verarbeitet werden, umfassen und diese im zu führenden Verzeichnis hinterlegt sind. Zum anderen wird dadurch sichergestellt, dass alle IKT-Drittdienstleister den Anforderungen seitens des EU-Aufsichtsrahmen Folge leisten, womit diese den Qualitätsstandards und den möglichen Sanktionen der EBA unterliegen.

- **Informationsaustausch**
  Die EBA sieht außerdem einen allgemeinen Informationsaustausch zwischen den Finanzunternehmen vor. Durch das Melden von IKT relevanten Vorfällen hat die Behörde die Vorfälle zentral zu sammeln. In Folge werden die gesammelten Daten ausgewertet und die Trendentwicklung durch die EBA zur Verfügung gestellt. Dies

[15] TLPT- Threat-Led Penetration Testing

gibt den Unternehmen und der EBA selbst die Möglichkeit, ein Überblick der internationalen Bedrohungslage zu erhalten und gegebenenfalls konkrete Maßnahmen zum Ausschluss oder Milderung bestimmter Angriffsvektoren bzw. Risiken zur Verfügung zu stellen.

3.7. DSGVO

Die Datenschutzgrundverordnung (DSGVO) dient dem Zweck Daten natürlicher Personen und die Grundfreiheit sowie die Grundrechte der Bürger weiter zu schützen. Sollte es in der Bank einen Vorfall geben, bei denen Kundendaten betroffen sind, so ist den Vorgaben der Verordnung zu folgen. Aus diesem Grund muss die DSGVO auch mit in Betracht gezogen werden, da sie sich aus einem Sicherheitsvorfall ggf. auch Bürgerrechte geltend gemacht werden können. Um diese Anforderungen durchzusetzen, sieht die DSGVO ebenfalls Sanktionen vor, welche die Unternehmen, zu denen ebenfalls die Banken zählen dazu zu bewegen die Daten ihrer Kunden besonders zu schützen.[27], [28]

Die DSGVO definiert dabei im Art. 4 den Begriff „personenbezogene Daten“. Dabei kann es sich um eine Information handeln, die direkt auf eine Person schließen lässt, wie beispielsweise ein Name, oder die Summe von Teilinformationen, die eine Identifizierung möglich machen kann. Ein Beispiel für eine Summe von Teilinformationen. welche eine Identifizierung möglich machen kann ist die Kombination aus Geschlecht, Mail-Adresse (in der Form „V.Nachname@mail.de“ und Standortdaten. [29]–[32]

Artikel 9 definiert dabei einen Ausschluss, dass besonders schützenswerte Daten nicht ohne besonderes Interesse verarbeitet werden dürfen. Ein besonderes Interesse kann beispielsweise eine Bank oder Versicherung haben, wenn es sich um den Abschluss einer Gesundheit-Versicherung handelt, für deren Abschluss medizinische Fragen gestellt werden müssen. Allgemeinen Zählen folgende Daten als besonders schützenswert:[33]

- Genetische Daten
- Biometrische Daten
- Gesundheitsdaten
- Informationen über die Sexualität
- ethnische und kulturelle Herkunft
- politische Zugehörigkeit
- religiöse und philosophische Überzeugungen

- Gewerkschaftszugehörigkeit

Weiterverarbeitung

Wie Daten weiterverarbeitet werden dürfen, wird in Artikel 6 „Rechtmäßigkeit der Verarbeitung“ der DSGVO bestimmt. Banken haben sich vor allem an die folgenden Punkte relevant:

- Personen müssen der Verarbeitung zu einem bestimmten Zweck zustimmen.
- Das Unternehmen darf die erhobenen Daten nur zum Zweck des eingewilligten Rahmens der Auftragserfüllung verwenden.
- Das Unternehmen darf die erhobenen Daten weiterverarbeiten um rechtlich auferlegten Pflichten nachzugehen.

Diese Punkte sollen vor allem dafür sorgen, dass Unternehmen keine Daten erheben oder gar verarbeiten, an denen kein legitimes Interesse besteht.[34]

Datensicherheit:

Um die Sicherheit der erhobenen Daten zu gewährleisten, schreibt der Gesetzgeber einige Maßnahmen. Dafür wurde der §64 „Anforderungen an die Sicherheit der Datenverarbeitung“ im Bundesdatenschutzgesetzt, welches Teil der DSGVO ist eingeführt. Dieser gliedert sich in 3 Bestandteile:

- Eigenverantwortung:
  Unternehmen haben die technischen und organisatorischen Maßnahmen zu treffen, um ein angemessenes Schutzniveau zu etablieren. Hierbei soll der aktuelle Stand der Technik und die Eintrittswahrscheinlichkeit verschiedener Szenarien einbezogenen werden. Ebenfalls wird auf gängige technische Richtlinien und Empfehlungen des BSI verwiesen.
- Anforderungen:
  Während des gesamten Prozesses der Verarbeitung der Daten sollen die Prinzipien der Datensicherheit aufrechterhalten werden. Dabei handelt es sich um Vertraulichkeit, Verfügbarkeit, Belastbarkeit und Integrität. Weiterhin wird auch eine Verschlüsselung und eine Pseudonymisierung der Daten empfohlen, aber nicht vorgeschrieben. Im Falle eines physischen oder technischen Ereignisses ist vorgeschrieben, dass Daten schnellstmöglich wiederherstellbar sind.

- Risikobewertung:
  Im Rahmen der Risikobewertung, sind Maßnahmen für die Folgenden Aspekte zu treffen:[35]

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Zugriffskontrolle
- Übertragungskontrolle
- Eingabekontrolle
- Wiederherstellbarkeit
- Zuverlässigkeit
- Datenintegrität
- Verfügbarkeitskontrolle
- Trennbarkeit
- Benutzerkontrolle
- Transportkontrolle
- Auftragskontrolle

Meldepflicht

Sollte es zu einer Verletzung des Schutzes von personenbezogenen Daten gekommen sein, so ist dieser Vorfall 72 Stunden nach dem Bekanntwerden der zuständigen Datenschutzbehörde zu melden, dies wird im Artikel 33 –Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde festgehalten.

Verletzungen des Datenschutzes können durch folgende Formen auftreten:

- Verlust von Hardware mit Kundendaten
- Verlust von Unterlagen
- Mangelhafte Datenvernichtung
- Mangelhafte Transportverschlüsselung von Daten
- Hacking-Angriff
- Versehentliche Informationsweitergabe

Sollte ein Fall gemeldet werden, so ist zusätzlich zur Meldung des Vorfalls, die Art der betroffenen Daten, die Anzahl von betroffenen Personen, der Name des Datenschutzbeauftragten, die Auswirkungen des Vorfalls und die getroffenen Gegenmaßnahmen zu melden. In einigen Fällen ist das Melden nicht zwingend notwendig,

hierbei muss allerdings durch den Datenschutzbeauftragten des Unternehmens eine entsprechende Risikobewertung und Begründung abgegeben werden.[36]

Sanktionen

Welche Sanktionen mit einem datenschutzrelevanten Vorfall einhergehen, wird im Artikel 83 „Allgemeine Bedingungen für die Verhängung von Geldbußen“ und Artikel 84 „Sanktionen“ bestimmt. Dort werden die Kategorien definiert, in die ein relevanter Vorfall eingeordnet werden kann. Es wird beispielsweise beurteilt ob es sich bei dem Verstoß um Vorsatz oder Fahrlässigkeit handelt, ob dies die erste Handlung diesbezüglich war oder es eine Wiederholung gleichkommt und welche Daten, sowohl die Menge als auch die Art der Informationen, es sich dabei handelt. Ein Datenschutzverstoß kann rechtlich bis zu 20.000.000€ oder 4% den gesamten weltweiten Jahresumsatz und teilweise auch bis zu drei Jahre Haft bedeuten. Ebenfalls werden Datenschutzverstöße öffentlich gemacht und können online frei eingesehen werden, im DSGVO-Portal.[37]

3.8. Zusammenfassung Informationssicherheit der Banken

Abschließend lässt sich nach Betrachtung feststellen, dass Finanzunternehmen durch die gesetzlichen Auflagen und die zur Verfügung stehenden finanziellen Mittel mit dem aktuellen Stand der Technik gehen müssen, um ihre Systeme gegen Cyber-Attacken zu härten. Das hohe Maß an Sicherheitsanforderungen sorgt ebenfalls dafür, dass Cyberkriminelle es schwerer haben, große Summen von Banken zu erbeuten. Der Fokus der Kriminellen schiebt sich daher auf Privatpersonen und Unternehmen, welche weniger stark abgesichert sind. Banken und Versicherungen sind durch die Anforderungen zwar nicht unantastbar gegenüber einer Cyber-Kriminellen, allerdings kommt es weniger zu sicherheitsrelevanten Vorfällen als bei Privatpersonen. Die Kunden der Banken werden somit attraktive Ziele gegenüber den Kriminellen.

4. Absicherung des Kundengeschäfts durch die Banken

Banken sind nicht nur verpflichtet sich selbst vor Cyberattacken abzusichern, sondern auch die Kundenseite muss aktiv vor unbefugten Zugriffen geschützt werden. Um zu verstehen, vor welchen Hürden Cyberkriminelle stehen und welche Mittel sie verwenden um diese zu umgehen, ist es notwendig die Sicherheitsmechanismen vorher zu betrachten. Das folgende Kapitel befasst sich dabei im Detail mit den einzelnen Schutzmaßnahmen und wie diese teils historisch gewachsen sind. Ebenfalls wird auf die Notwendigkeit der Weiterentwicklung auf Basis des Fortschritts der Technik und den entstandenen Sicherheitslücken eingegangen.

4.1. Ablauf Online-Banking

Das Online-Banking stellt aus heutiger Sicht einen immer größeren Kontaktpunkt zwischen Kunden und Banken dar. Neben Überweisungen und Daueraufträgen können in der virtuellen Filiale häufig auch ganze Bankgeschäfte in Form von Kreditfinanzierungen oder auch Konto-Eröffnungen und -Verwaltungen durchgeführt werden. Da die Kunden allerdings meist nicht die gleichen Sicherheitsvorkehrungen wie die Banken selbst haben, geraten diese häufiger ins Visier der Kriminellen. Der Trend zur digitalen Filiale begann zwar schon weit vor der COVID-19 Pandemie 2020, diese beschleunigte aber den Prozess der Digitalisierung immens, wie ein Artikel des IT-Finanzmagazins aus dem Jahr 2022 aufzeigt. So wurden allein von 2021 auf 2022 2.388 Bank-Filialen geschlossen, was 9,9% der Gesamtmenge ausmacht.[38] Um zu verstehen, welche Einfallstore die Kriminellen nutzen, um an das Geld der Bankkunden zu gelangen, sollte man sich zuvor mit den einzelnen Modulen und Sicherungen des Online-Bankings befassen. Im Grunde besteht ein Online-Banking aus 3 Punkten:

- Login: Hierfür wird der Nutzer nach seinem Usernamen und Passwort gefragt, welches selbst vergeben werden kann.
- Produkt-/ Aktionswahl: Hierbei kann es sich um den Abschluss einer Bankdienstleistung handeln oder um einen Transaktionsauftrag wie zum Beispiel eine Überweisung oder einen Dauerauftrag
- TAN[16]-Abfrage: Diese wird benötigt, um den Nutzer zusätzlich zu authentifizieren und dient als Unterschriftsersatz für die Willenserklärung des Kunden. Für die

[16] TAN - Transaktionsnummer

Erstellung der TAN kann eine Vielzahl von Verfahren herangezogen werden, welche im entsprechenden Unterkapitel gesondert beleuchtet werden.

4.2. HTTPS

Damit die Kommunikation zwischen Bank und Kunden möglichst abhörsicher ist, bedarf es einer Form der sicheren Kommunikation. Bevor HTTPS (Hypertext Transfer Protocol Secure) etabliert wurde, fand die Kommunikation im Internet unverschlüsselt über HTTP (Hypertext Transfer Protocol) statt. Dabei wurde eine unverschlüsselte Kommunikation zwischen Client und Server etabliert, wobei der Client eine Anfrage an den Server schickt und dieser in der Regel mit einer Webseite antwortet.
HTTPS ist eine Weiterentwicklung von HTTP und ermöglicht den sicheren und verschlüsselten Datenaustausch im Internet. Dabei kann HTTPS das RSA[17]-Verfahren, verwenden, um die Kommunikation zu verschlüsseln. In diesem Fall geht das Protokoll wie folgt vor:[39]

1. Client baut Kontakt zum Server auf
2. Server nimmt die Verbindung an und sendet sein Zertifikat zusammen mit dem Public Key (PK)
3. Client Browser prüft das Zertifikat und geht anhand der 2 Fälle vor
    a. Zertifikat ist ungültig → Verbindung wird beendet
    b. Zertifikat ist gültig → geheimer Session Key wird erstellt und dieser mit dem Public Key verschlüsselt und an den Server geschickt
4. Server entschlüsselt den Session Key mit seinem Private Key
5. Server bestätigt den Erhalt des Session Keys im Folgenden
6. Sichere Kommunikation zwischen Client und Server besteht nun für die Session

Eine Verwendung ohne entsprechende Verschlüsselung, würde dazu führen, dass Kundendaten zwischen dem Nutzer und der Bank in Klartext übertragen werden würden und somit für Man-in-the-Middle-Attacken[18] angreifbar wären. Durch das Hinzuziehen eines Verschlüsslungsalgorithmus, wie beispielsweise RSA, würden in einem solchen Fall nur

[17] RSA – Rivest-Shamir-Adleman Algorithmus - Asymmetrisches Verschlüsselungsverfahren, wobei ein gemeinsames Geheimnis vereinbart wird und durch mathematische Operationen, ein verschlüsseltes Signieren von Daten erzielt werden kann.

[18] Man-in-the-Middle-Attack – Ist ein Cyberangriff, wobei der Angreifer einer Kommunikation zwischen User und Server beiwohnt, ohne das Wissen der anderen Parteien.

verschlüsselte Daten beim Hacker ankommen. Für Banken ist es heute zwar gängiger Standard, die Kommunikation zu verschlüsseln, jedoch wurden erst 2016 Webseitenbetreiber mit Kontaktformular in die Pflicht genommen, HTTPS zu verwenden (§13 Abs. 7 TMG). Seit 2018 wurde im Zuge der DSGVO die Pflicht zur Nutzung von verschlüsselten Verbindungen eingeführt.[40]
Ebenfalls Bestandteil von HTTPS sind entweder SSL oder mittlerweile TLS:[41]

	SSL	TLS
Bedeutung der Abkürzung	Secure Sockets Layer	Transport Layer Security
Algorithmus zum Schlüsselaustausch	RSA + Diffie- Hellmann	Digital Signature + Ephemeral Diffie-Hellmann
Protokollaufzeichnung (exemplarisch)	Hash Message Authentication Code (HMAC)	Message Authentication Code (MAC)

Hierbei sei festzustellen, dass es sich dabei nur um mögliche Algorithmen handelt, welche SSL und TLS benutzen können.

Wichtig bei sowohl SSL als auch TLS ist, dass diese Protokolle ein entsprechendes Zertifikat benötigen, um die Verschlüsselung bereitzustellen. Diese Zertifikate unterteilen sich in:

- **Domain Validated (DV)** – wird ausgestellt, nach der erfolgreichen Nachweißerbringung, dass der Antragsteller die Domain nutzen darf. Hierfür wird meist eine Mail an den Domaininhaber versendet, auf welche dieser reagieren muss. Darüber hinaus wird eine rudimentäre Kontrolle ausgeführt, ob es sich dabei um eine Seite mit Betrugspotenzial handelt wie zum Beispiel „Faceb00k.com“ oder „ammazon.de“. Im Zertifikat ist lediglich der Name enthalten. Aufgrund dessen bietet es weniger Sicherheit für den Nutzer, ist dafür aber günstiger und schneller in der Ausstellung. Anwendungsbeispiele hierfür wären Blogs oder non-kommerzielle Webseiten.
- **Organization Validated (OV)** – wird ausgestellt nach Prüfung, ob der Antragsteller berechtigt ist die Domain zu nutzen und durch Überprüfung der Firma mittels öffentlich zugänglicher Informationen. Inhalt des Zertifikats sind sowohl Domainname als auch Firmenname. Aufgrund der Eigenschaften des Zertifikats eignet es sich besonders für Onlineshops und Firmenwebseiten.

- **Extended Validation (EV)** – Prüfungsinhalte sind neben der Domainberechtigung, die juristische Person der Firmierung, Legitimierung der Firmierung, sowie der Firma selbst. Bestandteile des Zertifikats sind Name der Firma, Geschäftsadresse, Name der juristischen Person, Registrierungsnummer, Gründungsdatum und Gerichtsbarkeit. Ziel dessen ist zum einen die Sicherstellung, dass es sich bei der zu identifizierenden Entität wirklich um diese handelt und somit klar zuordenbar ist. Zum anderen soll somit der Einsatz von Phishing oder Identitätsdiebstahl erschwert werden, da die Firmierung klar identifiziert wurde. Dieses Zertifikat wird vor allem von Banken, Versicherung sowie großen Online-Shops verwendet, da es die größte Plausibilität gegenüber dem Nutzer bietet. [42]

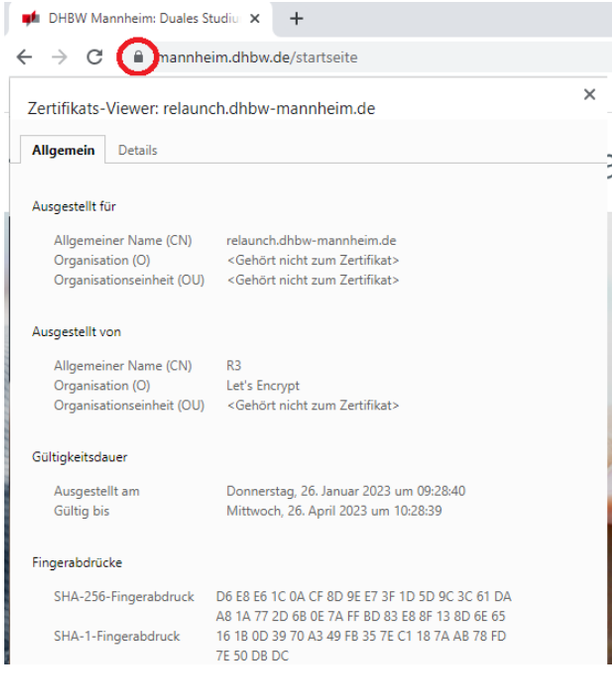

Abbildung 1 Zertifikat der DHBW Mannheim

Zertifikate sind aus einem bestimmten Grund nur bis zu einem Jahr, bei der Verwendung von gängigen Browsern gültig. Um zu überprüfen, um welche Art der Zertifizierung es sich bei einer Webseite handelt und wie lange diese noch gültig ist, kann das Schloss neben der Adresszeile im Browserfenster angeklickt werden (Abbildung 6 Zertifikat der DHBW Mannheim). Eine lange Gültigkeitsdauer würde es erschweren, neue kryptographische Methoden, bzw. neue Sicherheitsstandards zu implementieren. Folglich gäbe es eine verschiedene Wertigkeit innerhalb der drei Zertifizierungsarten und demnach ein intransparenterer Sicherheitsstandard für die Nutzer der Webseiten. Die einjährige Gültigkeit von Zertifikaten verhindert dies und begünstig somit die Durchsetzung neuer kryptographischer Standards. Ein Beispiel eine technische Umstellung wäre hierbei der Übergang von SHA[19]-1 zu SHA-2. Des Weiteren kann durch eine kürzere Identitätsdauer auch festgestellt werden, ob der Nutzer der Domain wirklich noch berechtigt ist, diese zu nutzen oder ob sich zwischenzeitlich Änderungen ergeben haben, die im Zertifikat vermerkt werden würden oder gar zur Aberkennung dieser führen würden. Demnach schafft es auch eine erhöhte Vertrauenswürdigkeit.[43]

[19] SHA – Secure Hash Algorithm

Das Verzichten auf eine HTTPS-Verbindung, seitens der Bank ermöglichte es den Hackern unter Verwendung von Schadsoftware auf Seiten des Kunden, das Mitlesen der Kommunikation. Ebenfalls wurde in der Vergangenheit häufiger darauf verzichtet, Betrugsseiten mit einem HTTPS Zertifikat zu versehen, was zur Folge hatte, dass die Browser eine Warnung ausgaben, dass die Seite nicht sicher sei. Dies bewegte Kunden häufig zum Überdenken ihrer Handlung und einige vielen nicht mehr auf die Maschen der Betrüger herein. Heute sind sowohl die Banking-Seiten als auch leider die Phishing-Seiten mit entsprechenden HTTPS-Verbindungen ausgestatten, wodurch eine entsprechende Warnung Seitens der Browser nicht mehr funktionieren würde.

