HOCHSCHULE
MITTWEIDA
University of Applied Sciences

BACHELORARBEIT

Frau
Sophie Matschke

Untersuchung der allgemeinen Gefahrensituation Cybercrime

Mittweida, April 2023

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Untersuchung der allgemeinen Gefahrensituation Cybercrime

Autorin:
Sophie Matschke

Studiengang:
Allgemeine und digitale Forensik

Seminargruppe:
FO19w3-B

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

Zweitprüferin:
Laura Pistorius, B.Sc.

Einreichung:
Mittweida, 16.04.2023

Verteidigung/Bewertung:
Mittweida, 2023

Faculty of **Applied Computer Sciences and Biosciences**

BACHELOR THESIS

Investigation of the general danger situation of cybercrime

Author:
Sophie Matschke

Course of Study:
General and Digital Forensic Science

Seminar Group:
FO19w3-B

First Examiner:
Prof. Dr. rer. nat. Dirk Labudde

Second Examiner:
Laura Pistorius, B.Sc.

Submission:
Mittweida, 16.04.2023

Defense/Evaluation:
Mittweida, 2023

Bibliografische Beschreibung:

Matschke, Sophie:
Untersuchung der allgemeinen Gefahrensituation Cybercrime. – 2023. – 83 S.
Mittweida, Hochschule Mittweida – University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2023.

Referat:

Die vorliegende Arbeit beschäftigt sich mit der Betrachtung und Analyse der Bedrohungslage durch Cybercrime in Deutschland im Jahr 2021. Dafür werden verschiedene Berichte und Studien untersucht und anschließend miteinander verglichen. Außerdem sollen daraus abgeleitet Aussagen zur inhaltlichen Gestaltung von Awareness-Schulungen getroffen werden. Dafür werden verschiedene Angebote betrachtet und einander gegenüber gestellt. Der anschließende Vergleich dieser beiden Themenschwerpunkte soll Empfehlungen für eine optimale Gestaltung von Mitarbeitersensibilisierung liefern. Insgesamt sind eindeutige Aussagen zu einzelnen Angriffsarten im Cybercrime-Bereich schwierig, weshalb nur bedingt Empfehlungen für Awareness-Schulungen gegeben werden können. Die Vielfältigkeit aktuell angebotener Schulungen bietet geeignete Möglichkeiten zur Mitarbeitersensibilisierung.

Gender-Hinweis

In der vorliegenden Arbeit wird darauf verzichtet, bei Personenbezeichnungen sowohl die männliche als auch die weibliche Form zu nennen. Die männliche Form gilt in allen Fällen, in denen dies nicht explizit ausgeschlossen wird, für beide Geschlechter.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

APT ..... Advanced Persistent Threats

APWG ..... Anti-Phishing-Working-Group

BKA ..... Bundeskriminalamt

BMI ..... Bundesministerium des Inneren und für Heimat

BSI ..... Bundesamt für Sicherheit in der Informationstechnik

BYOD ..... Bring Your Own Device

CaaS ..... Cybercime-as-a-Service

CVSS ..... Common Vulnerability Scoring System

DDoS ..... Distributed Denial of Service

DoS ..... Denial of Service

DsiN ..... Deutschland sicher im Netz

DTAG ..... Deutsche Telekom AG

HPI ..... Hasso-Plattner-Institut

IAB ..... Initial Access Broker

ISMS ..... Information Security Management System

KI ..... Künstliche Intelligenz

KMU ..... kleinere und mittlere Unternehmen

KRITIS ..... Kritische Infrastrukturen

MaaS ..... Malware-as-a-Service

PKS ..... Polizeiliche Kriminalstatistik

RaaS ..... Ransomware-as-a-Service

RAT ..... Remote-Access-Tools

VSA ..... Virtual System Administrator

WIK ..... Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

1 Einleitung

In diesem einleitenden Kapitel wird die Motivation, die Problemstellung und die damit einhergehende Zielsetzung dieser Arbeit aufgezeigt. Außerdem wird mit der Vorstellung des Aufbaus der Arbeit ein kurzer Einblick in die einzelnen Kapitel gegeben.

1.1 Motivation, Problemstellung und Zielsetzung

Das in der vergangenen Zeit vermehrte Auftreten von Cyber-Angriffen auf Forschungseinrichtungen wie Universitäten und Hochschulen sowie öffentliche Verwaltungen deutet auf ein erhöhtes Cybercrime-Aufkommen hin. Doch wie steht es um die Bedrohungslage in Deutschland ganz konkret und wie sind Unternehmen und Privathaushalte darauf vorbereitet? Mit diesen Themen beschäftigt sich die vorliegende Arbeit.
Zum Thema Cybercrime existieren zahlreiche Umfragen, Studien und Berichte. In der Polizeilichen Kriminalstatistik (PKS) werden nur die bei der Polizei angezeigten Straftaten erfasst, das sogenannte Hellfeld, und es wird von einer hohen Dunkelziffer ausgegangen. Häufig ist in den Medien die Rede von einer erhöhten Bedrohung durch Cybercrime und deshalb werden mehr Sicherheitsmaßnahmen empfohlen, konkrete Zahlenwerte sind jedoch selten zu finden. Ziel dieser Arbeit ist es, eindeutige Aussagen darüber zu treffen, wie das Ausmaß verschiedener Angriffsmethoden aussieht. Aus diesen Werte sollen dann Empfehlungen für notwendige Inhalte von Awareness-Schulungen entwickelt werden, damit Mitarbeitende und Privatpersonen entsprechend sensibilisiert werden können. Dafür werden die verschiedenen Berichte und Studien einander gegenüber gestellt, um Gemeinsamkeiten und Unterschiede zu entdecken, und dann mit Themen von Awareness-Trainings verglichen. Die Relevanz des Themas ergibt sich daraus, dass Sicherheitsmaßnahmen dazu bestimmt sind, Cyber-Angriffe abzuwehren oder zumindest die Schäden zu begrenzen und deshalb auf die aktuelle Bedrohungslage abgestimmt sein sollten. Es werden sowohl Unternehmen als auch Privathaushalte betrachtet. Ein weiterer Aspekt ist die genauere Erforschung des Dunkelfelds. Aus der Betrachtung verschiedener Statistiken können möglicherweise Aussagen darüber getroffen und zahlenmäßige Näherungen zu stattgefundenen Cybercrime-Straftaten abgeschätzt werden. Weiterhin steht die Beobachtung der Entwicklung von Cybercrime über die vergangenen Jahre hinweg im Fokus.
Bei der Recherche wurde eine bereits bestehende Studie vom Wissenschaftlichen Institut für Infrastruktur und Kommunikationsdienste (WIK) mit ähnlichem Inhalt aus dem Jahr 2017 entdeckt [1]. Ein kurzer Vergleich mit dieser wird auch Bestandteil der Arbeit sein.
Die vorliegende Arbeit bezieht sich auf das Jahr 2021, da das zuletzt erschienene Bundeslagebild Cybercrime und auch der zuletzt erschienene Bericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Lage der IT-Sicherheit in Deutschland das Jahr 2021 sowie lediglich den Anfang von 2022 umfassen. Vollständige Daten für das Jahr 2022 liegen daher derzeit noch nicht vor.

1.2 Aufbau der Arbeit

Nach diesen einführenden Worten in das Thema werden im nächsten Kapitel die Grundlagen von Cybercrime und deren Deliktbereiche und Angriffsmethoden sowie der Begriff Awareness erklärt. Im Kapitel „Bedrohungslage Cybercrime“ werden die einzelnen Berichte und Studien mit Hintergrundinformationen und einer Beschreibung der Inhalte vorgestellt und im Anschluss unter verschiedenen

Aspekten miteinander verglichen. Danach wird auf das Thema Awareness-Maßnahmen eingegangen. Nach der zusammenfassenden Gegenüberstellung dieser beiden Themenschwerpunkte folgt der Diskussionsteil mit anschließendem Fazit.

2 Grundlagen

Cybercrime beschreibt laut dem Bundeskriminalamt (BKA) einen Sammelbegriff für alle Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten oder die mittels dieser Informationstechnik begangen werden. Dabei handelt es sich um einen dynamischen Deliktbereich, denn infolge der zunehmenden Digitalisierung verändern sich die Kriminalitätserscheinungen in diesem Bereich stetig. Angreifende passen ihre Aktivitäten flexibel und schnell an neue Entwicklungen und Trends an. [2]
Cybercrime gliedert sich in zwei Teilbereiche: Cybercrime im engeren Sinne und Cybercrime im weiteren Sinne. Cybercrime im engeren Sinne sind „Straftaten, die sich gegen des Internet, informationstechnische System oder deren Daten richten." [3] Darunter werden hochtechnische Straftaten verstanden, welche ebenso hochtechnische Ermittlungsarbeit erfordern. [2] Cybercrime im weiteren Sinne meint hingegen „Straftaten, die unter Nutzung von Informationstechnik begangen werden (Tatmittel Internet)." [3] Dazu gehören Taten, die in der analogen Welt begangen werden können. [2]
Zusammenfassend ist Cybercrime im Allgemeinen also jegliche Kriminalität, die mit Informationstechnologien begangen wird, wobei große Unterschiede hinsichtlich der Ausprägung und Professionalität existieren. Es wird von Cyber-Angriffen oder Cyber-Attacken gesprochen.

2.1 Cyber-Angriffe

Der Duden definiert eine Cyber-Attacke oder Cyber-Angriff als „von außen (durch einen einzelnen Hacker, durch eine Institution o.Ä.) zum Zweck der Sabotage oder der Informationsgewinnung geführter Angriff auf ein Computernetzwerk". [4]
Angriffe erfolgen in der Regel über Angriffsvektoren, auch Eintrittsvektoren genannt. Damit ist die Kombination von Angriffsweg und Angriffstechnik gemeint, mit welcher sich Zugang zum IT-System verschafft wird. [5, S. 106] Typische Angriffsvektoren sind Phishing und IT-Schwachstellen. [6]
In den nächsten Abschnitten folgt eine überblicksartige Erklärung einzelner, im weiteren Teil der Arbeit relevanter Cybercrime-Angriffe.

2.1.1 Phishing

Phishing setzt sich aus den Wörtern *password* und *fishing* zusammen und bedeutet demnach „Passwörter angeln". [5, S. 109] Dabei versuchen Angreifende mittels elektronischer Kommunikationswege und Social-Engineering-Methoden an vertrauliche Daten der Kommunikationsteilnehmer zu gelangen. [6]
Social-Engineering versucht grundlegend die vermeintlichen menschlichen Schwächen wie Neugier oder Angst auszunutzen und dadurch Zugriff auf sensible Daten und Informationen zu erhalten. Das ist ebenso in der analogen Welt möglich. [5, S. 111] Häufig findet Phishing über E-Mails statt. Weitere Methoden sind Kurznachrichten, gefälschte Webseiten und Telefonanrufe. Dabei wird häufig ein Vertrauensverhältnis des vermeintlich vertrauenswürdigen Absenders zum Empfänger suggeriert oder durch dringliche Aufforderung Druck auf den Empfänger ausgeübt. [6]
Phishing richtet sich in der Regel massenhaft und ungezielt verteilt gegen die breite Bevölkerung. Beim Spear-Phishing hingegen werden gezielt einzelne Personen adressiert, welche häufig personalisierte Nachrichten erhalten. [6]

Phishing-Mails werden den Scam-Mails zugeordnet. Das meint Betrugsmails, eine Kategorie der Spam-Mails. [5, S. 110]
Als Spam werden allgemein unerwünscht zugesandte E-Mails bezeichnet. Das inkludiert sowohl unschädlichen Werbe-Spam als auch Erpressungs- oder Betrugs-Mails. [5, S. 27–28]

2.1.2 IT-Schwachstellen

Einen weiteren Angriffsvektor stellen IT-Schwachstellen dar. Darunter werden Sicherheitslücken in Hardware oder Software verstanden. Diese können von Angreifenden ausgenutzt werden, um Zugriff zum System zu erhalten und dieses zielgerichtet anzugreifen und zu kompromittieren. [6] Das Aufspüren, Melden und schnellstmögliche Schließen der Schwachstellen hat daher eine hohe Bedeutung für die Abwehr von Angriffen. [5, S. 13]
Eine Zero-Day-Schwachstelle beschreibt eine Sicherheitslücke von der ein Angreifer noch vor dem Hersteller oder der Öffentlichkeit Kenntnis hat und für die somit noch kein Patch verfügbar ist. Ein Patch ist die Korrektur des Fehlers im Softwarecode, der die Sicherheitslücke verursacht. [6]
Unterschieden wird zwischen Schwachstellen in Softwareprodukten und in Hardwareprodukten. Schwachstellen in Hardwareprodukten sind meist tief in der jeweiligen Architektur oder dem Herstellungsprozess begründet. Der Aufwand und die Kosten für das Ausnutzen dieser ist höher als bei Software-Schwachstellen. Jedoch ist ebenfalls der potenzielle Nutzen höher, da solche Schwachstellen nicht durch einfache Software-Patches behebbar sind. [5, S. 35]
Für das Ausnutzen von Sicherheitslücke kommen in der Regel Exploits zum Einsatz. Diese Methode oder Programmcode werden eingesetzt, um nicht vorgesehene Befehle oder Funktionen durch das Ausnutzen einer Schwachstelle auszuführen. Je nach Art der Schwachstelle sind unterschiedliche Angriffe möglich. [5, S. 108]
Um Schwachstellen im Webbrowser oder dessen Plug-Ins automatisiert zu finden und diese zur Installation von Schadprogrammen zu verwenden, kommen sogenannte Exploit-Kits zum Einsatz. Diese werden auf legitimen Webseiten platziert. [5, S. 108]

2.1.3 Schadprogramme

Schadprogramme werden auch als Schadsoftware oder Malware betitelt. Malware ist ein Kunstwort, das sich aus *Malicious Software* ableitet. [5, S. 108] Allgemein werden damit Computerprogramme bezeichnet, die schädliche Funktionen auf IT-Systemen ausführen können oder andere Programme dazu befähigen. [5, S. 12] Derartige Programme sind üblicherweise für eine bestimmte, weit verbreitete Betriebssystemvariante konzipiert. [5, S. 108] Es gibt verschiedene Malware-Arten.

2.1.3.1 Ransomware

Definiert ist diese besondere Form der Schadprogramme als Malware, die durch Verschlüsselung den Zugriff auf Daten und Systeme einschränkt oder verhindert und nur gegen Zahlung eines Lösegelds (engl. ransom) wieder freigibt. Das stellt einen Angriff auf das Sicherheitsziel der Verfügbarkeit dar und ist eine Form digitaler Erpressung. [5, S. 109–110] Dabei werden häufig Nutzerdaten wie Office-, Bild- und Videodateien oder komplette Dateninfrastrukturen verschlüsselt. Die Daten sind dadurch nur mit dem für die eingesetzte Ransomware spezifischen Tool entschlüsselbar. Von den

Angreifenden wird eine Erpressernachricht hinterlassen, in welcher damit gedroht wird, das Schlüsselmaterial zu vernichten, sollte keine Zahlung des Lösegelder erfolgen. [5, S. 13–14] Die Lösegeldforderung erfolgt meist in digitaler Währung und durch das Setzen von kurzen Fristen wird der Druck auf die Angriffsopfer erhöht. [7] Eine neue Variante dieser Erpressungsform ist es, zusätzlich zur Verschlüsselung der Daten mit deren Veröffentlichung zu drohen. Dadurch erhöht sich der Druck. Dieses Verfahren wird als Double Extortion bezeichnet. [5, S. 13–14]

2.1.3.2 Bots

Hierbei handelt es sich um Schadprogramme, die sich mit Hilfe von Command-and-Control-Servern fernsteuern lassen. [5, S. 12] Die infizierten Systeme werden zu Systemen, den Botnetzen, zusammengeschlossen und durch einen Bot-Master kontrolliert. Heutzutage können davon nahezu alle internetfähigen Geräte, auch Router, Smartphones und weitere betroffen sein. Direkte Schäden entstehen durch das Abgreifen persönlicher Daten, Online-Banking-Betrug und andere. Durch die Nutzung dieser Botnetze für den massenhaften Versand von Spam-Mails oder für die Ausführung von Distributed Denial of Service (DDoS)-Angriffen folgen Schäden für Dritte. [5, S. 24]

2.1.4 (Distributed) Denial of Service

Denial of Service (DoS)-Angriffe sind gezielte Überlastungsangriffe auf Internetdienste. Als Distributed Denial of Service (DDoS) werden diese bezeichnet, wenn der Angriff von mehreren Systemen parallel erfolgt, also verteilt (eng. distributed) ist. Diese Angriffsart zählt zu den Hauptbedrohungen für die Cyber-Sicherheit. [5, S. 41] Sie richtet sich gegen die Verfügbarkeit von Diensten, Webseiten, Systemen oder ganzen Netzwerken. [5, S. 107] In der Regel erfolgen die Angriffe durch eine Vielzahl einzelner Anfragen über eine große Anzahl an Rechnern oder zumeist mittels großer, ferngesteuerter Botnetze. [8]

2.1.5 Hybride Bedrohungen

In diese Kategorie fallen alle Angriffe, durch die fremde Staaten illegitim Einfluss nehmen. Ziel ist meist die Destabilisierung eines Landes. Das bedeutet, dass physische Angriffe durch Cyber-Angriffe oder Desinformationskampagnen begleitet werden können. [5, S. 44, 108]

2.1.6 Advanced Persistent Threats (APT)

Die Bezeichnung Advanced Persistent Threats (APT) betrifft Angriffe, die langfristig und mit großem Aufwand geplant auf einzelne ausgewählte Institutionen und Einrichtungen abzielen. Dadurch wird sich meist ein dauerhafter Zugang zu Netzwerken verschafft, um Informationen über das Ziel zu erlangen und dieses gegebenenfalls zu sabotieren. Der sehr hohe Ressourceneinsatz und die erheblichen technischen Fähigkeiten bedingen, dass derartige Angriffe schwierig zu detektieren sind. [5, S. 38, 106] Ursprung dieser Angriffe sind nicht ausschließlich staatliche Akteure, sondern ebenfalls Angehörige der organisierten Kriminalität. [9]

Des Weiteren wird das Kürzel APT, gefolgt von einer fortlaufenden Nummerierung, für die Benennung von Akteuren aus der Cybercrime, vor allem staatliche Akteure, verwendet. Dies ist jedoch nicht einheitlich definiert und andere Namenskonventionen werden ebenfalls eingesetzt. [9]

2.1.7 Supply-Chain-Angriffe

Beim sogenannten Lieferketten-Angriff wird während der Herstellung einer legitimen Software Schadcode eingebaut. [5, S. 36] Diese Angriffsart zeichnet sich durch ihre hohe Komplexität aus. Ein besonders großes Bedrohungspotenzial geht davon aus, weil derartige Angriffe eine hohe Reichweite und ungezielte Weiterverbreitung aufweisen. Dadurch kann die Zahl der Betroffenen deutlich höher als bei gezielten Angriffen sein. Zudem können ebenfalls sicherheitstechnisch gut abgesicherte Systeme betroffen sein, da angenommen wird, eine legitime Software auszuführen und IT-Standards und Cyber-Security-Maßnahmen unterlaufen werden können. [10, S. 28–29]

2.2 Weitere Phänomenbereiche Cybercrime

Cybercrime tritt nicht nur in Form verschiedener Angriffe auf. Zu diesem Deliktbereich gehören weitere Erscheinungsformen, welche im Folgenden erläutert werden.

2.2.1 Underground Economy

Diese Bezeichnung umfasst die Gesamtheit aller täterseitig illegal genutzten Plattformen. [11] Sie bildet die Grundlage für viele Straftaten im Cyber-Bereich, weil auf diesen Plattformen Werkzeuge, Jobs und relevantes Täterwissen zum Kauf angeboten wird. [10, S. 8] Der Begriff entwickelte sich aufgrund der starken wirtschaftlichen und illegalen Ausrichtung. [11]

2.2.2 Data-Leak

Auf den Foren und Marktplätzen werden Daten zum Kauf angeboten, die durch unberechtigten Zugriff erlangt wurden. Dazu gehören Anmeldedaten, Zahlungsdaten, personenbezogene Daten und viele weitere. Kriminelle setzen diese Daten ein, um weitere Straftaten wie Phishing oder die Übernahme entwendeter Konten und Identitäten zu begehen. Data-Leaks sind ein elementarer Bestandteil von Cybercime-as-a-Service (CaaS). [10, S. 12]

2.2.3 Cybercime-as-a-Service (CaaS)

In diesem Phänomenbereich der Cybercrime werden Straftaten von Cyber-Kriminellen auftragsorientiert begangen oder dienstleistungsorientiert ermöglicht. [5, S. 107] Damit ist gemeint, dass sich Angreifende einzelne Bestandteile eines Angriffes, wie beispielsweise die Schadsoftware, kaufen oder andere damit beauftragen können.
Eine Kategorie davon ist Malware-as-a-Service (MaaS). Dabei wird von Außenstehenden die Malware zur Verfügung gestellt. [5, S. 107] Dazu gehört Ransomware-as-a-Service (RaaS). Ransomware-Entwickler vermieten ihre Schadsoftware und geben Unterstützung bei deren Einsatz. [7]
Zusammenfassend ist zu sagen, dass es durch diese Angebote Angreifenden ohne eigene umfangreiche technische Fähigkeiten möglich wird, technisch anspruchsvolle Cyber-Angriffe durchzuführen. [5, S. 107]

2.3 Awareness-Schulungen

Der Begriff Awareness ist eine verkürzte Form von Security Awareness und das ist wiederum eine Verkürzung von Information Security Awareness. Im Deutschen wird dieser Ausdruck meist mit der Umschreibung Sensibilisierung bezeichnet. Genaugenommen ist das jedoch fehlerhaft, weil Sensibilisierung einen Prozess beschreibt und unter Awareness ein Zustand verstanden wird. Unterschieden wird weiterhin zwischen IT Security Awareness und Information Security Awareness. Ersteres beschreibt eine Untermenge, nur die Informationstechnik und die darin verarbeiteten Informationen und Daten. Information Security Awareness umfasst auch nicht digitale Informationen, wie beispielsweise Papierdokumente. [12, S. 9]
Information Security Awareness meint den, bezüglich der Sicherheitsgefahren, bewussten Umgang mit Informationen, unabhängig vom Medium. [13, S. 8]
Grundsätzlich lässt sich sagen, dass Anwendende überzeugt werden sollen, sich im beruflichen und privaten Kontext so zu verhalten, dass sie weder wissentlich noch unwissentlich der Informationssicherheit oder der Sicherheit der Informationssysteme des Unternehmens Schäden zufügen. Das inkludiert, dass Informationen und Informationssysteme aktiv vor Gefahren geschützt werden. Das wird als informationssicherheitskonformes Verhalten bezeichnet. [12, S. 3] Um dieses Verhalten zu erreichen, also um den Sensibilisierungsgrad zu erhöhen, werden Awareness-Maßnahmen eingesetzt. [12, S. 9] Um beste Ergebnisse erzielen zu können, müssen solche Maßnahmen an die konkrete Situation im Unternehmen angepasst werden. Dazu gehört es, die Situation immer wieder zu analysieren und dann eine passende Umsetzung zu etablieren, denn Mitarbeitersensibilisierung ist ein kontinuierlicher Prozess. [12, S. 49]

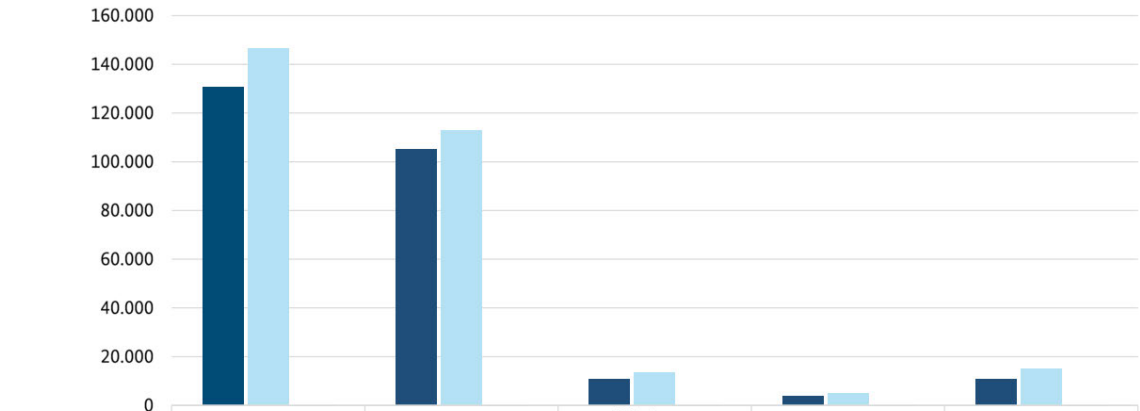
3 Bedrohungslage Cybercrime

Der erste Themenkomplex der vorliegenden Arbeit ist die Bedrohungslage durch Cybercrime in Deutschland im Jahr 2021.
Um Vergleiche der Studien und Berichte anstellen zu können, werden diese zunächst jeweils eigenständig analysiert und die Inhalte vorgestellt. Danach werden die Unterschiede und Gemeinsamkeiten herausgearbeitet und zusammengefasst.
Eine Übersicht A.1 der betrachteten Studien befindet sich im Anhang. Im oberen Bereich werden allgemeine Informationen wie Herausgeber, Veröffentlichungsdatum und Informationen zur Befragung vorgestellt. Dazu gehören die eingesetzte Methode oder Datenbasis, der Befragungszeitraum, der Umfang und die Befragungsgruppe. Im unteren Abschnitt sind die enthaltenen Themenkomplexe sowie Sonderthemen genannt.

