HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Bachelorarbeit

Frau
Antonia Damisch

Phishing Bedrohungen in Unternehmen: Eine Untersuchung von Angriffstrends und Schutzmaßnahmen

Mittweida, 2023

Fakultät Angewandte Computer- und Biowissenschaften

Bachelorarbeit

Phishing Bedrohungen für Unternehmen: Eine Untersuchung von Angriffstrends und Schutzmaßnahmen

Autor:
Frau

Antonia Damisch

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO19w4-B

Erstprüfer:
Prof. Dr. rer. nat. Dirk Labudde

Zweitprüfer:
Dr. Michael Gschwender

Einreichung:
Plauen, 26.04.2023

Verteidigung/Bewertung:
Mittweida, 2023

Faculty Applied Computer Sciences and Biosciences

Bachelor Thesis

Phishing Threads for Companies: An Examination of Attack Trends and Protective Measures

author:
Ms.

Antonia Damisch

course of studies:
General and Digital Forensic Science

seminar group:
FO19w4-B

first examiner:
Prof. Dr. rer. nat. Dirk Labudde

second examiner:
Dr. Michael Gschwender

submission:
Plauen, 26.04.2023

defence/ evaluation:
Mittweida, 2023

Bibliografische Beschreibung:

Damisch, Antonia:

Phishing Bedrohungen in Unternehmen: Eine Untersuchung von Angriffstrends und Schutzmaßnahmen. - 2023. – XII, 49 S.
Mittweida, Hochschule Mittweida – University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften.

Bachelorarbeit, 2023.

Referat:

Diese Bachelorarbeit befasst sich mit Phishing Bedrohungen für Unternehmen, sowohl Angriffstrends als auch Schutzmaßnahmen.

Ziel der vorliegenden Arbeit ist es, bisher getroffene Schutzmaßnahmen zu analysieren und ihre Wirksamkeit anhand von zwei ausgewählten Fallbeispiele zu untersuchen. Dafür werden die Phishing Angriffe auf die amerikanischen Unternehmen „Twitter“ und „Uber“ genauer betrachtet und warum diese erfolgreich waren. Es soll beurteilt werden, ob die vorgestellten Leitfäden und Schutzmaßnahmen diese beiden Phishing Angriffe hätten verhindern können.

Die Untersuchung zeigte, dass die gängigen Schutzmaßnahmen und das Einhalten von Leitfäden nicht ausgereicht haben, um die Unternehmen vor einem erfolgreichen Phishing Angriff zu schützen. Außerdem kommt dem Mensch bei der Bekämpfung von Phishing eine viel zu große Bedeutung zu und vernachlässigt das Handeln auf Managementebene.

Danksagung

Ich danke hiermit allen, die mich bei dieser Bachelorarbeit und mein gesamtes Studium begleitet und unterstützt haben.

Ein besonderer Dank gilt meinen Eltern, die mir immer zur Seite standen und meinen Weg finanziell und emotional unterstützt haben.

Außerdem möchte ich meinem Betreuer Herrn Michael Gschwender danken, für das Betreuen der Bachelorarbeit und der Näherbringung des Themas Phishings mit spannenden Insider-Geschichten.

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
z.B.	zum Beispiel

1. Einleitung

Phishing hat jeder schon mal gehört, eine Warnung davor gesehen oder eine offensichtliche Spam Mail im Postfach gehabt – also kein großes Thema mehr, oder? In einer Studie der Interisle Consulting Group wurden im Zeitraum von Mai 2021 bis April 2022 1.122.579 Phishing Angriffe gezählt [68]. Dabei gehört Phishing zu den zentralen Phänomenen der Computerkriminalität, auch Cybercrime genannt [2]. Der deutschen Wirtschaft entstand durch Cybercrime im Jahr 2022 ein Schaden von 203 Milliarden Euro, im Rekordjahr 2021 waren es sogar 223 Milliarden Euro. Es wird davon ausgegangen, dass fast jedes Unternehmen einmal Opfer wird [1]. Phishing gilt als Haupteintrittsvektor von Schadsoftware wie beispielsweise Ransomware. Für Unternehmen kann ein solcher Angriff weitreichende Folgen mit sich bringen. Von einem hohen finanziellen Schaden, über den Verlust von sensiblen Kunden- oder Unternehmensdaten bis hin zu Existenzbedrohungen ist alles möglich [2]. Zusätzlich entsteht ein massiver Reputationsschaden durch welche Partner oder Kunden ihr Vertrauen in das Unternehmen verlieren [5].

In der Periode Mai 2021 bis April 2022 wurden über 2.000 Unternehmen oder Organisationen zum Opfer von Phishing Angriffen. Besonders große US-Konzerne wie z.B. Amazon, Facebook oder Microsoft sind ein beliebtes Ziel [68]. Doch auch deutsche Unternehmen bleiben davon nicht verschont. Die Organisation Bitkom hat in einer Studie von 2022 mehr als 1.000 deutsche Unternehmen befragt und fast 45% dieser meinen, dass die Folgen von Cyberattacken ihre geschäftliche Existenz bedrohen können [2]. Besonders aktuell ist das Thema Phishing, weil viele Menschen es nach wie vor unterschätzen. Die Art und Weise des Phishings befindet sich in einem stetigen Wandel und wird zunehmend professioneller. Auch der Täterkreis hat sich mit 51% in die Richtung der organisierten Kriminalität verschoben, was einen Anstieg um 22% bedeutet [1]. Zudem befinden sich viele Arbeitnehmer seit der Corona Pandemie im Homeoffice, was bei unzureichender Sicherung der IT-Prozesse zu vielen neuen Angriffsmöglichkeiten führt [2].

Deshalb stellt sich die Frage, welche Schutzmaßnahmen haben Unternehmen bisher getroffen und wie wirksam waren diese? Ziel dieser Arbeit soll es sein, diverse Leitfäden und Schutzmaßnahmen zu analysieren und ihre Wirksamkeit anhand von zwei ausgewählten Fallbeispielen zu untersuchen.

Dafür werden die Phishing Angriffe auf die amerikanischen Unternehmen „Twitter“ und „Uber“ genauer betrachtet und warum diese erfolgreich waren. Im Anschluss soll beurteilt werden, ob die vorgestellten Leitfäden und Schutzmaßnahmen diese beiden Phishing Angriffe hätten verhindern können.

Nachdem die Zielstellung dieser Bachelorarbeit definiert ist, sollen zunächst im folgenden Kapitel 2 die Grundlagen geklärt werden. Dazu gehört sowohl die Definition des Oberbegriffs Cybercrime als auch des Phishings sowie die Abgrenzung zum Social Engineering. Unter Kapitel 3 soll dann das Phishing vor dem Unternehmenskontext analysiert werden. Dies umfasst Angriffsvektoren und das recht neuartige Phänomen Ransomware. Im Anschluss wird die Möglichkeit für Unternehmen eine Cyberversicherung abzuschließen untersucht. Das vierte Kapitel ist ausschließlich den technischen und nichttechnischen Schutzmaßnahmen gewidmet. Anhand dieser einzelnen Maßnahmen und den unterschiedlichen Leitfäden staatlicher Organisationen wird eine Grundlage erstellt, wie man sich theoretisch vor Phishing Angriffen schützen kann. Zuletzt werden unter Kapitel 5 die beiden Fallbeispiele erläutert und deren Angriffsart sowie die getroffenen Schutzmaßnahmen analysiert. Es soll eine Bewertung im Kontext der Schutzmaßnahmen erfolgen und der theoretische Schutz vor Phishing Angriffen mit den Erkenntnissen aus zwei realen Angriffen verglichen werden. Daraus resultierend sollen weitere praktische Möglichkeiten für einen besseren Schutz erläutert werden. Durch das Fazit und einen abschließenden Ausblick sollen die Erkenntnisse noch einmal zusammengefasst und die Zukunft des Phishings betrachtet werden.

** Zur besseren Lesbarkeit wird in dieser Bachelorarbeit das generische Maskulin verwendet. Die in der Arbeit verwendeten Personenbezeichnungen beziehen sich auf alle Geschlechter.*

2. Grundlagen

Um die Leitfrage klären zu können, müssen zuerst einige Grundlagen dargelegt werden. Für die Betrachtung des Phishings im Bezug des Unternehmenskontextes werden in diesem Kapitel die Begriffe Phishing und Social Engineering definiert und im Bereich der Cyberkriminalität eingeordnet. Anschließend wird eine Abgrenzung der beiden definierten Begriffe vorgenommen.

2.1 Cyberkriminalität

Für Cybercrime als Begriff liegt keine einheitliche Definition vor [9]. Das Bundeskriminalamt beschreibt Cybercrime oder auch Cyberkriminalität als einen kriminellen Wirtschaftszweig mit eigenen Wertschöpfungsketten. Es wird dabei unterschieden in Cybercrime im weiteren und engeren Sinne. Letzteres umfasst Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten wenden. Es ist längst ein professionelles Geschäft und auf sogenannten Untergrund Märkten werden gestohlene Daten und Identitäten gehandelt. Ein weiteres Geschäft ist das Cybercrime-as-a-Service, bei dem Cyber-Straftaten zum Kauf angeboten werden [2].

Auch wenn die Erscheinungsformen im engeren Sinne variieren, werden besonders häufig Ransomware, Phishing, Malware und Denial-of-Service (DDoS) Angriffe genutzt [8]. Dabei spielt es keine Rolle, ob die Taten von Einzelpersonen oder organisierten Gruppen begangen werden.

Laut dem Cybercrime Bundeslagebild war besonders die Corona Pandemie ein Katalysator für Cyberstraftaten. Durch die fortschreitende Digitalisierung und Homeoffice kann es besonders bei nicht ausreichender Sicherung der IT-Prozesse zu vielen neuen Angriffsmöglichkeiten kommen. Dabei können Cyberangriffe existenzbedrohende Notlagen, insbesondere für Unternehmen auslösen [2].

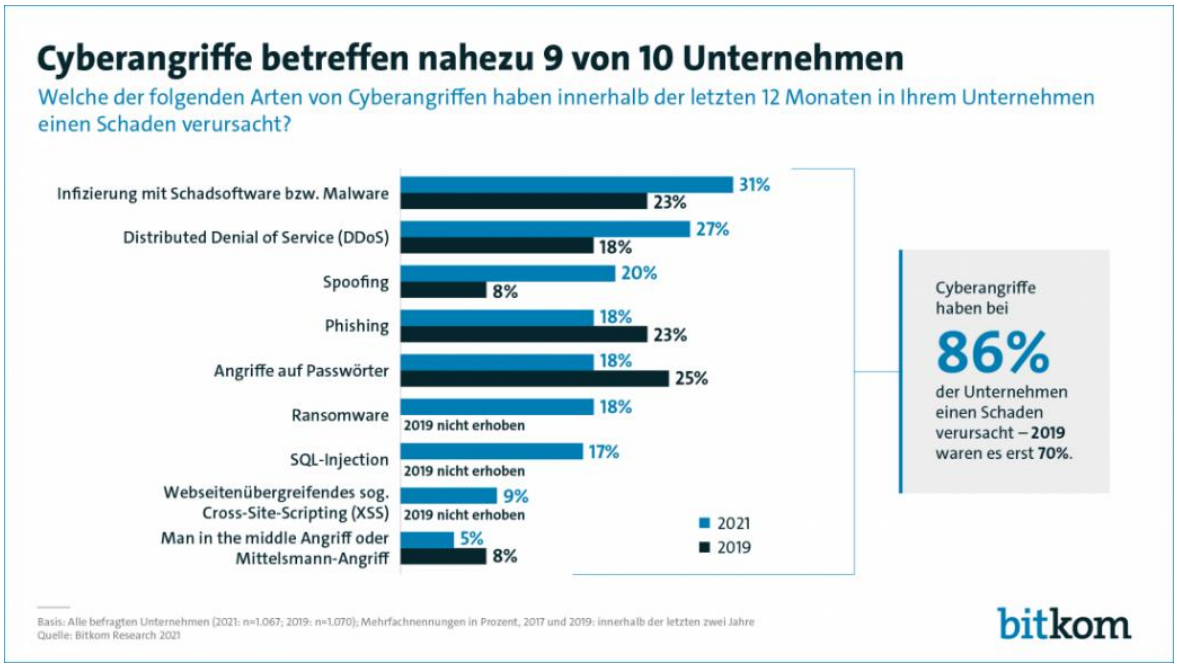

Abbildung 1: Cyberangriffe in Unternehmen im Vergleich 2019 und 2021 [35]

Die Abbildung zeigt bei Cyberangriffen einen generellen Anstieg zwischen den Jahren 2019 und 2021. Es ist zu erkennen, dass die Infizierung mit Schadsoftware innerhalb von zwei Jahren, um 8% gestiegen ist. Laut der Statistik haben sich Phishing und Angriffe auf Passwörter sogar verringert. Erschreckend ist jedoch trotz Zu- oder Abnahmen bestimmter Phänomene, dass nahezu neun von zehn Unternehmen von Cyberangriffen getroffen werden und in 86% ein Schaden verursacht wird [36]. Diese Statistik bestätigt noch einmal die Aktualität und Präsenz des Themas.

2.2 Phishing

Der Begriff Phishing ist ein englisches Kunstwort aus „P“ für „Password“ und „fishing“ für „fischen“ [3]. Es beschreibt den Vorgang des Datendiebstahls, indem mittels gefälschten E-Mails, falschen Webseiten oder Malware Passwörter abgegriffen werden. Dazu werden gefälschte E-Mails, SMS Nachrichten oder Webseiten genutzt [2]. Oft werden Spam Mails mit Phishing verwechselt, wobei Spam lediglich ein Begriff für alle unerwünschten E-Mails darstellt. Wenn die Opfer dann auf Links oder Anhänge klicken, werden sie in den meisten Fällen dazu aufgefordert, sensible Daten einzugeben. Obwohl es hauptsächlich um die Passwörter geht, können auch andere sensible Daten wie Bankdaten gestohlen werden. Diese wiederum werden dann auf Darknet-Marktplätzen gehandelt und können im Anschluss für neue Straftaten genutzt werden [2].

Phishing ist jedoch nicht nur Passwort angeln, denn bei einem solchen Angriff kann ebenfalls Schadsoftware eingeschleust werden. Insbesondere für Ransomware ist Phishing ein häufig genutztes Einfallstor [9].

Für Unternehmen entstehen dadurch finanzielle Schäden in Millionenhöhe. Doch neben diesem Schaden hat ein solcher Angriff zusätzlich meist Systemausfälle, Produktionsausfälle oder Reputationsschäden zur Folge [5]. Seit dem Beginn des russischen Angriffskrieges auf die Ukraine ist auch die Bedrohung der Wirtschaft durch Cyberattacken in den Fokus gerückt. Insbesondere wird eine Zunahme von Cyberattacken auf kritische Infrastrukturen erwartet [2].

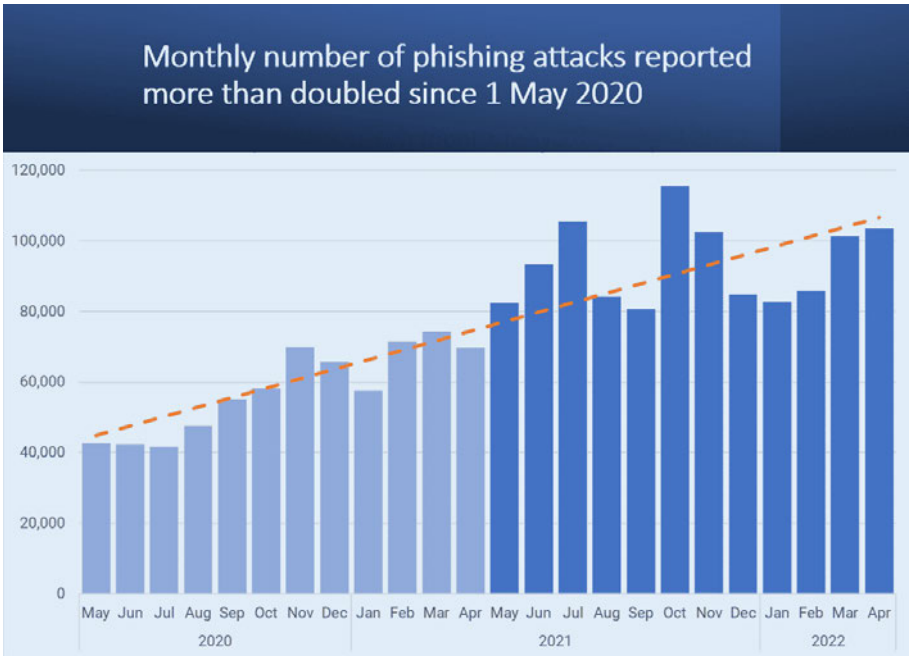

Abbildung 2: Entwicklung Phishing Angriffe 2020-2022 [36]

Die Statistik der Anti-Phishing-Working-Group zeigt einen deutlichen Anstieg der Phishing Angriffe allein zwischen den Jahren 2020 und 2022. Von circa 40.000 Angriffen im Monat Mai 2020 sind die Zahlen auf durchschnittlich 100.000 Angriffe in den Monaten März und April 2022 gestiegen. Doch Monate wie Juli und Oktober 2021 zeigen auch, dass Angriffszahlen jenseits der 100.000 realistisch sind. Dabei wurden über 2.000 Unternehmen zum Ziel von Phishing Angriffen [36].