4.3. TAN-Verfahren

4.3.1. Historie des TAN-Verfahrens

Bereits in den 1970ern etablierte die Verbraucherbank GmbH als erste Bank weltweit die elektronische Überweisung. Im Jahre 1976 erfand der technische Leiter Alfred Richter dort das Pin/ TAN Verfahren, welches vorerst für die bankinternen Mitarbeiter war. Ziel dessen war es, die Konten der Mitarbeiter vor unautorisierten Zugriffen innerhalb der Bank zu schützen. 1977, ein Jahr später, folgte die Etablierung des SB[20]-Bankings. Hierfür wurden auf Hubwagen Selbstbedienungs-Terminals, nach Filialschluss, in die Vorräume der Bank gerollt und den Kunden zur Verfügung gestellt. Im gleichen Jahr stellte die Verbraucherbank GmbH auch den ersten Geldautomaten zur Verfügung, sodass Kunden gegen ihre Kundenkarte, sowie den dazugehörigen Pin, Geld abheben konnten. 1978 sollte die Einführung der „Electronic Cash“ Karte, kurz EC-Karte, folgen. Auf Basis der Erfahrungen der Verbraucherbank GmbH sollte sich im Verlauf der Jahre das Online-Banking von anderen Banken etablieren.

Das Online-Banking beruhte zunächst auf sehr rudimentären Sicherheitsvorgaben. So war es anfangs noch Standard, neben dem Login und Passwort mit mindestens 10 Stellen eine Liste von Transaktionsnummern, kurz TAN, auf Papier zu nutzen.[44] Das Verfahren der TAN-Listen kam bis etwa 2005 zur Anwendung. Dabei wurde dem Kunden eine Liste mit TANs postalisch übersendet. Im Folgenden konnte zur Authentifizierung ein beliebiger TAN für die Geldübertragung verwendet werden. Grund für die Abschaltung der Methode war, dass es

[20] Selbstbedienung

immer häufiger zu Phishing Angriffen kam, wodurch das Verfahren zunehmend unsicherer wurde. [45]

Infolgedessen wurden die TAN-Listen modernisiert und indizierte TAN-Listen (iTAN) ins Leben gerufen. Der Unterschied zur herkömmlichen TAN-Liste war, dass die Bank nun spezielle indizierte TANs abfragen konnte, anstatt dem Kunden die willkürliche Wahl zu lassen, welche TANs er verwenden wolle. Dies sorgte zwar zunächst dafür, dass die Phishing-Fälle zurück gingen, aber gleichzeitig auch für ein vermehrtes Aufkommen von „Man-in-the-Middle-Attacken“ welche Transaktionen manipulierten. In diesem Fall wird das System des Opfers mit Schadsoftware infiziert und die Kommunikation im Folgenden ausgespäht. Der Angreifer hat zu diesem Zeitpunkt die Möglichkeit sein Opfer auszuspähen, kann aber auch eine gefälschte Internetseite der Bank des Opfers aufrufen. Das Resultat aus dem Szenario ist, dass Kriminelle Transaktionen der Opfer umleiten konnten und diese keine Anhaltspunkte dafür hatten, da der Bildschirmtext die richtigen Daten aufführte. Dass die Transaktion manipuliert war, konnte erst mit der Einsicht in die Kontoauszüge festgestellt werden.[46], [47] Zwei Fälle, die in diesem Zusammenhang medienwirksam wurden, war der Ermittlungserfolg 2010 des LKAs in Baden-Württemberg und Nordrhein-Westfalen. Dort zerschlugen die Beamten einen Ring von Internetkriminellen. Die Täter hatten mithilfe von Trojanern 260 Überweisungen in einer Gesamthöhe von 1,65 Millionen € manipuliert und auf ihre eigenen Konten umgeleitet. [48] Der andere Fall sollte jedoch schon 5 Jahre vorher auf das entstehende Problem aufmerksam machen. 2005 veröffentlichte das Red Team[21] der RWTH Aachen einen Proof of Concept (POC), der genau das Vorgehen der gefassten Täter von 2010 aufzeigen sollte. Die Grundprämisse des POC war zu zeigen, dass der indizierte TAN lediglich den Zeitraum einschränkt, indem Kriminelle die Transaktionen beeinflussen können, jedoch nicht den Umstand eine schädliche Transaktion durchführen zu können. Somit sei das iTAN-Verfahren nicht ausreichend sicher, um die nötigen Sicherheitsaspekte, welche bereits bei den TAN-Listen kritisiert wurden, zu erbringen. Maximillian Donseif, Sicherheitsexperte der RWTH Aachen, sagte hierzu: "Ein typisches Beispiel für Security Theater […] Die Banken haben geschickt die Haftung für elektronischen Zahlungsverkehr auf die Kunden abgewälzt. Nach den Phishing-Vorfällen wird eine Maßnahme eingeführt, die nur minimale

[21] Red Team is ein Begriff aus der Cybersecurity, welcher ein Team beschreibt, welches Hacking-Methoden verwendet um im Rahmen eines Audits Sicherheitslücken in Applikationen zu identifizieren.

Sicherheitsverbesserungen bringt, den Kunden aber vorspielt, dass sie nun vor Missbrauch sicher seien." – (Maximillian Donseif, 2010). Eine Verwendung von TAN-Listen, sowie iTAN wäre jedoch sicher gewesen, wenn Kunden die Webseiten auf eine sichere SSL-Verbindung prüfen würden.[47], [49]

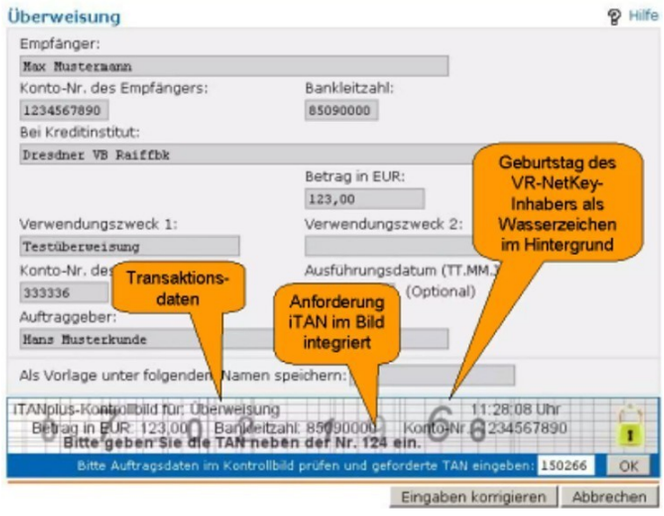

Abbildung 2 Beispiel iTANplus Verfahren

Während der Anwendungsperiode wurde allerdings auch stetig versucht, das iTAN-Verfahren zu verbessern und sicherer zu machen. Da der POC der Man-in-the-Middle-Attacke bekannt war, versuchte man die Finalisierung der Überweisung fälschungssicherer zu machen. Eine Methode hierfür war das iTANplus Verfahren. Entwickelt vom IT-Dienstleister Fiducia-IT, sollte für eine Überweisung neben der PIN und der iTAN zusätzlich ein Kontrollbild generiert werden. Dies wies alle Transaktionsdaten auf, sowie das Geburtsdatum als ein digitales Wasserzeichen, welches an heutige CAPTCHA-Verfahren[22] erinnert. Da das Geburtsdatum in der Regel den Angreifern nicht bekannt war, sollten diese die Überweisung noch sicherer für den Kunden machen (Abbildung 7 Beispiel iTANplus Verfahren).[50] Da iTAN allerdings zu unsicher ist, wurde mit der europäischen Zahlungsdienstrichtlinie (PSD2) beschlossen, dass dieses seit dem 14. September 2019 keine Anwendung mehr finden darf. [50]

2006 sollte bereits ein neues TAN-Verfahren auf den Markt kommen, denn die Postbank AG ließ sich das mTAN- oder auch SMS-TAN TÜV zertifizieren. Im Gegensatz zu den vorher üblichen TAN-Listen wurde nun eine SMS mit dem zu verwendenden TAN an eine zuvor hinterlegte Mobiltelefonnummer versendet.[51] Der Vorteil des mTAN-Verfahrens gegenüber herkömmlichen TAN-Listen war, dass es Online-Banking zugänglicher machte, da hierfür lediglich das eigene Mobiltelefon anstelle der ausgedruckten TAN-Listen benötigt wurde. Auch gingen Banken von einer erhöhten Sicherheit aus, da ein Verlust des eigenen Geräts eher auffallen würde als der Verlust der TAN-Liste. Problematisch ist bei mobilen TAN-Verfahren aber immer die Sicherung des eigenen Geräts. Sollte das Mobiltelefon nicht

[22] CAPTCHA ist eine Methode zur Verifizierung einer echten Person. Dem Nutzer wird ein verfremdetes Bild mit einem Code vorgelegt, welchen er in ein dafür vorgesehenes Feld tippen muss. Viele Bots können diese Sicherheitsmethode nicht umgehen, da die Bilder oft nicht maschinenlesbar sind.

ausreichend abgesichert sein und die Zugangsdaten für das Online-Banking im Telefon hinterlegt sein, so haben Kriminelle schlimmstenfalls vollen Zugriff auf das Konto des Opfers.[50] Darüber hinaus gibt es auch für dieses TAN-Verfahren Angriffsvektoren, um Überweisungen zu manipulieren oder unautorisierte TANs zu erzeugen. Einerseits ist es möglich bei einigen Banken, welche ihre Kunden online nicht ausreichend legitimieren, nur mit den Login-Daten das TAN-Verfahren zu ändern. Das bedeutet auch, dass im Falle des mTAN-Verfahrens eine neue Nummer hinterlegt werden kann und somit TANs über das Mobiltelefons des Angreifers generiert werden könnten. Darüber hinaus kann auch ein direkter Angriff auf die Nummer erfolgen, indem entweder eine zweite SIM-Karte auf die Nummer ausgestellt wird oder die Rufnummer zu einem anderen Anbieter umgezogen wird. In beiden Fällen müssten entsprechende Legitimierungen und Dokumente gefälscht werden, um ein entsprechendes Vorhaben umzusetzen. Wie erfolgreich jedoch ein solcher Angriff sein kann, zeigt ein Fall aus Australien. 2009 stahlen Täter über 80.000 australische Dollar von ihrem Opfer. Zunächst wurde diesem eine Phishing-Mail zukommen gelassen, welche alle für den Online-Banking Login und den Rufnummern Umzug benötigten Informationen abfragte. Darauffolgend nahmen die Täter alle nötigen Schritte vor, um die Rufnummer ihres Opfers bei dem neuen Anbieter zu registrieren, welcher die Identität seiner Kunden nicht ausreichend prüfte. Die Täter hatten infolgedessen die Chance, die notwendigen TANs zu erstellen, um im Namen ihres Opfers Überweisungen zu tätigen. Ein weiteres Einfallstor, welches Angreifer ausnutzen können, um an die Daten bzw. die TANs ihrer Opfer zu kommen, ist das Installieren von Trojanern auf den Mobilfunkgeräten. Aus der aktuellen Sicht wird auch das SMS-TAN-Verfahren ein baldiges Ende finden. Viele Banken, wie der Sparkassenverbund, bieten das Verfahren ihren Kunden nicht mehr an und haben bereits umgestellt. Darüber hinaus rieten sowohl der Verbraucherschutz als auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) von der Nutzung des mTAN-Verfahrens aus den oben genannten Gründen ab.[50], [52]

Das Chip-TAN Verfahren wurde 2006 eingeführt und zählt als eines der sichersten TAN-Verfahren, da es bis heute noch Anwendung findet und teilweise sogar weiterentwickelt wird. Hierbei benötigt der Kunde zunächst sowohl seine Karte des Kreditinstituts als auch einen entsprechenden TAN-Generator. Um eine TAN zu erzeugen, wird im Online-Banking Portal einen „Flickercode“ angezeigt, welcher aus 5 weißen Balken besteht, an diese der TAN-Generator mit der eingesteckten Karte angelegt werden muss. Wichtig ist, dass die Sensoren

auf der Rückseite des Generators mit dem Rand des Flickercodes übereinstimmen. Der Generator entschlüsselt im Folgenden den angezeigten Code und gibt zunächst zur Überprüfung die IBAN, BIC und den zu überweisenden Betrag zur Kontrolle aus und danach erst die erzeugte TAN. Jedoch wurde auch Kritik an dem Verfahren laut, da die Erkennung des Flickercodes bei mangelnder Bildschirmhelligkeit nicht funktioniert. Ebenfalls kann das Flickern der weißen Blöcke ebenfalls schwer erträglich für Menschen mit Epilepsie sein, weswegen immer mehr Banken von diesem Verfahren Abstand nehmen und auf neuere Iterationen des Chip-TAN-Verfahrens setzen. So setzt die Frankfurter Sparkasse beispielsweise auf eine QR-Code Version, andere Banken wiederum auf einen tanJack-photo-QR, welcher eine Ansammlung von roten, grünen und blauen Punkten innerhalb einer Matrix ist (Abbildung 8 QR-TAN (links) & tanJack-photo-QR (rechts)). [53], [54] Angriffsszenarien bei diesem Verfahren beschränken sich hauptsächlich auf Phishing Angriffe, sowie Maleware oder einfache Social Engineering Anrufe, auf welche genauer in Kapitel 5. Online-Banking Betrug eingegangen wird. Die Methode ist vor allem sicher, da diese eine Multi-Faktor Authentifizierung[23] zur TAN-Erstellung benötigt. Einerseits wird der Besitz der Karte mit einem TAN-Generator vorausgesetzt (Haben) und andererseits die Zugangsdaten zum Online-Banking (Wissen). Einziges Szenario, welches es Tätern möglich machen würde, an die TANs der Opfer zu gelangen, ist das Registrieren einer weiteren Karte oder das Ummelden auf ein anderes TAN-Verfahren. Da dies von den meisten Banken diesen Prozess aber besonders überwachen und die Täter dafür Zugriff zum Online-Banking ihres Opfers benötigen, ist ein solcher Angriff nur selten erfolgreich.

Abbildung 3 QR-TAN (links) & tanJack-photo-QR (rechts)

PushTAN ist mittlerweile als geistiger Nachfolger des mTAN-Verfahrens auf dem Markt weit verbreitet. Mit dem Aufkommen des Smartphones konnten auch mobile Banking-Apps immer weiterentwickelt werden. Durch die weite Etablierung der Betriebssysteme Android und iOS konnten standardisierte Entwicklungsumgebungen etabliert werden, welche die

[23] Multi-Faktor Authentifizierung definiert eine Art der Legitimierung einer Person, bei der mindestens zwei Faktoren der Kategorien „Sein“, „Haben“ und „Wissen“ vorausgesetzt werden. „Sein“ definiert biometrische Eigenschaften des Nutzers, „Haben“ den Besitz eines physischen Schlüssels und „Wissen“ die Kenntnis über ein gemeinsames Geheimnis, welches vorab vereinbart wurde.

Programmierung von Apps mit einheitlichen Sicherheitsstandards begünstigte. Bei der pushTAN-App handelt es sich häufig um eine dedizierte Anwendung, welche von der regulären Online-Banking App getrennt ist. Eine zusätzlicher Passwortschutz, sowie eine verschlüsselte Kommunikation zwischen den Applikationen ist dabei meist von Seiten der Bank etabliert worden. Wird ein Auftrag erstellt, welcher eine TAN benötigt, wird auf das Smartphone des Nutzers eine Push-Benachrichtigung gesendet, welche dieser bestätigen muss, um im Anschluss die TAN zu erzeugen.[54], [55]

4.3.2. Aktuelle Anforderungen an TANs

Im Rahmen der seit Januar 2018 geltenden Auflagen, sind alle europäischen Zahlungsdienstleister verpflichtet, sich an die Payment Services Directive 2 (PSD2) zu halten. Diese wurde erlassen, um unter anderem eine höhere Sicherheit im Zahlungsverkehr zu gewährleisten und den Wettbewerb zwischen den Banken anzukurbeln. Ein weiterer Schlüsselpunkt im PSD2, ist die Verpflichtung zur starken Kundenauthentifizierung. Diese Änderung traf allerdings erst mit der zweiten Stufe am 14. September 2019 in Kraft.

Dies hat für die Sicherheit des Onlinebanking die Auswirkung, dass Kreditinstitute dazu verpflichtet sind, den Kunden nach mindestens zwei der drei folgenden Verfahren zu authentifizieren, bevor eine TAN generiert wird.[56]

- Wissen: setzt die Kenntnis über ein gemeinsames Geheimnis voraus (Passwort, Pin)
- Besitz: setzt voraus einen Gegenstand der Legitimierung zu besitzen (TAN-Generator + Karte, Token, bei der Bank registriertes Mobiltelefon)
- Inhärenz: Physische Charakteristik des Nutzers (FaceID, Fingerabdruck, Iris, Stimme)

Da TAN-Listen nur eines der drei Anforderungen erfüllen konnten, hatten sie somit nach der Definition der PSD2 keine Freigabe mehr, da sie nun auch von Rechtswegen nicht mehr sicher genug für den Kundeneinsatz waren.

Die kryptographischen Sicherheitsmechanismen für die TAN-Erstellung im Detail sind weitestgehend unter Verschluss, demnach kann auch nicht genau gesagt werden ob Bankenverbünde jeweils eigene oder vorgefertigte Lösungen hierfür verwenden. Dennoch sind Finanzinstitute an diverse kryptographische Sicherheitsstandards gebunden, welche sie

erfüllen müssen. Durch das chipTAN-Verfahren beispielsweise, sind Banken dazu verpflichtet, den Advanced Eycryption Standard (AES) mit einer maximalen Schlüssellänge bei der Chipverwendung den Kontenkarten einzuhalten. Bei AES handelt es sich um eine symmetrische Blockverschlüsselung, welche Schlüssellängen in 128,192 und 256 Bit zur Verfügung stellt und diese zum Ver- und Entschlüsseln verwendet. Aufgrund des aktuellen Stands der Technik, ist es zusätzlich nahezu unmöglich, mittels Bruteforce[24] eine Entschlüsselung vorzunehmen, da eine Berechnung zu viel Zeit in Anspruch nehmen würde. [57]

Im Bereich des Mobile Bankings gibt es durch das PSD2 die Pflicht, Kunden zur Multi-Factor-Authentication (MFA) zu legitimieren. Dies bietet allerdings auch den Vorteil, dass der Anbieter das mobile Endgerät zur TAN-Erstellung verwenden kann. Simplifiziert sind TANs One-Time-Passwords (OTP). Diese können ähnlich wie beim chipTAN das AES-Verfahren anwenden, um ein gemeinsames Geheimnis in Form der TAN zu erzeugen. Hierfür kann die TAN-App mit einem Passwort oder einer biometrischen Sicherung zusätzlich geschützt sein. Das Mobiltelefon baut beim Aufruf der App eine Verbindung zum Applikationsserver auf und im Anschluss zum Authentifizierungsserver. Dort wird im Anschluss eine TAN von der verbundenen Datenbank ausgegeben und infolgedessen zurück an den Authentifizierungsserver und den Applikationsserver gegeben. Abschließend wird dem Mobiltelefon die TAN mittels einer TLS-Verbindung[25] mitgeteilt, wodurch der Nutzer die Überweisung nun Freigeben kann.[58]

4.3.3. Perspektive zur aktuellen TAN-Entwicklung

Die Frage, die man sich bei Betrachtung der historischen Entwicklung der TANs auch stellen muss, ist die Perspektive, in welche Richtung sich diese künftig entwickeln wird. Von der Peripherie mit der Bankkarte wird tendenziell immer häufiger abgesehen. Eine Umfrage des Bankenverbands aus dem Jahre 2022 gibt über einige Trendentwicklungen Aufschluss. Für die Datenerhebung wurden 1027 Personen im Alter ab 18 Jahren bis zur Gruppe der über60-

[24] Bruteforce beschreibt eine Hacking-Praktik, bei der jede mögliche Kombination eines Schlüssels/Passwort ausprobiert wird, bis dies zum Erfolg führt.