3.1 Polizeiliche Kriminalstatistik (PKS) und Bundeslagebild Cybercrime 2021

Die PKS umfasst die der Polizei bekannt gewordenen rechtswidrigen Straftaten. Das beinhaltet die Versuche, die Anzahl der ermittelten Tatverdächtigen und weitere Informationen zu Fällen, Opfern und Tatverdächtigen. [3] Damit bildet dieser Bericht die einzige bundesweit geführte und qualitätsgesicherte Statistik basierend auf polizeilichen Ermittlungen. [10, S. 4] Ausgegliedert sind Staatsschutz- und Verkehrsdelikte, Ordnungswidrigkeiten und Delikte, die außerhalb der Zuständigkeit der Polizei liegen, ebenso wie Straftaten, die direkt bei der Staatsanwaltschaft angezeigt werden. [3]
Der Summenschlüssel Cybercrime inkludiert die Straftatbestände Computerbetrug (§ 263a StGB), Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen und Daten-Hehlerei (§§ 2020a, 202b, 202c, 202d StGB), Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr (§§ 269, 279 StGB) und Datenveränderung/Computersabotage (§§ 303a, 303b StGB). [3]
Das BKA generiert aus den Zahlen der PKS jährlich das Bundeslagebild Cybercrime. Schwerpunkte dieser Veröffentlichung sind Delikte, die sich gegen das Internet und informationstechnische Systeme richten. Der statistische Teil bildet durch die Daten der PKS das Hellfeld des Deliktbereiches ab. In diesem Deliktbereich wird aufgrund verschiedener Aspekte von einem weit überdurchschnittlich ausgeprägten Dunkelfeld ausgegangen. Um die Qualität der Aussagen zu verstärken, fließen daher zusätzlich Erkenntnisse und Einschätzungen anderer Behörden und wissenschaftlicher Einrichtungen in diesen Bericht des BKA ein. Das Bundeslagebild Cybercrime 2021 wurde im Mai 2022 veröffentlicht. Der thematische Fokus liegt auf den verschiedenen Phänomenbereichen der Cybercrime. [10, S. i, 4]
Es wird angenommen, dass das Dunkelfeld in diesem Bereich weit überdurchschnittlich ausgeprägt ist. Dafür spricht, dass eine große Anzahl strafbarer Handlungen im Internet durch zunehmende technische Sicherheitseinrichtungen nicht über das Versuchsstadium hinauskommen und deshalb von den Geschädigten nicht bemerkt werden. Außerdem werden Geräte häufig unbemerkt zum Begehen von Straftaten verwendet, wie beispielsweise bei der Nutzung infizierter Geräte als Teil eines Botnetzes zum Ausführen von DDoS-Angriffen. Des Weiteren werden Straftaten von Betroffenen oftmals nicht angezeigt, besonders wenn noch kein finanzieller Schaden eingetreten ist. Ein weiterer Grund für den Verzicht auf eine Anzeige ist es, den guten Ruf im Kundenkreis nicht zu schädigen.

Anzeigen werden oft erst erstattet, wenn beispielsweise in Erpressungsfällen nach der Lösegeldzahlung dennoch keine Entschlüsselung der betroffenen Daten erfolgt. [14, S. 9]
Im Cybercrime-Bereich sind wiederholt signifikant steigende Fallzahlen zu beobachten. Im Summenschlüssel Cybercrime ist ein Anstieg von 12 % zu verzeichnen. Zu den möglichen Erklärungsansätzen für diese Entwicklung zählt zum einen, dass die Anzahl der Cybercrime-Vorfälle gestiegen ist und Angreifende sich den Möglichkeiten der Underground Economy bedienen. Weiterhin wird die Corona-Pandemie als Digitalisierungsschub und damit auch Treiber der Cybercrime-Fallzahlen gesehen. Zudem ist festzustellen, dass sich Straftaten im Allgemeinen vermehrt vom analogen in den digitalen Raum verlagern. Möglicherweise ist zusätzlich der Anteil der Anzeigen gestiegen und somit sind trotz einen großen Dunkelfeld mehr Fälle in das polizeiliche Hellfeld gelangt. Mit knapp 30 % befindet sich die Aufklärungsquote bei Cybercrime weiterhin deutlich unter dem PKS-Durchschnitt von 58,7 %. [10, S. 4]
Wie die Abbildung 3.1 zeigt, ist ein Anstieg nicht nur im Summenschlüssel Cybercrime zu erkennen, sondern ebenfalls in allen darin enthaltenen cyberspezifischen Delikten. Daraus lässt sich schließen, dass Cybercrime-Straftaten zunehmend an Bedeutung gewinnen. Die größte Steigerung mit 38,6 % ist beim Ausspähen von Daten und Datenhehlerei zu verzeichnen.



	CC gesamt	Computerbetrug	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	Datenveränderung, Computersabotage	Ausspähen von Daten einschl. Vorbereitungshand-lungen und Datenhehlerei
2020	130.477	105.049	10.895	3.770	10.763
2021	146.363	113.002	13.390	5.053	14.918
Veränderungsrate	12,2%	7,6%	22,9%	34%	38,6%

Abbildung 3.1: Fallaufkommen von Cybercrime-Straftaten 2020 und 2021 [10, S. 7]

Die Verteilung der Cybercrime-Straftaten 2021 in Abbildung 3.2 zeigt eine deutliche Ungleichmäßigkeit. Demnach macht Computerbetrug mit 77 % den größten Teil der Cybercrime-Straftaten aus. Datenveränderung und Computersabotage ist jedoch eher gering mit 3,4 % vertreten.

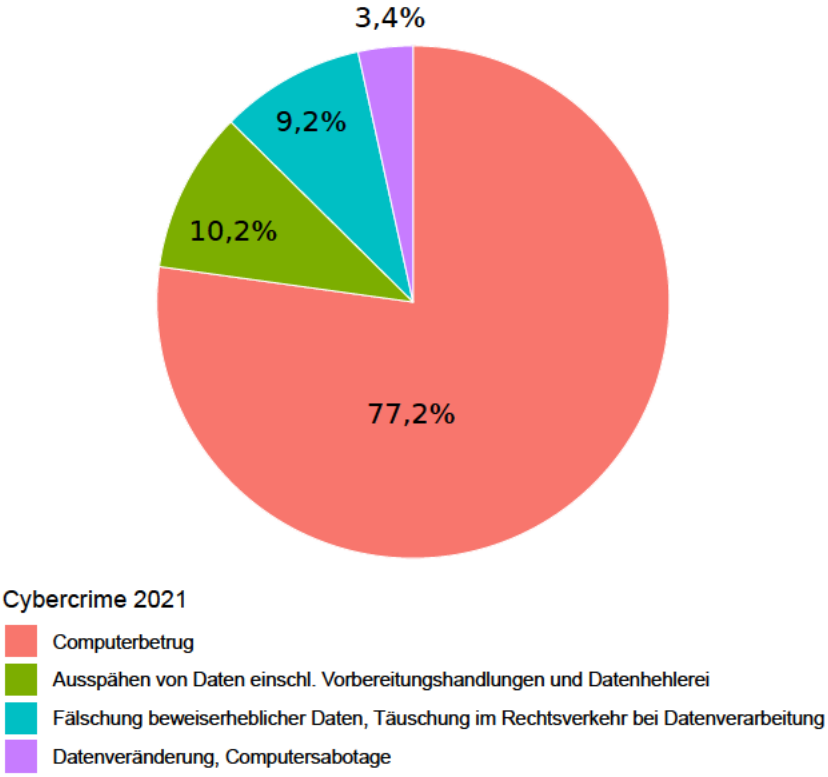


Abbildung 3.2: Verteilung der Cybercrime-Delikte, basierend auf Daten des BKA [10, S. 7]

Demgegenüber steht die Entwicklung, dass die Gesamtzahl der in der PKS erfassten Straftaten um 4,9 % im Vergleich zum Vorjahr zurückgegangen ist. Es wird versucht die gegenläufige Entwicklung bei der Aufklärungsquote damit zu erklären, dass die verstärkte Anonymisierung im Internet, die erforderliche komplexe Ermittlungsarbeit und häufig im Ausland verortete Täter Herausforderungen für die Polizei darstellen. [10, S. 6–7]
Im Bereich der Underground Economy sind 2021 besonders sogenannte Initial Access Broker (IAB) und online angebotene gefälschte Impfzertifikate bedeutungsvoll geworden. IAB bezeichnet Handelnde mit unrechtmäßig erlangten Zugängen zu Netzwerken vor allem zu Unternehmens- oder Behördennetzwerken. [10, S. 8–10]
Beim Thema Data-Leaks werden Daten aus externen Quellen wiedergegeben. Der Identity Leak Checker des Hasso-Plattner-Instituts (HPI) [15] erfasst jeden Monat Millionen von Data-Leaks kompromittierter Konten. Dabei sind quartalsweise Schwankungen zu verzeichnen, besonders herausragend ist die Anzahl im November 2021. Im Jahr 2021 wurden insgesamt ca. 184,65 Millionen kompromittierte Nutzerkonten festgestellt. [10, S. 12]
Einen der Haupteintrittsvektoren 2021 stellt Phishing dar. Die Zahl an Phishing-Vorfällen erlebte in den vergangenen Jahren einen deutlichen Aufschwung. Wie die Anti-Phishing-Working-Group (APWG) [16] in den quartalsweise erscheinenden Trendberichten feststellt, ist die Anzahl neu bekannt gewordener Phishing-Webseiten seit der Corona-Pandemie massiv angestiegen. Dabei besteht weiterhin der inhaltliche Bezug der Phishing-Nachrichten auf aktuelle gesellschaftliche Themen. Eingesetzt werden vielfältige Phishing-Methoden: E-Mails, Fake-Webseiten, SMS, Telefonie und Soziale Medien. Die Echtheits-Wirksamkeit wird dadurch erhöht, dass Nachrichten als Antwort auf vermeintlich geführte Konversationen versendet werden. [10, S. 13–15] Bei der Beobachtung des Spam-Niveaus fällt ein hohes Spam-Aufkommen bis zum Sommer 2021 auf. Die Sommer- und Herbstmonate über sinkt dieses und steigt gegen Ende des Jahres wieder graduell an. [10, S. 15]

Das Aufkommen und die Entwicklung von Malware-Angriffen auf Netze des Bundes per E-Mail und präventive Sperrungen von maliziösen Webseiten werden vom BSI als Abwehr-Indizes gemessen. Herausragende Zahlen bei den abgewehrten Schadprogramm-Angriffen sind im März und November 2021 zu verzeichnen. Peaks im März und August sind bei der Sperrung maliziöser Webseiten festzustellen. Insgesamt sank die Zahl der abgewehrten Malware-Angriffe um 40 % und die Sperrungen von Webseiten sank um 12 % im Vergleich zum Vorjahr. [10, S. 14–15]
Einen weiteren Eintrittsvektor stellen IT-Schwachstellen dar. Dazu wird auf eine Veröffentlichung des IT-Security-Dienstleisters Trend Micro verwiesen [17]. Bei der Betrachtung der Anzahl entdeckter IT-Schwachstellen ist der enorme Anstieg seit 2017 deutlich zu erkennen. In gleicher Weise entwickeln sich ebenfalls Zero-Day-Exploits. Mit Log4Shell wurde im Dezember 2021 eine schwerwiegende Schwachstelle in der Java-Programm-Bibliothek Log4j mit potenziell erheblichen Folgen für Betroffene entdeckt. [10, S. 15–17]
Zu den primären Angriffen zählt erneut Malware. Darunter ist Ransomware der Typus mit medial höchster Relevanz aufgrund des großen Schadenspotenzials. Zu den bedeutendsten Malware-Typen zählen außerdem Remote-Access-Tools (RAT) und Info-Stealer. Diese sind weniger offensiv als Ransomware und DDoS-Angriffe, sind aber dennoch in der Lage, beträchtliche finanzielle Schäden zu verursachen. Dafür wird sich mittels der Malware Zugriff zu Systemen verschafft, um daraus Daten abzuleiten und diese für den Gebrauch in darauf aufbauenden Angriffen in der Underground Economy zu verkaufen. [10, S. 18]
Der Fokus des Berichts liegt 2021 auf Ransomware. Dieses Phänomen war erneut die primäre, gesamtgesellschaftliche Bedrohung im Bereich Cybercrime, wobei das Bedrohungs- und Schadenspotenzial nochmals deutlich angestiegen ist. Im Berichtsjahr erfolgten Angriffe auf Kritische Infrastrukturen (KRITIS), öffentliche Verwaltungen und internationale Lieferketten. Daraus folgten zudem nicht-monetäre Schäden durch die Beeinträchtigung der Funktionsfähigkeit des Gemeinwesens. Bei dieser Angriffsmethode gibt es drei typische Modi Operandi. Double Extortion ist mittlerweile der Standard-Modus-Operandi und meint die Verschlüsselung und Veröffentlichung der Daten. Mit Triple Extortion werden zusätzliche DDoS-Attacken bei den Geschädigten bezeichnet. Bei der Second-Stage-Extortion werden zusätzlich Kunden der Geschädigten mit der Veröffentlichung ihrer Daten erpresst. [10, S. 2] Laut IT-Security-Dienstleister Coveware umfasste Double Extortion durchschnittlich 81 % der Ransomware-Vorfälle [18]. [10, S. 20]
Im internationalen Vergleich ist Deutschland laut dem Cyber Threat Report 2021 von Sonicwall überdurchschnittlich häufig von Ransomware-Angriffe betroffen [19]. Die durchschnittlich gezahlte Lösegeldsumme schwankt im Verlauf des Jahres deutlich. Ein Höchstwert von 322 168 US-Dollar wurde im vierten Quartal 2021 verzeichnet [20]. [10, S. 20]
Ein medial bekanntes Beispiel eines Ransomware-Vorfalls 2021 in Deutschland ist der Angriff auf die Landkreisverwaltung von Anhalt-Bitterfeld im Sommer 2021. Als Folge der Datenverschlüsselung des Netzwerkes der Verwaltung im Hauptsitz und weiteren Nebenstellen kam es zu erheblichen Beeinträchtigungen der Verwaltungsprozesse. Die Tätergruppierung „Grief“ forderte mit Double Extortion und der Veröffentlichung von 200 MB der abgeflossenen Daten Lösegeld in der Kryptowährung Monero. Als Folge des Angriffes wurde erstmals ein Cyber-Katastrophenfall ausgerufen, welcher erst über ein Jahr später aufgehoben wurde. Weitere medienwirksame Ransomware-Vorfälle waren international der Angriff auf den US-Pipelinebetreiber Colonial Pipeline und der Angriff auf das Washington Police Department. Als weitere bedeutende Entwicklung im Bereich der Ransomware ist das Verbot des Verkaufs und der Vermietung dieses Malware-Typus in den beiden größten russischsprachigen Foren der Underground Economy durch die Administratoren zu nennen. Als Gründe nannten die Verantwortlichen, dass das Angebot von RaaS zu viel Aufmerksamkeit auf die Foren lenke und die Möglichkeit auf schnelles Geld eine große Anziehung auf viele unprofessionelle und

unseriöse RaaS-Anbieter habe. In Folge dieses Verbotes sank die Attraktivität von Ransomware und damit einhergehenden Affiliate-Programmen nicht. [10, S. 20–21]
Angreifende fokussierten mit Ransomware-Angriffen im Berichtsjahr besonders das Finanzwesen, Einzelhandel, öffentliche Einrichtungen und das verarbeitende Gewerbe. Grundsätzlich bleibt zu sagen, dass jeder Ziel werden kann. Tendenziell wird eher auf größere Unternehmen abgezielt. Als prägende Ereignisse 2021 gelten Angriffe auf KRITIS und öffentliche Verwaltung. Solche Ziele sind ab der Hälfte des Jahres 2021 besonders betroffen und werden weiterhin zunehmend fokussiert. [10, S. 27]
In der Entwicklung der DDoS-Angriffe sind sowohl quantitative als auch qualitative Steigerungen zu verzeichnen. Quantitativ weist die Anzahl solcher Angriffe starke saisonale Schwankungen auf und ist nicht konstant über das Jahr verteilt. Nach Daten der Deutsche Telekom AG (DTAG) sind besonders im ersten und letzten Quartal 2021 überdurchschnittlich hohe Angriffszahlen festzustellen. Diese Beobachtung erläutert der DDoS-Mitigationsdienstleister Link11 [21] damit, dass vor allem Ende des Jahres 2020 ein enormer Anstieg zu verzeichnen ist und die Zahlen im ersten Quartal 2021 ein Nachbeben darstellen. Hohe Anstiege im vierten Quartal werden mit der erhöhten Relevanz von E-Commerce-Plattformen in der Weihnachtsgeschäftszeit und um den Black Friday erklärt. Zusätzlich zur Steigerung der Quantität der Angriffe sind qualitative Anstiege wahrzunehmen. Wie aus der Datenlage der DTAG hervorgeht, sind besonders im ersten und letzten Quartal Anstiege in der durchschnittlichen Bandbreite, den durchschnittlichen Bandbreiten-Peaks und der durchschnittlichen Maximalpaketrate zu verzeichnen. Die hohen Anstiege gegen Jahresenden sind auf die gleichen Gründe wie die der quantitativen Entwicklung zurückzuführen. [10, S.23–24]
Als Trends in der Entwicklung der DDoS-Angriffe sind verstärkt Multivektor-Angriffe und die Kombination mit Ransomware-Angriffen zu nennen. Zu den Multivektor-Angriffen, das heißt Angriffe, die sich auf mehrere Ebenen einer Netzwerkverbindung richten, gehört sogenanntes Carpet-Bombing. Damit werden meist nicht erkannte Angriffe mit niedrigem Datenverkehr pro IP-Adresse auf ganze Netzwerkblöcke bezeichnet. Aufgrund der nachgelagerten DDoS-Angriffen nach einer Infektion mit Ransomware, dem sogenannten Triple Extortion, sind DDoS-Angriffe noch relevanter als in den Vorjahren. [10, S. 25]
Ein bekanntes Beispiel eines DDoS-Angriffs in Deutschland sind die Angriffe auf Systeme der Universität Mainz zu Beginn des Jahres 2021. Betroffen war davon der Home-Schooling-Lehrbetrieb des Bundeslandes Rheinland-Pfalz durch Schwierigkeiten bei der Erreichbarkeit der Lernplattform, den darauf befindlichen Lernmaterialien und des damit verbundenen Webkonferenzsystems. [10, S. 26]
Die Steigerung der Bedrohung durch Cybercrime spiegelt sich auch in Supply-Chain-Angriffen wieder. Diese Angriffsart hat ebenfalls merklich an Bedeutung gewonnen, wie ENISA, die Agentur der Europäischen Union für Cybersicherheit, in ihrer Veröffentlichung schreibt [22]. Eine besondere Gefahr geht von Supply-Chain-Angriffen in Kombination mit Ransomware-Infektionen aus. Hier besteht die Möglichkeit, dass alle Unternehmen und Akteure innerhalb der Lieferkette getroffen werden können und dadurch ein immenses Schadensausmaß entstehen würde. Eine weitere Motivation für Angreifende für den Einsatz von Supply-Chain-Angriffen ist die Datenspionage, da in besser gesicherte Systeme eingedrungen werden kann und eine große Menge von Angriffszielen erreicht wird. Ein bemerkenswertes Ereignis war der Ransomware-Angriff im Zusammenspiel mit Supply-Chain-Angriff auf das amerikanische Unternehmen Kasey Ltd. und seiner Software Virtual System Administrator (VSA) für Fernwartungen. Mittels des später veröffentlichten Master Keys konnten die verschlüsselte Daten wiederhergestellt werden. [10, S. 28–29]
Im Bereich der Täterkreise setzte sich der Trend der Vorjahre fort. Eine Unterscheidung der Tätergruppierungen nach Professionalität, verwendeter Malware und Vorgehensweise ist kaum noch möglich. Der zentrale Unterschied, besonders zwischen organisierten Cyberkriminellen und staatlichen

APT, ist die Motivationslage. Beide Gruppierungen setzen zunehmend komplexe Angriffsmethoden ein. Dazu gehören Ransomware- und DDoS-Angriffe und sie fokussieren sich primär auf wichtige funktionelle Institutionen der Gesellschaft. Hybride Bedrohungen bleiben insbesondere staatlichen Akteuren vorbehalten. [10, S. 30]
Anhand der Motivationslage entstehen drei Bereiche: unabhängige Cyberkriminelle, staatliche Akteure und dazwischen State-Sponsored-Gruppierungen. Unabhängige Cyberkriminelle arbeiten vor allem finanziell motiviert. Doch dazu gehören auch Hacktivisten wie beispielsweise Anonymous. Staatliche Akteure hingegen verfolgen ideologische Ziele und eine politische Agenda. State-Sponsored-Gruppierungen kooperieren und arbeiten lose mit Staaten zusammen und werden durch die Annahme von Aufträgen in gewisser Weise durch staatliche Strukturen gefördert und geduldet. Die zunehmende Professionalisierung der Angreifenden bewirkt die Angleichung des Wissens, der verfügbaren Ressourcen und des Gefährdungspotenzials der Gruppierungen auf ein ähnliches Niveau. [10, S. 31]
Der Phänomenbereich Cybercrime bietet ein hohes Schadenspotenzial. Als Folge der Angriffe können existenzschädigende Probleme auftreten und Einschränkungen der Funktionalität und Verfügbarkeit kritischer Dienstleistungen. Das Ausmaß der Schäden ist auf Grundlage der PKS nicht valide einschätzbar. Dafür sind weitere externe Quellen erforderlich. Außerdem sind die Folgeschäden nicht abschätzbar. An dieser Stelle wird sich auf die durch den Bitkom e.V. erhobenen Schadensquantifizierungen bezogen. Demnach ist eine Gesamtsumme der Schäden von 223,5 Milliarden Euro für den Berichtszeitraum 2020/2021 zu nennen. Im Vergleich mit den Vorjahren ist eine signifikante Steigerung deutlich erkennbar. Besonders die Schadenssummen in Folge von Ransomware-Angriffen nehmen stetig zu und sind ein bedeutender Teil der Gesamtsumme. Data-Leaks hingegen verursachen zunächst keine monetären Schäden, aber die veröffentlichten Daten können als Grundlage für weitere Angriffe dienen. Dadurch sind die Schäden dieser Angriffsart nicht direkt quantifizierbar. Allgemein ist festzustellen, dass Betroffene in Folge von Angriffen nicht nur mit großen Herausforderungen zu kämpfen haben, sondern sich daraus existenzbedrohende Notlagen entwickeln können. [10, S. 34–35]
Die Bekämpfung der Cybercrime stellt sich als gesamtgesellschaftliche Aufgabe dar. Dafür sind repressive Maßnahmen und vorausschauende IT-Sicherheitsmaßnahmen sowie Sensibilisierung der Gesellschaft notwendig. [10, S. 36–37]

