MASTERARBEIT

CYBERANGRIFFE ALS HERAUSFORDERUNG FÜR UNTERNEHMEN MIT TELEARBEIT

ausgeführt am

Studiengang

Informationstechnologien und Wirtschaftsinformatik

Von: Ernst Tippl

Personenkennzeichen: 2110320031

Graz, am 27.März 2023

Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

.....

Unterschrift

DANKSAGUNG

Anlässlich dieses Meilensteins in meinem Leben möchte ich mich bei meiner Familie und meinen Freunden bedanken. Vor fünf Jahren habe ich mich auf eine Reise begeben, die mich gezwungen hat, auf vieles zu verzichten. Diese Zeit war für alle nicht immer einfach, aber ich bin unglaublich dankbar für die Unterstützung, die ich vor allem von meiner Frau Doris, aber auch von meinen zwei Mädels Anna und Sophia erhalten habe.

Lorenz, unser jüngstes Familienmitglied, war sechs Monate alt, als ich mit dem berufsbegleitenden Studium begann. Ich werde versuchen, all jene Zeit, die ich gerne mit ihm verbracht hätte, aber nicht konnte, nachzuholen.

Auch meinen Freunden möchte ich danken. Immer stand die Familie, die Arbeit oder das Studium im Vordergrund. Ich hoffe, ihr wisst dennoch, dass mir eure Freundschaft sehr wichtig ist.

Ein ganz besonderer Dank gilt auf diesem Wege auch meinem Betreuer, Dipl.-Ing. (FH) Günther Zwetti. Er hat mir viele Male dabei geholfen, die Ruhe zu bewahren und hatte immer und jederzeit ein offenes Ohr für meine Fragen und Probleme. Lieber Günther, ich bin dir wirklich sehr dankbar.

Jetzt, da ich an diesem wichtigen Punkt in meinem Leben angekommen bin, möchte ich euch allen nochmals von ganzem Herzen danken. Ohne eure Liebe, eure Unterstützung und eure Geduld hätte ich nicht durchgehalten. Ich werde mich bemühen, die Zeit, die ich verloren habe, wieder gutzumachen und dafür sorgen, dass ich in eurem Leben wieder eine größere Rolle spiele.

Diese Arbeit widme ich meiner Frau Doris, denn ohne ihre Unterstützung wäre ich nicht bis zu diesem Punkt in meinem Leben gekommen.

KURZFASSUNG

In der heutigen Arbeitswelt bietet die Informationstechnologie viele Vorteile, aber auch erhebliche Risiken für Unternehmen. Mit der zunehmenden Veränderung der Arbeitsweise in unserer Gesellschaft hat sich Telearbeit zu einem wichtigen Bestandteil des Arbeitslebens entwickelt. Die COVID-19-Pandemie hat die Bedeutung von Telearbeit weiter unterstrichen, da es für viele Unternehmen die einzige Möglichkeit war, ihre Existenz zu sichern. Es wird erwartet, dass Telearbeit auch nach der Pandemie ein wichtiger Bestandteil des Arbeitslebens bleiben wird.

Allerdings ist die Tatsache, dass immer mehr Mitarbeiterinnen und Mitarbeiter von verschiedenen Orten aus arbeiten, auch eine Einladung für Cyberkriminelle. Diese versuchen auf verschiedene Weise und über verschiedene Kanäle, auf die Geräte von Telearbeitern zuzugreifen und Unternehmen zu schädigen. Daher ist das Ziel dieser Masterarbeit, Unternehmen dabei zu unterstützen, sich gegen solche Cyberangriffe zu schützen.

Zur Erreichung dieses Ziels wird eine systematische Literaturrecherche durchgeführt, um Informationen zum Thema Cybersecurity in der Telearbeit aus verschiedenen Literaturdatenbanken zu sammeln. Diese Informationen werden sortiert und interpretiert, um eine Handlungsempfehlung bezüglich Sicherheitsmaßnahmen bei der Telearbeit zu erstellen.

Diese Empfehlungen werden anhand eines Kano-Modells dargestellt, das die Maßnahmen nach ihrem Grad der momentanen Umsetzung und nach ihrem Grad der Notwendigkeit in verschiedenen Kategorien einordnet. Sie zielen darauf ab, Unternehmen dabei zu helfen, ihre Sicherheitsmaßnahmen zu verbessern und sich besser gegen Cyberangriffe zu schützen.

Es ist wichtig, dass Unternehmen sich bewusst sind, dass sie ein Ziel für Cyberkriminelle sind und dass sie aktiv Maßnahmen ergreifen müssen, um ihre Daten und Kunden zu schützen.

ABSTRACT

Information technology has many advantages for companies, but also many risks. With the rapid changes in the way our society works, telecommuting has become an important part of working life. In fact, through the COVID-19 pandemic, telecommuting was the only way for many companies to secure their existence. Even after the pandemic, telecommuting will continue to be an important part of working life.

The fact that more and more employees work in different locations also attracts cybercriminals. They try to access teleworkers' devices and harm companies in different ways and through different channels. The primary goal of this thesis is to help companies protect themselves against such cyberattacks.

With the help of a systematic literature search, which includes sources from the last 8 years, a lot of information on this topic could be collected. Subsequently, this knowledge was used to create recommendations for action to protect against cyber risks in telework. The recommendations were presented using a Kano model, which divides the measures into different categories depending on how far they have already been implemented and how necessary they are.

Companies should be aware that they are a target for cybercriminals and that they need to actively protect themselves against them to protect their data and their customers.

INHALTSVERZEICHNIS

1 EINLEITUNG

"Die größte Bedrohung für die Sicherheit beim Arbeiten von zu Hause aus ist, dass viele Menschen denken, dass es sicherer ist." - Stephen Cobb, Sicherheitsforscher

Mit Beginn der Coronakrise im Frühjahr 2020 waren viele Unternehmen dazu gezwungen, ihre Mitarbeiterinnen und Mitarbeiter von zu Hause aus arbeiten zu lassen, um die Gefahr einer Ansteckung zu verringern. Daher wurden so schnell als möglich Mittel und Wege gesucht, die Mitarbeiterinnen und Mitarbeiter mit der nötigen IT-Infrastruktur auszustatten.

Die Herstellung solcher Remote-Arbeitsplätze stellte für viele Unternehmen eine wirtschaftliche Herausforderung dar. Waren in Deutschland vor der Pandemie nur 4 Prozent im Homeoffice, so stieg der Anteil im ersten Lockdown auf 27 Prozent. Nach einem zwischenzeitlichen Rückgang waren es im Jänner 2021 wieder 24 Prozent. (Weidenbach, 2021) Durch diesen Anstieg ergaben sich auch Engpässe bei den IT-Personalressourcen. Umstände wie dieser und der zeitliche Druck für die Unternehmen führten zu einer sicherheitstechnisch bedenklichen Ausgangslage in Bezug auf Cyberrisiken. Nicht nur die Anzahl an Homeoffice-Usern, sondern auch der Anteil der Cyberangriffe, welche durch diese User verursacht wurden, hat sich seither stark erhöht.

Diese Situation führt zur Untersuchung im Rahmen dieser Arbeit und soll Unternehmen Maßnahmen und Richtlinien aufzeigen, mit denen sie sich effektiv gegen solche Angriffe schützen können.

1.1 Problemstellung

Die Gefahr für Unternehmen, Opfer einer Cyberattacke zu werden, stieg in den letzten Jahren eklatant. Eine von KPMG und dem Kuratorium Sicheres Österreich veröffentlichte Studie aus dem Jahr 2021 zeigt, dass 57 Prozent der Unternehmen in Österreich Opfer von Cyberattacken waren, wobei 18 Prozent gar nicht wissen, dass sie angegriffen wurden (Eckhart, 2021).

Ein Grund dafür ist laut Engels (2021) die höhere Anzahl an Angriffspunkten, welche die unternehmenseigene IT vulnerabler machen. Diese Erweiterung der IT-Infrastruktur wurde durch die, während der Coronapandemie nötige, Verlagerung der Mitarbeiterinnen und Mitarbeiter ins Homeoffice erzwungen. Seit Beginn der Coronapandemie hat sich eine besondere Art der mobilen Tätigkeit etabliert, welche teils erheblich von der üblichen Gestaltungsform abweicht. Das sogenannte „Corona Office“ ist jener Zustand, in dem Arbeitnehmer ganz oder teilweise und mehr oder weniger strukturiert versuchen, ihre Tätigkeit von einem behelfsmäßig eingerichteten Homeoffice aus zu verrichten (Bertram et al., 2021).

Genau dieser Aspekt bringt viele Gefahren mit sich. Pohlmann (2019) behauptet zum Beispiel, dass jeder zweite Homeoffice-Arbeitsplatz nicht sicher ist. Angreifer sind sich dieser Problematik bewusst und konzentrieren sich verstärkt auf diesen Bereich.

Engels (2021) zeigt in Abbildung 1, dass in Deutschland im Jahr 2020 von 223,5 Milliarden Euro Schaden durch Cyberkriminalität 52,5 Milliarden Euro auf Angriffe im Homeoffice zurückzuführen sind. Im Vergleich dazu waren es vor der Coronapandemie um 31 Milliarden Euro weniger.

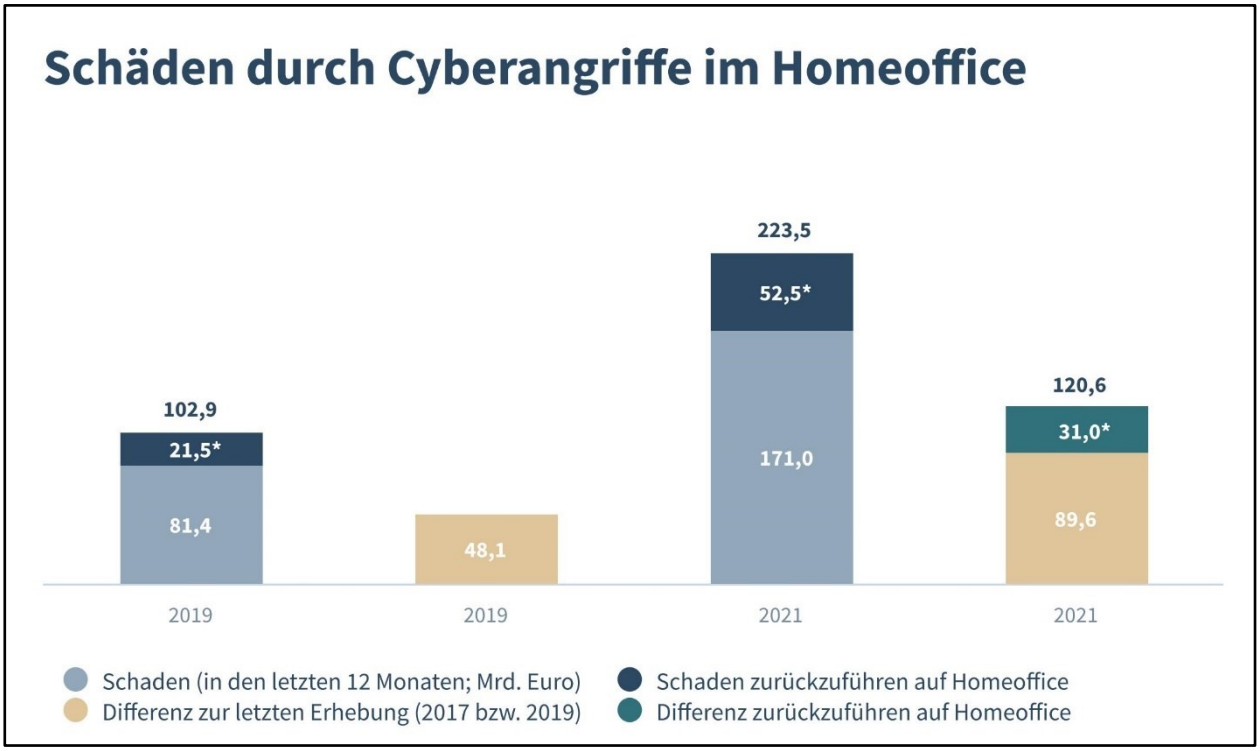

Abbildung 1: Schäden durch Cyberangriffe im Homeoffice (Engels, 2021)

Diese Entwicklung bedarf einer genaueren Betrachtung, um Maßnahmen für den sicheren IT-Betrieb im Homeoffice seitens der Unternehmens-IT, aber auch seitens der Mitarbeiterinnen und Mitarbeiter ableiten zu können.

1.2 Zielsetzung

Im Rahmen dieser Masterarbeit sollen die IT-Schwachstellen, welche sich durch die Telearbeit für die Unternehmen ergeben haben, erarbeitet und analysiert werden. Auf Basis der Literaturrecherche und den daraus gewonnenen Erkenntnissen werden Hypothesen abgeleitet, welche im empirischen Teil der Arbeit betrachtet werden. Die Bestätigung oder auch Widerlegung dieser Hypothesen ermöglicht es, Gefahren, Maßnahmen und Richtlinien für den sicheren IT-Betrieb in der Telearbeit zu erstellen.

Da bei dieser Masterarbeit die Forschung mittels deduktiver Vorgehensweise erfolgt, werden Hypothesen als Ausgangspunkt der empirischen Forschung verwendet. Die im Zuge des Theorieteils abgeleiteten Hypothesen betrachten fünf verschiedene Bereiche, welche die Cyberrisiken bei der Telearbeit betreffen.

1.2.1 Hypothesen

Folgend werden Hypothesen für die fünf Kategorien der empirischen Forschung aufgestellt.

- Angriffsarten
- Angriffskanal Nutzer
- Angriffskanal System
- Technische Sicherheitssysteme
- Organisatorische Sicherheitssysteme

1.2.1.1 Hypothesen - Angriffsarten

Bei der Erarbeitung des Theorieteils wurde Phishing als großes Sicherheitsrisiko erkannt. Daher wurde hier folgende Hypothese abgeleitet:

H1: Phishing wird als größtes Sicherheitsrisiko bei der Telearbeit erkannt.

H0: Phishing ist im Bereich der Telearbeit nicht die relevanteste Angriffsart.

1.2.1.2 Hypothesen - Angriffskanal Nutzer

Es wird versucht, User über verschiedenste Kanäle zu erreichen. Laut Literatur sind hier kompromittierte Webseiten der Hauptkanal, über den Nutzer angegriffen werden.

H1: Kompromittierte Webseiten stellen das größte Problem bei der Erkennung von Angriffen für den Telearbeiter / die Telearbeiterin dar.

H0: Kompromittierte Webseiten sind nicht das primäre Problem bei der Erkennung von Angriffen für den Telearbeiter / die Telearbeiterin.

1.2.1.3 Hypothesen - Angriffskanal System

Angriffe ohne Mithilfe des Users, sondern die Nutzung von Schwächen des Systems lassen weitere Hypothese erkennen. Während der Suche von Informationen für den Literaturteil wurde oft die steigende Anzahl an mobilen Endgeräten als großer Angriffsvektor genannt. Deshalb wurde folgende Hypothese aufgestellt:

H1: Mobile Endgeräte stellen das größte Risiko bei Angriffen auf die IT-Systeme der Unternehmen dar.

H0: Mobile Endgeräte spielen eine untergeordnete Rolle als Angriffsvektor.

1.2.1.4 Hypothesen - Technische Sicherheitssysteme

Die Theorie hat hier viele Möglichkeiten aufgezeigt, wobei jedoch eine technische Sicherheitsmaßnahme immer wieder in Verbindung mit der Telearbeit genannt wird.

H1: VPN wird als wichtigstes, technisches Sicherheitssystem im Einsatz gegen Cyberangriffe bei der Telearbeit angesehen.

H0: VPN spielt eine untergeordnete Rolle beim Schutz vor Cyberangriffen bei der Telearbeit.

Die Theorie nennt immer wieder die Gefahren durch E-Mails. Dadurch ergab sich in diesem Bereich eine weitere Theorie.

H1: Verschlüsselung des Mailverkehrs spielt eine wichtige Rolle beim Schutz der Unternehmenssysteme.

H0: Momentan wird die Verschlüsselung des Mailverkehrs nicht als notwendige Maßnahme angesehen.

1.2.1.5 Hypothesen - Organisatorische Sicherheitssysteme

Nach Beginn der Corona-Pandemie wurde vermehrt damit begonnen, Richtlinien für die Telearbeit zu erstellen.

Daraus ergibt sich folgende Hypothese:

H1: Je aktueller die Quellen, desto öfter werden Richtlinien für die Telearbeit als notwendig erwähnt.

H0: Es ist kein Trend erkennbar, der auf einen Anstieg von Richtlinien für die Telearbeit hinweist.

1.3 Abgrenzung

Diese Arbeit soll einen Überblick über die gängigsten, in der Literatur genannten, Cyberrisiken in Bezug auf Telearbeit schaffen und aufzeigen, wie diese verringert werden können. Zielgruppe dieser Arbeit sind Personen im Managementbereich von Unternehmen, welche Entscheidungen hinsichtlich weiterer Vorgehensweisen beim Kampf gegen Cybersecurity in der Telearbeit treffen müssen.

Es soll ein „Big Picture“ in Form eines Kano-Models entstehen, mit dessen Hilfe alle jene Entscheidungsträger auf einfachste Art und Weise den momentanen Sicherheitsstand überprüfen und auch weitere Schritte zur IT-Sicherheit setzen können.

Angesichts der nahezu unüberschaubaren Anzahl von IT-Sicherheitsrisiken ist es in dieser Arbeit nicht möglich, sämtliche auf dem Markt verfügbaren Risiken und Sicherheitssysteme zu behandeln. Vielmehr fokussiert die vorliegende Literaturrecherche die bedeutendsten Einflussfaktoren in diesem Bereich.

1.4 Forschungsfrage

Welche Handlungsempfehlungen können in Bezug auf Telearbeit gegeben werden, um einer Gefährdung der Unternehmenssicherheit durch Cyberangriffe effektiv entgegenwirken zu können?

1.5 Aufbau der Arbeit

In den Kapiteln zwei bis vier wird die grundlegende Theorie des Forschungsgebietes beschrieben. Als Einführung in das Thema wird im zweiten Kapitel genauer auf Cyberangriffe eingegangen. Neben der allgemeinen Definition und der Geschichte von Cyberattacken wird auch auf die häufigsten Varianten eingegangen. Auch die Schwachstellen beim Schutz vor Cyberangriffen und das daraus resultierende Schadensausmaß werden hier erläutert. Im Kapitel drei werden mögliche technische als auch nicht-technische Maßnahmen zur Schadensvermeidung aufgezeigt. Im vierten Kapitel wird näher auf das Thema Telearbeit eingegangen. Es werden hier die allgemeinen Begrifflichkeiten dazu zusammengefasst und die Auswirkungen auf IT-Konzepte und Mitarbeiterinnen und Mitarbeiter beschrieben.

Ab dem fünften Kapitel wird näher auf den empirischen Teil der Arbeit eingegangen. Die verwendeten wissenschaftlichen Methoden werden in Kapitel sechs genauer beschrieben und direkt auf die Arbeit angewendet. Das Kapitel sieben beschäftigt sich mit den Ergebnissen der empirischen Forschung. Der Empirie-Teil schließt mit Kapitel acht, den Schlussfolgerungen aus den gesamten Ergebnissen. Dabei werden die Ergebnisse interpretiert und die Hypothesen zu bestätigen oder widerlegen versucht. Die gewonnenen Erkenntnisse aus der Interpretation werden am Ende dieses Kapitels verschriftlicht.

Im Kapitel neun wird die Forschungsfrage beantwortet. Die weiteren beiden Kapitel zeigen eine kritische Betrachtung der Arbeit und eventuelle Forschungsmöglichkeiten, die aus dieser Arbeit resultieren.

2 CYBERCRIME

Zu Beginn wird in diesem Kapitel definiert, wann man von Cybercrime, der Computerkriminalität, im Allgemeinen spricht. Danach wird der tatsächliche Akt, die Cyberattacke geschichtlich betrachtet. Das Hauptaugenmerk liegt aber in diesem Kapitel auf den verschiedenen Angriffsvarianten, deren Schadensausmaßen und welche Schwachstellen dabei genutzt werden.

2.1 Begriffsdefinitionen

Für das Verständnis dieser Masterarbeit ist es wichtig, klare Begriffsdefinitionen zu verschriftlichen, um Fehlinterpretationen zu vermeiden.

2.1.1 Cybercrime

Huber (2019) definiert als Cybercrime alle Straftaten, die unter der Ausnutzung der Informations- und Kommunikationstechnik begangen werden. Unter der Bezeichnung Cybercrime werden im österreichischen Strafgesetzbuch mehrere Deliktsarten gelistet:

- §118a: Widerrechtlicher Zugriff auf ein Computersystem
- §119: Verletzung des Telekommunikationsgeheimnisses
- §119a: Missbräuchliches Abfangen von Daten
- §126a: Datenbeschädigung
- §126b: Störung der Funktionsfähigkeit eines Computersystems
- §126c: Missbrauch von Computerprogrammen
- §148a: Betrügerischer Datenverarbeitungsmissbrauch
- §207a: Kinderpornographie
- §208a: Anbahnung von Sexualkontakten zu Unmündigen
- §225a: Datenfälschung

2.1.2 Cybersecurity

Ein Thema, welches sehr oft im Zusammenhang mit Cybercrime genannt wird, ist Cybersecurity oder auch Cybersicherheit. Cybersecurity beschäftigt sich unter anderem mit dem Schutz von Netzwerken, Systemen, Geräten und deren Nutzern. Der Fokus liegt hier klar auf der digitalen Welt. Cybercrime hingegen zielt auf den Einsatz technischer Hilfsmittel ab, um „offline“ Verbrechen zu begehen.

2.2 Geschichte von Cyberangriffen

Die Geschichte der Cyberangriffe reicht bis in die frühen 80er Jahre. Der erste bekannte Cyberangriff geht auf das Jahr 1982 zurück, als Russland versuchte, hochtechnologische Steuerungssysteme für Pipelines von Amerika zu stehlen. Diese bauten in die Software ein Schadprogramm ein, welche eine Explosionsstärke von ca. 3 Kilotonnen hatte und so die gesamte Pipeline zerstörte. (Kloiber & Welchering, 2011)

Der erste bekannte „Wurm“, der im November 1988 eine Schwachstelle in Hilfsprogrammen von Unix-Derivaten nutzte, infizierte tausende Rechner und störte den Betrieb der Internetverbindung massiv (Spafford, 1988). Primäres Ziel blieb dennoch die Schwächung von gegnerischen Infrastrukturen im Kriegseinsatz. Beispiele dafür sind der Jugoslawienkrieg, in dem 1999 die NATO das jugoslawische Telefonnetz sabotierte, oder auch die Cyberangriffe auf Estland und Syrien im Jahr 2007 oder Georgien 2008 (Saalbach, 2019).

Mit dem Einzug der Informationstechnologie in die Unternehmenswelt hat sich in den letzten 25 Jahren als Antwort auf diese Veränderung eine Cybercrime-Industrie entwickelt. Diese nutzt Schwächen der Nutzer und Schwachstellen der Systeme, um Schaden anzurichten oder sich illegal zu bereichern. (Huber, 2019)

Einer der bekanntesten Angriffe war Stuxnet im Jahr 2010, ein Computerwurm, der das Ziel hatte, iranische Uran-Anreicherungszentrifugen zu zerstören. Er konnte sich über USB-Laufwerke unbemerkt verbreiten, infizierte hunderttausende Computer weltweit und nutzte Lücken im Windows Betriebssystem als auch in Siemens-Steuerungen.

Die wohl aufsehenserregendste Cyberattacke war der 2017 durchgeführte Ransomware-Angriff Wannacry. Innerhalb von vier Tagen wurden mehr als 200.000 Computer in 150 Ländern lahmgelegt. Natürlich befanden sich darunter auch Geräte kritischer Infrastrukturen, die verschlüsselt und nur nach Zahlung eines Lösegeldes wieder freigegeben wurden. (Brockhaus, 2022)

Das momentan aktivste Schadprogramm Emotet wurde im Jahr 2014 durch die Sicherheitsfirma Trendmicro entdeckt. Ursprünglich wurde die Software entwickelt, um Bankdaten auszuspähen. Heute dient Emotet als Basis über die anderen Schadprogramme, die auf die infizierten Systeme nachgeladen werden. In der Regel gelangt es über Spammails mit infizierten Links oder Anhängen auf den Rechner. (Wölbert, 2020)

Heutzutage ist es auch einem Laien möglich, solche gezielten Attacken auszuführen. Illegale Leistungen wie Crime as a Service nehmen stetig zu. Hierbei können verschiedenste Dienste in Anspruch genommen werden. Am häufigsten werden folgende Services angeboten:

- Angebot an Hackingtools
- Angebot an Schadsoftware (Verschlüsselungstrojaner)
- Dienstleistungen zur Geldwäsche
- Services für den „Opfer-Support“

- Dienste zur Nutzung von Bot-Netzwerken
- Inverkehrbringung von Falschgeld, Kreditkartendaten (Bundesministerium für Inneres, 2021, S. 10)

2.3 Typen von Cyberangriffen

Um die Vielzahl der verschiedenen Cyberangriffstypen überblicken zu können, sollten diese nach der Angriffsart unterschieden werden.

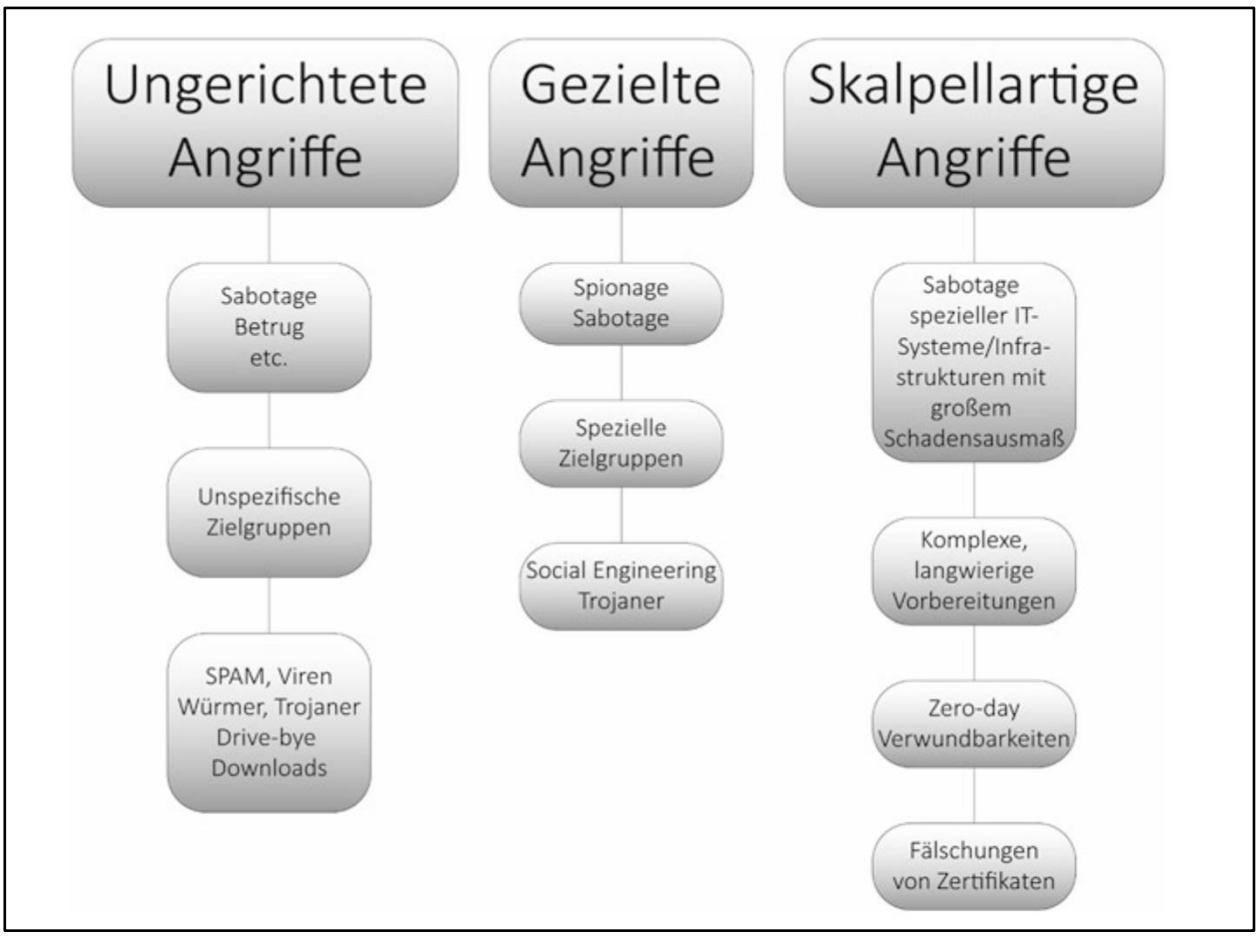

Abbildung 2: Struktur von Cyberangriffen (Huber, 2019)

Im Verlauf des Kapitels gibt es immer wieder Überschneidungen in der Einteilung der Angriffe, da einige sowohl ungerichtet als auch gezielt eingesetzt werden können. Auch der Einsatz mehrerer Angriffstypen innerhalb eines Angriffes ist in einigen Fällen üblich. Dennoch soll diese Unterteilung einen besseren Überblick über die einzelnen Arten schaffen.

2.3.1 Ungerichtete Angriffe

Da sich diese Form der Angriffe nicht gegen ein bestimmtes Ziel richtet, werden sie als ungerichtet oder auch „opportunistisch“ beschrieben. Es wird, zum Beispiel, das Internet unwillkürlich nach Schwachstellen durchsucht, um diese auszunutzen und möglichst viele Nutzer zu schädigen. (Huber, 2019)

Um einen Überblick über diese Art von Attacke zu bekommen, werden nun einige bekannte Varianten beschrieben.

- Phishing

  Der Begriff Phishing ist angelehnt an das englische Wort fishing. Das „P“ steht hierbei für den ersten Buchstaben von Passwort. Es bedeutet also das Fischen nach Passwörtern. (Huber, 2019)

  Dabei handelt es sich um eine Form des Identitätsdiebstahls, bei dem mit Hilfe von Social Engineering versucht wird, die Opfer dazu zu bewegen, sensible Daten preiszugeben. (Bundesamt für Sicherheit in der Informationstechnik, 2020b)

  Es kommen hierbei gefälschte Webseiten, E-Mails oder andere Messenger-Nachrichten zum Einsatz. (Bundesministerium für Inneres, 2020, 2020)

  Das Erkennen von solchen Angriffen wird durch die immer besser werdende Qualität sehr erschwert. So berichtet das deutsche Bundesamt für Sicherheit in der Informationstechnik (2020b), dass im Berichtszeitraum 60 Prozent der Phishing- Nachrichten bereits HTTPS verwenden.

- Spam

  Ebenfalls ungerichtet versuchen Täter mit Massen-E-Mails, sogenannten Spam, tausende Personen zu erreichen, um durch Vortäuschung falscher Tatsachen Geld von den Opfern zu bekommen. Hierzu werden unerlaubt erworbene Absender-E-Mail-Adressen verwendet. Oft handelt es sich dabei um E-Mail-Adressen von Behörden oder anderen öffentlichen Stellen. (Huber, 2019)

  Das Ausspähen der Zugangsdaten von legitimen E-Mail-Accounts ist nur ein möglicher Ansatz, Spammails zu verschicken. Oft werden auch kompromittierte oder kommerziell angemietete Serverkapazitäten dazu verwendet. Ebenso werden infizierte Systeme, welche zu Botnetzen zusammengeschlossen werden, für Spam-Dienstleistungen verwendet. (Bundesamt für Sicherheit in der Informationstechnik, 2020b)

- Malware

  Bei dem Begriff Malware, einem englischen Kunstwort für „malicious Software“, im deutschen bösartige Software, handelt es sich laut Pohlmann (2022) um den Oberbegriff für Schadsoftware wie Viren, Würmer, trojanische Pferde, Exploits und einigen mehr. Durch Softwareschwachstellen oder Bedienerfehler wird Malware mittels Drive-by-Downloads auf Endgeräten unbemerkt eingeschleust. Drive-by-Downloads nutzen

Schwachstellen in Browsern, Zusatzprogrammen von Browsern oder im Betriebssystem, um ohne weitere Nutzerinteraktion Schadsoftware unbemerkt auf einem Endgerät zu installieren. (Bundesamt für Sicherheit in der Informationstechnik, 2020b) Die Anzahl der täglich neuen Schadprogrammvarianten wird laut Pohlmann (2019) auf ca. 320 000 geschätzt.