2.2.1 Spear Phishing

Spear Phishing war im Jahr 2019 der beliebteste Angriffsvektor bei Cyberangriffen [6]. Diese Unterform des Phishings beschreibt zielgerichtete Phishing-Angriffe, welche speziell auf eine Person oder ein Unternehmen gerichtet sind. Dabei werden bereits bestehende Vertrauensverhältnisse ausgenutzt wie z.B. E-Mails im Namen von Kollegen oder gefälschte Rechnungen von tatsächlichen Lieferanten [5]. Es werden also nicht hunderte Spam Mails an willkürliche Adressen gesendet in der Hoffnung auf Erfolg, sondern es wird individuell ein direkter Angriffspunkt ausgewählt und attackiert. Die durchschnittlichen Kosten eines solchen Angriffs beliefen sich im Jahr 2015/2016 in US-Unternehmen auf 1,8 Millionen Dollar [7].

2.3 Social Engineering

Der Begriff „Social Engineering“ bezeichnet eine Vorgehensweise, bei der die Schwachstelle Mensch ausgenutzt wird. Ziel ist es, durch menschliche Kommunikation Informationen, Passwörter oder Konfigurationen zu erlangen [4]. Es geht darum Menschen zu verstehen, Vertrauen aufzubauen und dieses zu missbrauchen, um an vertrauliche Informationen, die auch zur digitalen Identität gehören können, zu gelangen. Dazu gehören z.B. Daten zur eindeutigen Authentifizierung, Daten zur pseudonymen Identifizierung oder persönliche Merkmale [39].

Oftmals werden dafür Identitäten oder Autorität vorgetäuscht, um die Glaubwürdigkeit zu stützen. Im Gegensatz zum Phishing treten hier in seltenen Fällen die Personen auch direkt in Erscheinung, z.B. beim Voice Phishing, wobei das Opfer direkt vom Täter kontaktiert wird. Im Vergleich zum Jahr 2021 wurde im Jahr 2022 ein deutlicher Anstieg von Social Engineering Angriffen festgestellt. Rund 48% der Unternehmen berichteten von Versuchen sowohl über das Telefon als auch über E-Mails [2].

Open Source Intelligence (OSINT) ist die Grundlage des Social Engineerings. Es beschreibt das Sammeln von sicherheitsrelevanten Informationen, die frei verfügbar und jedem zugänglich sind [39]. Allerdings kaufen Kriminelle auch oft solche Informationen, welche als „Leads“ bezeichnet werden. Dabei handelt es sich z.B. um spezielles Insider Wissen, E-Mail Adressen oder Daten von früheren Leaks.

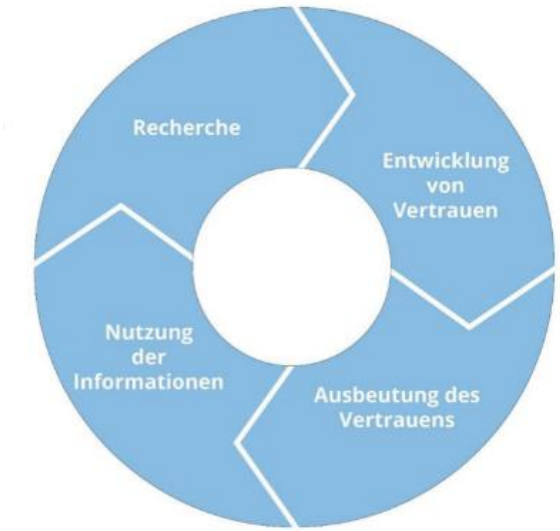

Abbildung 3: Zyklus des Social Engineering [39]

Diese Grafik beschreibt das Social Engineering als Zyklus aus vier unterschiedlichen Teilen, die sich immer wiederholen. Man beginnt mit einer Recherche, um mit diesem Wissen Vertrauen aufzubauen, welches im Anschluss missbraucht wird. Mit den neuen, ausgebeuteten Informationen kann man durch eine erneute Recherche wieder einen Schritt mehr Vertrauen aufbauen [39]. Dieser Zyklus zeigt damit auch, dass beim Social Engineering nicht zwingend Angriffe durch technische Mittel im Vordergrund stehen.

2.4 Abgrenzung

Phishing und Social Engineering sind zwei Begriffe, die oft als Synonym verwendet werden, jedoch trotzdem unterschiedliche Bedeutungen haben. Es sind beides Methoden, die von Cyberkriminellen eingesetzt werden, um an sensible und private Informationen zu gelangen. Dabei ist Phishing eine spezielle Form des Social Engineerings.

Beim Phishing richtet sich die Vorgehensweise klar nach dem Ziel. Denn hier erfolgen die Angriffe in den meisten Fällen über Kommunikationskanäle wie gefälschte E-Mails oder Webseiten. Der Angreifer täuscht vor, eine legitime Quelle zu sein.

Das Social Engineering hingegen ist generell allgemeiner und besitzt eine große Palette an Methoden, die sich hauptsächlich auf die Ausnutzung menschlicher Schwächen bezieht. Dafür können Täuschung, Manipulation, Bestechung oder Drohungen angewandt werden. Dieses Vorgehen hat nicht immer Daten oder Passwörter als Ziel. Es wird z.B. auch im Wahlkampf oder in der Werbung eingesetzt, um Menschen zu manipulieren. Man kann Social Engineering auch in Verbindung mit Phishing einsetzen, aber es ist nicht auf das Sammeln von Informationen beschränkt.

In dieser Arbeit soll jedoch das Phishing mit seinen Angriffsmöglichkeiten im Vordergrund stehen. Angriffe in Person sollen in dem Fall vernachlässigt werden.

3. Auswirkungen im Unternehmenskontext

Begriffe wie Cyberangriffe, Hacking, Phishing oder Malware gehören mittlerweile in den täglichen Sprachgebrauch und spielen sowohl bei Privatpersonen als auch in Unternehmen eine große Rolle. Doch besonders Unternehmen haben eine weitaus größere Verantwortung, wenn es um Cybersicherheit geht. Sie müssen Geschäftsgeheimnisse und Kundendaten gleichermaßen schützen, da sonst ein enormer Imageschaden oder sogar Bußgelder drohen [20]. Doch auch die eigene IT ist schützenswert, denn wenn ein totaler Systemausfall droht, könnte das Unternehmen mit seiner Existenz bezahlen.

Unternehmen sind oft das Ziel von Phishing Angriffen, da sie über wertvolle Informationen wie Finanzdaten, geistiges Firmeneigentum oder Kundendaten verfügen. Die größte Bedrohung durch einen erfolgreichen Phishing Angriff entsteht allerdings durch Ransomware. Da bei beiden ausgewählten Fallbeispielen keine Ransomware zum Einsatz kam, diese aber eine nicht zu unterschätzende Gefahr ist, soll diese Bedrohung im folgenden Kapitel näher erläutert werden.

Durch Ransomware kann es zu Betriebsausfällen und finanziellen Verlusten kommen, da entweder Teile oder das gesamte System verschlüsselt werden. Weitere Arten von Angriffen zielen im Gegenzug darauf ab, Benutzernamen und Passwörter aber auch Kreditkarteninformationen von Mitarbeitern zu stehlen. Durch das Einschleusen von Schadsoftware in Systeme des Unternehmens kann es zu Identitätsdiebstahl, Datendiebstahl oder auch Datenverlusten kommen [5]. Deshalb ist nahezu jedes Unternehmen auf eine lückenlose aber vor allem sichere IT-Infrastruktur angewiesen [20].

3.1 Angriffsvektoren in Unternehmen

Ein Angriffsvektor beschreibt sowohl einen Weg als auch eine Technik, die von Angreifern genutzt werden, um ein IT-System zu attackieren oder zu kompromittieren. Es handelt sich dabei um spezifische Schwachstellen oder Sicherheitslücken. Möglich ist auch eine Kombination dieser mit der Folge, Zugang zu unautorisierten Bereichen im System zu erhalten.

Der Anteil von Spam E-Mails im gesamten Verkehr lag im Jahr 2015 bei circa 77,3%. Der Teil mit infiltrierten Schadprogrammen im gesamten Kommunikationsaufkommen macht ungefähr 1,6% aus. Der Anteil von Rechnern mit Windows XP in deutschen Unternehmen liegt bei 6%. Das bedeutet, dass insgesamt 12% der Bürorechner kein gepatchtes Betriebssystem verwenden oder eines mit verwundbaren Standardanwendungen. Durch bereits bekannte Sicherheitslücken ist es für Angreifer ein leichtes diese auszunutzen. Fast genauso angreifbar sind diese Systeme durch infiltrierte Webseiten. Etwa 3% aller Webseiten sind mit Drive-by Exploits infiziert. Wie leicht die Kompromittierung eines Systems gelingt zeigten interne Tests in verschiedenen Unternehmen im Jahr 2015, welche von der Industrial Control System Security des BSI veröffentlicht wurden. Während simulierten Phishing Angriffen konnte eine Erfolgsquote von 15-25% festgestellt werden. Nur auf die Managementebene bezogen waren es sogar bis zu 80% [23].

Generell werden professionelle, sehr spezifische zielgerichtete Angriffe immer häufiger. Das Problem darin besteht, dass der erste Schritt häufig den Mensch und die ihn umgebenden Prozesse als Schwachstelle ausnutzt.

3.2 Ransomware

Das Bundeskriminalamt nennt 2021 auch das Jahr der Ransomware. Im Gegensatz zum Vorjahr 2020 steigt die durchschnittliche Schadensumme um 21 Prozent auf rund 204.695 US-Dollar pro Angriff. Der dadurch entstandene Schaden beläuft sich jährlich auf circa 24,3 Milliarden Euro [2]. Im zweiten Quartal 2022 betrugen die Lösegeldforderungen laut dem IT-Unternehmen Coveware im Durchschnitt 230.000 Euro. Von Mitte 2021 bis Mitte 2022 zählte das BSI 117 Millionen neue Schadprogramm Varianten [58]. In diesem Kapitel soll die Brisanz von Ransomware ausführlich beleuchtet werden, da sie nicht nur existenzbedrohend für Unternehmen sein kann, sondern Phishing auch als häufigster Angriffsvektor zählt [9].

Aufgrund des hohen Schadenpotenzials erlangte Ransomware in Fachkreisen aber auch medial die höchste Aufmerksamkeit [2]. „Ransom“ bedeutet im englischen Lösegeld und unter Ransomware versteht man eine Schadsoftware, die Lösegeld erpressen soll. Ransomware kann auf verschiedene Arten verbreitet werden wie z.B. Schwachstellen im Betriebssystem, Phishing-Angriffe oder E-Mail Anhänge. Die häufigsten Angriffsvektoren laut dem BSI sind dabei [65]:

- Spam mit gefälschten Links und Anhängen
- Drive-By Infektionen mittels Exploit-Kits
- Schwachstellen in Servern
- Ungeschützte Fernzugänge

Sobald das System infiziert wurde, werden entweder bestimmte Daten oder das ganze System verschlüsselt und blockiert. Im Anschluss taucht dann meist eine Forderung nach Lösegeld, meist in Form von Kryptowährung, auf, um den Zugriff wieder herzustellen [9]. Ebendiese Kryptowährungen machen es nahezu unmöglich der Spur des Geldes zu folgen, was kriminalistisch gesehen eine Spur zum Täter sein kann [34]. Eigentlich ist dieser direkte Geldtransfer für Kriminelle ein großer Vorteil, denn es werden weder Mittelsmänner noch Warenagenten benötigt [65]. Doch in diesem Punkt unterscheiden sich gewisse Kryprowährungen. Bei Bitcoin werden auch weiterhin Mittelsmänner eingesetzt, um die Verschleierung bei einem Geldtransfer gewährleisten zu können. Diese Vorgehensweise wird auch als Mixer bezeichnet. Die neuere Kryptowährung Monero hingegen hat zunehmend an Akzeptanz gewonnen, da sie sehr viel Wert auf die tatsächliche Anonymität der Transaktionen und der Nutzer legt [69].

Die Folgen eines Ransomware Angriffs können für Unternehmen existenzbedrohend sein. Ein solcher Vorfall führt typischerweise zum Ausfall des kompletten Geschäftsbetriebs sowie einem massiven Reputationsverlust gegenüber Kunden und Partnern. Keine Seltenheit sind auch Datenverluste wie Kundendaten, Mitarbeiterdaten, Unternehmensstrukturen oder Geschäftsgeheimnisse [62]. Viele Unternehmen zahlen aus Angst vor einem Totalausfall und ihrem Bankrott das Lösegeld. Die Polizei wiederum rät von diesem Vorgehen ab, weil es für die Täter einen Anreiz schafft [9].

Weiterhin garantiert die Zahlung nicht, dass das Unternehmen den Zugriff auf ihr System wiedererlangt. Ein Bericht aus dem Jahr 2020 zeigt, dass im Vorjahr 2019 mehr als die Hälfte (56 %) aller Ransomware Opfer das Lösegeld bezahlt haben, um den Zugriff auf ihre Daten wieder herzustellen. Bei 17 Prozent war dies jedoch keine Garantie für die Rückgabe [22]. Im Endeffekt gibt es jedoch Unternehmen, die ebenfalls zahlen und dann niemals zugeben, dass es einen solchen Vorfall überhaupt gegeben hat.

Die Abwehr eines Ransomware Angriffs hängt davon ab, wie gut man darauf vorbereitet ist. Die Vermeidungsstrategie wird nach S. Evers [34] in fünf Schritte eingeteilt:

- Vorbereitung
- Entdecken und Feststellen
- Eindämmung und Quarantäne
- Systembereinigung und Entfernung von Ransomware
- Wiederherstellung von Netzwerken, Systemen und Daten

Neben der Vermeidungsstrategie ist in einem solchen Angriffsfall ein Backup der Daten oder des Systems in regelmäßigen Abständen unerlässlich. Denn dieses kann im Notfall aufgespielt werden und man kann vorerst die Wiederherstellung der Daten erreichen. Ein nachhaltiger Schutz ist wohl nur möglich, wenn mit Schreib- und Ausführungsrechten sparsam umgegangen wird [57].

3.2.1 Double Extortion

Die Möglichkeit ein Backup nach einem Ransomware Angriff einzuspielen, galt lange Zeit als eine gute Methode gegen Cybererpresser. Doch auch diese entwickeln ihre Taktiken immer weiter, sodass ein neuer Modus Operandi entstand – die Double Extortion, also eine doppelte Erpressung. Bevor die Malware auf das System des Unternehmens gespielt wird, stehlen die Angreifer zusätzlich die Daten. Dann verschlüsselt die Ransomware wie üblich die Daten.

Es folgt die Lösegeldforderung im Austausch für die Entschlüsselung [21]. Die vorher erbeuteten Daten dienen dann bei Lösegeldverhandlungen als zusätzliches Druckmittel, um die Unternehmen zur Zahlung zu nötigen [62].

Zusätzlich wird den Opfern dann aber gedroht, bei Nichtzahlung die gestohlenen Daten online zu veröffentlichen [21]. Die Anzahl sogenannter Data-Leak Seiten, ist laut dem BSI im Zeitraum von 2020 bis 2021 um 360% gestiegen [63].

Um das Ziel einer Lösegeldzahlung zu erreichen, kann der Druck auf betroffene Unternehmen noch weiter erhöht werden. Sodass es für ein Unternehmen den Anschein hat, keinen anderen Ausweg zu haben, als die Zahlung zu tätigen. Angreifer nutzen dahingehend auch die öffentliche Aufmerksamkeit oder drohen mit der Meldung bei Daten- oder Steuerbehörden. Bei einem Cyberangriff können Verstöße gegen die Datenschutzgrundverordnung begangen werden, weshalb Unternehmen eine Meldepflicht bei den zuständigen Behörden haben. Geschieht dies nicht innerhalb eines vorgegebenen Zeitraums droht eine Strafe [63]. Damit soll verhindert werden, dass Unternehmen das Lösegeld zahlen aber nie offiziell bekannt wird, dass es einen Ransomware Angriff gab bei dem eventuell sensible Daten abgeflossen sind.