3.2 Die Lage der IT-Sicherheit in Deutschland 2021 und 2022

Dieser Bericht wird jährlich vom BSI publiziert. Der Berichtszeitraum des Lageberichts 2021 umfasst den Zeitraum Juni 2020 bis Ende Mai 2021. Der Lagebericht 2022 berichtet über den Zeitraum Juni 2021 bis Mai 2022. Um das gesamte Jahr 2021 zu Überblicken, werden in dieser Arbeit beide Berichte betrachtet. Inhaltlich basieren die Berichte auf Daten, welche vom BSI erhoben wurden, sowie auf einzelnen ausgewählten externen Quellen wie z.B. dem Mitigationsdienstleister Link11. Neben aktuellen Zahlen im Bereich Cybercrime in Deutschland werden zusätzlich Empfehlungen zum Umgang mit der zunehmenden Bedrohungslage gegeben. Zudem werden die Aufgabenbereiche mit Ergebnissen und das nationale und internationale Arbeiten des BSI aufgezeigt. [5] [23]
Diese beiden Publikationen des BSI werden im Folgenden gemeinsam unter den verschiedenen Teilbereichen zusammengefasst. Somit ergibt sich eine Zusammenfassung über das Jahr 2021.
Die bereits kritische und angespannte Lage spitzte sich weiter zu, sodass die Bedrohung im Cyberraum ihren bisherigen Höhepunkt erlangt. [5, S. 11] [23, S. 9]
Im Berichtsjahr ist die Produktion neuer Schadprogramm-Varianten deutlich beschleunigt worden. Im

Bereich der Produktion von Schadprogrammen zeigt sich bei der Betrachtung des durchschnittlichen täglichen Zuwachses in Abbildung 3.3 eine Sommerpause. In den Sommermonaten sank diese Rate bis unter den täglichen Zuwachs im Zwölf-Monatsdurchschnitt. Dieser lag bei 409 500 neuen Malwarevarianten. Im Vergleich zum Vorjahr stellte der durchschnittliche tägliche Zuwachs im Februar einen besonders starken Höhepunkt dar. Mit durchschnittlich 553 000 neuen Varianten pro Tag war das der höchste gemessene Wert. [23, S. 11–12]

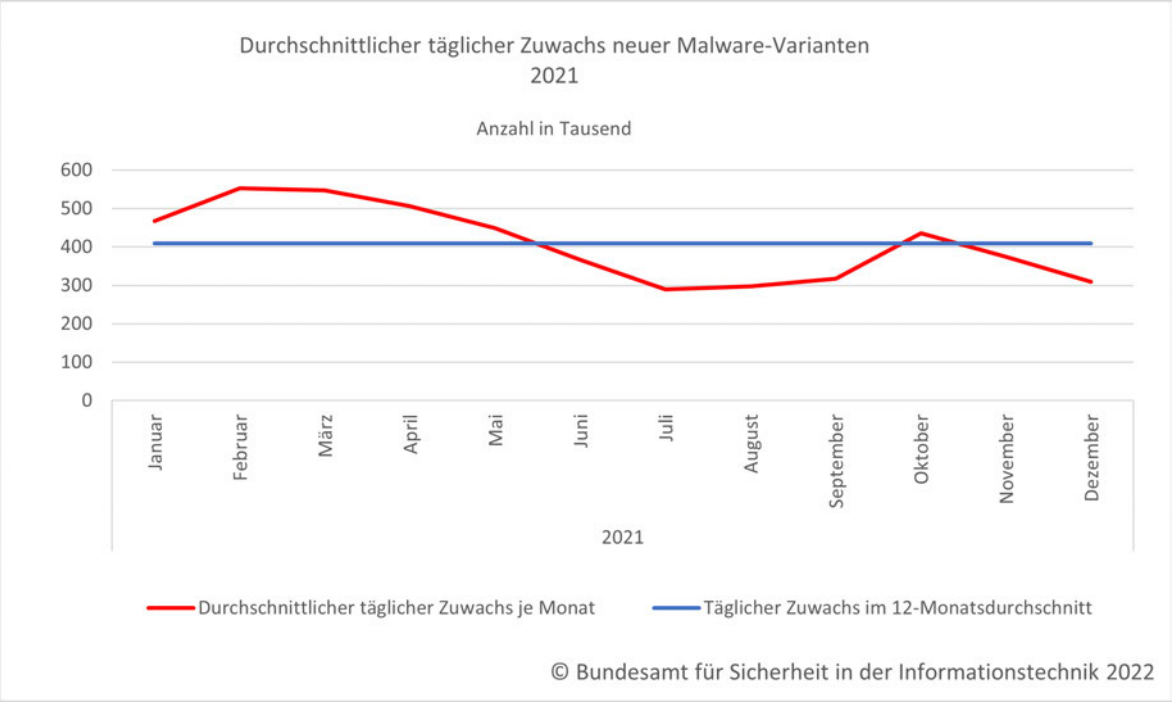


Abbildung 3.3: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH [24]

Als größte Cyber-Bedrohung für Staat, Wirtschaft und Gesellschaft gilt Ransomware. [5, S. 14] Im Lagebericht 2021 wird eine neue Entwicklung diesbezüglich beschrieben: Double Extortion, das heißt das zusätzliche Androhen der Veröffentlichung der Daten. [23, S. 12] Im darauffolgenden Lagebericht wird diese Angriffsmethode als Regelfall dargelegt. [5, S. 14] Dabei ist festzustellen, dass die Anzahl der monatlich aktiven Data-Leak-Seiten um fast 360 % zugenommen hat. [23, S. 13] Im Ransomware-Bereich ist die Fokussierung der Angreifenden auf finanzstarke Opfer zu beobachten. Damit lassen sich möglichst hohe Lösegelder erpressen. Bezeichnet wird dieses Phänomen als Big Game Hunting, zu deutsch Großwildjagd. [23, S. 12] Eine weitere Beobachtung der Entwicklung ist das Phänomen CaaS. Diese Form der Arbeitsteilung breitet sich auch im Ransomware-Bereich aus. [5, S. 14] Für den Rückgang von Data-Leaks nach Mai 2021 ist mit großer Wahrscheinlichkeit die Abschaltung einer Reihe von RaaS-Angeboten ursächlich. Bereits im Sommer 2021 wurden alternative Angeboten geschaffen. Eine genaue Anzahl der Ransomware-Angriffe 2021 ist nicht feststellbar. Die gemeldeten Fälle beim BSI werden von einer mutmaßlich hohen Dunkelziffer begleitet. Aus den meisten Quellen diesbezüglich geht die gleiche Schlussfolgerung hervor: die erpressten Lösegeldbeträge nehmen zu. Absolute Zahlen gestalten sich schwierig, da in einzelnen Statistiken verschiedener IT-Sicherheitsdienstleister lediglich der eigene Kundenstamm betrachtet wird und viele Opfer nicht bekannt werden. [5, S. 16] Als herausragende Vorfälle in diesem Phänomenbereich der Cybercrime ist der Katastrophenfall nach einem Ransomware-Angriff auf eine deutsche Kreisverwaltung im Juni

2021 und auf ein Handelsunternehmen im November 2021 zu nennen. [5, S. 21–22]
Data-Leaks stehen aufgrund von Ransomware-Angriffen mit anschließender Schweigegeld-Erpressung eng in Verbindung mit Ransomware. Diese Art der Opfer nimmt stetig zu. An dieser Stelle wird auf eine externe Quelle, die Nachrichtenseite „The Record“ [25], verwiesen. Die Entwicklung der Data-Leaks infolge von Ransomware-Angriffen, basierend auf Daten der externen Quelle, ist in Abbildung 3.4 zu sehen. Darin zeigt sich, dass erste Schweigegelderpressungen Anfang 2020 zu verzeichnen sind und diese Angriffsart sich im weiteren Jahresverlauf immer mehr etablierte. Anfang 2021 kam es zur Abschaltung der Infrastruktur der Schadsoftware Emotet und verschiedener RaaS-Angebote. Diese können für den Rückgang von Data-Leaks im Januar 2021 ursächlich sein. Außerdem ist ein Rückgang ab Mai 2021 zu verzeichnen. Dieser wird ebenfalls mit der Abschaltung einer Reihe von RaaS-Angeboten erklärt. Im Laufe des Jahres nahmen Data-Leaks wieder zu. Ein besonderer Höhepunkt ist im November feststellbar. [5, S. 16–17]

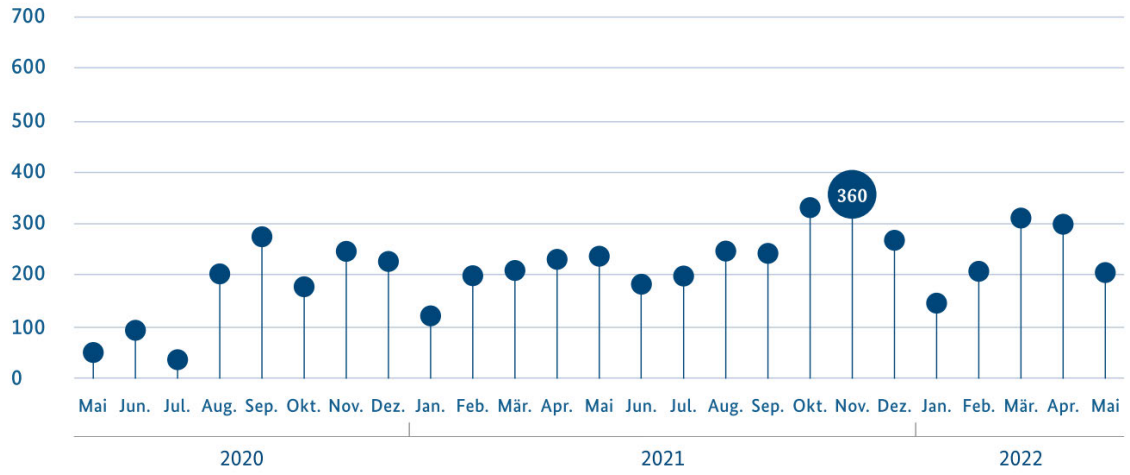


Abbildung 3.4: Opfer von Data-Leaks von Januar 2020 bis Mai 2022 [5, S. 17], Daten: The Record [25]

Im Phänomenbereich Botnetze bezieht das BSI seine Daten von externen Quellen und durch eigene Sinkhole-Systeme. Dabei nehmen die Systeme anstelle der Command-and-Control-Server der Angreifenden die Kontaktanfragen der Bots entgegen und zeichnen diese auf. [23, S. 20] Die Nutzung von Botnotzen entwickelte sich dahingehend, dass diese überwiegend zum Ausspionieren persönlicher Informationen und zur Verbreitung weiterer Schadprogramme verwendet werden. Hingegen nahm die Anzahl bekannter DDoS-Botnetze weiter ab. Der Fokus liegt zunehmend auf mobilen Endgeräten: sieben von zehn beobachteten Botnetze im BSI-Sinkholing zielten auf Tablets und Smartphones mit dem Betriebssystem Android. Außerdem erfolgte eine Steigerung der Qualität. Seit Januar 2021 wurde mittels SMS-Spam-Kampagnen die Verbreitung der Schadsoftware MoqHao betrieben. Nach Installation der App wird das mobile Endgerät in ein Botnetz eingegliedert und zum Ausspähen persönlicher Informationen und zur Weiterverbreitung missbraucht. In diesem Bereich der Botnetze lässt sich eine steigende Professionalisierung verzeichnen, die zur zunehmenden Gefährdung beiträgt. Der größte Anteil aktuell aktiver Bot-Software wird als MaaS auf einschlägigen Plattformen angeboten. Dadurch weitet sich die Nutzung dieser Mechanismen auf weniger technisch versierte Angreifende aus. [23, S. 20] Durch das BSI werden täglich infizierte Geräte an deutsche Provider gemeldet, um deren Kunden zu informieren. Im Berichtszeitraum des Lageberichts 2021 wurden täglich bis zu 40 000 infizierte Geräte in Deutschland gemeldet. Diese Zahl stellt eine Untergrenze dar, es wird angenommen, dass die tatsächliche Zahl deutlich größer ist. [23, S. 20] Die

Anzahl der Meldungen im Lagebericht 2022 wird auf täglich durchschnittlich 41 000 datiert. [5, S. 25] Eine vollständige Erfassung aller Infektionen ist nicht möglich, es wird eine hohe Dunkelziffer vermutet. [23, S. 20] Um den Umfang des Dunkelfeldes genauer abzuschätzen, erfolgt die Beobachtung des Unique-IP-Index. Damit werden anhand einzigartiger IP-Adressen das Aufkommen und die Entwicklung der Infektionszahlen in den beobachteten Botnetzen gemessen. [23, S. 20] Eine grafische Darstellung des gesamten Jahres 2021 ist nicht verfügbar. Abbildung 3.5 aus dem Lagebericht 2021 stellt die Monate Januar bis Mai 2021 dar [23, S. 21] und Abbildung 3.6 bildet den Rest des Jahres ab [5, S. 24].

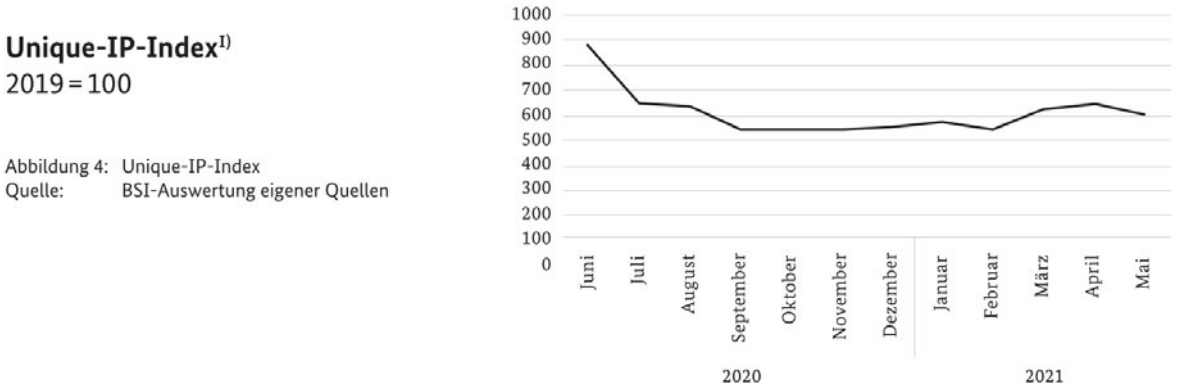


Abbildung 3.5: Unique-IP-Index 2020–2021[23, S. 21]

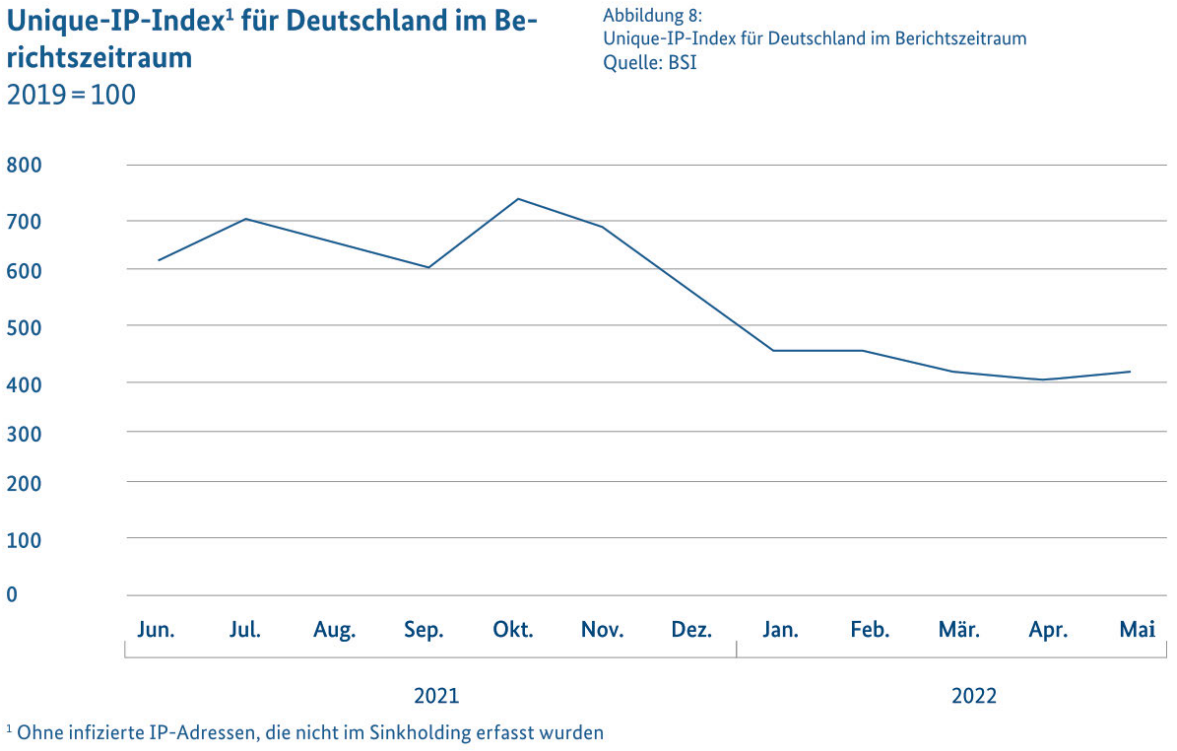


Abbildung 3.6: Unique-IP-Index 2021–2022 [5, S. 24]

Gezielte Angriffe auf finanzstarke Opfer zielen besonders auf populäre Server- und Desktop-Betriebssysteme wie Linux und Microsoft Windows ab. Dabei geht es primär um die Verbreitung von Ransomware. [5, S. 25] Im Januar 2021 gelang internationalen Strafverfolgungsbehörden die Abschaltung des

Botnetzes Emotet. Diese Schadsoftware galt als größte Bedrohung weltweit. Die Verbreitung fand über weltweite Spam-Kampagnen statt. Die Funktionen der Schadsoftware sind die Ausnutzung der E-Mail-Postfächer auf den Geräten zur Weiterverbreitung und das Nachladen weiterer Schadprogramme wie den Banking-Trojaner Trickbot. Dazu kam es zu ganzen kompromittierten Netzwerken und in zahlreichen Fällen zur Verschlüsselung durch die Ransomware Ryuk. [23, S. 21–22] Seit November wurden Symptome des Wiederaufbaus beobachtet, wie nach dem monatelangen Ausbleiben neuer regelmäßiger Spam-Versand von Emotet-Spam seitdem verriet. Das Niveau vor der Abschaltung wurde noch nicht erreicht, da sich der bisherige Fokus des Spam-Versands auf den asiatischen Raum bezieht. Präventiv hatte das BSI im November 2021 eine Cyber-Sicherheitswarnung herausgegeben, um vor einer neuen Welle zu warnen. [5, S. 26]
Im Phänomenbereich Spam und Phishing sind im Januar, März und Mai 2021 Sextortion-Kampagnen mit großer Reichweite herausragend. [23, S. 19] Dabei behaupten Angreifende in Spam-Mails, kompromittierende und intime Geheimnisse des Opers zu besitzen und diese zu veröffentlichen. Für die Nicht-Veröffentlichung der Daten wird das Opfer erpresst. [5, S. 11] Im Lagebericht 2022 ist eine Grafik mit der Aufteilung des Spams nach seiner Art zu finden. Daraus geht hervor, dass im Berichtszeitraum mit 36 % Erpressungs-Spam den größten Teil ausmachte, dicht gefolgt von Betrug mit 33 %. Werbungs-Spam machte lediglich einen Anteil von 16 % aus, die verbliebenen 15 % werden als Sonstiges kategorisiert. [5, S. 27] Auch der Lagebericht 2021 enthält die Aussage, dass Erpressungs-Mails die größte Spam-Kategorie ausmachten. [23, S. 19] Sextortion-Mails umfassten mit 76 % den größten Teil der Erpressungs-Mails. In der Kategorie Betrugs-Mails waren rund 90 % als Phishing-Mails einzuordnen. [5, S. 27]

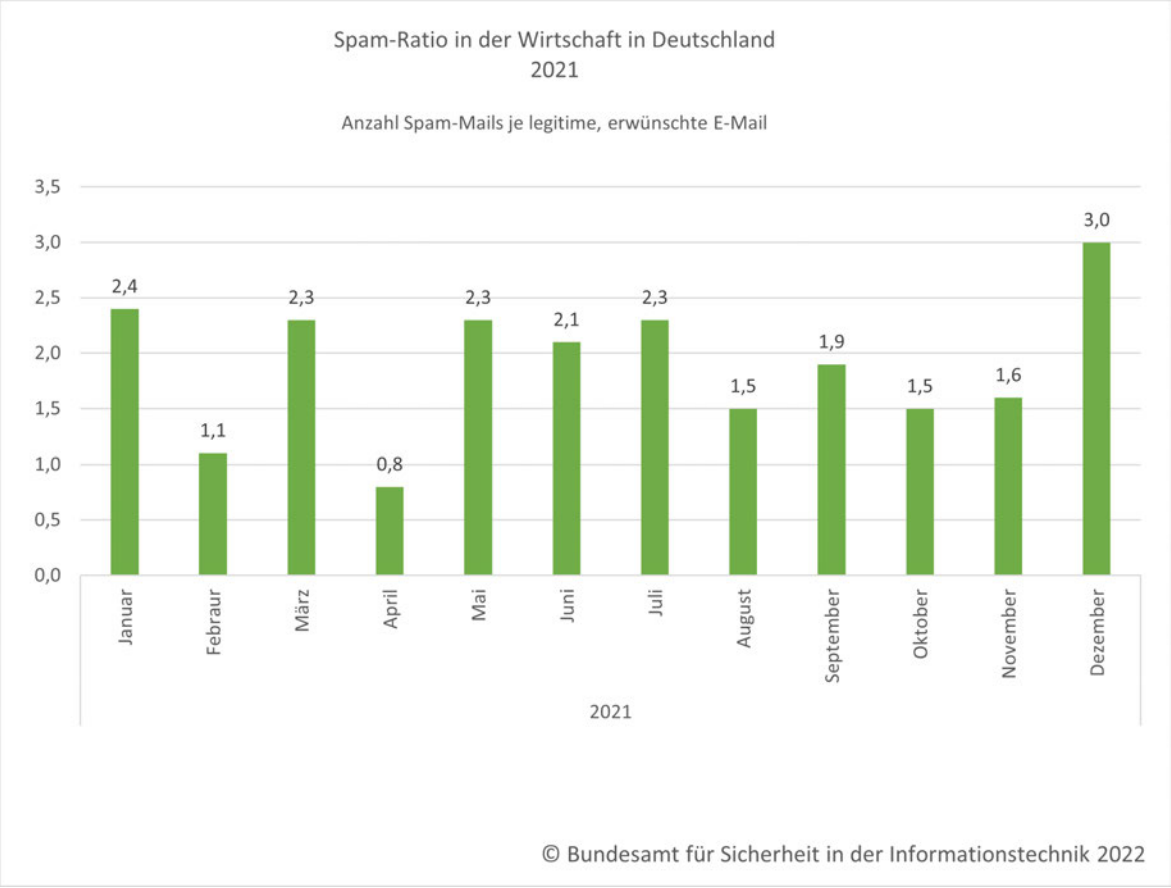


Abbildung 3.7: Spam-Ratio in der Wirtschaft [26]