Viren sind wohl die bekannteste Gattung von Malware. Es handelt sich dabei um Programme, die an einen Wirt, ein betroffenes Endgerät gebunden sind. Um sich zu reproduzieren, fertigen sie beim Ausführen dieser Software eine Kopie von sich selbst auf einem weiteren betroffenen Endgerät an. Der Schaden bezieht sich jedoch nicht nur auf den Wirten, hier kann das ganze System nach Ausführung des bösartigen Teils der Software betroffen sein. (Hof et al., 2007)

Ähnlich verhalten sich Würmer, jedoch sind sie nicht an einen Wirt gebunden und verbreiten sich selbstständig innerhalb eines Netzwerks. Dabei werden keine Dateien direkt befallen und auch kein Nutzereingriff ist notwendig. Bevorzugt verbreiten sich dabei Würmer über E-Mail-Anhänge. (Huber, 2019)

Trojaner verfolgen einen anderen Ansatz. Es handelt sich hierbei um Programme, die einen nützlichen Zweck vortäuschen, jedoch einen, für den Anwender nicht erkennbaren, Teil mit schädlichen Funktionen aufweisen. Das bedeutet, der User installiert den Trojaner meist selbst. Dieser pflanzt sich aber nicht selbständig fort. Er liest sensible Daten des Opfers aus und sendet diese an dessen Autor zurück. (Hof et al., 2007)

Exploits, der Name kommt vom englischen Begriff „to exploit“ und bedeutet ausnutzen, sind Schadprogramme, die Sicherheitslücken in Hilfs- oder Anwendungsprogrammen ausnutzen. Dadurch ergeben sich Möglichkeiten zur Manipulation der IT-Systeme. Zum Beispiel können Änderungen in der Berechtigungsverwaltung vorgenommen werden oder durch die Verwendung von Denial of Service, kurz DoS, -Attacken ganze Systeme lahmgelegt werden. (Siller, 2018a)

- Botnetze

  Die Verbreitung dieser Schadsoftwaretypen wird über sogenannte Botnetze gesteuert. Als Bot bezeichnet man ein Schadprogramm, mit dem Angreifer einen Fernzugriff auf infizierte Systeme bekommen. Ein infiziertes System baut eine Verbindung zu einem Kontrollserver der Angreifer auf und nimmt dort Befehle entgegen. (Bundesamt für Sicherheit in der Informationstechnik, 2020b)

  Ein solcher Kontrollserver bildet vernetzte Systeme wie zum Beispiel PCs, Router oder Webcams, die ferngesteuert einen DDoS-Angriff auf ein Zielsystem ausführen oder dieses nutzen, um Spam oder Malware zu verbreiten. (Porath, 2020)

  All diese Typen von opportunistischen Attacken haben das Ziel, möglichst viele Nutzer zu schädigen, um den normalen Betrieb der Systeme zu stören beziehungsweise zu vermeiden. (Kshetri, 2010)

Angemerkt werden muss, dass ein Botnetz an sich kein krimineller Zusammenschluss von Systemen ist. Eigentlich handelt es sich dabei vielmehr um ein Computerprogramm, das automatisch Aufgaben abarbeitet, ohne dabei auf menschlichen Eingriff angewiesen zu sein. Erst im Zusammenhang mit Malware wird das Botnetz als kriminell eingestuft. (Huber, 2019)

- Ransomware

  Wie Hange (2012) aufzeigt, werden auch Ransomware-Angriffe den ungezielten beziehungsweise ungerichteten Angriffen zugeordnet. Der Begriff „ransom“ kommt aus dem englischen und bedeutet Lösegeld. Daher ist es im deutschen auch als Erpressungssoftware bekannt. Es handelt sich dabei um Schadsoftware welche Daten oder Bereiche des Betriebssystems verschlüsselt und damit den Zugriff auf diese Ressourcen einschränkt oder verhindert. (Bundesministerium für Inneres, 2020)

  Die Software gelangt meist durch versehentlichen oder einen im Hintergrund versteckten Download von einer infizierten Webseite auf das Zielsystem. Nachdem die Software selbst startet, oder ferngesteuert gestartet wird, verschlüsselt sie die erreichbaren Daten oder gibt vor sie verschlüsselt zu haben. Danach kommt es zu einer Lösegeldforderung. Bezahlen die Opfer erhalten sie im besten Fallen den Code zur Entschlüsselung der Daten. (Porath, 2020)

2.3.2 Zielgerichtete Angriffe

Im Gegensatz zu den ungerichteten handelt es sich bei den zielgerichteten Angriffen um einen geplanten Angriff auf ein bestimmtes Opfer, welches dem Täter typischerweise bekannt ist, aber nicht sein muss. (Huber, 2019) Zielgerichtete Attacken werden in der Regel von sehr gut ausgebildeten Tätern durchgeführt. Folgende Möglichkeiten stehen dem Angreifer hier mitunter zur Verfügung:

- Social Engineering

  Die menschlichen Schwächen wie Neugier und Angst stehen beim Social Engineering im Vordergrund. Diese werden ausgenutzt, um Zugriff auf sensible Daten zu erhalten. Das Ausforschen der Informationen gelingt oft schon durch das reine Ausspähen von Social-Media-Plattformen. (Bundesministerium für Inneres, 2020)

  Bei einer Umfrage von Bitkom (Berg & Selen, 2021) unter mehr als 1000 Unternehmen gaben 40 Prozent davon an, dass ihre Mitarbeiterinnen und Mitarbeiter mittels Social Engineering beeinflusst wurden. Viele Firmen wurden dabei über verschiedenste Kanäle erreicht. Am häufigsten wurden hier Telefon (27 Prozentpunkte) und E-Mail (24 Prozentpunkte) genannt. 63 Prozent der Unternehmen betrachten Social Engineering als sehr – beziehungsweise eher bedrohlich. Mit Hilfe von Social Engineering werden laut Pohlmann (2022) Angriffe wie Spear-Phishing (Mail von angeblich vertraulichen Quellen) oder Whaling (erreichen von Führungskräften) vorbereitet um dann Ziel-IT-Systeme anzugreifen.

In den letzten Jahren hat sich hier eine weitere, ernst zu nehmende Bedrohung, stetig weiterentwickelt. Mittels Deep Fakes, eine KI-basierende Technologie, mit der Bilder, Audio- und Videodateien erstellt und verändert werden, kann authentischer, jedoch falscher Content, erzeugt werden. Nachbildung von Stimmen bekannter Führungskräfte oder Remote-Meetings mit Darstellung von genauen Abbildern in Echtzeit stellt die Mitarbeiterinnen und Mitarbeiter vor täuschend echte Tatsachen. (Lanzenhofer et al., 2021)

- Distributed Denial of Service

  Laut einem Pressebericht von Kaspersky (2022) stieg die Anzahl von DDoS-Angriffen weltweit im dritten Quartal 2021 um 24 Prozent gegenüber dem dritten Quartal 2020. Die smarten, zielgerichteten Angriffe stiegen jedoch um 31 Prozent im gleichen Zeitraum. Das bedeutet, die DDoS-Angriffe werden immer zielgerichteter auf bestimmte Unternehmen, Institutionen oder Einzelpersonen ausgeführt. Deshalb wird der DDoS-Angriff in dieser Masterarbeit als zielgerichteter Angriff geführt. Es handelt sich dabei um eine verteilte Attacke, die zu einem Ausfall oder einer Unterbrechung eines Online-Dienstes führen soll.

  Dies soll durch eine temporäre oder dauerhafte Überlastung des Opfer-Systems durch beispielsweise Hypertext Transfer Protocol, kurz http, -Anfragen erreicht werden. Malware wird auf nicht- oder schlecht geschützten Devices wie zum Beispiel Webcams oder Routern installiert, um von dort zu einem bestimmten Zeitpunkt aktiv zu werden. (Porath, 2020)

  Als Schutz vor solchen DDoS-Angriffen wurden Schutzsysteme an den Netzwerkgrenzen eingeführt, die mittels eines Detektions-Schwellenwertes solche Angriffe erkennen sollen. Bereits Ende 2017 trat verstärkt eine Strategie namens „Carpet Bombing“ auf, welche den Angriff auf eine große Anzahl von IP-Adressen in dem Zielnetzwerk richtet. Dadurch bleibt die Datenmenge pro IP-Adresse klein und wird daher von den Schutzsystemen nicht detektiert. (Bundesamt für Sicherheit in der Informationstechnik, 2020b)

- Advanced Persistent Threat

  Unter die Art der gezielten Angriffe fällt laut Pohlmann (2022) auch die Advanced Persistent Threat, kurz APT, zu Deutsch „fortgeschrittene andauernde Bedrohung“. Es wird dabei versucht, das IT-System des Opfers mit komplexen Angriffstechnologien sowie aufwendigen Hintergrundinformationen anzugreifen. Der Angreifer nimmt hier großen Aufwand auf sich, um möglichst lange unbemerkt das infizierte IT-System auszuspähen.

  Die Motivation und Vorgehensweise des Angreifers unterscheiden sich hier von anderen Attacken. Während die meisten Schadprogramme in der Regel von finanziell motivierten Angreifern massenhaft und wahllos verteilt werden, wird hier langfristig geplant und es werden nur ausgewählte Ziele angegriffen. (Bundesamt für Sicherheit in der Informationstechnik, 2020b) Um Zugriff zu den Systemen zu erhalten, kommt zumeist Social Engineering zum Einsatz. Es werden also bewusst menschliche Schwachstellen ausgenutzt. (Schiebeck et al., 2015)

Das Bundesamt für Sicherheit in der Informationstechnik (2020b) berichtet, dass diese Angriffe meist von Spezialisten-Gruppen ausgeführt werden. Im Zeitraum der Berichtserstellung waren etwas mehr als ein Duzend solcher APT-Gruppen in Deutschland aktiv. Weltweit lag die Anzahl im dreistelligen Bereich. Auch immer mehr Staaten geben bekannt, solche Cyberfähigkeiten weiterzuentwickeln, wodurch man davon ausgehen kann, dass sich die Anzahl stetig erhöhen wird. Der Bericht weist auch darauf hin, dass in der Regel taktische und strategische Absichten wie Spionage und Sabotage im Fokus stehen.

2.3.3 Skalpellartige Angriffe

Immer häufiger werden laut Huber (2019) solche skalpellartigen Angriffe durchgeführt, jedoch setzt diese Angriffsform eine intensive Vorbereitung voraus. Ziel einer solchen Attacke ist zumeist die Zerstörung der Infrastruktur.

- Zero-Day-Attacken

  Ausgangspunkt solcher Attacken sind grundsätzlich Zero-Day-Verwundbarkeiten. Von einer solchen Null-Tage-Schwachstelle spricht man, wenn eine Software eine gefährliche Sicherheitslücke aufweist und diese ausgenutzt wird, bevor der Softwarehersteller die Möglichkeit hat, sein Produkt dagegen zu schützen. Die Hersteller der Systeme als auch die Opfer haben demnach „null Tage“ Zeit, diese Schwachstelle zu beheben. (Porath, 2020)

  Angreifer verwenden Zero-Day-Exploits, kleine Schadprogramme, welche diese Sicherheitslücken ausnutzen, um sich Möglichkeiten zur Manipulation der betroffenen Systeme zu verschaffen. Zum Beispiel wird versucht, die Administrationsrechte zu erlangen. (Siller, 2018)

- Würmer

  Auch Würmer wie der in Kapitel 2.2 beschriebene Wurm Stuxnet und dessen Nachfolger Duqu fallen laut Hange (2012) in die Kategorie der skalpellartigen Angriffe.

2.4 Schwachstellen

In diesem Punkt werden jene Schwachstellen erarbeitet, die von den verschiedenen Cyberattacken des Kapitels 2.3 genutzt werden, um Zugriff auf die Opfersysteme zu erlangen. Laut Engels (2017) wird im Rahmen von Cyberkriminalität von einer asymmetrischen Bedrohung gesprochen. Während ein Angreifer nur ein Schlupfloch finden muss, so hat ein Unternehmen beziehungsweise das Opfer viele Systeme mit zahlreichen Schwachstellen abzusichern.

Wie Kersten et al. (2016) erwähnen, wird bei den Schwachstellen zwischen konstruktiven und operativen unterschieden. Huber (2019) fasst die Unterscheidung als Schwächen der Nutzer und

als Schwachstellen der Systeme zusammen. In den folgenden Unterkapiteln werden diese Schwächen und Schwachstellen genauer betrachtet.

2.4.1 Schwachstelle Nutzer

In einem Bericht der Kaspersky Labs GmbH (2018) wird erwähnt, dass mehr als 90 Prozent aller Sicherheitsvorfälle auf menschliche Fehler zurückzuführen sind. Täter nutzen menschliche Schwächen wie Anerkennung, Gier oder Sehnsucht nach Beziehungen aus, um sich zu bereichern. Social Engineering ist daher auch in den letzten Jahren ein maßgeblicher Faktor. (Bundesministerium für Inneres, 2021)

Maßgebliche Gefahren für User sind mitunter die folgenden Beispiele:

- Phishing-Webseiten

  Als Beispiel werden in dem genannten Bericht von Kaspersky angeklickte Links angeführt, die zu Phishing-Seiten führen. Bei dem in Kapitel 2.3.1 erwähnten Phishing wird versucht, mittels Social Engineering sensible Daten von Opfern zu erschleichen. Gefälschte Webseiten spielen hier, wie bereits in jenem Kapitel erwähnt, eine große Rolle. Im Zusammenhang mit Corona wurden mehrere tausend Domains angemeldet und eine starke Zunahme von betrügerischen Webseiten beobachtet. (Bundesministerium für Inneres, 2020)

  Weiters erwähnt Kaspersky (Kaspersky Labs GmbH, 2018; 2018) bösartige Webseiten, hinter denen Viren und weitere hochentwickelte Bedrohungen lauern und mittels Drive-by-Downloads auf das Opfersystem gelangen.

- Phishing E-Mails

  Sogenannte Spear Phishing-Angriffe, das sind fortgeschrittene, zielgerichtete Phishing Attacken per E-Mail, welche individuell auf Personen ausgerichtet sind, waren im Jahr 2019 die beliebteste Methode von Cyberangriffen. (Symantec, 2019)

- Soziale Medien

  Das Bundesministerium für Inneres (2021) erwähnt das Ausspähen von Daten auf Social-Media-Plattformen und Anrufe mit falschen Identitäten ebenfalls als probates Mittel des Social Engineering.

- Deep Fakes

  Eine weitere Bedrohung, die in Zukunft immer mehr Beachtung finden wird, sind Deep Fakes. Der Begriff ist eine Kombination aus „Deep Learning“ und „Fake“ und verweist auf eine KI-basierte Technologie, mit der Bilder, Audio- oder Videodateien erstellt oder verändert werden, um falsche Inhalte zu erzeugen. Diese Deep Fakes wirken immer authentischer, wodurch ein Erkennen solcher Deep Fakes immer schwieriger wird. (Lanzenhofer et al., 2021)

> Durch Deep Learning mit neuronalen Netzen können zum Beispiel Filmaufnahmen der Zielperson und des Täters gespeichert und mittels einer digitalen Maske Gesichtsregungen des Täters auf das Gesicht der Zielperson projiziert werden. (Porath, 2020)
>
> Bei der Zielperson kann es sich um zum Beispiel um den CEO oder CFO eines Unternehmens handeln, der telefonisch um eine Geldüberweisung bittet oder auch dessen genaues Abbild in einem Video. (Lanzenhofer et al., 2021)

Laut Henseler-Unger, Hillebrand et al (Henseler-Unger et al., 2018; 2018) sind auch noch weitere Schwachstellen im personellen Bereich zu orten. Hauptproblem stellen hier die fehlenden beziehungsweise nicht gut ausgebildeten Mitarbeiterinnen und Mitarbeiter dar, welche für die IT-Sicherheit in Unternehmen zuständig sind. Gerade im Bereich der kleinen und mittleren Unternehmen, kurz KMU, wird IT-Sicherheit oft von mehr oder weniger fachfremden Mitarbeiterinnen und Mitarbeitern in Personalunion ausgeübt.

2.4.2 Schwachstelle System

Neben den in 2.4.1 erwähnten menschlichen Schwächen gibt es aber natürlich auch eine Vielzahl von Systemschwachstellen. Pohlmann (2022) identifiziert unter anderem folgende Systemschwachstellen:

- schlechte Softwarequalität
- ungenügender Schutz vor Schadsoftware
- keine internationalen Lösungen zur Identifikation und Authentifikation
- unsichere Webseiten
- Gefahren durch mobile Endgeräte
- Gefahren durch Internet of Things-Geräte (kurz IoT)
- E-Mail-Dienste
- manipulierte IT-Sicherheitssysteme

Um einen besseren Einblick zu erlangen, werden in diesem Kapitel einige dieser Ansätze im Detail erklärt.

Einer der wichtigsten Punkte in Bezug auf Cyberrisiken ist die schlechte Softwarequalität. In einem Bericht des Bundeskriminalamtes aus dem Jahr 2022 wird der Anstieg der veröffentlichten Software-Schwachstellen basierend auf deren CVE-Nummern aufgezeigt.

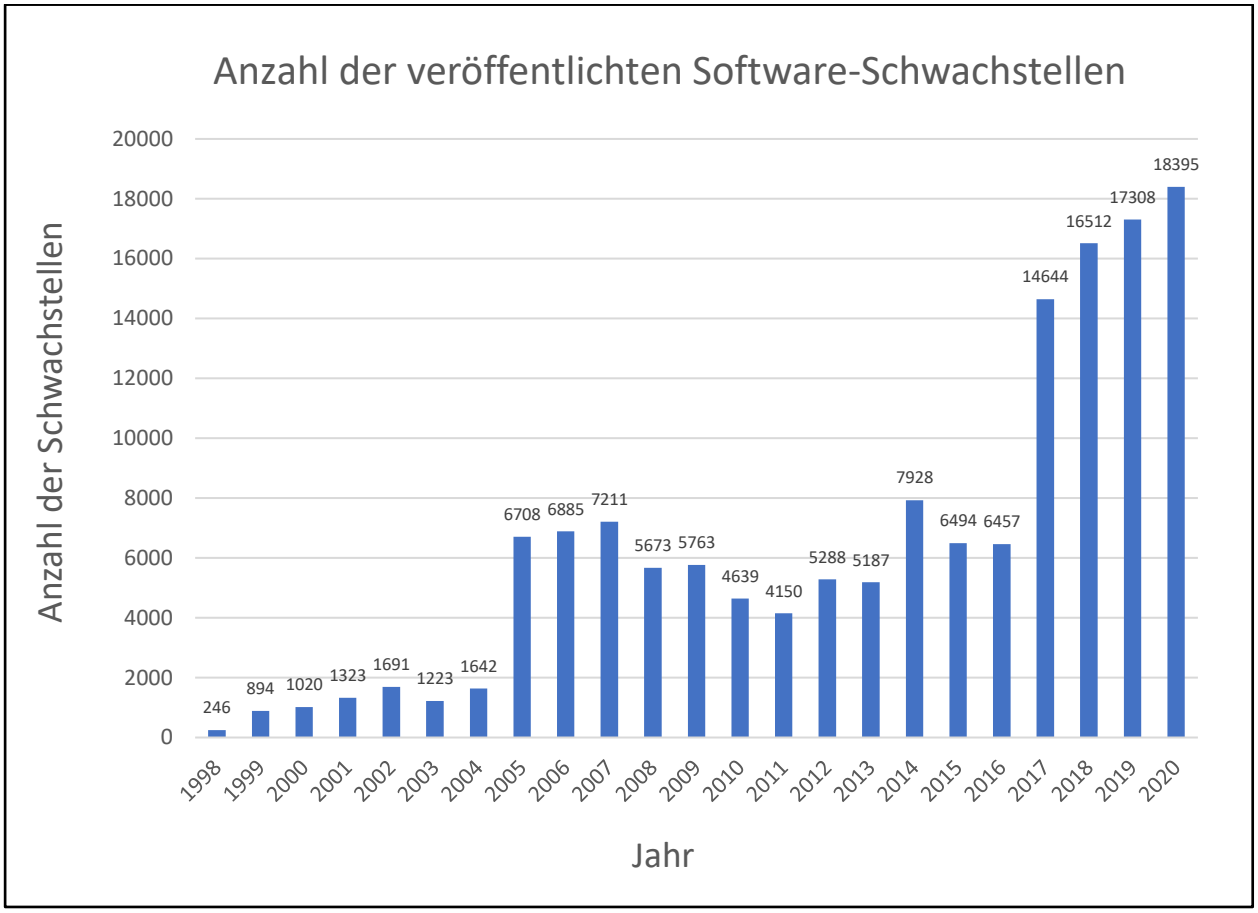

Abbildung 3: IT-Schwachstellen 1998-2020 (in Anlehnung an Bundeskriminalamt, 2022)

Wie auf Abbildung 3 zu erkennen ist, hat sich die Anzahl der benannten Software-Schwachstellen mehr als verdoppelt und steigt stetig weiter. Die Softwarequalität von Betriebssystemen und anderen Anwendungen ist laut Pohlmann (2022) für die heutige Bedrohungslage nicht mehr ausreichend. Er stellt fest, dass die Anzahl der Softwarefehler pro 1.000 Zeilen Code, bei qualitativ hochwertiger Software, im Schnitt bei 0,3 liegt. Gängige Betriebssysteme mit circa 10 Millionen Zeilen Code weisen hier im Schnitt 3000 Softwarefehler auf.

Die Zahl der Vorfälle, die durch Ausnutzung von Schwachstellen verursacht wurden, stiegen von 2020 auf 2021 um 33 Prozent. Vier der fünf am häufigsten ausgenutzten Schwachstellen wurden neu entdeckt. (Singleton et al., 2022). Im Umkehrschluss bedeutet das, dass eine dieser fünf Schwachstellen schon länger bekannt war, aber noch nicht geschlossen wurde. Solange dies der Fall ist, können weiterhin Angreifer diese Schwäche ausnutzen. Teilweise werden keine Sicherheitsupdates mehr zur Verfügung gestellt. So ist der Support für Windows 7 und Windows Server 2008 R2 bereits im Jänner 2020 eingestellt worden, obwohl diese Systeme durchaus noch verwendet werden. (Bundesamt für Sicherheit in der Informationstechnik, 2020b)

Ein Angriffsvektor, der speziell bei Unternehmen mit größerer IT-Infrastruktur eine Gefahrenquelle darstellt, sind VPN-Zugänge für die Fernwartung durch andere Unternehmen. Diese Firmen haben Zugriff zum System, um aus der Ferne Arbeiten zu erledigen. (Bundesamt für Sicherheit in der Informationstechnik, 2020b)

Der ungenügende Schutz vor Schadsoftware ist ein weiterer Punkt zu fehlender IT-Sicherheit. Die Erkennungsrate von Anti-Malware-Lösungen liegt bei Massenangriffen heutzutage bei 75 bis 95 Prozent. Sind dies bereits schwache Erkennungswerte, so fallen diese bei gezielten und direkten Angriffen im Schnitt sogar auf 27 Prozent. Pohlmann (2022) erklärt, dass die signaturbasierte Erkennung bei gezielten Angriffen ihre Wirkung verliert, weil keine Signaturen mehr verteilt werden und diese bei jedem direkten Angriff individuell sind.

Auch unsichere Webseiten stellen ein nicht unerhebliches Risiko für die Nutzer dar. Nur die wenigsten der Webseitenersteller haben das Fachwissen und die nötigen Finanzressourcen, um die nötigen Cyber-Schutzmechanismen einzubinden. Das Institut für Internetsicherheit hat festgestellt, dass auf 2,5 Prozent der begutachteten, deutschen Webseiten direkt oder indirekt Malware vorhanden war. Daraus ergibt sich eine große Angriffsfläche, besonders, wenn Webseiten großer Unternehmen Schwachstellen aufweisen. (Pohlmann, 2022)

Bei der Erkennung von unsicheren Webseiten sind gerade Smartphone-User im Nachteil. Durch das kleinere Display kann oft nicht alles auf dem Bildschirm dargestellt werden und dem User ist die Identifizierung einer illegitimen Domain sehr schwierig. (Huber, 2019)

Abbildung 4: Sicherheitsprüfung am Smartphone (Pohlmann, 2022)

Europol (2021) sieht neben dem Identitätsdiebstahl durch die Malware eine weitere Gefahr für Unternehmen, die ihren Mitarbeiterinnen und Mitarbeitern Smartphones zur Verfügung stellen.

So können vertrauliche Firmendaten, Kontakte oder andere schützenswerte Inhalte ausgelesen werden.

Doch nicht nur die Gefahr von kompromittierten Smartphones auch die zunehmende Vernetzung von Gegenständen mit dem Internet, dem sogenannten Internet of Things, hat die Angriffsfläche für Cyberattacken weiter signifikant verschärft. Ein durchschnittlicher Haushalt in Europa weist bereits 14 solcher IoT auf. Schwache Passwörter, teils ohne Möglichkeit einer Passwortänderung bilden hier die Sicherheitslücke. (Wirtschaftsagentur Wien, 2020)

Eine Schwachstelle, die laut Bundesministerium für Inneres in deren Cybercrime Report von 2021 eine der primären Infektionsvektoren darstellt, sind E-Mails. Schädliche Dateianhänge oder auch Links zum Nachladen schädlicher Software stellen User aber auch Systeme vor große Probleme. Die Echtheit eines Absenders beziehungsweise dessen E-Mail-Adresse als auch die Echtheit eines E-Mail-Inhaltes können nicht verifiziert werden. Es ist für den Empfänger nicht feststellbar, ob das E-Mail während der Sendung nicht manipuliert wurde. Auch weiß er nicht, ob der Sender die vorgegebene Person ist. (Pohlmann, 2022)
Die Deutschland sicher im Netz e.V. (2021) hat in einem Bericht, unter der Schirmherrschaft des deutschen Bundesministerium des Inneren, für Bau und Heimat, eine Wertung der in Deutschland registrierten Sicherheitsvorfälle im Jahr 2021 vorgenommen. Phishing-Versuche und der Erhalt von infizierten E-Mails belegen hier die ersten beiden Plätze. Ebenfalls wird hier erwähnt, dass über die Hälfte der Internetuser ein unsicheres Gefühl beim Öffnen von Anhängen in E-Mails haben. Deshalb wird in den Kapiteln 3.2.3 und 3.2.4 hier genauer auf die Möglichkeiten zum Schutz des E-Mail-Verkehrs eingegangen.

Auf technischer Seite hat sich das Spektrum der Angriffsmethoden stark erweitert. Vor allem im Bereich der Advanced Persistent Threats, also im Bereich der komplexen Angriffstechnologien.
Erfolgten APT-Angriffe früher hauptsächlich über E-Mail-Anhänge oder Links zu schadhaften Webseiten, so stellen nun die Kompromittierung von Softwareprodukten, das Ausnutzen von Schwachstellen in Fernwartungsdiensten oder das Ausspähen von Zugangsdaten das größte Potenzial für Angreifer dar. Viele dieser APTs versuchen über Schwachstellen von Zulieferern ihre eigentlichen Ziele zu kompromittieren. (Bundesamt für Sicherheit in der Informationstechnik, 2020b)

2.5 Schadensausmaße

In diesem Kapitel wird kurz auf das Schadensausmaß, welches durch Cyberattacken entsteht, eingegangen. Auch die Auswirkungen des mobilen Arbeitens auf das Schadenspotenzial wird aufgezeigt.

Im Cybercrime Report des Bundesministeriums für Inneres (2020) wird grafisch dargestellt, wie sich stetig die Anzahl der in Österreich begangenen Straftaten im Zusammenhang mit Cybercrime erhöht.

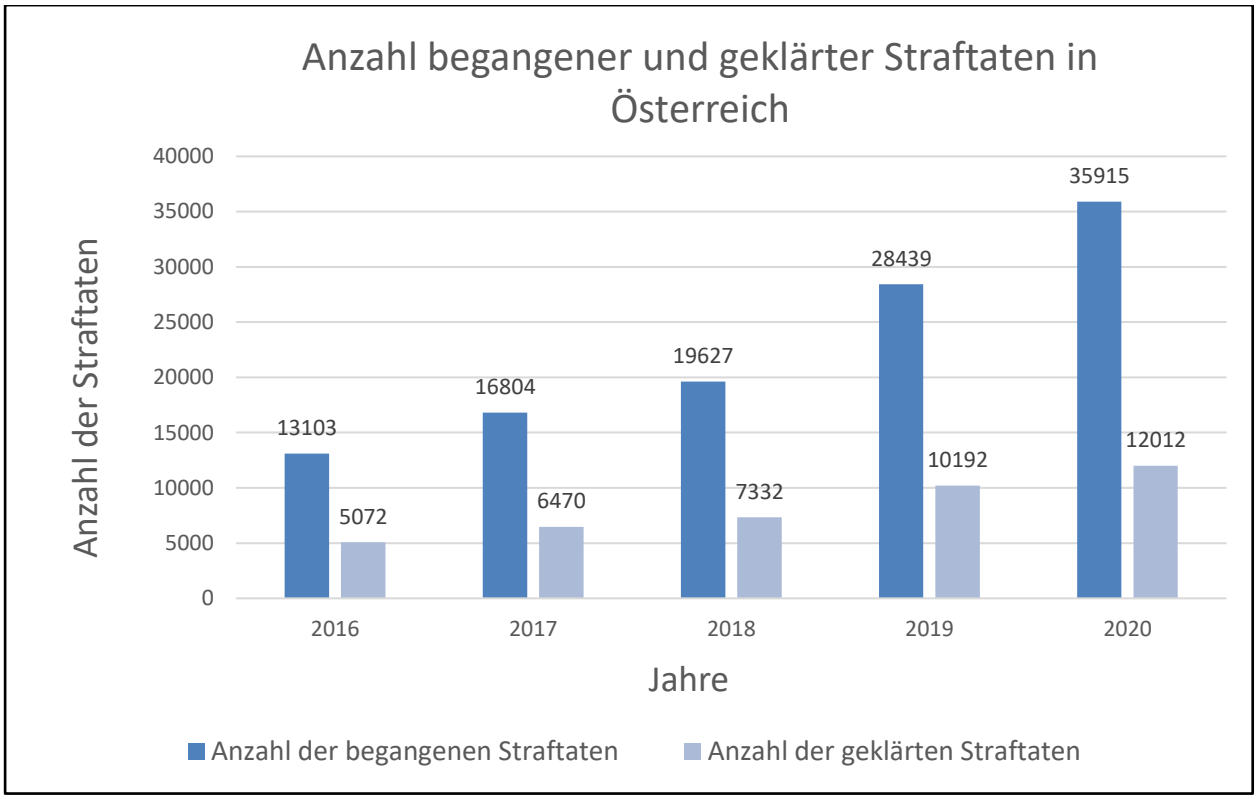

Abbildung 5: Cybercrime Straftaten Österreich (in Anlehnung an Bundesministerium für Inneres, 2020)

Waren es laut Abbildung 1 im Jahr 2016 noch knapp 13.000 Anzeigen, so stieg die Anzahl bis 2020 auf über 35.000 Anzeigen. Die Dunkelziffer wird hier vermutlich deutlich höher liegen. Auch 2021 scheint hier keine Grenze erreicht zu werden. So hat sich in Deutschland laut Bundeskriminalamt (2022) die Anzahl der erfassten Straften um 12 Prozent gegenüber 2020 erhöht.

Die größte Bedrohung blieben laut eines 2020 erstellten Berichtes des nationalen Computer Emergency Response Teams, kurz CERT, weiterhin Ransomware-Angriffe. Als wichtiger Faktor wird darin die Coronapandemie und die dadurch vielerorts eingeführten Homeoffice-Arbeitsplätze erwähnt. Die Möglichkeit, die Arbeitsgeräte effektiv zu schützen, wurde durch Einsatz von privaten Geräten und der grundsätzlichen Schwierigkeit, mobile Endgeräte sicher zu machen, noch weiter erschwert und eröffnet den Angreifern weitere Möglichkeiten.

Allein in Deutschland entstand so im Jahr 2021 ein Schaden von circa 24,3 Milliarden Euro aufgrund von Ransomware-Angriffen. Hingegen waren es 2019, vor der Coronapandemie, nur 5,5 Milliarden Euro. Das bedeutet, der Schaden hat sich innerhalb von zwei Jahren mehr als vervierfacht. (Bundeskriminalamt, 2022)

Unabhängig der Angriffsart war, wie in Abbildung 1 ersichtlich, beinahe ein Viertel der Schäden in Deutschland auf Cyberangriffe im Homeoffice zurückzuführen. (Engels, 2021)

Besonders gefährdet sind hier kleinere und mittelgroße Unternehmen, sogenannte KMUs. Allein im Jahr 2020 waren laut des Kapsch Cybersecurity Reports (2021) 80 Prozent der österreichischen KMUs von Cyberattacken betroffen. Bei 39 Prozent kam es dadurch auch zu finanziellen Schäden von bis zu 150.000 Euro. Das ist eine Steigerung gegenüber dem Vorjahr von 5 Prozent.