3.2.2 Schutzmaßnahmen gegen Ransomware

Da Ransomware eine der größten Bedrohungen für Unternehmen ist, die auch mit einem Bankrott einhergehen kann, sollte in jedem Fall in den Schutz gegen solche Angriffe investiert werden. Kriminelle haben daraus ein Geschäftsmodell entwickelt, dabei sind Desktop-Betriebssysteme wie Microsoft Windows und Apple Mac OS oder auch Server-Systeme wie Linux gleichermaßen betroffen [66]. Es ist besonders wichtig bereits in der Vorbereitung Sicherheitsmaßnahmen zu ergreifen, um eine Ransomware-Infektion im besten Falle zu vermeiden. Die einzige Möglichkeit besteht darin, sich einen Überblick über Verhaltensindikatoren zu verschaffen, sodass die Angriffskette visualisiert und unterbrochen werden kann [21].

Um geeignete Maßnahmen gegen einen Ransomware Angriff ergreifen zu können, muss man den Ablauf zuerst verstehen. Diesbezüglich hat das BSI eine sogenannte „Ransomware Killchain“, bestehend aus sechs Schritten erstellt [66].

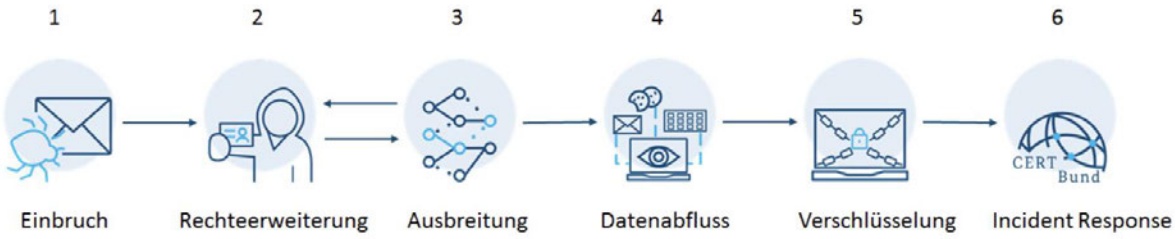

Abbildung 4: BSI Ransomware Killchain [66]

Die „Ransomware Killchain“ beschreibt den typischen Ablauf eines Ransomware Angriffs und gibt einen Überblick über den Ablauf einer solchen Attacke.

Es zeigt die Schritte die ein Angreifer durchläuft (Einbruch und die Rechteerweiterung), bis er die Ransomware ins System geschleust hat. Daraufhin folgt dann die größtmögliche Ausbreitung zum Sammeln von Daten. Im Worst-Case (deutsch: schlimmster Fall) steht das Unternehmen am Ende vor seinem verschlüsselten System und versucht mit einem Incident Response Plan zu retten was möglich ist.

Eine Erweiterung mit konkreten Vorschlägen zu Schutzmaßnahmen sieht ein zehn Phasen Plan mit folgenden Punkten vor [67]:

- **Patches und Updates:** sollten unverzüglich eingespielt werden, um vor Softwareprogramm Schwachstellen (vom Hersteller) geschützt zu sein
- **Remote Zugänge:** der Zugriff von außen sollte nur über VPNs zusammen mit der Zwei-Faktor-Authentifizierung genutzt werden
- **E-Mails und Makros:** die Darstellung des Inhalts sollte als reine Textdarstellung erfolgen und nicht in „HTML-Mail“, Webadressen können so nicht verschleiert werden
- **Ausführen von Programmen: „**Application Whitelisting“ verhindert das Öffnen von nicht freigegebenen Programmen, es sollten nur Programme ausgeführt werden, die nicht von Benutzern beschrieben werden können
- **Virenschutz:** es sollten besonders die Module „Intrusion Prevention“ und Cloud Dienste der AV-Software genutzt werden
- **Administrator Accounts:** mit privilegierten Accounts sollten ausschließlich Administratortätigkeiten ausgeführt werden, d.h. keine E-Mails lesen oder im Internet surfen, diese Accounts sollten immer über eine Zwei-Faktor-Authentifizierung verfügen

- **Netzwerk segmentieren:** hilft den Schaden zu begrenzen da die Ransomware nur die Systeme in unmittelbarer Nachbarschaft erreichen kann, Voraussetzung dafür ist die sichere Umsetzung der Administrator Accounts
- **Backups und Datensicherungskonzept:** gewährleisten die Verfügbarkeit der Daten während eines Ausfalls, sie müssen in einem Offline-Backup gesichert werden, ein Praxistest des Wiederanlaufs wird empfohlen
- **Netzlaufwerke:** wichtige Dokumente sollten nie nur lokal gespeichert sein, besser auf einem Netzlaufwerk ablegen
- **Notfallplan:** für das Worst-Case Szenario, geschäftskritische Systeme müssen identifiziert werden und alternative Kommunikationsmöglichkeiten vorbereitet sein

Besonders in der Vorbereitung können bereits präventiv einige Schutzmaßnahmen getroffen werden, die nicht nur allein vor Phishing schützen, sondern eben auch vor Ransomware. Weitere umfassende technische Schutzmaßnahmen inklusive Vorfallreaktionsplänen und Mitarbeiter Awareness werden in Kapitel 4 noch ausführlich betrachtet.

3.2.3 Beispiel Ransomware Angriff

Ein sehr bekanntes Beispiel für einen erfolgreichen Ransomware Angriff ist Continental. Im August 2022 gibt der deutsche Autozulieferer in einer Pressemitteilung bekannt, dass Eindringlinge das interne Netzwerk infiltriert haben und sie den Cyberangriff daraufhin selbst abgewendet haben. Es wurden umfassende Maßnahmen ergriffen, um die Integrität der Systeme wiederherzustellen. Die zuständigen Behörden wurden ebenfalls informiert, da vermutet wurde, dass es zu Datenverlusten gekommen ist [61]. Erst rund drei Monate nach dem Angriff, im November 2022 wird öffentlich bekannt, dass Continental erpresst wird. Die Ransomware-Gruppe „Lockbit 3.0“ teilte im Darknet ein Screenshot der Verhandlung mit dem Unternehmen. Daraus wird auch das Scheitern dieser ersichtlich. Nachdem Continental versucht hat die Gruppe hinzuhalten, haben diese ihre Drohung, die erbeuteten Daten zu veröffentlichen, teilweise wahr gemacht. Auf einer Seite im Darknet wurde eine Liste von Dateinamen mit 40 Terabyte veröffentlicht. Diese Liste steht für „nur“ 40 Millionen Dollar zum Verkauf [60]. Darin enthalten waren unter anderem [60]:

- 4650 Dateinamen mit dem Begriff „geheim“
- 15.000 Dokumente enthielten den Begriff „Gehalt“
- 76.000 Dokumente behandeln den Jahresabschluss

- 2500 Dateinamen enthielten den Begriff „Aufsichtsrat“
- 28.000 Dateien mit Vorgängen des Betriebsrats
- 18.000 Dokumente gehören zum Ordner „IT_Administration“
- 50.000 Dokumente enthielten den Begriff „Security“
- 400 Dateinamen mit dem Begriff „Passwort“
- 47.000 Dateien mit den Begriffen „Arbeitssicherheit“ und „Unfälle“

Anhand der gestohlenen Daten können die Angreifer sehr genau einschätzen, wie die wirtschaftliche Situation des Unternehmens ist und wie hoch der Schaden bei einer Veröffentlichung der Daten wäre. Entsprechend danach haben sie auch einen guten Überblick, was Continental bereit wäre zu zahlen [60].

Continental beteuert in seiner Pressemitteilung, dass die Sicherheit der Informationen von Mitarbeiterinnen und Mitarbeitern, Kunden und Partnern von größter Bedeutung seien. Demzufolge seien auch schon in der Vergangenheit entsprechende Maßnahmen ergriffen worden, um die Cybersicherheit des Unternehmens stetig zu verbessern [61]. Aus Unternehmenskreisen geht hervor, dass Continental nicht zahlen wird, egal wie hoch der Schaden sei, der bei einer Veröffentlichung entstehen würde [60].

3.3 Cyberversicherungen

Durch Cyberangriffe auf Unternehmen entstehen nicht nur hohe finanzielle Schäden, sondern auch der Ruf und das Vertrauen von Kunden kann darunter leiden. Kein Unternehmen ist, egal mit welchen Schutzmaßnahmen, zu einhundert Prozent sicher vor Cyberangriffen und insbesondere Phishing Angriffen. Viele Versicherungen bieten deshalb seit einigen Jahren einen umfassenden Schutz gegen Hacking- oder Cyberangriffe an [34]. Sogenannte Cyber-Policen fassen dabei mehrere verstreute Risiken zusammen und können sowohl Eigen- als auch Drittschäden abdecken. Sie greifen z.B. bei Datendiebstahl, unerlaubter Veröffentlichung von Daten, Datenwiederherstellung, Betriebsunterbrechung, Kostenerstattung für Ursachensuche, IT-forensische Untersuchungen und Software-Spezialisten ein [43].

Es gibt jedoch sehr unterschiedliche Versicherungsbedingungen für Unternehmen. Vermeintlich sind alle Risiken mit einer Police abgedeckt, doch der russische Angriffskrieg auf die Ukraine verändert dieses Bild. Denn viele Verträge schließen einen Schaden, der durch kriegerische Aktionen entsteht, aus. Genauso wie Kollateralschäden. Weiterhin können die Versicherungen gewisse Bedingungen für einen Vertrag stellen. Sie können z.B. eine Zwei-Faktor-Authentifizierung oder ein Anti-Phishing Training für Mitarbeiter fordern [58]. Sind solche Vertragsbedingungen im Schadenfall jedoch nicht erfüllt, kann die Versicherung eine Auszahlung verweigern und das Unternehmen bleibt auf den Kosten sitzen. Umstritten ist auch, ob die erhöhten Auflagen immer für mehr Sicherheit sorgen. Die Unternehmen könnten einfach mehr für die Versicherungspolice zahlen, anstatt ihre eigenen Systeme zu verbessern [58].

Eine Cyberversicherung wird besonders häufig abgeschlossen, um bei einem Ransomware Angriff mit Lösegeldforderungen abgesichert zu sein. Die immer höheren Abdeckungssummen sollen dann im Schadenfall die hohen Lösegeldforderungen übernehmen [34]. Doch damit könnten sich Unternehmen in falscher Sicherheit wiegen, denn oft reicht die Deckungssumme nicht für den gesamten Schaden der entsteht [58]. Durch diese vermeintliche Sicherheit werden teilweise gezielt Unternehmen mit einer solchen Versicherung angegriffen. Denn damit können die Erpresser sicher sein, dass sich die Zahlungsbereitschaft erhöht [34]. Selbst die Polizei rät von Lösegeldzahlungen ab [9]. Denn diese würden das Geschäftsmodell der Kriminellen stärken und Nachahmer anlocken [58].

Doch auch für die Versicherungen entstehen durch eben solche Policen und die hohen Schadenssummen, die ausbezahlt werden müssen, eine enorme Belastung.

Deshalb ist der Preis für eine Cyberversicherung oft sehr hoch und beinhaltet eine hohe Selbstbeteiligung. Bei vielen Policen ist der Versicherungsschutz dann auf konkrete und eingeschränkte Gefahrenszenarien beschränkt [44]. Manche wollen sogar generell Schäden ausschließen, die durch staatliche Hacker entstehen [58]. Dabei kann von niemandem klar definiert werden, wer ein staatlicher Hacker ist und wer nicht. Demzufolge ist diese Thematik sehr unsicher. Ob Cyberversicherungen für die Versicherungsunternehmen attraktiv sind, kann man als außenstehende Person nur vermuten, aber sicher ist, dass die Preise für Policen durch die vielen Schadenfälle in Zukunft steigen werden.

4. Schutzmaßnahmen

In Anbetracht der steigenden Bedrohung durch Phishing Angriffe ist es für Unternehmen von entscheidender Bedeutung, geeignete Schutzmaßnahmen zu ergreifen. Dabei geht die Informationssicherheit keinesfalls nur die IT etwas an. Schutzmaßnahmen müssen auf allen Ebenen eines Unternehmens verankert sein, um die Sicherheitsziele „Vertraulichkeit“, „Verfügbarkeit“ und „Integrität“ erreichen zu können [32]. Die existierenden und nur schwer vermeidbaren Angriffsvektoren führen dazu, dass jedes Unternehmen eine eigene spezifische Cyberabwehrstrategie braucht. In der Literatur werden die Maßnahmen dafür meist in nutzerabhängige (z.B. richtiges Verhalten, Filter, Browser Plug-ins) und nutzerunabhängige Verfahren (z.B. Spam-Trap, Domain-Watch, Validierung von Absenderdaten, Fraud Detection Systeme) unterteilt [15]. In dieser Arbeit werden besonders verschiedene technische Schutzmaßnahmen im Detail untersucht und wie sie dazu beitragen können, die Sicherheit eines Unternehmens zu erhöhen. Ein trotzdem nicht zu vernachlässigender Punkt ist die Schulung von Mitarbeitern, um Security Awareness zu schaffen. Nur durch die Implementierung unterschiedlicher Schutzmaßnahmen können Unternehmen ihre Systeme und Daten besser schützen. Doch dafür müssen Technik und Mensch Hand in Hand gehen.

4.1 Technische Schutzmaßnahmen

Die technischen Schutzmaßnamen spielen bei Phishing Angriffen womöglich eine deutlich größere Rolle als viele es wahrhaben möchten. Denn Menschen können immer Fehler machen oder unter Druck falsch reagieren. Doch ein System sollte den Angreifern danach nicht zu Füßen liegen, sondern durch weitere Maßnahmen geschützt sein. Mit der ständig wachsenden Anzahl von Angriffen und der steigenden Professionalität sind die folgenden technischen Schutzmaßnahmen essenziell für den Schutz eines Unternehmens.

4.1.1 E-Mail Filterung

Bei dem oben genannten Spam Anteil von 77% im gesamten E-Mail Verkehr ist es unabdingbar den Verkehr zu Filtern. Die Filterung basiert auf bestimmten Algorithmen, die von der Filter-Software festgelegt werden. Eine Methode ist die Filterung nach den Absendern.

Spam-Filter nutzen sogenannte Blockierlisten, welche bekannte und zugelassene Absender, aber auch unbekannte Absender enthält. In der Literatur wird auch der Begriff weiße und schwarze Liste verwendet. Die Wirksamkeit der schwarzen Liste ist jedoch beschränkt, da die Spam-Versender laufend ihre Adresse ändern [24]. Eine weitere sinnvolle Möglichkeit ist, den E-Mail Verkehr nach einem heuristischen Verfahren zu filtern. Hierfür wird nach Mustern wie bestimmte Wörter, Phrasen oder Groß- / Kleinschreibung gesucht, die verdächtig sein können. Es wird sowohl der Header als auch der eigentliche Textteil gescannt. Der Erfolg bei dieser Methode hängt stark von den Regeln ab. Gut entwickelte Filter können aber 90-95% von Spamnachrichten erkennen [40].
Anhand dieser vielen unterschiedlichen Filtermöglichkeiten kann man den einzelnen E-Mails auch einen Spam-Score zuweisen und damit dann entscheiden, ob diese Spam sind oder nicht. Es gibt viele unterschiedliche oder individuelle Möglichkeiten der Umsetzung, aber das Prinzip ist jedes Mal gleich. Jede Mail hat beim Eintreffen den Score 0, welcher sich bei Erfüllen von Filterkriterien ändert. Wird dann ein expliziter, vorher festgelegter Wert überschritten wird die E-Mail als Spam deklariert [41]. Die E-Mail Filterung bezieht sich hauptsächlich auf unerwünschte Spam-Mails. In den Anfängen des Phishings wurden allerdings häufig in solchen Spam-Mails gefälschte Anhänge oder Links versteckt. Diese Filterung sollte also auch vor Phishing Angriffen schützen. Doch die Art des Phishings hat sich weiterentwickelt, sodass Angriffe häufig viel gezielter vorgenommen werden und zum Teil bereits bestehende Vertrauensverhältnisse ausgenutzt werden [5]. Somit werden sensible Daten nicht zufällig durch eine Spam-Mail erbeutet, sondern gezielt von angeblichen Kollegen oder dem Chef gefordert. Da in Firmen meist eine Hierarchie herrscht, werden die meisten Menschen den Forderungen nachgehen. Diese Tatsachen verdeutlichen aber auch, dass eine E-Mail Filterung allein nicht ausreicht, um sich vor Phishing Angriffen zu schützen und weitere Maßnahmen erforderlich sind.