Die Spam-Ratio ist ein Messwert, mit welchem angegeben wird, wie viele Spam-Mails auf eine legitime, erwünschte Mail gezählt werden. In der Abbildung 3.7 ist die Spam-Ratio in der Wirtschaft dargestellt. Dabei sind deutlich die Höhepunkte der Sextortion-Kampagne im Januar, März und Mai 2021 zu erkennen. [23, S. 19] Außerdem sind weitere Höhepunkte im Juli und besonders stark im Dezember zu sehen.
Abbildung 3.8 stellt die Spam-Ratio der Bundesverwaltung dar. Mit der Abschaltung des Botnetzes Emotet im Januar 2021 kam es im Februar zu einer deutlichen Entspannung. Das Spam-Aufkommen im Spätsommer und Herbst 2021 weist ein unterdurchschnittliches Niveau auf. Der Anstieg im Dezember ist mit der Sextortion-Kampagne nach den Online-Shopping-Events Black Friday und Cyber Monday und dem Wiederaufbau des Botnetze Emotet zu erklären. [5, S. 84–86] Bei der Spam-Mail-Angriffswelle im März 2021 handelt es sich um Bounce-Mails. Dabei wurden als gefälschte Absender-Adressen in Malware-Spam-Kampagnen zahlreiche E-Mail-Adressen der Bundesverwaltung angegeben und der Großteil der Empfänger-Adressen existierte nicht. Damit wurden die angegebenen E-Mail-Adressen der Bundesregierung mit Fehlermeldungen bombardiert. Es erfolgte eine Detektion und zentrale Abwehr dieser Mails, weil diese Anhänge mit Schadcode enthielten. [23, S. 69–70]

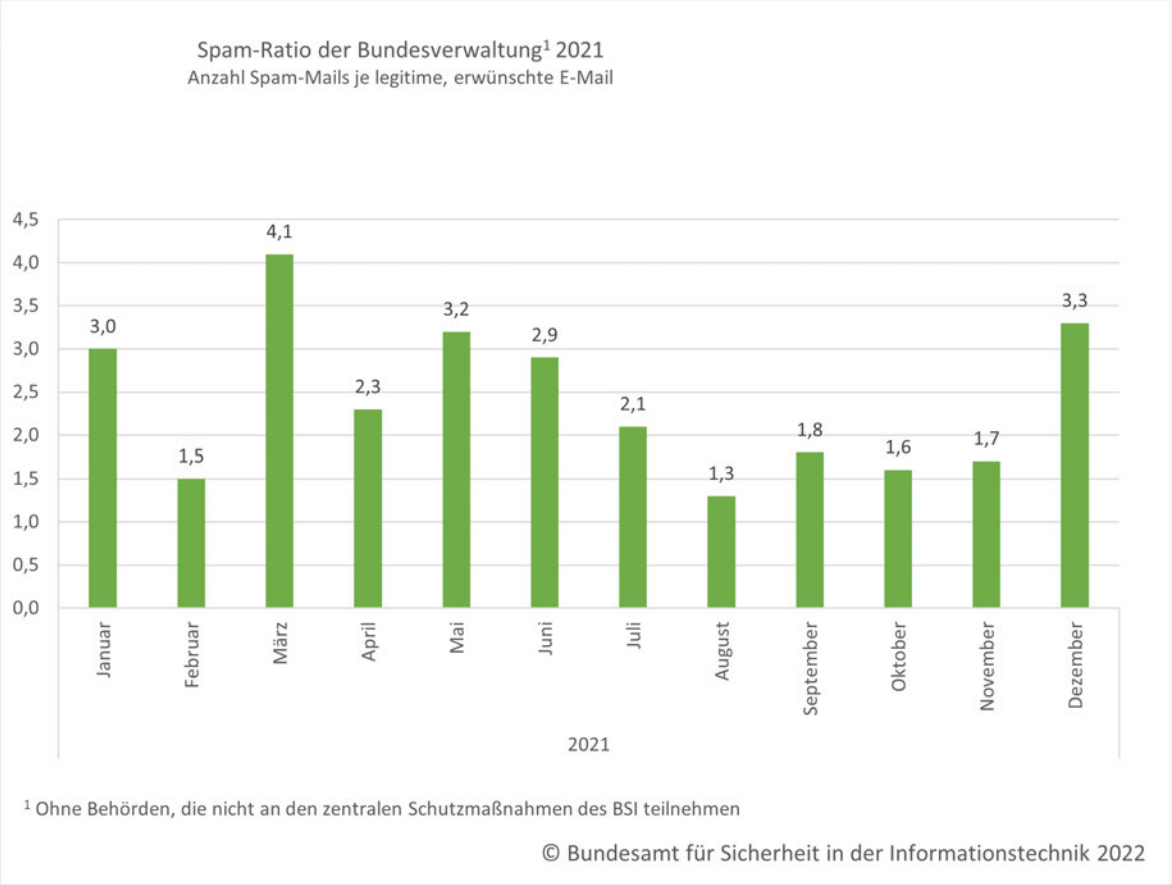


Abbildung 3.8: Spam-Ratio in der Bundesverwaltung [27]

Bemerkenswert sind bei der Entwicklung der Spam-Mails die mittlerweile sehr guten Deutschkenntnisse und besonders beim Finance-Phishing der Fokus auf gutes Design im Stil der einzelnen Banken. Besonders in Folge der Flutkatastrophe im westlichen Teil Deutschlands im Sommer 2021

wurde das vermehrte Aufkommen von Charity-Spam beobachtet. Damit werden betrügerische Spendenaufrufe bezeichnet, die versuchen, die Hilfsbereitschaft der Bevölkerung auszunutzen. [5, S. 28]
Im Bereich Schwachstellen sind besonders kritische Lücken in Microsoft Exchange-Server zu nennen. Außerplanmäßig veröffentlichte Microsoft im März 2021 Sicherheitsupdates, um vier kritische Schwachstellen zu patchen. Bereits kurz nach der Veröffentlichung kam es zu zahlreichen Angriffsversuchen, die diese Schwachstellen ausnutzen wollten. Probleme im Umgang mit den Schwachstellen bildeten stark veraltete Versionen, die keine Updates geliefert bekamen. Außerdem besitzt der Exchange-Server standardmäßig hohe Rechte und durch die schnelle Verfügbarkeit von Exploits mussten auch zeitnah gepatchte Systeme auf Kompromittierungen überprüft werden. Im Mai 2021 stellte das BSI immer noch knapp neun Prozent der geprüften Exchange-Server als verwundbar fest. [23, S. 26–27]
Mit Log4Shell wurde Anfang Dezember 2021 eine Schwachstelle in der freien und quelloffenen java-Bibliothek Log4j entdeckt. Diese ist in zahlreichen Anwendungen eingebunden. Durch die Schwachstelle besteht die Möglichkeit, beliebige Schadsoftware auf Systemen mit anfälligen Anwendungen auszuführen. Aufgrund der einfache Möglichkeit der Ausnutzung wurde dieser Schwachstelle eine hohe Kritikalität zugewiesen und das BSI veröffentlichte eine Cyber-Sicherheits-Warnung Stufe rot, der höchsten Warnstufe. [5, S. 37]

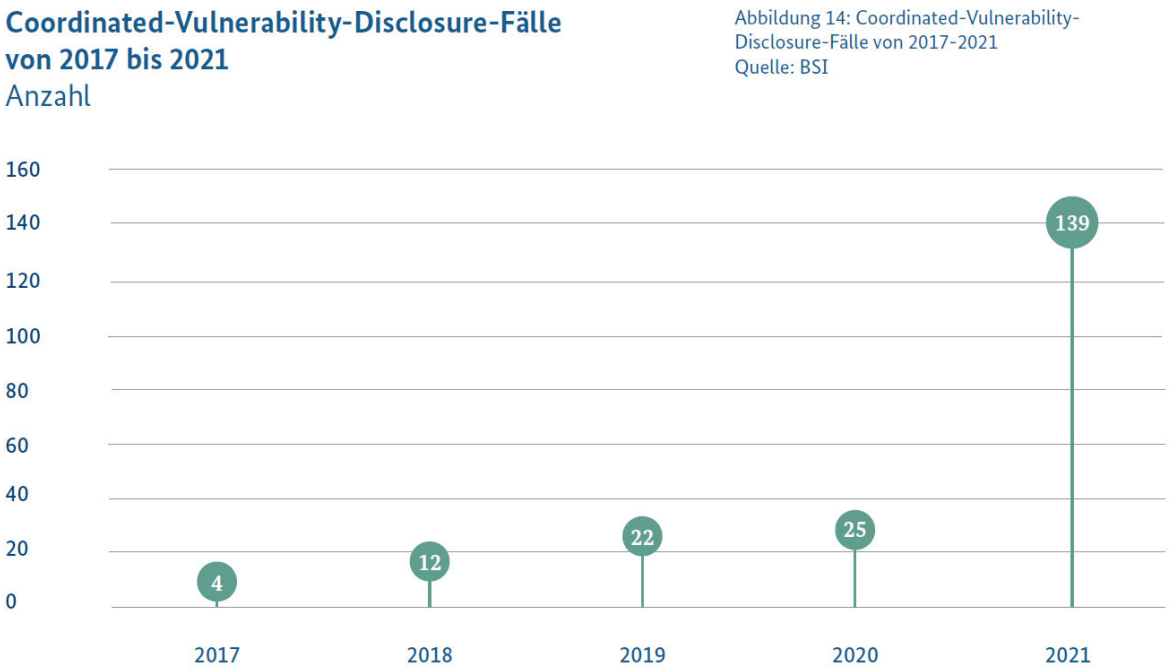


Abbildung 3.9: Entwicklung von Coordinated-Vulnerability-Disclosure-Fällen [5, S. 32]

Allgemein lässt sich sagen, dass die Zahl bekannt gewordener Schwachstellen in den letzten Jahren gestiegen ist. Im Berichtszeitraum des Lageberichts 2022 wurde ein neues Online-Meldeformular des BSI für Schwachstellen eingeführt. Das stellt mutmaßlich einen Grund für den enormen Anstieg in den Meldezahlen des BSI von 25 im Vorjahr auf 139 dar. Das BSI prüft zu diesem Thema auch externe öffentliche Quellen. Daraus entwickelte sich die These, dass die Lage im Berichtszeitraum überdurchschnittlich bedrohlich war. Im Common Vulnerability Scoring System (CVSS), einem Industriestandard um die Kritikalität von Schwachstellen international vergleichen zu können, wurden

2021 rund 10 % mehr Schwachstellen in Softwareprodukten beobachtet als im Jahr davor. Diese Entwicklung zeigt Abbildung 3.9. Dabei trat eine gemischte Verteilung der Kritikalität auf: zwei Prozent der Schwachstellen wiesen niedrige Kritikalität auf (Skalenwerte 1–4), 42 % mittlere (Skalenwerte 4–7) und mehr als die Hälfte wiesen hohe (Skalenwerte 7–9) oder kritische (Skalenwerte 9–10) CVSS-Scores auf der zehn-stufigen Skala auf. Im Bereich der Hardware-Schwachstellen dominierten zwei Angriffsklassen. Einerseits Angriffe, die die Besonderheiten der transienten Ausführung von Befehlen bei Prozessoren ausnutzen. Seit der Veröffentlichung der Schwachstellen Meltdown und Spectre 2017 entwickelten sich mehr als 25 derartiger Schwachstellen und Angriffe. 2021 wurden die neuen Schwachstellen „I see dead Micro-Ops“, Blindside und CIPHERLEAKS entdeckt. Andererseits dominiert die Angriffsart, die Seiteneffekte bei Operationen im Arbeitsspeicher ausnutzt. Dabei können durch gezielte hochfrequente Zugriffe auf Speicherzellen die Datenwerte in benachbarten Speicherzellen verändert werden. Dieses Phänomen ist seit 2014 bekannt, jedoch existieren bisher keine Gegenmaßnahmen. Im Jahr 2021 zeigte die Angriffsmethode BlackSmith, dass auch moderne DDR4-Speicher für derartige Seiteneffekte anfällig sind. Durch aktuelle Entwicklungen im Bereich der Anfälligkeit von Softwaresystemen wird vermehrt auf hardwarebasierte Lösungen zur Absicherung, wie beispielsweise Mehr-Faktor-Authentisierung, gesetzt. Der Einsatz von handelsüblichen Microcontrollern ist dafür weit verbreitet. 2021 wurden mehrere Hardware-Schwachstellen in derartigen Geräten bekannt. Dabei kann der Ausleseschutz durch gezielte Veränderung der Spannungsversorgung umgangen werden und dadurch beispielsweise geheime Schlüssel ausgelesen werden. Diese Entdeckungen zeigen, dass auch Hardwareschwachstellen eine ernsthafte Bedrohung darstellen und dadurch Schäden entstehen können. Software-Schwachstellen stellen jedoch die einfacheren Angriffsvektoren dar, denn Angriffe auf Hardwareschwachstellen gestalten sich in der Praxis sehr aufwendig und finden daher weniger Anwendung als softwarebasierte. [5, S. 35, 38]
Die Kompromittierung von Software-Supply-Chains stellte ebenfalls wieder einen schwer zu kontrollierbaren Angriffsvektor dar. [23, S. 28–29] Ein herausragendes Ereignis in diesem Bereich im Juli 2021 waren die Lieferketten-Angriffe auf die Software VSA eines amerikanischen Softwareherstellers, die auch in Deutschland vielfach eingesetzt wird. Das Programm findet vor allem Verwendung zur Fernwartung, Monitoring und Management von IT-Systemen von Kunden. Beim Angriff wurde über die Zero-Day-Schwachstelle CVE-2021-30116 die Ransomware REvil verbreitet. Das Unternehmen reagierte mit Sicherheitspatches innerhalb weniger Tage und mithilfe des Schlüsselmaterials aus einer vertrauenswürdigen Drittquelle konnten die verschlüsselten Systeme wiederhergestellt werden. [5, S. 36]
Im Bereich der APT zeigen aktuelle Entwicklungen einen Trend hin zu Angriffen auf Perimeter-Systeme, weg von mailbasierten Angriffen. Dazu gehören Geräte, die direkt aus dem Internet erreicht werden können wie Server, Firewalls, VPN-Gateways und Router. Gesucht wird dafür nach nicht gepatchten Schwachstellen. Für den Angriff werden Exploits, zunehmend auch altbekannte und einfache Methoden wie Brute-Forcing, eingesetzt. Um dauerhaften Zugriff auf die Systeme zu gewährleisten und Befehle auszuführen, werden auf kompromittierten Servern Webshells eingerichtet. Mit diesen, oftmals wenige Zeilen umfassenden, Code erlauben sich Angreifende ständigen Zugriff auf die Systeme. [5, S. 38–39] Perimeter-Systeme bieten die Vorteile, dass sie in der Regel nicht automatisiert mit Sicherheitsupdates versorgt werden und es außerdem für die Angreifenden bequemer ist, einen stets verfügbaren Server zu verwenden, als auf den Start von infizierten Rechnern zu warten. [23, S. 28–29] Einen weiteren Trend in diesem Bereich stellen Cloud-Anwendungen als Einstiegspunkte dar. Im Berichtszeitraum kam es zu deren Verwendung von der Gruppe APT29/Nobelium, um in interne IT-Netze zu gelangen. Nachdem Zugänge zu Cloudsystemen gestohlen oder erraten wurden, wird die Vertrauensbeziehung zwischen Cloud und Kunde ausgenutzt, um Zugang zu internen Netzen zu beschaffen. Es wird angenommen, dass diese Entwicklung weitere Verbreitung findet.

Eine weitere neue Erscheinung sind Hackers-for-Hire. Diese zeichnen sich durch den Verkauf von Produkten und Dienstleistungen für offensive Cyber-Operationen aus. Damit geht die Zunahme der Bedrohungslage einher, da steigende Angreiferzahlen und die Verfügbarkeit qualitativ hochentwickelter Exploits und Malware zu verzeichnen sind. [5, S. 39]
Trotz der Verwendung bekannter und öffentlich verfügbarer Werkzeuge für Angriffe setzen Angreifende weiterhin auf gruppenspezifische Malware-Entwicklung. In Deutschland zielten die meisten Angriffe von APT-Gruppen auf Regierungsbehörden ab. Das unterstützt die These, dass Regierungsbehörden im weltweiten Trend das häufigste Ziel gezielter Angriffe sind. Zugeordnet wurden diese Angriffe mindestens vier unterschiedlichen Ursprungsländern. Als beliebtes Ziel zählt weiterhin der Rüstungssektor. Eine Entwicklung der letzten Jahr ist zudem der Trend, vermehrt auch Nichtregierungsorganisationen und Thinktanks anzugreifen. Ein weiteres Ziel stellen in Deutschland lebende ausländische Regierungskritiker dar. [23, S. 28–29]
Einen herausragenden Vorfall bildeten im Jahr 2021 Spear-Phishing-Wellen durch die APT-Gruppe GhostWriter. Diese richteten sich an eine Vielzahl deutscher Politiker und Aktivisten und zielten nicht auf dienstliche Postfächer ab. Die Motivation der Kampagne war es, an privaten E-Mail-Zugangsdaten der Adressaten zu gelangen. Ein Zusammenhang mit der Bundestagswahl und den Landtagswahlen 2021 ist nicht auszuschließen, da diese APT-Gruppe sich bisher gegen osteuropäische Ziele richtete. Es wurden keine Desinformationsinhalte festgestellt. Im September 2021 erfolgte die Einschätzung, die Gruppe sei dem russischen Militärgeheimdienst GRU zuzuordnen. [5, S. 40]
DDoS stellen weiterhin eine der Hauptbedrohungen für die Cyber-Sicherheit dar. Seit der verstärkten Nutzung von Home-Office bietet sich eine größere Angriffsfläche an, da beispielsweise Remote-Zugänge und Mailserver aus dem öffentlichen Internet zugänglich sind. Dennoch wurden seit dieser Entwicklung nicht mehr DDoS-Angriffe in Deutschland beobachtet. Erstmals wurden langanhaltende DDoS-Epressungskampagnen registriert. Diese Schutzgelderpressung bildet eine neue Erscheinungsform der Cyber-Epressungen. Im DDoS-Bereich sind zunehmend Attacken auf Lernplattformen, die für das Home-Schooling essentiell sind, wahrzunehmen. Der Zusammenhang zwischen Lernplattformen und Pandemie-Maßnahmen bildet den Grund für derartige politisch motivierte Angriffe. [23, S. 31–33] Die im Berichtszeitraum des Lageberichts 2022 durchschnittlich gemessene Bandbreite der DDoS-Attacken beträgt rund 684 Mbps. Der Maximalwert wurde bei einem Angriff am 02. Dezember 2021 mit über 290 000 Mbits und einer Dauer von 228 Minuten gemessen. Hingegen sinken die durchschnittlichen Bandbreiten über alle Angriffe gemittelt tendenziell. Die Entwicklung begründet sich in den Strukturveränderungen innerhalb der DDoS-Angriffsarten: es wird nicht mehr auf hohe Bandbreite gezielt, sondern verstärkt mit geringerer Bandbreite auf Netzwerk- und Transportebene gearbeitet. Im internationalen Umfeld verzeichnete der deutsche Mitigationsdienstleister Link11 einen Anstieg der Angriffe von 41 % im Vergleich zum Vorjahr und maß Rekordwerte im dritten Quartal 2021. Das BSI nahm Anstiege der DDoS-Attacken besonders in umsatzstarken Zeiten wie dem Vorweihnachtsgeschäft und vor Online-Aktivitäten wie dem Black Friday wahr. Im Zusammenhang mit der Bundestagswahl 2021 wurden Fälle politisch motivierter Schutzgelderpressungen beobachtet. [5, S. 41–43]
Diese Art politisch motivierter Kriminalität steht im engen Zusammenhang mit hybriden Bedrohungen. Besonders von Desinformations-Angriffen betroffen waren europäische Impfkampagnen. Desinformation ist ein weit verbreitetes Mittel derartiger Bedrohungen. [23, S. 37–38] Im „Superwahljahr 2021“ waren verschiedene Phishing-Mail-Wellen vor der Wahl gegen deutsche Mandatstragende in Bund und Ländern zu beobachten. Diese wurden als Vorbereitungshandlungen für weitere Angriffe und Desinformationskampagnen eingeschätzt. Das BSI und der Verfassungsschutz warnten und ergriffen Maßnahmen dagegen. [5, S. 44–45]
Der Lagebericht 2021 widmet sich explizit in einem Kapitel den Gefährdungen der Cybersicherheit

durch die Covid19-Pandemie. Diese wird als Katalysator der Digitalisierung in Deutschland, sowohl für die Wirtschaft als auch für die Gesellschaft, dargestellt. Auf digitalem Weg wurden vermehrt Dienstleistungen und Geschäftstätigkeiten angeboten. Durch die schlagartige Einführung digitaler Arbeitsmittel und des Home-Office konnten Cyber-Kriminelle deren Schwachstellen und andere Angriffsmöglichkeiten ausnutzen. Trotzdem stellt das BSI keine signifikante Steigerung der Angriffszahlen fest. Damit steht im Zusammenhang, dass keine oder nur wenig neue Angriffsmethoden entwickelt wurden, sondern lediglich neue thematische Aufhänger eingesetzt wurden. So thematisierten beispielsweise Phishing- und Social-Engineering-Angriffe die Pandemie und deren Auswirkungen und Maßnahmen. Eine neue Entwicklung ist der verstärkte Fokus der Angreifenden auf Institutionen im Gesundheitsbereich. Als beispielhafte Vorfälle sind hier der Angriff auf die Europäische Arzneimittelagentur EMA, das Impfportal des Bundeslandes Thüringen und einen deutschen Hersteller von COVID-19-Antigentests zu nennen. Wie bereits erwähnt stellen Videokonferenzen ein leicht zu erreichendes Ziel dar. VPN-Sicherheit bildet einen wichtigen Bereich in der Absicherung des Home-Office und der Firmennetze. Herausforderungen und Chancen bietet das System Bring Your Own Device (BYOD). Dabei werden private Geräte im beruflichen Kontext eingesetzt. Allgemein ist das eine komfortable Lösung für Arbeitgeber und Arbeitnehmer. Doch es birgt Risiken wie verstärkter E-Mail-Verkehr auf dem Gerät und damit potenziell mehr Spam- und Phishing-Mails und eine erhöhte Gefahr der Infizierung mit Schadprogrammen. Schatten-IT bildet ebenso ein großes Gefahrenpotenzial. Das sind Geräte, die beschafft wurden und nicht zentral administriert werden können. Dadurch können automatische Sicherheitsupdates stagnieren und die Geräte können dadurch als Zugangspunkte für Angreifende fungieren. [23, S. 38–41]

Im Zuge der Corona-Pandemie erlebte der Einsatz von Videokonferenzen eine deutliche Zunahme. Diese bieten sich als attraktives Ziel für Angreifende an. Beim sogenannten Credential Stuffing werden veröffentlichte Nutzerdaten aus Data-Leaks automatisiert bei verschiedenen Dienstanbietern ausprobiert. Bei Treffern können sich die Angreifenden somit, als legitime Teilnehmende getarnt, in geschlossene Sitzungen einschleusen. Dadurch ist Wirtschaftsspionage und im Nachgang Erpressung möglich. Ein weiterer Angriffsvektor sind Phishing-Mails als vermeintliche Sitzungseinladungen mit Weiterleitung auf eine gefälschte Seite zur Anmeldung. Dadurch lassen sich Anmeldedaten sammeln. Als Zoom-Bombing wird der Zutritt zu Videokonferenzen des Anbieters Zoom bezeichnet, um diese gezielt zu stören. Das ist einfach möglich, weil Zugangsinformationen oft über öffentliche Kanäle verteilt werden. Besonders betroffen war von diesem Phänomen die Online-Lehre. Allgemein ist festzustellen, dass durch die Pandemie die physische Distanz zunahm und damit das Vertrauen in die digitale Identität immer bedeutungsvoller wurde. [23, S. 25–26]

Der zweite große Teilbereich der Lageberichte beschäftigt sich mit zielgruppenspezifischen Erkenntnissen und Maßnahmen.