Die erpressten Beträge werden hier gezielt nach der Finanzkraft des kompromittierten Unternehmens ausgerichtet. Um der Zahlung Nachdruck zu verleihen, wird oft auch mit der Veröffentlichung der Unternehmensdaten gedroht. (Bundesministerium für Inneres, 2021)

Auch die Ziele von Cybercrime reichen laut Bundeskriminalamt (2022) durch alle Sparten. Neben öffentlichen Einrichtungen, dem E-Commerce, dem Gesundheits- und Bildungssektor sowie kritischen Infrastrukturen ist 2021 beinahe jede Branche Ziel von Cybercrime geworden.

3 MAßNAHMEN ZUR SCHADENSVERMEIDUNG

Dieses Kapitel soll zu den jeweiligen Angriffstypen, welche unter 2.3 aufgeführt wurden, Maßnahmen aufzeigen, mit denen Schäden beziehungsweise das Risiko einer Kompromittierung vermieden werden können. Dazu wird in dieser Arbeit eine Unterteilung der Sicherheitsmaßnahmen nach technischen und nicht technischen, sogenannten organisatorischen Maßnahmen, vorgenommen. Diese Maßnahmen sind in weiterer Folge in dieser Arbeit wichtig, da die Häufigkeit und der Grad der Umsetzung im empirischen Teil genauer betrachtet werden.

3.1 Organisatorische Sicherheitsmaßnahmen

Im Abschnitt 2.4.1 wurde bereits näher auf die Schwachstelle Nutzer eingegangen. Besonders in KMUs ist häufig das Bewusstsein bezüglich Cyberrisiken eher gering ausgeprägt, obwohl über 90 Prozent dieser Unternehmen wesentliche Geschäftsprozesse über Arbeitsplätze mit Internetzugang abwickeln. (Griesbacher & Griesbacher, 2020)

Um solche individuellen Fehler zu vermeiden, wird Unternehmen empfohlen, Verhaltensregeln zum Datenschutz zu formulieren. (Volkmer, 2021)

3.1.1 Verhaltensregeln

Volkmer (2021) erwähnt in diesem Paper auch die Notwendigkeit, diese Regeln auch an die gesamte Belegschaft zu kommunizieren und dies auch regelmäßig in Form von Sicherheitstrainings zu wiederholen.

3.1.2 Awareness-Schulungen

Awareness-Schulungen als nicht-technische Maßnahmen können das Bewusstsein der Nutzer gegenüber Cyberattacken stärken und dadurch die Leistung der technischen Lösungen stark verbessern. (Al-Daeef M.M. et al., 2017)

Der Erfolg von solchen Sicherheitsschulungen hängt dabei von der Bewusstseinsbildung der Mitarbeiterinnen und Mitarbeiter ab. Show et al. erwähnen hier 2009 die drei Stufen zur Erreichung eines Bewusstseins für Sicherheitsrisiken:

- Wahrnehmung

  Die Chancen, sich ein korrektes Bild von Bedrohungen zu machen, können durch die Verbesserung der Wahrnehmung des Sicherheitsbewusstseins erheblich gesteigert werden.

- Verständnis

  Benutzer müssen Gefahren, die von diversen Sicherheitsrisiken ausgehen, kennen, verstehen und richtig einschätzen können. Benutzer sollen aber auch in der Lage sein, diese Informationen verbreiten zu können, um die Bekämpfung der Sicherheitsrisiken zu verbessern. Highland (1995) erwähnt, dass in dieser zweiten Phase der Überzeugungs- und Argumentationsprozess, welcher nötig ist, um die Aufmerksamkeit des gesamten Unternehmens zu gewinnen, erleichtert wird.

- Projektion

  Endanwender müssen in der Lage sein, den zukünftigen Verlauf von Sicherheitsangriffen zu prognostizieren. Die Fähigkeit der Endnutzer, zukünftige Sicherheitsereignisse vorherzusagen, zeigt schlussendlich, dass sie ihr System und dessen Schutz auf hohem Niveau verstehen.

3.1.3 Notfallübungen

Bönsch (2021) berichtet, dass laut einer Studie des Bundesministerium für Sicherheit in der Informationstechnik, kurz BSI, nur 2 Prozent der Unternehmen Abläufe, die während einer Attacke auszuführen sind, durchspielen. Das Bundesministerium für Inneres (2021) empfiehlt hier das Erstellen solcher Notfallpläne samt Telefonlisten und das Festlegen von Kompetenzen.

Solche und ähnliche Basisanforderungen könnten in einem ganzheitlichen Informationssicherheitsmanagementsystem, kurz ISMS, festgelegt und niedergeschrieben werden. (Eckhart, 2021)

3.1.4 Information Security Management System

Als Management-System wird all das bezeichnet, was eingesetzt wird, um die wesentlichen Ziele für ein Thema zu ermitteln, um diese Ziele zu erreichen und deren Aufrechterhaltung zu überwachen. (Kersten et al., 2016)

Durch die Einführung eines ISMS, kann laut Eckhart (2021) der Schutz der Informationen, bezogen auf die Vertraulichkeit, Verfügbarkeit und Integrität, in einem Unternehmen oder Organisation gemanagt werden.

Kersten et al. (2016) nennen hier wichtige Aufgaben eines ISMS:

- die Formulierung von Zielen (Sicherheitszielen)
- die Bestimmung der Assets
- die Risikobeurteilung
- die Risikobehandlung
- die kontinuierliche Verbesserung

Wichtig bei der Einführung ist auch die Bestimmung des Geltungsbereiches. Jendrian (2014) schreibt dazu, dass das ISMS nicht immer für eine ganze Organisation gelten muss. Der sogenannte „Scope“ kann sich daher auch auf den IT-Bereich beschränken.

Auch eine Zertifizierung solcher Managementsysteme wird angeboten. Die weit verbreitete Zertifizierung nach ISO/IEC 27001 wird auf Basis des vom BSI entwickelten IT-Grundschutzes durchgeführt. Die darin enthaltenen Empfehlungen von Standard-Sicherheitsmaßnahmen stellen inzwischen einen De-Facto-Standard für IT-Sicherheit dar. (Bundesamt für Sicherheit in der Informationstechnik, 2020b)

All die genannten organisatorischen Maßnahmen bewegen sich jedoch auf einer Unternehmens- bzw. Organisationsebene. Aber auch auf Staats- beziehungsweise EU-Ebene wird an Richtlinien und Vorschriften gearbeitet, die dem Schutz vor Cybercrime dienen sollen. So berichtet das Bundeskanzleramt (2021) über die österreichische Strategie für Cybersicherheit, kurz ÖSCS 2021. Diese schuf, basierend auf der ÖSCS 2013, die wesentlichen Strukturen und Prozesse für den Aufbau einer umfassenden Cybersicherheitspolitik auf europäischer und internationaler Ebene. Einen Teil dieses Rahmenwerkes bildet hier die Richtlinie für Netz- und Informationssystemsicherheit, kurz NIS-Richtlinie.

3.1.5 NIS-Richtlinie

Die Europäische Kommission hat im Dezember 2020 die neue Netz- und Informationssystemsicherheit-Richtlinie vorgelegt, um ein hohes, gemeinsames Sicherheitsniveau in der EU zu erreichen. (Cert.at, 2020) Im Fokus dieser Richtlinie steht dabei die Definition von einheitlichen Sicherheitsstandards und Meldewegen für Unternehmen, welche für einen funktionierenden Binnenmarkt essenziell sind. In Österreich wurde hierfür das Netz- und Informationssystemsicherheitsgesetz NISG umgesetzt.(Bundeskanzleramt, 2021)

In der Erläuterung des NIS-Gesetzes aus dem Jahr 2018 werden folgende Hauptgesichtspunkte des Gesetzes genannt:

- Festlegen von Aufgaben, Behördenzuständigkeiten und Befugnissen
- Festlegen einer nationalen Strategie für Netz- und Informationssicherheit
- Ermittlung von Betreibern wesentlicher Dienste

- Regelung von Verpflichtungen für die ermittelten Betreiber
- Überprüfung geeigneter Sicherheitsvorkehrungen und der Einhaltung der Meldepflicht
- Einrichtung von Computer-Notfallteams und Festlegung derer Aufgaben
- Regelung von Strukturen und Aufgaben im Falle einer Cyberkrise
- Festlegung der Sanktionen bei Nichteinhaltung der einzuhaltenden Pflichten

Pohlmann (2022) stellt fest, dass ein Paradigmenwechsel vollzogen werden muss, da die vorhandenen Cyber-Sicherheitsmaßnahmen die Risiken nicht ausreichend reduzieren. Er sieht hier auch die Technologiehersteller in der Pflicht und fordert diese dazu auf, Verantwortung für Cybersicherheit und die Vertrauenswürdigkeit ihrer IT-Lösungen zu übernehmen. Verantwortung versus Gleichgültigkeit. Dieser Grundsatz würde die Unternehmen dazu zwingen, ihre Systeme besser aufeinander abzustimmen und Fehler leichter ausfindig zu machen.

3.2 Technische Sicherheitsmaßnahmen

Dieser Abschnitt soll die technischen Maßnahmen zur Vermeidung von Cyberrisiken genauer beleuchten. In Abschnitt 2.3, Typen von Cyberangriffen, wurden die einzelnen Gefahren erarbeitet. In diesem Bereich der Arbeit sollen nun die passenden Verfahren zum Schutz vor diesen Angriffstypen aufgelistet und beschrieben werden. Auch auf spezielle Sicherheitsverfahren zum Schutz bei der Telearbeit wird hier näher eingegangen.

3.2.1 Basisschutz

Henseler-Unger et al. (2018) listen technische Maßnahmen auf, die als Basisschutz in Unternehmen eingesetzt werden sollten.

Virenschutz, Passwörter als auch der Einsatz einer Firewall werden laut ihrer Umfrage unter 1505 Unternehmen bereits in über 94 Prozent aller KMUs eingesetzt. Daher wird auf eine genauere Betrachtung dieser Maßnahmen verzichtet. Die genaue Aufschlüsselung ist in Abbildung 6 ersichtlich.

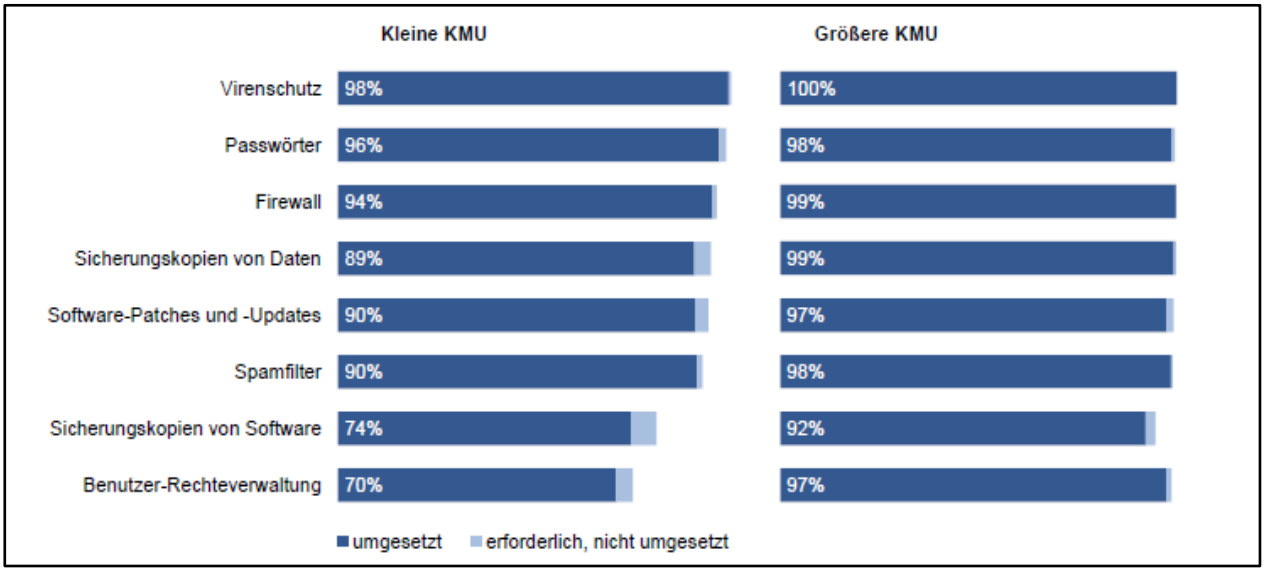

Abbildung 6 - Technische Maßnahmen des Basisschutzes (Henseler-Unger et al., 2018)

Fox (2021) berichtet in einem Artikel neben der Awareness der Mitarbeiterinnen und Mitarbeiter ebenfalls von dem im Basisschutz enthaltenen „üblichen“ Schutzmaßnahmen.

3.2.2 Regelmäßige Updates der Systeme

Auch das Bundesministerium für Inneres (2021) erwähnt, neben den organisatorischen Maßnahmen das regelmäßige Einspielen von Security Updates bei allen verwendeten Programmen beziehungsweise Systemen als essenziell.

Gerade kleine KMUs haben hier laut Henseler-Unger et al. (2018) Nachholbedarf. Jedes Zehnte von Ihnen führt keine regelmäßigen Software-Patches und Updates durch.

Oft wird aus Systemstabilitätsgründen oder auch Lizenzgründen darauf verzichtet. 2020 waren vor allem Instanzen von Microsoft Exchange Servern und diverse Firewall Produkte mit deren VPN-Lösungen durch öffentliche Exploits vielversprechende Angriffsziele. (Cert.at, 2020)

Um die Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme aufrecht zu erhalten, ist es laut Mett et al. (2005; Mell et al., 2005) nötig, Prozesse zur Verwaltung von Software-Sicherheitspatches zu etablieren. Abbildung 7 veranschaulicht die fünf Hauptphasen eines Software-Sicherheits-Patchmanagement-Prozesses.

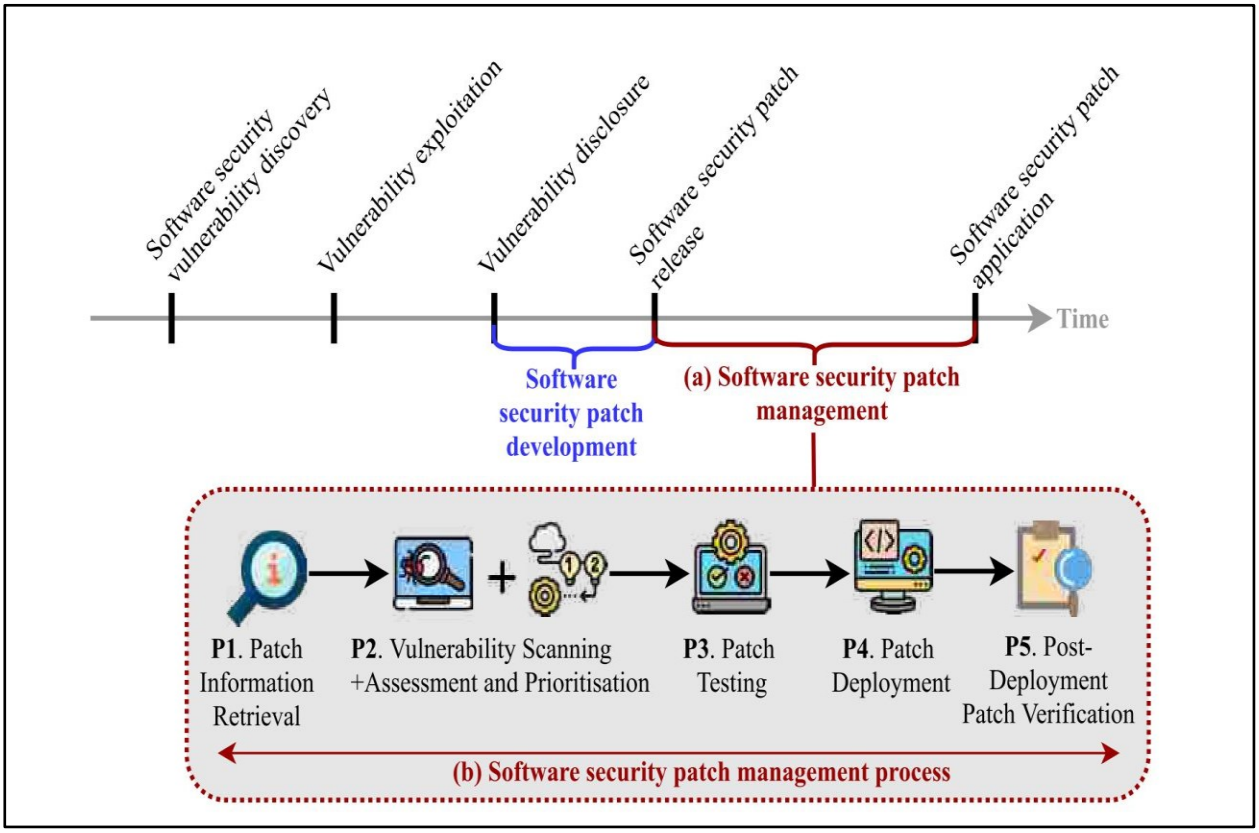

Abbildung 7: Software Security Patchmanagement (Dissanayake et al., 2022)

In der ersten Phase, der Patch-Informationsbeschaffung, erfahren Fachleute von neuen Patches und erwerben diese. Die nächste Phase behandelt das Scannen, Beurteilen und Priorisieren von Sicherheitslücken, um die Anwendbarkeit der Patches festzulegen. Auch die Risikoeinschätzung wird hier vorgenommen. Anschließend erfolgt die Patch-Testphase. Dabei wird die Stabilität der Patches getestet, werden die Systeme für die Installation vorbereitet und Sicherungskopien erstellt. In der Patch-Verteilungsphase werden diese auf den Ziel-Systemen ausgerollt. In der letzten Phase, der Patch-Verifizierung, werden die Patches überwacht, ob eventuelle Dienstunterbrechungen vorliegen. (Dissanayake et al., 2022)

Natürlich können auch Patchmanagement-Tools bei der Erkennung von Patchproblemen helfen. Zum Beispiel stellt Microsoft die Windows Server Update Services, kurz WSUS, zur Verfügung. Dieser stellt IT-Verantwortlichen die aktuellen Microsoft-Produktupdates, welche über Microsoft Update zur Verfügung gestellt werden, bereit. Somit kann dieser Service die Verteilung der Updates im gesamten Firmennetz vollständig verwalten. (Gerend, 2022)

Es gibt aber auch eine Vielzahl an Drittanbietern, die Alternativen zur Verfügung stellen. Stethi (2022) listet auf der Webseite Geekflare folgende zehn Alternativen auf:

- ManageEngine Patch Manager Plus
- SolarWind Patch Manager
- Heimdal

- NinjaOne
- Jetpatch
- Automox
- Action1
- Jumpcloud
- GFI LanGuard
- Atera's Patch Management

3.2.3 E-Mail-Filterung

Beim Filtern von E-Mails sollte eine Unterscheidung vorgenommen werden. Während es sich laut Enisa Threat Landscape - Spam (2020) beim sogenannten Phishing um gezielte Aktionen handelt, bei denen Social Engineering-Taktiken angewendet werden, ist Spam eine Taktik zum Senden unerwünschter E-Mails an eine Massenliste. Wie schon in Kapitel 2.3.1 erwähnt, steht beim Social Engineering die Anfälligkeit des Users im Vordergrund. Beim Spam versucht man, Benutzer mit gefährdeten Webseiten zu verknüpfen, um Malware zu installieren oder personenbezogene Daten zu stehlen.

Um die Zustellung solcher Spamnachrichten zu vermeiden, werden sogenannte Spamfilter eingesetzt. Siller (2018b) erwähnt hier drei verschiedene Methoden der Filterung.

- Blacklist-Methode

  Hierbei wird der Inhalt der E-Mail nach bestimmten Ausdrücken beziehungsweise Stichworten, welche auf einer sogenannten Blacklist stehen, durchsucht. Das gleiche wird beim Absender durchgeführt.

- Bayes-Filter-Methode

  Hier wird ein selbsterlernender Filter nach der bayesschen Wahrscheinlichkeitstheorie verwendet. Der User muss Vorarbeit leisten und das System anlernen.

- Datenbankbasierende Lösungen

  Diese versuchen aufgrund des Uniform Ressource Locators, kurz URL, welche in den E-Mails beworben werden, Spam zu erkennen.

Trendmicro (2021) erwähnt in einem Bericht, dass weitere Hilfsmittel hilfreich sind, um solche E-Mails vor dem Erreichen des Users abzufangen.

- Threat Intelligence

  Zum Beispiel verwendet Microsoft laut Kjerland et al. (2023) Microsoft Defender für Office 365, früher Advanced Threat Protection, um Unternehmen vor böswilligen Websites zu

schützen, welche von Usern über Links in E-Mails angeklickt werden. Weiters unterstützt diese Advanced Threat Protection den Schutz für sichere Anlagen, da eine Erkennung für den Enduser nicht einfach ist.

- Machine learning

  Dada et al. erwähnen in einem Paper von 2019, welches Machine learning zur E-Mail-Filterung als Thema hat, dass die führenden E-Mail-Anbieter die Kombination von verschiedenen Techniken des maschinellen Lernens in ihren Spamfiltern anwenden. Als Beispiel werden neurale Netzwerke genannt. Auch Pohlmann (2022) sieht in der Verwendung von künstlicher Intelligenz, kurz KI, großes Potenzial, Spammails effektiv klassifizieren zu können. Dadurch wird das Automatisierungspotenzial erhöht und eine Entlastung von IT-Spezialisten erreicht.

- Sandboxing

  Als Beispiel dient hier die bereits bei Threat Intelligence erwähnte Advanced Threat Protection von Microsoft. Diese arbeitet laut Joos (2018) mit einem Sandbox Verfahren. Hierbei werden potenziell gefährliche Anhänge und Links in einem geschlossenen Container getestet. Bei schädlichem Verhalten wird die Malware entsprechend blockiert. Die Tests führen jedoch zu verzögerter Zustellung der E-Mails. Eine weitere Sandboxing Funktionalität wird von Davis et al. (2023) auf der Microsoft Learn Webseite vorgestellt. Es handelt sich dabei um die Funktionalität „Sichere Links“. Hierbei wird jeder Link in einer Nachricht so umschlossen, dass dieser auf den Microsoft Safe Links-Server verweist. Bei einem Klick auf den Link wird dieser asynchron in eine Sandbox umgewandelt und dort überprüft.

3.2.4 Verschlüsselung von E-Mails

Pohlmann (2022) erwähnt in einem seiner Bücher, dass 43 Prozent aller E-Mails in Businessprozessen verwendet werden und aus diesem Grund den Mitarbeiterinnen und Mitarbeitern im Unternehmen eine E-Mail-Verschlüsselungstechnologie zur Verfügung gestellt werden sollte. Hier sind zwei Standards maßgeblich. Einerseits Secure/Mulitpurpose Internet Mail Extension, kurz S/MIME, welcher vermehrt in großen Unternehmen verwendet wird. Zum anderen Open Pretty Good Privacy, kurz OpenPGP, der ohne zusätzliche Server auf den IT-Systemen des Anwenders betrieben werden kann.

- S/MIME

  Dieser Standard ist bereits in vielen E-Mail-Programmen integriert und muss nur aktiviert werden. Im Menü des E-Mail-Programms sind danach zwei Auswahlfelder vorhanden, über die die Signatur und die Verschlüsselung eingestellt werden können. Die benötigten Schlüsselpaare können dabei aber nicht durch den User erzeugt werden, sondern müssen über Organisationen und Firmen kostenpflichtig bezogen werden. Daher ist dieses Verfahren eher in größeren Unternehmen und Behörden im Einsatz. (Bundesamt für Sicherheit in der Informationstechnik, 2023)

- OpenPGP

  Bei diesem Standard spricht das Bundesamt für Sicherheit in der Informationstechnik (2023) von einer kommerziellen Verschlüsselungssoftware, bei der alle Schlüssel vom Nutzenden selbst erzeugt und verwaltet werden können. Bei der Anwendung der Schlüssel unterstützt entweder das E-Mail-Programm direkt oder es muss ein Plugin dafür installiert werden.

Obwohl die Verschlüsselung Vertraulichkeit bietet, wird der Absender damit nicht authentifiziert. Um eine Identität des Absenders nachzuweisen, muss die Nachricht laut Hendrickson (2023) eine digitale Signatur verwenden.

Pohlmann stellt diesbezüglich fest, dass mit Hilfe einer solchen digitalen Signatur, auf Basis eines Public-Key-Verfahrens, eine gesetzliche Verbindlichkeit von E-Mails realisierbar ist.

3.2.5 Rechteverwaltung

Ein wichtiger Punkt, der laut Henseler-Unger et al. (2018) im Kapitel 3.2.1 Basisschutz auftauchen sollte, wird hier einzeln nochmals betrachtet. In ihrer Studie zum Basisschutz (Abbildung 6) ist zu erkennen, dass gerade im Bereich der kleineren KMUs hier nur rund 70 Prozent über eine Rechteverwaltung verfügen.

Berghoff (2020) meint dazu in einem Experteninterview, dass ein zentrales Management, mit dem sich sehr granulare Benutzerrechte vergeben lassen, ein Vorteil wäre, da interne und externe Anwender nur Zugriff auf die Daten und Programme haben, die für ihre Aufgaben relevant sind.

Vor allem in Bezug auf mobiles Arbeiten erwähnt Pohlmann (2022) die Notwendigkeit einer Rechteverwaltung, da durch diese festgelegt werden kann, mit welchen Protokollen und Diensten zu welchen Zeiten über das Firewall-System eine Kommunikation des externen Users mit dem internen System stattfinden darf.

3.2.6 Backup

Fox (2021) nennt als wichtige Schutzmaßnahme bei Ransomware-Angriffen den Einsatz von Backups. Meist wird das Thema Backup interessant, wenn der Angreifer bereits die digitale Infrastruktur lahmgelegt hat. Evers (2022) zeigt in seinem Artikel die Problematik für die Unternehmen auf. Einziger Ausweg geforderten Lösegeldzahlungen zu entgehen, ist die Datenrettung von etwaigen, nicht verschlüsselten Backupsystemen. Dabei erwähnt Evers die Wichtigkeit von zyklischen Offline-Backups wie beispielsweise Tapes, externe Festplatten oder Offline-Storage-Backups. Permanent verbundene Systeme wie NAS-Storages oder Cloud-Speicher sieht er problematisch, da die Gefahr einer automatischen Sicherung der verschlüsselten Dateien hoch ist.

Um ein Backup ideal aufzubauen, empfiehlt Jung (2021), die Faustregel 3-2-1 zu verwenden. Dabei sollte jedes Backup in dreifacher Ausführung, über mindestens zwei Medien hinweg,

abgelegt sein. Eine der Kopien soll dabei extern aufbewahrt werden. Zu dieser altbekannten Regel sollten laut dem Artikel von Jung noch zwei weitere Punkte aufgenommen werden. Dabei sollte einerseits eine Kopie mittels Datei-Attribut unveränderlich abgespeichert werden. Andererseits muss regelmäßig versucht werden, diese Backups wiederherzustellen, um die einwandfreie Funktion gewährleisten zu können.

3.2.7 Sichere Gestaltung von Softwareprodukten

Auch selbst entwickelte Software spielt im Kontext von Cybersecurity eine wichtige Rolle. Das Bundesamt für Sicherheit in der Informationstechnik (2020b) empfiehlt hier zur sicheren Gestaltung der Softwareprodukte die Umsetzung der Designphilosophien „Security by Design“ und „Security by Default“.

- Security by Design

  Diese Philosophie setzt bereits bei Beginn der Softwareentwicklung an und wird im gesamten Produktlebenszyklus berücksichtigt. Der Stellenwert der Sicherheit wird hier der Nutzerfreundlichkeit gleichgestellt, in sensiblen Bereichen sogar als höher definiert.

- Security by Default

  Bei Auslieferung von Software ist in diesem Fall die sicherste Konfiguration die Standardeinstellung (Default). Weist die initiale Konfiguration Fehler auf, werden diese oft nicht angepasst und bieten daher Angreifern einen Angriffspunkt. (Bundesamt für Sicherheit in der Informationstechnik, 2020b)

Die bisher im Kapitel 3.2 erarbeiteten Sicherheitsmaßnahmen bilden jedoch nur den bereits erwähnten Basisschutz. In den folgenden Unterkapiteln werden weitere, gerade in Bezug auf Cybersicherheit im Homeoffice, wichtige Sicherheitsvorkehrungen genauer betrachtet.

3.2.8 Mobile Device Management

Wird in dieser Masterarbeit von einem „Mobile Device“ oder einem „mobilen Endgerät“ gesprochen, so bezieht sich dieser Ausdruck auf die Definition, welche das Bundesamt für Sicherheit in der Informationstechnik (2022, S. 6) in ihrem Bericht zu Mindeststandards für Mobile Device Management, kurz MDM, verwendet.

> „Unter dem Begriff mobile Endgeräte versteht dieser Mindeststandard Smartphones und Tablets mit einem Betriebssystem (z.B. Android oder iOS), das für den mobilen Einsatz angepasst ist.“

Geräte mit Betriebssystemen für den Desktopbereich liegen daher außerhalb der Betrachtung, da solche Geräte sehr eng mit zusätzlichen Diensten, wie zum Beispiel Active Directory verknüpft und über diese verwaltet werden.

Während Personal Computer, kurz PC, und Serversysteme meist über erprobte und weit entwickelte Sicherheitsvorkehrungen sowie homogene Betriebssysteme verfügen, sind hier bei mobilen Endgeräten laut Eckhart (2021) Mischformen im Einsatz. Weiters wird es für die IT immer herausfordernder, die Gesamtheit dieser mobilen Geräte zu überblicken. Teilweise greifen daher firmenfremde Geräte auf Unternehmensdaten zu, ohne dabei kontrolliert zu werden.

Auch befinden sich PCs und Server nicht selten in überwachten Bereichen im Unternehmen. Mobile Geräte werden hingegen stets mitherumgeführt. Daher sind diese einem weitaus größerem Risiko des Verlustes oder des Diebstahls ausgesetzt. Ein vollständiger Schutz der darauf gespeicherten Daten ist daher nicht möglich. (Büllingen et al., 2009)

Wie bereits im Kapitel 2.4.2 erwähnt, ist auch eine Sicherheitsprüfung am mobilen Endgerät nur bedingt möglich. Wie dort in Abbildung 4 gezeigt wird, ist durch die Größe des Displays oft nicht genügend Platz, um gefährliche Webseiten zu erkennen. Wie Pohlmann (2022) in diesem Kapitel bereits zitiert wurde, ist auf jeder fünfzigsten deutsche Webseite direkt oder indirekt Malware vorhanden. Dies stellt in Verbindung mit der Erkennbarkeit ein weiteres Risiko dar.

Unabhängig von der Produktauswahl ist es laut Bundesamt für Sicherheit in der Informationstechnik (2022) wichtig, eine Strategie für den Einsatz eines solchen Mobile Device Management Systems, kurz MDMS, zu erstellen.

Die im Bericht erwähnten Fragen hierzu kurz zusammengefasst:

- Wie soll das MDMS in das Netzwerk eingebunden werden?
- Welche Maßnahmen zur Absicherung des MDMS sollen getroffen werden?
- Welche mobilen Endgeräte werden erlaubt?

Laut Kersten und Klett (2017) gibt es zwei Modelle, wie ein MDM eingeführt werden kann. Einerseits nach dem klassischen Client-Server-Modell, bei dem auf dem Endgerät ein Software-Agent installiert wird, der die Kommunikation zum zentralen Managementserver abwickelt. Andererseits kann ein MDM auch in Form eines Software as a Service, kurz SaaS, von einem Cloud Service Provider bezogen werden.

Kersten und Klett (2017) zählen folgende Features eines MDM auf:

- die Inventarisierung der mobilen Geräte
- das Ausrollen von Policies
- die Verteilung von Patches, Updates und Applikationssoftware
- das Backup und den Restore
- die Prüfung der Einhaltung bestehender Sicherheitsrichtlinien

- das Sperren eines mobilen Geräts und das Löschen sensibler Daten sowie
- das Incident- und Problem-Management

3.2.9 Schutz vor Schwachstelle IoT

Ebenfalls in Kapitel 2.4.2 wurden die Gefahren durch IoT-Geräte erwähnt. In dieser Arbeit wird nicht auf den grundsätzlichen Schutz in Unternehmen gegen Schwachstellen durch IoT-Geräte eingegangen, sondern nur auf den für die Arbeit relevanten Bereich der Telearbeit. Die genannten Maßnahmen sollen nur dem privaten Netzwerk dienen, um dieses gegenüber Angriffen zu härten und keine Einfallsmöglichkeit in das Firmensystem zu bieten. Kulkarni (2021) beschreibt in einem Zeitungsbericht folgende Vorsichtsmaßnahmen:

- ändern der Standardeinstellungen des privaten Routers
- IoT-Geräte vom Netz trennen, wenn diese nicht benötigt werden
- ändern der Standardpasswörter von IoT-Geräten auf neue, einzigartige Passwörter
- deaktivieren der Universal Plug and Play - Funktion, kurz UPnP, um die Geräte nicht außerhalb des Netzwerks sichtbar zu machen
- Software- beziehungsweise Firmwarestand aktuell halten

4 TELEARBEIT

In diesem Kapitel werden wiederum zunächst die theoretischen Grundlagen zum Thema Remote-Arbeitsplatz erläutert. Beginnend mit der Definition der Begrifflichkeiten werden danach die Auswirkungen auf die IT-Sicherheitskonzepte genauer beschrieben.