[25] TLS – Transport Layer Security, beschreibt ein Sicherheitsprotokoll. Der TLS-Handshake sorgt bei einem gemeinsamen Schlüsselaustausch dafür, dass die Kommunikation zwischen dem Client und der Seite überwachungssicher ist.

Jährigen zu den Themen Online-Banking, Tan-Verfahren, Nutzerverhalten, sowie Sicherheitsgefühl befragt.

Dabei kristallisierte sich erwartungsgemäß raus, dass die Zielgruppe für das Online-Banking zunächst in der Zielgruppe zwischen 18 bis zu den unter 60-Jährigen liegt. Ebenfalls geht aber auch hervor, dass 48% der 18- bis 29-Jährigen eine Nutzung des mobilen Onlinebankings, dem des an dem eignen PC (28%) vorzogen. Daraus kann eine Trend-Entwicklung abgeleitet werden. Sollte sich das Smartphone als Banking Instrument perspektivisch als Spitzenreiter etablieren, so ließen sich künftig TAN-Verfahren entsprechend des Nutzerverhalten ausrichten. Die Studie des Bankenverbands zeigt auch, dass mit 35% die meistgenutzte TAN-Variante das push-TAN Verfahren ist und demnach das Smartphone auch hier als Authentifizierungsmittel die Nutzer überzeugen kann. Die Peripherie der eigenen Bankkarte verliert somit an Bedeutung, womit Photo-Tan (19%) und Chip-Tan (13%) auf den letzten Plätzen liegen. Dies würde auch erklären, warum das HBCI-Verfahren[26] von einigen Banken nicht mehr angeboten wird, da TAN-Verfahren, welche außerhalb des Smartphones stattfinden, an Bedeutung verlieren. [59]

Perspektivisch würde eine steigende Bereitschaft zur Nutzung des Smartphones einerseits eine höhere Sicherheit bei der Authentifizierung des Nutzers bedeuten, da hierbei stärker auf die Bordmittel des Endgeräts zurückgegriffen werden kann. So gibt Apple beispielsweise an, dass ein Knacken des im iPhone verbauten Fingerabdrucksensors eine Chance von 1:50.000 und der Gesichtserkennung 1:1.000.000 zugrunde liegt. Das BSI geht auch davon aus, dass die Verhaltensbiometrie, welche sich mit dem Nutz-, sowie Tippverhalten des Users auseinandersetzt, an Bedeutung gewinnen könnte und dies keine teuren Sensoren benötigen würde, welche meist nur in High-End Smartphones zu finden sind.[60] Dass Betrüger allerdings auch die biometrischen Hürden überwinden können, zeigte der Chaos Computer Club bereits 2013 indem sie in der Lage waren, einen Fingerabdruck mittels eines Fotos so zu replizieren, dass der Touchsensor des iPhones 5s den künstlichen Fingerabdruck als echt erkannte.[61] Ein weiterer Fall stammt aus dem Jahr 2017, wobei es Mitarbeitern des vietnamesischen Softwareherstellers Bkav gelang, mittels eines 3D-Druckers und den genauen Maßen des Gesichts, sowie einer Nase aus Silikon und 2D Abbildungen der Augen und des Munds, die Face-ID des iPhone X zu umgehen.[62] Die beiden Fälle zeigen zwar auf,

[26] HBCI – Home-Banking Computer Interface, ist eine Schnittstelle für eine Finanzsoftware, welche einen Kartenleser benötigt, der Bank Chipkarten unterstützt. Der Nutzer kann Transaktionen durch Eingabe seines Kartenpins, ähnlich wie am Geldautomaten, anweisen.

dass es nicht unmöglich ist, die biometrischen Kontrollen zu umgehen, es allerdings auch mit sehr viel Aufwand verbunden sein kann und mit viel Fachwissen verbunden ist.

4.4. Zusammenfassung - Absicherung des Kundengeschäfts durch die Banken

In diesem Kapitel wurde zunächst die auf die Notwendigkeiten aufmerksam gemacht, wie Banken ihr Kundengeschäft absichern. Hierfür wurde zunächst auf die allgemeinen Funktionalitäten des Online-Bankings aufmerksam gemacht, um im Folgenden die Sicherheitsmechanismen zu beleuchten. Hierfür wurde zunächst die Notwendigkeit von verschlüsselten Kommunikationswegen in Form von HTTPS erläutert und wie ein Schlüsselaustausch unter Verwendung des RSA-Schlüsselaustausches funktioniert. Weiterhin wurde erläutert, wie Täter die Geschäfte zwischen Kunden und Banken ohne die Verwendung von des HTTPS Protokolls abhören und bearbeiten konnten.

Des weitern wurden einzelne TAN-Verfahren betrachtet und erläutert, warum diese mit der Weiterentwicklung von technischen Mitteln anfällig für Angriffe wurden. Darüber hinaus wurde die Multi-Faktor-Authentifizierung erläutert. Hierbei wurde herausgestellt, dass die Identität der Nutzer besser festgestellt werden kann, wenn mindestens zwei von drei der Kriterien „Wissen“, „Haben“ und „Sein“ verwendet werden.

Ebenfalls wurde erläutert, dass die Hinzunahme von mobilen Endgeräten den Authentifizierungsprozess unterstützen kann, durch die technologischen Mittel wie Biometrieerkennung.

5. Online-Banking Betrug

Im folgenden Kapitel wird die Motivation hinter Online-Banking Betrug beleuchtet. Dabei wird zunächst die Frage beantwortet, aus welchen Teilen eine Betrugsmasche besteht und im Folgenden erklärt, wie die im Kapitel 4 eingeführten Sicherheitsmaßnahmen von den Betrügern umgangen werden. Die Vorgehensweise wird dabei im Detail erklärt und durch Praxisbeispielen verdeutlicht. Ebenso wird ein Anwendungsbeispiel vorgeführt, durch dessen eine Phishing-Seite simuliert werden soll. Zusätzlich wird die Frage behandelt, wie sich Privatpersonen vor Phishing schützen können, indem Präventionsmaßnahmen betrachtet werden.

5.1. Motivation hinter Online-Banking Betrug

Dass die Fallzahlen der Online-Betrügereien in den vergangenen Jahren kontinuierlich gestiegen sind, wurde bereits im Kapitel 2.3 Aktuelle Bedrohungslage erläutert. Im Gegensatz dazu sind Banküberfalle in den vergangenen Jahren deutlich gesunken. 2021 gab das Landeskriminalamt Bayern bekannt, dass die Fälle von Bankraub seit 1993 um 95% gefallen seien. 1993 waren noch 133 Fälle zu verzeichnen, diese Zahl sank allerdings auf sechs im Jahr 2020. Das Sinken der Fallzahlen ist auch kein Einzelfall für das Bundesland, sondern lässt sich auf die komplette Bundesrepublik verallgemeinern. [63], [64]

Einerseits lässt sich dies auf die stärkere Sicherung des Geldes innerhalb der Filialen zurückführen. Viele Banken haben heute nur noch stark begrenzte Bargeldsummen in ihren Zweigstellen. Besonderes in bei kleineren Liegenschaften spricht man hierbei maximal von geringen sechsstelligen Summen, die über mehrere Geldautomaten verteilt sind. Zudem gibt es nur noch selten Auszahlungen direkt am Schalter. Häufig werden Blanko-Karten oder gar die eigene Bankkarte mit Geld beladen, wodurch die gewünschte Summe durch den Kunden am Geldautomaten abgehoben werden kann. Sollte die gewünschte Geldsumme einen gewissen Wert überschreiten, ist die Auszahlung häufig noch mit einer Wartezeit am Automaten verbunden. Das gleiche System gilt ebenfalls für eine Auszahlung am Schalter. Des Weiteren müssen Täter Sicherheitsmaßnahmen beachten. Hierzu gehören beispielsweise stille Alarme, welche sowohl durch einen Knopf am Platz des Bankmitarbeiters als auch durch die Eingabe einer speziellen Kontonummer ausgelöst werden können.

Andererseits kann man aber auch davon ausgehen, dass Täter sich bewusst nicht einer direkten physischen Konfrontation stellen möchten und die damit verbundenen Aspekten des Raubs, wie Fluchtfahrzeug, einem möglichen Polizeieinsatz oder gar das Ausbleiben der Beute riskieren möchten, dafür sprechen auch die Zahlen der Polizeistatistik.

Folglich sprechen viele Faktoren eher für den Umstieg in die Cyberkriminalität, da man schon mit wenig Aufwand Betrugsmaschen anwenden kann und das Risiko von den Strafverfolgungsbehörden gefasst zu werden deutlich niedriger ist.

5.2. Schematischer Ablauf eines Online-Banking Betrugs

In den folgenden Unterkapiteln wird erklärt, wie es zur Kontaktaufnahme kommt, woher die Cyberkriminellen dabei die Daten ihrer Opfer erlangen und mit welchen Methoden die Opfer manipuliert werden. Darüber hinaus wird die Begrifflichkeit des Social Engineerings eingeführt und anhand von Beispielen wird erläutert, was die Betrugsmaschen so effektiv machen. Ebenfalls werden die technischen Mittel, die für einen erfolgreichen Angriff benötigt werden, analysiert und ein Angriff exemplarisch rekonstruiert. Abschließend werden Möglichkeiten vorgestellt, um sich vor Betrugsmaschen im Bereich des Online-Bankings zu schützen.

5.2.1. Arten des Social Engineerings

Social Engineering ist ein Begriff, welcher durch den Politikwissenschaftler Karl Popper 1945 in seinem Werk „The Open Society and it‘s Enemies“ eingeführt wurde. In Poppers ursprünglicher Auffassung ging er davon aus, dass die Gesellschaft durch rationale und ingenieurgleiche Manipulationen positiv umgestaltet werden könnte.

In den 1980ern bis 1990ern wurde der Begriff allerdings grundlegend neu definiert, nachdem Hacker, wie Kevin Mitnick, durch geschickte Frage- und Manipulation-Techniken an vertrauliche Informationen von Firmen wie Motorola gekommen waren. Social Engineering beschreibt das Verleiten einer Person zu Handlungen oder zur Preisgabe von Informationen, welche sie unter normalen Umständen nicht ausführen oder preisgeben würde.[65], [66]

Social Engineering lässt sich in 3 Kategorien unterteilen:

- Human-Based Social Engineering

- Computer-Based Social Engineering
- Reverse Social Engineering

Alle 3 Kategorien lassen sich auch in den verschiedenen Maschen der Online-Banking Betrüger wiedererkennen.[67]

Human-Based Social Engineering:

- Setzt auf soziale Interaktionen und zwischenmenschliche Beziehungen
- In der Praxis z.B.: Kontakt, der einen privaten Anlageberater empfiehlt, welcher sich später als Betrüger herausstellt

Computer-Based Social Eningeering:

- Setzt auf technische Mittel wie Computer oder Mobiltelefone
- In der Praxis z.B.: gefälschte Mail von der Bank des Opfers, welche aufruft, dass Kunde sich auf einer Seite anzumelden und eine TAN zu bestätigen

Reverse Social Engineering:

- Opfer dazu gebracht Informationen von sich preiszugeben, wobei es davon ausgeht, bei dem Angreifer handelt es sich beispielsweise um einen Mitarbeiter der Bank.
- In der Praxis z.B.: falsche Bankmitarbeiter, welcher das Opfer anruft um eine vermeintliche Überweisung zu verhindern, diese aber dabei ausführt.

Genauer wird auf die einzelnen Maschen im weiteren Verlauf des Kapitels 5.2.4 Methoden des Online-Banking Betrugs Bezug genommen.

5.2.2. Kontaktaufnahme

Bevor eine Kontaktaufnahme überhaupt starten kann, werden persönliche Daten benötigt, damit die Betrüger mit ihren potenziellen Opfern in Kontakt treten können. Prinzipiell gilt, je mehr Informationen die Angreifer über ihre Opfer haben, desto authentischer kann ein Angriff konzeptioniert werden. Je nachdem welche Art des Social Engineerings genutzt werden soll, kann die Wahl der Informationsbeschaffung variieren.

Phishing:

Christopher Hadnagy beschreibt in seinem Buch „Die Kunst des Human Hacking – Social Engineering in der Praxis“ Phishing als solches:

„Mit Phishing ist gemeint, dass böswillige Scammer >>große Netze auswerfen<<, indem sie per E-Mail Leute auf Webseiten locken, die dort dann bösartige Dateien öffnen oder Informationen eintragen, die man für spätere Angriffe nutzen kann.“ .[68, S. 352]

Für ein solches Unterfangen bedarf es folglich auch eines großen Adressatenkreises. Kriminelle bedienen sich herbei häufig gekaufter E-Mail-Listen, welche sie teils im Darknet oder anderweitige Kontakte erhalten. E-Mail-Listen können allerdings auch durch den autorisierten Weiterverkauf nach beispielsweise einer Registrierung in einem Newsletter oder auf einer Webseite in die Hände von Betrügern gelangen. Eine der größten zugänglichen Listen, ist dabei die „Collection #1“ mit 773 Millionen Einträgen. Troy Hunt, Betreiber der Webseite „haveibeenpwned.com“, schrieb 2019 in seinem Blog, dass diese Sammlung von Mailadressen, Passwörtern und anderen persönlichen Daten, in einem nicht namentlich benannten Hacker-Forum frei geteilt wurde. Daraufhin beschloss er sich, die Daten aufzubereiten und in seinem Abfragedienst zu hinterlegen, um Nutzern die Möglichkeit zu geben, zu prüfen, ob ihre Accountdaten gegebenenfalls geleaked worden sein könnten, mitsamt der Information von welchem Leak sie betroffen waren.[69]

Eine Quelle, die für die Erstellung von Mail-Listen nutzen lässt, sind Datenlecks. Hierbei ist es Hackern in der Vergangenheit gelungen, nicht ausreichend gesicherte Daten von Webseiten zu erbeuten und die gewonnen Informationen für Phishing Kampagnen zu nutzen. Eine Übersicht über die fünf größten Datenlecks findet sich in Abbildung 9 „Top 5 Datenlecks“.

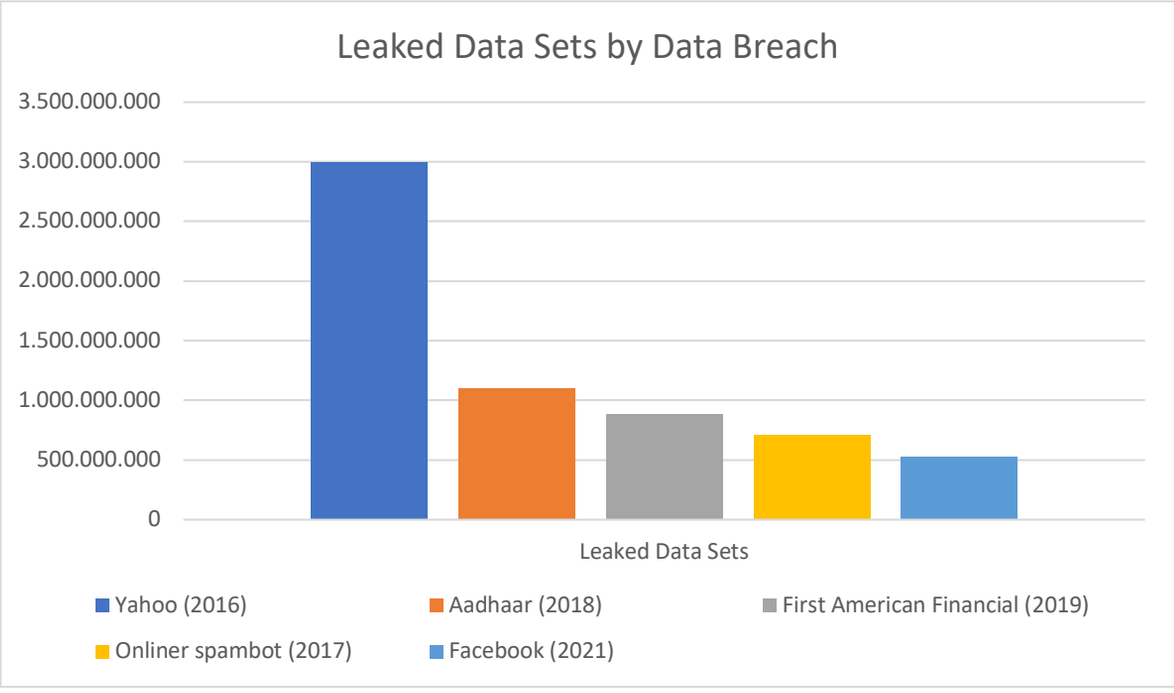

Abbildung 4 Top 5 Datenlecks [70]

Eine weitere Methode an Mail-Adressen zu gelangen ist das „Scrapen“[27] von Webseiten und mitunter auch gezielt Social Media Accounts. Dabei handelt es sich um Daten, die meist frei verfügbar im Netz liegen und für jedermann einsehbar sind. Weit verbreitet ist zudem auch das Nutzen von bereits erbeuteten Daten aus vorherigen Angriffen. Phishing ist dabei die häufigste Form bei dem Opfer in Kontakt mit Online-Banking Betrug kommen, da Täter hierdurch breite Massen adressieren können und somit schnell Kampagnen fahren können.[71] Hierfür wird meist eine Phishing-Seiten genutzt, welche eine existierende Seite simulieren soll. Auf dieses Vorgehen wird genauer im Anwendungsbeispiel in Punkt 5.3 eingegangen.[72]

Spear Phishing:

Während Phishing eine möglichst breite Masse abdeckt, ist eine Spear Phishing gezieltere Methode. Spear Phishing kommt besonders bei vulnerablen einzelnen Personen zum Einsatz. Ziel hierbei ist es, entweder eine einzelne Person oder einen gewissen Personenkreis mit einer Masche zu adressieren. Wie auch beim Phishing ist die Menge an relevanten Informationen,

[27] Scrapen beschreibt den Vorgang eines Programmes, welches Daten aus beispielsweise Webseiten auslesen kann. Dabei kann der „Scraper“ gezielt nach Informationen wie E-Mail-Adressen, Namen oder Telefonnummern suchen.

die für den Vorwand benötigt wird, hierbei maßgebend für den Erfolg eines Angriffs. Jedoch werden für Spear Phishing teils deutlich mehr Details benötigt, um den Vorwand glaubwürdiger zu gestalten.

Damit Betrüger gezielt an Informationen ihrer Opfer gelangen können, bedienen sich die Mehrzahl vorwiegend der Open-Source Intelligence[28]. Hierbei kann der initiale Schritt die Recherche in Social-Media sein, um Ansatzpunkte für einen möglichen Angriff zu finden.

Darüber hinaus kann das Dumpster Diving[29] auch eine effektive Methode sein, um Auskunft über private Daten eines Opfers zu erhalten. Häufig ist es so, dass viele Menschen ihre privaten Dokumente, wie Kontoauszüge und Informationen zur Gesundheit, wie Rechnungen, Schreiben oder Atteste nicht ausreichend sicher vernichten oder verfremden, wodurch Betrüger zumindest bei Privatpersonen leicht an schützenswerte Informationen gelangen. In Bezug auf Unternehmenssicherheit ist das Dumpster Diving selbst mit viel Aufwand und auch Glück verbunden. Die Dokumente und Datenträger sowie deren Vernichtung sind für Unternehmen, welche mit sensiblen Daten arbeiten in Schutzklassen unterteilt. Dies wird durch die europäische Norm EN 15713 seit August 2009 bestimmt. Diese sieht vor, dass Daten endgültig vernichtet werden sollen, um eine Wiederherstellung unbefugter Dritter zu verhindern.