Unabhängig von der E-Mail Filterung ist es trotzdem möglich, das Phishing E-Mails übersehen werden und im Postfach landen. Dafür hat das BSI weitere Vorschläge in der folgenden Grafik zum Erkennen von Phishing E-Mails zusammengestellt die jeder anwenden kann [46].

Abbildung 5: Phishing E-Mails erkennen [46]

Wenn E-Mails einen oder mehrere dieser Punkte enthalten, sollte Vorsicht walten, denn dies könnten Hinweise auf eine Phishing E-Mail sein. Es ist weit verbreitet, dass sprachliche Ungenauigkeiten oder die Abfrage vertraulicher Daten auf Phishing schließen lassen. Eine Garantie dafür gibt es allerdings nicht.

4.1.2 Anti-Malware Software

Durch infizierte E-Mail Anhänge wird häufig Malware, also Schadsoftware in ein System geschleust. Um dies zu verhindern ist besonders Prävention gefragt. Das Unternehmen sollte in jedem Fall darauf achten, dass die aktuelle Version der Software genutzt wird und diese auch auf dem neuesten Stand zu halten. Denn kein Anti-Malware Programm kann vor Angriffen schützen, wenn die Virenbeschreibungen und Signaturen nicht auf dem neuesten Stand sind [25].

Viren bestehen in der Regel aus den folgenden Teilen, wobei nicht alle in jedem Virus vorhanden sein müssen [25]:

- Erkennungsteil
- Installations- oder Infektionsteil
- Schadensteil („Payload“)
- Bedingungsteil („Trigger“)
- Tarnungsteil

Des Weiteren lassen sich Viren auch nach der Art des Wirtes unterscheiden. Boot-Viren, Datei-Viren und Multi-partite Viren (Mischformen) zählen zu den bekanntesten Wirt-Formen [26].

In den meisten Fällen wird deshalb ein Antivirenscanner zur Erkennung von Malware genutzt. Dabei unterscheidet man generell in zwei Arten. Der OnDemand Scanner ist nur dann aktiv, wenn der Nutzer ihn zu einem bestimmten Zeitpunkt einsetzt. Das wiederum setzt voraus, dass die Malware sich bereits im System befinden muss, um erkannt zu werden. Der OnAccess Scanner hingegen scannt jedes Dokument, das geöffnet wird oder Dateien, die gespeichert werden. Der Vorteil dieser Variante liegt im eigenständigen Scannen im Hintergrund, bei dem es keine Interaktion mit dem Nutzer braucht. Somit ist es möglich, Malware frühzeitig zu erkennen und das Eindringen im besten Fall zu vermeiden. Unabhängig davon, welche der beiden Arten man vorzieht, sollte mindestens eine der folgenden Erkennungsstrategien implementiert sein, um einen Schutz vor Eindringlingen garantieren zu können [25]:

- Prüfsummen, um ungewollte Änderungen an Dateien zu verhindern
- Signaturen, um nach Malwaresignaturen zu suchen
- Suchheuristiken, um im gesamten System nach Malware-Charakteristiken zu suchen (z.B. bestimmte Code-Abfolgen oder Verhaltensmuster von Applikationen)

Da Malware sich rasant verbreiten kann und zum Teil nur schwer zu entdecken ist, ist es für Unternehmen äußerst ratsam in eine Anti-Malware Software zu investieren. Denn die Schäden reichen von absichtlich verursacht über zufällig verursacht bis hin zu den Folgeschäden [26]. In einem Unternehmen kann dies zu fatalen Betriebsausfällen oder hohen finanziellen Kosten führen.

Ein Großteil der Unternehmen bei denen es zu Ransomware Vorfällen kam, hatten allerdings bereits einen Anti-Viren Scanner. Unter anderem muss aus Compliance Gründen einer verwendet werden. Doch wie sich gezeigt hat reicht ein solcher Anti-Viren Scanner allein nicht aus, um sich gegen Phishing Angriffe zu schützen. Es ist wichtig zu erwähnen, dass eine Anti-Malware Software nur einen Teil einer umfassenden Sicherheitsstrategie darstellt und es noch weiteren Maßnahmen bedingt, um das gesamte System zu schützen.

4.1.3 Zwei-Faktor Authentifizierung

Noch im Jahr 2016 war es jedem Dienstanbieter selbst überlassen, wie sich seine Nutzer identifizieren und authentifizieren. Zum einen bestimmt die Art der Authentifizierung wie hoch der Schutz der Nutzerdaten ist, zum anderen aber auch den Grad der Benutzerfreundlichkeit bei der Verwendung eines Dienstes.

Demzufolge war auch in Unternehmen die am häufigsten verwendete Methode die sehr schwache passwortbasierte Ein-Faktor-Authentifizierung [55].

Und das obwohl bereits 1980 für eine erhöhte Sicherheit z.B. bei Transaktionen die Zwei-Faktor-Authentifizierung (2FA) eingeführt wurde [16]. Diese Authentifizierungsart gehört zur Multi-Faktor-Authentifizierung (MFA).

Bisher hatte lediglich ein Benutzername und das zugehörige Passwort für eine Authentifikation gereicht. Jetzt werden diese beiden Eigenschaften zusammen als erster Faktor gesehen, während der Besitz einer physischen Transaktionsnummer (TAN) den zweiten Faktor darstellt [16]. Dabei sollte die TAN ein Einmalkennwort und nur für begrenzte Zeit gültig sein. Für die Erzeugung wird meist ein Codegenerator, auch Token genannt, genutzt. Wichtig bei einer klassischen 2FA ist die Kombination aus einer Wissens- und Besitzkomponente. Das bedeutet, dass Passwort weiß der Nutzer und die TAN hat der Nutzer [17]. Diese Art der Multifaktor Authentifizierung wurde eingeführt, um dem Nutzer eine einfache, schnelle und vor allem sichere Authentifizierung zu gewährleisten.

Im folgenden Abschnitt soll eine der gängigsten Methoden der 2FA näher betrachtet werden und aktuelle Risiken erläutert werden. Bei vielen Authentifizierungsvorgängen wird der zweite Faktor, ein sogenanntes Einmalpasswort, als Push-Benachrichtigung wie z.B. per SMS an den Nutzer gesandt. Der Vorteil insbesondere für die Nutzer ist die einfache Anwendung, denn es ist keine extra Software dafür notwendig. Wie bereits erläutert sollten beide Faktoren Unabhängigkeit voneinander garantieren, was bereits zum ersten Problem werden kann. Erlaubt der Besitz eines Smartphones den Zugriff sowohl auf ein darauf gespeichertes Passwort als auch auf die empfangene SMS-Nachricht, stellt es die Wirksamkeit dieses Verfahrens in Frage. Zudem ist SIM-Swapping eine gängige Angriffsform, um eben diese SMS für eine Authentifizierung abzufangen. Um im Falle eines SIM-Karten Verlusts nicht die Rufnummer wechseln zu müssen, stellen Mobilfunkbetreiber Ersatzkarten aus. Die verlorene Karte wird im Anschluss gesperrt. Diesen Vorgang nutzen Kriminelle aus, um sich als Opfer auszugeben und eine neue SIM-Karte zu beantragen. Der Anbieter sperrt die ursprüngliche SIM daraufhin und der Angreifer bekommt die Ersatzkarte.

Ab diesem Zeitpunkt laufen alle SMS-Nachrichten des Opfers über das Smartphone des Angreifers [27]. Neben dieser spezifischen Angriffsart gibt es allerdings noch weitere Möglichkeiten, um an die Push-Benachrichtigungen zu gelangen. Das Opfer kann direkt vom Angreifer kontaktiert werden und durch den Einsatz von Social Engineering dazu gebracht werden, eine solche Push-Benachrichtigung zu bestätigen. Doch auch ohne direkten persönlichen Kontakt kann ein Angriff Erfolg haben. Bei einer Flut von Push-Anfragen neigen Menschen dazu, eine von diesen vielen Anfragen falsch zu beantworten [14].

Eine weitere Methode die Multi-Faktor-Authentifizierung auszunutzen sind Ermüdungsangriffe. Laut Microsoft sind diese Angriffe, auch bekannt als MFA-Spamming, seit der zunehmenden Akzeptanz von starker Authentifizierung deutlich gestiegen [54].

Der Erfolg dieser Angriffe beruht auf der Tatsache, dass ein Nutzer Push-Benachrichtigungen bestätigt, ohne deren Kontext zu kennen. Bei Aufforderungen wie „Klicken, um zu bestätigen“ oder „PIN eingeben, um zu bestätigen“ werden lediglich einfache Bestätigungen ausgeführt. Eine bessere und sichere Variante wäre es einen Code direkt auf dem Bildschirm einzugeben. Eine Studie zeigt, dass ca. 1% aller Nutzer eine einfache Genehmigungsanfrage beim ersten Versuch akzeptieren [54].

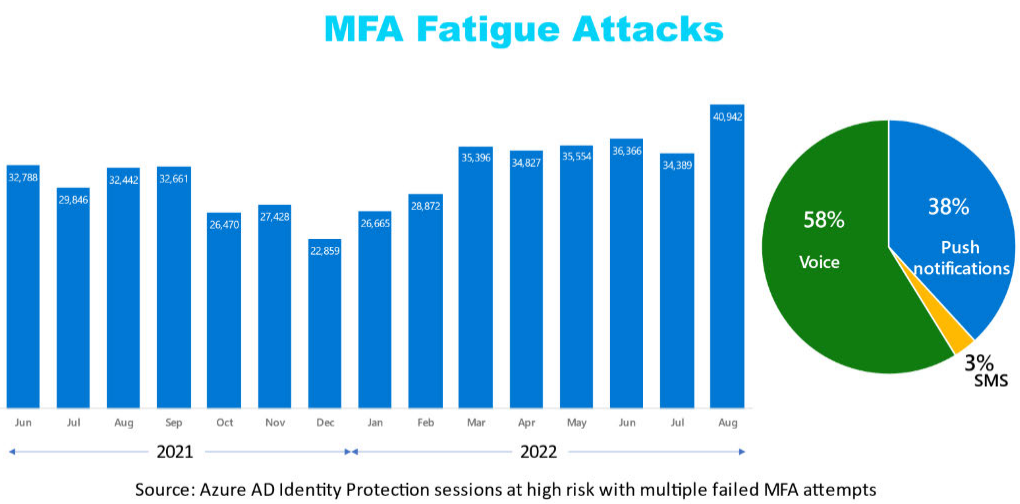

Abbildung 6: MFA Ermüdungsangriffe [54]

Wie die Statistik zeigt, werden 38% der MFA-Ermüdungsangriffe durch Push-Benachrichtigungen ausgelöst. Auch im Fall von Uber konnte so die Multi-Faktor-Authentifikation überwunden werden.

Dahingehend will Microsoft seine Nutzer schützen und hat dafür drei Änderungen entwickelt [54]:

- Zahlenabgleich auf dem Anmeldebildschirm und einer Authentifikations-App
- Kontext der Anmeldung in der Push-Benachrichtigung (z.B. Standort, auf welche App soll zugegriffen werden)
- Bei Personen, die immer noch dazu neigen einfache MFA-Anfragen zu akzeptieren, eine Passwortänderung automatisieren

Die Zwei-Faktor-Authentifizierung wurde entwickelt, um Anmeldeverfahren sicherer zu gestalten. Zusammenfassend kann man aber sagen, dass es in der heutigen Zeit trotz alledem recht anfällig für Phishing Angriffe sein kann und es nicht mehr so sicher ist, wie man einst geglaubt hat. Unternehmen wie Microsoft versuchen deshalb mit kleinen Änderungen, ihre Mitarbeiter aber auch ihre Nutzer vor z.B. Ermüdungsangriffen zu schützen. Denn einfach keine Multi-Faktor-Authentifizierung zu nutzen, stellt keine Option dar. Unternehmen sollten deshalb ihre Systeme im Hinblick auf die veränderte Bedrohungslage neu bewerten und sich gegebenenfalls nach Alternativen umschauen.

4.2 Schulung und Sensibilisierung der Mitarbeiter

Ein Begriff, der neben technischen Sicherheitsmaßnahmen immer präsenter wird, ist Security Awareness, was so viel bedeutet wie Sicherheitsbewusstsein. Es sollte sich bewusst davon verabschiedet werden, den Menschen als besondere Schwachstelle zu bezeichnen. Stattdessen sollte man ihn deutlich mehr in den Vordergrund rücken und als Komponente des eigenen Informationssystems sehen [27]. Denn dafür reichen die technischen Sicherheitsmaßnahmen allein nicht aus. Die Mitarbeiter der Unternehmen sollen in Bezug auf Bedrohungen und Risiken, die mit IT-Sicherheit verbunden sind, aufmerksam gemacht und sensibilisiert werden. Es geht darum, dass sie die Tragweite ihrer Entscheidungen erkennen und lernen wie man sich schützen und im Notfall angemessen reagieren kann [5]. Jedoch fehlt häufig das Verständnis, wie individuell solche Maßnahmen eigentlich sein sollten, denn 39% aller Unternehmen nutzen das gleiche Maßnahmenpaket für alle Mitarbeiter und 15% davon schulen lediglich die IT-Mitarbeiter. Die Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt hat 2017 in einem Informationssicherheitskonzept folgenden Vorschlag für die zielgerichtete Sensibilisierung gemacht [28]:

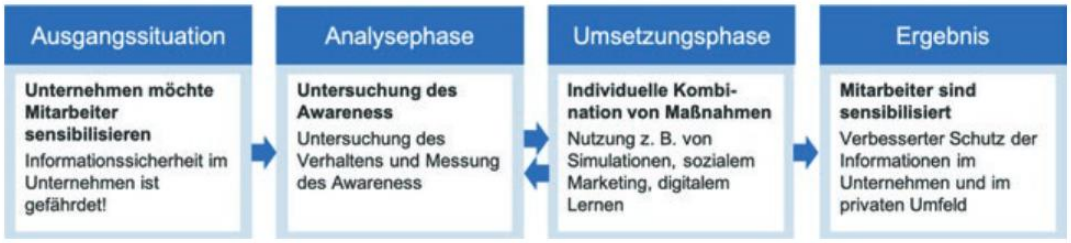

Abbildung 7: Kernidee zielgerichtete Sensibilisierung der FHWS [28]

Dabei sollten die Analysephase und Umsetzungsphase mehrmals durchlaufen werden. Die Ergebnisse fließen dann wieder in die Analyse ein.

Ein weiterer Vorschlag aus der Literatur [5] beschreibt den Aufbau eines Security Awareness Trainings in drei Teilen. Begonnen wird dabei mit einer Präsenzschulung in der grundlegende Themen wie Social Engineering, Phishing oder E-Mail Sicherheit behandelt werden. Ebenfalls werden aus den Medien bekannte Fälle besprochen und bei einem Live-Hacking wird der Ablauf eines möglichen Phishing Angriffs gezeigt. Im Anschluss folgt ein E-Learning, welches die Inhalte aus der Präsenzschulung in einem Web-Based Training erneut aufgreift und vertieft. Als dritte Komponente wird eine Phishing Simulation angeboten. Es bietet die Möglichkeit eine „Selbsterfahrung“ zu machen, und selbst bei einem Fehlverhalten einen Lernmoment zu schaffen.

Bei einem falschen Klick wird man auf eine Website weitergeleitet mit der Erklärung, wie man das Phishing hätte erkennen können [5].

Solche Trainings für Mitarbeiter sollten in regelmäßigen Abständen stattfinden, um eine dauerhafte Awareness aufrecht zu erhalten, und auf neue Verhaltensmuster eingehen zu können. Da sich das Phishing und seine Angriffsmuster stetig verändern, muss Security Awareness dementsprechend als dynamischer Prozess verstanden werden [5]. Ein hohes Sicherheitsbewusstsein kann dazu beitragen, das Risiko von Cyberangriffen oder Datendiebstahl zu reduzieren. In einem Unternehmen ist es wichtig, dass alle Mitarbeiter über ein hohes Sicherheitsbewusstsein verfügen, um eine gut funktionierende IT-Sicherheitsstrategie zu gewährleisten.