4.1 Definitionen

Um im Verlauf der weiteren Arbeit zu verstehen um welche Art des „externen Arbeitens“ es sich handelt, werden in diesem Kapitel die Unterschiede der Begrifflichkeiten herausgearbeitet.

Der österreichische Gesetzgeber hat bislang weitgehend darauf verzichtet, „Homeoffice“, „Telearbeit“ oder vergleichbare Begriffe genau zu definieren. Das Beamtendienstrecht kennt seit der 2. Dienstrechts-Novelle 2018 in § 36a BDG den Begriff „Telearbeit“. Auch in Kollektivverträgen finden sich Regelungen und meist unterschiedlich lautende Begriffsbestimmungen dazu. Auch im Home-Office-Maßnahmenpaket 202145 findet sich bislang ebenfalls keine Begriffsdefinition dazu. (Endres, 2021).

4.1.1 Homeoffice

In § 2h des Arbeitsvertragsrechts-Anpassungsgesetzes (2021) wird Homeoffice folgendermaßen erwähnt:

> „Arbeit im Homeoffice liegt dann vor, wenn eine Arbeitnehmerin oder ein Arbeitnehmer regelmäßig Arbeitsleistungen in der Wohnung erbringt.“

Der Begriff Homeoffice beschreibt grundsätzlich die Situation von Arbeitnehmern, die zumindest einen Teil ihrer Arbeitsleistung von der eigenen Wohnung aus erbringen. (Bertram et al., 2021)

Sturm (2021) erwähnt, dass die Arbeit im Homeoffice nach § 2h Abs 1 AVRAG in einer Privatwohnung verrichtet wird. Dies kann die eigene Wohnung des Arbeitnehmers, der Zweitwohnsitz, die Wohnung des Partners, der Eltern und so weiter sein.

Typischerweise handelt es sich dabei um Bürotätigkeiten. Da es Arbeitnehmern und Arbeitgebern freisteht, über Dauer und Umfang selbst zu entscheiden, kommt es hier zu verschiedenen Varianten der Tätigkeit: Von anlassbezogenem- über teilweisen- bis hin zum ausschließlichen Homeoffice. (Bertram et al., 2021)

4.1.2 Remote working

Wird die Arbeit außerhalb der betrieblichen Räumlichkeiten an einem beliebigen Ort, aber eben nicht in der Privatwohnung verrichtet, sondern beispielsweise im Café ums Eck oder im Freibad, dann handelt es sich, laut Sturm (2021), um Remote working.

4.1.3 Telearbeit

Der Begriff „Telearbeit“ wird in der Regel als Oberbegriff für Homeoffice und Mobile Working verwendet. Im Homeoffice erfolgt die Arbeitsleistung, wie in Kapitel 4.1.1 erwähnt, an einem fixen Arbeitsort, nämlich in der Wohnung der Arbeitnehmerin bzw. des Arbeitnehmers. Beim Mobile Working sind die Beschäftigten hinsichtlich der Wahl ihres Arbeitsortes nicht auf die Wohnung beschränkt.

Der Begriff Telearbeit kann in drei verschiedene Formen unterteilt werden, welche die Begriffe Homeoffice und Mobile Working miteinschließen. (Institut für Wissen in der Wirtschaft, 2018, 2018)

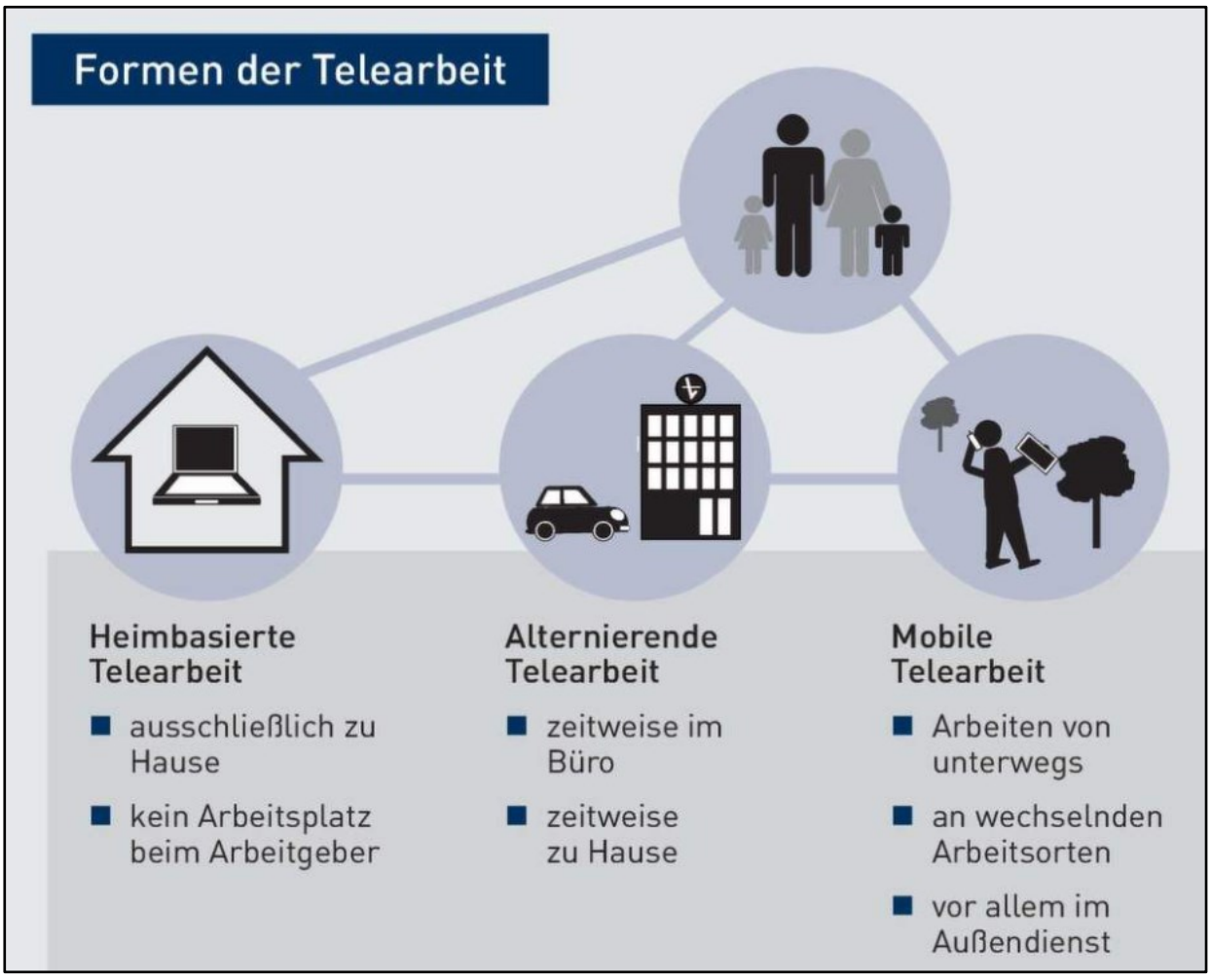

Abbildung 8 - Formen der Telearbeit (Institut für Wissen in der Wirtschaft, 2018)

Um alle Aspekte des „externen Arbeitens“ abzudecken, wird in dieser Arbeit die Definition der Telearbeit als Basis für alle Ausarbeitungen herangezogen. Ausnahme bilden hier Zitate, in denen die Begrifflichkeiten laut Quelle verwendet werden.

4.2 Nötige Anpassung von IT-Sicherheitskonzepten

Unternehmen müssen aufgrund geänderter Anforderungen durch die Telearbeit reagieren und ihre IT-Konzepte anpassen. In diesem Unterkapitel wird auf die gängigsten Maßnahmen zum Schutz vor Cyberrisiken während der Telearbeit eingegangen.

4.2.1 Bring your own device

Porath (2020) definiert bring your own device, kurz BYOD, als die Verwendung des eigenen, privaten, Gerätes innerhalb des Firmennetzwerks. Er erwähnt auch, dass es zwar von vielen Firmen in den letzten Jahren ermöglicht und akzeptiert wurde, jedoch aber auch ein Sicherheitsrisiko darstellt.

Bergler (2017) geht bei der Definition weiter und erklärt, dass BYOD für eine IT-Richtlinie steht, welche die Nutzung privater Endgeräte wie Smartphones und Notebooks durch Mitarbeiterinnen und Mitarbeiter für dienstliche Zwecke regelt. In diesem Artikel wird explizit auf die Unerlässlichkeit einer solchen Richtlinie hingewiesen, denn nur wenn die Bedingungen für den Einsatz von privaten Geräten klar definiert sind, ist auch die Frage der Haftung eindeutig geregelt.

Einige Probleme bei dem Einsatz von BYOD erwähnt Hayes (2013):

- erhöhte Komplexität des firmeneigenen IT-Support
- mögliche Kompatibilitätsprobleme bei firmeneigenen Softwaresystemen
- fehlende Abgrenzung von persönlichen und beruflichen Informationen
- Problematik des regelmäßigen Aktualisierens der Systeme

Da jedes dieser Endgeräte, welche Zugriff auf betriebliche Daten haben, ein theoretisches Sicherheitsrisiko darstellt, sollte in solchen Fällen ein Mobile Device Management implementiert werden. Ein solches, bereits in Kapitel 3.2.8 angeführtes, Managementsystem stellt für all diese Geräte eine zentrale Verwaltungseinheit dar. Ein MDM ermöglicht auch die Löschung der Daten bei Verlust oder Diebstahl und ist daher eine wirksame Absicherung. (Proofpoint, 2022)

Kersten et al. (2016) erwähnen jedoch, dass gerade aus Sicht der Informationssicherheit dringend angeraten wird, so weit als möglich, auf die Anwendung von BYOD zu verzichten.

4.2.2 Virtual Private Network

Bereits (1999) erklärte Badach, dass sich mittels der Virtual Private Network -Technologie die Unternehmensnetze ausdehnen lassen. So kann ein solches Netz übers Internet beziehungsweise über ein anderes, öffentliches IP-Weiterverkehrsnetz beliebig räumlich erweitert werden, ohne weitere Sicherheitsrisiken zu erzeugen.

Virtual Private Networks, kurz VPNs, sind in der Netzkommunikation eine wichtige Komponente. Im Gegensatz zu herkömmlichen Netzen sind VPNs durch die Eigenschaften privat und virtuell erkennbar. Die Begrifflichkeiten privat und virtuell haben laut Bök et al. (2020) jeweils zwei Bedeutungen.

- privat
    - Obwohl bestehende Kommunikationskanäle genutzt werden, ist ein solcher VPN eigenständig, das bedeutet, abgetrennt von jeglicher anderen Kommunikation auf diesem Kanal.
    - Vertraulichkeit, Authentizität und Integrität: Die Kommunikation über VPNs ist vertraulich durch den Einsatz von Verschlüsselung. Authentizität entsteht durch das Wissen, die Gegenstelle des VPNs zu kennen. Integrität bedeutet die Daten sind vor Veränderung durch Dritte geschützt.
- virtuell
    - Es sind keine dezidierten Kommunikationskanäle wie Hardware und Verkabelung notwendig.
    - Bedeutet Transparenz, da der Endbenutzer bis auf die fehlende Verkabelung keinen Unterschied zu einem herkömmlichen Netz erkennen kann.

Um Heim- und Außendienstmitarbeiterinnen und -mitarbeiter sicher in die Unternehmensnetze integrieren zu können, werden heute meist VPNs in Form von Softwareclients genutzt. Auch die Verbindung von ganzen Netzwerken wird mittels VPN-Gateways an den Zugangspunkten der Netzwerke zum Internet ermöglicht. VPN-Technologien setzen auf Nutzer-Authentifikation sowie verschlüsselte und integritätsgesicherte Datenübertragung durch Internet Protocol Security (IPSec) und Transport Layer Security (TLS) oder der Vorgängerbezeichnung Secure Sockets Layer (SSL). (Pohlmann, 2022)

Steinmann (2018) unterscheidet die Verwendung der einzelnen VPN-Arten folgendermaßen: IPSec-VPNs werden hauptsächlich zum Verbinden von verschiedenen Standorten in Unternehmen verwendet. Die Kommunikation läuft dabei über die Netzwerkschicht und kann sämtliche IP-Protokolle übertragen.

SSL-VPNs wurden hingegen für die mobile Arbeit entwickelt. Die wird nicht zwingend über einen Client durchgeführt, er kann zum Beispiel auch per Browser verwendet werden.

Das Bundesamt für Sicherheit in der Informationstechnik (2020b) gibt die Empfehlung, VPN-Lösungen für den Zugriff auf berufliche Dokumente anderen Lösungen wie Dateiversand und öffentlichen Cloud-Diensten, vorzuziehen.

Jedoch sind auch VPN-Technologien kein vollständiger Schutz. Pohlmann (2022) erwähnt hier die Gefahr von durch Malware kompromittierten IT-Systemen. Da eine Überprüfung der Integrität des IT-Systems fehlt, gibt es für die zu schützenden Netze mit seinen angeschlossenen IT-Systemen und Diensten keinen Schutz. Ebenfalls kann nicht festgestellt werden, ob das System, mit dem kommuniziert wird, wirklich jenes ist, das es vorgibt, zu sein. Angreifer können an Zugangsdaten gelangen und für einen unberechtigten Zugriff nutzen.

Solche kompromittierten Anmeldeinformationen stellen weiterhin eines der größten Sicherheitsrisiken dar. Grund dafür ist, dass viele Unternehmen weiterhin auf die Einfaktor-Anmeldevariante mit Passwörtern setzen. (Ping Identiy, 2017)

Das nächste Unterkapitel soll daher die Möglichkeit der Multi-Faktor Authentifizierung erläutern.

4.2.3 Multi-Faktor-Authentifizierung

> „Eine Multifaktor-Authentifizierung dient der Verifizierung der Identität eines Nutzers mittels der Kombination verschiedener unterschiedlicher und insbesondere unabhängiger Klassen von Authentifizierungsverfahren.“ (Pohlmann, 2022)

Die Authentifizierungsverfahren werden laut einem Whitepaper von Ping Identiy (2017; Pohlmann, 2022) in folgende drei Kategorien unterteilt:

- Etwas, das man weiß.
- Etwas, das man hat.
- Etwas, das man ist.

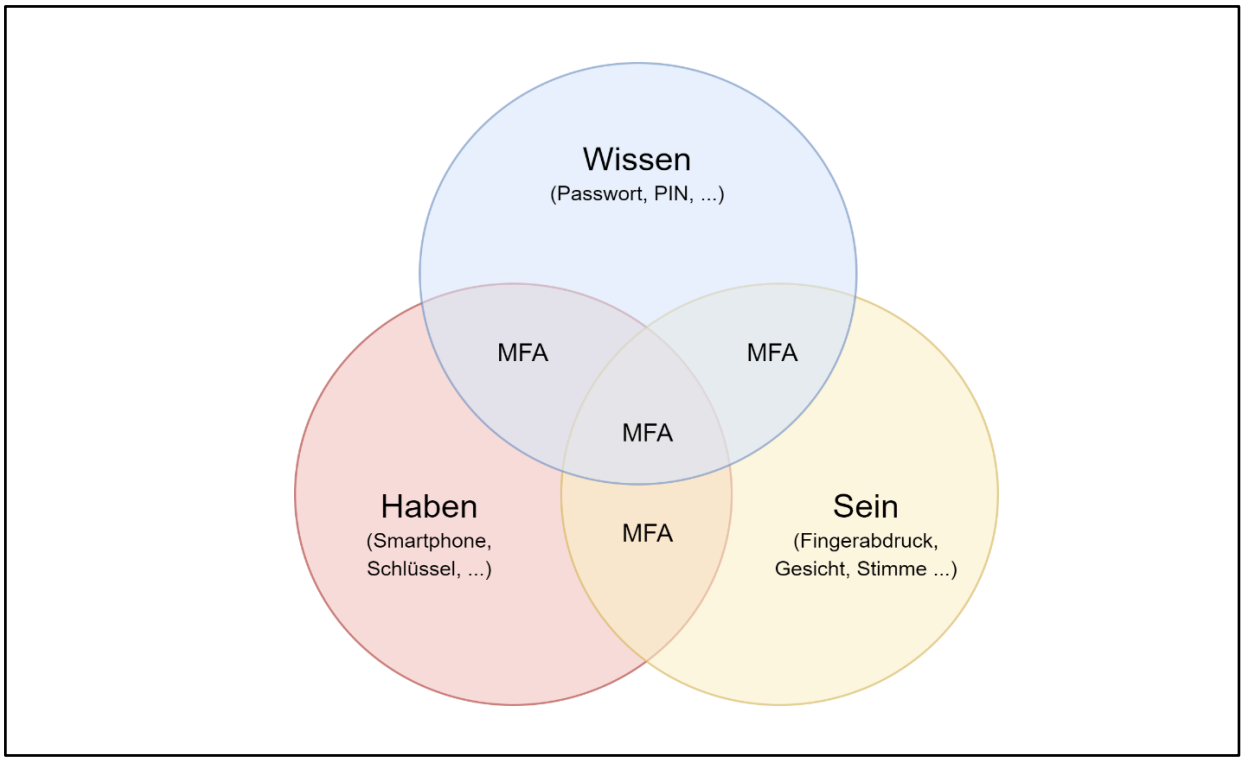

Abbildung 9 - Kategorien der Multifaktor-Authentifizierung (in Anlehnung an Ping Identiy, 2017)

Die Problematik, dass bei VPNs standardmäßig keine hohen Anforderungen gelten, um die Identität des Benutzers zu überprüfen, wurde im Kapitel 4.2.2 bereits erwähnt. Crafford (2021) sieht die beste Methode, um dieses Risiko zu minimieren in der Multifaktor-Authentifizierung, kurz MFA. Vor allem im Bereich der dezentralen Belegschaft wird die MFA als äußerst wichtige Sicherheitsmaßnahme genannt.

Pohlmann (2022) erwähnt, dass durch eine MFA noch flexibler reagiert und mit einer höheren Vertrauenswürdigkeit authentifiziert werden kann. Er erwähnt hier auch die, bei VPNs weitverbreitete, Zweifaktor-Authentifizierung, kurz 2FA, mittels „Besitz“ und „Wissen“. Dabei werden Sicherheitsmodule wie Smartcard oder Token zusammen mit Pin oder Passwort zur Anmeldung verwendet.

Jedoch setzt laut Bönsch (2021) nur die Hälfte der Unternehmen auf VPN-Sicherheitssysteme mit Multifaktor-Authentifizierung.

5 EMPIRISCHE FORSCHUNG

Nachdem in den vorherigen Kapiteln die nötige Theorie erarbeitet wurde, wird in diesem Kapitel auf den Forschungsablauf in dieser Arbeit näher eingegangen. Dieser erfolgt nach einem Modell von Raithel (2008).

Er erklärt die 7 Schritte einer empirischen Forschung:

1. Untersuchungsziel, Problemformulierung, Forschungsfragen
2. Theorie- und Hypothesenbildung
3. Konzeptualisierungsphase
4. Erhebungsvorbereitung und Datenerhebung
5. Datenaufbereitung
6. Datenanalyse
7. Interpretation und Verschriftlichung

5.1 Untersuchungsziel, Problemformulierung, Forschungsfragen

Die erste Phase des hier erwähnten Modells wurde bereits in den Kapiteln 1.1 Problemstellung, 1.2 Zielsetzung und 1.4 Forschungsfrage behandelt und niedergeschrieben.

5.2 Theorie- und Hypothesenbildung

Auch die Hypothesen in der zweiten Phase wurden bereits in der Zielsetzung verschriftlicht. Diese wurden während der primären Literaturrecherche erarbeitet und sollen nun mit der empirischen Untersuchung geprüft werden.

5.3 Konzeptualisierungsphase

In dieser Phase wird die Untersuchungsart ausgewählt, mit dem das Forschungsproblem empirisch erfasst wird. In dieser Arbeit wird eine Literaturrecherche durchgeführt, um auf bereits bestehende Informationen zurückgreifen zu können. In Kapitel 6 Methode-Literaturrecherche wird detailliert erklärt, mit welchem Erhebungsinstrument die Messung durchgeführt wird. Laut Raithel (2008) wird in dieser Phase auch die Größe der Stichprobe definiert.

5.4 Erhebungsvorbereitung und Datenerhebung

Nachdem die Methode gewählt wurde, wird in dieser Phase mit dem Einsatz der Methode begonnen. Bei der in dieser Arbeit verwendeten Literaturrecherche wird hier festgelegt, wie nach der benötigten Literatur gesucht wird und welche Literaturergebnisse ausgeschlossen oder in die Recherche mit aufgenommen werden. Wurde ein Dokument in die Recherche aufgenommen, wird hier noch festgelegt, wie die Informationen in diesem Dokument ausgewertet werden.

5.5 Datenaufbereitung

Hier soll festgelegt werden, wie die weitere Verarbeitung der durch die Datenerhebung gewonnenen Daten erfolgt. Die Literaturrecherche wird für die weitere Analyse in dieser Arbeit mittels einer Excel-Matrix aufbereitet. Näher wird auf die Datenaufbereitung im Kapitel 6.2.5 Literaturanalyse eingegangen. Alle Informationen werden in diesem Schritt abschließend nochmals auf Plausibilität und Validität geprüft.

5.6 Datenanalyse

Die bereinigte Matrix der gewonnenen Daten wird in diesem Schritt im Kapitel 7 Ergebnisse detailliert ausgewertet. So können Kenntnisse zur Bestätigung oder Widerlegung der Hypothesen gewonnen werden. Ebenfalls werden in diesem Schritt bereits bestehende Statistiken herangezogen, um die Aussagekraft der Literaturrecherche zu stärken oder auch abzuschwächen.

5.7 Interpretation und Verschriftlichung

In Kapitel 8 Schlussfolgerungen sollen die gewonnenen Erkenntnisse aus der durchgeführten Forschung abgefragt werden. Danach werden in Kapitel 9 alle diese Erkenntnisse zur Beantwortung der Forschungsfrage herangezogen.

Eine methodenkritische Betrachtung dieser Arbeit erfolgt in Kapitel 10. Können alle Hypothesen und auch die Forschungsfrage durch diese Arbeit beantwortet werden oder gibt es Einschränkungen bezüglich der Übertragbarkeit der Studie?

Abschließend wird noch in Kapitel 11 auf weitere Forschungsmöglichkeiten hingewiesen.

6 METHODE-LITERATURRECHERCHE

Als passende Methode wurde für diese Arbeit die Literaturrecherche gewählt. Da es eine Vielzahl an Informationen zu dieser Thematik gibt, ist es sinnvoller, bestehende Informationen mit großer Aussagekraft zu bündeln und auszuwerten, anstatt mittels kleiner Stichprobe eventuell nicht aussagekräftige Ergebnisse zu erhalten.

6.1 Arten der Literaturrecherche

Rosert (2009) berichtet von zwei Methoden der Literaturrecherche, der systematischen Methode und der Schneeballmethode. In der Regel werden beide Methoden verwendet, jedoch gibt es Unterschiede bei der Suche. Je nachdem, welche der beiden Methoden zum Einstieg verwendet wird. In den Unterkapiteln werden diese Typen der Literaturrecherche genauer erklärt.

6.1.1 Die systematische Literaturrecherche

Heil (2020) erwähnt, dass eine „Systematic Literature Review“ eine eigenständige, wissenschaftliche Methode mit dem Ziel ist, sämtliche relevante Literatur zum Forschungsthema zu finden und diese kritisch zu bewerten.

Diese Art der Literaturrecherche sollte laut Rosert (2009) verwendet werden, wenn lediglich ein Thema, jedoch wenige oder keine Literaturhinweise vorhanden sind. Es werden dabei Bibliothekskataloge, Datenbanken und relevante Fachzeitschriften nach sinnvollen Stichwörtern durchsucht.

In der Literatur werden zwei Grundlagenwerke erwähnt, welche die Methodik der systematischen Literaturrecherche beschreiben. Dies sind Webster und Watson (2002), die in ihrem Artikel „Analyzing the Past to Prepare for the Future – Writing a Literature Review“ die Vorgehensweise bei der Literaturrecherche und auch wie die Ergebnisse zu dokumentieren sind, sehr genau beschreiben.

Während die Recherche von Webster und Watson laut von Gersdorff (2020) auf die Ableitung der Forschungslücke abzielt wird, bei der zweiten, bekannten Methode, der systematischen Literaturrecherche nach vom Brocke et al., der Schwerpunkt auf die Literaturprüfung gelegt.

Beide Methoden können sowohl einzeln als auch kombiniert verwendet werden. In dieser Arbeit wird primär die Methode von vom Brocke et al. verwendet werden. Jedoch werden einzelne Schritte, wie die in den nächsten Kapiteln erwähnte Konzeptmatrix und auch die Identifikation relevanter Literatur, an Webster und Watson angelehnt.

6.1.2 Die unsystematische Literaturrecherche

Diese Art der Literaturrecherche bietet sich laut Rosert (2009) an, wenn bereits ein guter Ausgangspunkt, zum Beispiel ein Aufsatz in einer Zeitschrift, ein Sammelband oder ein Buch, vorhanden ist. Das entsprechende Literaturverzeichnis dient als Suche für vielversprechende Texte, welche wiederum interessante Literaturverweise enthalten können.

Lindner (2020) erwähnt eine Erweiterung dieser Art von Suche. Die Forward-Backward-Search recherchiert in zwei verschiedene Zeitrichtungen. Sucht man Paper, in denen das Ausgangspaper zitiert wird, so handelt es sich um eine Forward-Search, da nur neuere Artikel gefunden werden können. Sucht man aber, wie vorher bei der Schneeballmethode, nur in den Literaturverzeichnissen der Paper, so handelt es sich um eine Backward-Search, da nur ältere Artikel gefunden werden können.

In dieser Arbeit wird parallel zur Suche mittels Suchstrings diese Art der Recherche eingesetzt. Dadurch werden auch Paper, welche nicht den Suchkriterien im Titel entsprechen, aber dennoch eine sehr gute Datenbasis für die Recherche darstellen, in die Arbeit mit aufgenommen.

6.2 Systematische Literaturrecherche nach vom Brocke et al.

Die Vorgehensweise nach vom Brock et al. ist in fünf Phasen unterteilt:

1. Definition des Anwendungsbereiches
2. Konzeptionalisierung des Themas
3. Literatursuche
4. Literaturanalyse
5. Zusammenfassung der Resultate

In Abbildung 10 ist erkennbar, dass es sich nicht um einen einmaligen Prozess handelt. Ein einmaliger Durchlauf dieses Prozesses muss aber nicht den Abschluss der Recherche darstellen. Dieser kann beziehungsweise sollte immer wieder iterativ neu gestartet werden.

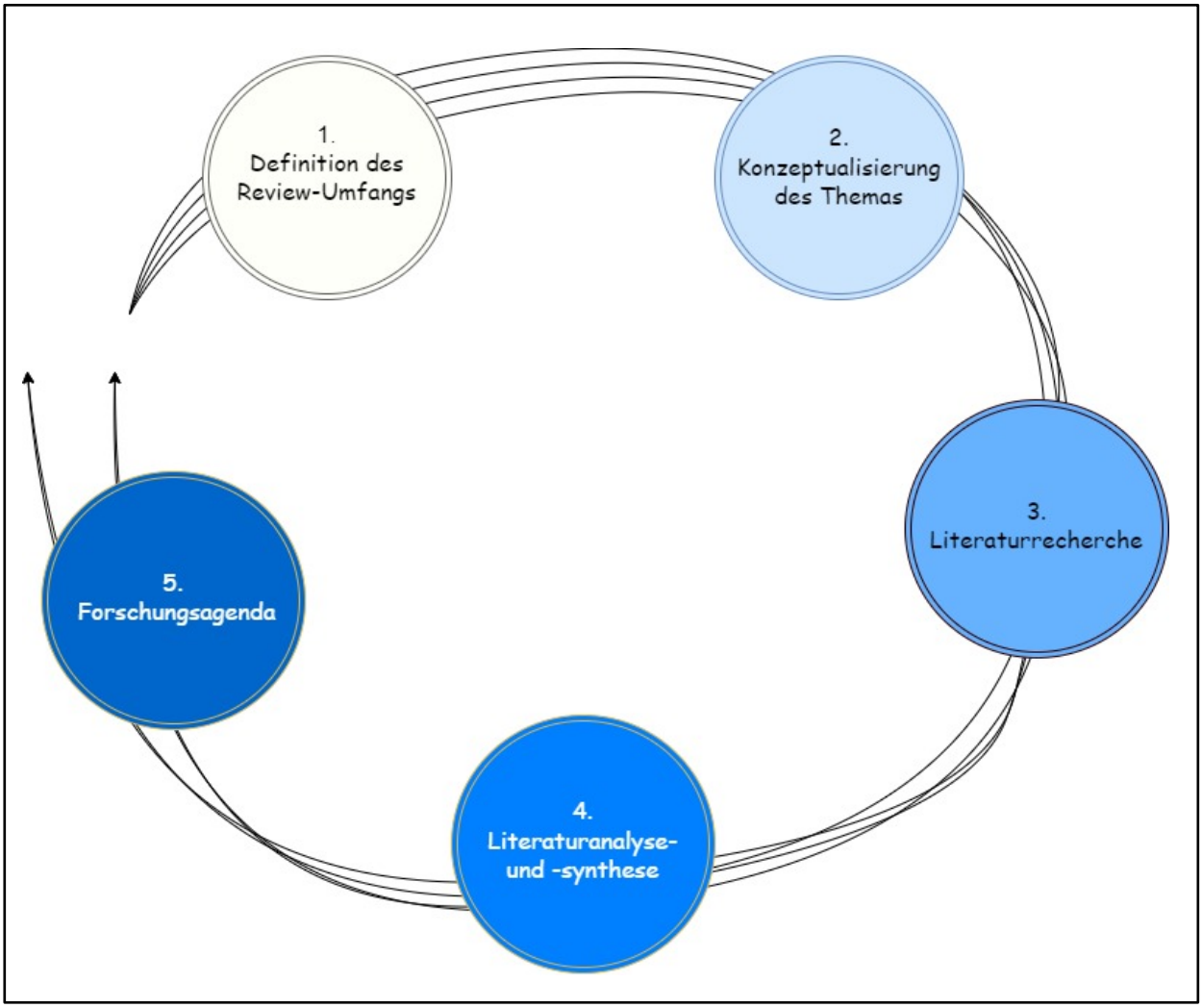

Abbildung 10 - Phasen der Systematischen Literaturrecherche (in Anlehnung an vom Brocke et al., 2009, Figure 3)

6.2.1 Definition des Anwendungsbereiches

Laut vom Brocke et al. (2009) muss in der ersten Phase der Literaturrecherche der Umfang der Suche festgelegt werden. Ebenfalls erwähnen die Autoren hier mehrere Ausrichtungen, die eine solche Review haben kann:

- kritisch
- interpretierend
- spekulativ
- auf dem neuesten Stand der Technik
- historisch

Vom Brocke et al. schlagen daher vor, sich an den von Cooper (1988) konstituierenden Merkmalen zu orientieren, um den Anwendungsbereich klar zu definieren.

Die von Cooper erwähnten sechs Merkmale haben jeweils mehrere Auswahlmöglichkeiten mit Hilfe derer die Ausrichtung festgelegt wird.

6.2.1.1 Fokus

Hier wird bestimmt, worauf sich die Literaturübersicht bezieht. Cooper (1988) zeigt hier folgende Ausrichtungen auf:

- **Forschungsergebnisse**
- Forschungsmethoden
- Theorien
- Anwendungen

Diese Arbeit legt keinen Wert darauf, auf welche Art die Erkenntnisse gewonnen werden. Ob es sich um Umfragen, Interviews oder ähnliche Methoden handelt, ist nicht relevant. Verschiedene Methoden führen eher zu einer höheren Aussagekraft der Literaturrecherche.

Daher zielt diese Arbeit auf die Forschungsergebnisse der einzelnen Quellen ab.

6.2.1.2 Ziel

Dieses Merkmal soll das schlussendliche Ergebnis der Recherche definieren.

- Integration (Verallgemeinerung, Lösung von Konflikten, linguistischer Brückenschlag)
- Kritik
- **Zusammenfassung**

In dieser Arbeit sollen die einzelnen Erkenntnisse aus der Recherche zu einer Aussage über die Handlungsempfehlungen bei der Telearbeit zusammengefasst werden.

6.2.1.3 Perspektive

Die Perspektive gibt darüber Auskunft, ob der Verfasser eine neutrale Rolle einnimmt oder für eine Position eintritt.