[28] Open-Source Intelligence beschreit das Sammeln von Information über ein Ziel (Person, Server, Dienst), welche sich frei in den Medien finden lassen. Dabei kann es sich um Soziale Medien, Anleitungen oder Veröffentlichungen in jeglicher Form von Medien handeln, die frei zugänglich sind.

[29] Durchsuchen des privaten Mülls nach vertraulichen Dokumenten, Informationen oder Datenträgern, die Auskunft über eine Person oder ein Unternehmen geben.

Die Grafik in Abbildung 10 „Informationen und deren Schutzklassen“ veranschaulicht, die 3 Schutzklassen und die wesentlichen 5 Sicherheitsstufen dabei.[73]

Abbildung 5 Informationen und deren Schutzklassen[74]

Neben der Open Source Intelligence Suche und dem Dumpster Diving, kann bei speziellen Situationen auch eine Personenbeschattung in Betracht gezogen werden. Dies findet allerdings in der Praxis bei einem Online-Banking Betrug unter Betrügern nur selten Anwendung, da die Täter sich wie bereits eingänglich erwähnt oft im Ausland befinden und auch das Risiko des entdeckt werden eine große Rolle dabei spielt. Jedoch ist es nicht auszuschließen, dass eine Überwachung stattfinden könnte, um im Vorfeld Informationen über die finanziellen Verhältnisse auf Basis von Eigentum, den Arbeitgeber oder des Tagesablaufs ermitteln zu können. Auf Basis der erbeuteten Informationen können speziell zugeschnittene Betrugsmaschen geschaffen werden, welche für das Opfer umso glaubwürdiger erscheinen, durch die Masse der Informationen.

5.2.3. Pretexting

Bei der Erstellung einer Betrugsmaschen, ist es zwingend notwendig vorher einen Pretext festzulegen, welcher den Rahmen für die Umsetzung vorgibt. Im Laufe des Kapitels wird daher aufgezeigt, welche psychologischen Tricks Betrüger verwenden, um ihre Geschichte möglichst glaubhaft auszugestalten und dabei gleichzeitig Druck auf ihre Opfer aufbauen.

Im Buch „Die Kunst des Human Hackings – Social Engineering in der Praxis“ beschreibt Christopher Hadnagy Pretexting als: „die Schaffung eines erfundenen Szenarios, um die Zielperson als Opfer dazu zu überreden, Informationen herauszurücken oder eine Aktion auszuführen. Dazu gehört mehr, als nur eine Lüge vorzugaukeln. In manchen Fällen schafft man dazu eine komplette Identität, mit der man sich dann die Informationen erschwindelt. Social Engineers nutzen Pretexting, um Menschen in bestimmten Jobs oder Rollen zu verkörpern, die sie selbst noch nie ausgeführt haben.“ [68, S. 111]

Pretexting ist demzufolge das Erschaffen eines Vorwands, um mit einem Opfer in Kontakt zu treten. Hierfür werden häufig auch psychologische Tricks verwendet, um das Opfer zu diesen Handlungen zu verleiten. In den folgenden Punkten dieses Kapitels wird für die Erläuterung der Beispiele, lediglich von einem telefonischen oder einem Kontakt per Mail ausgegangen, da dies die häufigsten Mittel der Kontaktaufnahme sind.

5.2.3.1. Pretexting Rahmen

Die meisten Pretexting Ansätze von Betrügern lassen sich auf 3 wesentliche Rahmenbedingungen für deren Erfolg zurückführen.

- Einfaches Pretexting:

  Das Anliegen der Betrüger muss meist für das Opfer leicht verständlich und bestenfalls ein aktuelles Thema in den Medien sein. In Zeiten von Cyberangriffen und Datenleaks ist beispielsweise ein Hackerangriff für ein potenzielles Opfer ein valider Grund, warum es handeln sollte. Leichtverständliche Gründe wären auch Gesetzesänderungen oder Änderungen der Allgemeinen Geschäftsbedingungen. Diese sind recht häufig und von den meisten Menschen werden diese nicht weiter hinterfragt oder besonders im Fall der AGBs selten erst gelesen. Aufschluss gibt eine Studie der Plattform Statista von 2017, welche 896 Personen befragt hat, wie häufig diese die AGBs bei Onlinekäufen gelesen haben. Nur 7% der Befragten gaben an, dass sie immer die AGBs lesen würden und 22% gaben

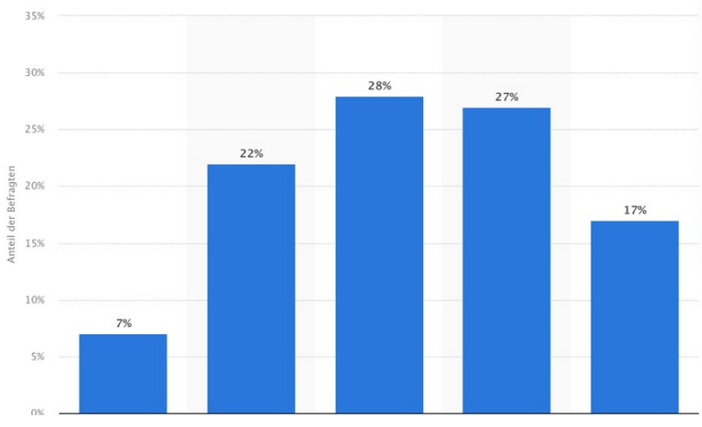

Abbildung 6 Statistik "Wie viele Personen lesen AGB's"

an, dass sie sie meistens lesen würden (Abbildung 11 Statistik "Wie viele Personen lesen AGB's"). Diese niedrigen Zahlen geben im Umkehrschluss darüber Auskunft, dass die Wahl dieses Vorwands bei ca. 72% aller Betroffenen funktionieren könnte und unterstreicht die These.[68], [75, S. 121–123]

- Flexibilität

  Ein weiterer Punkt, warum Betrüger oft mit ihren Pretexting erfolgreich sind, ist die Fähigkeit flexibel auf Fragen ihres Opfers. Häufig ist es zwar so, dass es für viele Telefonbetrugsmaschen einen Leitfaden gibt, an denen sich die Kriminellen orientieren können, jedoch sind diese dadurch nicht auf unerwartete Ereignisse vorbereitet. Ebenfalls kann das zu starke Orientieren an dem Telefonleitfaden, auf das Opfer als unerfahren oder zu steif wirken, wodurch gegebenenfalls Misstrauen entstehen könnte. [68, S. 124–125]

  Der Punkt der Spontanität lässt sich ebenfalls auch auf das Anpassen des Pretexts beziehen. Häufig werden bestehende Maschen einfach weiterentwickelt und dem aktuellen Weltgeschehen angepasst. Mit steigenden Cyberattacken aus Russland und Nordkorea ließe sich somit die Idee der geänderten AGBs leicht weiterentwickeln, dass für weitere Schutzmaßnahmen beispielsweise die Freigabe des Kunden benötigt wird und hierfür eine TAN bestätigt werden muss.

- Interesse wecken/ Notwendigkeit schaffen

  Damit Betrüger ihr Opfer möglichst schnell an sich binden, ist es für die Umsetzung des Pretextings elementar notwendig. Dabei wird der Vorwand so zu gestalten, dass das Opfer entweder eine Notwendigkeit sieht, weiter mit dem Betrüger zu kommunizieren oder das Interesse zu wecken. Wichtig für den Täter ist es nur, dass der Pretext glaubhaft bleibt und das Opfer weiterhin gewillt ist, auf ihn einzugehen. Wichtig bei dem Schaffen der Notwendigkeit ist es, dass dem Opfer suggeriert wird, dass es auf das Problem eine einfache und bestenfalls schnelle Lösung gibt, welche der Betrüger bietet. Um den Sachverhalt etwas besser darzustellen sind konkrete Beispiele geeignet.[68, S. 114–116]

Pretexting Beispiel - Eigeninteresse des Opfers:
„Im Rahmen der Urteilssprechung des BGH sind die Banken dazu verpflichtet Kunden über die Änderung der AGBs und damit verbunden der Änderung der Kontoführungsgebühren zu informieren. Im Rahmen dessen möchten wir Ihnen die zu Unrecht erhobenen Gebühren zurückerstatten. Diese belaufen sich auf die Summe X, bitte geben Sie die TAN frei, damit wir Ihnen die Summe Gutschreiben können.“ Der Betrüger hat in diesem Fall bereits Zugriff auf das Online-Banking des Opfers und erstellt eine Überweisung zu seinen Gunsten. In dem Moment in dem das Opfer die TAN herausgibt, kann die Überweisung durchgeführt werden.[76]

Pretexting Beispiel – Notwendigkeit schaffen:
„Im Rahmen unserer regelmäßigen Überprüfungen konnten wir drei verdächtige Überweisungen ausfindig machen, welche sich auf Betrüger zurückführen lassen. Bitte geben Sie die TANs frei, damit wir die Überweisungen noch aufhalten können.“ Auch hier haben die Betrüger bereits Zugriff auf das Online-Banking des Opfers. Die Kriminellen erstellen im Vorfeld die Überweisungen während des Telefonats. Dadurch soll der Eindruck entstehen, die Anrufer wären wirklich vom Kundensupport der Bank. Der Kunde sieht folglich die Notwendigkeit des Handlungsbedarfs, da er nicht das Geld verlieren möchte und der Betrüger ihm eine leichte Lösung auf sein Problem bietet. In Folge dessen führt das Opfer eine unüberlegte Handlung durch und gibt die Überweisungen frei. Wie die Emotionen durch Betrüger so manipuliert werden, dass diese auf ihre Opfer gezielt Druck ausüben können wird im folgenden Kapitel näher erläutert.

5.2.3.2. Spiel mit Emotionen

Damit Betrüger ihre Opfer für Ihre Methoden gefügsamer machen, wird für jeden Masche immer mindestens eine Emotion als fester Bestandteil des Pretext verwendet. Dies macht Menschen in der Regel empfänglicher für den gewählten Pretext und kann je nach gewähltem Ansatz das Gespräch bzw. die Masche in eine spezifische Richtung lenken.[77], [78]

- Vertrauen
  Vertrauen ist einer der häufigsten Faktoren, der genutzt wird, um das Opfer in den Betrug zu verwickeln. Zum einem nutzen Betrüger hierfür Informationen, welche sie

über das Opfer gesammelt haben, um sich beispielsweise als Mitarbeiter der Bank auszugeben. Zum anderen sind Betrüger meist geübt darin, ihre Stimmlage möglichst ruhig und sympathisch klingen zu lassen, um dem Opfer möglichst freundlich entgegenzutreten. [79]

- Gutgläubigkeit

  Sind Menschen in dem Glauben, sie würden etwas Gutes tun, sind deutlich eher gewillt Anweisungen Folge zu leisten. Dies setzt voraus, dass sie in dem Glauben gelassen werden, dass sie in einem Eigeninteresse handeln oder aus Nächstenliebe etwas für andere wie z.B. Familienangehörige tun. Exemplarisch für einen Pretext mit diesem Ansatz wäre z.B. das Investieren in eine Versicherung zu Gunsten der Kinder oder der Enkel.

- Angst/ Druck

  Durch das Schaffen von Angst und daraus folgend Druck, kann ein Opfer zu Entscheidungen gezwungen werden, welche aus Verzweiflung resultieren. Das Aufzeigen von einer erfundenen Notwendigkeit des Handelns (z.B. Geldverlust), wird häufig durch die Faktoren Druck (z.B. begrenzter Zeitraum „wir müssen jetzt handeln“) und das Aufzeigen von vermeintlichen Konsequenzen (z.B. Drohen mit Strafen) ergänzt. Ebenfalls werden dabei Dysphemismen [30]wie „Drahtzieher, finanzielles Desaster oder Justiz-Albtraum“ verwendet, um das Opfer von möglichst fatalistischen Ausgängen des Szenarios zu erzeugen.

- Neugier

  Neugier ist ein Urinstinkt des Menschen, was sich Betrüger auch zu Nutze machen. Besonders kommt diese Taktik bei Phishing-Mails zum Einsatz, wobei das Interesse des Opfers geweckt werden soll. Dies wird besonders gut veranschaulicht, in Mails wie „es befindet sich eine neue Nachricht in Ihrem Postfach“ oder „nähere Detail finden Sie im Anhang dieser Mail“. Ebenfalls kann dies auch häufig mit

[30] Dysphemismen – negativ behaftete Synonym oder Übertreibung eins Wortes. Bsp.: Justizalptraum statt rechtliche Konsequenzen.

Glücksgefühlen kombiniert werden, bei denen Betreffe wie „Sie haben gewonnen“ verwendet werden können.

- Ungewissheit
  Vielen Menschen ist es häufig gar nicht bewusst, welcher Schaden durch die Herausgabe von Informationen entstehen kann. Durch das Schaffen von „quid pro quo“ [31] Situationen durch geübte Social Engineering Methoden, können gezielt unscheinbare Informationen entlockt werden. Eine mögliche Situation kann beispielsweise das Benötigen einer Ausweiskopie sein, oder Bankinformationen, um im Nachhinein diese Informationen für kriminelle Machenschaften zu verwenden. Eine Ausweiskopie kann beispielsweise schon verwendet werden, um bei einigen Banken ein Konto zu eröffnen, sollten die Identifikationsverfahren nur unzureichend durchgeführt werden.

- Gier/ Neid
  Häufig werden bei Betrugsmaschen, welche in Verbindung mit Geld stehen, die Emotionen Gier und Neid angesprochen. Potenzielle Opfer werden häufig mit unrealistischen Renditen gelockt, um diese in ein System zu ziehen, in dem häufig hohe Verluste zu erwarten sind. Betrüger versuchen dabei gezielt auf große Wünsche ihres Ziels einzugehen (z.B. teure Sachwerte) und dessen Vertrauen mit vermeintlich Sicherheiten zu gewinnen. Ergänzt wird dies durch Aussagen, welche das Opfer entweder in falscher Sicherheit wiegen sollen oder es zum Kauf anreizen wie „100% Sicherheit, schnelle Erträge, absolute Flexibilität“. Ergänzend kommt die Verwendung von Suggestion durch Sozialen Bewährtheit hinzu, wie viele schon mit dem Angebot erfolgreich waren.

5.2.4. Methoden des Online-Banking Betrugs

Im Kapitel 5.2.2 Kontaktaufnahme wurde näher erläutert, wie Betrüger an die Daten der Opfer gelangen. Im Folgenden werden die Methoden genauer analysiert, wie einzelne Ansätze

[31] Gegenleistung – wie du mir so ich dir

konkret ablaufen können, welche Social Engineering Verfahren den Ansätzen zugrunde liegen, sowie auf die Historie eingegangen. Zur Veranschaulichung werden die vorgestellten Ansätze anhand von Beispielen verdeutlicht.

Falscher Bankmitarbeiter:

Geht man davon aus, dass die Kriminellen bereits über Kontaktdaten des Opfers verfügen, so kann das Opfer mit Hilfe eines geeigneten Pretextings angerufen werden. Damit der falsche Berater nicht bei diesem Schritt schon fehlschlägt, bedienen sich viele einer Methodik des Telefon-Spoofings.[79] Dabei handelt es sich um eine Manipulation der Call-ID des Anrufers. Dies erfolgt häufig über die Verwendung eines VoIP[32]-Telefons, bei denen die „Display-Information“ im Vorfeld angegeben werden können, um eine falsche Telefonnummer zu simulieren. Ziel dessen ist es, das Vertrauen des Opfers zu erhalten, indem man mit einer ihm bekannten Telefonnummer anruft. Für diese Vorgehensweise wird demnach meist die Telefonnummer der Bank, oder gar des Kundenberaters verwendet. [80]

Im weiteren Verlauf des Gesprächs wird ein Vorwand angegeben, um den Kunden zu einer Überweisung zu bringen. Meist haben die Täter dafür bereits Zugriff auf den Account des Online-Banking des Opfers. Mögliche Pretexting Ansätze können hierbei das Abwehren einer fingierten Bedrohung sein oder das Vorspielen des kundenorientierten Bankmitarbeiters, der nur helfen möchte.

Im ersten Fall wird meistens mit Angst und Druck gearbeitet und dem Opfer eingeredet, dass es einen immensen Geldschaden hätte oder gar rechtliche Konsequenzen, wenn man jetzt nicht handeln würde. Täter haben hierbei bereits eine Überweisung vorbereitet, deren TAN nur durch das Opfer verifiziert werden kann. Um das Pretexting weiter auszubauen, wird dem Kunden unterbreitet, dass die Überweisung gestoppt werden kann. Dafür benötige man nur eine TAN als Bestätigung, dass man hier im Kundeninteresse handle. Das Opfer wird dabei so manipuliert und unter Druck gesetzt, dass es dabei nicht bemerkt, wie es letztendlich die Überweisung freigibt, anstelle dass es den tatsächlichen Betrug verhindert.

[32] VoIP- Voice over IP, stellt eine Möglichkeit dar, über das Internet zu telefonieren

Im zweiten Fall wird sich dem Vertrauen, der Gutgläubigkeit und dem Gefühl des Glücks bedient. Viele Kunden befassen sich wenig bis gar nicht mit aktuellen Gesetzestexten und Banken-Regulatoren, sodass Kriminelle dies gut als Pretexting verwenden können. Ein Beispiel hierfür wäre die Ausdehnung der EU-Richtlinie PSD2, die Banken dazu auffordert, das Online-Banking alle 180 Tage durch ihre Kunden verifizieren zu lassen.[56] Ändert man die Auswirkungen des Ausbleibens ab und zwar, dass das Online-Banking nicht nur gesperrt wird, sondern das ganze Konto, so können besonders in Vorweihnachtszeiten oder in der Urlaubssaison Drucksituationen entstehen. Ein solches Szenario bedient sich der Angst der Opfer. Bietet der falsche Kundenberater jetzt auf das vermeintliche Problem die einfache Lösung und geht den Prozess mit dem Kunden gemeinsam durch, so tendieren Opfer in der Regel folgsamer zu sein, da gerade technisch unbedarfte Menschen über die Hilfe dankbar sind. Wie auch im ersten Fall wird jetzt dem Opfer im fingierten Verifikationsprozess eine Überweisung vorgelegt, welches das Ziel allerdings nicht realisiert, sodass dieses im Zweifelsfall der Auftrag des Betrügers freigegeben wird, um die Situation schnellstmöglich zu lösen.

Mit Hilfe von Vishing[33] können geübte Täter ihr Ziel so manipulieren, dass dieses trotz alledem denkt, der Täter sei ein Angestellter seiner Bank.[81] Ein geübter Social Engineer kann somit auch ohne große technische Mittel sein Opfer in die Falle locken. Dass Betrüger für diese Art von Online-Banking-Phishing wenig technische Vorkenntnisse benötigen, zeigt auch das Angebot von Crimeware-As-A-Service. Dabei stellen Cyberkriminelle Schadsoftware bereits für umgerechnet rund 15$ auf Darknet-Markplätzen ein, welche Betrüger bei ihren Phishing-Kampagnen unterstützen sollen. [82]

[33] Vishing – stellt eine spezielle Form des Phishings dar, bei dem Kriminelle organisiert Personen anrufen (häufig unter der Verwendung von Spoofing), um finanzielle oder persönliche Informationen von dem Opfer zu erhalten um entweder eine spätere Masche vorzubereiten oder die Person dazu zu bringen, Geld zu überweisen oder eine andere Handlung durchzuführen.