4.3 Incident Response Plan

Unter dem Begriff „Incident“ (deutsch: Vorfall) versteht man in der Sprache der IT ein auftretendes Ereignis in einem System oder Netzwerk. Bei einem solchen Vorfall gilt es zu klären, ob es sich um eine normale Betriebsstörung oder einen Systemeinbruch handelt. Letzteres bedeutet einen Sicherheitsverstoß und ist oft mit negativen Konsequenzen verbunden. Falls ein echter Sicherheitsvorfall diagnostiziert wird, muss sofort ein „Incident Response“ (deutsch: Vorfallsreaktion) eingeleitet werden [29]. Um bestmöglich auf einen solchen Angriff reagieren zu können, ist ein Incident Response Plan von Vorteil. Er beschreibt die systematische Reaktion auf Vorfälle und besitzt eine einheitliche Methodik, sodass die richtigen Maßnahmen ergriffen werden können [31]. Ein gutes Incident Management ist demzufolge unerlässlich für ein Unternehmen. Das Spektrum der Aufgaben umfasst nicht nur technische Probleme, Schwachstellen oder konkrete Angriffe, sondern auch organisatorische und rechtliche Fragen [30]. Ein guter Incident Response Plan kann Datendiebstahl oder -verlust sowie die Unterbrechung von Diensten im besten Fall verhindern oder den Ausfall minimieren [31].

In der Literatur wird ein Incident Response auch als Prozess mit sechs Phasen beschrieben [33]:

- Vorbereitung
- Erkennung
- Analyse
- Eindämmung
- Ausrottung und Wiederherstellung
- Aktivitäten nach einem Vorfall

Wurde der Alarm erst einmal ausgelöst, beginnt das Unternehmen den Vorfall zu analysieren und ergreift Maßnahmen zur Eindämmung, um das Informationssystem wieder in den Normalbetrieb zurückzuführen. Die untenstehende Abbildung zeigt, wie diese in einem Zyklus ablaufen, beginnend mit der Vorbereitungsphase. Bei einer genaueren Betrachtung fällt auf, dass jeder Vorfall dazu beiträgt, das Unternehmen besser auf zukünftige Vorfälle vorzubereiten. Denn die Aktivitäten nach einem Vorfall werden wieder zur Vorbereitung auf den nächsten Vorfall genutzt [33].

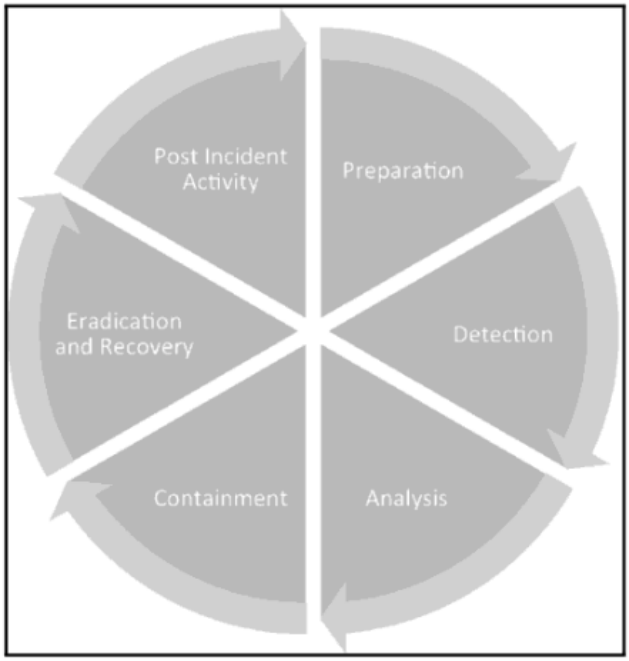

Abbildung 8: Incident Response Prozess [33]

4.4 BSI Empfehlungen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde in Deutschland, die für eine sichere Digitalisierung zuständig ist. Vom Schutz der Regierungsnetze bis hin zum Ratgeber für Privatpersonen sind sämtliche Angebote vertreten. 2009 konnte das BSI für Bundesbehörden verbindliche Sicherheitsstandards für die Beschaffung und den Einsatz von IT entwickeln [18]. Für den Schutz gegen Phishing Angriffe gibt es keine konkrete Unterteilung für Privatpersonen und Unternehmen. Die Schutzmaßnahmen können jedoch von beiden Gruppen gleichermaßen beachtet werden. Es gibt direkt vom BSI eine Phishing Checkliste für den Notfall in der die folgenden Empfehlungen aufgeführt sind, um sich in Zukunft vor Phishing schützen zu können [19]:

- Aktualisierung von Software und Betriebssystemen sofort durchführen
- Antivirenprogramme installieren
- Skepsis bei E-Mails mit unbekanntem Absender und Aufforderungen, sensible Daten herauszugeben oder über einen Link zu ändern
- Echtheit einer E-Mail telefonisch bestätigen lassen, aber nicht die Telefonnummer aus der E-Mail verwenden, sondern eigenständig recherchieren
- Achtung bei Anhängen mit .exe oder .scr, diese können Schadsoftware enthalten und direkt auf das Gerät laden
- Zwei-Faktor-Authentisierung verwenden, kein Zugriff auf Daten möglich nach Erbeutung des Passwortes
- Schulung des Personals

Weiterhin gibt es eine extra Seite mit weiteren aufgeführten Punkten unter dem Titel „Wie schützt man sich gegen Phishing?“ [46]:

- Überprüfen der Adressleiste im Browser
- Niemals auf dubiose Links in E-Mails klicken
- Bei Unsicherheit telefonisch beim genannten Anbieter nachfragen
- Niemals private Daten (Passwörter, Kreditkarten- oder Transaktionsnummern) via E-Mail preisgeben
- Niemals einen Download Link direkt aus einer E-Mail heraus starten
- Keine Dateien aus Anhängen verdächtiger E-Mails öffnen
- Jede Online Session durch einen regulären Logout beenden, nicht nur den Browser schließen

- Regelmäßig den Saldo des Bankkontos kontrollieren sowie die Umsätze
- Keine Daten auf Webseiten mit unverschlüsselter Verbindung eingeben (erkennbar an dem kleinen Schloss in der Adresszeile des Browsers)
- Auf eine aktuelle Antivirus Software und aktive Firewall achten

4.4.1 Weitere Leitfäden

Unternehmen müssen nicht nur einige Grundregeln beachten, um sich vor Phishing zu schützen. Wenn das Unternehmen zusätzlich auch ein Zahlungsdienstleister ist, gibt es weitere Standards, die eingehalten werden müssen. Besonders im mobilen Zahlungsverkehr geben öffentliche Institutionen wie das Europäische Parlament regulatorische Vorgaben an die Akteure. Aber auch private Unternehmen wie MasterCard und Visa oder freiwillige Organisationen wie die International Organization for Standardization (ISO) können Standards setzen [47].

Der PCI Security Standards Council ist eine Organisation, welche mit mehreren Kartenorganisationen zusammen gegründet wurde mit dem Ziel, global gültige Standards für kartenbasierten Zahlungsverkehr zu schaffen. Der Payment Card Industry Data Security Standard (PCI DSS) soll die breite Annahme von konsistenten Datensicherheitsmaßnahmen weltweit erleichtern. PCI DSS ist dafür ein umfassender Standard, der insbesondere auf die Sicherheit bei der Verarbeitung und Speicherung von Karteninhaberdaten, sowie dem Schutz von Zahlungskontodaten, gerichtet ist. Dafür bietet das PCI DSS zwölf Grundanforderungen [48]:

- Installation und Wartung von Netzwerksicherheitskontrollen
- Aufbau und Wartung eines sicheren Netzwerkes und sicherer Systeme
- Schutz von gespeicherten Kontodaten
- Schutz von Karteninhaberdaten mit starker Kryptografie während der Übertragung über offene, öffentliche Netzwerke
- Schutz aller Systeme und Netzwerke vor bösartiger Software
- Entwicklung und Wartung sicherer Systeme und Software
- Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten nach geschäftlichem Bedarf
- Identifizierung von Benutzern und Authentisierung von Zugriff auf Systemkomponenten
- Beschränkung des physischen Zugriffs auf Karteninhaberdaten

- Protokollierung und Überwachung aller Zugriffe auf Systemkomponenten und Karteninhaberdaten
- Regelmäßige Prüfung der Sicherheit von Systemen und Netzen
- Unterstützung der Informationssicherheit durch organisatorische Richtlinien und Programme

Im Fallbeispiel Uber handelt es sich um ein Unternehmen, welches mit Zahlungsdienstleistern zusammenarbeitet. Es muss sich also selbst vor Angriffen schützen, aber sollte aus Eigeninteresse auch darauf vertrauen, dass sich der Zahlungsdienstleister an gewisse Standards hält, um die Uber-Kundendaten sicher verarbeiten zu können.

Zuletzt soll noch ein kurzer Blick auf die Kritischen Infrastrukturen (KRITIS) erfolgen. Laut der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI Gesetz müssen diese Art von Unternehmen „angemessene Vorkehrungen zur Vermeidung von Störungen [...] ihrer informationstechnischen Systeme, Komponenten und Prozesse“ treffen und nach dem „Stand der Technik“ umsetzen. Gegenüber dem BSI ist dies nachzuweisen. Für die unterschiedlichen Branchen wie Energie, Wasser, Ernährung und Gesundheit gibt es jeweils noch branchenspezifische Sicherheitsstandards (B3S). Im Sektor IT und Telekommunikationssicherheit werden sowohl Phishing als auch Social Engineering lediglich im Anhang A – Bedrohungskategorien aufgeführt [49].

5. Fallbeispiele

Fallbeispiele zeigen Szenarien aus der Realität, die es ermöglichen Situationen und Angriffe genauer zu betrachten, um daraus Handlungsempfehlungen abzuleiten. Deshalb sollen in diesem Kapitel zwei Fallbeispiele von erfolgreichen Phishing Angriffen auf die US-Großkonzerne Twitter und Uber analysiert werden. Es wird auf die Vorgehensweise der Angreifer sowie auf die damaligen Sicherheitsmaßnahmen eingegangen. Im Folgenden soll eine Bewertung im Kontext der Schutzmaßnahmen erfolgen, welche bereits in Kapitel 4 untersucht wurden. Dabei soll untersucht werden, ob z.B. die vom BSI empfohlenen Maßnahmen die Phishing Angriffe hätten verhindern oder vorbeugen können. Im Anschluss sollen weitere, verbesserte Maßnahmen für einen höheren Unternehmensschutz vorgestellt werden. Zuletzt soll ein, in der Literatur, bisher noch sehr seltenes Phänomen beschrieben werden, was als Framing oder auch Blame Game bezeichnet wird.

5.1 Twitter-Bitcoin Scam

Am 15. Juli 2020, um vier Uhr an der US-Ostküste, erschienen auf der Plattform Twitter mysteriöse Tweets von ungefähr 130 Personen, darunter waren insbesondere prominente und reichweitenstarke Accounts. Vertreten waren unter anderem Barack Obama, Kanye West, Bill Gates und Elon Musk. Das verlockende Angebot an die Follower war eine Verdoppelung ihrer Bitcoins. So lauteten die meisten der Tweets „Du sendest $1,000 und ich sende $2,000 zurück!“ [45]. Der Hauptakteur war zum Tatzeitpunkt gerade einmal 17 Jahre alt [53]. Mit seinen zwei Komplizen führte er einen der größten Social Engineering Angriffe der heutigen Zeit durch. Die drei Hauptakteure konnten jedoch von der Polizei leicht ausfindig gemacht werden, da sie auf sämtliche OPSEC (Operational Security) Maßnahmen verzichtet haben. Auch mit einem Schaden von ca. 100.000 Dollar kam Twitter damit recht glimpflich davon. Besonders Accounts wie die von Joe Biden oder auch Warren Buffet hätten mit diplomatischen Krisen oder Aktiencrashs deutlich mehr Schaden anrichten können [11].

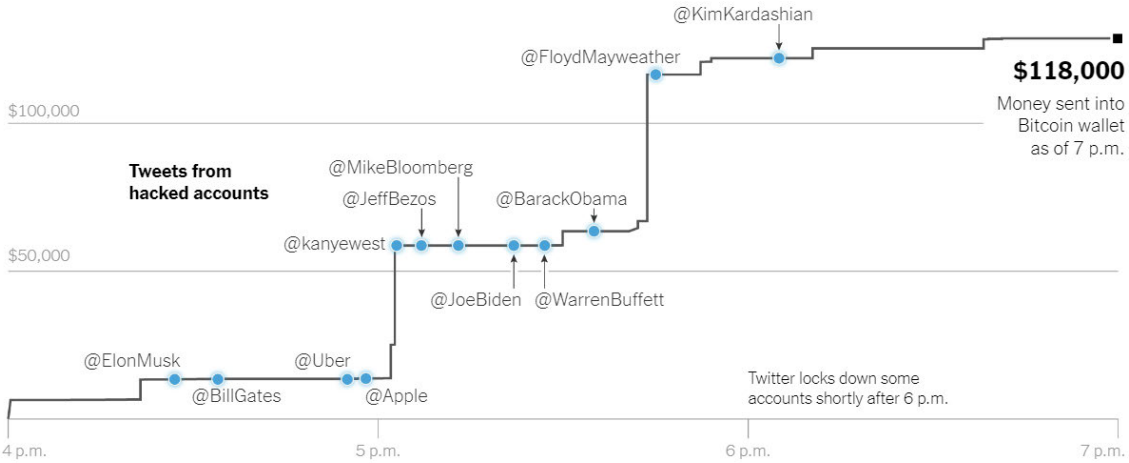

Abbildung 9: Tweets von gehackten Accounts [45]

5.1.1 Vorgehen der Akteure

Das generelle Vorgehen wird von Experten als „effektiv, aber amateurhaft“ beschrieben. Damit konnten auch die ersten Vermutungen, es handele sich um einen Staat wie Nordkorea oder Russland schnell beiseite geräumt werden [45]. Schließlich konnten drei Hauptakteure Graham Ivan Clark (17 Jahre), Mason Sheppard und Nima Fazeli als Angreifer identifiziert werden. Gemeinsam nutzten sie kostenpflichtige Tools, um bei LinkedIn nach Kontaktinformationen von Twitter-Mitarbeitern zu suchen. Im Fokus standen dabei Mitarbeiter, die über höhere administrative Rechte verfügten. Im Anschluss wurden Web-Logins erstellt, die denen von Twitter-VPN-Anmeldungen nachempfunden waren und damit dann als gefälschte VPN-Logins dienten. Durch die pandemische Lage befanden sich viele Mitarbeiter zu diesem Zeitpunkt im Homeoffice [11].

Bekannt ist, dass die Hacker eine Reihe von Social Engineering Angriffen gegen Twitter-Mitarbeiter durchgeführt haben die Zugang zu den internen Verwaltungstools hatten. Mit diesem Zugang können Twitter Konten wiederhergestellt oder zurückgesetzt werden. Per Anruf nahmen die drei Angreifer selbst Kontakt mit den ausgewählten Mitarbeitern auf und gaben sich als interner Twitter-Supportdienst aus, der aufgrund eines E-Mail Ausfalls eine nicht standardmäßige Authentifizierung verwendet [52]. Damit überzeugten sie die Opfer ihre Anmeldedaten inklusive zwei-Faktor Authentifizierung auf der Fake Login-Seite einzugeben. Ab diesem Moment konnten sich die Hacker mit den Zugangsdaten auf der echten VPN-Seite einloggen. Über diesen Weg konnten die Angreifer in das interne Netz von Twitter eindringen und sich eigene Konten erstellen. Die Konten hatten weitreichende Berechtigungen und Zugriff auf interne Tools [11].

Diese wiederum ermöglichten es, die E-Mail Adressen von Nutzern zurückzusetzen und somit die Kontrolle über diese Accounts zu erhalten. Der Bitcoin-Scam musste nur noch ausgeführt werden [11].

Bereits zwei Wochen nach dem Angriff konnten Graham C. und seine beiden Komplizen durch IP-Adressen, Bitcoin Konten und einer belastenden Aussage überführt werden [53]. Wie aus den Gerichtsdokumenten hervorgeht, haben sie keinerlei OPSEC wie VPNs, Proxys oder kompromittierte Systeme angewendet. Zusätzlich wurden genau am selben Tag im Forum „OGusers“ gehackte Twitter Accounts zum Verkauf angeboten. Da die Seite wohl häufiger gehackt wird, hat die Polizei auf einen solchen Leak zurückgegriffen, um den gesamten Chatverlauf der Twitter-Account Anbieter zu lesen. Einer der Angreifer hatte dort seine private E-Mail Adresse mit Vor- und Nachnamen zur Anmeldung genutzt. Als die Ermittler der Spur des Geldes folgten, stellten sie fest, dass ebendiese Bitcoin Adressen auch bei Coinbase verwendet wurden. Durch eine Anfrage an die Krypto-Handelsplattform konnten die Daten des Besitzers des Wallets ermittelt werden, denn dieser nutzte keine Fake-Identität für die Registrierung [11].