- **neutrale Darstellung**
- eintreten für eine Position

Es soll durch diese Recherche eine neutrale Sicht auf die Gefahren der Telearbeit bezogen auf die Cybersicherheit erstellt werden.

6.2.1.4 Erfassungsgrad

Laut Cooper ist dies der deutlichste Aspekt der Literaturrecherche. Hier wird definiert, wie Literatur gesucht wird und wie Entscheidungen über die Eignung und Qualität des Materials getroffen werden.

- ausführlich
- ausführlich, aber mit selektiver Erwähnung
- **repräsentativ**
- zentral oder entscheidend

Da es sich bei der Literaturrecherche für diese Arbeit nur um einen Auszug (Stichprobe) der relevanten Werke handelt, wird der Erfassungsgrad als repräsentativ angegeben.

6.2.1.5 Gliederung

Bei der Gliederung erwähnt Cooper folgende drei Strukturen:

- **historisch**
- **konzeptionell**
- methodologisch

Diese Masterarbeit weist fünf Bereiche auf, die erarbeitet werden. Die Angriffsart, den Angriffskanal Nutzer, den Angriffskanal System, die technischen Maßnahmen und die organisatorischen Maßnahmen. Daher handelt es sich hier um eine konzeptionelle Gliederung. Jedoch wird auch die historische Veränderung in den letzten Jahren hinterfragt. Deshalb ist hier auch eine historische Gliederung von Nöten.

6.2.1.6 Zielgruppe

Wie der Name dieses Merkmals bereits aussagt, wird hier bestimmt, für wen diese Arbeit erstellt wird.

- spezialisierte Forschergruppen
- allgemeine Forscher
- **Praktiker oder politische Entscheidungsträger**
- allgemeine Öffentlichkeit

Die Zielgruppe legt die Tiefe der Recherche und die Ausdrucksweise bei den Ergebnissen fest. Handelt es sich um eine Recherche für die breite Öffentlichkeit, wird weniger Fachjargon eingesetzt, hingegen sind Ergebnisse für spezialisierte Forschergruppen umso detaillierter.

Diese Arbeit soll nicht IT-Security-Spezialisten von Unternehmen als Wissensgrundlage für Cyberrisiken dienen, die Arbeit richtet sich an Personen im Management, die einen Eindruck über die momentane Ausprägung der IT-Security für ihre Telearbeitsplätze bekommen wollen.

Daher werden die Praktiker beziehungsweise die politischen Entscheidungsträger als Zielgruppe definiert.

In **Fehler! Verweisquelle konnte nicht gefunden werden.** ist zusammenfassend erkennbar, welcher Anwendungsbereich im Zuge dieser Literaturrecherche gewählt wurde.

Charakteristik	**Kategorien**			
Fokus	**Forschungsergebnisse**	Forschungsmethoden	Theorien	Anwendungen
Ziel	Integration	Kritik	**Zusammenfassung**	
Perspektive	**neutrale Darstellung**	eintreten für eine Position		
Erfassungsgrad	ausführlich	ausführlich mit selektiver Erwähnung	**repräsentativ**	zentral oder entscheidend
Gliederung	**historisch**	**konzeptionell**	methodologisch	
Zielgruppe	spezialisierte Forschergruppen	allgemeine Forscher	**Praktiker pol. Entscheidungsträger**	allgemeine Öffentlichkeit

Tabelle 1 – Klassifizierung des Anwendungsbereichs der Literaturrecherche (in Anlehnung an Cooper, 1988, S. 109)

6.2.2 Konzeptualisierung des Themas

In diesem Kapitel erwähnen vom Brocke et al. (2009), dass die Überprüfung mit einer Vorstellung beginnen muss, was über dieses Thema bekannt ist. Daher sollte zu diesem Zeitpunkt eine Identifizierung der Schlüsselbegriffe durchgeführt werden.

Vom Brocke et al. empfehlen hier die Methode des „Concept Mapping“.

„Concept Mapping“, welches laut Krüger (2014) sachlogische Zusammenhänge grafisch darstellt oder konzeptionelle Vorstellungen von Personen erfasst, sollte von „Mind Mapping“ streng unterschieden werden. Diese Methode wird eher für Brainstorming beziehungsweise zum Visualisieren von Gedanken verwendet.

6.2.2.1 Concept Map

Abbildung 11 - Concept Map

Heil (2020) teilt die Dokumentation des Recherchefundaments in 5 Arbeitsschritte auf.

- Forschungsfrage und Rechercheziel definieren
- Ein- und Ausschlusskriterien
- Datenbanken definieren
- Suchkomponenten definieren
- Suchstring festlegen

6.2.2.2 Forschungsfrage und Rechercheziel

Forschungsfrage:

„Welche Handlungsempfehlungen können in Bezug auf Telearbeit gegeben werden, um einer Gefährdung der Unternehmenssicherheit durch Cyberangriffe effektiv entgegenwirken zu können?“

Rechercheziel:

Die bestehende Literatur soll nach folgenden fünf Kriterien durchsucht werden, um Handlungsempfehlungen formulieren zu können:

- Angriffsarten
- Angriffskanal User
- Angriffskanal System
- Technische Sicherheitssysteme
- Organisatorische Sicherheitssysteme

6.2.2.3 Ein- und Ausschlusskriterien

Heil (2020) erwähnt als einen Punkt des Recherchefundamentes die Definition der Kriterien. Um den Scope der Suche eingrenzen zu können, müssen gewisse Einschluss- beziehungsweise Ausschlusskriterien definiert werden. Folgende Kriterien wurden bei der Suche berücksichtigt:

- Kriterium 1
    - Die Quellen wurden zwischen 2015 und 2023 veröffentlicht

Gerade in den Bereichen Cybersecurity und Telearbeit gab es in den letzten Jahren massive Veränderungen. Vor allem die Coronapandemie, welche 2019 begann, stellt hier einen wichtigen Faktor dar. Die Literaturrecherche soll aber nicht nur diesen Zeitraum abdecken. Eventuell wichtige Veränderungen würden ansonsten nicht erkannt werden. Deshalb wurde ein Zeitraum gewählt, bei dem der Ausbruch von COVID-19 genau in der Mitte liegt und die vier Jahre vor sowie die vier Jahre nach Ausbruch betrachtet werden.

- Kriterium 2
    - Online-Verfügbarkeit des gesamten Dokuments

Durch dieses Kriterium können viele Ergebnisse sofort ausgeschlossen werden. Eine vollständige Recherche ist ohne Volltext-Verfügbarkeit der Quelle nicht möglich.

- Kriterium 3
    - Sprache der Ergebnisse ist Deutsch oder Englisch

Um Fehler bei der Übersetzung zu vermeiden, werden nur Ergebnisse in diesen beiden Sprachen in die Recherche aufgenommen.

- Kriterium 4
    - Liegt der Fokus des Dokuments auf den gewünschten Informationen?

Aufgrund der Vielzahl an Ergebnissen werden einige davon nicht den erwarteten Inhalt aufweisen. Diese werden im Zuge der Sichtung nachträglich aus der Recherche ausgeschlossen.

6.2.2.4 Datenbanken definieren

Als nächsten Schritt erwähnt Heil (2020) die Auswahl der Datenbanken, welche nach relevantem Material durchsucht werden. Aufgrund der eingeschränkten Zugriffsmöglichkeiten hat sich diese Arbeit auf frei zugängliche Datenbanken konzentriert.

Folgende Datenbanken wurden gesichtet:

- Google Scholar
- IEEE
- ScienceDirect
- BASE (Bielefeld Academic Search Engine)

6.2.2.5 Suchkomponenten definieren

Randolph (2009) empfiehlt die Schlüsselwörter, die in der Forschung verwendet werden, zu dokumentieren. Schlüsselwörter sind für eine effektive Forschung von entscheidender Bedeutung, da sie die Grundlage für die Forschung bilden.

Es ist wichtig, auch alle Synonyme und ähnliche Wörter zu den Schlüsselwörtern zu berücksichtigen. Werden bei der Suche Synonyme oder Wörter mit ähnlicher Bedeutung mit einbezogen, wird der boolsche Operator „OR“ zum Gruppieren verwendet. Bei der Suche nach Begriffen und Konzepten, die sich voneinander unterscheiden, wird der boolsche Operator „AND“ verwendet. (Timmins & McCabe, 2005)

Aufgrund der viel höheren Anzahl an englischsprachiger Literatur wurden englische Schlüsselwörter ausgewählt. Dadurch wird auch eine regionale Einseitigkeit vermieden.

In dieser Arbeit wurden folgende Schlüsselwörter zur Thematik Telearbeit erkannt:

- telework, teleworker, teleworkers
- homework
- remote working, remote work
- home-office, homeoffice

Zur Thematik Sicherheit wurden folgende Begriffe gewählt:

- security
- threat, threats

- awarness
- measures
- attack, attacks

6.2.2.6 Suchstring festlegen

Erster Ansatz bei der Erstellung des Suchstrings war, die Begriffe „telework“ und „threats“ beziehungsweise „telework“ und „security“, ohne Einschränkung auf den Titel, zu verwenden.

- `telework threats`
    - 20.400 Ergebnisse in Google Scholar
- `telework security`
    - 30.200 Ergebnisse in Google Scholar

Dieser erste Versuch ergab bereits bei Google Scholar zu viele Ergebnisse. Der Ansatz, die Suche auf den Titel einzugrenzen, brachte folgende Ergebnisse:

- `telework threats`
    - 1 Ergebniss in Google Scholar
- `telework security`
    - 19 Ergebnisse in Google Scholar

Nun wurde versucht, auch einige Synonyme in den Suchstring mitaufzunehmen. Weiterhin wurden die Begriffe aber nur auf den Titel gefiltert.

- Google Scholar
    - `allintitle: (telework OR homework OR "remote working" OR "remote work" OR teleworkers OR "Home office" OR "homeoffice") (security OR threats OR threat OR awareness OR measures OR attack OR attacks)`
    - 126 Ergebnisse
- BASE
    - `tit:(telework OR homework OR "remote working" OR "remote work‟ OR teleworkers OR homeoffice) tit:(security OR threats OR threat OR awareness OR measures OR attack OR attacks)`
    - 107 Ergebnisse

- IEEE
  - `(("Document Title":telework* OR "Document Title":homework OR "Document Title":"remote work*" OR "Document Title":homeoffice OR "Document Title":"home office") AND ("Document Title":security OR "Document Title":threat* OR "Document Title":awareness OR "Document Title":measure* OR "Document Title":attack*))`
  - 11 Ergebnisse
- ScienceDirect
  - `(telework OR homework OR "remote working" OR "remote work" OR "Home office") AND (security OR threat OR measures OR attack)`
  - Hier gab es eine Einschränkung auf 8 boolsche Operatoren, deshalb konnten nicht alle Begriffe verwendet werden. Durch Versuche wurden die relevantesten Begriffe verwendet.
  - 13 Ergebnisse

Diese Suchstrings, die aus den Schüsselwörtern gebildet wurden, bildeten den Ausgangspunkt der Literatursuche.

6.2.3 Literatursuche nach Moher et al.

Die unter 6.2.2.6 erarbeiteten Suchstrings werden nun in Phase 3 der systematischen Literaturrecherche nach vom Brocke et al. (2009) eingesetzt.

Der eigentliche Suchprozess folgt dem PRISMA-Statement von Moher et al. (2009). Dabei kann der Suchprozess in mehrere Phasen unterteilt werden.

- Identifikation
- Screening Phase
- Eignung
- Inklusion

6.2.3.1 Identifikation

In dieser Phase werden die gewählten Datenbanken mittels Suchstrings durchsucht, bis die Suchergebnisse eine passende Anzahl an Quellen liefern. Die verschiedenen Versuche wurden bereits ausführlich im Kapitel 6.2.2.6 Suchstring festlegen aufgelistet.

Insgesamt wurden mit Hilfe dieser Suche 257 Ergebnisse in den vier Datenbanken gefunden. Ebenfalls wird in der Identifikationsphase das Kriterium 1 der Ein- und Ausschlusskriterien aus

Kapitel 6.2.2.3 überprüft. Alle Ergebnisse mussten zwischen 2015 und 2023 veröffentlicht worden sein.

- Google Scholar
    - 126 Ergebnisse → zwischen 2015 und 2023 → 74 Ergebnisse
    - 52 Ergebnisse entfernt
- BASE
    - 107 Ergebnisse → zwischen 2015 und 2023 → 78 Ergebnisse
    - 29 Ergebnisse entfernt
- IEEE
    - 11 Ergebnisse → zwischen 2015 und 2023 → 6 Ergebnisse
    - 5 Ergebnisse entfernt
- ScienceDirect
    - 13 Ergebnisse → zwischen 2015 und 2023 → 6 Ergebnisse
    - 7 Ergebnisse entfernt

Die Gesamtanzahl nach der Identifikationsphase beträgt 164 Ergebnisse. Diese werden in den nächsten Phasen der Literatursuche auf ihre Eignung überprüft.

6.2.3.2 Screening-Phase

In der Screening-Phase werden die Ergebnisse auf Duplikate überprüft. Duplikate kommen hauptsächlich bei der Suche mit verschiedenen Datenbanken vor, es kommt jedoch auch vereinzelt zu Duplikaten innerhalb der Datenbanken. Durch diesen Schritt wurde folgende Anzahl an Ergebnissen für die Recherche übernommen.

- Google Scholar
    - 74 Ergebnisse → 2 Ergebnisse doppelt → 72 Ergebnisse
- BASE
    - 78 Ergebnisse → 52 Ergebnisse doppelt → 26 Ergebnisse
- IEEE
    - 6 Ergebnisse → 4 Ergebnisse doppelt → 2 Ergebnisse
- ScienceDirect
    - 6 Ergebnisse → 2 Ergebnisse doppelt → 4 Ergebnisse

Nach dem Entfernen der 60 Duplikate blieben 104 Ergebnisse für die weitere Filterung übrig. Ein weiteres Ausschlusskriterium war die Online-Verfügbarkeit der Texte. Von 104 Quellen waren nur 63 Quellen als Volltext online verfügbar.

Diese 63 Ergebnisse wurden noch auf das Kriterium 3, die Sprache, kontrolliert. 9 Ergebnisse waren in einer anderen Sprache als Deutsch oder Englisch. Somit blieben 54 Quellen für die weitere Betrachtung übrig.

6.2.3.3 Eignung

Jene 54 Quellen, welche nach der Screening-Phase zur weiteren Betrachtung zur Verfügung standen, wurden in dieser Phase inhaltlich auf deren Eignung überprüft. Hierbei handelt es sich um das Kriterium 4, dem Fokus des Dokuments. Nachdem eine Volltextdurchsicht der Quellen durchgeführt wurde, mussten 29 Ergebnisse ausgeschlossen werden, da sie inhaltlich nicht genügend Informationsgehalt aufwiesen. Teilweise waren zwar die Schlüsselwörter der Paper passend, jedoch wurden relevante Themenbereiche nur angeschnitten oder gar nicht behandelt.

6.2.3.4 Inklusion

Nachdem aufgrund des fehlenden Fokus weitere 29 Ergebnisse ausgeschlossen werden mussten, wurden nur 25 Quellen für die systematische Literaturrecherche herangezogen. Um den Ablauf der Literatursuche nach Moher et al. (2009) übersichtlich zusammenzufassen, wurde dieser in Abbildung 12 grafisch dargestellt.

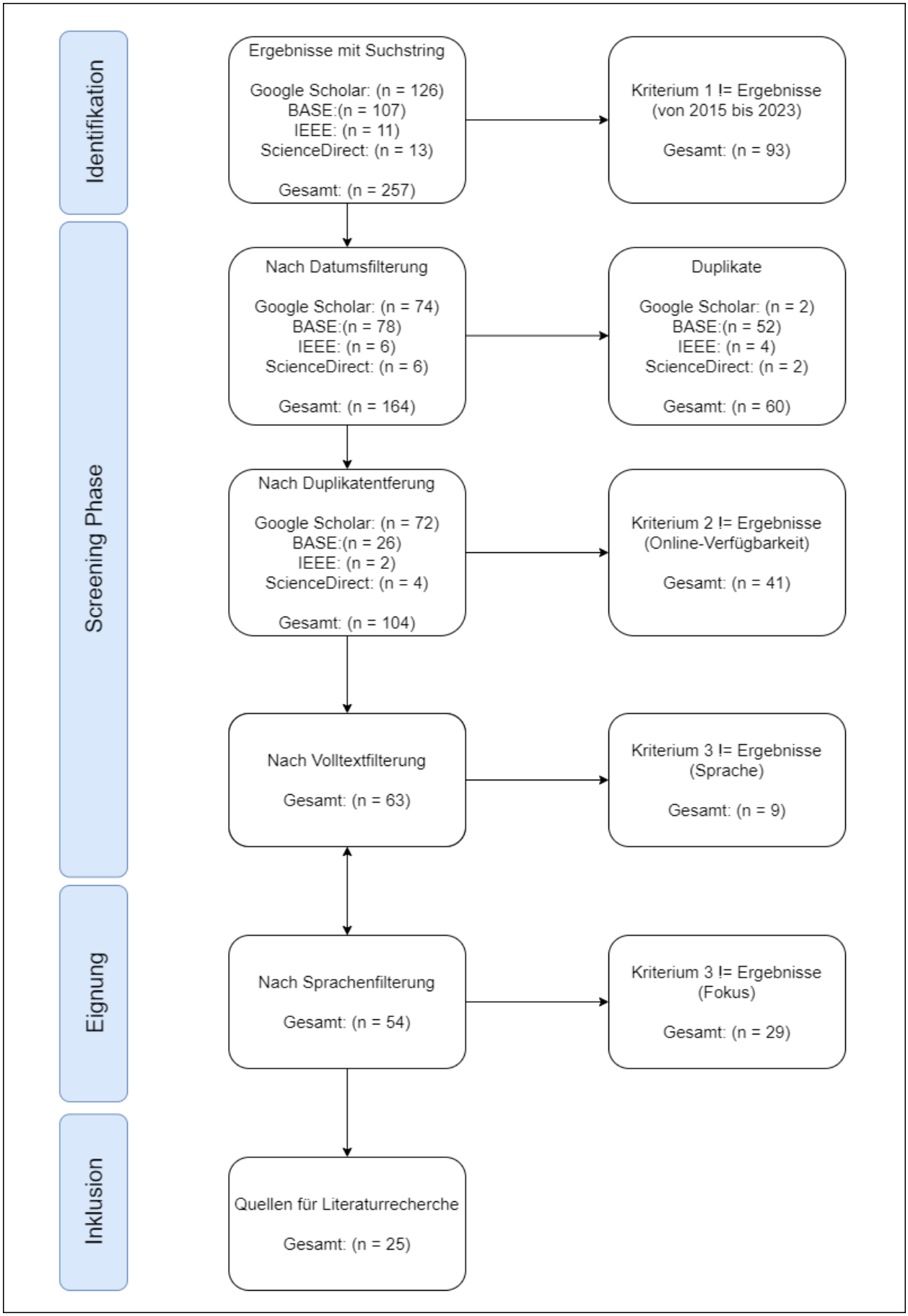

Abbildung 12 - Das PRISMA Flussdiagramm der Literatursuche (in Anlehnung an Moher et al. 2009)

Nachdem die Literatursuche nach Moher et al. aufgrund der vielen, durch die Kriterien ausgeschlossenen Quellen, nur 25 Ergebnisse lieferte, musste die Suche noch erweitert werden.

Im Kapitel 10 Kritische Betrachtung wird auf die Problematik der Literatursuche nach Moher et al. nocheinmal genauer eingegangen.

6.2.4 Literatursuche „forward-backward-search“

vom Brocke et al. (2009) erwähnen eine weitere Möglichkeit der Literatursuche, welche anstatt oder in Verbindung mit der Suche nach Moher et al. angewendet werden kann. Es handelt sich hierbei um die sogenannte „forward search“ beziehungsweise „backward search“ von Haddaway et al. (2022) auch „forward citation chasing“ und „backward citation chasing“ genannt.

Das Grundprinzip dieser Art von Literaturrecherche wurde bereits im Kapitel 6.1.2 Die unsystematische Literaturrecherche kurz beschrieben.

Haddaway et al. (2022) erwähnen diese Suche nach Zitaten als beliebte ergänzende Suchmethode, da sie auf der Arbeit von Primär- und Review-Autoren aufbaut. Dabei werden relevante Studien identifiziert, die mit anderen Suchmethoden nicht gefunden werden. Grund dafür ist hier oft die Kombination der Schlüsselwörter im Suchstring. Zum Beispiel kann es vorkommen, dass die Suchbegriffe der Review-Autoren nicht in angegebener Kombination im Titel oder in den Schlüsselwörtern vorkommen.

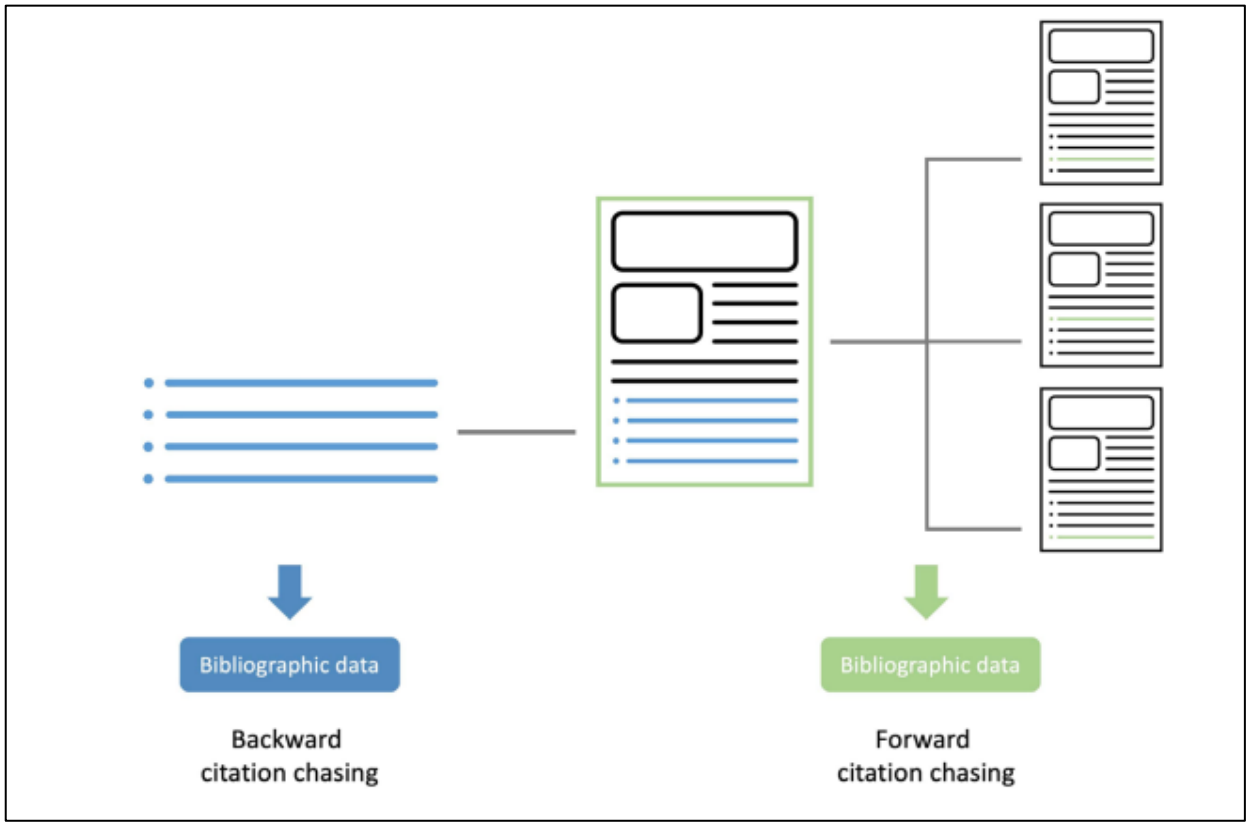

Abbildung 13 - Grafische Darstellung von forward und backward citation chasing (Haddaway et al., 2022, S. 2)

Daher wurde nun parallel zur Literatursuche nach Moher et al. mittels dieser Methode versucht, relevante Quellen für die Literaturrecherche zu finden.

Ausgangspunkt dieser Suche waren die Quellen „Overcoming the security risks of remote working“ und „Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond“ aus der vorgehenden Literatursuche.

Beide Quellen wurden auf Google Scholar bereits über 50-mal zitiert. Jene Artikel, in denen diese Quellen zitiert wurden, konnten in weiterer Folge auf relevantes Material gesichtet werden. Abbildung 14 zeigt wie eine solche forward search ermöglicht wird.

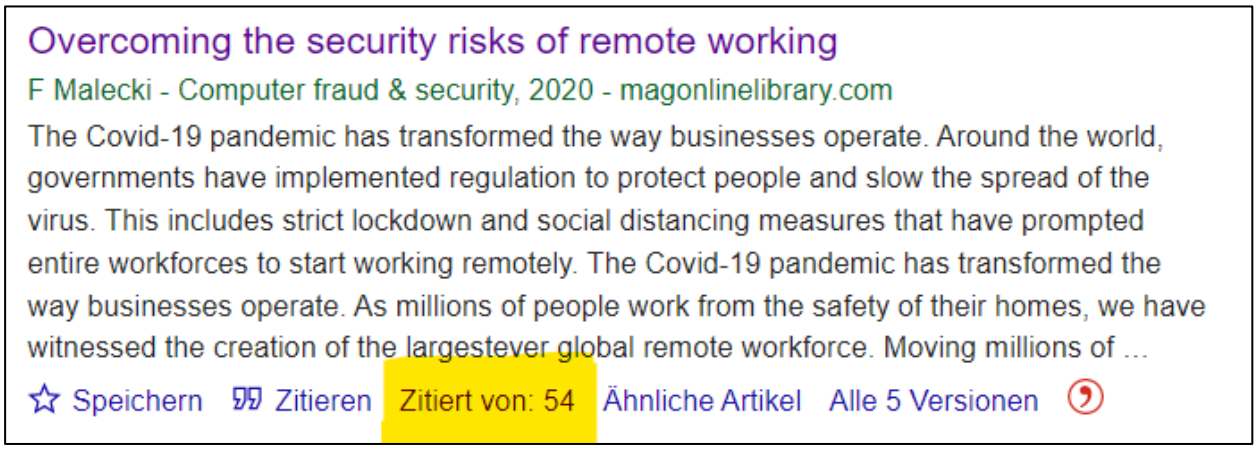

Abbildung 14 - Forward Search in Google Scholar (Eigener Screenshot aus Google Scholar)

Ausgehend von diesen beiden Papers wurden mittels forward- und backward search weitere 42 Quellen mit passenden Titeln gefunden. Die Kriterien aus Kapitel 6.2.3 wurden auch bei dieser Art der Suche übernommen. Zwei Quellen mussten, aufgrund des fehlenden Volltextes, zwei Quellen aufgrund des fehlenden Fokus ausgeschlossen werden. Daher wurden 38 Quellen für die erweiterte Literaturrecherche übernommen. Welche Ergebnisse für die forward- und backward search verwendet wurden, ist in der Konzeptmatrix, welche in weiterer Folge erstellt wurde, in Spalte C nachzulesen.

Insgesamt wurden aus beiden Literatursuchen 63 Quellen für die weiteren Schritte der Literaturrecherche nach vom Brocke et al. gewonnen.

6.2.5 Literaturanalyse

Die vierte Phase der systematischen Literaturrecherche nach vom Brocke et al. ist die Literaturanalyse. Die mit Hilfe der Literatursuche gefundenen Quellen können nun genauer betrachtet und ausgewertet werden. Wie bereits in Kapitel 6.1.1 Die systematische Literaturrecherche erwähnt wird, kommt es in dieser Arbeit zu einer Vermischung zweier Methoden, jener von vom Brocke et al. (2009) und jener von Webster und Watson (2002).

In diesem Kapitel wird zur Analyse der Quellen die Matrixdarstellung von Webster und Watson aus Abbildung 15 - Konzeptmatrix (Webster & Watson, 2002, S. xvii) herangezogen.

Table 2. Concept Matrix

Articles	Concepts				
	A	B	C	D	...
1		✖	✖		✖
2	✖	✖			
...			✖	✖	

Abbildung 15 - Konzeptmatrix (Webster & Watson, 2002, S. xvii)

Webster und Watson (2002) erwähnen in ihrem Paper, dass Artikel anhand eines zuvor durchdachten Schemas kategorisiert werden sollten. Die Artikel werden in dieser Matrix vertikal aufgetragen. Horizontal werden die einzelnen Erwähnungen in den selbst erstellten Kategorien aufgetragen.

Neben Nummer und Titel wurde auch aufgenommen, ob bei diesem Artikel eine forward- oder backward search durchgeführt wurde und welcher Artikel dabei gefunden wurde. Auch das Erscheinungsjahr, die Datenbank und die vier Kriterien wurden in der Matrix mitaufgenommen.

Im Zuge dieser Arbeit wurden fünf Kategorien erstellt, nach denen in den einzelnen Quellen gesucht wurden.

- Angriffsart
- Angriffskanal Nutzer
- Angriffskanal System
- Sicherheitssysteme technisch
- Sicherheitssysteme organisatorisch

Aufbauend auf die Theorie wurden diese Kategorien nun Themen zugeordnet, auf die in der Literaturrecherche geachtet werden musste. Während der Recherche wurden Themen, die noch nicht in der Theorie vorgekommen sind, mitaufgenommen. Am Ende der Recherche wurden diese Einträge nochmals bewertet und, wenn nötig, in die Theorie mitaufgenommen.

In Folge werden alle Themen der einzelnen Kategorien aufgelistet.

- Angriffsarten
    - Phishing
    - Spam
    - Man in the middle
    - Brut Force
    - Malware
    - Botnetze
    - Ransomware
    - Social Engineering
    - DDoS
    - Wurm
    - Advanced Persistant Threat
    - Zero-Day Exploits
- Angriffskanal Nutzer
    - bösartige Webseiten
    - E-Mails
    - Social Media
    - kompromittierte Zugangsdaten
    - Deep Fakes / Fake News
    - unerlaubter Zugang zu Geräten
    - Verlust / Diebstahl der Geräte
- Angriffskanal System
    - Softwarequalität
    - fehlende Patches und Updates
    - unsichere Webseiten
    - Mobile Applikation
    - Mobile Endgeräte
    - IoT
    - Private Router
    - E-Mail
    - removable Media
    - unsichere Geräte
    - unsichere Netze

    - manipulierte Collaborationstools
    - manipulierte IT-Systeme
- Technische Sicherheitssysteme
    - Virenschutz
    - Anti-Malware
    - Firewall
    - Passwort-Policy
    - Spamfilter
    - Threat Intelligence
    - Sandbox
    - WLAN Encryption
    - digitale Mail-Signatur
    - E-Mail-Verschlüsselung
    - Benutzerrechteverwaltung (PAM)
    - Software-Patching und -Updates
    - no BYOD
    - VPN
    - Multifaktor-Authentifizierung
    - Backup
    - Mobile Device Management
    - Data Encryption
    - Private Cloud Speicherung
    - IoT-Anpassungen
    - Zero Trust Access
    - Sperrbildschirm
    - Heimnetz-Segmentierung
- Organisatorische Sicherheitssysteme
    - Awareness (Schulungen, Infos)
    - Verhaltensregeln
    - Notfallpläne
    - Kommunikation zur IT
    - Penetration Test
    - ISMS
    - ISO27001

7 ERGEBNISSE

In diesem Kapitel sollen die Ergebnisse der empirischen Forschung aufgezeigt werden. Die Literaturrecherche, welche als Konzeptmatrix dargestellt wird, wurde dabei nach verschiedenen Gesichtspunkten ausgewertet.

7.1 Ergebnisse Literaturanalyse

Die erstellte Konzeptmatrix nach Webster und Watson wurde als Basis für die Auswertung der einzelnen Quellen herangezogen. Insgesamt wurden hier 63 Quellen analysiert. Um den Aufbau der Konzeptmatrix zu zeigen, wurde Abbildung 16 eingefügt. Weiters ist die gesamte Tabelle als Excel-Datei auf dem beigelegten Datenträger unter dem Namen Literaturanalyse_Matrix.xslx abgelegt.