Im Kapitel Gesellschaft wird jeweils zunächst auf Ergebnisse des Digitalbarometers eingegangen. Diese Untersuchung wird daher in diesem Kapitel nicht behandelt, weil sie eine eigenständige Studie dieser Arbeit darstellt und deshalb gesondert analysiert wird.

Im Bereich der medialen Identitäten, insbesondere sichere elektronische Identitäten auf dem Smartphone, hat die Bedrohungslage durch Manipulationsversuche deutlich zugenommen. Ein bedeutendes Ereignis war der CEO-Fraud im Oktober 2021. Dabei wurde mit einem Anruf mit einer gefälschten Stimme bei einem Bankdirektor in Hongkong bewirkt, dass dieser 35 Millionen US-Dollar an Cyber-Kriminelle überwies. Im Berichtszeitraum wurde beobachtet, dass durch die vermehrte Echtzeitfähigkeit der Manipulationsmethoden und deren Qualität die Gefährdungslage weiter zunimmt. Damit sind Fälschungen schwieriger zu detektieren. [5, S. 64–65]

Das Kapitel Wirtschaft geht zunächst auf allgemeine Erkenntnisse zur Gefährdungslage in der Wirtschaft ein. Als Hauptbedrohung werden Ransomware-Angriffe genannt. Allgemein ist die zentrale

Herausforderung für Unternehmen in Deutschland die Steigerung der Cyber-Resilienz. Damit ist die Kombination einer guten Präventionsarbeit zusammen mit der Möglichkeit, gut auf Angriffe zu reagieren und damit den Betrieb des Unternehmens zu sichern, gemeint. [5, S. 67] Insbesondere KRITIS sind auf einen störungsfreien Betrieb angewiesen. Eine besonders gefährliche Entwicklung der letzten Jahre sind beobachtete Angriffe auf Software-Lieferketten. KRITIS-Betreiber stehen in der Pflicht, aller zwei Jahre nachzuweisen, dass die IT auf dem neuesten und sichersten Stand ist. Im Zwei-Jahres-Zeitraum vom 01. April 2020 bis zum 31. März 2022 wurden 2941 Sicherheitsmängel festgestellt. [5, S. 66–70]
In Hinblick auf die Sicherheit von Cloud-Diensten sind 2021 einige größere Sicherheitsvorfälle zu nennen. In diesem Bereich ist eine intensive Überwachung der Aktivitäten, um die Kosten genau abzurechnen, etabliert, sodass Vorfälle schnell detektiert werden können. Beispielsweise kam es zur Manipulation eines Cloud-Dienstes, sodass Ransomware auf den Kundensystemen installiert wurde. Bei einem weiteren Vorfall wurden durch einen Brand bei einem Cloud-Anbieter Anfang des Jahres 2021 ganze Rechenzentren und damit auch Kundendaten zerstört. Allgemein ist festzustellen, dass Kunden die Risiken von geteilten Plattformen abwägen sollten und dabei die Sensibilität der Daten beachten und zusätzliche Schutzmaßnahmen wie Verschlüsselung in Betracht ziehen sollten. [5, S. 78–79]
Der Abschnitt Staat und Verwaltung fokussiert besonders die Gefährdungslage der Bundesverwaltung, weil die Abwehr von Cyber-Angriffen auf Regierungsnetze und Bundesverwaltung die Kernaufgabe des BSI darstellt. Die detektierten Angriffe sind eine Mischung aus ungezielten Massenangriffen und gezielten Angriffen gegen Bundesbehörden. Die Angriffe erfolgten dabei überwiegend mittels Schadprogrammen. Diese wurden über E-Mail-Anhänge, Download-Links in E-Mails, Social-Media-Accounts und andere Webseiten verbreitet und die Empfänger mittels Social-Engineering zur Installation verleitet. Als Maßnahmen dagegen setzt das BSI Webfilter ein, um zentral den Zugriff aus der Bundesverwaltung zu sperren. [23, S. 69–70]
Beim Thema der aktuellen Trends und Entwicklungen in der IT-Sicherheit im Bereich der Künstlichen Intelligenz (KI) wird diese als Zukunftstechnologie mit Chancen sowie Risiken als mögliches Angriffswerkzeug dargestellt. Als Risiko erweist sich die Manipulation von Medien beispielsweise für Fake News. Momentan lassen sich diese noch gut an Artefakten erkennen, doch in Zukunft wird sich die Technologie weiter verbessern. Im Bereich der Kryptografie ist eine Gefährdung der Sicherheit durch Quantencomputer vorstellbar. Aktuelle Sicherheitsmaßnahmen basieren zu großen Teilen auf dem klassischen weit verbreiteten Public-Key-Verfahren. Daher gestaltet sich die Post-Quanten-Kryptografie als notwendig. [5, S. 96–97]

3.3 Cyber Security Report 2021 Deutschland

Deloitte, ein internationales Unternehmen in der Wirtschaftsbranche, führte zusammen mit dem Institut für Demoskopie Allensbach eine repräsentative Trendstudie mit führenden Akteuren aus Politik und Wirtschaft durch. Dafür wurden 404 Führungskräfte aus Unternehmen und 104 Abgeordnete aus Landtag, Bundestag und Europaparlament zu ihrer Sichtweise zum Thema Cyber-Security befragt. Damit stellt dieser Bericht eine Einschätzung aus politischer und wirtschaftlicher Sicht dar. Der Bericht wurde im August 2021 veröffentlicht. [28]
Das für diese Arbeit interessante Thema der Studie ist eine Aufstellung der größten Cyber-Risiken für Menschen in Deutschland 2021. Wie in Abbildung 3.10 zu erkennen ist, liegen die größten Ri-

siken in diesem Jahr sehr nah beieinander: Datenbetrug im Internet (77 %), Computerviren oder Schadsoftware (76 %) und Fake News (75 %). [28, S. 6–7]

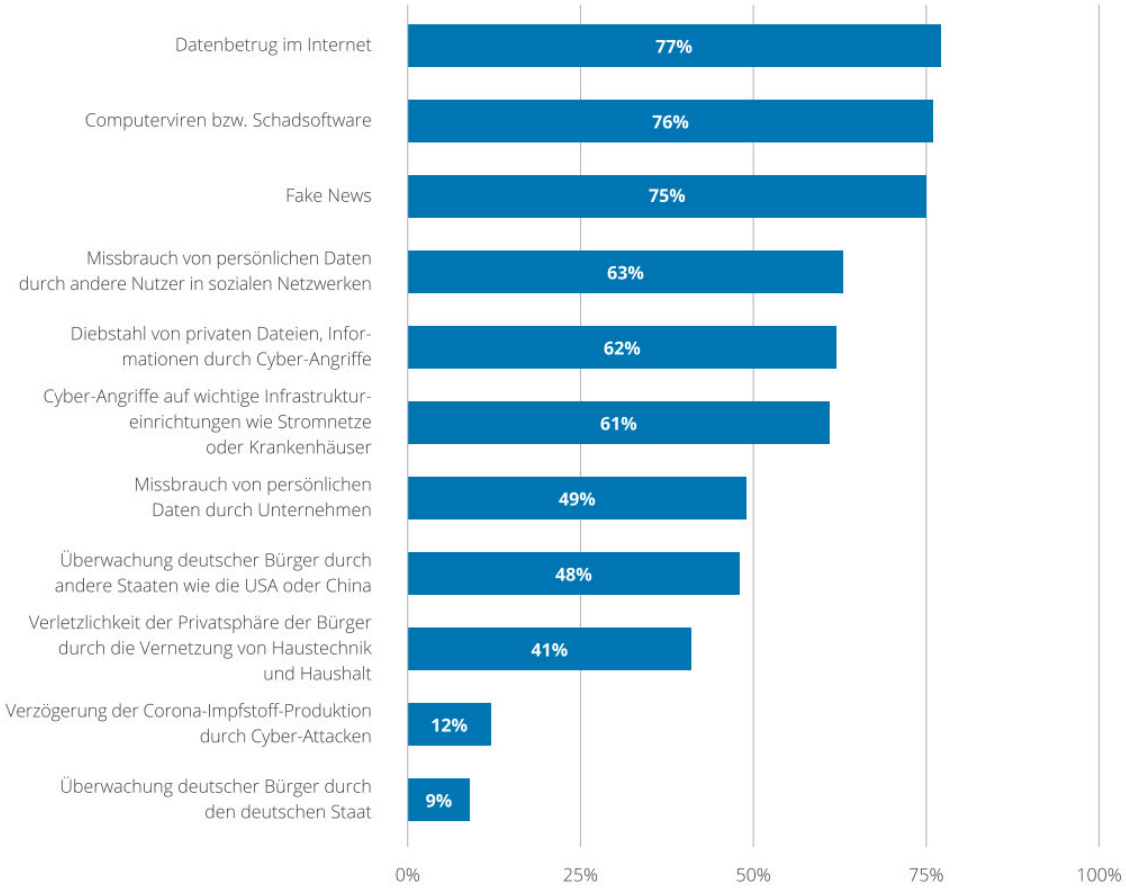


Abbildung 3.10: Die größten Cyber-Risiken für die Menschen in Deutschland 2021 [28, S. 7]

Die weiteren Inhalte des Berichts sind für diese Arbeit nicht von Bedeutung.

3.4 Wirtschaftsschutz 2022

Diese durch den Digitalverband Bitkom beauftragte und von Bitkom Research durchgeführte computergestützte telefonische Befragung fand von Januar bis März 2022 statt. Befragt wurden 1066 Unternehmen verschiedener Branchen in Deutschland, die die Mindestanforderungen von zehn Beschäftigten und einem Jahresumsatz von 1 Mio. Euro erfüllten. Die Umfrage ist repräsentativ für die Gesamtwirtschaft. Veröffentlicht wurden die Ergebnisse in Form einer Präsentation mit verschiedenen grafischen Darstellungen der Untersuchungsergebnisse am 31. August 2022.
Thematisch beschäftigt sich die Umfrage damit, ob Unternehmen bereits von Cyber-Attacken betroffen waren und welche Angriffsarten dabei eingesetzt wurden. Zudem werden die dadurch entstandenen Schäden sowie die hinter den Angriffen vermuteten Täter beleuchtet. Zusätzlich liefert der Bericht einen Ausblick auf die Zukunft: es wird betrachtet, welche Bedrohungen Unternehmen zunehmend sehen und welche Maßnahmen und Hilfen von der Politik gewünscht werden. [29]
Den Beginn der Umfrage bildet die Frage, ob das Unternehmen innerhalb der letzten zwölf Monate

von Angriffen wie Diebstahl, Industriespionage oder Sabotage betroffen war. Der Anstieg der Betroffenen von 2017 mit 53 % zu 2019 mit 75 % ist mit 22 Prozentpunkten stark ausgeprägt. Weniger stark ist er bei der Betrachtung der Differenz auf 2021 mit 88 % und danach ist der Anstieg sogar rückläufig auf 84 % 2022. Die Zahl der, laut eigenen Angaben, vermutlich Betroffenen ist ebenso rückläufig. Insgesamt nimmt die Zahl der Betroffenen also ab. [29, S. 2]
Die zweite Frage beschäftigt sich in Abbildung 3.11 mit der Unterscheidung der Angriffsarten, besonders zwischen digitalen und analogen Angriffen. Dabei ist festzustellen, dass Angriffe zunehmend digital stattfinden. Angriffe der Kategorie digital weisen eine Zunahme von jeweils mindestens drei Prozentpunkten und analoge Angriffe eine Abnahme von jeweils mindestens drei Prozentpunkten auf. [29, S. 3]

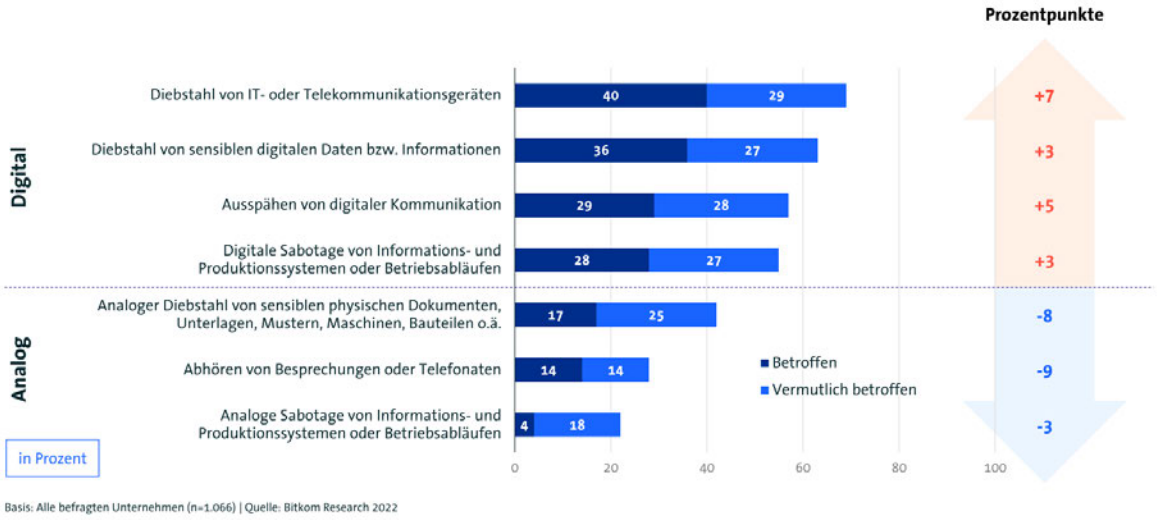


Abbildung 3.11: Angriffe im analogen und digitalen Raum [29, S. 3]

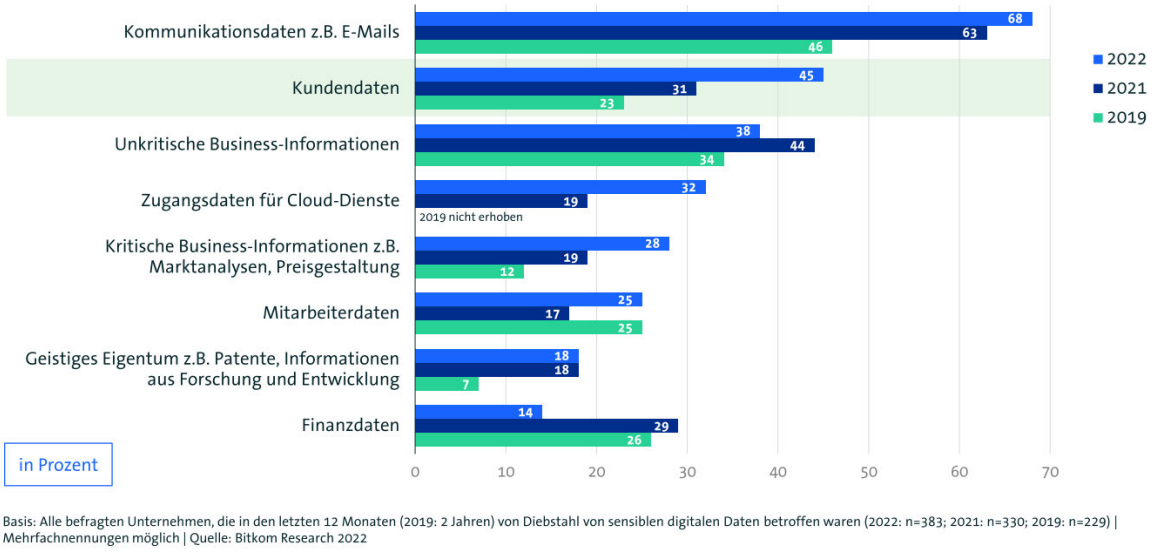


Abbildung 3.12: Datendiebstahl [29, S. 4]

Die Kategorie Datendiebstahl wird in der nächsten Frage in Abbildung 3.12 genauer beleuchtet. Dabei geht es darum, welche digitalen Daten gestohlen wurden. Die Angaben beziehen sich auf die befragten Unternehmen, die angaben, von Datendiebstahl in den letzten zwölf Monaten betroffen gewesen zu sein. Am häufigsten kam es mit 68 % zum Diebstahl von Kommunikationsdaten und auf Platz zwei befinden sich Kundendaten mit 45 %. Im Vergleich mit den Vorjahresbefragungen zeigt sich, dass Kommunikationsdaten immer das häufigste Ziel darstellten, jedoch die Reihenfolge der anderen Datenarten fluktuiert. Besonders sticht hier die Entwicklung der Finanzdaten hervor. Diese sind vom dritten Platz 2019 auf den letzten Platz 2022 gesunken. [29, S. 4]
Der Frage, ob Cyberattacken die Existenz der Unternehmen bedrohen, stimmen zwei Prozent und 2022 sogar 45 % zu. [29, S. 5]
Im Bereich der Bewertung, wie sich Cyberangriffe im letzten Jahr verändert haben, geben lediglich 14 % der Befragten unverändert an. Der Großteil stimmt für eher zugenommen mit 45 % und stark zugenommen mit 39 %. Unter Berücksichtigung der Zugehörigkeit zu KRITIS-Sektoren zeigt sich, dass besonders in diesem Sektor eine stark zugenommene Bedrohung wahrgenommen wird. [29, S. 6]
Bei der genaueren Untersuchung der stattgefundenen Angriffe auf Unternehmen innerhalb der letzten zwölf Monate in Abbildung 3.13 wird deutlich, dass diese teilweise stark anders als im Vorjahr ausgeprägt sind. Angriffe auf Passwörter, Phishing und Infizierung mit Schadsoftware oder Malware befinden sich mit jeweils 25 % auf Platz eins. Im Vergleich zum Vorjahr ist festzustellen, dass Angriffe auf Passwörter, Phishing, Cross-Site-Scripting und Man-in-the-middle-Angriffe jeweils um mindestens fünf Prozentpunkte zugenommen haben, während Schadsoftwareinfizierungen, DDoS-Angriffe, Spoofing, Ransomware und SQL-Injektion abnahmen. [29, S. 7]

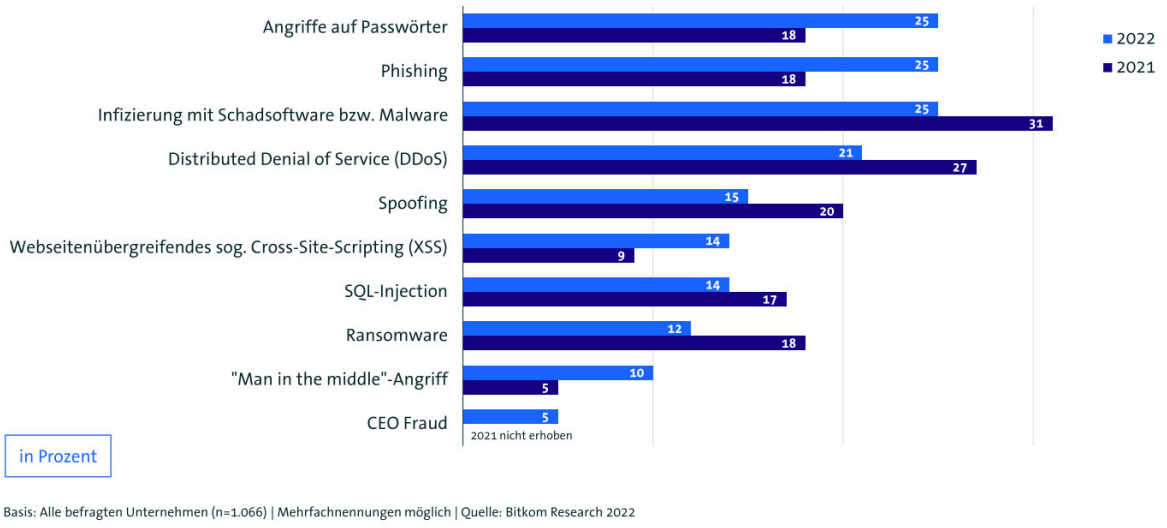


Abbildung 3.13: Stattgefundene Angriffe [29, S. 7]

Eine genauere Betrachtung der Kommunikationswege bei Social-Engineering zeigt, dass ein großer Teil der Angriffe mit 38 % über das Telefon erfolgte, dicht gefolgt von Kommunikation per E-Mail mit 34 %. Mit größerem Abstand folgt mit 13 % Kommunikation im privaten Umfeld. Dahinter folgen mit jeweils unter 10 % berufliche Netzwerke (9 %), private soziale Netzwerke (5 %), Videokonferenzen (4 %) und Kommunikationsversuche auf Messen und anderen Veranstaltungen (3 %). [29, S. 8]
Bei der Schadensbetrachtung summiert sich ein Gesamtschaden von 202,7 Milliarden Euro pro Jahr. Eine Aufschlüsselung der Schäden ist in Abbildung 3.14 zu sehen. Am meisten Schaden entstand

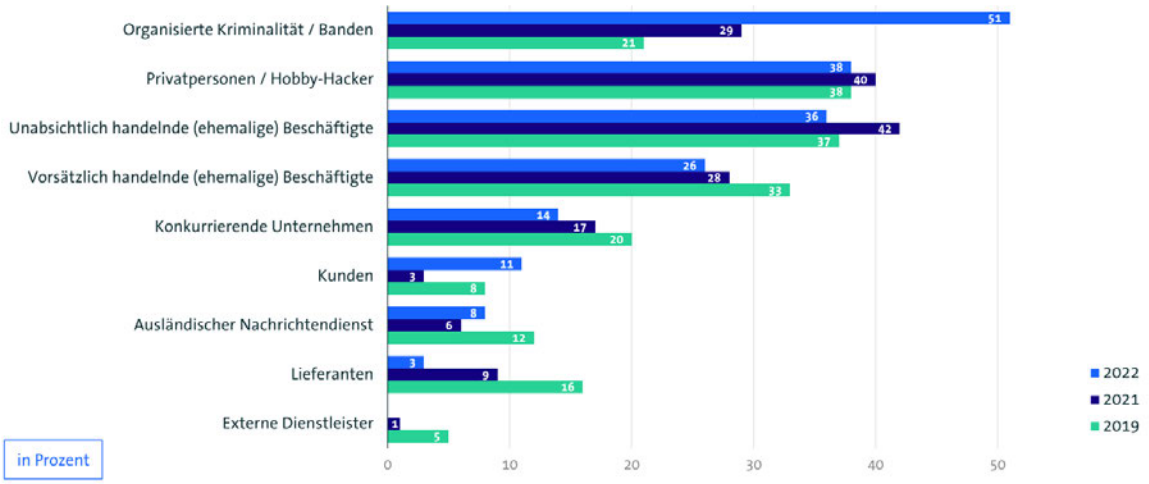
durch den Ausfall, Diebstahl oder Schädigung von Betriebsabläufen oder Systemen für die Produktion (20 %) und durch Umsatzeinbußen als Folge vom Verlust von Wettbewerbsvorteilen (20 %). Negative Medienberichterstattung und damit einhergehender Imageschaden machten 11 % und Umsatzeinbußen durch nachgemachte Produkte 10 % der Schäden aus. Erpressungen mit gestohlenen oder verschlüsselten Daten bewirkten fünf Prozent der Gesamtschadenssumme. [29, S. 9]