Dadurch konnte bewiesen werden, dass die Angeklagten für die Taten verantwortlich sind. Ein Geständnis durch Clark vor Gericht bestätigte dies. Er akzeptierte eine Verurteilung zu drei Jahren Jugendhaft [53].

5.1.2 Twitters Sicherheitsmaßnahmen

Laut Bloomberg [10] soll Twitter von dem Potenzial eines internen Angriffs sowie weiteren Sicherheitslücken bereits seit 2015 gewusst haben. Schon seit mehreren Jahren gabt es Probleme mit der wachsenden Zahl von Mitarbeitern, die Konten von Nutzern zurücksetzen und Sicherheitseinstellungen außer Kraft setzen können. Der Chief Executive Officer Jack Dorsey und der Vorstand wurden daraufhin mehrfach gewarnt, aber aufgrund von umsatzsteigernden Initiativen hat man sich gegen eine Änderung entschieden.

Peiter „Mudge“ Zatko ist der ehemalige Leiter der Sicherheitsabteilung von Twitter, welcher als Whistleblower eine circa 80-seitige Beschwerde an die amerikanische Börsenaufsicht Securities Exchange Commission, die Wettbewerbsbehörde Federal Trade Commission und das Justizministerium schrieb [38]. Darin kritisiert er, dass rund 10.000 Twitter Mitarbeiter Zugriff auf schützenswerte Personendaten haben, was Hacks vereinfachen würde. Weiterhin sind wohl auch nach Kontoschließungen Nutzerdaten nicht gelöscht wurden, obwohl die Nutzer davon ausgingen.

Ebenfalls soll Twitter nach Zatkos Aussagen Elon Musk (Gründer von Tesla und SpaceX) in Bezug auf Bot-Accounts angelogen haben. Von Twitters Seite wurde stets behauptet, dass die Anzahl bei unter 5% liege, in Wirklichkeit sollen es jedoch um die 20% sein [37].

Einer der kritischsten Sicherheitsmängel ist jedoch die Tatsache, dass ein unzureichendes PAM (Privileged Account Management) dazu führte. Diese Schwachstelle ermöglichte es, dass der missbräuchliche Zugriff auf das interne Twitter Tool, das für die Zurücksetzung und Verwaltung von Twitter-Konten verwendet wird, für eine recht lange Zeit unbemerkt erfolgen konnte [52].

5.2 Uber

Am 15. September 2022 wurde der Fahrdienstleister Uber gehackt. Bis heute ist nicht endgültig geklärt, ob dieser Angriff von einem Einzeltäter oder einer Gruppe ausging. Es wird vermutet, dass es sich dabei um einen erst 18-jährigen Teenager handelt, der vermutlich mit der Gruppe „Lapsus$“ in Verbindung steht. Einen finanziellen Schaden hat das Unternehmen wohl nicht erlitten, da es dem Täter lediglich um Aufmerksamkeit ging. Die Schädigung des Ansehens der Firma Uber bleibt jedoch. Zumindest konnten einige Tage nach dem Vorfall die Fahrdienste wieder ohne Einschränkungen in Betrieb genommen werden [12].

5.2.1 Vorgehen der Akteure

Das Konto eines Vertragspartners wurde kompromittiert, indem das Gerät mit Malware infiziert wurde. Dabei wurden vermutlich die Anmeldedaten offengelegt. Der Angreifer konnte dann das Unternehmenspasswort von Uber im Darknet käuflich erwerben [13]. Im Anschluss daran versuchte sich der Angreifer immer und immer wieder in dem Konto anzumelden. Durch die Zwei-Faktor Authentifizierung war die Anmeldung zunächst blockiert. Der Vertragspartner bekam dadurch aber immer wieder neue Push-Benachrichtigungen [14]. Nach eigenen Aussagen des Täters hat er das Opfer kontaktiert und sich selbst als Uber Mitarbeiter ausgegeben, um ihn so zur Bestätigung der Push-Benachrichtigung zu überreden [12]. Damit erlangte der Angreifer einen VPN-Zugang zum Intranet von Uber. Das Nutzerkonto hatte zwar keine administrativen Privilegien aber war ausreichend, um das interne Netz zu scannen. Dadurch fand er ein ungeschütztes Netzlaufwerk, auf dem ein Powershell-Skript gespeichert war. In diesem wiederum befand sich unter anderem auch das Passwort eines Super-Administrators im Klartext. Der Angreifer hatte damit praktisch den vollen administrativen Zugang auf sowohl interne als auch externe IT Systeme wie z.B. Gsuite. Insbesondere durch Gsuite erhielt er den vollen Zugriff auf das Identity Management und das Single Sign-On System, was bedeutet, dass sich potenziell alle Nutzerkonten in seiner Gewalt befanden [14]. Des Weiteren habe sich der Angreifer administrativen Zugriff auf Dienste wie Amazon-Web-Services und Google-Cloud verschafft. Er selbst behauptet, Uber vollständig kompromittiert zu haben und veröffentlichte davon auch Screenshots [42].

5.2.2 Ubers Sicherheitsmaßnahmen

Eine Kombination aus Zero Trust und Multi-Faktor-Authentifizierung galt in der Sicherheitsbranche lange Zeit als Versprechen für totale Sicherheit. Doch auch dieser Ansatz hat Lücken wie der Fall von Uber zeigt. Durch Techniken des Social Engineerings konnte der Täter in die Systeme eindringen [42].

Aus dem beschriebenen Angriffsablauf lässt sich schließen, dass Uber wahrscheinlich eine klassische Sicherheitsarchitektur verwendet hat. Das Intranet dient dem Schutz vor externen Zugriffen aus dem Internet. Zugriff auf das Intranet von außen ist nur über einen VPN-Zugang möglich, was auf eine erste Sicherheitsvorkehrung hinweist. Den Nutzern im Intranet wird in der Regel vertraut [14]. Trotzdem muss an diesem Punkt noch einmal deutlich hervorgehoben werden, dass Passwörter für die wichtigsten internen Vorgänge im Klartext gespeichert wurden, sodass jeder der in das Skript geschaut hat, diese lesen konnte. Ein solches Vorgehen ist definitiv als Fehlverhalten des Unternehmens zu beurteilen. In diesem Fall aber scheint es so, als ob ungewöhnliches Verhalten und Zugriffe im Intranet nicht ausreichend überwacht wurden. Das interne Monitoring zeigt hier offensichtlich eine Schwachstelle in der Sicherheitsstrategie von Uber [14]. Ein weiterer Punkt der auf eine Schwachstelle hindeutet, sind die hochprivilegierten Anmeldeinformationen auf Netzwerkdateifreigaben die dazu führten, dass der Täter auf alles zugreifen konnte. Sowohl die Produktionssysteme, die Slackverwaltungsoberfläche als auch die EDR (Endpoint-Detection und Response) -Konsole waren betroffen [42].

5.3 Bewertung im Kontext der Schutzmaßnahmen

Anhand der beiden Fallbeispiele sollen die, in Kapitel 4 vorgestellten, Schutzmaßnahmen bewertet werden. Schutzmaßnahmen dienen dazu, potenzielle Risiken und Schäden bestmöglich zu vermeiden. Doch um sicherzustellen, dass diese Maßnahmen auch effektiv sind, müssen sie stetig verbessert werden. Der Ablauf und die Vorgehensweise wurde jeweils schon analysiert, doch was hätten die technischen Schutzmaßnahmen, die Sensibilisierung von Mitarbeitern, ein Incident Response Plan oder die Leitfäden des BSI in diesen beiden Fällen bewirkt? Wurden vielleicht zu wenige Schutzmaßnahmen vorgenommen oder gar die Falschen?

Angefangen damit, dass bei vielen Menschen Phishing als erstes mit gefälschten E-Mails verbunden wird. Doch sowohl im Twitter als auch im Uber Fall waren es keine klassischen Phishing E-Mails, die versucht haben Daten abzufischen. Es gab also keine Möglichkeit wie in Abbildung vier [46] empfohlen, den Absender zu verifizieren, es gab keine Aufforderung sensible Daten einzugeben, es gab ebenfalls keinen dringenden Handlungsbedarf oder Links zu gefälschten Webseiten und auch gab es keine sprachlichen Ungenauigkeiten. Weiterhin gab es auch keine dubiösen Anhänge in einer bereits verdächtig erscheinenden E-Mail, die Schadsoftware enthalten könnte wie z.B. bei .exe oder .scr [19]. All diese Merkmale zur Erkennung einer Phishing E-Mail waren in beiden Fällen zwecklos, da der Angriffsvektor keine E-Mail war. Ohne E-Mail kann logischerweise auch eine Filterung ihr Potenzial nicht entfalten und spielt beim Schutz vor Phishing zumindest in diesen beiden Fällen keine Rolle.

Für Malware ist Phishing eins der am häufigsten genutzten Einfallstore [9]. Daher steht es außer Frage, dass jedes Unternehmen eine Anti-Malware Software nutzen sollte, um nach einem erfolgreichen Phishing Angriff weitreichende Schäden durch Malware zu vermeiden. Diese hätte jedoch in beiden Fällen den Verlauf des Angriffs nicht verändert, da die beiden Unternehmen nicht mit einer Schadsoftware wie z.B. Ransomware angegriffen wurden. Die dahingehende Empfehlung des BSI, stets auf eine aktuelle Antivirus Software zu achten, hätte zumindest Twitter und Uber nicht vor einem Phishing Angriff schützen können.

Weiterhin empfiehlt unter anderem das BSI [19] die Zwei-Faktor-Authentifizierung, da somit kein Zugriff auf Daten möglich ist, falls doch mal ein Passwort abgefischt wurde. Im Twitter Fall gaben sich die Angreifer jedoch per Telefon selbst als Twitter-Supportdienst aus, der aufgrund eines E-Mail Ausfalls eine nicht standardmäßige Authentifizierung nutzt [52]. Die Mitarbeiter gaben daher aus Überzeugung ihre Anmeldedaten auf einer Fake Login- Seite ein.

Durch die Information, dass sogar der vermeintlich eigene IT-Dienst einen anderen, nicht üblichen Login nutzte, wurde diesem aus Hierarchie-Gründen auch geglaubt. Rein theoretisch betrachtet, rechnet wahrscheinlich auch niemand damit, dass eine wichtige Information von der IT-Abteilung unglaubwürdig ist oder gar einen Angriff darstellt. Aus diesem Grund würden die meisten Mitarbeiter wohl eine solche Information nicht in Frage stellen oder anzweifeln. Im Gegensatz dazu wurde im Uber Fall ein Mitarbeiter mit MFA Push-Benachrichtigungen nahezu überhäuft [14]. Daraufhin hat sich hier ebenfalls ein Angreifer bei dem betroffenen Mitarbeiter gemeldet und sich selbst als Uber Mitarbeiter ausgegeben, um ihn zu überreden die Push-Benachrichtigungen zu bestätigen, da diese sonst nie aufhören würden [12]. In diesem Fall kann man ganz klar sagen, dass Menschen Fehler machen. Insbesondere wenn sie unter Druck stehen, ist es möglich, dass sie eine Zwei-Faktor-Authentifizierung bestätigen, ohne diese vielleicht genau überprüft zu haben. Doch auch wenn dieser Umstand im Uber Fall als erfolgreiches Einfallstor fungierte, sollte es nicht üblich sein, dass Angreifer im Anschluss das ganze System ohne weitere Sicherheitshürden kompromittieren können. Besonders inakzeptabel ist die Tatsache, dass Superadministratoren-Passwörter irgendwo in einem ungeschützten Netzlaufwerk im Klartext gespeichert werden [14].

Im Twitter Fall diente eine gefälschte VPN-Login Webseite als Einfallstor. Um diesem Vorgehen vorzubeugen, sollte man laut BSI immer die Adressleiste im Browser überprüfen und niemals Daten auf Webseiten mit einer unverschlüsselten Verbindung eingeben [46]. Schreibfehler in der Adressleiste sind ebenfalls möglich. Die Mitarbeiter wurden jedoch vom vermeintlich eigenen Twitter-Supportdienst darauf hingewiesen, dass sie eine andere Webseite für den Login nutzen können, die nicht standardmäßig ist. Dahingehend ist es nachvollziehbar, dass auf der Fake-Login Seite kleine Unterschiede zur eigentlichen Originalseite nicht zur Kenntnis genommen wurden. Oder vielleicht sind sie den Mitarbeitern auch aufgefallen aber im Hinterkopf war ihnen bewusst, dass eine nicht standardmäßige Webseite vielleicht anders aussehen kann.

An dieser Stelle kommt das Thema Kommunikation ins Spiel. Diese ist gerade bei Phishing äußerst wichtig, wird aber sehr oft vernachlässigt. Es ist wichtig, dass Mitarbeiter insofern sensibilisiert sind, dass sie ungewöhnliche E-Mails, Aufforderungen oder Anrufe an die IT-Abteilung zur Überprüfung weitergeben. Doch dafür muss in einem Unternehmen eine flache Hierarchie herrschen und eine offene Kommunikation möglich sein. Die Basis liegt aber auf dem Vertrauen. Wenn ungewöhnliche Vorfälle gemeldet werden sollen, müssen die Mitarbeiter wissen, dass sie im Falle eines Fehlers nicht bloßgestellt werden. Ein solches blamieren würde nur die Angst und Unsicherheit fördern.

Im nachfolgenden Kapitel werden weitere Schutzmaßnahmen aufgegriffen. Sowohl Monitoring als auch Prozesse und Berechtigungen prüfen, hätten im Twitter und Uber Fall das Ausmaß eines Phishing Angriffs eindämmen können. Warum diese Maßnahmen so wichtig sind, wird im Folgenden erklärt.

Bei Uber konnte der Angreifer, nachdem er in das interne Netz eingedrungen ist, ohne administrative Privilegien das komplette Netz scannen [14]. Dabei ist dieser Vorgang in der IT-Abteilung anscheinend niemandem aufgefallen und der Angriff konnte nicht frühzeitig gestoppt werden.

Darüber hinaus hat dieses unzureichende Monitoring zur Folge, dass der Angreifer administrativen Zugriff auf interne und externe IT-Systeme erlangte und somit das gesamte System kompromittiert wurde [42]. Twitter hatte bei weitem kein besseres Monitoring. Der Unterschied ist nur, dass sie über ihr schlechtes Monitoring bereits informiert waren. Bei einem so großen Konzern mit so vielen Nutzern würde man meinen, dass sie diese Sicherheitslücke schnell behoben haben. Doch weit gefehlt. Im Zeitraum von 2015 bis 2020 lief der Twitter Betrieb ganz normal weiter, obwohl der Vorstand über das Potenzial eines internen Angriffs Bescheid wusste [10]. Es gab also über einen sehr langen Zeitraum das Bewusstsein, dass es IT-Fehler gibt und auch der Whistle Blower „Mudge“ bestätigte, dass die internen Prozesse mehr geprüft werden müssen. Denn es gab zu viele Mitarbeiter mit Low Level Admin Rechten, die Zugriff auf personenbezogene Daten hatten und ebenfalls die Berechtigung, Twitter-Konten zurückzusetzen [37]. Dadurch war es den Angreifern überhaupt erst möglich, die prominenten Accounts zu kompromittieren und die Betrugsmasche zu veröffentlichen.

5.4 Best Practices zur Abwehr von Phishing Angriffen

Nachdem bereits verschiedene Schutzmaßnahmen genauer betrachtet und mit zwei realen Fallbeispielen gezeigt wurde, dass diese nicht immer zum gewünschten Erfolg führen, sollen in diesem Kapitel weitere sogenannte „Best Practices“ für die Abwehr von Phishing Angriffen vorgestellt werden. Dabei handelt es sich um bewährte Methoden und Verfahren die sich bereits als erfolgreich und effektiv erwiesen haben. Anhand der Betrachtung der Fallbeispiele ist jedoch aufgefallen, dass insbesondere diese Methoden entweder nicht eingesetzt wurden oder nicht optimal funktioniert haben. Ebenfalls konnte festgestellt werden, dass die Schutzmaßnahmen aus Kapitel 4 allein nicht ausreichten, um die beiden Unternehmen Twitter und Uber vor einem Angriff zu schützen.