	A	B	C	D	E	F	G	H	I	J	K	T	U	W	X
1	Nummer	Titel	Forward-Search	Backward - Search	Duplikate	Erscheinungsjahr	Datenbank	E/A Kriterien				Angriffsart			
2								K1 2015-2023	K2 Online	K3 Sprache	K4 Fokus	Phishing	Spam	Brute Force	Malware
3					60			146	103	94	63	46	19	2	35
113	110	Cybersecurity issues and challenges during COVID-19				2020	Scholar	1	1	1	1	1	1		1
114	111	Covid-19 effects on cybersecurity issues				2021	Scholar	1	1	1	1				
115	112	Remote Working and Cybersecurity in the Pandemic: Research on the Employee Perceptions of Remote				2021	Scholar	1	1	1	1	1			1
116	113	Information systems security in the age of pandemics:		119,122		2021	Scholar	1	1	1	1				
117	114	Data security and privacy in times of pandemic		121		2021	Scholar	1	1	1	1	1	1		1
118	115	Cyber security threats during the pandemic	171			2020	Scholar	1	1	1	1	1			
119	116	Managing the Cybersecurity Risks of Teleworking in		122,123,124		2021	Scholar	1	1	1	1	1	1		1
120	117	Work from Home-Information Security Threats and				2021	Scholar	1	1	1	1	1			1
121	118	Understanding the Effects of Cyber Security Risks and				2021	Scholar	1	1	1	1				1
122	119	Cybersecurity during the COVID-19 pandemic	131			2021	Scholar	1	1	1	1		1		1
123	120	Cyber attacks in the era of covid-19 and possible	125			2020	Scholar	1	1	1	1	1	1		1
124	121	Ten Deadly Cyber Security Threats Amid COVID-19				2020	Scholar	1	1	1	1		1		1
125	122	Working from home during COVID-19 crisis: a cyber		126		2022	Scholar	1	1	1	1	1	1		
126	123	Working from home: cybersecurity in the age of COVID-				2020	Scholar	1	1	1	1	1			1
127	124	Home working and cyber security–an outbreak of	127,128,129			2020	Scholar	1	1	1	1		1		
128	125	The Increase in Security Breaches through Remote		132		2022	Scholar	1	1	1	1	1			
129	126	Home working: preparing your organisation and staff				2022	Scholar	1	1	1	1	1			
130	127	Remote Working and (In) Security		133		2021	Scholar	1	1	1	1	1	1		
131	128	The Walls Have Ears: Gauging Security Awareness in a		134		2023	Scholar	1	1	1	1	1			
132	129	Cyber Security and COVID-19 Pandemic				2021	Scholar	1	1	1	1	1	1		1
133	130	Towards Assessing Organizational Cybersecurity Risks via Remote Workers' Cyberslacking and Their				2022	Scholar	1	1	1	1				
134	131	Addressing telecommuting in cyber security		135		2022	Scholar	1	1	1	1	1			1
135	132	Cyber Security and the Remote Workforce. Computer	136			2020	Scholar	1	0						
136	133	Remote working and Cyber Security: Literature Review				2021	Scholar	1	1	1	1		1		1
137	134	Cybersecurity during COVID-19				2020	IEEE	1	1	1	0				
138	135	Challenges and Threats of Mass Telecommuting: A		140,141		2021	Scholar	1	1	1	1	1			
139	136	Securing a Remote Workforce		142,143		2021	Scholar	1	1	1	1				1
140	137	Develop and adopt the organizational cybersecurity		144,145		2022	Scholar	1	1	1	1	1	1		1
141	138	Recommendations for maintaining data security when working remotely: Interviews with IT stakeholders		146		2022	Scholar	1	1	1	1	1			
142	139	Cybersecurity risks in a pandemic				2020	Scholar	1	1	1	1	1			
143	140	Interpol report shows alarming rate of cyberattacks				2020	Scholar	1	1	1	1	1			1
144	141	Security for Telecommuting and Broadband Communications: Recommendations of the National				2020	Scholar	1	1	1	1				
145	142	Impact of COVID-19 on cybersecurity				2022	Scholar	1	1	1	1	1			1
146	143	A study on how the pandemic changed the				2021	Scholar	1	1	1	1	1		1	
147	144	Keeping critical assets safe when teleworking is the				2020	Scholar	1	0						
148	145	A descriptive study on cybersecurity challenges of working from home during COVID-19 pandemic and a				2021	Scholar	1	1	1	1	1	1		
149	146	The Rise of Telework and the Struggle Towards Cyber				2021	Scholar	1	1	1	1	1			

Abbildung 16 - Ausschnitt der Konzeptmatrix

7.1.1 Ergebnisse nach Jahren

Werden die gefundenen Quellen nach dem Jahr der Veröffentlichung sortiert, so ist zu erkennen, dass mit Ausbruch der Coronapandemie im Jahr 2019 ein extremer Anstieg der Veröffentlichungen zu erkennen ist. Abbildung 17 zeigt diesen Trend. Durch den extremen Anstieg der Remotearbeitsplätze wurde das Gefahrenpotenzial vervielfacht. Dadurch stieg auch die Anzahl der Publikationen, die sich diesem Thema widmeten, an. Um eine breitere Datenbasis für diese grafische Darstellung zu erreichen, wurden ebenfalls alle gesichteten Quellen nach Jahren sortiert. Der Trend ist hier ebenfalls eindeutig zu erkennen.

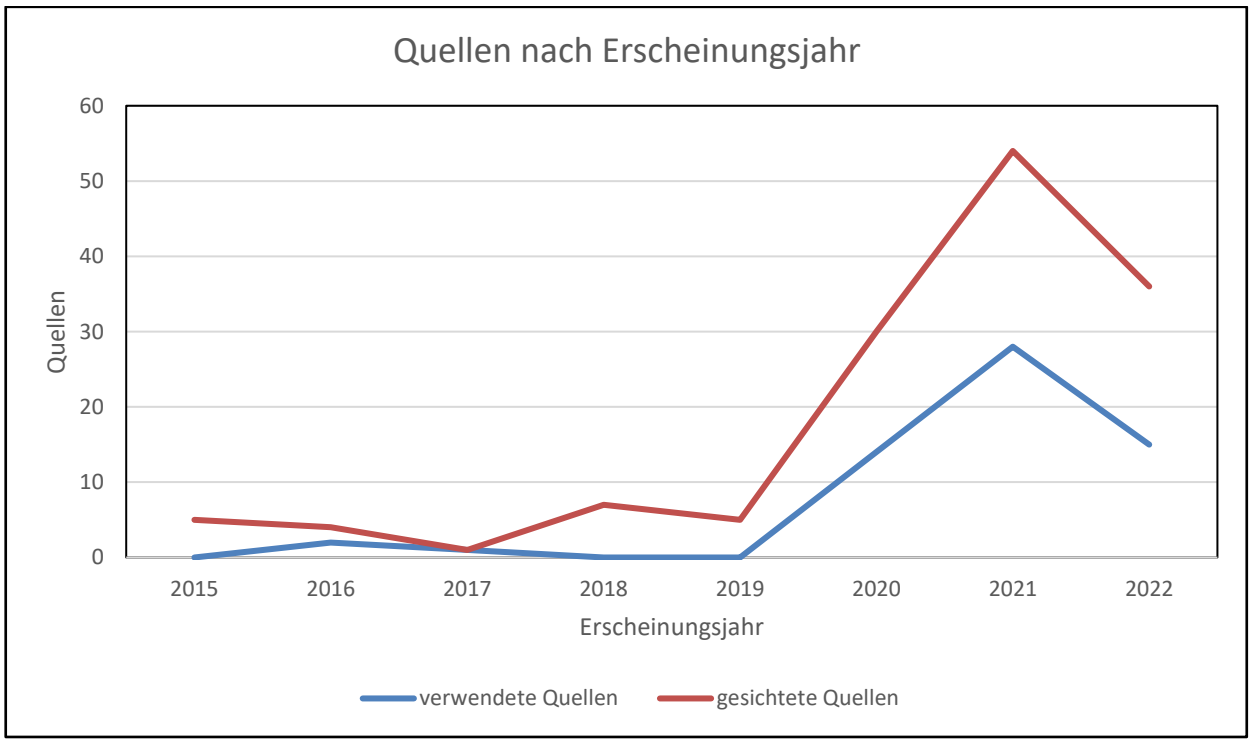

Abbildung 17 - Quellen nach Erscheinungsjahr

7.1.2 Ergebnisse nach Datenbanken

Insgesamt wurden vier Datenbanken für die Literaturrecherche verwendet. 59 der insgesamt 63 verwendeten Quellen stammen aus der Google Scholar Datenbank. Drei Quellen stammen aus der Base Datenbank und eine Quelle aus der ScienceDirect Datenbank. Die Quellen der IEEE-Datenbank waren entweder Duplikate oder wurden durch die vier Kriterien entfernt. Grund der Einseitigkeit ist, dass bei allen 60 Duplikaten immer Google Scholar als Basis Datenbank verwendet wurde und daher die Einträge der anderen Datenbanken entfernt wurden. Ein weiterer Grund war, dass die „forward-search“ bei Google Scholar am einfachsten durchzuführen ist. Die folgende Abbildung veranschaulicht das Verhältnis der verwendeten Datenbanken.

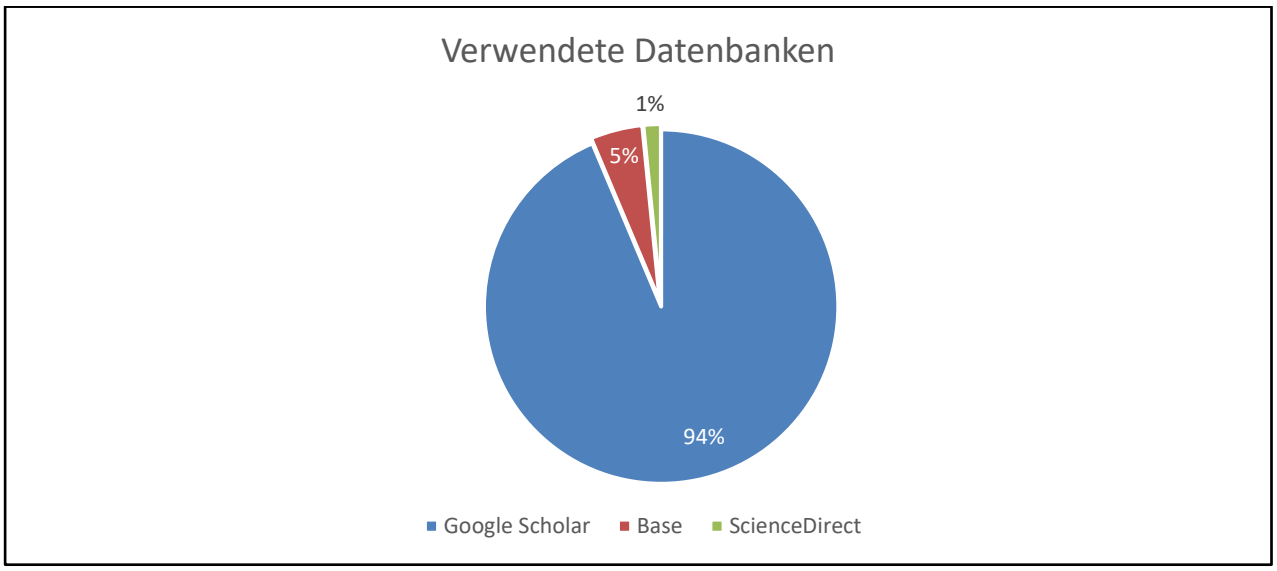

Abbildung 18 - Quellen nach Datenbanken

7.1.3 Ergebnisse - Angriffsart

Die Angriffsart gibt Auskunft darüber, welche Typen von Angriffen vermehrt in Verbindung mit der Telearbeit ein Risiko darstellen.

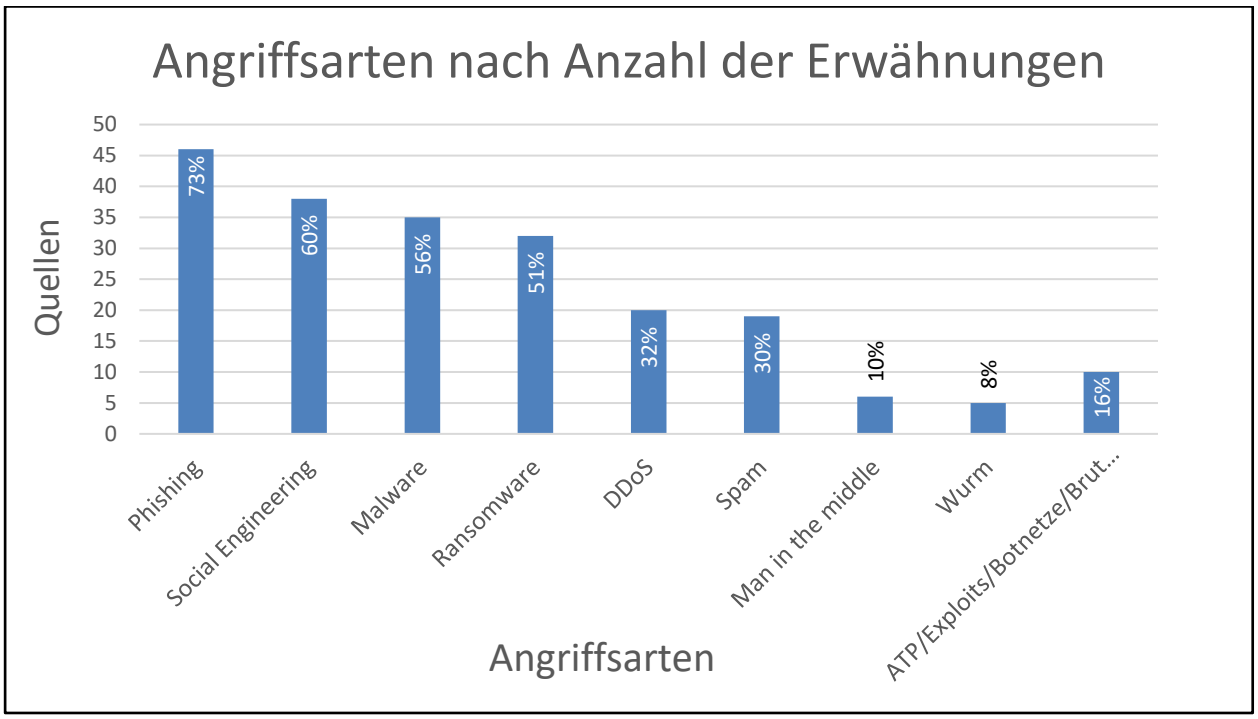

Abbildung 19 - Ergebnisse Angriffsart

Die Recherche zeigte, dass in 73 Prozent der Quellen Phishing als Angriffsvektor erwähnt wird. Social Engineering wird in 60 Prozent der Quellen diesbezüglich erwähnt, dicht gefolgt von Malware und Ransomware, welche beide noch in über 50 Prozent der Paper genannt werden.

7.1.4 Ergebnisse - Angriffskanal Nutzer

Dieses Kapitel soll jene Kanäle aufzeigen, über die Angreifer versuchen, den User zu erreichen und mit dessen Hilfe sie ins System eindringen versuchen.

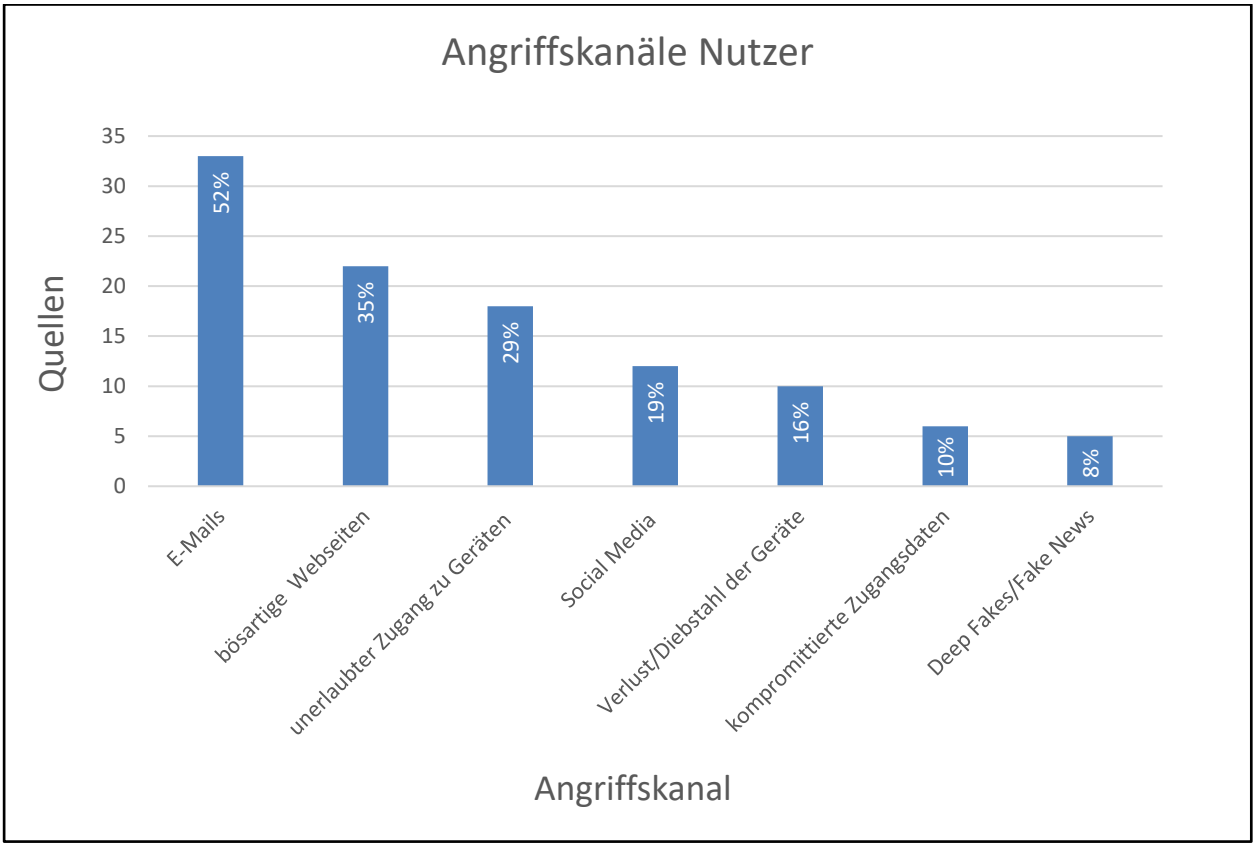

Abbildung 20 – Ergebnisse - Angriffskanal Nutzer

Die User werden laut Recherche am öftesten per E-Mail angegriffen. In mehr als der Hälfte der Quellen wird dieser Kanal als risikoreich identifiziert. Auch bösartige Webseiten stellen für User laut Recherche ein großes Problem dar. Unerlaubter Zugriff auf Geräte, damit ist der Zugriff durch Familienmitglieder, Besucher oder auch shoulder surfing durch Fremde gemeint, wird in beinahe einem Drittel der Quellen als Angriffsvektor genannt.

Vergleicht man die Ergebnisse mit einer Studie von Statista aus dem Jahr 2021 so wurden bereits im Jahr 2019 mit Abstand betrügerische Nachrichten und gefälschte Webseiten als die häufigsten Sicherheitsvorfälle, die durch Menschen ausgelöst wurden, erkannt. Auch Social Media als Einfallstor wurde hier bereits erwähnt.

7.1.5 Ergebnisse - Angriffskanal System

Nicht nur der User stellt eine Gefahr für die IT-Systeme dar, die Angreifer können auch durch Schwachstellen der verwendeten Assets (Hardware als auch Software) Zugriff auf die IT-Infrastruktur erlangen. Abbildung 21 zeigt die in der Literatur erkennbaren Ergebnisse.

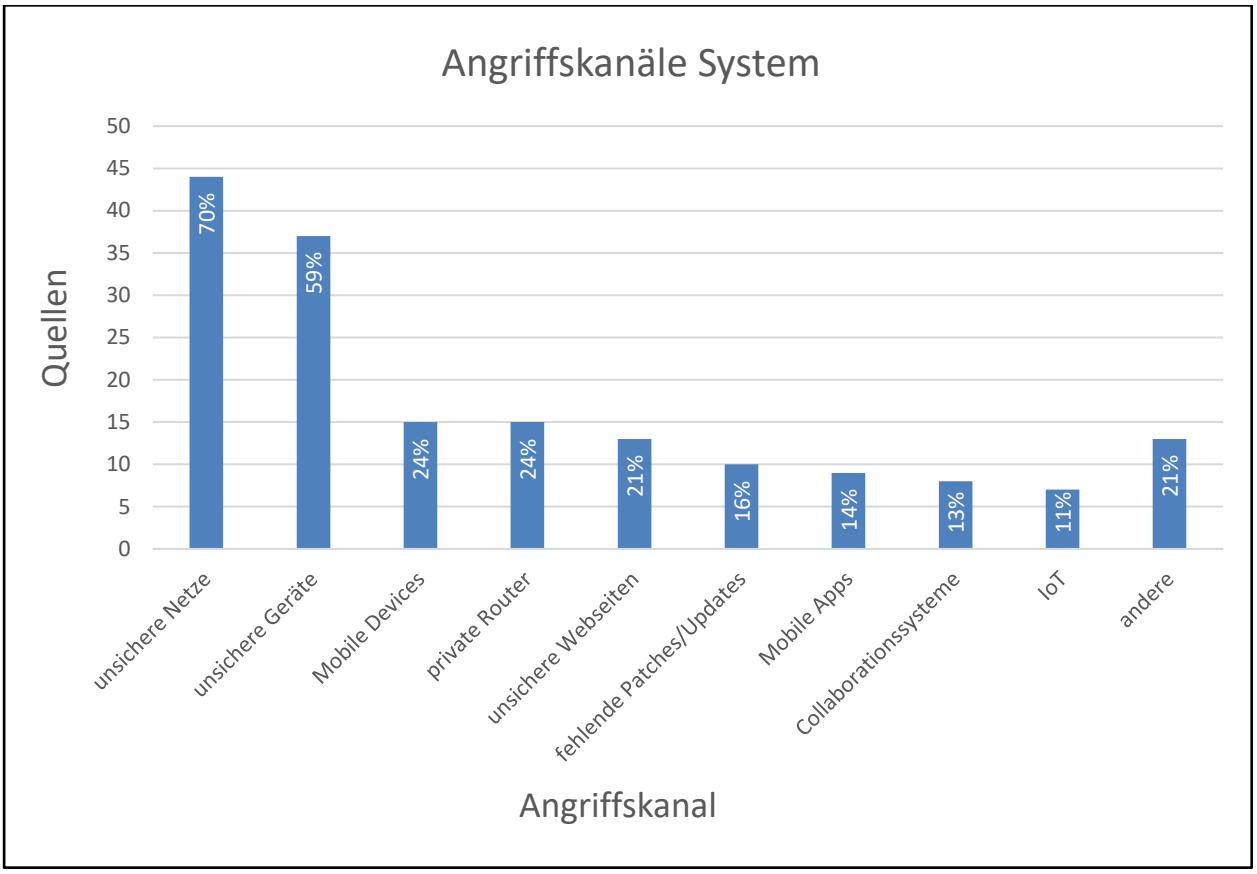

Abbildung 21 – Ergebnisse - Angriffskanal System

Die Recherche zeigte klar auf, dass unsichere Netze, wie öffentliche Hotspots oder schlecht geschützte WLAN-Verbindungen, das größte Gefahrenpotenzial bergen. Unsichere Geräte, wie zum Beispiel BYOD, welche zu einer Schatten-IT führen, werden am zweithäufigsten als Gefahrenquelle genannt. Auch Smartphone und private, meist schlecht geschützte Router werden in knapp einem Viertel der Quellen erwähnt. Schlecht geschützte Webseiten werden auch immer wieder angegriffen und kommen daher in 21 Prozent aller Quellen vor.

Die Kaspersky Labs GmbH (2023) listet auf ihrer Homepage IT-Sicherheitstipps für das Homeoffice auf. Als primärer Punkt wird dort die Absicherung des Netzwerks genannt. WLAN-Absicherung, ändern von SSIDs als auch Updates und geänderte Passwörter für den Router sind weitere Themen.

Auch Karl (2023) erwähnt als erstes Risiko die privaten Netzwerke. Als zweites Risiko wird die Verwendung von privaten Geräten erwähnt.

7.1.6 Ergebnisse - Technische Sicherheitssysteme

Um all die, in den vorigen Kapitel genannten, Gefahren minimieren zu können, stehen verschiedene technische Sicherheitssysteme zur Verfügung. Diese wurden im Zuge der Literaturrecherche anhand der im Theorieteil beschriebenen Systeme einzuordnen versucht. Während der Recherche wurde die Matrix um zusätzliche, in den Quellen gefundene, Sicherheitssysteme erweitert, um die Forschung nicht durch eine zu enge Definition des Recherchebereichs zu verfälschen.

Bei den technischen Sicherheitssystemen werden einige Schutzmaßnahmen des von Henseler-Unger et al. (2018) in Kapitel 3.2.1 genannten Basisschutzes mitangeführt. Weiters wurden einige Sicherheitsvorkehrungen recherchiert, welche diesen Basisschutz übersteigen, aber nicht explizit in der Theorie erwähnt wurden.

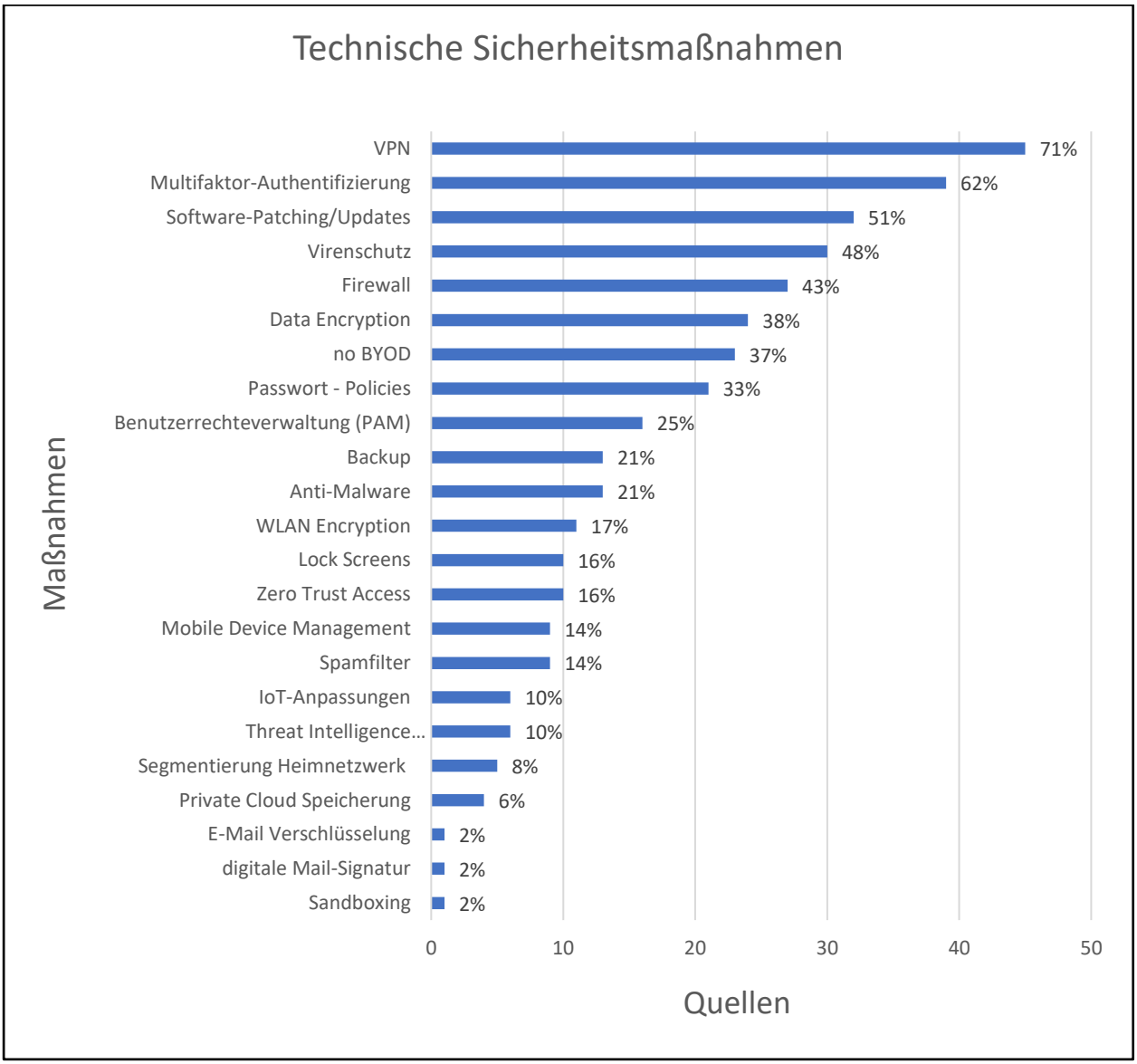

Abbildung 22 – Ergebnisse - Technische Sicherheitsmaßnahmen

Die Literaturrecherche zeigte, dass in Verbindung mit Telearbeit der VPN-Zugang zum internen Firmennetzwerk als äußerst wichtig angesehen wird. In 71 Prozent aller Quellen wurde dieser als effektive Schutzmaßnahme gegen Angreifer erwähnt. Ein weiterer wichtiger Sicherheitsfaktor ist die Authentifizierung, Multifaktor-Authentifizierung (62 Prozent), Passwort-Policies (33 Prozent) und Benutzerrechteverwaltung (25 Prozent) sind in der oberen Hälfte der 23 genannten Sicherheitsmaßnahmen angesiedelt. Die im Kapitel 3.2.1 Basisschutz genannten Schutzmaßnahmen finden sich ebenfalls vollumfänglich in der Auswertung wieder. Im Kapitel 8.2 Interpretation der Ergebnisse wird auf dem bereits bestehenden Wissenstand bezüglich der Absicherung der Unternehmen aufgebaut und mit den Ergebnissen der Literaturrecherche verglichen.

7.1.7 Ergebnisse - Organisatorische Sicherheitssysteme

Neben den technischen Möglichkeiten, Cyberangriffe effektiv abzuwehren, gibt es auch Ansätze seitens der Organisation, solchen Bedrohungen vorzubeugen. Im Kapitel 3.1 Organisatorische Sicherheitsmaßnahmen wurden bereits die verschiedenen Möglichkeiten erwähnt. Mittels der Recherche wurden folgende Ergebnisse gewonnen.

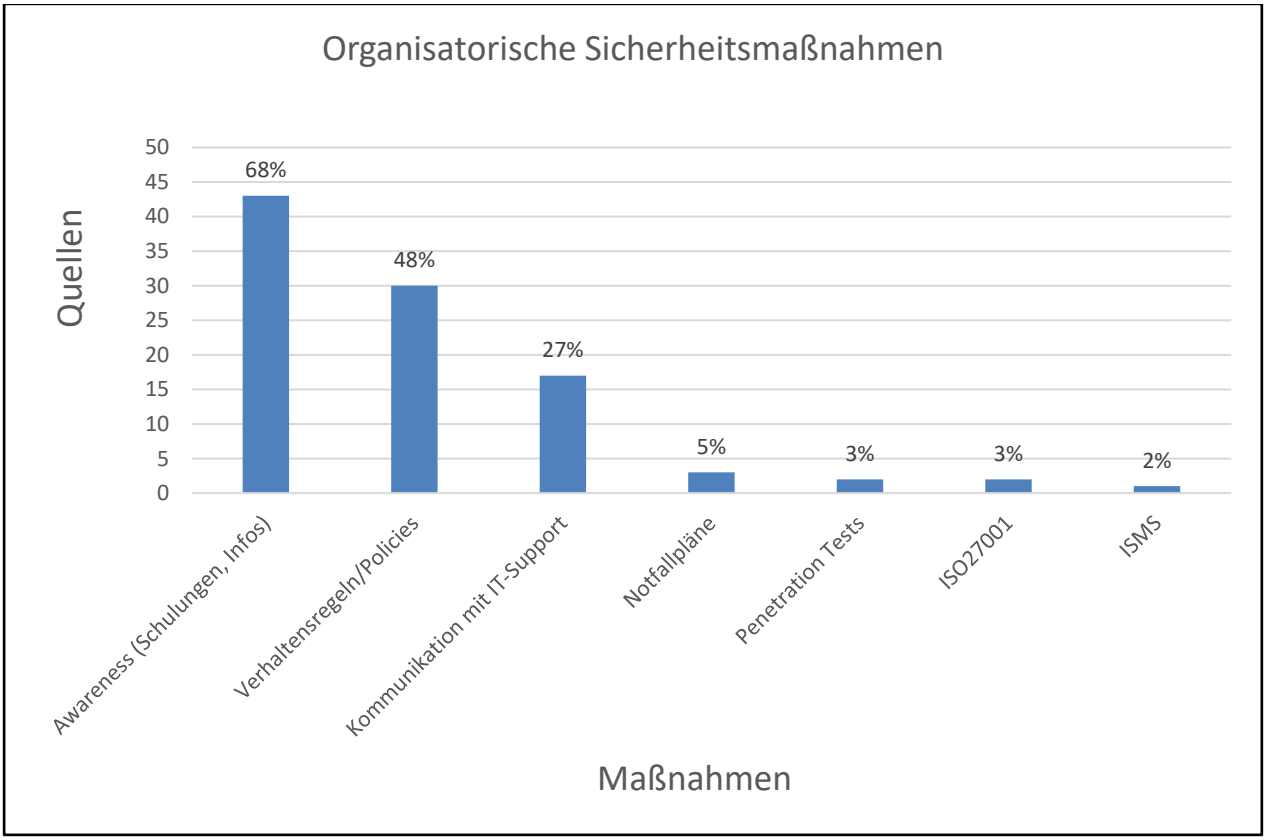

Abbildung 23 - Ergebnisse - Organisatorische Sicherheitssysteme

Die Awareness wurde bereits in der Theorie als wichtiger Faktor zum Schutz vor Cyberangriffen erwähnt. Die Ergebnisse der Literaturrecherche untermauern diese Aussage. In 68 Prozent der Quellen wurden die Awareness der Mitarbeiterinnen und Mitarbeiter in Telearbeit als wichtig erwähnt. Auch die Verhaltensregeln, welche die Arbeitsweise in der Telearbeit bezugnehmend auf die IT-Sicherheit vorgibt, spielt eine wichtige Rolle beim Schutz vor Angreifern.