Phishing/ Smishing:

Phishing und Smishing [34] stellen im Vergleich zu Vishing einen unpersönlicheren Ansatz dar, da das Pretexting meist initial nur schriftlich erfolgt. Die Kriminellen haben folglich keine Möglichkeit, um auf eventuelle Bedenken der Opfer zu reagieren. Zunächst wird durch eine fingierte Nachricht das Opfer dazu bewegt, auf einen Link zu klicken, um die Masche der Betrüger zu starten. Meist bedienen sich diese Nachrichten einem bankenüblichen Sprachgebrauch, um möglichst glaubhaft zu wirken und bei ihrem Opfer eine Vertrautheit zu bewirken. Dies kann verstärkt werden durch die Hinzunahme von E-Mail-Header Spoofing.

E-Mail-Header Spoofing beschreibt den Vorgang von Betrügern, bei dem sie die Mailadresse des Absenders verschleiern. Dies kann durch verschiedene Methoden erreicht werden. Beispielsweise kann dies durch die Verwendung des Dienstes „sendemail“ erfolgen, welcher bereits bei Kali Linux vorinstalliert ist. Allerdings können sich Betrüger auch den mangelnden technischen Kenntnissen der Empfänger zunutze machen und schlicht den Autorennamen der Mail verändern um einen anderen Absender vorzutäuschen, da dies der Teil der Mail ist, der üblicherweise bei E-Mail-Dienstleistern angezeigt wird.[83]–[85]

Die Ziele der Methode lassen sich im Grund auf zwei Möglichkeiten beschränken.

Einerseits versuchen Täter das Opfer zur Preisgabe von persönlichen bzw. vertraulichen Daten zu überzeugen. Andererseits kann auch Schadsoftware auf dem Gerät des Nutzers installiert werden, um eine Attacke auszuführen oder eine künftige vorzubereiten.

Dabei ist ein möglicher Ansatz unter anderem der folgende, welcher eine reelle Phishing-Mail darstellt (Abbildung 12 Phishing-Mail).

[34] Smishing – stellt eine Sonderform des Phishings dar, bei der Kriminelle ihre dem Opfer fingerte Nachrichten (wie bei Phishing) via SMS oder Mobile Messenger wie Whatsapp oder Telegram schicken. Ziel ist es dem Opfer vertrauliche Daten zu entlocken oder es zu Handlungen zu bewegen, welche es normalerweise nicht tun würde, wie das Tätigen von Überweisungen oder die Installation von Schadsoftware auf dem Mobilen Endgerät.

Abbildung 7 Phishing-Mail

Wie bereits im Pretexting näher erläutert, versuchen Betrüger hier mit der Änderung von internen Leitlinien durch den Satz „Es ist zwingend erforderlich, dass Sie dieses Update durchführen." Druck auf das Opfer auszuüben, um es zu einer Entscheidung zu zwingen. Im weiteren Verlauf leiten die Täter das Opfer zu einer Phishing-Seite weiter. Dabei kann es sich entweder um gehackte Domains handeln, in denen Phishing-Seiten versteckt werden aber auch um sogenanntes Squatting. Bei Squatting verwenden Täter ähnliche Namen für ihre URL oder verwenden andere Top-Level-Domains[35], um ihre Opfer in die Irre zu führen und die Phising-Seite zu verschleiern.[86] Im Anschluss dazu versuchen die Kriminellen, den Login des Bankkunden durch eine gefälschte Login-Maske zu erlangen, um sich Zutritt zum Konto des Nutzers zu verschaffen. Nachdem der Nutzer seine Daten eingegeben hat, haben die Betrüger nahezu uneingeschränkten Zugriff auf das Konto des Opfers. Im Folgenden können die Täter sich auf Methodiken berufen, welche bereit im Teil „Falscher Bankberater" erläutert wurden.

Ebenfalls können Phishing-Kampagnen auch dazu genutzt werden Opfer mit Spam Mails nahezu handlungsunfähig zu machen. Während für das Versenden der Phishing-Mails entweder unzureichend gesicherte Mailserver oder E-Mail-Header Spoofing verwendet wird, kann die Return-Adresse der Mail ebenso angepasst werden. Dies hat zur Folge, dass die E-Mail-Adresse, welche als Return-Adresse hinterlegt wurde, jede Unzustellbarkeitsbenachrichtigung einer Phishing-Kampagne erhält. Im Rahmen dieser Arbeit konnte ein Opfer dieser Masche ermittelt werden. Hierfür wurde der Mail-Header der in

[35] Bei Top-Level-Domains handelt es sich um die Endung einer URL, welche Aufschluss über die Art oder Herkunft einer Seite geben kann. Bekannte Endungen können z.B. „.de", „.com" oder „.net" sein.

„Abbildung 12 Phishing-Mail“ gezeigten Mail genauer analysiert und der Kontakt hieraus ermittelt. Das Opfer (welches darum bat nicht namentlich in dieser Arbeit genannt zu werden) gab an, dass es sich dabei um mehrere tausend Nachrichten handle, welche über einen Zeitraum der letzten sechs Monate auf seine Geschäftsmailadresse gesendet wurden.

5.3. Anwendungsbeispiel – Aufbau einer eigenen Phishing-Seite

Um die erläuterten Techniken besser zu verdeutlichen, wurde ein Anwendungsbeispiel konzipiert, welches ein Angriffsszenario darstellen soll. Dabei wurde sich an reellen Konzepten orientiert, sodass der Ansatz der eigens erstellen Phishing-Seite möglichst praxisnah ist (Abbildung 13 Aufbau des Praxisversuchs).

Abbildung 8 Aufbau des Praxisversuchs

Schritt 1 Pretexting:

Bei der Erstellung des Pretextings wurde zunächst darauf geachtet, dass es sich um ein aktuelles Thema handelt, welches medial häufiger aufgetreten ist. Optionen hierfür waren unter anderem die Gültigkeit von DORA oder eine Änderung des Zinssatzes, wofür die Bank ein Einverständnis vom Kunden benötigen würde. Aufgrund des aktuellen Weltgeschehens wurde sich allerdings auf eine Cyberattacke gegenüber dem Sparkassenverbund festgelegt. Die Thematik war in der Vergangenheit immer häufiger in den Medien zu sehen, wie unter anderem die Überschrift auf der Startseite des Mailproviders WEB.de „BSI-Chefin: Bedrohung durch Cyberangriffe so groß wie nie zuvor“.[87]

Der Pretext für den Betrugsversuch sieht also wie folgt aus:

Das Opfer soll durch den Vorwand eines Datenlecks angeschrieben werden. Als Absender soll hierbei der Sparkassenverbund dienen, welcher alle Kunden initial anschreiben soll, um darauf hinzuweisen, dass ein Datenleck vorlag und russische Hacker einige Daten deutschlandweit erbeuten konnten. Der Sparkassenkunde soll nun seine Daten zur Legitimierung angeben, um einerseits zu prüfen, ob er selbst von dem Datenleck betroffen ist und andererseits ob ggf. Schadensersatzansprüche vorliegen könnten. Dies soll sowohl Angst als auch die Ungewissheit im Opfer auslösen, sodass dieses nicht darüber nachdenkt, ob es sich dabei um eine Falle handeln könnte.

Schritt 2 Aufsetzen der Phishing-Seite:

Als technische Basis für das Anwendungsbeispiel wurde Docker[36] gewählt. Hierbei wurden drei Docker Images verwendet, um die Grundstruktur für einen einfachen Webserver zu simulieren. Diese wurden hierbei mittels eines YAML-Scrips automatisch aufgesetzt. Hierfür wurde Apache als lokaler Webserver verwendet, MariaDB als Datenbankmanagementsystem und phpMyAdmin zur Administration und Verbindung der php Seiten mit dem Backend.[88], [89]

Name	Version	Docker Image ID
webdevops/php-apache	8.0	dfd22e1ea3bdb3fce9dd2f854cc0c0fa0341302f33823034cf209372f27c4905
mariadb	latest	4c3b22c29944fa51bc89674137073c8d979ddece8d6f0fd7cc996167ec9f01f3
phpmyadmin/phpmyadmin	latest	e4be0d1537f54c943b8489cdf0d4af0369e1a6110ea978090ae5e95a9a3f2c24

Darüber hinaus wurde eine stilähnliche Seite anhand des Sparkassen Farbschemas erstellt, um dem Nutzer ein möglichst vertrautes Gefühl zu geben. Sobald der Nutzer auf die Seite geht, wird ein Session Cookie gesetzt, welches das Zuordnen der Eingaben in der Datenbank ermöglicht. Im Verlauf der Simulation werden die Daten aus den Formularen der einzelnen Seiten in die Datenbank übertragen. [89]

[36] Docker ist ein Programm welche virtuellen Umgebungen in Form von Containern erstellt und in seinen isolierten Umgebungen laufen lässt.

Schritt 3 Durchführung eines hypothetischen Phishing-Szenarios:

Im Rahmen des Anwendungsversuchs ist es vorgesehen, dass der Link der Phishing-Seite per Mail an einen Empfängerkreis gesendet wird. In der Mail wird das Opfer der Phishing Kampagne darüber informiert, dass Hacker Daten der Sparkassen erbeutet haben. Der Nutzer wird dazu aufgerufen, seine Daten in die verlinkten Seiten einzugeben, um seine Identität zu bestätigen und zu prüfen, ob er von dem Daten-Leak betroffen ist. Nach dem Ausfüllen der Seite wird eine gefälschte Bestätigung angezeigt, dass die Daten des Nutzers erbeutet wurden. Da nun einem Betrüger die Daten eines Opfers vorliegen, kann dieser sich in dessen Account einloggen und einen neuen Registrierungsbrief für das Online-Banking an eine neue Adresse senden lassen. Letztendlich erhalten Betrüger somit einen kompletten Zugriff auf das Konto des Opfers. Im Rahmen des Proof of Concept wurde von einem Online-Login auf der tatsächlichen Sparkassen Seite abgesehen. Dies hat den Hintergrund, dass die Daten der Phishing-Seite öffentlich auf Github liegen, als auch, dass etwaige rechtliche Konsequenzen vermieden werden sollen.

Alternativ können Kriminelle auch auf Basis der erbeuteten Daten den Pretext des falschen Kundenberaters verwenden und unter Verwendung der Kundendaten Rapport und Authentizität gegenüber dem Opfer erreichen.

5.4. Prävention gegen Phishing

Die Möglichkeiten der Prävention gegen Phishing können unterschieden werden in automatisierte und manuelle Maßnahmen. Automatisierte Maßnahmen können systemseitig implementiert werden und sind häufig in vielen Anwendungen vertreten. Bei manuellen Maßnahmen handelt es sich um Prävention, welche vom Nutzer verinnerlicht werden sollte, sollte er Zweifel an der Echtheit einer Mail haben.

5.4.1. Automatisierte Präventionsmaßnahmen

Mail-Header

Wie bereits im Punkt 4.2.4.1. Betrugsmaschen im Fokus angesprochen, ist es Betrügern möglich den Mail-Header einer Nachricht zu bearbeiten. Dem kann sowohl automatischer als auch von manueller Seite entgegengewirkt werden. Um zu überprüfen, ob es sich um eine Phishing-Mail handelt, kann wie folgt vorgegangen werden:

Im 1. Schritt sollte geprüft werden, ob der Name und die Absende-Adresse der Mail übereinstimmen. Sollte dies bereits nicht der Fall sein, ist stark davon auszugehen, dass es sich hierbei um eine gefälschte Mail handelt (Abbildung 14 Falscher Absender).

Abbildung 9 Falscher Absender

Für Schritt 2. sollte die Return-Adresse genauer überprüft werden. Diese ist für die Übermittlung einer Unzustellbarkeitsmitteilung verantwortlich und kann von der regulären Absende-Adresse abweichen. Auffälligkeiten ergeben sich allerdings, sollte dabei ein völlig anderer Mailserver, welcher in keiner Verbindung zum Absender steht, angegeben sein.

Mit Schritt 3 wird das Sender Policy Framework, kurz SPF durch den Mail-Server Provider geprüft. Dafür werden im Vorfeld dem Domain Name System (DNS) alle IP-Adressen, welche berechtigt sind im Namen der Domain zu handeln und demnach auch Mails zu versenden, übermittelt. Im Folgenden wird beim Empfang einer Mail eine DNS-Abfrage gestellt und geprüft, ob die IP-Adresse des Versenders autorisiert war, im Namen des Absenders zu handeln (Abbildung 15 Ablauf SPF). Dafür gibt es vier Fälle, welche das SPF annehmen kann:

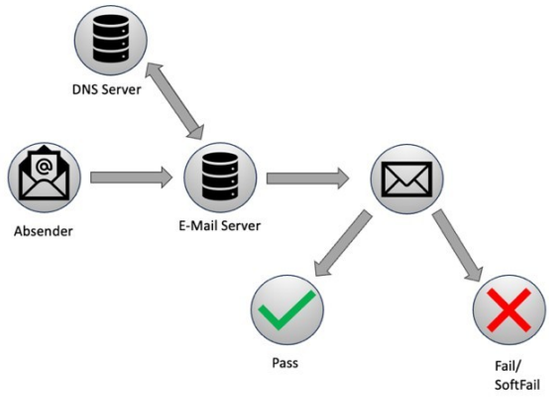

Abbildung 10 Ablauf SPF

- Pass – Mail wurde von einer legitimierten Adresse aus verschickt
- Fail – Der Absender war nicht legitimiert und wurde nicht vom Empfängermailserver akzeptiert
- SoftFail – Der Absender war nicht legitimiert, die Mail wurde jedoch akzeptiert und als Spam gekennzeichnet
- Neutral – Es können keine Aussagen zur Mail gemacht werden.[90]

Der 4. Schritt befasst sich mit DKIM – Domainkey Identified Mail und DMARC - Domain-based Message Authentication, Reporting and Conformance. Bei DKIM handelt es sich um eine Verschlüsselungsmethode mit dem SHA-256 Algorithmus um verschlüsselte Mails zu versenden und zu signieren. Dabei wird ein Hashwert aus Teilen der Mail und deren Header gebildet und mit einem Verschlüsselungsverfahren wie etwa RSA durch den privaten Schlüssel signiert. Erhält der Empfänger die Mail, prüft dessen Mailserver nun über den DNS-Server des Absenders, ob es einen passenden öffentlichen Schlüssel für die Nachricht gibt. Dies stellt die Sicherheitsaspekte der Integrität sicher, da es eine Aussage treffen kann, ob es sich dabei wirklich um den echten Absender handelt und ob die Nachricht nachträglich bearbeitet worden ist, was eine Veränderung des Hashs mit sich führen würde.[91]
DMARC wiederum dient ergänzend zu SPF und DKIM und gibt weitere Vorgaben durch den Absender wie mit der Verarbeitung von Nachrichten umgegangen werden soll. Hierfür werden ebenfalls wie bei DKIM und SPF auch Informationen vom DNS-Server des Absenders gelesen. Dies beinhaltet unter anderem:

- Wie soll eine Mail authentifiziert werden
- Umgang mit nicht authentifizierten Mails
- Berichterstattung an den Absender an extra hinterlegte Mails[92]

Passwortsicherheit

Passwortsicherheit schützt nicht vor Phishingversuchen, jedoch im Ernstfall vor einer Kontenübernahme oder dem Missbrauch der eigenen Daten durch Betrüger, in Form von Identitätsdiebstahl. Um dem vorzubeugen, sollte falls möglich immer eine geeignete Multi-Faktor Authentifizierung verwendet werden, da diese mindestens zwei der drei Faktoren „Haben“, „Wissen“, „Sein“ erfordert (wie in Kapitel 4.1.1 Historie des Tan-Verfahrens erläutert). Dies ist durch die Verwendung von TAN-Verfahren bei Banken immer mit enthalten. Nutzer sollten immer, sofern die Möglichkeit besteht, auf zusätzliche Sicherheitsmaßnahmen der Seiten zurückgreifen. Ebenfalls sinnvoll für die Passwortsicherheit ist die Verwendung eines Passwortmanagers, bzw. eines Passwortgenerators. Ziel dessen ist es, nicht für mehrere Seiten ein Passwort oder Iterationen dessen zu verwenden, welche durch ein Datenleak im Internet frei einsehbar wären, hierbei spricht man von Credential Stuffing.

Mailanhänge

Ein verbreitetes Einfallstor für Schadsoftware und folglich auch für Phishing-Maschen ist das Versenden von manipulierten Anhängen via Mail. Eine Statistik der Seite Purplesec zeigt auf, dass mehr als die Hälfte aller Schadsoftware, welche in Verbindung mit Social Engineering und Phishing steht, im Jahr 2020 mit Microsoft Office Produkten in Verbindung steht: [93]

- Microsoft Word (39.3%)
- Microsoft Excel (8.7%)
- Executable (19.5%)
- Rich text (14%)
- Java archive files (5.6%)

Um diesen Faktor auszuschließen, sollten im Allgemeinen keine Anhänge von Mails geöffnet werden, deren Herkunft unbekannt ist und welche von einer abweichenden Mailadresse als die übliche Kommunikation stammen. Ebenfalls sollte geprüft werden, ob die übermittelten Daten auch anderweitig abrufbar wären. Banken versenden in der Regel keine Kontoauszüge per Mail, sondern würden diese eher in das Online-Postfach des Nutzers einstellen. Dies bezieht sich beispielsweise auf Kommunikation mit Banken. Diese würden dem Kunden in der Regel keine Kontoauszüge oder Rechnungen per Mail zukommen lassen, da hierfür der Account und ein entsprechendes Postfach auf Seiten der Bank verwendet wird.

Anti-Virus Programme

Phishing-Mails sind ein Einfallstor für Schadsoftware. Um einer möglichen Übernahme durch Cyberkriminelle vorzubeugen, lohnt es sich eine geeignete Anti-Viren Software zu installieren, um verdächte Programme direkt bei Ausführungen zu stoppen und zu isolieren.

5.4.2. Manuelle Präventionsmaßnahmen

Allgemeiner Umgang mit sensiblen Informationen:

Der Umgang mit sensiblen Daten muss geschult sein, dies fängt mit dem aktiven Hinterfragen an, wo Informationen benötigt werden, warum diese benötigt werden und wie diese ggf. verarbeitet werden. Um diese Handlungsempfehlung auf Phishing zu beziehen, kann man sich folglich die Fragen stellen:

- Warum benötigt der Absender mein Einverständnis für eine Handlung, die er selbst durchführen könnte?
    - Zinssätze müssen zwar kommuniziert werden von der Bank, allerdings benötigen diese dafür nicht die Erlaubnis des Kunden, um diese anzupassen. Der Kunde hat dafür meist ein Sonderkündigungsrecht, sollte er diesen widersprechen.
- Warum benötigt der Absender Daten, die er eigentlich haben müsste?
    - Eine Postzusteller wird in der Regel nicht nach der persönlichen Adresse des Empfängers fragen, da diese auf dem Paket steht. Sollte dies nicht der Fall sein, würde dies eher wieder an den Absender gesendet werden.
- Warum benötigt der Absender neue Daten?
    - Wozu benötigt das Finanzamt die privaten Kreditkarten-Daten?
- Habe ich bereits unbewusst Informationen Preis gegeben, welche gegen mich genutzt werden können?
    - Telefonmeldung mit vollständigen Namen
    - Fragen nach einer Person „bist du es, XY?“

Nachrichten prüfen:

Phishing-Mails können mit verschiedensten Betreffen auftreten, seien es falsche Rechnungen, Angebote, Aufforderungen, sowie Informationen zu einem Produkt oder einer Dienstleistung. Meist sollten die Empfänger durch einige Fragen allerdings schon misstrauisch werden:

- Wird der Empfänger direkt angesprochen mit den Informationen, die dem Absender vorliegen sollten?
    - Verwendung des vollständigen Namens, Kundennummer, Adresse, Details die für das Anliegen benötigt werden

- Ist die Art der Kontaktaufnahme üblich?
    - Bsp.: Das Finanzamt wird eine Mahnung nicht per Mail verschicken
- Ist die Nachricht in einem adressatenüblichen Sprachgebrauch formuliert?
    - Förmliche Sprache bei Banken, Versicherungen und Ämtern
    - Befinden sich Rechtschreibfehler in der Mail?
    - Befinden sich Wörter wie „Dringlich“, „Mahnung“ oder „Wichtig“ im Betreff?
- Ist das Angebot oder die Forderung legitim und realistisch?
    - Ein überdurchschnittlich hoher Zinssatz bei einer Geldanlage
    - Wurde in einem Onlinehandel wirklich Ware bestellt?