Schaden durch...	Schadenssummen in Mrd. Euro (2022)	Schadenssummen in Mrd. Euro (2021)	Schadenssummen in Mrd. Euro (2019)	Schadenssummen in Mrd. Euro (2017)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	41,5	61,9	13,5	5,3
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	10,7	24,3	5,3	0,7
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	18,3	17,1	4,4	3,2
Patentrechtsverletzungen (auch schon vor der Anmeldung)	18,8	30,5	14,3	7,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	41,5	29	11,1	8,6
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	21,1	22,7	11,1	3,5
Imageschaden bei Kunden oder Lieferanten/ Negative Medienberichterstattung	23,6	12,3	9,3	7,7
Kosten für Ermittlungen und Ersatzmaßnahmen	10,1	13,3	18,3	10,6
Kosten für Rechtsstreitigkeiten	16,2	12,4	15,6	5,5
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-	-	-	2,2
Sonstige Schäden	0,9	0	<0,1	<0,1
Gesamtschaden pro Jahr	202,7	223,5	102,9	54,8

Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019 und 2017: 2 Jahren) von Diebstahl von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935; 2019: n=801; 2017: n=571) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

Abbildung 3.14: Entstandene Schäden [29, S. 9]

Den Ursprung der Angriffe geben 35 % der befragten Unternehmen, die in den letzten zwölf Monaten von Angriffen betroffen waren, als unklar an. Im Vergleich der Ursprungsländer steht China mit 43 % an erster Stelle. Russland mit 36 % wird dicht gefolgt von Deutschland mit 32 %. Zusammengefasst machten osteuropäische Länder ohne Russland 27 % aus, die USA 21 % und EU-Länder ausgenommen Deutschland acht Prozent. Damit verzeichnen alle Gebiete Anstiege, mit den Ausnahmen von Deutschland und Osteuropa. Besonders Russland und China zeichnen sich durch einen großen Anstieg von jeweils 13 Prozentpunkten aus. [29, S. 10]



Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019: 2 Jahren) von Diebstahl von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935; 2019: n=801) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

Abbildung 3.15: Täterkreise [29, S. 11]

Bei der Untersuchung des Täterkreises in Abbildung 3.15 zeigen sich deutliche Steigerungen in den einzelnen Gruppierungen. Den größten Anstieg im Vergleich zum Vorjahr und damit auch die größte Bedrohung weist organisierte Kriminalität mit nun 51 % auf. Danach reihen sich die bisherigen größten Bedrohungen ein: 38 % Privatpersonen bzw. Hobby-Hacker und 36 % unabsichtlich handelnde Beschäftigte. [29, S. 11]
Die Prognosen der Befragten für die Zukunft fallen eher düster aus. Insgesamt erwarten 42 % eine starke Zunahme der Cyber-Attacken. 36 % stimmen eher der Zunahme zu und lediglich 18 % erwarten eine gleichbleibende Entwicklung. Besonders KRITIS-Sektoren rechnen zu 51 % mit einer stärkeren Zunahme und nur zu 10 % mit einem gleichbleibenden Stand. Hingegen vermuten nur 40 % der Nicht-KRITIS-Sektoren einen starken Anstieg und sogar 20 % mutmaßen mit einer gleichbleibenden Entwicklung. [29, S. 12]
Damit gehen steigende Investitionen in IT-Sicherheit einher. Der Anteil des Budgets für IT-Sicherheit macht am gesamten IT-Budget des Unternehmens durchschnittlich neun Prozent aus. Damit steigt dieser Wert um 2 Prozentpunkte im Vergleich zum Vorjahr. Wie Abbildung 3.16 darstellt, investieren 38 % der Unternehmen fünf bis zehn Prozent. [29, S. 13]

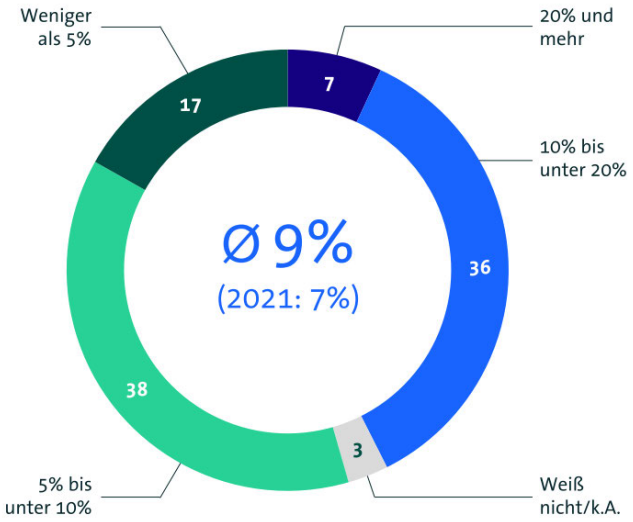


Abbildung 3.16: Investitionen in IT-Sicherheit [29, S. 13]

Bei der Bewertung der zukünftigen Bedrohungen in Abbildung 3.17 sieht mehr als die Hälfte (59 %) Ransomware-Angriffe als sehr bedrohlich. Insgesamt wird diese Angriffsart von 92 % als bedrohlich eingeschätzt. Danach folgen, nach der Bedrohlichkeit sortiert, die Angriffsarten Zero-Day-Exploit (91 %), Spyware (85 %) und Backdoors (73 %). Das geringste Risiko wird im Anzapfen von Rechenleistung, beispielsweise zum heimlichen Schürfen von Kryptowährungen, mit 47 % gesehen. [29, S. 14]

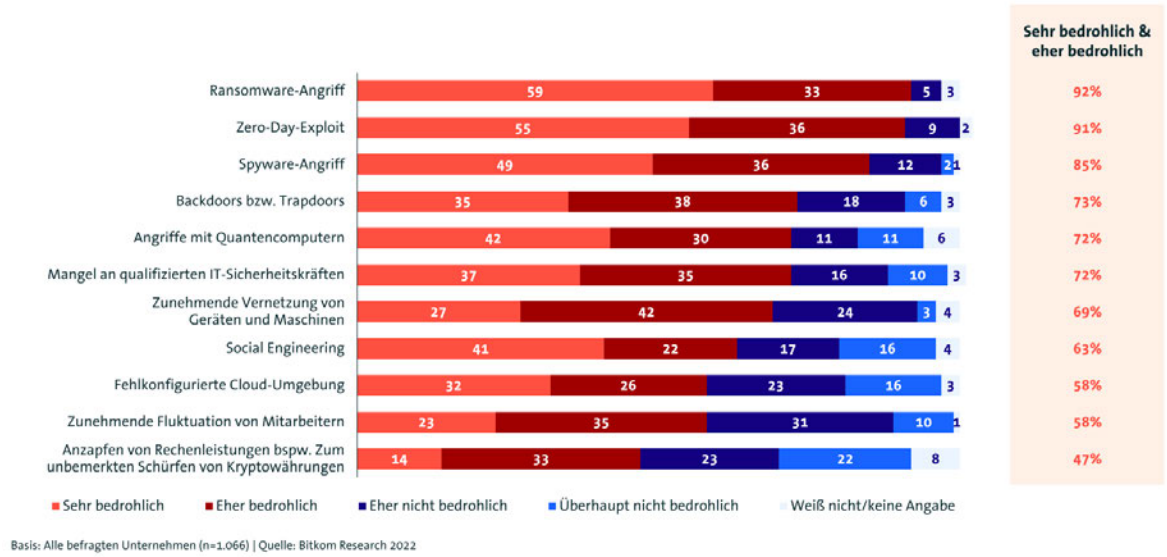


Abbildung 3.17: Prognose zukünftiger Bedrohungen [29, S. 14]

Der letzten Teil der Befragung beschäftigt sich mit gewünschten politischen Maßnahmen zum Wirtschaftsschutz. 98 % Zustimmung erfährt der Wunsch, dass die Politik sich mehr um eine EU-weite Zusammenarbeit im Bereich der Cybersicherheit einsetzen sollte. Außerdem stimmen 97 % dafür, dass die Politik auch verstärkt gegen Cyberattacken aus dem Ausland vorgehen sollte. Lediglich 77 % befürworten erweiterte Ermittlungsbefugnisse um Cyberangriffe aufzuklären. Weiterhin vertreten 77 % der Befragten die Meinung, dass der bürokratische Aufwand zur Meldung von Vorfällen zu hoch ist. [29, S. 15]

3.5 eco Umfrage Internetsicherheit 2022

Eco, der Verband der Internetwirtschaft, veröffentlicht jährlich eine Umfrage zur IT-Sicherheit. Durchgeführt wurde die Umfrage gegen Ende des Jahres 2021 und die Ergebnisse erschienen am 17. Februar 2022. Es wurden 145 Experten aus verschiedenen Branchen befragt. Darunter sind verschiedene Unternehmensgrößen vertreten.
Neben der Betroffenheit durch Cyber-Angriffe und deren Schäden wird eine Einschätzung der aktuelle Bedrohungslage, der Tätergruppen und die Bedeutung von Sicherheitsmaßnahmen sowie vermutete Trends für die Zukunft beleuchtet. [30]
Die Umfrage beginnt mit einer Einschätzung der Bedrohungslage im Bezug auf die Internet-Sicherheit. 93,8 % schätzen diese als mindestens wachsend ein. Damit zeigt sich eine deutliche Steigerung gegenüber dem Vorjahr mit 77,4 %. [30, S. 4]
Die Lage der deutschen Wirtschaft gegenüber Cybercrime wird im Allgemeinen als unzureichend aufgestellt eingeschätzt (71 %). Hingegen sieht diese Einschätzung im eigenen Unternehmen deutlich anders aus. Dort sehen nur 12,4 % unzureichende Maßnahmen. [30, S. 5]
Auf die Frage, ob es im Unternehmen im vergangenen Jahr mindestens einen gravierenden Sicherheitsvorfall gab, antworten 17 % mit ja. Dieser Prozentwert ist gering weniger als im Vorjahr mit 20 %. [30, S. 6]
Die Unterscheidung dieser Angriffe nach ihrer Art zeigt, dass Ransomware an erster Stelle steht, dicht gefolgt von Webseiten-Hacking, Datendiebstahl und DDoS-Angriffen. An letzter Stelle befindet sich Wirtschaftsspionage. [30, S. 7] Bei der Betrachtung aller bisherigen Sicherheitsvorfälle in

Abbildung 3.18 ist festzustellen, dass Ransomware die größte Bedrohung bleibt, allerdings weniger signifikant ist als im Vorjahr. Alle weiteren Angriffsarten sind im Vergleich zum Vorjahr auf ähnlichem Niveau geblieben oder angestiegen. Der größte Anstieg ist beim Datendiebstahl zu verzeichnen. [30, S. 10]

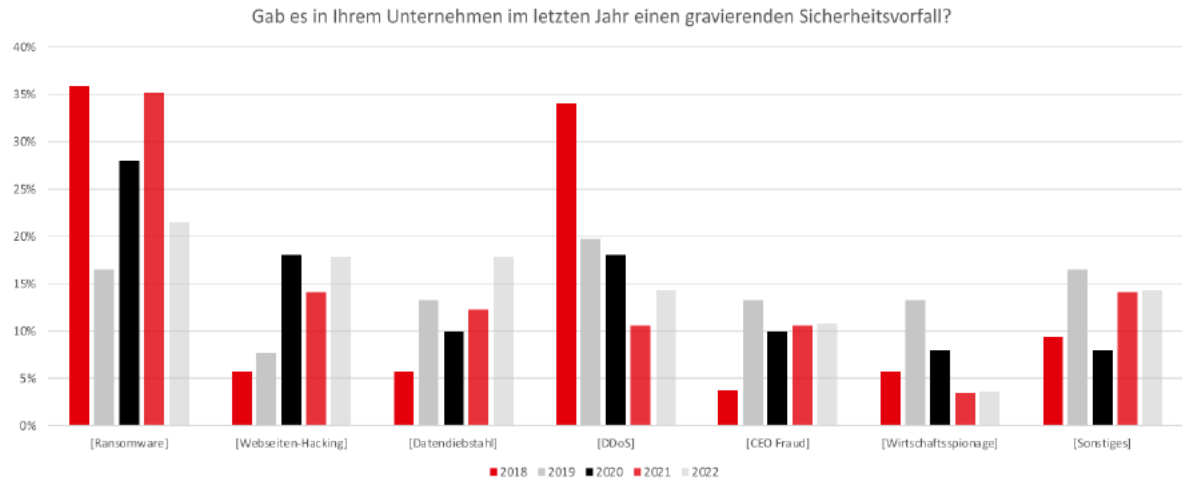


Abbildung 3.18: Sicherheitsvorfälle in den vergangenen Jahren [30, S. 10]

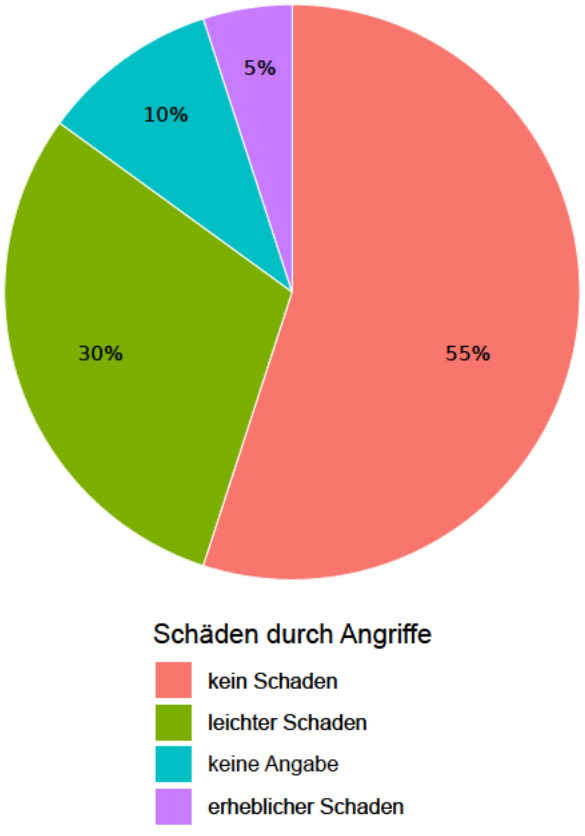


Abbildung 3.19: Entstandene Schäden, basierend auf Daten der Umfrage von eco 2022 [30, S. 8]

Als Reaktion auf Sicherheitsvorfälle wurden die entstandenen Probleme meist intern gelöst. In einigen Fällen wurde externe Hilfe in Anspruch genommen und in noch weniger Fällen erfolgten Informationen an die Kunden und Einschaltung der Strafverfolgung. [30, S. 7]
Die entstandenen Schäden nach Angriffen sind in Abbildung 3.19 dargestellt. Für einen geringen Teil (5 %) entstand nach den Vorfällen erheblicher wirtschaftlicher Schaden und für etwa 30 % folgte ein leichter Schaden. Mehr als die Hälfte (55 %) gab an, keinen Schaden erlitten zu haben. In unter 10 % fing eine Cyberversicherung den Schaden zumindest teilweise auf. [30, S. 8]
Im Vergleich zum Vorjahr sind die Schäden eher gleichbleibend (37 %). Für acht Prozent ist das Schadensniveau etwas angestiegen und für drei Prozent sehr stark gestiegen. Hingegen sagen drei Prozent, die Schäden haben sich stark verringert und vier Prozent sind der Meinung, die Schäden sind eher weniger geworden. Doch die Ausgaben für IT-Sicherheit haben sich im letzten Jahr bei 44 % der Befragten leicht erhöht, wie in Abbildung 3.20 zu sehen ist. [30, S. 9]

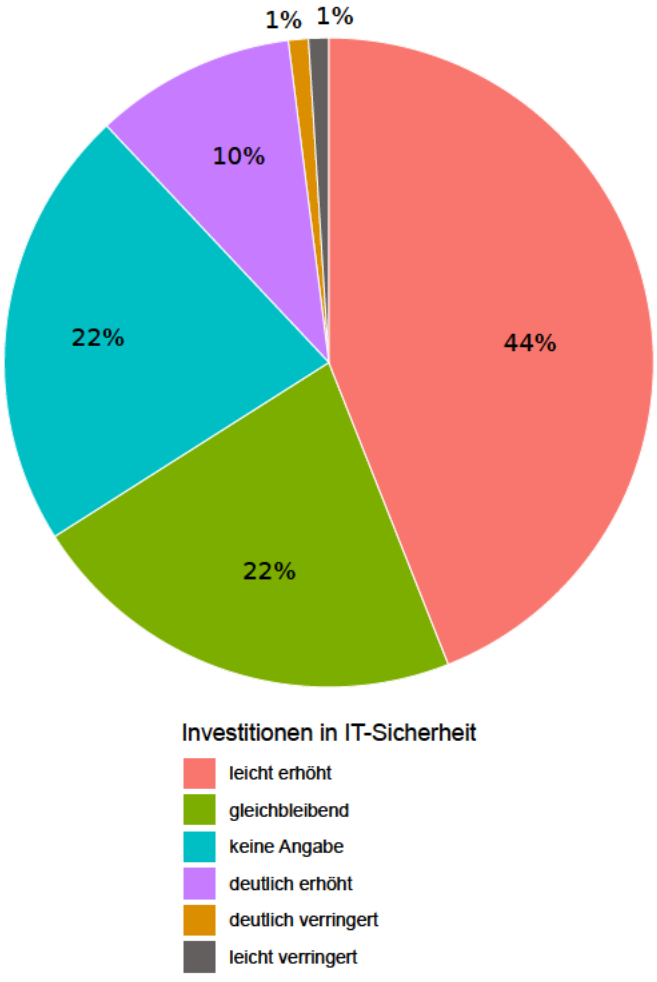


Abbildung 3.20: Investitionen in IT-Sicherheit, basierend auf Daten der Umfrage von eco 2022 [30, S. 9]

Beim Thema Tätergruppen stehen profitgetriebene Cyberkriminelle (83 %) an erster Stelle. Aber auch unbeabsichtigte Innentäter (50 %), sogenannte Cyber-Unfälle, machen eine großen Teil aus. Weniger häufig sind internationale Wirtschaftsspionage (25 %) und absichtliche Innentäter (18 %). [30, S. 11]

Weiterhin wird das Thema beleuchtet, inwieweit sich die Sicherheitslage durch die Corona-Pandemie verändert hat. 80 % sehen eine Verschärfung der Sicherheitslage. Allerdings nehmen nur 16 % in ihrem Unternehmen mehr erfolgreiche Angriffe durch das vermehrt stattfindende Home-Office wahr. [30, S. 12]
Im Bereich der Bedeutung von Sicherheitsthemen zeigt Abbildung 3.21 deutlich, dass Mitarbeitersensibilisierung mit 51 % „sehr wichtig“ eine vergleichsweise hohe Priorität hat. [30, S. 13]

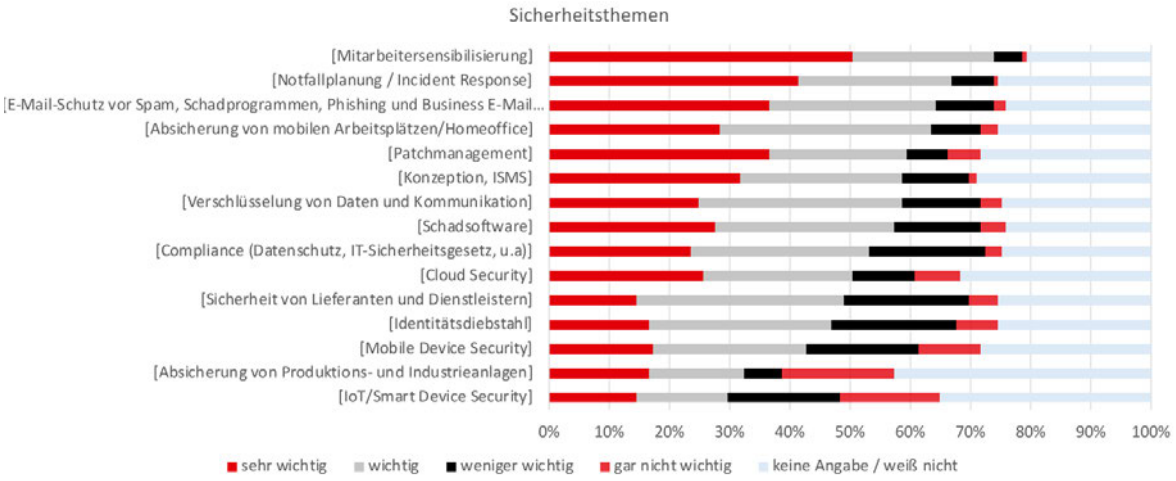


Abbildung 3.21: Bedeutung von Sicherheitsthemen [30, S. 13]

Bezüglich der Vorsorge von Angriffe stimmen 63 % der Befragten zu, dass ihr Unternehmen mit einen Notfallplan oder anderen internen Prozessen auf mögliche Cyber-Angriffe vorbereitet ist. In Planung sind weitere 24 %. Regelmäßige Mitarbeiterschulungen und Sensibilisierungen führen 62 % der Befragten durch, 35 % tun dies unregelmäßig und nur drei Prozent gar nicht. [30, S. 14]
Bei der Einschätzung der stärksten Veränderungstreiber hinsichtlich der nächsten fünf Jahre zeigt sich, dass dem Anstieg von Cyberkriminalität eine große Bedeutung beigemessen wird. Als weitere starke Einflussfaktoren stimmen die Befragten für vernetzte KRITIS und Cloud-Computing. [30, S. 15]

3.6 Deutschland sicher im Netz (DsiN)-Praxisreport 2021/22 Mittelstand@IT-Sicherheit

Deutschland sicher im Netz (DsiN) ist ein gemeinnütziger Verein mit Sitz in Berlin unter der Schirmherrschaft des Bundesministeriums des Inneren und für Heimat (BMI). [31]
Datengrundlage des Praxisreports bildet die Erhebung des DsiN-Sicherheitschecks von Mitarbeitenden und Führungskräften aus dem Mittelstand. Der Sicherheitscheck ist ein Onlinetest zur Ermittlung des IT-Sicherheitsniveaus in kleineren und mittleren Unternehmen (KMU). Zusätzlich bietet dieser Test Empfehlungen für zu ergreifende Maßnahmen und weiterführende Informationen. [32]
Für den Bericht werden Befragungen aus 24 Themenfeldern in regelmäßigen Abständen ausgewertet. In diesem, aufgrund der Corona-Pandemie verlängerten, Befragungszeitraum von Mai 2020 bis Januar 2022 entstanden 1339 vollständig ausgefüllte Fragebögen. Darunter sind verschiedene Unternehmensgrößen und Branchen vertreten. [31]
Inhaltlich geht es im Praxisreport darum, wie abhängig Unternehmen von funktionierender IT-Sicherheit

sind und inwiefern Sicherheitsmaßnahmen zum Schutz eingesetzt werden. Außerdem werden die personellen Zuständigkeiten für IT-Sicherheit innerhalb der Unternehmen und der Umgang mit Angriffen beleuchtet. [31]
Das erste Kapitel beschäftigt sich mit dem Thema IT-Sicherheitsbedarfe und Vorkehrungen.
In der ersten Frage geht es um das grundlegende Thema, ob der Erfolg des Unternehmens von der IT-Sicherheit abhängt. Für fast die Hälfte der Befragten hängt das unmittelbar zusammen (49 %). 37 % sagen, der Schutz sei wichtig, aber nicht essenziell. Für jeweils sieben Prozent sind Integrität, Vertraulichkeit und Verfügbarkeit von Informationen nicht wichtig und die Betriebsabläufe sind weitgehend nicht darauf angewiesen. Den direkten Zusammenhang zwischen wirtschaftlichem Wohlergehen und IT-Sicherheit sehen besonders KMU mit unter zehn Beschäftigten (33 %). Es ist festzustellen, dass größere Unternehmen diese Abhängigkeit weniger stark fühlen. Als Grund dafür werden stärkere Resilienzen dieser Unternehmen gesehen. Bei KMU hingegen wirken sich Störungen unmittelbar aus. Bei der Betrachtung der Branchenzugehörigkeit in dieser Frage wird deutlich, dass insbesondere die Dienstleistungsbranche den Zusammenhang sieht (29 %), weil diese während der Pandemie ihr Angebot verstärkt in den digitalen Raum ausweitete. [31, S. 8]
Die Frage nach einer Gefährdung, insbesondere der Vertraulichkeit und Integrität der IT-gestützten Informationen, durch Angriffe anderer Unternehmen zeigt einen geringen Wert dieser Informationen für die Konkurrenz (35 %). 32 % sehen das Interesse der ausländischen Konkurrenten als unkritisch. Hingegen meinen 21 % der Befragten, die Wettbewerbsfähigkeit des Unternehmens und 11 % die Unternehmensexistenz hängt unmittelbar davon ab. [31, S. 8–9]