5.4.1 Monitoring

Beim Monitoring werden Systeme, Prozesse und Aktivitäten überprüft, um Probleme in einem Netzwerk frühzeitig zu erkennen. Neben den präventiven Schutzmaßnahmen ist es besonders wichtig auch detektive Maßnahmen, die zur Entdeckung eines Angriffs beitragen, zu besitzen. Der frühzeitigen Erkennung fällt eine besonders hohe Bedeutung zu, denn je schneller ein Angriff erkannt wird, desto schneller [59]:

- kann der Angriff analysiert und die ausgenutzte Schwachstelle geschlossen werden
- können Gegenmaßnahmen eingeleitet und die Fortführung des Angriffs unterbunden werden
- kann der entstandene Schaden eingegrenzt oder behoben werden

Dafür kann unter anderem ein Intrusion Detection System (IDS) verwendet werden. Dieses überwacht, ob ein System oder Netzwerk Anomalien besitzt und vom Normalzustand abweicht [59]. Sobald ein Angriff erkannt wird, wird die Sicherheitsadministration benachrichtigt und Gegenmaßnahmen eingeleitet. Der Angriff wird protokolliert und es erfolgt gegebenenfalls eine Meldung bei den Sicherheitsbehörden. Im Extremfall kann es so weit kommen, dass alle Verbindungen getrennt werden und das System heruntergefahren werden muss [64].

Besonders der Fall von Uber zeigt, wie wichtig das Monitoring ist. Denn die Angreifer konnten in das System eindringen und selbst das Netz scannen. Dieses Verhaltensmuster im Intranet ist anscheinend nicht weiter aufgefallen [14].

Bei einem guten Monitoring des eigenen Systems hätten diese und weitere Aktivitäten auffallen müssen. So hätte man den Angriff deutlich besser und vor allem frühzeitiger abwenden können, trotz dem Einfallstor Phishing bzw. Social Engineering.

5.4.2 Hardware Token

In Bezug auf die Multi-Faktor und Zwei-Faktor Authentifizierung mittels Push-Benachrichtigungen oder auch SMS lässt sich sagen, dass diese bei weitem keine 100%-ige Garantie mehr für eine sichere Authentifizierung darstellt. Um Phishing entgegenzuwirken, sollte ein zweiter Faktor aus einem speziellen Hardware-Token bestehen [14]. Hardware Token können in unterschiedlichen Bauformen verfügbar sein wie z.B. USB, SD oder Mikro SD [56]. Sie sind zwar teurer als Push-Benachrichtigungen, aber im Gegenzug auch deutlich sicherer [14].

In Verbindung mit einem Hardware Token wird meist das Challenge Response Verfahren genutzt. Dabei handelt es sich um ein Sicherheitsprotokoll zur Authentifizierung von Benutzern. Es wird eine Challenge (Herausforderung) an den Nutzer gesendet, welche dieser mit einer bestimmten Antwort beantworten (Response) muss, um seine Identität zu bestätigen. Nur dann wird ihm der Zugang gewährt [14]. Ein Beispiel dafür ist ein One-Time-Passwort. Dabei wird von dem Hardware Token ein Passwort generiert, welches nur eine sehr kurze Gültigkeit besitzt. Dieses Passwort bildet somit dann als Besitzfaktor den zweiten Faktor der Authentifizierung [55]. Um sich also authentifizieren zu können, müssen der richtige Benutzername mit dem zugehörigen Passwort eingegeben werden und in Verbindung mit der korrekten Signatur des Hardware Tokens im Challenge-Response Verfahren vorliegen [56].

Ein Vorteil dieser Variante der Multi-Faktor Authentifizierung ist es, dass allein durch den Besitz von Benutzername und Passwort ein Phishing Angriff nicht zum Erfolg führen kann, da der Angreifer nicht im Besitz des Hardware Tokens ist [56]. Einer der größten Nachteile ist jedoch der Fakt, dass diese Methode nicht vor sogenannten „Man-in-the-middle“ Angriffen schützt [14]. Das Ziel bei einem „Man-in-the-middle“ Angriff ist es, sich unbemerkt in die Kommunikation zwischen mehreren Parteien einzuschleichen und diese beispielsweise zu manipulieren [70]. Der Angreifer gibt sich also als „Mann in der Mitte“ abwechselnd als Sender und Empfänger aus. Aus diesem Grund ist es sinnvoll, die Gültigkeit der Challenges auf einen kurzen Zeitraum zu beschränken [14].

5.4.3 Berechtigungen prüfen

Moderne Netzwerke verfügen über den Zugriff auf verschiedenste Ressourcen wie Anwendungen oder Dateien. Bei der Verwaltung von Ressourcen stehen dabei Authentifikation und Autorisation im Vordergrund [59]. Die Überprüfung von Berechtigungen ist dabei ein wesentlicher Aspekt in der Netzwerksicherheit.

In einem internen IT-System muss also ein Berechtigungskonzept implementiert sein. Mit diesem lässt sich festhalten, welcher Benutzer was darf und auf was er Zugriff erhält. Voraussetzung dafür ist, das System muss die einzelnen Benutzer authentifizieren können. Dies erfordert wiederum für jeden Benutzer einen eigenen Account [59].

Im Fall von Twitter hat selbst der ehemalige Sicherheitschef bestätigt, wie fahrlässig es ist, wenn 10.000 Mitarbeiter Zugriff auf hochsensible Daten haben [37]. Dadurch hatten zu viele Accounts die Berechtigung und Möglichkeit Twitter-Konten zurückzusetzen. Das schlechte Privileged Account Management führte außerdem dazu, dass dieses Tool zum Zurücksetzen viel zu lang unentdeckt blieb [52].

5.4.4 Managementebene

Wenn man die stetige Weiterentwicklung und Aggressivität von Phishing Angriffen in den letzten Jahren beobachtet hat, wird klar mit welchen Herausforderungen das Management eines Unternehmens konfrontiert wird. Es muss stets auf neue Angriffstrends reagieren, die technischen Sicherheitsmaßnahmen müssen immer auf dem aktuellen Stand sein und die Mitarbeiter müssen geschult werden. Cyberangriffe stellen jedoch nicht nur ein technisches Problem dar, sondern beinhalten auch viele nichttechnische Aspekte. Aus diesem Grund sollten auch die Schutzmaßnahmen sowohl technische als auch nichttechnische Mittel enthalten [65]. In dieser Arbeit wurden bereits einige technische Schutzmaßnahmen näher betrachtet, aber auch die Sensibilisierung von Mitarbeitern näher erläutert. Doch eine meist unbeachtete Verbesserungsmöglichkeit im Kampf gegen Phishing Angriffe liegt in der Managementebene.

Vor dem Hintergrund dieser Arbeit wird sogar klar, dass Cybersicherheit hauptsächlich in der Management-Verantwortung liegt und deshalb auf der obersten Führungsebene behandelt werden muss [65]. In der Literatur [5] liest man häufig davon, wie wichtig es ist die Mitarbeiter zu sensibilisieren, aber ein Abwälzen der Problematik auf diese ist nicht unbedingt zielführend. Es reicht also dementsprechend nicht aus, zu denken, wenn die Mitarbeiter geschult sind, kann dem Unternehmen nichts mehr passieren. Ebenfalls reicht es nicht, die Cyberproblematik an die IT-Abteilung zu delegieren [65].

Besonders kleine und mittelständische Unternehmen haben vielleicht nicht immer die Mittel für eine schlagkräftige IT-Sicherheit. Deshalb sollten flache Hierarchien und Kommunikation immer an erster Stelle stehen. Dafür ist es essenziell, dass spezifisches Wissen auch in der Managementebene vorhanden ist, um Fehlentscheidungen vorzubeugen [66]. Oftmals fehlt es den Managern oder Geschäftsführern selbst an Affinität für das Thema. Deshalb sollten Geschäftsführer oder Manager den Umgang und die Relevanz des Themas Cyber-Security vorleben [66]. Dann könnten sich auch Mitarbeiter ein Beispiel daran nehmen und werden inspiriert, das Thema mit einer gewissen Ernsthaftigkeit zu behandeln. Außerdem haben die Mitarbeiter oft selbst keinen Einfluss darauf, wie im Fall von Twitter, die Privilegien von Accounts zu ändern. Da das Management was sowohl Prozesse als auch Entscheidungshoheit angeht, die höchste Instanz ist, kann auch nur die Leitungsebene die richtigen Weichen für gute IT-Sicherheit stellen. Damit ist Awareness auch auf dieser Ebene von größter Bedeutung.

5.5 Framing

„Blame Designers, Not Users“ [50]. Dieser Satz bedeutet so viel wie „Beschuldige die Entwickler und nicht die Nutzer“ und sollte in Unternehmen auf der Managementebene deutlich mehr beherzigt werden. Beim sogenannten Framing (deutsch: Einrahmung) oder Blame Game (deutsch: Blamier Spiel) wird versucht, die Verantwortung für Fehler auf eine andere Person zu übertragen, um sich von der eigenen Schuld zu befreien. In diesem Kapitel bezieht sich das Blame Game nur auf den beruflichen Kontext zwischen Management und Mitarbeitern.

Immer häufiger kommt es bei erfolgreichen Phishing Angriffen zu Situationen, in denen die komplette Schuld auf einen oder mehrere Mitarbeiter abgewälzt wird. Gern wird dann ausgenutzt, dass viele Mitarbeiter vielleicht nicht das beste technische Verständnis der IT-Sicherheit haben. In den sieben Todsünden des Cyber Crisis Managements findet sich unter Punkt vier das „öffentliche Blame Game“. In Krisensituationen kommt es schnell zu Schuldzuweisungen, was als Unternehmen jedoch sehr unsouverän wirkt. Besonders öffentliche Schlammschlachten sind tabu, denn Kunden wollen eine Lösung vom Unternehmen und keinen Sündenbock [51].

Im Fall des Uber Hacks wurde in einer Pressemitteilung öffentlich erwähnt, dass es sich bei dem kompromittierten Account, um den eines EXT-Vertragspartners handelt [13]. Der Fokus lag also von Beginn an auf dem Mitarbeiter. Es wird so dargestellt, als wäre der Angriff nur deshalb erfolgreich gewesen, weil der Mitarbeiter die Multi-Faktor-Authentifizierung bestätigt hat [13]. In der Mitteilung hingegen nicht erwähnt wurde, dass die Manager die Passwörter im Klartext in einem Skript gespeichert hatten und somit das gesamte System kompromittiert werden konnte [42]. Es gibt also keinerlei Schuldeingeständnis seitens der Managementebene.

Die Konsequenzen von einem Bloßstellen, vielleicht sogar in der Öffentlichkeit, können fatale Folgen haben. Neben einer negativen Auswirkung auf die Zusammenarbeit wird auch das Vertrauen der beteiligten Parteien massiv beschädigt. Es folgt die Unsicherheit der Mitarbeiter, die in Zukunft bei einer dubiosen E-Mail bestimmt nicht freiwillig nochmal extra beim Manager nachfragen.

6. Fazit und Ausblick

Beide Unternehmen Twitter und Uber haben zum damaligen Zeitpunkt der jeweiligen Phishing Angriffe die gängigen Schutzmaßnahmen verwendet, sowohl technische Maßnahmen als auch die Sensibilisierung von Mitarbeitern. Es konnte jedoch nach der Analysierung der Fallbeispiele festgestellt werden, dass die gängigen Schutzmaßnahmen und das Einhalten der Leitfäden nicht ausgereicht haben, um die Unternehmen vor einem erfolgreichen Phishing Angriff zu schützen. Entweder konnten die Sicherheitsmaßnahmen mit der Hilfe von Social Engineering umgangen werden oder aber Empfehlungen konnten in diesen Fällen nicht angewandt werden, da die Angriffsvektoren andere waren. Weiterhin kann gesagt werden, dass der Mensch zwar ein Schlüsselfaktor zum Eindringen in ein System sein kann, jedoch ist dies meist nur das Einfallstor und nicht die Grundlage für unverschlüsselte Netzwerke oder schlechte Prozesse. Es ist aufgefallen, dass der Faktor Mensch in der Literatur sehr häufig als schwächstes Glied bezeichnet wird und man Phishingschutz auf der Schulung von Mitarbeitern aufbauen sollte. Viel zu selten wird auch die Managementebene für unzureichende Maßnahmen oder Schuldzuweisungen in die Kritik genommen. Es kann sich eben nicht ausschließlich auf das Können der Mitarbeiter in Ausnahmesituationen verlassen werden, sondern in die eigene IT sollte ebenfalls investiert werden, sodass diese im Notfall auch funktionstüchtig ist. Die vorgestellten Best Practices sind hauptsächlich auf die beiden Fallbeispiele bezogene Empfehlungen, um die vorhandenen Systeme weiter zu verbessern. Doch auch das Bewusstsein über bestehende IT-Fehler und ein Umdenken in der Managementebene sollen damit gefördert werden. Ein wichtiger Punkt, der immer wieder vernachlässigt wird, ist die Kommunikation. Diese muss von den Managern vorgelebt werden, denn nur bei einer flachen Hierarchie werden Mitarbeiter dubiose Vorfälle melden oder bei Unklarheit nachfragen. Werden sie stattdessen blamiert, führt dies zu Unsicherheit und bewirkt eher das Gegenteil von dem, was bei einer guten Anti-Phishing Strategie benötigt wird.

Phishing hat sich in den letzten Jahren stark gewandelt. Wer immer noch glaubt Phishing bestehe nur aus unseriösen E-Mails, die leicht zu erkennen sind, liegt falsch. Sowohl der Modus Operandi als auch die Professionalität haben zugenommen. Es werden nicht mehr nur wahllos Angriffe ohne konkretes Ziel ausgeführt, sondern es werden spezifisch Mitarbeiter mit administrativen Zugängen oder zahlungsstarke Unternehmen angegriffen.

In der Zukunft werden sowohl die kritischen Infrastrukturen als auch Kryptowährungsunternehmen im Fokus von Phishing Angriffen stehen.

Es bleibt offen abzuwarten, welche neuen Methoden sich Kriminelle ausdenken, um weiterhin an sensible Daten zu gelangen oder Unternehmen mit Schadsoftware erpressen zu können. Ob die vorgestellten erweiterten Maßnahmen jedoch vollkommen ausreichen, um vor zukünftigen Phishing Angriffen zu schützen bleibt abzuwarten. Realistisch gesehen wird es durch die andauernde rasante Weiterentwicklung neuer Methoden wohl nie einen einhundertprozentigen Schutz gegen Phishing geben.