In 27 Prozent der Papers wurde ebenfalls die nötige, wichtige als auch sofortige Kommunikation mit dem IT-Support-Team erwähnt. Hier geht es darum, eventuelle Fehler im Vorhinein zu vermeiden oder bei bereits gemachten Fehlern die IT-Teams sofort zu informieren, um etwaige, folgende Probleme zumindest eindämmen zu können. Allumfassende Sicherheitsansätze wie ein Informationssicherheitsmanagementsystem oder die dadurch mögliche ISO 27001 Zertifizierung werden nur am Rande erwähnt.

In einer Studie vom Bundesamt für Sicherheit in der Informationstechnik (2021) wurde ebenfalls die Mitarbeiterinnen- und Mitarbeitersensibilisierung als primärer Vektor zur Vermeidung von erfolgreichen Angriffen genannt. Auch die Punkte Notfallpläne, ISMS und Richtlinien in Form einer IT-Sicherheitsstrategie werden hier unter den zehn am meisten umgesetzten organisatorischen Sicherheitsvorkehrungen genannt.

8 SCHLUSSFOLGERUNGEN

Das Ziel dieses Kapitels besteht darin, die zentralen Aspekte der vorliegenden Arbeit zu bündeln und die Erkenntnisse aus dem vorherigen Kapitel auszuwerten, um eine solide Grundlage für die Hypothesenprüfung zu schaffen. Des Weiteren wird im Anschluss an die Überprüfung der Hypothesen eine Handlungsempfehlung für den Einsatz von Sicherheitsmaßnahmen in der Telearbeit ausgesprochen und in diesem Zuge auch die Forschungsfrage beantwortet. Die Handlungsempfehlung wird als Kano-Modell dargestellt, um eine gewisse Unterscheidung bei der Notwendigkeit der Sicherheitsmaßnahmen vornehmen zu können. Abgerundet wird das abschließende Kapitel durch eine kurze kritische Reflexion sowie einen Blick auf die Beschränkungen dieser Masterarbeit und mögliche Forschungsoptionen.

8.1 Zusammenfassung

Im ersten, theoretischen Teil der Arbeit wurde zu Beginn das Problem erfasst und ein genaues Ziel definiert.

Daraus ergab sich die Forschungsfrage, welche durch diese Arbeit beantwortet werden sollte. Auf Basis der Theorieausarbeitung konnten Hypothesen erkannt und aufgestellt werden. Diese Hypothesen sollten bei der Beantwortung der Forschungsfrage unterstützen.

In den Kapiteln 2 bis 4 wurde die notwendige Theorie zu dem Thema der Arbeit erfasst. Es wurde das Thema Cybercrime samt Begriffsdefinitionen und Geschichte in Kapitel 2 erarbeitet. Auch die verschiedenen Typen von Cyberangriffen und die genutzten Schwachstellen wurden in diesem Kapitel angeführt.

Kapitel 3 widmete sich den Maßnahmen, die getroffen werden können, um sich effektiv vor Cyberbedrohungen zu schützen. Hier wurden die Maßnahmen in technisch und organisatorisch eingeteilt, um einen besseren Überblick zu erhalten.

Zum Abschluss des Theorieteils wurde in Kapitel 4 die Telearbeit genauer behandelt. Die genaue Begriffsdefinition war hier von wichtiger Bedeutung. Auch speziell für die Telearbeit wichtige Sicherheitsmaßnahmen wurden in diesem Kapitel zusammengefasst.

Kapitel 5 und 6 beschäftigten sich mit dem empirischen Teil der Masterarbeit. Kapitel 5 erklärte den grundsätzlichen Aufbau dieser empirischen Forschung mit den einzelnen Phasen, die dabei durchlaufen werden. In Kapitel 6 wurde die Methodik der Arbeit genauer beschrieben. Da die Literaturrecherche als Methode gewählt wurde, musste hier noch der Unterschied zwischen systematischer und unsystematischer Literaturrecherche erarbeitet werden. Danach wurde die gewählte Methode in ihren einzelnen Phasen erklärt und parallel dazu die durchgeführten Schritte in jeder einzelnen Phase dokumentiert.

In Kapitel 7 wurden alle Ergebnisse der Literaturrecherche grafisch dargestellt und erklärt. In diesem Kapitel werden nun diese Ergebnisse genauer betrachtet und interpretiert. Die Interpretation und die damit einhergehende Beantwortung der Hypothesen bildet schlussendlich die Grundlage zur Beantwortung der Forschungsfrage, welche in Form eines Kano-Modells dargestellt wird.

8.2 Interpretation der Ergebnisse

Dieses Kapitel soll nun die Ergebnisse in Kontext zu bereits bekanntem Wissen setzen um eventuelle Ungereimtheiten, Schwachstellen oder Handlungsansätze zu erkennen.

8.2.1 Interpretation - Angriffsarten

Die Ergebnisse, bezogen auf die Angriffsarten, zeigen ein klares Bild. Die beiden meist genannten Angriffsarten weisen auf die Wichtigkeit der User hin, da diese Angriffsfläche erst durch die ungewollte Mithilfe der Telearbeiterinnen und Telearbeiter geboten wird.

Untermauern lassen sich die gewonnen Daten durch eine Umfrage von Bitkom (2022). Mehr als 1000 Unternehmen wurden zu den Schäden durch IT-Angriffe in den letzten 12 Monaten befragt. Dabei wurde Phishing ebenfalls am häufigsten genannt. Malware, DDoS Attacken, Ransomware und Mittelsmann – Angriffe waren auch hier unter den zehn meistgenannten Angriffsarten.

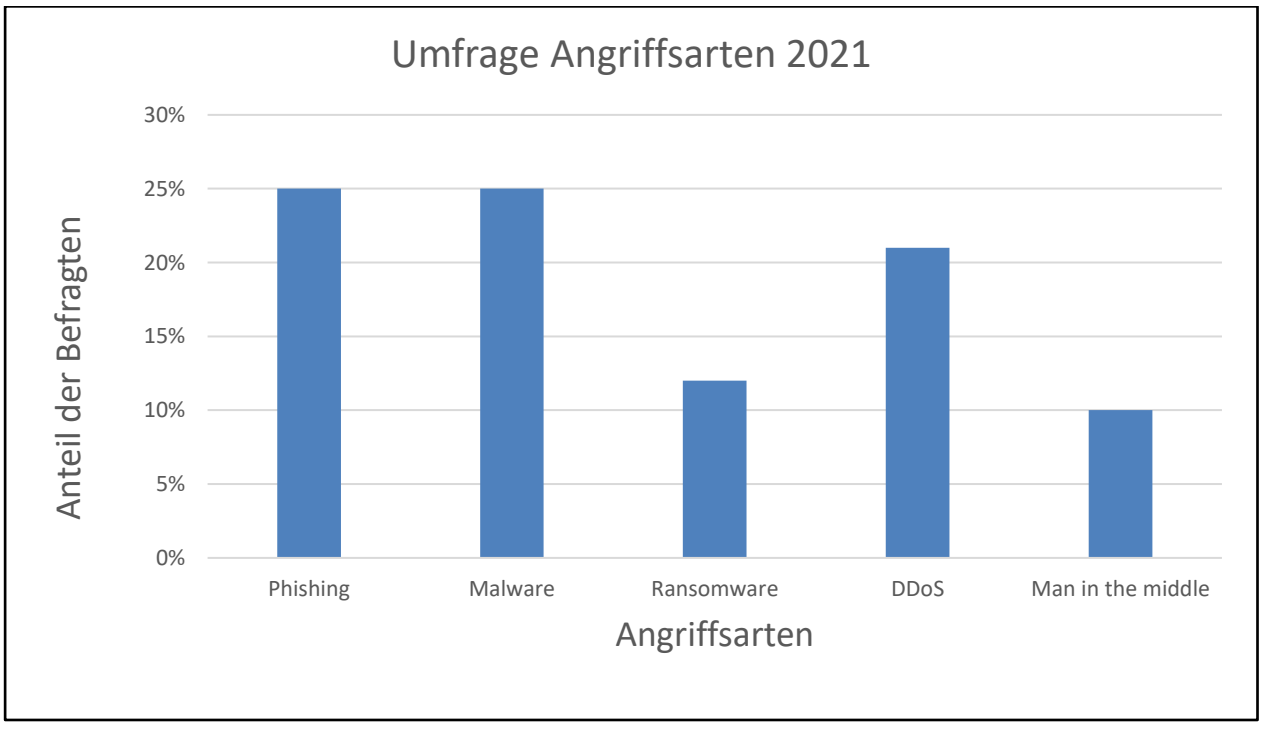

Abbildung 24 - Angriffsarten 2021 (in Anlehnung an Bitkom, 2022)

Einzig Ransomware-Angriffe werden von den Befragten weniger oft genannt, als die Recherche ergeben hat.

Ein möglicher Grund hätte hier die Entwicklung 2022 sein können. Laut den Quellen der Literaturrecherche nimmt der Anteil von Ransomware-Angriffen immer mehr zu. Jedoch kann dieser Umstand nicht durch die Nennungen pro Jahr in den Quellen bestätigt werden.

8.2.2 Hypothesen - Angriffsarten

H1: Phishing wird als größtes Sicherheitsrisiko bei der Telearbeit erkannt.

H0: Phishing ist im Bereich der Telearbeit keine relevante Angriffsart.

Durch die Literaturrecherche wurde klar, das Phishing mit einer Nennung in 73 Prozent der Quellen die größte Rolle im Bereich der Angriffsarten einnimmt. Durch eine weitere Studie (Bitkom, 2022) wurde diese Erkenntnis noch untermauert.

Aus diesem Grund wird die Nullhypothese verworfen und die Alternativhypothese bestätigt.

Jedoch ist eine zyklische Betrachtung dieser Hypothese von Nöten, da der Bereich der Cyberangriffe immer neue Varianten mit sich bringt.

8.2.3 Interpretation - Angriffskanal Nutzer

Durch die Literaturrecherche wurde herausgefunden, dass Angriffe meist über E-Mails eingeleitet werden, die der Benutzer nicht als schadhaft wahrnimmt. Auch die Anzahl der bösartigen Webseiten ist ein massiver Angriffsvektor. Fake-Seiten wie Corona-Informations-Webseiten traten laut Recherche vermehrt auf. Ein in der Theorie nicht behandelter Punkt spielt ebenfalls eine nicht unwesentliche Rolle und muss daher ein Bestandteil der Handlungsempfehlung sein. Der unerlaubte Zugang zu IT-Gerätschaften wurde in 29 Prozent der Quellen als Sicherheitsrisiko eingestuft. Gemeinsame Nutzung der Geräte mit Familienmitgliedern oder Mitbewohnerinnen und Mitbewohnern, aber auch das bekannte shoulder surfing in der Öffentlichkeit sind ein nicht zu unterschätzendes Risiko. Bei der Interpretation der Sicherheitssysteme wurde abgeglichen, ob technische Systeme hier mitbedacht wurden oder, ob hier organisatorische Hilfen genannt werden. Ansonsten wäre eine Nachrecherche notwendig.

Die Ergebnisse spiegeln die Umfragewerte einer EU-weit durchgeführten Befragung von Statista (2021) wider. Am meisten, insgesamt 25 Prozent aller Befragten, gaben dort an, bereits per Phishing attackiert worden zu sein. An zweiter Stelle, wie auch bei der Literaturrecherche, wurden hier bösartige Webseiten als Gefahr für den User genannt.

8.2.4 Hypothesen - Angriffskanal Nutzer

H1: Kompromittierte Webseiten stellen das größte Problem bei der Erkennung von Angriffen für den Telearbeiter / die Telearbeiterin dar.

H0: Kompromittierte Webseiten sind nicht das primäre Problem bei der Erkennung von Angriffen für den Telearbeiter / die Telearbeiterin.

Bösartige Webseiten spielen zwar eine wichtige Rolle bei dem Versuch mit Hilfe des Nutzers in das IT-System des Unternehmens einzudringen, jedoch stellt der Angriff über das Medium E-Mail das größte Gefahrenpotenzial dar. Die Literaturrecherche als auch eine repräsentative Umfrage widerlegen in diesem Fall die Alternativhypothese und bestätigen die Nullhypothese.

8.2.5 Interpretation - Angriffskanal System

Geht es um die Angriffskanäle, die unabhängig vom Nutzer angreifbar sind, stellen unsichere Netze bei der Telearbeit das größte Risiko dar. Bei unsicheren Netzen gibt es verschiedene Arten, die hier betrachtet werden müssen. Öffentliche Hotspots, private WLAN-Verbindungen ohne, oder mit schlechter Verschlüsselung sind hier vorab zu nennen. Auch unsichere LAN-Verbindungen im privaten Bereich sind ein großes Risiko, da die Geräte meist per Dynamic Host Configuration Protocol, kurz DHCP, eine IP-Adresse zugewiesen bekommen und sofortigen Zugriff zum Heimnetzwerk haben.

Bei der Verwendung von öffentlichen Hotspots für die Telearbeit wäre die grundsätzliche Empfehlung, diese nicht zu nutzen, sondern eigene vom Unternehmen gestellte Verbindungen zu verwenden. Sollte dies nicht möglich sein, ist es notwendig, genaue Richtlinien zu erstellen, um den Umfang der erlaubten Tätigkeiten in öffentlichen Netzen einzugrenzen. Private WLAN-Verbindungen können durch bessere Verschlüsselungen abgesichert werden. Auch eine Segmentierung der Netze zwischen privatem WLAN und geschäftlichem Netz wäre laut Recherche möglich. Der LAN-Zugriff sollte ebenfalls reglementiert werden. Dazu sind Routereinstellungen notwendig. Gefahren durch schlecht oder gewartete Router oder Router im Auslieferungszustand wurden ebenfalls in 24 Prozent der Paper erwähnt. Deshalb können hier Policies zur Verwendung von öffentlichen Netzen, Bereitstellung von betriebseigenen Internetverbindungen, stark verschlüsselte WLAN-Zugriffspunkte und auch die Reglementierung von LAN-Zugriffen in die Handlungsempfehlungen mitaufgenommen werden.

Unter dem Begriff unsichere Geräte fällt die Verwendung von betriebsfremder IT-Hardware als auch schlecht gewartete Systeme. Da in 59 Prozent der Quellen dies als Gefahr angegeben wird, müssen auch hier Handlungsempfehlungen erstellt werden. Die Thematik BYOD stellt hier das größte Problem dar. Laut einer Studie des Bundesamt für Sicherheit in der Informationstechnik (2020a) nutzen nur 42 Prozent der Unternehmen ausschließlich unternehmenseigene IT. Dies untermauert nochmals die Wichtigkeit dieses Angriffskanals. Da dies in den technischen Maßnahmen ebenfalls vorkommt, wird hier nur über schlecht gewartete Unternehmensgeräte

gesprochen. Eine Handlungsempfehlung wäre hier, die IT-Systeme zu verwalten und dadurch eine Härtung der Systeme durch regelmäßiges Patchen und Updaten zu erreichen.

Im privaten Bereich wurden auch die IoT-Geräte als Gefahr genannt, da diese meist über keine standardmäßigen Sicherheitseinstellungen verfügen und oft auch nicht nachträglich eingerichtet werden. Daher wäre hier eine Trennung der IoT-Geräte vom Arbeitsbereich zu empfehlen. Dies könnte durch eine Netzwerksegmentierung erreicht werden.

8.2.6 Hypothesen - Angriffskanal System

H1: Mobile Endgeräte stellen das größte Risiko bei Angriffen auf die IT-Systeme der Unternehmen dar.

H0: Mobile Endgeräte spielen eine untergeordnete Rolle als Angriffsvektor.

Durch die systematische Literaturrecherche ergab sich das Bild, dass die Verbindungen, die zur Telearbeit genutzt werden, die primäre Problematik darstellen. Durch bestehende Literatur von Karl (2023) und Kaspersky Labs GmbH (2023) konnte diese Sichtweise auch nochmals untermauert werden. Mobile Endgeräte fanden zwar in 24 Prozent der Quellen Erwähnung, stellen hier aber ein untergeordnetes Risiko dar.

Deshalb wird die Nullhypothese durch diese Arbeit bestätigt.

8.2.7 Interpretation - Technische Sicherheitssysteme

Bei der Interpretation der Ergebnisse bei den technischen Sicherheitssystemen wird auf bestehende Informationen zurückgegriffen, um die Ergebnisse einordnen zu können, aber auch, um die Ausbreitung der einzelnen Maßnahmen zu erkennen, um dadurch Handlungsempfehlungen erstellen zu können.

Bei der Literaturrecherche wurden eindeutig Sicherheitsmaßnahmen, die meist in Verbindung mit Telearbeit auftreten, am öftesten genannt. VPN als auch Multifaktor-Authentifizierung weisen darauf hin. Vermutlich liegt das daran, dass jene Maßnahmen, die als Basisschutz gelten, nicht explizit für Telearbeit nötig sind, sondern eine allgemeine Wichtigkeit beim Schutz von IT-Systemen darstellen. Dennoch finden all diese Maßnahmen auch Erwähnung und werden in die Handlungsempfehlungen miteinfließen.

Auffällig ist auch, dass einige der Maßnahmen bei der Literaturrecherche des Theorieteils noch keine Erwähnung fanden. Beispiel dafür sein Gerät zu schützen ist der Sperrbildschirm oder auch die Verschlüsselung der Datenträger.

Als weitere Handlungsempfehlung kann hier ein „Nein“ zu einer BYOD-Strategie genannt werden. In 37 Prozent aller Paper wird dies vorgeschlagen.

Überraschend war, dass trotz massiver Erwähnung des Angriffskanals E-Mail die digitale E-Mail-Signatur beziehungsweise die Verschlüsselung der E-Mails nur ein einziges Mal als technische

Maßnahme erwähnt wurden. Vermutlich ist eine Umsetzung eines solchen Systems nicht für jedes Unternehmen realistisch. Dennoch muss es bei den Handlungsempfehlungen genannt werden. Hier wäre vielleicht ein Ansatz für eine weitere Arbeit zu finden. Es könnten die Gelingensbedingungen bei der Einführung einer solchen Schutzmaßnahme erforscht werden.

8.2.8 Hypothesen - Technische Sicherheitssysteme

H1: VPN wird als wichtigstes, technisches Sicherheitssystem im Einsatz gegen Cyberangriffe bei der Telearbeit angesehen.

H0: VPN spielt eine untergeordnete Rolle beim Schutz vor Cyberangriffen bei der Telearbeit.

Durch die Literaturrecherche wird bestätigt, dass der VPN als wichtigstes Instrument zum Schutz der IT-Struktur des Unternehmens beiträgt. Henseler-Unger et al. (2018) unterstreichen mit einer Umfrage unter 1505 KMUs diese Einschätzung. 86 Prozent der Befragten (Höchstwert) sehen den VPN als notwendig an.

Somit kann die Nullhypothese widerlegt werden und die die Alternativhypothese bestätigt werden.

H1: Verschlüsselung des Mailverkehrs spielt eine wichtige Rolle beim Schutz der Unternehmenssysteme.

H0: Momentan wird die Verschlüsselung des Mailverkehrs nicht als notwendige Maßnahme angesehen.

Zum Zeitpunkt der Erstellung dieser Arbeit findet die E-Mail-Verschlüsselung nur einmalig in allen durchsuchten Quellen Erwähnung. Daher wird in diesem Punkt die Nullhypothese bestätigt, jedoch kann die Alternativhypothese nicht widerlegt werden.

8.2.9 Interpretation - Organisatorische Sicherheitssysteme

Die Ergebnisse der Literaturrecherche sprechen hier eine klare Sprache. Hauptaugenmerk muss auch bei den Handlungsempfehlungen auf die Awareness der Mitarbeiterinnen und Mitarbeiter in der Telearbeit gelegt werden. Schulungen, Infos und zyklische Überprüfungen werden immer wieder als Notwendigkeit genannt.

Als neue Erkenntnis kann die gute Kommunikation mit dem IT-Support genannt werden. Es wird hier von der Vermeidung von Problemen als auch von der möglichen, schnellen Reaktion des IT-Personals auf etwaige Angriffe geschrieben. Eine Handlungsempfehlung dahingehend wäre die Einrichtung eines direkten Kommunikationskanals zum IT-Personal. Seitens des Unternehmens wäre die Handlungsempfehlung ein Bereitschaftsdienst, um diesen Kanal ohne Verzögerung zu bespielen.

Organisatorische Maßnahmen, welche einen größeren IT-Aufwand benötigen würden, werden zwar erwähnt, jedoch spielt hier vermutlich der, in den Quellen öfters aufgezeigte, Mangel an IT-Personal eine große Rolle.

8.2.10 Hypothesen - Organisatorische Sicherheitssysteme

H1: Je aktueller die Quellen, desto öfter werden Richtlinien für die Telearbeit als notwendig erwähnt.

H0: Es ist kein Trend erkennbar, der auf einen Anstieg von Richtlinien für die Telearbeit hinweist.

Um diese Hypothesen bestätigen oder widerlegen zu können, wurde die Anzahl der jährlichen Erwähnungen im Verhältnis zu der Anzahl der gesichteten Quellen gesetzt. Wie in Abbildung 25 ersichtlich, ist hier ein klarer Trend zu erkennen. Erst mit Ausbruch der Coronapandemie und des damit verbundenen, vermehrten Einsatzes von Telearbeit ist die Wichtigkeit von Richtlinien, welche das Verhalten bei der Telearbeit definieren, gestiegen. Deshalb kann die Alternativhypothese bestätigt werden.

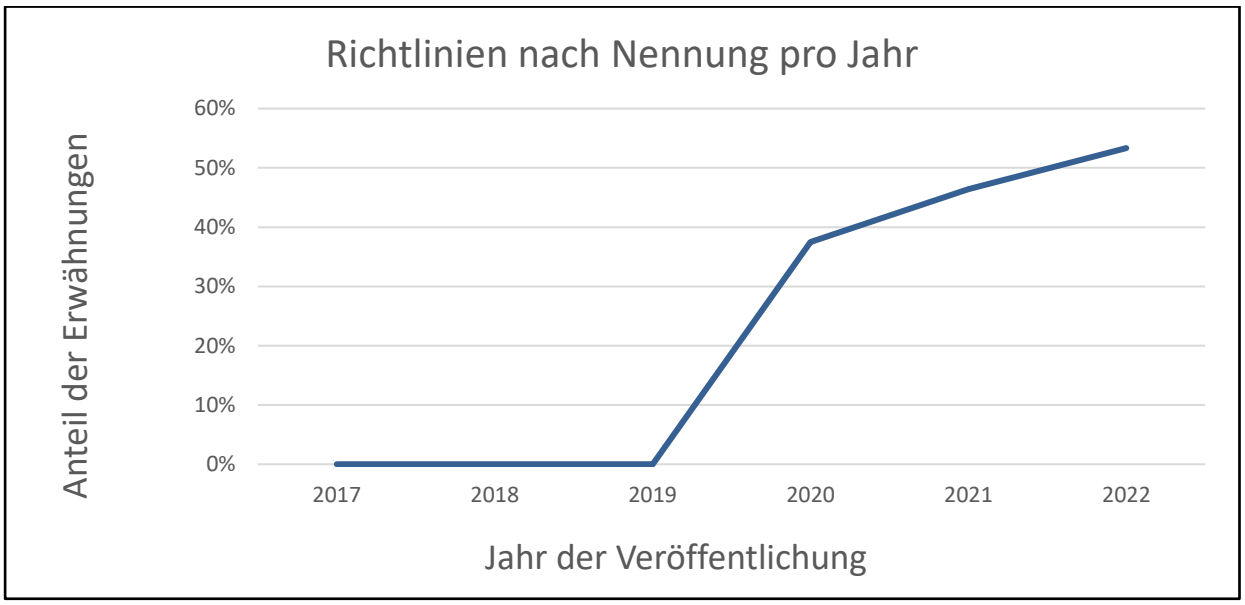

Abbildung 25 - Entwicklung der Erwähnungen von Richtlinien bei der Telearbeit

8.3 Erkenntnisse der Interpretation

Durch die systematische Literaturrecherche konnten in den fünf benannten Bereichen viele Informationen gewonnen werden, um eine umfassende Handlungsempfehlung erarbeiten zu können.

Im Bereich der Angriffsarten wurde der dafür notwendige Grundstein gelegt. Es sollten dadurch die Gefahren aufgezeigt werden und die Sicherheitsvorkehrungen daraufhin überprüft werden, ob für die jeweiligen Angriffsarten ein Schutz genannt wurde.

Durch die organisatorische Sicherheitsmaßnahmen Awarenesstraining und Richtlinien in der Telearbeit wurden die Angriffsarten Phishing und Social Engineering bereits bearbeitet. Technische Sicherheitsmaßnahmen wie Anti-Malware, Spamfilter und E-Mail-Verschlüsselung

decken weitere Angriffsarten wie Spam, Malware und auch Phishing ab. Der Einsatz von Firewalls kann DDoS Angriffen entgegenwirken.

Auch im Bereich der Angriffskanäle, den Nutzer betreffend, konnten einige Empfehlungen erkannt werden und nach Vorhandensein in den Maßnahmen abgefragt werden. So wird der Angriffskanal E-Mails durch die bereits erwähnten Maßnahmen Spamfilter, E-Mail-Verschlüsselung und auch Sandboxing überwacht.

Ebenso wird der unerlaubte Zugang zu den Gerätschaften durch einen Sperrbildschirm, Passwort-Policies und Benutzerrechteverwaltung in die Handlungsempfehlung eingepflegt. Zusätzlich wäre ein versperrbarer Bereich für das Homeoffice eine Empfehlung. Achtsamkeit in der Öffentlichkeit betreffend shoulder surfing sollte in den Richtlinien für Telearbeiterin und Telearbeiter niedergeschrieben werden. Der Umgang mit relevanten Daten auf Social Media sollte ebenfalls in diesen Richtlinien niedergeschrieben und in Awarenessschulungen gelehrt werden. Die Gefahren durch Verlust und Diebstahl der Geräte könnte durch Verschlüsselung der Datenträger vermindert werden. Auch Passwortrichtlinien schützen hier. Schutz vor kompromittierten Zugangsdaten bietet zum einen der Umgang mit diesen Daten. Dies sollte auch in Telearbeit-Richtlinien erfasst sein. Andererseits könnten Passwort-Management-Tools bei der Aufbewahrung von Zugangsdaten helfen.

Es konnten auch einige Informationen aus den Angriffskanälen des Systems gewonnen werden. Zum Beispiel können unsichere Netze durch sichere, vom Unternehmen zur Verfügung gestellte, Internetverbindungen vermieden werden. Auch Anpassungen am privaten Router würden die Arbeit sicherer gestalten. Updates, Patches und veränderte Zugangsdaten zum Router wären hier probate Mittel und sollten in die technischen Maßnahmen mitaufgenommen werden. Ändern der SSID, verstärken der Verschlüsselung und auch Segmentierung des privaten Netzes sind ebenfalls zu empfehlen. Diese Segmentierung würde auch die IoT-Geräte vom beruflich genutzten Netz trennen.

Unsichere Geräte werden durch die Ausstattung mit dem Basisschutz, durch regelmäßiges Patchen und Updaten als auch durch ein grundsätzliches Verbot zum Nutzen privater Geräte, bei der Telearbeit erreicht. Im Bereich der mobilen Endgeräte ist ein Mobile Device Management System zu empfehlen. Bei eigenen Webseiten und bei den eingesetzten Collaborationssystemen gilt eine Update- und Patch Empfehlung.

Nachdem nun alle Gefahren und Maßnahmen erfasst und zugeordnet wurden, folgt abschließend im Kapitel 9 die Beantwortung der Forschungsfrage.

9 BEANTWORTUNG DER FORSCHUNGSFRAGE

Mit Hilfe der gewonnen Kenntnisse aus der systematischen Literaturrecherche kann nun eine Handlungsempfehlung abgegeben werden. Diese wird grafisch in Form eines Kano-Modells umgesetzt.

Das Kano-Modell beschreibt laut Sauerwein et al. (1996) drei Arten von Merkmalen, die ein Produkt oder eine Dienstleistung haben kann.

1. Basismerkmale: Das sind grundlegende Anforderungen, die Kunden als selbstverständlich betrachten und erwarten. Wenn diese Anforderungen nicht erfüllt werden, führt das zu Unzufriedenheit.
2. Leistungsmerkmale: Das sind Eigenschaften, die Kunden bewusst suchen und bewerten. Je besser diese Merkmale erfüllt werden, desto zufriedener sind Kunden.
3. Begeisterungsmerkmale: Das sind unerwartete Eigenschaften, die Kunden überraschen und begeistern. Sie tragen dazu bei, Kundenbindung zu schaffen und sind oft ausschlaggebend für die Kaufentscheidung.

Aufgrund der Anforderungen dieser Arbeit muss diese Definition leicht angepasst werden.

1. Basismerkmale: Das sind grundlegende Sicherheitssysteme, deren Einsatz als selbstverständlich gelten sollte und erwartet wird. Wenn diese Systeme nicht eingesetzt werden, führt das zu Unzufriedenheit und sollte schnellstmöglich behoben werden.
2. Leistungsmerkmale: Das sind Sicherheitssysteme, die von Unternehmen bewusst zum Schutz ihrer IT-Infrastruktur eingesetzt werden. Je mehr dieser Systeme eingesetzt werden, desto zufriedener sind die Unternehmen.
3. Begeisterungsmerkmale: Das sind nicht zwingend nötige Systeme, aber Unternehmen sind stolz und begeistert, wenn diese Sicherheitssysteme eingesetzt werden.

Zusätzlich sollte erwähnt werden, dass eine weitere Änderung im Kano-Modell erfolgt. Die X-Achse des Modells zeigt im Originalmodell die Erfüllung der Kundenanforderung. Im angepassten Modell der Arbeit werden hier nicht die Erwartungen gezeigt, sondern der Grad der Umsetzung. Mit Hilfe einer groß angelegten Studie des Bundesamt für Sicherheit in der Informationstechnik (2020a) wurde ein Großteil der Maßnahmen mit dem Grad der Umsetzung festgehalten. Diese Informationen wurden übernommen, um eine horizontale Einordnung gewährleisten zu können.