Datenvernichtung:

Das Dumpster Diving oder Datenwiederherstellung bei Phishing-Attacken, welche tendenziell breite Massen aus der Ferne angreifen, unüblich sind wurde bereits in Kapitel 5.2.2. Kontaktaufnahme erläutert. Dennoch ist es wichtig seine eigenen Daten sicher zu entsorgen, um eventuelle Daten-Leaks vorzubeugen.

Um Dumpster Diving und ggf. Datenwiederherstellung von ausrangierten Festplatten zu vermeiden, sollte dabei darauf geachtet werden eine Lösung zu finden, welche es möglichst schwer macht, die Daten wiederherzustellen. So kann beispielsweise ein Aktenvernichter angeschafft werden, welcher Dokumente ausreichend klein zerteilt oder ggf. sogar CDs oder USB-Sticks vernichten kann. Ein anderer Weg zur Papiervernichtung kann daher schon das Zerreißen und getrennte Entsorgen der Dokumentenreste sein, sodass das Dumpster Diving erschwert wird. Alternativ dazu stellt das Verbrennen des Papiermülls auch eine Möglichkeit dar. Um Datenträger vor einer Datenwiederherstellung zu schützen, sollten diese fachgerecht formatiert oder zerstört werden. Hierfür sind Firmen ebenfalls an die europäische Norm EN 15713 gebunden. Für Privathaushalte gilt daher die Empfehlung, Datenträger entweder komplett zu vernichten, beispielsweise mittels Feuer, Dokumentenshredder oder durch physisches Einwirken. Alternativ kann eine Festplatte auch formatiert werden. Das BSI spricht für alte Festplatten dabei als Empfehlung das siebenfache Überschreiben der Festplatte aus, neuere Solid-State-Disks (SSD) wiederrum können durch die Anwendung des Befehls ATA-"Enhanced Security Erase" und der Hinzuziehung von einer Überschreibung der Daten resistent gegen eine Widerherstellung gemacht werden. Ebenfalls sinnvoll ist das

Verwenden von Programmen, welche dem Nutzer das Überschreiben der Daten vereinfachen.[94]

5.5. Fazit - Warum ist Online-Banking Betrug erfolgreich?

In dem Kapitel wurden zunächst die Motivation der Täter beleuchtet und der damit verbundene Wandel von Banküberfällen hin zur Online-Kriminalität. Es wurde anhand mehrerer Aspekte das Thema Social Engineerings verdeutlicht. Unter anderem wurde darauf eingegangen, dass Betrüger häufig bewusst die Emotionen des Opfers missbrauchen, um es zu Handlungen zu verleiten, welche es sonst nicht ausführen würde. Ebenfalls wurde das Pretexting erläutert, bei dem ein Vorwand erzeugt wird, um mit dem Opfer in Kontakt zu treten. Dieser Sachverhalt wurde an mehrere Praxisbeispielen gezeigt und es wurde erklärt, warum Opfer die verschiedenen Vorwände für glaubhaft halten. Anhand eines Anwendungsbeispiels wurde aufgezeigt, wie in der Praxis eine Phishing-Seite aufgebaut ist, und welche Möglichkeiten Betrüger haben, die erbeuteten Daten zu nutzen. Schlussendlich wurde auf die Möglichkeiten und Präventionsmaßnahmen des Phishings eingegangen und erläutert, technischen Mittel der Betrüger verwenden, bzw. wie sich dagegen geschützt werden kann.

Zusammenfassend lässt sich zu diesem Kapitel sagen, dass einer Bank zwar daran gelegen ist, sichere Systeme für ihre Nutzer zu implementieren, diese aber nur so sicher sind, wie das schwächste Glied der Kette. Nutzer sollten sich zumindest grundlegend über den Umgang mit den Onlineportalen, beschäftigen. Darüber hinaus sollten sie ihre eigenen Handlungen hinterfragen, insbesondere wann und ob die Preisgabe von Informationen wirklich sinnvoll und notwendig ist.

6. Angriffe auf Banken

Auch wenn Bankkunden ein leichteres Ziel für Hacker sind als die Banken selbst, sind diese nicht von Cyberattacken ausgenommen. Im Folgenden werden Angriffs-Methodiken sowie dazugehörige Praxisfälle aufgezeigt, wie Banken in der Vergangenheit Ziel von Cyberattacken wurden.

6.1. DDOS-Attacken

DDOS steht für Distributed-Denial-Of-Service und stellt eine Attacke dar, deren Ziel es ist einen Dienst vorrübergehend lahm zu legen. Hierfür werden die Dienste eines Servers adressiert und solange Anfragen gesendet, bis der Server diese nicht mehr verarbeiten kann und der Dienst zum Erliegen kommt.

2021 vermeldete die Nachrichtenagentur Reuters, dass die Fiducia & GAD IT AG Ziel einer solchen Attacke geworden ist. Diese stellte zu dem Zeitpunkt IT-Services für über 800 Banken, wie der Berliner Volksbank, zur Verfügung. Folge des Angriffs war, dass die Kunden des Dienstleisters, die zur Verfügung gestellten Services nicht mehr verwenden konnten und der Bankbetrieb nur eingeschränkt möglich gewesen ist. [95]

Hieraus lässt sich demnach der Schluss ziehen, dass nicht nur die Banken selbst, sondern auch deren Zahlungsdienstleister Ziel von Attacken werden können, da diese ebenfalls wie die Banken selbst, attraktive Ziele für die Kriminellen sein können.

6.2. Ransomeware-Attacken

Bei Ransomeware handelt es sich um Schadsoftware, welche über Umwege auf einem Gerät oder in einem Netzwerk installiert werden kann. Dabei muss die Attacke nicht unmittelbar erfolgen, die eingesetzte Schadsoftware kann auch vorerst entweder schlafen oder nur mithören. Ziel der Attacke ist es so viele Geräte wie möglich mit der Schadsoftware zu infizieren und vor allem möglichst kritische Bereiche zu erreichen, um anschließend die eigentliche Attacke auszulösen. Dabei werden die Daten verschlüsselt, teilweise auch kopiert und nur gegen eine Zahlung wieder frei gegeben. Der Nutzer wird also erpresst und dazu aufgefordert ein Lösegeld zu zahlen, im englischen „Ransome“. Dabei wird spezifische Summe in einer Kryptowährung zu verlang, damit der Nutzer seine Daten und den Zugriff zu seinem System wieder zurückzuerlangen.

Einer der wohl bekanntesten Fälle war die Ransomeware „Wanna Cry“ aus dem Jahr 2017, welche sich in den folgenden Jahren immer weiter entwickeln sollte. 2020 wurde die Spanische Bank Banco Bilbao Vizcaya Argentaria von einer Weiterentwicklung der Wanna Cry Schadsoftware namens „REvil“ infiziert.[96]

Die Bank ist nicht darauf eingegangen, ob das Lösegeld an die Kriminellen bezahlt wurde oder ob es ihnen möglich war, das System auf Basis ihrer Backups wieder herzustellen. Hieraus geht aber auch hervor, wie wichtig ein Notfallmanagement ist, sollte es zu einem kritischen Ereignis kommen.

6.3. Insider Attacken

Bei Insider Attacken handelt es sich um Angriffe, welche von Mitarbeitern innerhalb des Unternehmens ausgeführt werden. Das Besondere hierbei ist, dass sich Insider im Gegensatz zu anderen Angreifern, nicht erst Zugriffe und Privilegien zum System organisieren müssen, da sie bereits im Unternehmen sind. Ziel der Angreifer ist es hierbei, Schadsoftware in das Unternehmen einzuschleusen, gegebenenfalls Daten zu entwenden oder dem Unternehmen zu schaden.

Ein Fall der Capital One Financial Corporation aus dem Jahr 2019 zeigt auf, welche Folgen ein solcher Angriff haben kann. Page Thompson war damals eine Mitarbeiterin für Amazon Web Hosting (AWS), welche damals das Hosting für die Datenbanken der Capital One übernahmen. Während Ihrer Zeit bei AWS stahl die Mitarbeiterin 140.000 Sozialversicherungsnummern und 80.000 Bankaccount Nummern und stellte diese in ein soziales Netzwerk. Die Bank schätzt dabei den Schaden auf 150 Millionen Dollar. [97]

Durch den Fall wird deutlich, dass Sicherheit nicht nur im eigenen Unternehmen eine Rolle spielt, sondern ebenfalls bei den Dienstleistern, auf welche sich die Bank verlässt. Besonders die BAIT und DORA sehen extra Regelungen für die Dienstleister von Banken vor.

6.4. Malware

Bei Malware handelt es sich klassisch um Schadsoftware, welche in Form von Viren, Trojanern oder Würmern auftreten kann. Die Auswirkungen können dabei sehr unterschiedlich sein und reichen von Spionage, über unautorisierten Zugriffe bis hin zur kompletten Zerstörung eines Systems. Ein gängiges Mittel für die Übersendung von Malware sind Phishing-Mails.

Welche Auswirkungen Malware haben kann, zeigt der Fall der Bangladesh Central Bank, welcher als heute als größter Online-Bankraub bekannt ist.

2015 wurde eine Mail mit dem Vorwand einer Bewerbung, an mehrere Mitarbeiter des Unternehmens gesendet. Im Anhang befand sich ein Remote Access Trojaner[37], welche durch den Download des Anhangs und der Ausführung der Datei installiert wurde. Bei der Mail handelte es sich um eine Spear-Phishing-Mail, welche als Ziel bewusst mehrere Personen der Personalabteilung der Zentralbank adressierte. Nach Infizierung eines Rechners, weiteten die Hacker ihren Zugriff auf die Systeme der Zentralbank über den Zeitraum von einem Jahr aus. Letztendlich gelang es den Tätern, Zugriff auf einen Account zu erhalten, welcher Zugriff auf das SWIFT [38]Netzwerk[98] hatte. Die Hacker arbeiteten im Folgenden nun einen Plan aus, welcher vorsah, am Donnerstag, den 04.02.2016, 35 Zahlungsaufträge an die Federal Reserve Bank of New York über das SWIFT Netzwerk zu senden und somit 951 Millionen Dollar zu überweisen. Die New Yorker Bank hatte aufgrund von Formfehlern allerdings Rückfragen und wies die Aufträge zunächst ab. Im Folgenden wurden Diese korrigiert und erneut am Freitag, den 05.02.2016 gestellt und dieses Mal teilweise akzeptiert. Ziel der Überweisung waren vier Konten auf falschen Namen auf den Philippinen. Aufgrund der sabotierten Kommunikation innerhalb der Bangladesh Central Bank und der Wahl den Angriffszeitpunkt an einen Donnerstag auf Freitag zu legen, bemerkte den Angriff in Bangladesch zunächst keiner, da Freitag in Bangladesch ein Wochenendtag ist. Erst am Samstag, dem 06.02.2016 wurde der Angriff in Bangladesch bemerkt, jedoch konnte durch das Wochenende in New York und die Zeitumstellung zunächst niemand erreicht werden. New York überwies zunächst nur 101 Millionen Dollar an die vier falschen Konten auf den Philippinen, welche allerdings am Montag, den 08.02.2016 einen Feiertag hatten, wodurch auch hier niemand erreicht werden konnte. Aufgrund der präzisen Terminplanung konnte durch Ausnutzung der Feiertagsregelung eine maximale Diskoordination erreicht werden. Eine der zugelassenen Überweisungen enthielt jedoch einen Tippfehler, wodurch von den 101 Millionen nur 81 Millionen auf den Zielkonten ankamen. Die erbeutete Summe wurde danach in Casinos auf den Philippinen und in China gewaschen und mutmaßlich nach Nord-Korea überwiesen.

---

[37] Remote Access Trojaner ist eine Form der Maleware. Dabei haben Hacker die Möglichkeit Kommunikation und Programme des infizierten Nutzers auszuspähen, zu bearbeiten oder gänzlich die Kontrolle über das Gerät zu übernehmen.

[38] SWIFT - Society for Worldwide Interbank Financial Telecommunication, ist ein internationales Netzwerk zum Austausch von Informationen und Finanztransaktionen.

Demnach geht man hierbei von einer staatlich beauftragten Cyber-Attacke der Lazarus Gruppe aus. [99]–[102]

Zusammenfassend kann man zu diesem Fall sagen, das dieser als perfekte Fallstudie dient, wie das Zusammenspiel aus Phishing und Malware für ein Finanzunternehmen gefährlich werden kann und wie wichtig eine umfangreiche Cybersicherheit ist um sich auch vor staatlich organisierten Hacking-Angriffen zu schützen.

7. Rechtliche Einordnung

Um sowohl das Strafmaß für gefasste Täter, als auch die rechtlichen Absicherungen von Kreditinstituten und deren Kunden näher zu beleuchten, werden im folgenden Kapitel die rechtlichen Komponenten in den Vordergrund gestellt und anhand von Rechtsprechungen erläutert, was für Auswirkungen die Handlungen der einzelnen Parteien mit sich ziehen können.

7.1. Täterseite

Bei dem Online-Banking Scam spricht man in Deutschland von einer Straftat nach § 263a StGB, diese definiert sich als der Tatbestand des Computerbetrugs, welcher 1986 durch das zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität eingeführt wurde. In seiner Ursprungsform des Paragraphs § 263 wurde der Tatbestand vorher nicht auf elektronische Betrugsformen bezogen, wodurch somit der Handlungsspielraum der Justiz erweitert wurde. Besonders der 1. Absatz „(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.“ –§ 263a StGB [103], findet bei der Urteilsfindung der Täter Anwendung.

Die Tathandlung kann sich hierbei in verschiedene Aspekte unterteilen:

1. Unrichtige Gestaltung des Programms:
   Dabei muss der Betrüger, ein Programm oder eine Webseite so bearbeiten, dass es bewusst falsche Daten erfasst oder verarbeitet. Hierbei müsste es sich nach gängiger Auslegung um ein Programm handeln, was beispielsweise bewusst mehr an einen

Empfänger überweist. Wichtig hierbei ist, dass bewusst ein Programm(teil) vom Angreifer neugeschrieben werden muss, da der Entwickler hierfür in der Regel nicht als Tatverdächtiger in Betracht gezogen wird. Der Angreifer unterscheidet sich hierbei vom Entwickler, durch die bewusste Manipulation des Programms, welche aus einem Vorsatz heraus entstanden sein muss.

2. Unrichtige Daten:
   Um unrichtige Daten handelt es sich, wenn die vom Nutzer eingegebenen Daten so verändert wurden, dass diese nicht mehr der Wirklichkeit entsprechen.
   Denkbar ist für einen solchen Fall, dass der Kunde einer Bank eine IBAN im entsprechenden Empfänger Feld einträgt, welche allerdings im Hintergrund entweder gar nicht erfasst oder mit den gewünschten Daten des Betrügers überschrieben wird.

3. Verwendung von Daten:
   Die widerrechtliche Verwendung von Daten wird definiert durch eine nicht gestattete Nutzung Dritter, welche zuvor gutgläubig an diese durch die Betrüger übergeben wurden. Ein recht simples Beispiel wäre das Nutzen einer gefälschten Login Maske, welche die Daten des Nutzers abfängt und speichert, sodass die Angreifer später noch Zugriff auf das Konto haben. Wichtig ist, dass in diesem Beispiel von einer Täuschung des Nutzers ausgegangen werden muss und nicht von einer computerspezifischen Täuschung, da die Bank nicht prüfen kann, wer auf das Konto zugreift und ob diese Person berechtigt, dafür wäre.

In einem Schadensfall steht ein Vermögensschaden im Raum, kann Dieser laut § 263 StGB mit bis zu 5 Jahren Haft, sowie einer Geldstrafte geahndet werden kann. Ebenfalls ist allerdings der Versuch bzw. die Vorbereitung der Tat und der Erwerb oder die Verbreitung von Software zu diesem Zwecke schon strafbar wie in § 263a Absatz 1 § 263a Absatz 3 StGB beschrieben [104].

Neben dem Tatbestand des Betrugs bzw. der Täuschung, steht ebenfalls auch das Ausspähen von Daten § 202a StGB aus. Je nach Vorgehen der Täter werden auch häufig falsche Login Fenster erstellt, die zum Abgreifen der Login-Daten genutzt werden. In diesem Falle greifen die beiden folgenden Absätze des § 202a StGB - Ausspähen von Daten:

„(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.“ – § 202a StGB[105]

7.2. Banken-/ Kundenseite

Der Kunde der Bank ist rechtlich abgesichert, sollte die Bank ein Mitverschulden in einem Schadensfall haben. Dieser wird durch § 675u BGB „Haftung des Zahlungsdienstleisters für nicht autorisierte Zahlungsvorgänge“, sowie § 254 BGB „Mitschuld“ gesichert.

In § 675u BGB heißt es: „Im Fall eines nicht autorisierten Zahlungsvorgangs hat der Zahlungsdienstleister des Zahlers gegen diesen keinen Anspruch auf Erstattung seiner Aufwendungen. Er ist verpflichtet, dem Zahler den Zahlungsbetrag unverzüglich zu erstatten und, sofern der Betrag einem Zahlungskonto belastet worden ist, dieses Zahlungskonto wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung durch den nicht autorisierten Zahlungsvorgang befunden hätte.“- BGB [106]. Somit kann der Geschädigte in dem Fall, Schadensersatz von seinem Kreditinstitut verlangen, sollte dieses aufgrund von mangelnder Absicherung eine mit-/ oder die alleinige Schuld an dem Schaden haben. Ob das Kreditinstitut eine Mitschuld trägt, wird im § 254 BGB – Mitverschulden geregelt. Hier heißt es „Hat bei der Entstehung des Schadens ein Verschulden des Beschädigten mitgewirkt, so hängt die Verpflichtung zum Ersatz sowie der Umfang des zu leistenden Ersatzes von den Umständen, insbesondere davon ab, inwieweit der Schaden vorwiegend von dem einen oder dem anderen Teil verursacht worden ist.“[107]

In der Praxis wird dies allerdings von den Kreditinstituten abgewiesen, da eine Mitschuld nur im Raum steht, sofern der Kunde nicht grob fahrlässig gehandelt hat. Dies kann durch die Unternehmen mittels dem § 675v BGB „Haftung des Zahlers bei missbräuchlicher Nutzung eines Zahlungsinstruments“ begründet werden. Denn dort steht in Absatz 4 geschrieben, dass: „Abweichend von den Absätzen 1 und 3 ist der Zahler seinem Zahlungsdienstleister nicht zum Schadensersatz verpflichtet, wenn

1. der Zahlungsdienstleister des Zahlers eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 des Zahlungsdiensteaufsichtsgesetzes nicht verlangt oder

2. der Zahlungsempfänger oder sein Zahlungsdienstleister eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 des Zahlungsdiensteaufsichtsgesetzes nicht akzeptiert.“-BGB [108].

Die Kreditinstitute sichern sich also bei Transaktionen mit der TAN-Kontrolle und ggf. einer MFA ab, sodass der Kunde hier die Aufgabe hat, die Transaktionen freizugeben und sicher zu stellen, dass eine Überweisung wirklich nach seinem Willen geschieht. -BGB [108]

7.3. Rechtsprechung

Im Folgenden werden ähnlich gelagerte Rechtsprechungen näher beleuchtet, um die Argumentation in Punkt 2.1 sowie 2.2 zu stützen.