Literatur

[1] Bitkom, 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen. Zugriff: 27.02.2023 https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

[2] Bundeskriminalamt, Bundeslagebild 2021. Cybercrime Bundeslagebild. Zugriff: 28.02.2023 https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html?nn=28110

[3] C. Stammer, Einblick in die Cybercrime am Beispiel des Phishing. Berlin, 2014. [Online] Zugriff: 05.02.2023 https://opus4.kobv.de/opus4-hwr/files/906/FB4_2014_Stammer.pdf

[4] N. Heinrich, Kompetenzentwicklung im Bereich „IT-Sicherheit durch Ethical-Hacking “. lernen lehren 2/2017, Heckner Druck- und Verlagsgesellschaft mbH & Co. KG. [Online] Zugriff: 07.03.2023 http://lernenundlehren.de/heft_dl/Heft_126.pdf#page=43

[5] A. Franz, A. Benlian, Spear Phishing 2.0: Wie automatisierte Angriffe Organisationen vor neue Herausforderungen stellen. HMD 57, 597–612 (2020). [Online] Zugriff: 09.03.2023 https://doi.org/10.1365/s40702-020-00613-y

[6] Symantec, Internet security threat report Bd. 24 (2019). https://docs.broadcom.com/doc/istr-24-2019-en

[7] Cloudmark, Survey reveals spear phishing as a top security concern to enterprises (2016). Zugriff: 09.03.2023 https://www.cloudmark.com/en/blog/survey-reveals-spear-phishing-top-security-concern-enterprises

[8] Bundeskriminalamt, Was ist Cybercrime? Zugriff: 09.03.2023 https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_neu.html

[9] E. Huber, Cybercrime. In: Cybercrime. Springer VS, Wiesbaden (2019). [Online] Zugriff: 09.03.2023 https://doi.org/10.1007/978-3-658-26150-4_3

[10] J. Robertson, K. Mehrotra, K. Wagner, Twitter's Security Woes Included Broad Access to User Accounts (2020). [Online] Zugriff: 13.3.2023 https://www.bloomberg.com/news/articles/2020-07-27/twitter-s-security-woes-included-broad-access-to-user-accounts#xj4y7vzkg

[11] Dr. M. Gschwender, When Elon doubled your Bitcoin - Cyberthrowback Twitter-Hack (2021). Zugriff: 13.03.2023 https://www.rootcat.de/blog/cyberthrowbac_twitter_hack_dez21/

[12] Reuters, Hacker dringen in Uber Systeme ein (2022). Zugriff: 21.03.2023 https://www.spiegel.de/netzwelt/apps/uber-hacker-dringt-in-systeme-des-fahrdiensts-ein-a-0134cf9f-7a9c-4da7-98c5-555d2728ae2e

[13] Uber Team, Security update (2022). Zugriff: 21.03.2023 https://www.uber.com/newsroom/security-update/

[14] H. Shulman, M. Waidner, Der Uber-Hack und was wir aus ihm lernen können, Tagesspiegel Background (2022). Zugriff: 21.03.2023 https://background.tagesspiegel.de/cybersecurity/der-uber-hack-und-was-wir-aus-ihm-lernen-koennen

[15] K. Plößl, H. Federrath, T. Nowey, Schutzmöglichkeiten gegen Phishing, Universität Regensburg, 161-164 (2005). [Online] Zugriff: 21.03.2023 https://epub.uni-regensburg.de/5158/1/Si2005PlFN2005Phishing.pdf

[16] V. Haupert, T. Müller, Auf dem Weg verTAN: Über die Sicherheit App-basierter TAN-Verfahren. In: M. Meier, D. Reinhardt, S. Wendzel (Hrsg.), Sicherheit 2016 – Sicherheit, Schutz und Zuverlässigkeit, 101-112, Gesellschaft für Informatik e.V., Bonn (2016). [Online] Zugriff: 21.03.2023 https://dl.gi.de/handle/20.500.12116/859

[17] H. Rügheimer, Zwei Faktoren für mehr Sicherheit. Schmerzmedizin 35, 53 (2019). [Online] Zugriff: 21.03.2023 https://link.springer.com/article/10.1007/s00940-019-1131-4#citeas

[18] BSI, Auftrag. Zugriff: 21.03.2023 https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html

[19] BSI, Phishing: Checkliste für den Ernstfall. Zugriff: 21.03.2023 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/BSI-ProPK-Checkliste-Phishing.pdf?__blob=publicationFile&v=1

[20] J. Jahnke, M. Weitz, F. Echterbruch, S. Saleh, Biometrische Authentifizierungsverfahren im Spannungsfeld von Sicherheit und Nutzerfreundlichkeit. HMD Praxis der Wirtschaftsinformatik, 1-15 (2023).

[21] A. M. Freed, Rise of Double-Extortion Shines Spotlight on Ransomware Prevention. Cybereason (2021). Zugriff: 22.03.2023 https://www.cybereason.com/blog/rise-of-double-extortion-shines-spotlight-on-ransomware-prevention

[22] Kaspersky, Over half of ransomware victims pay the ransom, but only a quarter see their full data returned (2021). Zugriff: 22.03.2023 https://www.kaspersky.com/about/press-releases/2021_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned

[23] H.Junker, IT-Sicherheit für Industrie 4.0 und IoT: Aktuelle Bedrohungslage und Herausforderungen der Smart Factory. Datenschutz und Datensicherheit-DuD 39/10, 647-651 (2015). [Online] Zugriff: 22.03.2023 https://link.springer.com/article/10.1007/s11623-015-0491-8

[24] K.R. Müller, G. Neidhöfer, Schutz- und Abwehrmaßnahmen. IT für Manager: Mit geschäftszentrierter IT zu Innovation, Transparenz und Effizienz, 127-146 (2008). [Online] Zugriff: 24.03.2023 https://link.springer.com/content/pdf/10.1007/978-3-8348-9487-8_11.pdf

[25] M. Ewald, Malware: Viren, Würmer und Trojaner. Hacking und Hackerabwehr, 21-35 (2007). [Online] Zugriff: 24.03.2023 http://www.tm.uni-karlsruhe.de/doc/tr/TM-2007-1.pdf#page=24

[26] D. Aebi, D. Aebi, Malware. Praxishandbuch Sicherer IT-Betrieb: Risiken erkennen Schwachstellen beseitigen IT-Infrastrukturen schützen, 109-142 (2004). [Online] Zugriff: 24.03.2023 https://link.springer.com/chapter/10.1007/978-3-322-90469-0_6

[27] M. Leicht, F. Möllers, Zur (Un-)Sicherheit von Zwei-Faktor-Authentifizierung via SMS. Datenschutz und Datensicherheit – DuD 45, 541-545 (2021). [Online] Zugriff: 27.03.2023 https://link.springer.com/article/10.1007/s11623-021-1486-2#citeas

[28] K. Weber, A.E. Schütz, T. Fertig, Grundlagen und Anwendung von Information Security Awareness. Springer Vieweg (2019). [Online] Zugriff: 27.03.2023 https://link.springer.com/content/pdf/10.1007/978-3-658-26258-7.pdf

[29] W. Dolle, Incident Management. Datenschutz und Datensicherheit-DuD 29/7, 426 (2005). [Online] Zugriff: 28.03.2023 http://wdolle.de/paper/incident_management_dud05.pdf

[30] S. Frings, O. Göbel, D. Schadt, Incident Management. GI Fachgruppe Sidar. Zugriff: 28.03.2023 https://fg-sidar.gi.de/fachgruppe/themen/incident-management

[31] P. Cichonski, T. Millar, T. Grance, K. Scarfone, Computer Security Incident Handling Guide. National Institute of Standards and Technology, 2012. [Online] Zugriff: 28.03.2023 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[32] A. Weise, Digital Security – Wie Unternehmen den Sicherheitsrisiken des digitalen Wandels trotzen. In: Digitalisierung in Industrie-, Handels- und Dienstleistungsunternehmen – Konzepte-Lösungen-Beispiele, 353-374, Springer Fachmedien (2022) [Online] Zugriff: 28.03.2023 https://link.springer.com/chapter/10.1007/978-3-658-35950-8_16

[33] G. Johansen, Digital Forensics and Incident Response. Packt Publishing (2017). [Online] Zugriff: 28.03.2023 https://books.google.de/books?hl=de&lr=&id=4eZDDwAAQBAJ&oi=fnd&pg=PP1&dq=Digital+Forensics+and+Incident+Response:+A+Practical+Guide+to+Deploying+Digital+Forensic+Techniques+in+Response+to+Cyber+Security+Incidents&ots=aOHjmMtnCP&sig=tJpPVlB65ybzrKgDYqLRpjj361I&redir_esc=y#v=onepage&q&f=false

[34] S.Evers, Trügerische Sicherheit: Aus diesen Gründen bleibt Ransomware weiterhin eine Gefahr. Digitale Welt 6/1, 34-37 (2022). [Online] Zugriff: 28.03.2023 https://www.attingo.com/assets/NewsDateien/20211213_Digitale_Welt_01_2022_Seite_34-37_Truegerische_Sicherheit_aus_diesen_Gruenden_bleibt_Ransomware_weiterhin_eine_Gefahr_SCAN.pdf

[35] Bitkom, Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr. Zugriff: 30.03.2023 https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

[36] Anti Phishing Working Group, Monthly number of phishing attacks reported more than doubled since 1 May 2020. Zugriff: 30.03.2023 https://apwg.org/interisle-study-shows-61-increase-in-phishing-attacks-more-brands-targeted-and-257-increase-in-cryptocurrency-phishing/

[37] Whistleblower Aid Organization, Protected Disclosures of Federal Trade Commission Act Violations, Material Misrepresentations and Omissions, and Fraud by Twitter, Inc. (NASDAQ: TWTR) and CEO Parag Agrawal, SEC TCR, Further Redacted for Congress (2022). [Online] Zugriff: 30.03.2023 https://s3.documentcloud.org/documents/22186782/whistleblower_disclosure.pdf?utm_source=substack&utm_medium=email

[38] G. da Silva, R. Fulterer, Ein Whistleblower erhebt schwere Vorwürfe gegen Twitter – davon könnte Elon Musk profitieren. Neue Zürcher Zeitung (2022). [Online] Zugriff: 30.03.2023 https://www.nzz.ch/technologie/ein-whistleblower-erhebt-schwere-vorwuerfe-gegen-twitter-davon-duerfte-elon-musk-profitieren-ld.1699462

[39] D. Labudde, Zyklus Social Engineering. Social Engineering SoSe Vorlesung 1, 2021 Hochschule Mittweida.

[40] S. Färber, N. Mangold, K. Ruess, Abwehr von Spam und Viren im Unternehmen: was ist möglich und was ist erlaubt. FH München (2004) [Online] zugriff: 02.04.2023 http://webwave-media.de/_download/AbwehrSpamViren.pdf

[41] H. Weimer, Unerwünschte Werbe-E-Mails erkennen und bekämpfen. guardian (2002). [Online] Zugriff: 02.04.2023 https://www.enyo.de/guardian/downloads/jufo.pdf

[42] J. Wieringa, 18-jähriger Hacker nutzt kritische Sicherheitslücke bei Uber durch Social-Engineering-Techniken aus. Netzpalaver (2022). Zugriff: 03.04.2023 https://netzpalaver.de/2022/09/28/18-jaehriger-hacker-nutzt-kritische-sicherheitsluecke-bei-uber-durch-social-engineering-techniken-aus/

[43] U. Choudhry, Der Markt der Cyberversicherungen in Deutschland. Der Cyberversicherungsmarkt in Deutschland: Eine Einführung, 5-26, (2014). [Online] Zugriff: 03.04.2023 https://link.springer.com/chapter/10.1007/978-3-658-07098-4_2

[44] H. Lomen, Die zweite Verteidgungslinie – Cyber-Versicherungen – Versicherungsschutz für Risiken aus der Sphäre von Industrie 4.0. Industrie 4.0: Wie cyber-physische Systeme die Arbeitswelt verändern, 111-135 (2017). [Online] Zugriff: 03.04.2023 https://link.springer.com/chapter/10.1007/978-3-658-15557-5_9

[45] S. Frenkel, N. Popper, K. Conger, D.E. Sanger, A Brazen Online Attack Targets V.I.P. Twitter Users in a Bitcoin Scam. The New York Times (2020). [Online] Zugriff: 03.04.2023 https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html

[46] BSI, Wie schützt man sich vor Phishing? Zugriff: 03.04.2023 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Schutz-gegen-Phishing/schutz-gegen-phishing_node.html

[47] C.A. Göbel, Wesentliche Standards und Technologien im mobilen Zahlungsverkehr. Mobile Payment: Grundlagen – Strategien – Praxis, 143-154 (2017). [Online] Zugriff: 04.04.2023 https://link.springer.com/chapter/10.1007/978-3-658-14118-9_8

[48] PCI SSC, PCI DSS Kurzanleitung: Verständnis des Payment Card Industry Data Security Standard Version 4.0 (2022). Zugriff: 04.04.2023 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0-DE.pdf?lang=de

[49] BSI, Kritische Infrastrukturen und meldepflichtige Unternehmen - Ich suche grundsätzliche Informationen, um mich vor einem IT-Sicherheitsvorfall zu schützen. Zugriff: 03.04.2023 https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Kritische-Infrastrukturen-und-meldepflichtige-Unternehmen/Ich-suche-grundsaetzliche-Informationen-um-mich-vor-einem-IT-Sicherheitsvorfall-zu-schuetzen/ich-suche-grundsaetzliche-informationen-um-mich-vor-einem-it-sicherheitsvorfall-zu-schuetzen_node.html

[50] T. Straub, Usability challenges of PKI. Doctoral dissertation TU Darmstadt (2006). [Online] Zugriff: 04.04.2023 https://tuprints.ulb.tu-darmstadt.de/682/1/tstraub_diss.pdf

[51] H. Kaschner, Auf einem Blick: Sieben Todsünden des Cyber Crisis Managements. Cyber Crisis Management: Das Praxishandbuch zu Krisenmanagement und Krisenkommunikation, 201-2023 (2020) [Online] Zugriff: 05.04.2023 https://link.springer.com/chapter/10.1007/978-3-658-27914-1_7

[52] R. Meeuwisse, The Twitter Hack: How did they do? ISACA Now Blog (2020). Zugriff: 05.04.2023 https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/the-twitter-hack-how-did-they-do-it

[53] V. Först, Drei Jahre Haft für Teenager aus Florida. Netzpolitik.org (2021). Zugriff: 05.04.2023 https://netzpolitik.org/2021/twitter-hack-drei-jahre-haft-fuer-teenager-aus-florida/

[54] A. Weinert, Defend your users from MFA fatigue attacks. Microsoft Entra (Azure AD) Blog (2022). Zugriff: https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/defend-your-users-from-mfa-fatigue-attacks/ba-p/2365677

[55] P. Manaras, M. Hertlein, N. Pohlmann, Die Zeit nach dem Passwort: Handhabbare Multifaktor-Authentifizierung für ein gesundes Eco-System. Datenschutz und Datensicherheit-DuD 40/4, 206-211 (2016). [Online] Zugriff: 11.04.2023 https://link.springer.com/article/10.1007/s11623-016-0579-9

[56] J. Lehner, A. Oberweis, G. Schiefer, Kontextabhängige 3-Faktor-Authentifizierung für den mobilen Zugriff auf Unternehmensanwendungen. HMD Praxis der Wirtschaftsinformatik 51, 64-74 (2014). [Online] Zugriff: 12.04.2023 https://link.springer.com/article/10.1365/s40702-014-0008-1

[57] D. Fox, Secorvo Security News 04/2016. Zugriff: 12.04.2023 https://www.secorvo.de/security-news/secorvo-ssn1604.pdf

[58] E. Wolfangel, Cyberangriffe: Vorsicht, Falle. ZEIT Online (2022). Zugriff: 14.04.2023

[59] M. Kappes, Netzwerküberwachung. Netzwerk- und Datensicherheit: Eine praktische Einführung, 219-236 (2007). [Online] Zugriff: 12.04.2023 https://link.springer.com/chapter/10.1007/978-3-8351-9202-7_11

[60] E. Wolfangel, Cyberangriff auf Continental: Wenn psychische Probleme der Angestellten im Netz landen. ZEIT Online (2022). Zugriff: 16.04.2023

[61] M. Siedler, V. Charles, Continental informiert über abgewendeten Cyber-Angriff (2022). Zugriff: 16.04.2023 https://www.continental.com/de/presse/continental-informiert/

[62] T.A. Möller, Cybersicherheit für Staat, Wirtschaft und Gesellschaft. Zeitschrift für Außen- und Sicherheitspolitik, 1-12 (2023). [Online] Zugriff: 17.04.2023 https://link.springer.com/article/10.1007/s12399-023-00936-w

[63] BSI, Die Lage der IT-Sicherheit in Deutschland 2021. Zugriff: 17.04.2023 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf?__blob=publicationFile&v=4

[64] W. Juling, H. Hartenstein, J. Dinger, IT-Management in der Praxis. Universität Karlsruhe (TH) Fakultät für Informatik (2005). [Online] Zugriff: 17.04.2023 https://publikationen.bibliothek.kit.edu/1000003166

[65] M. Bartsch, F. St, Cyberstrategien für Unternehmen und Behörden. Springer Vieweg (2017). [Online] Zugriff: 17.04.2023 https://link.springer.com/content/pdf/10.1007/978-3-658-16139-2.pdf

[66] BSI, Ransomware – Bedrohungslage 2022. Zugriff: 18.04.2023 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=5

[67] BSI, Top 10 Ransomware-Maßnahmen. Zugriff: 18.04.2023 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/Top-10-Ransomware-Massnahmen/top-10-ransomware-massnahmen_node.html

[68] G. Aaron, L. Chapin, D. Piscitello, C. Strutt, Phishing Landscape 2022: An Annual Study oft he Scope and Distribution of Phishing. Interisle Consulting Group (2022). [Online] Zugriff: 19.04.2023 https://www.interisle.net/PhishingLandscape2022.pdf

[69] T. Henkel, Darknet-die dunkle Seite des Internets? Cyberkriminologie: Kriminologie für das digitale Zeitalter, 175-191 (2022). [Online] Zugriff: 20.04.2023 https://link.springer.com/chapter/10.1007/978-3-658-28507-4_7

[70] Bundeskriminalamt, Bundeslagebild 2016. Cybercrime Bundeslagebild. Zugriff: 20.04.2023 https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Plauen, den 26.04.2023

Antonia Damisch