Folgende Forschungsfrage wurde in Kapitel 1.4 definiert:

„Welche Handlungsempfehlungen können in Bezug auf Telearbeit gegeben werden, um einer Gefährdung der Unternehmenssicherheit durch Cyberangriffe effektiv entgegenwirken zu können?“

Die Forschungsfrage kann mittels dieses Kano-Modells beantwortet werden:

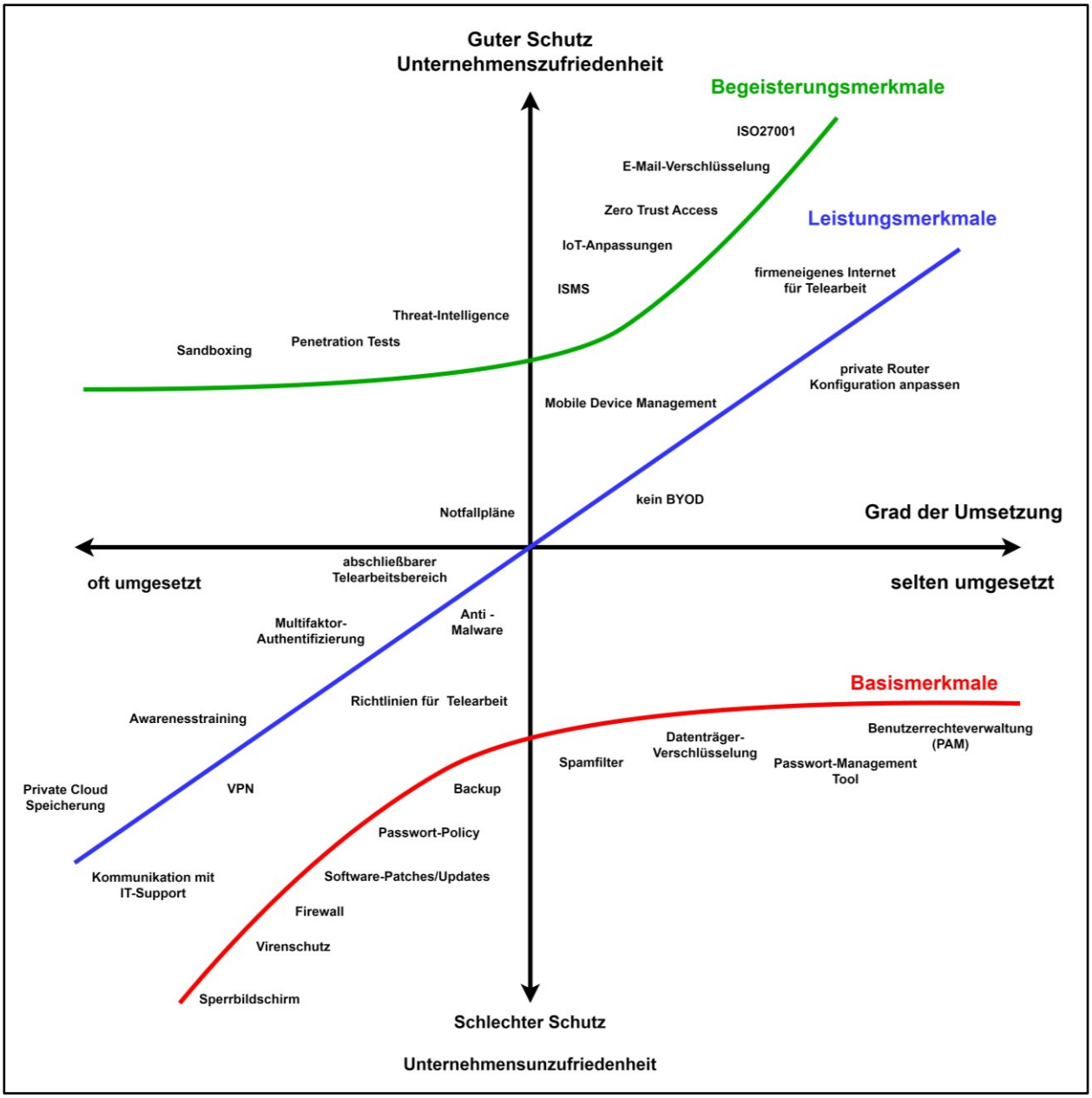

Abbildung 26 - Handlungsempfehlungen zur Sicherheit bei der Telearbeit

10 KRITISCHE BETRACHTUNG

Der erste methodische Ansatz war eine Befragung von IT-Verantwortlichen. Verständlicherweise sprechen IT-Verantwortliche ungern über Schwachstellen oder Sicherheitsrisiken in ihren Systemen. Auch Informationen zu ihren momentanen Sicherheitssystemen würden diese Personen wahrscheinlich nur ungern preisgeben. Ein weiterer Nachteil wäre die vermutlich kleine Grundgesamtheit dieser Befragung. Auch ein regionaler Einfluss würde sich nicht vermeiden lassen.

Deshalb wurde diese Methode wieder verworfen und die Methode der systematischen Literaturrecherche gewählt, um auf viele bereits bestehende Informationen ohne spezielle Einschränkungen zurückgreifen zu können.

Bei der Literatursuche nach dem PRISMA-Statement von Moher et al. (2009), welche in Abbildung 12 dargestellt wird, konnten 25 Quellen, diese allerdings mit hoher Relevanz und von hoher Qualität, für die weitere Literaturrecherche gewonnen werden.

Dies hatte meiner Meinung nach mehrere Gründe. Die Anzahl der Synonyme, die es für Telearbeit beziehungsweise für IT-Sicherheit gibt, ist zu groß, um durch die Erstellung eines Suchstrings die relevantesten Quellen zu diesem Thema zu finden. Gerade die Thematik um COVID-19 lässt viele sehr gute Quellen aufgrund eines anderen Titels nicht aufscheinen. Ein weiter gefasster Suchstring wiederrum würde zu viele Ergebnisse liefern.

Daher wurde zusätzlich eine forward search als auch eine backward search durchgeführt. Einige der 25 bereits gefundenen Quellen lieferten passende Zitationen aus anderen Quellen oder wurden wiederum selbst in anderen Dokumenten zitiert. So konnte die Qualität der Recherche noch einmal deutlich gesteigert werden.

Eine weitere Möglichkeit zur Verbesserung des Rechercheergebnisses wäre seitens der Datenbanken gegeben. Würde man hier neben den kostenlosen Datenbanken auch Datenbanken mit kostenpflichtigen Zugängen wählen, so könnte der relevante Output nochmals gesteigert werden.

11 FORSCHUNGSMÖGLICHKEITEN

Im Rahmen der Ergebnispräsentation wurde das E-Mail als besonders vulnerables Medium sowohl in Bezug auf Angriffsarten als auch -kanäle identifiziert. Allerdings wurde eine potenziell hochgradig sichere Maßnahme, nämlich die Verwendung digitaler Signaturen zur Absicherung von E-Mails, nur am Rande erwähnt. Eine zusätzliche Sicherheit könnte durch die Verschlüsselung von E-Mails gewährleistet werden. Eine mögliche Forschungsrichtung wäre die Untersuchung von Gründen oder Faktoren, die gegen die Implementierung solcher Maßnahmen sprechen.

Auch im Bereich der organisatorischen Maßnahmen gäbe es interessante Möglichkeiten der Forschung. So wurde in der Literatur des Öfteren von zyklischen Awarenessschulungen gesprochen, jedoch wurde nie die Dauer eines solchen Zyklus erwähnt. Eine Suche nach der optimalen Dauer zwischen Schulungen wäre hier sicher von Interesse.

ANHANG A - Literaturverzeichnis der Recherche

Abukari, A. M., & Bankas, E. K. (2020). Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. International Journal of Scientific & Engineering Research, 11(4), 1401-1407.

Malecki, F. (2020). Overcoming the security risks of remote working. Computer fraud & security, 2020(7), 10-12.

Souppaya, M., & Scarfone, K. (2016). Guide to enterprise telework, remote access, and bring your own device (BYOD) security. NIST Special Publication, 800, 46.

Škiljić, A. (2020). Cybersecurity and remote working: Croatia's (non-) response to increased cyber threats. International Cybersecurity Law Review, 1, 51-61.

Sabin, J. (2021). The future of security in a remote-work environment. Network Security, 2021(10), 15-17.

Nurse, J. R., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021). Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy. In HCI International 2021-Posters: 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings, Part III 23 (pp. 583-590). Springer International Publishing.

Souppaya, M., & Scarfone, K. (2016). User's Guide to Telework and Bring Your Own Device (BYOD) Security. NIST Special Publication, 800, 114.

Kolomoets, E. (2022, March). Ensuring information security in the field of remote work. In Journal of Physics: Conference Series (Vol. 2210, No. 1, p. 012008). IOP Publishing.

Porcius, I. (2021). The rise of telework and the struggle towards cyber security. Fiat Iustitia, 1(1), 148-157.

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors, 22(22), 8663.

Crossland, G. C., & Ertan, A. (2021). Remote Working and (In) Security. The Research Institute for Sociotechnical Cyber Security.

Lindroos, S., Hakkala, A., & Virtanen, S. (2022). The COVID-19 pandemic and remote working did not improve WLAN security. Procedia Computer Science, 201, 158-165.

Scarfone, K., Greene, J. E., & Souppaya, M. (2020). Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions.

Day, G. (2017). Security in the Digital World: For the home user, parent, consumer and home office. IT Governance Ltd.

Jawaid, S. A. (2022). The Increase in Security Breaches through Remote Working.

Fritzen, M. P. (2021). Remote working and Cyber Security threats in Ireland. Challenges and Prospective Solutions (Doctoral dissertation, Dublin, National College of Ireland).

Sidor-Rządkowska, M. (2022). HUMAN–THE WEAKEST OR THE STRONGEST LINK? THE ROLE OF ORGANISATIONAL CULTURE IN ENSURING CYBER SECURITY OF REMOTE WORK. Journal of Modern Science, 2(49), 609.

Davis, B. (2021). Cyber Security Issues Arising from a Remote Working Environment.

Zatonatskiy, D. PERSONNEL SECURITY FOR REMOTE WORKING DURING COVID-19 PANDEMIC.

Koehler, T., Cervini, P., & Vetter, J. (2020). The abrupt shift to remote working has amplified cyber security problems. USApp–American Politics and Policy Blog.

Arora, A., & Fava, S. The Impact of Covid-19 on Information Security in an Organisational Context due to Increased Levels of Remote Working.

Phillip Groce (2021): Remote Work: Vulnerabilities and Threats to the Enterprise.

Nurse, J. R., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021). Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy. In HCI International 2021-Posters: 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings, Part III 23 (pp. 583-590). Springer International Publishing.

Ensar Seker (2020): VPN TUNNELING AND REMOTE WORK CYBER THREAT PROJECT (VT-RW-CTP) REPORT CLASSIFICATION: UNCLASSIFIED. Unpublished.

Sabin, J. (2021). The future of security in a remote-work environment. Network Security, 2021(10)

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. Internet Technology Letters, 4(2), e247.

Al-Qahtani, A. F., & Cresci, S. (2022). The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. IET Information Security, 16(5), 324-345.

Mihailović, A., Cerović Smolović, J., Radević, I., Rašović, N., & Martinović, N. (2021). COVID-19 and beyond: employee perceptions of the efficiency of teleworking and its cybersecurity implications. Sustainability, 13(12), 6750.

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal of Information Management, 23(1), 1-11.

Kamal, A. H. A., Yen, C. C. Y., Ping, M. H., & Zahra, F. (2020). Cybersecurity issues and challenges during COVID-19 pandemic.

Machado, T. J. X., & Gouveia, L. B. (2021). Covid-19 effects on cybersecurity issues. Int. J. Adv. Eng. Res. Sci, 8, 222-229.

Yang, J., & Linkeschová, L. (2021). Remote working and cybersecurity in the pandemic: Research on the employee perceptions of remote work and cybersecurity in an international organisation during COVID-19 (Doctoral dissertation, University of Geneva).

Kitaria, D., Kibara, D., Mageto, S., & Njuguna, P. (2021). Information systems security in the age of pandemics: COVID-19 and beyond. American Journal of Multidisciplinary Research & Development (AJMRD), 3(07), 23-26.

Fernandes, L. (2021). Data security and privacy in times of pandemic. In Proceedings of the digital Privacy and security conference.

Aljohani, H. (2020). Cyber security threats during the pandemic. Journal of Contemporary Scientific Research (ISSN (Online) 2209-0142), 5(1).

Lang, M., & Connolly, L. (2021). Managing the Cybersecurity Risks of Teleworking in the Post-Pandemic'New Normal'. Available at SSRN 4146506.

Carlsten, F., Hultman, E., & Nilsson, D. E. (2021). Work from Home-Information Security Threats and Best Practices.

Sundström, F., Ekfors Elvin, A., & von Heland, W. (2021). Understanding the Effects of Cyber Security Risks and Threats on Forced Teleworking Organizations.

Wang, L., & Alexander, C. A. (2021). Cyber security during the COVID-19 pandemic. AIMS Electronics and Electrical Engineering, 5(2), 146-157.

Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H., & Fatima, Z. (2020). Cyber attacks in the era of covid-19 and possible solution domains.

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. Security Journal, 35(2), 486-505.

Borkovich, D. J., & Skovira, R. J. (2020). Working from home: Cybersecurity in the age of COVID-19. Issues in Information Systems, 21(4).

Furnell, S., & Shah, J. N. (2020). Home working and cyber security–an outbreak of unpreparedness?. Computer fraud & security, 2020(8), 6-12.

Jawaid, S. A. (2022). The Increase in Security Breaches through Remote Working.

Crossland, G. C., & Ertan, A. (2021). Remote Working and (In) Security. The Research Institute for Sociotechnical Cyber Security.

Jayakrishnan, G., Banahatti, V., & Lodha, S. The Walls Have Ears: Gauging Security Awareness in a Home Workspace.

Luna, A., Levy, Y., Simco, G., & Li, W. (2022). Towards Assessing Organizational Cybersecurity Risks via Remote Workers' Cyberslacking and Their Computer Security Posture.

Parppei, N. (2022). Addressing telecommuting in cyber security guidelines.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & security, 106, 102267.

Obada-Obieh, B., Huang, Y., & Beznosov, K. (2021, August). Challenges and Threats of Mass Telecommuting: A Qualitative Study of Workers. In SOUPS@ USENIX Security Symposium (pp. 675-694).

Buckley, B., & Dion, M. (2021). Securing a Remote Workforce.

Niu, Z. (2022). Develop and adopt the organizational cybersecurity culture in the Covid-19 teleworking scenario (Master's thesis, University of Twente).

Zebari, B. (2022). Recommendations for maintaining data security when working remotely: Interviews with IT stakeholders post COVID-19.

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. Journal of medical Internet research, 22(9), e23692.

Stock, J. (2020). INTERPOL report shows alarming rate of cyberattacks during COVID-19. Interpol.

Kuhn, D. R., Tracy, M. C., & Frankel, S. E. (2002). Security for Telecommuting and Broadband Communications: Recommendations of the National Institute of Standards and Technology. NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD.

Ghann, P., Tetteh, E. D., & Doe, N. (2022). The Impact of Covid-19 on Cybersecurity. Int. J. Recent Contributions Eng. Sci. IT, 10(1).

Georgescu, T. M. (2021). A Study on how the Pandemic Changed the Cybersecurity Landscape. Informatica Economica, 25(1).

Sebastian, G. (2021). A descriptive study on cybersecurity challenges of working from home during COVID-19 pandemic and a proposed 8 step WFH cyber-attack mitigation plan. Communications of the IBIMA, 2, 2-7.

Porcius, I. (2021). The rise of telework and the struggle towards cyber security. Fiat Iustitia, 1(1), 148-157.

ABKÜRZUNGSVERZEICHNIS

IT	Informationstechnik
VPN	Virtual Private Network
NATO	North Atlantic Treaty Organization
HTTPS	Hypertext Transfer Protocol Secure
DoS	Denial of Service
PC	Personal Computer
DDoS	Distributed Denial of Service
HTTP	Hypertext Transfer Protocol
APT	Advanced Persistent Threat
KMU	Kleine und mittlere Unternehmen
IoT	Internet of Things
CERT	Computer Emergency Response Team
BSI	Bundesamt für Sicherheit in der Informationstechnik
ISMS	Information Security Management System
ÖSCS	Österreichische Strategie für Cybersicherheit
NIS	Netz- und Informationssystemsicherheit
NISG	Netz- und Informationssystemsicherheitsgesetz
WSUS	Windows Server Update Services
URL	Uniform Resource Locator
KI	Künstliche Intelligenz
S/MIME	Secure / Multipurpose Internet Mail Extensions
OpenPGP	Open Pretty Good Privacy
MDM	Mobile Device Management
SaaS	Software as a Service
UPnP	Universal Plug and Play
BYOD	Bring Your Own Device
IP	Internet Protocol
IPSec	Internet Protocol Security
TLS	Transport Layer Security

SSL	Secure Sockets Layer
MFA	Multi-Faktor-Authentifizierung
2FA	2-Faktor-Authentifizierung
LAN	Local Area Network
WLAN	Wireless Local Area Network
DHCP	Dynamic Host Configuration Protocol

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

LITERATURVERZEICHNIS

Al-Daeef M.M., Basir N. & Saudi M.M. (2017). Security awareness training: A review. *20780958*. https://oarep.usim.edu.my/jspui/handle/123456789/1880

Anatol Badach. (1999). *Virtual Private Networks (VPNs)* (Bd. 9). https://www.researchgate.net/profile/anatol-badach/publication/301754498_virtual_private_networks_vpns

Berg, A. & Selen, S. (2021). Wirtschaftsschutz 2021.

Berghoff, T. (3. August 2020). Expertenmeinungen zu Cyber Security. *Digital Engineering Magazin,* 2020.

Bergler, A. (11. September 2017). Was ist „Bring Your Own Device“ (BYOD)? *IT-BUSINESS*. https://www.it-business.de/was-ist-bring-your-own-device-byod-a-651323/

Bertram, A., Falder, R. & Walk, F. (2021). *Arbeiten im Home Office in Zeiten von Corona: Ein Leitfaden zu Home Office und mobilem Arbeiten* (2. Auflage). C.H. Beck. https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=6465493

Bitkom. (2022, 31. August). *Cyberangriffe - betroffene Unternehmen nach Art des Angriffs 2022 | Statista*. https://de.statista.com/statistik/daten/studie/928943/umfrage/von-digitalen-angriffen-betroffene-unternehmen-nach-art-des-angriffs/

Bök, P.-B., Noack, A., Müller, M. & Behnke, D. (2020). *Computernetze und Internet of Things: Technische Grundlagen und Spezialwissen*. *Springer eBook Collection*. Springer Vieweg. https://doi.org/10.1007/978-3-658-29409-0

Bönsch, R. (2021). Homeoffice erhöht IT-Attacken drastisch. *VDI nachrichten*, *75*(16). https://doi.org/10.51202/0042-1758-2021-16-14

Brockhaus, A. (2022, 29. September). *Die spektakulärsten Cybervorfälle der letzten zehn Jahre.* isits AG International School of IT Security. https://www.is-its.org/it-security-blog/die-spektakulaersten-cybervorfaelle-der-letzten-zehn-jahre

Büllingen, F., Hillebrand, A., Oczko, M. & Ritscher, M. (2009). IT-Sicherheit als kritischer Erfolgsfaktor mobiler Geschäftsanwendungen. *Datenschutz und Datensicherheit - DuD*, *33*(10), 611–615. https://doi.org/10.1007/s11623-009-0159-3

Bundesamt für Sicherheit in der Informationstechnik. (2020a). *IT-Sicherheit im HOME-OFFICE.*

Bundesamt für Sicherheit in der Informationstechnik (2020b). Die Lage der IT-Sicherheit in Deutschland 2020, *2020*.

Bundesamt für Sicherheit in der Informationstechnik. (2021, 15. April). *Welche organisatorischen Sicherheitsmaßnahmen haben Sie in Ihrem Unternehmen bereits umgesetzt oder planen Sie umzusetzen?* https://de.statista.com/statistik/daten/studie/1252951/umfrage/umsetzung-organisatorische-sicherheitsmassnahmen-fuer-das-homeoffice/?locale=de

Bundesamt für Sicherheit in der Informationstechnik (2022). Mindeststandard des BSI für Mobile Device Management. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Mobile-Device-ManagementV2_0.pdf?__blob=publicationFile&v=2

Bundesamt für Sicherheit in der Informationstechnik. (2023, 12. Januar). *E-Mail-Verschlüsselung in der Praxis*. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/E-Mail-Verschluesselung/E-Mail-Verschluesselung-in-der-Praxis/e-mail-verschluesselung-in-der-praxis_node.html

Bundeskanzleramt (2018). Erläuterungen-NISG.

Bundeskanzleramt. (2021). *Österreichische Strategie für Cybersicherheit 2020 – Österreichische Strategie für Cybersicherheit 2021.*

Bundeskriminalamt (2022). Cybercrime Bundeslagebild: Bundeslagebild 2021.

§ 2h Arbeitsvertragsrechts-Anpassungsgesetz, 2021 (2021 & i.d.F.v. 27.04.2021). https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40232052/NOR40232052.pdf

Bundesministerium für Inneres (2020). Cybercrime Report: Lagebericht über die Entwicklung von Cybercrime.

Bundesministerium für Inneres (2021). Cybercrime Report 2021.

Cert.at (2020). Bericht Internet-Sicherheit Österreich 2020.

Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society*, *1*(1), 104–126. https://doi.org/10.1007/BF03177550

Crafford, L. (2021). *Lösungsübersicht Multifaktor-Authentifizierung für VPNs*. https://blog.lastpass.com/de/2021/01/loesungsuebersicht-multifaktor-authentifizierung-fuer-vpns/

Dada, E. G., Bassi, J. S., Chiroma, H., Abdulhamid, S. M., Adetunmbi, A. O. & Ajibuwa, O. E. (2019). Machine learning for email spam filtering: review, approaches and open research problems. *Heliyon*, *5*(6), e01802. https://doi.org/10.1016/j.heliyon.2019.e01802

Davis, C., vangel, D., Robins, B. & Tracy, M. (2023, 17. Januar). *Schritt-für-Schritt-Bedrohungsschutzstapel in Microsoft Defender for Office 365 - Office 365*. https://learn.microsoft.com/de-de/microsoft-365/security/office-365-security/protection-stack-microsoft-defender-for-office365?view=o365-worldwide

DDoS-Attacken nehmen zu und werden zielgerichteter | Kaspersky. (2022, 4. Oktober). https://www.kaspersky.de/about/press-releases/2021_ddos-attacken-nehmen-zu-und-werden-zielgerichteter

Deutschland sicher im Netz e.V. (2021). *DsiN Sichherheitsindex 2021: Digitale Sicherheitslage von Verbraucher:innen in Deutschland*. https://www.sicher-im-netz.de/file/13161/download?token=se3us1Mq

Dissanayake, N., Jayatilaka, A., Zahedi, M. & Babar, M. A. (2022). Software security patch management - A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, *144*, 106771. https://doi.org/10.1016/j.infsof.2021.106771

Eckhart, M. (2021). Security-Guide: Leitfaden für Unternehmen und Professionals inklusive Security Update.

Endres, M. (2021). *Home-Office nach der Krise: Weiterentwicklungspotentiale rechtlicher Rahmenbedingungen im Individualarbeitsrecht* [Diplomarbeit]. Johannes Kepler Universität Linz, Linz.

Engels, B. (2017). Wirtschaftliche Kosten der Cyberspionage für deutsche Unternehmen: Cybersicherheit als Grundvoraussetzung der digitalen Transformation.

Engels, B. (2021). *Cybersicherheit: 52,5 Mrd. Euro Schaden durch Angriffe im Homeoffice*. IW-Kurzbericht (54/2021). Köln. http://hdl.handle.net/10419/238281

Enisa Threat Landscape - Spam (2020). https://doi.org/10.2824/552242

Europol. (2021). *Mobile malware*. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/mobile-malware

Evers, S. (2022). Trügerische Sicherheit: Aus diesen Gründen bleibt Ransomware weiterhin eine Gefahr, 2022.

Fox, D. (2021). Phishing, *45*(11), 717. https://doi.org/10.1007/s11623-021-1521-3

Gerend, J. (2022, 23. Oktober). *Erste Schritte mit Windows Server Update Services (WSUS)*. https://learn.microsoft.com/de-de/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus

Griesbacher, E.-M. & Griesbacher, M. (2020). Cybersecurity im medialen Diskurs. *HMD Praxis der Wirtschaftsinformatik*, *57*(3), 584–596. https://doi.org/10.1365/s40702-020-00618-7

Haddaway, N. R., Grainger, M. J. & Gray, C. T. (2022). Citationchaser: A tool for transparent and efficient forward and backward citation chasing in systematic searching. *Research Synthesis Methods*, *13*(4), 533–545. https://doi.org/10.1002/jrsm.1563

Hange, M. (2012). Cyber-Sicherheit: Herausforderung in einer vernetzten Welt, *2012*.

Hayes, B. (2013). *Bring Your Own Device (BYOD) to Work: Trend Report*. *Risk management portfolio*. Elsevier Science. http://www.sciencedirect.com/science/book/9780124115927

Heil, E. A. (2020). Methode der Systematischen Literaturrecherche. https://www.uni-giessen.de/de/fbz/fb09/institute/VKE/nutr-ecol/lehre/SystematischeLiteraturrecherche.pdf

Hendrickson, J. (2023, 22. Januar). *S/MIME in Exchange Online*. https://learn.microsoft.com/de-de/exchange/security-and-compliance/smime-exo/smime-exo

Henseler-Unger, I., Hillebrand, A., Niederprüm, Schäfer & Thiele. (2018). *Aktuelle Lage der IT-Sicherheit in KMU* (Nr. 11). https://doi.org/10.1007/s11623-018-1025-y

Highland, H. (1995). *Security awareness and the persuasion of managers.: Computers & Security.*

Hof, H.-J., Krause, S., Völker, L., Walter, U. & Zitterbart, M. (2007). *Hacking und Hackerabwehr.* Institute of Telematics.

Huber, E. (2019). *Cybercrime: Eine Einführung*. *Springer eBook Collection*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-26150-4

Institut für Wissen in der Wirtschaft. (2018, 7. April). *Telearbeit – was es aus Arbeitgebersicht zu beachten gilt*. https://www.iww.de/bbp/unternehmensberatung/arbeitsrecht-telearbeit-was-es-aus-arbeitgebersicht-zu-beachten-gilt-f84577

Jendrian, K. (2014). Der Standard ISO/IEC 27001:2013. *Datenschutz und Datensicherheit - DuD*, *38*(8), 552–557. https://doi.org/10.1007/s11623-014-0182-x

Joos, T. (22. Februar 2018). E-Mail-Schutz mit Office 365 Advanced Threat Protection. *ComputerWeekly.com/de*. https://www.computerweekly.com/de/ratgeber/E-Mail-Schutz-mit-Office-365-Advanced-Threat-Protection

Jung, J. (7. September 2021). Backups gegen Ransomware. *ZDNet.de*. https://www.zdnet.de/88396561/backups-gegen-ransomware/

Kapsch Cyber Security Report 2021: Bedrohungen, Incidents, Lösungen (2021).

Karl, O. (2023, 12. März). *Wie Sie die IT-Sicherheit im Home Office gewährleisten*. https://www.acp.at/blog/wie-sie-die-it-sicherheit-im-home-office-gewaehrleisten

Kaspersky Labs GmbH. (2018). *Der Faktor Mensch in der Cybersecurity eines Unternehmens.*

Kaspersky Labs GmbH. (2023, 12. März). *10 Tipps für starke IT-Sicherheit im Home Office*. https://www.kaspersky.de/resource-center/threats/remote-working-how-to-stay-safe

Kersten, H. & Klett, G. (2017). *Business Continuity und IT-Notfallmanagement: Grundlagen, Methoden und Konzepte*. *SpringerLink Bücher*. Springer Vieweg. https://doi.org/10.1007/978-3-658-19118-4

Kersten, H., Klett, G., Reuter, J. & Schröder, K.-W. (2016). *IT-Sicherheitsmanagement nach der neuen ISO 27001*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-14694-8

Kjerland, S., Davis, C., Baumgartner, P. & McAtee, C. (2023, 17. Januar). *Erhöhen des Bedrohungsschutzes für Microsoft 365 für Unternehmen - Microsoft 365 admin*. https://learn.microsoft.com/de-de/microsoft-365/admin/security-and-compliance/increase-threat-protection?view=o365-worldwide

Kloiber, M. & Welchering, P. (2011). Militärs suchen Strategien gegen Cyberattacken. *Frankfurter Allgemeine Zeitung*(Nr.38/2011), T6.

Krüger, D. (2014). *Springer eBook Collection*. *Methoden in der naturwissenschaftsdidaktischen Forschung* (I. Parchmann & H. Schecker, Hg.). Springer Spektrum. https://doi.org/10.1007/978-3-642-37827-0

Kshetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Springer Berlin Heidelberg. http://nbn-resolving.org/urn:nbn:de:bsz:31-epflicht-1579148

Kulkarni, S. (13. August 2021). IoT-Geräte sichern und vor Cyberangriffen schützen. *ComputerWeekly.com/de*. https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40232052/NOR40232052.pdf

Lanzenhofer, M., Schauer, S., Sommerer, N. & Zieser, M. (2021). *Cybersecurity: Systematisierung, Forschungsstand und Innovationspotenziale: Endbericht.* Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften.

Lindner, D. (2020). *Forschungsdesigns der Wirtschaftsinformatik: Empfehlungen Für Die Bachelor- und Masterarbeit*. Springer Fachmedien Wiesbaden GmbH. https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=6273171

Mell, P., Bergeron, T. & Henning, D. (2005). Creating a Patch and Vulnerability Management Program. In.

Moher, D., Liberati, A., Tetzlaff, J. & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Annals of internal medicine*, *151*(4), 264-9, W64. https://doi.org/10.7326/0003-4819-151-4-200908180-00135

Ping Identiy. (2017). *Multifaktor-Authentifizierung: Best Practices zum Schutz moderner digitaler Unternehmen.*

Pohlmann, N. (2019). *Sicheres und vertrauenswürdiges Arbeiten im Homeoffice.*

Pohlmann, N. (2022). *Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung* (2. Auflage). Springer Vieweg.

Porath, R. (2020). *Internet, Cyber- und IT-Sicherheit von A-Z: Aktuelle Begriffe kurz und einfach erklärt - Für Beruf, Schule und Privatleben* (2. Auflage 2020). Springer Berlin; Springer Vieweg. https://doi.org/10.1007/978-3-662-60911-8_35

Proofpoint. (2022). *Was ist Bring-your-own-device (BYOD)?* https://www.proofpoint.com/de/threat-reference/byod

Raithel, J. (2008). *Quantitative Forschung: Ein Praxiskurs* (2. Aufl.). *Lehrbuch*. VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-91148-9

Randolph, J. (2009). *A guide to writing the dissertation literature review*. https://scholarworks.umass.edu/pare/vol14/iss1/13/

Rosert, E. (2009). Hinweise zum Recherchieren und Beschaffen wissenschaftlicher Literatur. https://www.fb03.uni-frankfurt.de/46036789/literaturrecherche.pdf

Saalbach (2019). Cyberwar 07 Juli 2019.

Sauerwein, E., Bailom, F., Matzler, K. & Hinterhuber, H. (1996). The Kano Model: How to Delight Your Customers. *International Working Seminar on Production Economics*, *1*.

Schiebeck, S., Latzenhofer, M., Palensky, B. & Schauer, S. (2015). IKT-Risikoanalyse am Beispiel APT.

Shaw, R. S., Chen, C. C., Harris, A. L. & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Shethi, S. (5. Juli 2022). Die 10 besten alternativen Microsoft WSUS-Patch-Management-Tools für KMU. *Geekflare*. https://geekflare.com/de/patch-management-software/

Siller, H. (2018a). Gabler Wirtschaftslexikon: Definiton ‚Exploit.'.

Siller, H. (2018b). *Spamfilter*. https://wirtschaftslexikon.gabler.de/definition/spamfilter-53427/version-276519

Singleton, Hammond, Onut & Zorabedian. (2022). *X-Force Threat Intelligence Index 2022.*

Spafford, E. H. (1988). *The Internet Worm Program: An Analysis* (a).

Statista. (2021). *Art der Sicherheitsvorfälle bei der privaten Internetnutzung | Statista*. https://de.statista.com/statistik/daten/studie/1243640/umfrage/art-der-sicherheitsvorfaelle-bei-der-privaten-internetnutzung-in-europa/

Steinmann, C. (2018). *IT-Sicherheit in Unternehmen: State of the Art, Gefahren und Trends*. https://www.hhz.de/fileadmin/user_upload/fakultaet_inf/bilder/aktuelles/news/2018/010_informatics_inside/tagungsband_informaticsinside2018_digital_final_inhalt.pdf#page=57

Sturm, M. (2021). *4 Unterschiede zwischen Homeoffice und Remote working*. https://www.fwp.at/news/blog/4-unterschiede-zwischen-homeoffice-und-remote-working

Symantec. (2019). *Internet security threat report.*

Timmins, F. & McCabe, C. (2005). How to conduct an effective literature search. *Nursing standard: official newspaper of the Royal College of Nursing*, *20*(11), 41–47. https://doi.org/10.7748/ns2005.11.20.11.41.c4010

Trendmicro (2021). Securing your organization from modern ransomware: Ransomware attacks are now a team effort.

Volkmer, C. (2021). Lehren für die IT-Sicherheit aus einem Jahr Homeoffice. *Wirtschaftsinformatik & Management*, *13*(4), 291–293. https://doi.org/10.1365/s35764-021-00346-7

vom Brocke, J., Simons, A., Niehaves, B., Reimer, K., Plattfaut, R. & Cleven, A. (2009). *Reconstructing the giant: On the importance of rigour in documenting the literature search process*. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1145&context=ecis2009

von Gersdorff, A. M. (2020). *Systematische Literaturrecherche - So meistern Sie alles!* https://gwriters.de/blog/systematische-literaturrecherche

Webster, J. & Watson, R. T. (2002). *Analyzing the past to prepare for the future: Writing a literature review*. https://www.jstor.org/stable/4132319

Weidenbach, B. (2021). *New Work: Homeoffice und Mobiles Arbeiten: Statista DossierPlus zur Neuen Arbeitswelt in Zeiten von Corona.*

Wirtschaftsagentur Wien (2020). IT-Security: Technologie Report.

Wölbert, C. (2020). Was emotet anrichtet und welche Lehren die Opfer daraus ziehen. *ct magazin für computer technick, available at: www. heise. de/ct/artikel/Was-Emotet-anrichtet-und-welche-Lehren-die-Opfer-daraus-ziehen-4665958. html (accessed 3 June 2020)*.