1. **Rechtsprechung gegen einen 24-jährigen Online-Betrüger aus dem Jahre 2022**
   1,3 Millionen € hatte ein 24-jähriger Online-Betrüger in 170 Taten von fremden Konten entwendet. Dafür stahl er Registrierungslinks für andere Onlinebanking-Accounts und gab sich als deren Eigentümer aus. Infolgedessen forderte er neue TAN-Registrierungsbriefe an und konnte somit das Geld auf Drittkonten überweisen. Da viele Banken diesem Schwindel erlagen, konnten die Geschädigten somit Gebrauch machen von § 254 BGB – Mitverschulden und von den Kreditinstituten Entschädigung fordern. Der Täter wurde am 17.05.2022 wegen gewerbsmäßigem Computerbetrug und gewerbsmäßiger Fälschung von beweiserheblichen Daten zu 6 Jahren Haft verurteilt. [109]
2. **Rechtsprechung zwischen Klägerin und Kreditinstitut mit Eigenverschulden**
   Die Klägerin erlag im Rahmen einer Phishing Attacke kombiniert mit Social Engineering einem Schaden von 44.782€. Hierfür hatte sie im Vorfeld einen TAN zur Erhöhung des Tageslimits und im Folgenden neun Überweisungen freigegeben. Die Geschädigte zog deswegen vor das Oberlandesgericht München und verlangte von ihrem Kreditinstitut Schadensersatz, da sie ein Mitverschulden sah. Dies wurde allerdings mit der Begründung zurückgewiesen, dass chip-Tan Verfahren sehr sicher seien und ein Erraten der TAN praktisch nahe zu unmöglich. [110]

7.4. Zusammenfassung

Zusammenfassend lässt sich sagen, dass Täter mit bis zu 5 Jahren Haft allein für den Tatbestand des Onlinebetrugs durchaus hart bestraft werden können. Hierzu kommen noch andere Straftatbestände wie im angesprochenen Fall die Fälschung von Beweismitteln, welche sich negativ auf die Haftzeit auswirken können.

Auf Seiten der Kreditinstitute, sowie deren Kunden, lässt sich zwar sagen, dass Kunden durchaus einen Schadensersatzanspruch haben, sich dieser aber in der Regel schwer einklagen lässt, da sich in einem Großteil der Fälle ein Eigenverschulden feststellen lässt, durch die Geschädigten meist leer ausgehen, auch wenn dies zu einem Reputationsschaden führen kann.

8. Fazit

Ziel der Arbeit war es zu erläutern, wie Online-Banking Betrug von statten geht. Darüber hinaus wurde die Frage gestellt, warum die Kunden der Banken häufiger Opfer von Cyberattacken werden, als die Banken selbst. Ziel war es dabei ebenfalls die Entwicklung und die Beweggründe hinter den Taten zu ermitteln. Ebenfalls sollte dem Leser nähergebracht werden, welche Mittel Kriminelle verwenden, um erfolgreich Angriffe durchzuführen und welche unterschiedlichen Arten des Online-Banking Betrugs es gibt.

Um zunächst die Frage zu klären, warum die Kunden von Banken häufiger in den Fokus der Betrüger geraten, wurde zunächst aufgezeigt, dass Banken vielen Gesetzen und Regularien unterliegen. Es wurde anhand des KWG, der MaRisk, der BAIT bzw. der KAIT sowie DSGVO und DORA gezeigt, welche Auflagen Banken haben, um einen sicheren Geschäftsbetrieb zu gewährleisten. Dabei wurden Kenntnisse über operative Sicherheit und Notfallmanagement, sowie Datenschutz vermittelt, welche Einblicke in die Aufgaben der Banken zum Schutz ihrer Kunden und der Absicherung ihrer Einlagen geben sollten. Ziel dessen war es zu verdeutlichen, dass Banken härteren Auflagen in der IT-Sicherheit unterliegen, als deren Kunden, was diese zu leichteren Zielen macht.

Ebenfalls wurde beschrieben, wie Banken trotz alledem für die Sicherheit ihrer Kunden in die Haftung genommen werden können. Um das Kundengeschäft abzusichern wurden Themen wie verschlüsselte Übertragungen in Form von HTTPS und TAN-Verfahren inklusive der Multi-Faktor Authentifizierung behandelt. Ebenso wurde deren Schwachstellen und daraus schließend die historisch gewachsene Notwendigkeit der Weiterentwicklung nähergebracht.

Ziel dessen war es dem Leser zu erläutern, vor welchen Hürden Betrüger bei der Durchführung ihren Cyberattacken stehen, um das Verständnis zu schaffen, wie diese umgangen werden.

Die Fragen zur Entwicklung von Online-Banking Betrug und wer die Opfer sind, wurden in dem Kapitel 2.3. Aktuelle Bedrohungslage gestellt. Um die Trendentwicklung zum Online-Banking Betrug zu ermitteln, wurden die Kriminalstatistiken der Jahre 2019 bis 2023 verglichen. Auf Basis dessen wurden der Verlauf der Nutzerzahlen des Online-Bankings und das Altersverhältnis mitberücksichtigt. Hierbei wurde die Erkenntnis gewonnen, dass besonders junge und alte Menschen auf die Maschen der Betrüger hereinfallen. Ebenfalls konnte festgehalten werden, dass mit steigenden Nutzerzahlen des Online-Bankings und Online-Geschäften im Allgemeinen auch die Anzahl der Betrugsfälle stieg. Die steigenden Fallzahlen konnten unter anderem auf die steigenden Nutzerzahlen und die Umstände durch die Covid-19 Pandemie zurückgeführt werden.

In Verbindung mit den steigenden Fallzahlen wurde die Frage gestellt, welche Motive die Täter haben. Hierfür wurde sich unter anderem wieder auf die Zahlen der Kriminalitätsstatistik bezogen und die Fallzahlen der Online-Kriminalität mit denen des Bankraubs verglichen. In das Ergebnis flossen auch die Aufklärungsraten mit ein, sodass festgestellt werden konnte, dass der finanzielle Profit und die Aufklärungsraten deutlich unter denen von Bankraub liegen. Ebenso kann eine Automatisierung in der Cyberkriminalität stattfinden, was sich auch positiv auf den finanziellen Ertrag der Betrüger auswirkt.

Um zu erläutern, wie Online-Banking Betrugsmaschen in der Praxis aussehen, wurden mehrere Beispiele zunächst analysiert und das abgeleitete Vorgehen in Schritte unterteilt. Dabei wurde verdeutlicht, wie Kriminelle Informationen für Phishing Kampagnen erlangen. Darüber hinaus wurde aufgezeigt, dass sich die Art der Informationsbeschaffung mit der Wahl des Pretexts und der Phishing Methode unterscheidet. Für diesen Zweck wurde ein Anwendungsbeispiel entwickelt, welches dem Leser aufzeigen sollte, wie eine Phishing Kampagne in der Praxis ablaufen kann. Ebenfalls konnte verdeutlicht werden, wie eine emotionale Manipulation bei der Wahl des Pretexts relevant ist und wie sich diese in der Praxis deutlich machen. Auf Basis der aufgezeigten Methoden der Cyberkriminellen wurde die Frage definiert, wie sich Betroffene vor Phishing Kampagnen schützen können. Dabei wurde auf automatische und manuelle Präventionsmaßnahmen eingegangen und die Erkenntnis gewonnen, dass nur durch ausreichende Aufklärung und technische

Sicherheitsmaßnahmen wie beispielsweise in Form von Spam-Filtern, ein hinreichender Schutz geschaffen werden kann.

Um die potenziellen Folgen von erfolgreichen Angriffen auf Banken aufzuzeigen, wurden zunächst exemplarisch verschiedenen Angriffsszenarien erklärt und diese Anhand von Praxisbeispielen verdeutlicht. Daraus konnte geschlossen werden, wie wichtig ein Notfallmanagement sowie die Schulung der Mitarbeiter ist, da sich Fehler wie im Fall der Bangladesh Central Bank auf menschliches Versagen zurückführen lassen.

9. Ausblick

Ziel der Arbeit war es, dem Leser näher zu bringen, wie Online-Banking Betrug von statten geht. Aufgrund des Umfangs der Arbeit konnte nicht auf Themen wie Banking-Trojaner eingegangen werden und welche Schwachstellen diese in der Vergangenheit genutzt haben. Ebenfalls ist bei der Betrachtung des Themas auch eine genauere Analyse von Sachverhalten wie Darknet-Marktplätzen und Crimeware-as-a-Service denkbar.

Des Weiteren wäre eine genauere Betrachtung der Punkte Prävention von Cyberattacken durch Banken und Kundenschutz denkbar. Besonderes letzteres bietet stetig neue Entwicklungen, welche sich nicht nur auf das Online-Banking beziehen. Exemplarisch hierfür wäre z.B. die Geräte-Erkennung und eine geografische Lokation von Bezahlaktivitäten, welche dem Kunden zusätzlichen Schutz bieten sollen. Dabei kann auch auf virtuelle Karten in Form von Bezahloptionen mit mobilen Endgeräten eingegangen werden, welche in der Arbeit nicht betrachtet wurden.

Unter Berücksichtigung der aktuellen Entwicklungen von „Large Language Models“ wie beispielsweise das GPT-Modell, wäre eine genauere Betrachtung eines KI-basierten Phishing Ansatzes möglich. Hierbei könnten sowohl Phishing-Mails, als auch Phishing-Seiten auf Basis der getroffenen Erkenntnisse dieser Arbeit detailliert betrachtet werden. Anhand von einer heterogenen Umfragegruppe könnte dabei geprüft werden, wie erfolgreich einzelne Kampagnen sind und wie sich die Menge an Informationen und die Wahl des Pretextes auf die Reaktionsrate auswirkt.

Im Bereich des Social Engineering wäre ein vertiefter Ansatz zum Thema Deep-Fake denkbar, welcher Spear-Phishing Methodiken genauer betrachtet. Dabei können auch auf Maßnahmen zur Generierung, sowie Erkennung von Fälschungen eingegangen werden. Ebenfalls wäre auch hier die Verwendung einer Umfrage denkbar, bei der die Befragten echte

von gefälschten Anfragen unterscheiden sollen, um somit die Effektivität der Fälschungen und der Ansätze zu prüfen.

10. Quellenverzeichnis

[1] L. Nickels, „Geschichte der Bank“, *planet wissen*, 20. Juli 2018. https://www.planet-wissen.de/gesellschaft/wirtschaft/banken/index.html (zugegriffen 23. Januar 2023).

[2] „Klarna-Studie: Bargeld bleibt Trumpf“, *FAZ*, 3. Mai 2021. https://www.faz.net/aktuell/wirtschaft/klarna-studie-bargeld-bleibt-trumpf-17322900.html (zugegriffen 29. März 2023).

[3] Deutsche Bundesbank, „Umfrage Zahlungsverhalten in Deutschland 2021“, Juli 2022. Zugegriffen: 15. Februar 2023. [Online]. Verfügbar unter: https://www.bundesbank.de/resource/blob/894078/aebb75f424c02846677ba50b0501ec5e/mL/zahlungsverhalten-in-deutschland-2021-data.pdf

[4] Bundeskriminalamt, „BKA -PKS 2019 Bund - Falltabellen“, 27. Januar 2020. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2019/PKSTabellen/BundFalltabellen/bundfalltabellen.html?nn=130872 (zugegriffen 6. Januar 2023).

[5] Bundeskriminalamt, „BKA - PKS 2020 Bund - Falltabellen“, 20. Januar 2021. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2020/PKSTabellen/BundFalltabellen/bundfalltabellen.html?nn=145506 (zugegriffen 6. Januar 2023).

[6] Bundeskriminalamt, „BKA -PKS 2021 Bund - Falltabellen“, 30. März 2022. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2021/PKSTabellen/pksTabellen_node.html (zugegriffen 6. Januar 2023).

[7] Bundeskriminalamt, „BKA -PKS 2022 Bund - Falltabellen“, 2023. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2022/PKSTabellen/pksTabellen_node.html (zugegriffen 27. Juni 2023).

[8] BSI, „Cyber-Kriminelle nutzen Corona-Krise vermehrt aus (archiviert)“, *bsi.bund.de*, 2. April 2020. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/Cyber-Kriminell_02042020.html (zugegriffen 27. Juni 2023).

[9] red, „Fraud Map: Kreditkartenbetrug nimmt in Deutschland weiter zu“, *geldinstitute.de*, 19. Oktober 2022. https://www.geldinstitute.de/trends/2022/fraud-map--kreditkartenbetrug-nimmt-in-deutschland-weiter-zu-.html (zugegriffen 27. Juni 2023).

[10] L. Daly und J. Caporal, „Identity Theft and Credit Card Fraud Statistics“, *fool.com*, 9. März 2023. https://www.fool.com/the-ascent/research/identity-theft-credit-card-fraud-statistics/ (zugegriffen 30. Juni 2023).

[11] Gitnux, „The Most Surprising Bank Fraud Statistics And Trends in 2023“, *blog.gitnux.com*, 25. April 2023. https://blog.gitnux.com/bank-fraud-statistics/ (zugegriffen 30. Juni 2023).

[12] Bundesamt für Sicherheit in der Informationstechnik, „Was sind Kritische Infrastrukturen?“, *bsi.bund.de*. https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html (zugegriffen 16. August 2023).

[13] Bafin, „Risikomanagement“, *Bafin.de*, 29. Dezember 2021. https://www.bafin.de/DE/Aufsicht/BankenFinanzdienstleister/Risikomanagement/risikomanagement_node.html (zugegriffen 30. Juli 2023).

[14] Bundesamt für Justiz, „Gesetz über das Kreditwesen (Kreditwesengesetz - KWG) § 25a Besondere organisatorische Pflichten, Bestimmungen für Risikoträger; Verordnungsermächtigung“, *Kreditwesengesetz*. https://www.gesetze-im-internet.de/kredwg/__25a.html (zugegriffen 20. Februar 2023).

[15] BaFin, „Rundschreiben 10/2021 (BA) - Mindestanforderungen an das Risikomanagement - MaRisk“, *MaRisk*, 4. Mai 2022. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2021/rs_1021_MaRisk_BA.html?nn=9450904#doc16502162bodyText30 (zugegriffen 20. Februar 2023).

[16] BaFin, „Bankaufsichtliche Anforderungen an die IT (BAIT)“, Okt. 2020.

[17] Tobias Scheible, „IT-Sicherheit Grundlagen: Schutzziele“, *scheible.it*, 14. Dezember 2013. https://scheible.it/it-sicherheit-grundlagen-schutzziele/ (zugegriffen 22. Februar 2023).

[18] W. Dr. Grudzien und L. Khomutovskaya, „ZAIT – Vergleich zur BAIT“, *core.se*. https://core.se/de/blog/zait-vergleich-zur-bait#:~:text=Grunds%C3%A4tzlich%20verweist%20die%20BAIT%20bei,9%20in%20gro%C3%9Fen%20Teilen%20neu. (zugegriffen 2. März 2023).

[19] BaFin, „Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs-und E-Geld-Instituten (ZAIT)“, Aug. 2021.

[20] BaFin, „Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT)“. Zugegriffen: 15. August 2023. [Online]. Verfügbar unter: https://www.google.com/search?q=kait+fremdbezug+definition&rlz=1C5CHFA_enDE1033DE1033&oq=kait&aqs=chrome.0.69i59l3j69i60l3.3602j0j4&sourceid=chrome&ie=UTF-8#:~:text=Kapitalverwaltungsaufsichtliche%20Anforderungen%20an,%E2%80%BA%20Downloads%20%E2%80%BA%20Konsultation

[21] S. Fach, „BAIT, VAIT, KAIT: IT-Sicherheit in der Finanzwirtschaft“, *endpointprotector.de*, 11. September 2020. https://www.endpointprotector.de/blog/bait-vait-kait-it-sicherheit-in-der-finanzwirtschaft/#:~:text=Inhaltlich%20stimmen%20BAIT%2C%20VAIT%20und,Erg

%C3%A4nzungen%20innerhalb%20der%20acht%20Anforderungsbereiche. (zugegriffen 15. August 2023).

[22] C. Dr. Conreder und F. Hausemann, „KAIT –Neue Anforderungen an die IT von Kapitalverwaltungsgesellschaften ab voraussichtlich Mitte / Ende Juli 2019“, *roedl.de*. https://www.roedl.de/themen/kapitalanlage-kompakt/2019-04/kait-neue-anforderungen-an-die-it-von-kapitalverwaltungsgesellschaften-ab-voraussichtlich-mitte-ende-juli-2019 (zugegriffen 15. August 2023).

[23] „Digital Operational Resilience Act (DORA): Widerstandsfähigkeit für Versicherer“. https://www2.deloitte.com/de/de/pages/risk/articles/digital-operational-resilience-act-dora.html (zugegriffen 6. März 2023).

[24] P. Schulz, „DORA: Alles was jetzt wichtig für Sie ist“, *PWC*. https://www.pwc.de/de/im-fokus/cyber-security/dora-alles-was-jetzt-wichtig-fuer-sie-ist.html (zugegriffen 6. März 2023).

[25] L. Weimer und N. Jankovic, „DORA: Warum Cyber-Resilienz einen europäischen Mantel braucht“, *EY.com*, 23. April 2021. https://www.ey.com/de_de/financial-services/dora-warum-cyber-resilienz-einen-europaischen-mantel-braucht (zugegriffen 6. März 2023).

[26] EUROPÄISCHEN PARLAMENTS UND DES RATES, „VERORDNUNG (EU) 2022/2554 (DORA)“, Dez. 2022. Zugegriffen: 6. März 2023. [Online]. Verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554&qid=1678096766480&from=EN

[27] Europäische Union, „Art. 1 DSGVO Gegenstand und Ziele“, *Amtsblatt der Europäischen Union*, 27. April 2016. https://dsgvo-gesetz.de/art-1-dsgvo/ (zugegriffen 6. August 2023).

[28] Europäische Union, „Art. 2 DSGVO Sachlicher Anwendungsbereich“, *Amtsblatt der Europäischen Union*, 27. April 2016. https://dsgvo-gesetz.de/art-2-dsgvo/ (zugegriffen 6. August 2023).

[29] intersoft consulting, „DSGVO Personenbezogene Daten“. https://dsgvo-gesetz.de/themen/personenbezogene-daten/

[30] Europäische Union, „Art. 4 DSGVO Begriffsbestimmungen“, *Amtsblatt der Europäischen Union*, 27. April 2016. https://dsgvo-gesetz.de/art-4-dsgvo/ (zugegriffen 6. August 2023).

[31] Datenschutz.org, „Was sind personenbezogene Daten?“, *Datenschutz.org*, 27. Mai 2023. https://www.datenschutz.org/personenbezogene-daten/#beispiele-fuer-personenbezogene-daten (zugegriffen 6. August 2023).

[32] Europäische Kommission, „Was sind personenbezogene Daten?“, *commission.europa.eu*. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_de#:~:text=considered%20personal%20data-,Antwort,stellen%20ebenfalls%20personenbezogene%20Daten%20dar. (zugegriffen 6. August 2023).

[33] Europäische Union, „Art. 9 DSGVO Verarbeitung besonderer Kategorien personenbezogener Daten“, *Amtsblatt der Europäischen Union*, 27. April 2016. https://dsgvo-gesetz.de/art-9-dsgvo/ (zugegriffen 6. August 2023).

[34] Europäischen Union, „Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung“, *Amtsblatt der Europäischen Union*, 27. April 2016. https://dsgvo-gesetz.de/art-6-dsgvo/ (zugegriffen 6. August 2023).

[35] Bundestag, „§ 64 BDSG Anforderungen an die Sicherheit der Datenverarbeitung“, 28. Mai 2018. https://dsgvo-gesetz.de/bdsg/64-bdsg/ (zugegriffen 6. August 2023).

[36] Europäische Union, „Art. 33 DSGVO Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde“, *Amtsblatt der Europäischen Union*, 27. April 2016. https://dsgvo-gesetz.de/art-33-dsgvo/ (zugegriffen 6. August 2023).

[37] Europäische Union, „Art. 83 DSGVO Allgemeine Bedingungen für die Verhängung von Geldbußen“, *Amtsblatt der Europäischen Union*, 27. April 2016. https://dsgvo-gesetz.de/art-83-dsgvo/ (zugegriffen 6. August 2023).

[38] IT-Finanzmagazin, „Online-Banking killt weitere Bankfilialen · IT Finanzmagazin“, *it-finanzmagazin.de*, 28. Juni 2022. https://www.it-finanzmagazin.de/online-banking-killt-weitere-bankfilialen-142807/ (zugegriffen 10. Februar 2023).

[39] G. Roden, „Asymmetrisch wird’s sicherer“, *entwickler magazin*, Februar 2020.