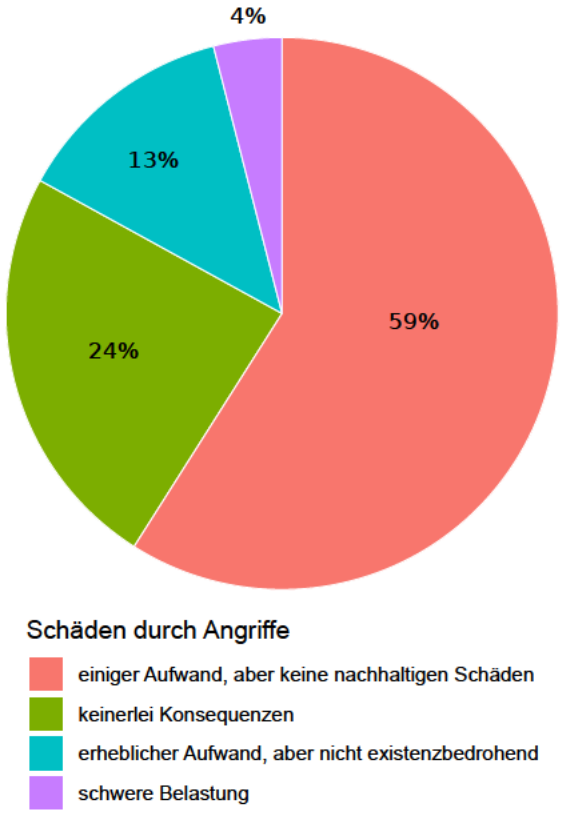


Abbildung 3.22: entstandene Schäden, basierend auf Daten des DsiN-Praxisreports [31, S. 11]

27 % der Unternehmen hatten in den vergangenen Jahren einige Probleme durch Schadsoftware. 10 % waren mindestens einmal Oper eines gezielten Angriffs und fünf Prozent kämpften sogar ständig mit Angriffen. Hingegen waren mehr als die Hälfte noch nie von Angriffen betroffen (58 %). [31, S. 10]
Die Betrachtung der verursachten Schäden zeigt ein eher geringes Schadenspotenzial. Eine Darstellung ist in Abbildung 3.22 zu sehen. Für 24 % hatten Angriffe keinerlei Konsequenzen und 59 % geben an, einigen Aufwand, aber keine nachhaltigen Schäden gehabt zu haben. Der Aufwand zur Behebung angriffsverursachender Schäden war für 13 % erheblich, aber nicht existenzbedrohend. Für lediglich vier Prozent folgten schwere Belastungen. Mit Blick auf die Branche zeigen sich deutliche Unterschiede im Anteil der erheblichen oder existenzbedrohenden Vorfälle. Im Gastgewerbe bewirkte die Hälfte aller Angriffe derartige Schäden. Im Handel beträgt der Anteil 21 %. Noch geringere Anteile sind in der Industrie mit 14 % und der Gesundheitsbranche mit 11 % zu verzeichnen. [31, S. 11]
Die Ermittlung von Risikosituationen wird von Unternehmen nicht ausreichend berücksichtigt. 37 % verzichten auf diesen Sicherheitsaspekt und 29 % ermittelten Risikofaktoren in einer einmaligen Bestandsaufnahmen und beziehen sich darauf. 18 % ermitteln einmal jährlich die konkrete Risikosituation und kontinuierliche Risikoermittlungen führen 16 % durch. [31, S. 11–12]
Das zweite Kapitel umfasst die Sicherheitskultur in den Unternehmen.
Im Bereich der personellen Sicherheitsmaßnahmen zeigt sich, dass in 35 % der befragten Unternehmen die Geschäftsleitung allein für IT-Sicherheit verantwortlich ist. In 27 % der Unternehmen wird diese durch Informationssicherheitsbeauftragte unterstützt. In fast jedem vierten Unternehmen (23 %) sind die Mitarbeitenden für sich selbst verantwortlich und 15 % beauftragen eine Person extra dafür. [31, S. 16] Bei der Betrachtung des Anteils der Beschäftigten, die unmittelbar für IT-Sicherheit zuständig sind, ist auffällig, dass dieser Anteil mit steigender Beschäftigtenzahl abnimmt. In Unternehmen mit weniger als zehn Beschäftigten beträgt dieser Anteil 45 %, in Unternehmen mit 200 bis 500 Beschäftigten lediglich sechs Prozent. Dieser Zusammenhang besteht außerdem bei der Anzahl der Unternehmen, in denen die Geschäftsleitung für die IT-Sicherheit zuständig ist. In jedem zweiten kleinen Unternehmen mit weniger als zehn Beschäftigten ist die Geschäftsleitung dafür zuständig. Bei der Umsetzung von Awareness-Trainings sollte dieser Zustand berücksichtigt werden. Dabei sollte eine Priorisierung der Leitungsebene für kleine Unternehmen erfolgen. [31, S. 17] Damit geht auch einher, dass in jedem zweiten Unternehmen die Geschäftsleitung über den konkreten Risikoumgang entscheidet. In 34 % der Unternehmen sind dafür die IT-Abteilung oder externe IT-Dienstleister zuständig, in 10 % Leitungspersonen der Abteilungen und in fünf Prozent die Beschäftigten selbst. [31, S. 18] Ähnlich zur Situation, dass in kleineren Unternehmen häufiger die Geschäftsleitung selbst für IT-Sicherheit zuständig ist, verhält sich auch die Entscheidungsgewalt der Geschäftsführung in einer akuten Bedrohungslage. Je größer ein Unternehmen ist, desto weniger fällt die Geschäftsleitung diese Entscheidungen. [31, S. 18] 44 % der befragten Unternehmen sind der Meinung, dass ihre Mitarbeitenden beim Thema IT-Sicherheit ausreichend informiert sind und keine Maßnahmen notwendig sind. 34 % informieren ihre Beschäftigten gelegentlich über kostenlose Online-Schulungen und aktuelle Veröffentlichungen. Hingegen haben 16 % ein verpflichtendes Sicherheitsschulungsprogramm und sechs Prozent ein Sicherheitsschulungsprogramm, das auf verschiedene Profile der Mitarbeitenden angepasst ist, inklusive der Durchführung regelmäßiger Tests. [31, S. 19]
Auch beim Thema Umsetzung von Schutzmaßnahmen beim Versand elektronischer Nachrichten zeigt sich Aufholbedarf. Nur jedes zweite Unternehmen sichert übertragene Daten in Anhängen ab und nur 18 % nutzt E-Mail-Verschlüsselung oder elektronische Signaturen. 21 % schützen übertragene Daten mit einem Passwort und bei 12 % erfolgt Datenaustausch nur über dedizierte Austauschplattformen. [31, S. 25]

Besonders im Home-Office hat die Bedeutung von Privatnutzung firmeneigener Geräte zugenommen. 30 % der Befragten geben an, private und geschäftliche Anwendungen der IT strikt zu trennen. Jedes vierte Unternehmen billigt die Nutzung geschäftlicher Endgeräte zusätzlich für private Angelegenheiten ohne besondere Regelungen. In 22 % der Unternehmen wurde für diesen privaten als auch geschäftlichen Einsatz der Geräte Nutzungsrichtlinien festgelegt. Das Prinzip BYOD wird in 23 % der befragten Unternehmen eingesetzt. [31, S. 25]
Ein weiteres wichtiges Thema in der Kategorie Schutzmaßnahmen ist die Überprüfung von deren Wirksamkeit. IT-Sicherheit ist ein kontinuierlicher Prozess und sollte an Veränderungen angepasst werden. Jedes dritte Unternehmen setzt zwar Schutzmaßnahmen ein, überprüft deren Wirksamkeit jedoch nicht. 22 % der Unternehmen setzen keine speziellen Schutzmaßnahmen ein. In 27 % der Unternehmen wird die Wirksamkeit erst im Verdachtsfall überprüft. Immerhin 19 % überprüfen die eingesetzten Schutzmaßnahmen regelmäßig. [31, S. 26] Ähnlich sieht es im Bereich der Angriffserkennung aus. 32 % sind der Meinung, nicht von Angriffen betroffen zu sein oder diese nicht zu erkennen. Ebenso viele Unternehmen überlassen den Mitarbeitenden die Angriffserkennung. Spezialisierte Dienstleistende dafür haben 15 % beauftragt und 21 % verfügen zudem über Sensoren in der Infrastruktur, um Anzeichen zu erkennen und diese an Spezialisten zu übermitteln. [31, S. 26]
Weiterhin gehört zu diesem Thema der Umgang mit Schwachstellen in Standardsoftware. 17 % der Befragten wissen nichts über mögliche Schwachstellen in eingesetzter Software. Auf Hinweise der Hersteller oder der Presse reagieren 26 % unmittelbar mit Softwarepatches und Updates. Regelmäßige und sofortige Updates und Patches nutzen nahezu die Hälfte der Unternehmen. Acht Prozent beziehen Informationen zu diesem Thema von einem Informationsdienst und befolgen dessen Empfehlungen. [31, S. 27] Auf mögliche Angriffe reagieren Unternehmen unterschiedlich. 34 % sind zunächst mit der Entwicklung geeigneter Maßnahmen und deren Umsetzung beschäftigt. 44 % der Unternehmen legen die Verantwortung in die Hand der Mitarbeitenden, da diese entsprechend instruiert sind. In 11 % der Unternehmen kommen digitale Ersthelfende zum Einsatz und der Ernstfall wird regelmäßig getestet. Weitere 11 % verfügen über spezielle Notfallpläne und testen diese regelmäßig. [31, S. 28] Ransomware wird als eine der gefährlichsten Bedrohungen angesehen und als geeignete Schadensbegrenzungsmaßnahme sind regelmäßige Back-Ups wichtig. Jedoch verzichten neun Prozent gänzlich darauf und 16 % führen Datensicherungen nur unregelmäßig durch. Immerhin 46 % verfügen über ein Konzept und setzen dieses regelmäßig um. Sogar 29 % verfügen über ein qualifiziertes Back-Up-Konzept. [31, S. 28]
Außerdem ist das Thema Cloud-Computing ein nicht zu vernachlässigender Trend. Etwas mehr als die Hälfte der Unternehmen nutzen Cloud-Anwendungen. Davon haben 44 % keine Kenntnis von IT-Sicherheitsanforderungen oder rechtlichen Rahmenbedingungen. 31 % der Cloud-nutzenden Unternehmen nehmen dazu eine externe Beratung in Anspruch und 25 % haben klare Regeln für den Einsatz und die Verwendung von Cloud-Anwendungen definiert. [31, S. 33]
Im Bezug auf Versicherungen gegen IT-Risiken besteht Nachholbedarf. Jedes vierte Unternehmen kennt diese Möglichkeit gar nicht und die Hälfte der Unternehmen wissen zwar davon, haben sich aber noch nicht mit diesem Thema befasst. Lediglich 21 % nutzen diese Versicherung und vier Prozent sind sogar dazu verpflichtet. [31, S. 34]
Zusammenfassend lässt sich sagen, dass Unternehmen sich mit Sicherheitsfragen aktiv befassen sollten und Sicherheitsmaßnahmen vermehrt umsetzen sollten. Außerdem sollte Wert auf Sicherheitsschulungsprogramme für alle Mitarbeitenden gelegt werden. Risikoermittlung muss mehr Beachtung erfahren und die unternehmensinterne Sicherheitskultur, besonders die personellen Verantwortlichkeiten, sollten überdacht werden.

3.7 Sicherheitsmaßnahmen 2021

Der Chart-Bericht zur IT-Sicherheit in der deutschen Wirtschaft 2021 wurde vom Digitalverband Bitkom am 14. Oktober 2021 publiziert. Die Ergebnisse der Befragung 2021 werden jeweils denen aus den bisherigen Befragungen von 2017 und 2019 gegenüber gestellt. Der Umfang der befragten Unternehmen 2021 beträgt 1067.
Im Fokus dieses Berichts stehen die umgesetzten und konkret geplanten Sicherheitsmaßnahmen der Unternehmen in verschiedenen Bereichen. Das umfasst technische, organisatorische und personelle Sicherheitsmaßnahmen. [33]

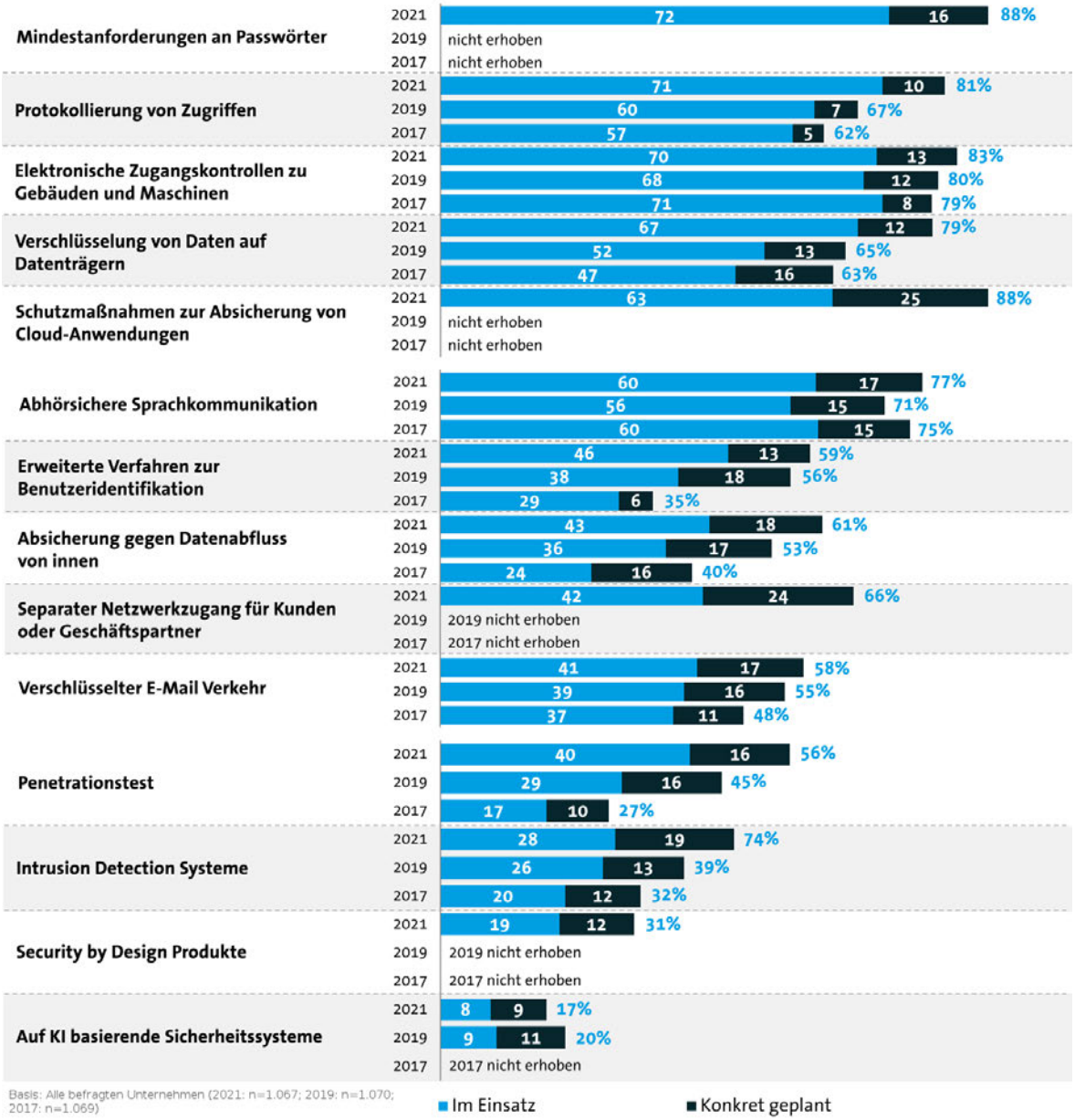


Abbildung 3.23: Umsetzung technischer Sicherheitsmaßnahmen [33, S. 3–5]
Anmerkung: fehlerhafter Prozentwert bei Intrusion Detection Systeme 2021, korrekt: 47 %

Zu Beginn wird die Frage gestellt, ob im Unternehmen ein Notfallmanagement, wie schriftlich geregelte Abläufe und Sofort-Maßnahmen für das Auftreten eines Angriffs, etabliert ist. Knapp mehr als die Hälfte (51 %) verfügen über derartige Maßnahmen. Im Vergleich der Beschäftigtenzahlen der Unternehmen zeigt sich, dass Unternehmen mit 500 oder mehr Mitarbeitenden dieser Aussage am meisten (68 %) zustimmten. Des Weiteren wird deutlich, dass diese Systeme in KRITIS-Sektoren (58 %) mehr etabliert sind, als in Nicht-KRITIS-Sektoren (50 %). [33, S. 2]
Bezüglich der Umsetzung der technischen Sicherheitsmaßnahmen ist eine Zunahme im Vergleich zu den Vorjahren in Abbildung 3.23 zu beobachten. Am meisten umgesetzt sind Mindestanforderungen an Passwörter (72 %) und konkret geplant 16 %, also gesamt 88 %. Am wenigsten umgesetzt wird verschlüsselte E-Mail-Kommunikation (41 %). [33, S. 3–5]
Wie Abbildung 3.24 zeigt, liegt die Festlegung von Zugriffsrechten für bestimmte Informationen im Bereich der organisatorischen Sicherheitsmaßnahmen mit einem aktuellen Höchstwert von 100-prozentiger Umsetzung ganz vorn. Allgemein sind Regelungen für den Umgang mit sensiblen Informationen weit vorn. Ausbaufähig ist weiterhin der Einsatz von Managementsystemen für die IT-Sicherheit. [33, S. 6–7]

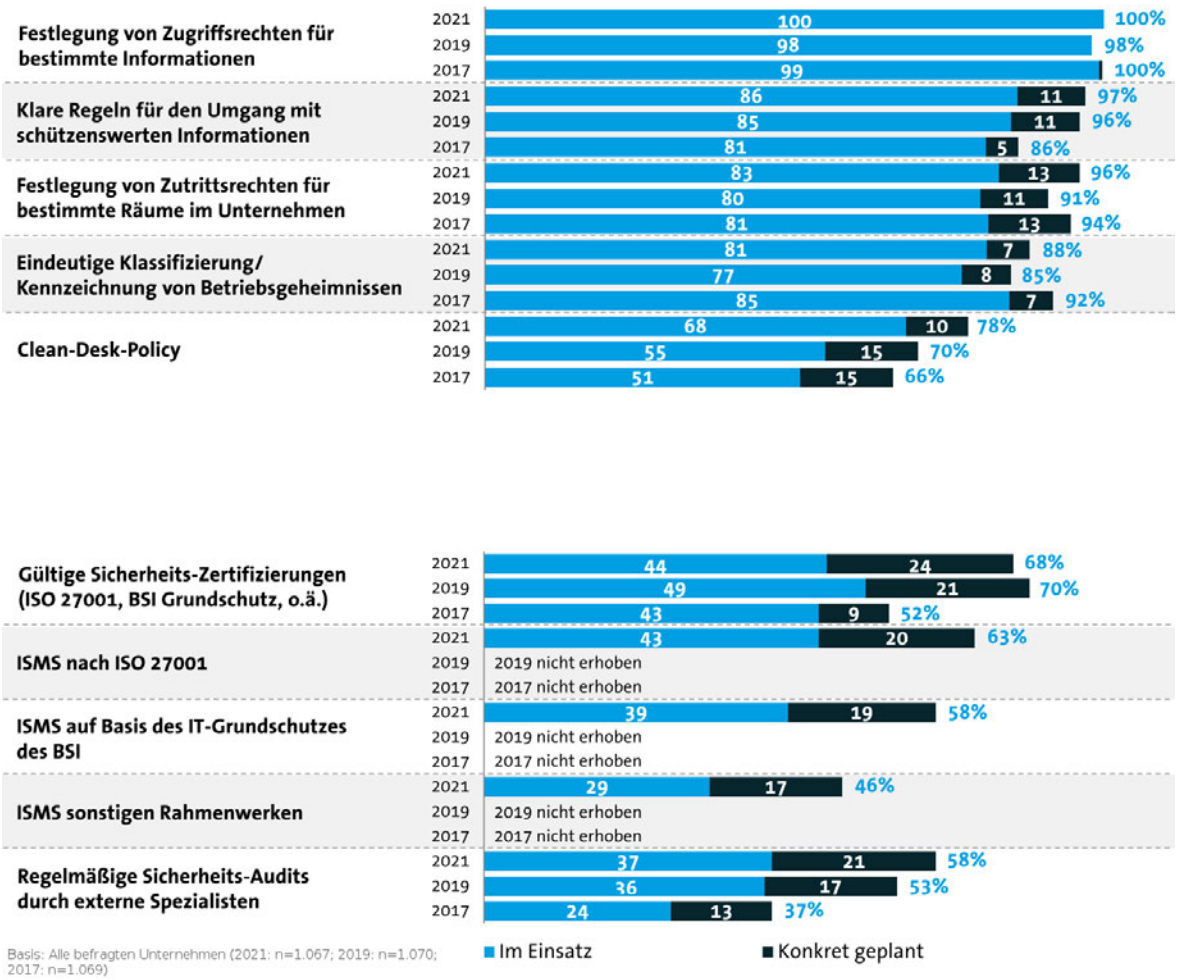


Abbildung 3.24: Umsetzung organisatorischer Sicherheitsmaßnahmen [33, S. 6–7]

Die Kategorie personelle Sicherheitsmaßnahmen ist in Abbildung 3.25 abgebildet. Dabei befindet sich die Bestellung eines Sicherheitsverantwortlichen mit einer Umsetzung von 59 % und konkrete Planung von 22 % an erster Stelle. Die Umsetzung und Planung von Mitarbeiterschulungen zu Sicherheitsthemen und Hintergrundüberprüfungen bei der Besetzung sensibler Positionen sind in letzter Zeit leicht zurückgegangen. Hingegen ist die Umsetzung eines anonymen Hinweis-Systems auf verdächtige Mitarbeitende leicht gestiegen auf 32 %. [33, S. 8]