[40] W. Angeli, „Sind HTTPS, SSL & TLS Pflicht für alle?“, *experte.one*, 14. September 2020. https://experte.one/ecommerce/https-ssl-tls-pflicht-fuer-alle (zugegriffen 2. Februar 2023).

[41] M. Mierke, „SSL und TLS - was ist der Unterschied?“, *heise.de*, 3. September 2020. https://www.heise.de/tipps-tricks/SSL-und-TLS-was-ist-der-Unterschied-4884686.html# (zugegriffen 10. Februar 2023).

[42] D. Coclin, „What Are the Different Types of SSL Certificates?“, *pkic.org*, 7. August 2013. https://pkic.org/2013/08/07/what-are-the-different-types-of-ssl-certificates/ (zugegriffen 11. Februar 2023).

[43] P. Nohe, „SSL/TLS-Zertifikate gelten nun maximal ein Jahr“, *GlobalSign Blog*, 1. Juli 2020. https://www.globalsign.com/de-de/blog/ssl-tls-zertifikate-gelten-nun-maximal-ein-jahr#:~:text=SSL%2FTLS%2DZertifikate%20gelten%20nun%20maximal%20ein%20Jahr (zugegriffen 12. Februar 2023).

[44] D. Borchers, „Vor 30 Jahren: Online-Banking startet in Deutschland“, *Heise*, 12. November 2010. https://www.heise.de/newsticker/meldung/Vor-30-Jahren-Online-Banking-startet-in-Deutschland-1135331.html (zugegriffen 23. Januar 2023).

[45] dpa, „Postbank mit neuem TAN-System gegen Phishing“, *heise.de*, 7. August 2005. https://www.heise.de/newsticker/meldung/Postbank-mit-neuem-TAN-System-gegen-Phishing-121126.html (zugegriffen 1. Februar 2023).

[46] M. Cobb und K. Yasar, „man-in-the-middle attack (MitM)“, *techtarget.com*, April 2022. techtarget.com (zugegriffen 2. Februar 2023).

[47] D. Bachfeld, „Erfolgreicher Angriff auf iTAN-Verfahren“, *heise,de*, 11. November 2005. https://www.heise.de/newsticker/meldung/Erfolgreicher-Angriff-auf-iTAN-Verfahren-147177.html (zugegriffen 2. Februar 2023).

[48] C. Kahle, „Katusha: LKA zerschlägt Ring von Online-Betrügern“, *winfuture.de*, 29. Oktober 2010. https://winfuture.de/news,59152.html (zugegriffen 2. Februar 2023).

[49] Redteam Pentesting, „Forschungsgruppe ‚RedTeam‘ der RWTH Aachen warnt vor trügerischer Sicherheit des neuen iTAN Verfahren.“, *redteam-pentesting.de*, 2010. https://www.redteam-pentesting.de/press/iTAN.txt (zugegriffen 2. Februar 2023).

[50] D. Bachfeld, „Verbessertes iTAN-Verfahren soll vor Manipulationen durch Trojaner schützen“, *heise.de*, 26. Oktober 2007. https://www.heise.de/security/meldung/Verbessertes-iTAN-Verfahren-soll-vor-Manipulationen-durch-Trojaner-schuetzen-189683.html (zugegriffen 2. Februar 2023).

[51] B. Behr, „TÜV-Plakette für mobile TAN“, *heise.de*, 18. April 2006. https://www.heise.de/newsticker/meldung/TueV-Plakette-fuer-mobile-TAN-117990.html (zugegriffen 2. Februar 2023).

[52] Verbraucherzentrale, „Onlinebanking: Wie sicher ist welches TAN-Verfahren?“, *verbraucherzentrale.de*, 23. März 2022. https://www.verbraucherzentrale.de/wissen/geld-versicherungen/sparen-und-anlegen/onlinebanking-wie-sicher-ist-welches-tanverfahren-21921#:~:text=Was%20ist%20eine%20TAN%3F,genehmigen%20%E2%80%93%20ersetzen%20also%20die%20Unterschrift. (zugegriffen 2. Februar 2023).

[53] R. Linsenbarth, „chipTAN ausgeflickert – die neuen Verfahren im Test“, *it-finanzmagazin.de*, 29. April 2019. https://www.it-finanzmagazin.de/chiptan-ausgeflickert-verfahren-im-test-88543/ (zugegriffen 3. Februar 2023).

[54] Sparkasse, „TAN-/Freigabeverfahren“, *Sparkasse.de*. https://www.sparkasse.de/service/sicherheit-im-internet/tan-verfahren.html (zugegriffen 3. Februar 2023).

[55] BSI, „Meine Bank schafft die smsTAN ab – Was nun?“, *bsi.bund.de*. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-Banking-Online-Shopping-und-mobil-bezahlen/Online-Banking/smsTAN/sms-tan_node.html (zugegriffen 3. Februar 2023).

[56] Bundesbank, „PSD2“, *bundesbank.de*. https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/psd2/psd2-775434 (zugegriffen 6. Februar 2023).

[57] S. Dipl.-Ing. (FH) Luber und P. Schmitz, „Was ist AES (Advanced Encryption Standard)?“, *Security Insider*, 23. Februar 2018. https://www.security-insider.de/was-ist-aes-advanced-encryption-standard-a-688378/ (zugegriffen 6. Februar 2023).

[58] J. Reynolds, „Cryptography and Security in Banking“, *medium.com*, 8. November 2019. https://medium.com/@joshuareynolds/cryptography-and-security-in-banking-2cce7691e70f (zugegriffen 6. Februar 2023).

[59] bankenverband, „Ergebnisse einer repräsentativen Bevölkerungsumfrage im Auftrag des Bundesverbandes deutscher Banken“, 2022. Zugegriffen: 9. Februar 2023. [Online]. Verfügbar unter: https://bankenverband.de/media/files/2022_02_08_Ergebnisse_Charts_U_Mobile-Banking_Mobiles-Bezahlen-final.pdf

[60] K. Schneider, „FINGERABDRUCK STATT PASSWORT Biometrische Verfahren werden beim Banking beliebter“, *handelsblatt.de*, 14. August 2020. https://www.handelsblatt.com/technik/sicherheit-im-netz/fingerabdruck-statt-passwort-biometrische-verfahren-werden-beim-banking-beliebter/26093358.html (zugegriffen 9. Februar 2023).

[61] frank, „Chaos Computer Club hackt Apple TouchID“, *ccc.de*, 21. September 2013.

[62] „So einfach haben Forscher die Face ID von Apple geknackt“, *welt.de*, 15. November 2017. https://www.welt.de/kmpkt/article170591535/So-einfach-haben-Forscher-die-Face-ID-von-Apple-geknackt.html (zugegriffen 9. Februar 2023).

[63] „Warum es immer weniger Bankräuber gibt“, *Frankfurter Allgemeine Zeitung*, 15. November 2021. https://www.faz.net/aktuell/finanzen/aussterbendes-verbrechen-warum-es-immer-weniger-bankraeuber-gibt-17635030.html (zugegriffen 1. Juli 2023).

[64] M. Wilms, „Drastischer Rückgang: Darum gibt es kaum noch Bankräuber“, *Berliner Zeitung*, 15. November 2021. https://www.berliner-zeitung.de/news/drastischer-rueckgang-darum-gibt-es-kaum-noch-bankraeuber-li.194835 (zugegriffen 1. Juli 2023).

[65] mitnicksecurity, „The History of Social Engineering & How to Stay Safe Today“, *mitnicksecurity*. https://www.mitnicksecurity.com/the-history-of-social-engineering#chapter-2 (zugegriffen 3. Juli 2023).

[66] ProSec Networks, „Social Engineering“, *ProSec Networks Blog*. https://www.prosec-networks.com/blog/social-engineering/ (zugegriffen 3. Juli 2023).

[67] T. Klir, „Vorlesung Social Engineering“, Thomas Klirr, Mai 2023.

[68] C. Hadnagy, *Die Kund des Human Hacking – Social Engineering in der Praxis*, 2. Auflage. mitp, 2011.

[69] T. Hunt, „The 773 Million Record ‚Collection #1‘ Data Breach“, *troyhunt.com*, 19. Januar 2019. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/ (zugegriffen 3. Juli 2023).

[70] I. Harford, „10 biggest data breaches in history, and how to prevent them“, *Tech Target* , Juli 2022. https://www.techtarget.com/searchsecurity/feature/10-biggest-data-breaches-in-history-and-how-to-prevent-them (zugegriffen 3. Juli 2023).

[71] C. Papesch, „Phishing: So funktioniert der Betrug beim Online-Banking“, *NDR*, 7. März 2022. https://www.ndr.de/ratgeber/verbraucher/Phishing-So-funktioniert-der-

Betrug-beim-Online-Banking,phishing158.html#:~:text=Phishing%20ist%20h%C3%A4ufigste%20Form%20f%C3%BCr%20Betrug%20bei%20Online%2DBanking&text=Der%20Absender%3A%20angeblich%20eine%20Bank,Zugriffe%20oder%20technische%20Probleme%20angegeben. (zugegriffen 16. August 2023).

[72] P. W. Dunne, „How Scammers Get Your Private Email Address (And What You Can Do About It)“, *startmail.com*, 27. August 2020. https://www.startmail.com/email-scammers/ (zugegriffen 3. Juli 2023).

[73] W. Teitscheid, „Schreddern oder Datentonne im Vermittlerbüro – welche Standards gilt es zu beachten?“, *AssCompact*, S. 108f., August 2015. Zugegriffen: 3. Juli 2023. [Online]. Verfügbar unter: https://www.asscompact.de/nachrichten/schreddern-oder-datentonne-im-vermittlerb%C3%BCro-%E2%80%93-welche-standards-gilt-es-zu-beachten

[74] JuRec-IT, „AKTEN- UND DATENVERNICHTUNG BEI DATEN GIBT ES KEIN RECYCLING – WIR VERNICHTEN SIE SPURLOS!“, *jurec-it.de*. https://jurec-it.de/datenvernichtung/ (zugegriffen 3. Juli 2023).

[75] A. Kunst, „Wie häufig lesen Sie die Allgemeinen Geschäftsbedingungen (AGB) von Online-Shops?“, *statista*, 6. November 2019. https://de.statista.com/statistik/daten/studie/4113/umfrage/aspekte-beim-online-banking-nach-geschlecht/ (zugegriffen 4. Juli 2023).

[76] tagesschau, „Kontogebühren-Streit - was Kunden beachten sollten“, *tagesschau*, 27. April 2022. https://www.tagesschau.de/wirtschaft/verbraucher/bgh-kontogebuehren-kuendigung-101.html (zugegriffen 5. Juli 2023).

[77] E. Abu, „Emotional Manipulation By Scammers“, *LinkedIn Pulse*, 10. Juni 2023. https://www.linkedin.com/pulse/emotional-manipulation-scammers-emmanuel-abu#:~:text=Emotional%20manipulation%20is%20a%20common,actions%20that%20benefit%20the%20scammer. (zugegriffen 6. Juli 2023).

[78] „Zwei Personen, die auf ein Handy schauen. Social Engineering: So schützt du dich vor Betrug im Netz“, *n26 Blog*, 9. März 2023. https://n26.com/de-de/blog/wie-du-dich-gegen-social-engineering-schuetzt (zugegriffen 6. Juli 2023).

[79] P. Ilg, „Cyberattacke am Arbeitsplatz“, *computerwoche*, 15. August 2015. https://www.computerwoche.de/a/cyberattacke-am-arbeitsplatz,3098962 (zugegriffen 23. Juli 2023).

[80] T. Wünsche, „Gefälschte Rufnummer im Display – ist Manipulation möglich?“, *dermike*, 5. November 2020. https://www.dermike.de/wissen/call-id-spoofing-wenn-rufnummern-im-display-manipuliert-werden/ (zugegriffen 8. Juli 2023).

[81] N26, „Vishing – Die neue Art von Telefonbetrug“, *N26 Blog*, 10. März 2023. https://n26.com/de-de/blog/vishing (zugegriffen 8. Juli 2023).

[82] R. Francis und F. Maier, „Hacking-Tools shoppen wie bei Amazon“, *Computerwoche*, 3. Februar 2017. https://www.computerwoche.de/a/hacking-tools-shoppen-wie-bei-amazon,3329675 (zugegriffen 23. Juli 2023).

[83] „Was ist E-Mail-Spoofing?“, *proofpoint.com*. https://www.proofpoint.com/de/threat-reference/email-spoofing (zugegriffen 11. Juli 2023).

[84] „sendemail“. Brandon Zehm, 5. August 2022. Zugegriffen: 11. Juli 2023. [Online]. Verfügbar unter: https://www.kali.org/tools/sendemail/

[85] „E-Mail-Header – Diese Angaben enthält er“, *mailvergleiche.de*, 14. Februar 2021. https://mailvergleich.de/blog/2021/02/e-mail-header-diese-angaben-enthaelt-er/#:~:text=Die%20Pflichtangaben%20des%20Headers%20in%20der%20%C3%9Cbersicht&text=Autor%20der%20E%2DMail%20in,und%20E%2DMail%2DAdresse.&text=To%20%2F%20An%3A%20Der%20Empf%C3%A4nger%20in,sind%20diese%20durch%20Kommata%20getrennt.&text=Cc%3A%20Optionale%20weitere%20Empf%C3%A4nger%2C%20die,der%20E%2DMail%20erhalten%20haben.

[86] J. Franke, „So erkennst du gefälschte Links & betrügerische Webseiten “, *easyname.at*. https://www.easyname.at/blog/cyber-security/so-erkennst-du-gefaelschte-links-betruegerische-webseiten/ (zugegriffen 20. August 2023).

[87] „BSI-Chefin: Bedrohung durch Cyberangriffe so groß wie nie zuvor“, *web.de News*, 15. Juli 2023. https://web.de/magazine/politik/bsi-chefin-bedrohung-cyberangriffe-gross-zuvor-38428244 (zugegriffen 16. Juli 2023).

[88] M. Wölke, „docker-php-mariadb“. Github, 13. April 2022. Zugegriffen: 26. Mai 2023. [Online]. Verfügbar unter: https://gist.github.com/mwoelke/a76ddea2df0973bf77c26fc769a39369/revisions

[89] K. Pistol, „Hausarbeit_OLBS_Anwendungsbeispiel“. Mannheim, 27. August 2023. Zugegriffen: 27. August 2023. [Online]. Verfügbar unter: https://github.com/Nevermindx3/Hausarbeit_OLBS_Anwendungsbeispiel

[90] S. Feist, „Absenderreputation und E-Mail-Sicherheit – Teil 2: Sender Policy Framework (SPF)“, *nospamproxy.de*. https://www.nospamproxy.de/de/sender-policy-framework-spf/ (zugegriffen 19. Juli 2023).

[91] S. Feist, „Absenderreputation und E-Mail-Sicherheit – Teil 3: DomainKeys Identified Mail (DKIM)“, *nospamproxy.de*. https://www.nospamproxy.de/de/domainkeys-identified-mail-dkim/ (zugegriffen 19. Juli 2023).

[92] S. Feist, „Absenderreputation und E-Mail-Sicherheit – Teil 4: Domain-based Message Authentication, Reporting and Conformance (DMARC)“, *nospamproxy.de*. https://www.nospamproxy.de/de/domain-based-message-authentication-reporting-conformance-dmarc/ (zugegriffen 19. Juli 2023).

[93] „Cyber Security Statistics The Ultimate List Of Stats Data, & Trends For 2023“, *Purplesec*. https://purplesec.us/resources/cyber-security-statistics/#FAQs (zugegriffen 17. Juli 2023).

[94] Bundesamt für Sicherheit in der Informationstechnik, „Daten auf Festplatten und Smartphones endgültig löschen“, *BSI Webseite - Basistipps zur IT-Sicherheit*. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html (zugegriffen 16. Juli 2023).

[95] T. Sims und K. Knolle, „German cooperative banks hit by DDoS hack attack on IT provider“, *Reuters*, 4. Juni 2021. https://www.reuters.com/technology/german-it-company-that-serves-banks-experiences-ddos-hack-attack-2021-06-04/ (zugegriffen 8. August 2023).

[96] „WannaCry“, *Rhebo*. https://rhebo.com/de/ressourcen/glossar/wannacry/ (zugegriffen 10. August 2023).

[97] E. Flitter und K. Weise, „Capital One Data Breach Compromises Data of Over 100 Million“, *The New York Times*, 29. Juli 2019. https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html (zugegriffen 10. August 2023).

[98] Deutsche Bundesbank, „SWIFT“, *Deutsche Bundesbank*. https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/ueberwachung/swift-603612#:~:text=Einf%C3%BChrung,zu%20Finanztransaktionen%20in%20standardisierter%20Form. (zugegriffen 14. August 2023).

[99] S. Peteranderl, „Kims Dotcom“, *Spiegel Online*, 8. März 2019. https://www.spiegel.de/netzwelt/netzpolitik/kim-jong-un-nordkoreas-hacker-kims-geheimwaffe-a-1256354.html (zugegriffen 14. August 2023).

[100] „Hacker dringen in Zahlungssystem Swift ein“, *Zeit Online*, 26. April 2016. https://www.zeit.de/wirtschaft/2016-04/cyber-angriff-swift-notenbank (zugegriffen 14. August 2023).

[101] K. N. Das und J. Spicer, „How the New York Fed fumbled over the Bangladesh Bank cyber-heist“, *Reuters.com*, 21. Juli 2016. https://www.reuters.com/investigates/special-report/cyber-heist-federal/ (zugegriffen 14. August 2023).

[102] „The Lazarus heist: How North Korea almost pulled off a billion-dollar hack“, *BBC.com*, 21. Juni 2021. https://www.bbc.com/news/stories-57520169 (zugegriffen 14. August 2023).

[103] Bundesregierung, „§ 263a StGB - Computerbetrug“. https://dejure.org/gesetze/StGB/263a.html (zugegriffen 8. Januar 2023).

[104] R. & M. Prof. Dr. Hefendehl, „§ 35: Computerbetrug (§ 263a StGB)“, *Rechtswissenschaftliche Fakultät der Universität Freiburg*. Institut für Kriminologie und Wirtschaftsstrafrecht, Freiburg, 2018. Zugegriffen: 8. Januar 2023. [Online]. Verfügbar unter: https://strafrecht-online.org/lehre/sos-2018/strafrecht-bt/%C2%A7%2035%20-%20Computerbetrug%20KK%20495-516.pdf

[105] Bunderegierung, „§ 202a StGB - Ausspähen von Daten“, *Strafgesetzbuch*. https://dejure.org/gesetze/StGB/202a.html (zugegriffen 8. Januar 2023).

[106] Bundesregierung, „§ 675u BGB - Haftung des Zahlungsdienstleisters für nicht autorisierte Zahlungsvorgänge“, *BGB*, 17. Juli 2017. https://dejure.org/gesetze/BGB/675u.html (zugegriffen 10. Januar 2023).

[107] Bundesrepublik, „§ 254 BGB - Mitverschulden“, *BGB*. https://dejure.org/gesetze/BGB/254.html (zugegriffen 10. Januar 2023).

[108] Bundesregierung, „§ 675v BGB - Haftung des Zahlers bei missbräuchlicher Nutzung eines Zahlungsinstruments“, *BGB*, 17. Juli 2017. https://dejure.org/gesetze/BGB/675v.html (zugegriffen 10. Januar 2023).

[109] S. Pfaller und K. Nöbauer, „Urteil in Ingolstadt: Online-Betrüger muss in Entziehungsanstalt | BR24“, 17. Mai 2022. https://www.br.de/nachrichten/bayern/urteil-in-ingolstadt-online-betrueger-muss-sechs-jahre-in-haft,T65NDSF (zugegriffen 11. Januar 2023).

[110] S. Kröger, „Bankseitige Mitwirkungs-/Schadensminderungspflichten im Online-Banking“, *fch-gruppe*, 18. Oktober 2022. https://www.fch-gruppe.de/Beitrag.aspx?ID=21862 (zugegriffen 11. Januar 2023).