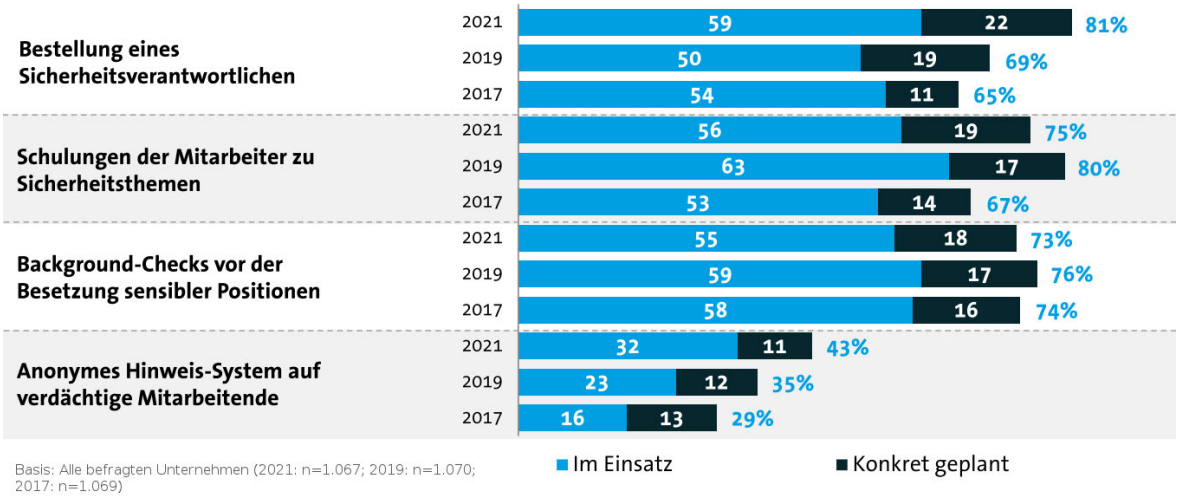


Abbildung 3.25: Umsetzung personeller Sicherheitsmaßnahmen [33, S. 8]

3.8 IT- und Cybersicherheit 2021

Bitkom Research führte als Grundlage eine Umfrage mit 1011 Internetnutzenden in Deutschland ab 16 Jahren im November 2021 telefonisch durch. Die Ergebnisse veröffentlichte Bitkom e.V. am 14. Dezember 2021 in Form mehrerer grafischer Darstellungen.
Die Fragen fokussieren allgemein den Bereich der IT- und Cybersicherheit. Es geht besonders um das Sicherheitsgefühl der Internetnutzenden. Die Themen umfassen das Gefühl der Datensicherheit im Internet und allgemein und die Bedrohungen und persönlichen Erfahrungen mit kriminellen Vorfällen der Nutzenden im Internet. Ein weiteres Thema sind die umgesetzten Sicherheitsmaßnahmen zum eigenen Schutz. [34]
Die erste Frage behandelt das Gefühl der Sicherheit der Befragten für ihre persönlichen Daten im Internet allgemein. Dabei zeigt sich im Vergleich zum Vorjahr ein Anstieg von neun Prozentpunkten auf 77 % bei den Befragten, die ihre Daten für unsicher halten. [34, S. 2]
Allgemein sind Veränderungen im Vertrauen gegenüber verschiedenen Instanzen beim Umgang mit persönlichen Informationen festzustellen. Dabei zeigt sich, dass gegenüber allen Instanzen das Misstrauen überwiegt, die Befragten also allgemein wenig Vertrauen in Instanzen wie Soziale Netzwerke, öffentliche Verwaltung, Polizei, Dienstleistende oder Banken haben. Am größten ist das Vertrauen in Online-Händler mit 47 % und E-Mail-Anbieter mit 46 %. Am meisten misstrauen die Befragten den selbst genutzten Sozialen Netzwerken (68 %). [34, S. 3]
In der Zuständigkeit für den Schutz persönlicher Daten sehen sich 88 % selbst in der Verantwortung, acht Prozent den Staat und zwei Prozent die Wirtschaft wie Dienstleister und Anbieter. Diese Verlagerung der Zuständigkeit hin zur Selbstverantwortung zeigt sich im Vergleich zu den Vorjahren besonders. [34, S. 4]

Im Bereich der Bedrohungen im Internet machen sich Nutzenden die größte Sorge vor illegaler Datennutzung (85 %) und die Infizierung mit Schadprogrammen (83 %). Die Sorge um Ausspähung durch staatliche Stellen ist in den letzten Jahren von 51 % im Jahr 2018 auf 30 % 2021 gesunken. Ein besonders starker Anstieg auf 27 % ist bei Hassrede im Internet zu beobachten. [34, S. 5–6]
Bei der Untersuchung der persönlichen Erfahrungen mit kriminellen Vorfällen im Internet zeigt sich in Abbildung 3.26, dass der Anteil der Befragten, die noch keine Erfahrungen in diesem Bereich gemacht haben, um 13 Prozentpunkte im Vergleich zur letzten Befragung gesunken ist. Am meisten wurden Menschen Opfer von Schadprogramminfektionen (47 %). Ungefragte Datenweitergabe an Dritte folgt mit 39 % auf Platz zwei. Auch Betrug bei privaten Käufen (19 %) und beim Online-Banking (15 %) sind eine Bedrohungsgefahr. [34, S. 7–8]

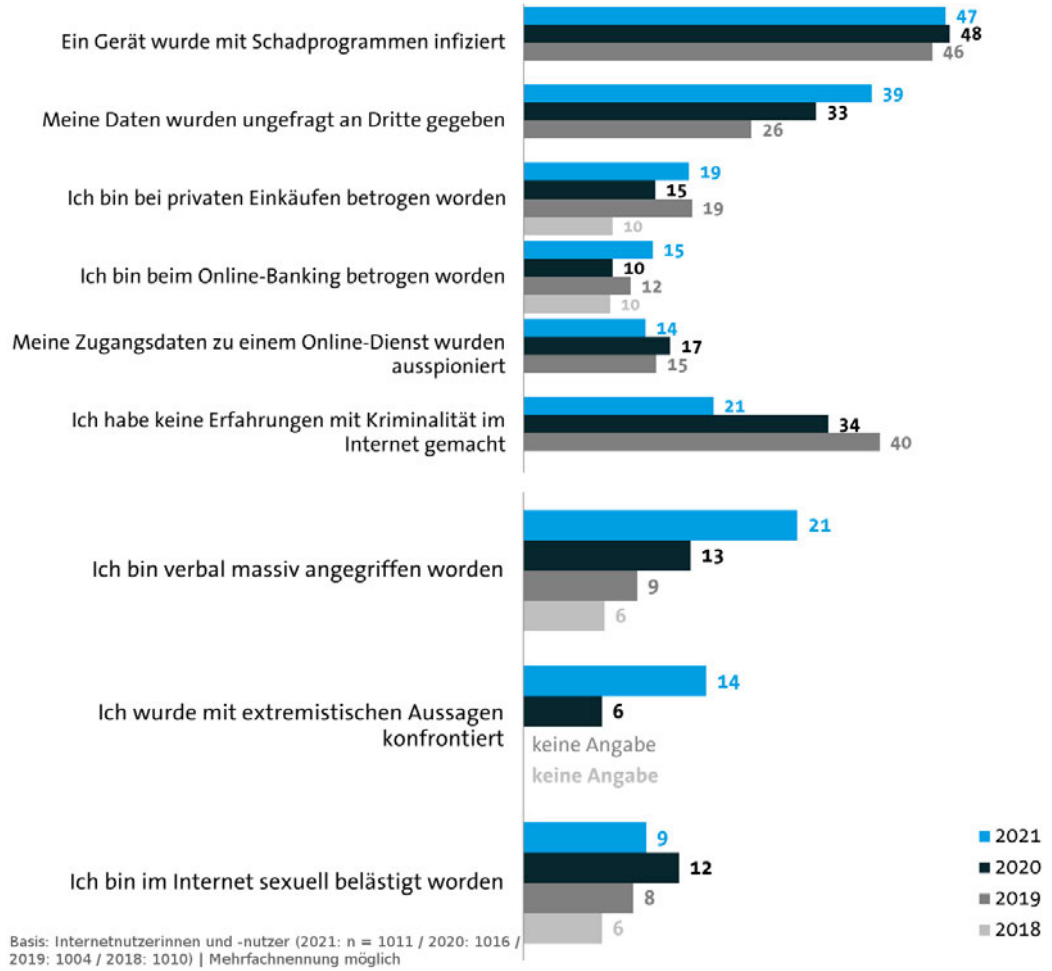


Abbildung 3.26: Angriffe (in Prozent) [34, S. 7–8]

Bei der Umsetzung von Sicherheitsmaßnahmen auf privaten Computern in Abbildung 3.27 befinden sich Virenschutzprogramme mit 86 % an erster Stelle. Mit wenig Abstand folgt auf dem zweiten Platz der Einsatz von Firewalls mit 71 %. Alle weiteren Maßnahmen werden deutlich weniger eingesetzt. Mit den Ausnahmen der Virenschutzprogramme und regelmäßigen Backups auf externen Speichern haben alle Maßnahme leicht oder stärker an Bedeutung gewonnen. Den meisten Anstieg mit acht Prozent verzeichnen Passwort-Safes mit nun 23 %. [34, S. 9]

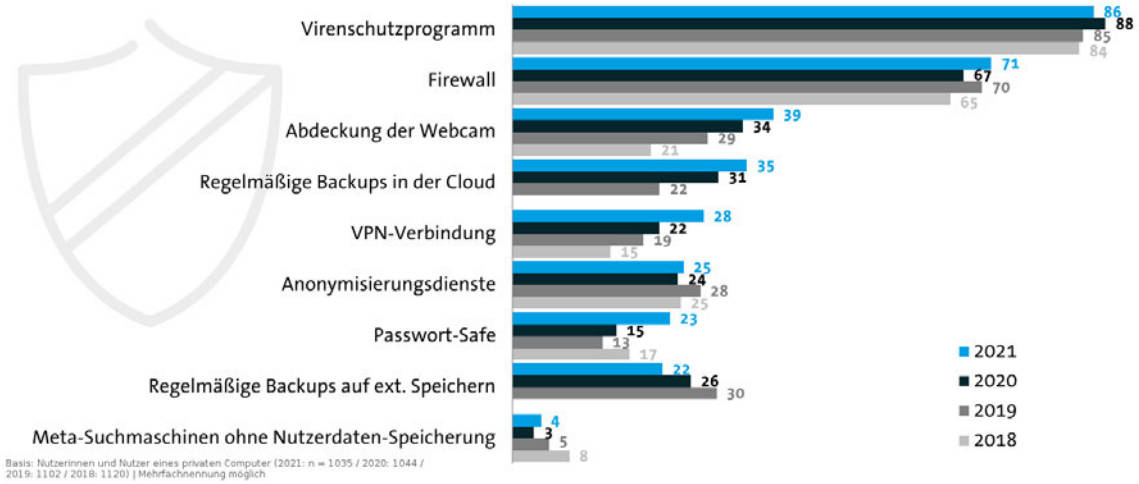


Abbildung 3.27: Sicherheitsmaßnahmen auf privaten Computern (in Prozent) [34, S. 9]

Bezüglich der Sicherheitsmaßnahmen auf privaten Smartphones in Abbildung 3.28 wird deutlich, dass diese nur unzureichend geschützt werden. Die meiste Umsetzung erfahren Lokalisierungsfunktionen bei Verlust mit 65 %. Alle Maßnahmen außer Abdeckungen auf Smartphone-Kameras verbreiteten sich im Vergleich zum Vorjahr. Die größte Steigerung ist bei regelmäßigen Backups in der Cloud zu beobachten. [34, S. 10]

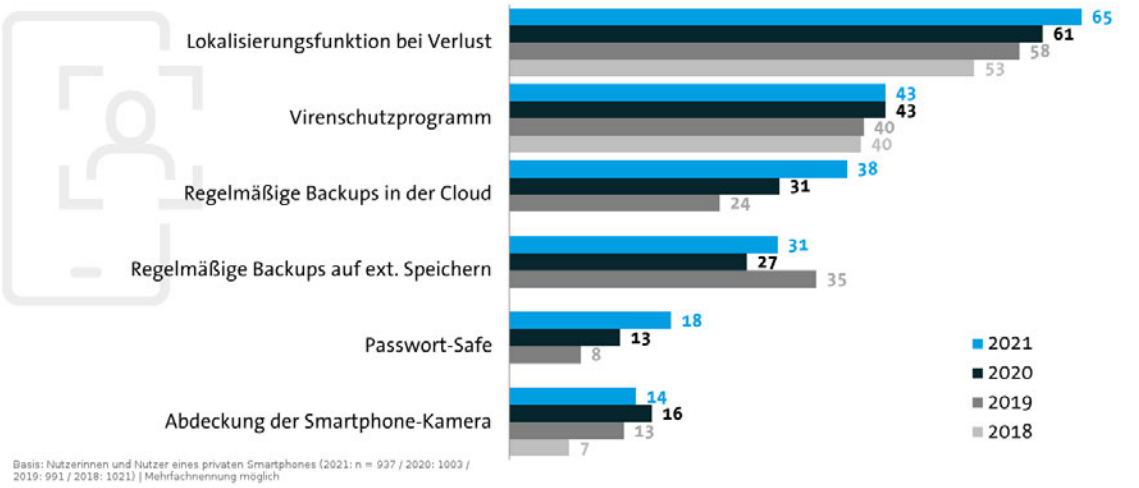


Abbildung 3.28: Sicherheitsmaßnahmen auf privaten Smartphones (in Prozent) [34, S. 10]

Die Nutzung der Zwei-Faktor-Authentifizierung ist noch stark ausbaufähig. Lediglich 37 % der Befragten geben an, zumindest für einige Online-Dienste diese Zugangsmöglichkeit zu nutzen. Die Untersuchung der möglichen Anmeldeoptionen ergibt ein Ranking von Code per SMS auf Platz eins mit 35 %, gefolgt von E-Mail mit 32 % und TAN-Generator mit 31 %. [34, S. 11]
69 % der Befragten meinen, es vermutlich nicht zu bemerken, wenn sie von Fremden über das Internet ausspioniert werden würden. Außerdem fürchten sich 48 % mehr vor Internetkriminalität als vor Kriminalität in der analogen Welt. Im Bezug auf Sicherheitsmaßnahmen schätzen sich 41 % als genügend informiert ein, ihre Geräte selbst ausreichend vor Internetkriminalität schützen zu können. Zudem stimmen 64 % zu, Software-Updates sofort zu installieren. Im Allgemeinen nimmt in der

Wahrnehmung der Befragten die Bedrohung durch Internetkriminalität immer mehr zu (98 %). Als geeignete Maßnahmen sehen 91 % mehr Präsenz der Polizei im digitalen Raum und sind der Meinung, dass finanzielle Hilfen von staatlichen Stellen in speziell auf Internetkriminalität spezialisierte Polizeieinheiten sinnvoll sind (92 %). Hingegen nehmen sechs Prozent der Befragten das Thema Internetkriminalität als medial übertrieben dargestellt wahr. [34, S. 12–13]

3.9 Digitalbarometer 2021 und 2022

Das ist eine jährlich stattfindende repräsentative Online-Befragung der deutschsprachigen Bevölkerung zwischen 14 und 69 Jahren mit Internetzugang. Sie wird durch die Polizeiliche Kriminalprävention der Länder und des Bundes und das BSI beauftragt. Das Digitalbarometer 2021 wurde im September 2021 publiziert. Der Befragungszeitraum umfasst Ende April bis Ende Mai 2021 und es wurden 2025 Interviews durchgeführt. [35, S. 2] Die Umfrage 2022 fand von Mitte April bis Mitte Mai 2022 statt und umfasst 2000 Interviews. [36, S. 2] Aufgrund einiger spezifischer Fragestellungen ist es notwendig, in dieser Arbeit Ausschnitte beider Befragungen zu betrachten. Die Themen reichen von der allgemeinen Internetnutzung und Schutzmaßnahmen über Erfahrungen mit Internetkriminalität bis zur Bekanntheit und der Nutzung des BSI und des Programms Polizeiliche Kriminalprävention. Der Themenfokus im Jahr 2021 liegt auf den Online-Aktivitäten während der Corona-Pandemie. Diese Umfrage analysiert besonders unterschiedliche Altersgruppen genauer. [35]
Das Digitalbarometer 2021 beschäftigt sich in der ersten Frage mit dem Besitz internetfähiger Geräte. 90 % der Befragten geben an, ein Smartphone zu besitzen, 75 % besitzen einen Laptop bzw. Notebook und jeweils knapp über die Hälfte geben an, Desktop-Computer (54 %) und Tablet (53 %) zu besitzen. Die größten Anstiege sind beim Besitz von vernetzten Heimgeräten auf 29 % und Fitnesstracker auf 23 % zu verzeichnen. Als häufigster Grund für die Internetnutzung wird Recherche (75 %), Onlinekauf (70 %) und Kommunikation (70 %) genannt. Im Allgemeinen wird ein großer Teil der Freizeit online verbracht: mehr als die Hälfte der Befragten gibt an, täglich zwei bis fünf Stunden im nicht-beruflichen Kontext online zu sein. [35, S. 3]
Beim Thema Informations- und Schutzverhalten stimmen zwei Drittel zu, von Schutzempfehlungen zu wissen. Jedoch setzen nur 12 % diese vollständig um. Als Gründe dafür werden zu hoher Aufwand und zu komplizierte Schutzmaßnahmen genannt. Hingegen schätzen die Personen, die Schutzempfehlungen beherzigen, den Aufwand geringer ein. In Abbildung 3.29 ist im Allgemeinen festzustellen, dass mehr Schutzmaßnahmen als in den Vorjahren im Einsatz sind. Am häufigsten werden Virenschutzprogramme (62 %), sichere Passwörter (60 %) und aktuelle Firewall (53 %) eingesetzt. [35, S. 4–5]
Im Themenfokus dieser Befragung geht es um die Online-Aktivitäten in der Corona-Pandemie. Seit Beginn der Pandemie ist eine deutliche Steigerung in der Internetnutzung zu verzeichnen. Dafür nennen die Befragten je nach Altersklasse unterschiedliche Gründe. Besonders im Fokus der Jüngeren standen Streaming-Dienste. 40- bis 59-Jährige bevorzugten den Onlinekauf und Grund für 60- bis 69-Jährige war vor allem die Kontaktaufrechterhaltung und Kommunikation mit anderen Menschen. Das Sicherheitsgefühl der Menschen war trotz der vermehrten Internetnutzung auf einem hohen Niveau, weil 80 % ein mindestens sicheres Gefühl bei der Nutzung hatten. [35, S. 9]

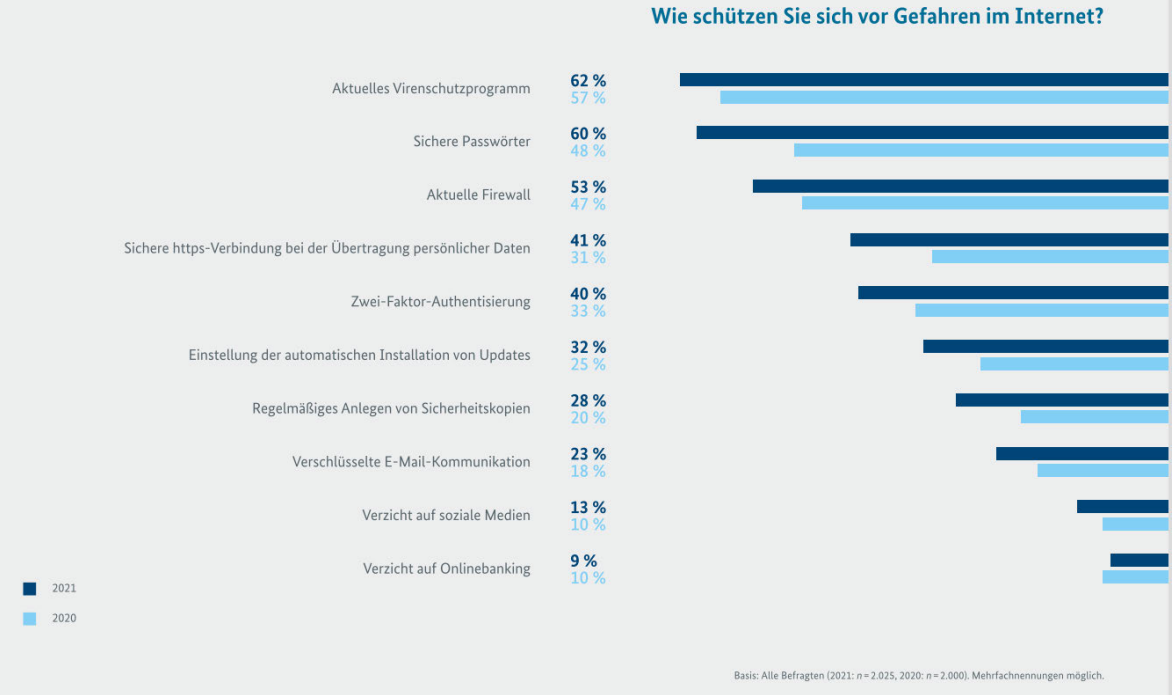


Abbildung 3.29: Umsetzung Sicherheitsmaßnahmen [35, S. 5]

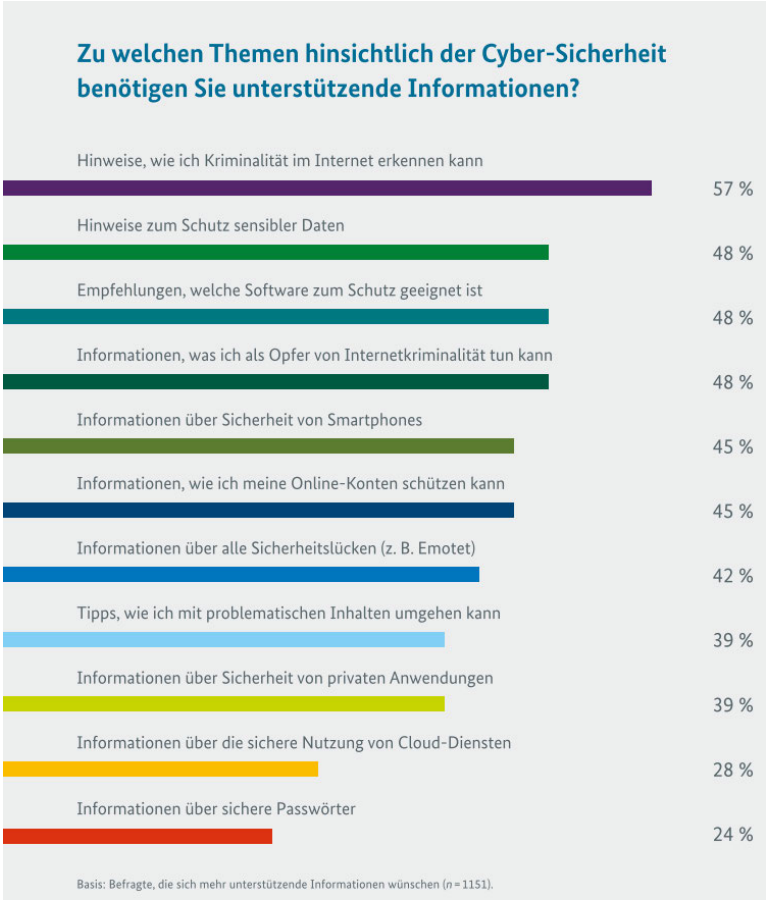


Abbildung 3.30: Informationswunsch [35, S. 13]

Im Allgemeinen ist festzustellen, dass sich besonders jüngere Menschen vorwiegend sicher fühlen, da 55 % eine sehr geringe oder eher geringe Gefahr von Cyberkriminalität sehen und vier Prozent diese sogar für ganz ausgeschlossen halten. Zudem setzen Jüngere durchschnittlich lediglich drei Sicherheitsmaßnahmen ein. Das liegt unter dem Gesamtdurchschnitt von vier Maßnahmen. Im Allgemeinen fühlt sich ein Drittel der Befragten sehr oder zumindest eher gut informiert. 18 % schätzen ihren Informationsstand als eher schlecht oder sehr schlecht ein und 45 % fühlen sich nur teilweise informiert. 57 % wünschen sich mehr Informationen über Cybersicherheit. Besonders beim älteren Teil der Befragten von 40 bis 69 Jahren werden Webseiten und E-Mail-Newsletter als bevorzugte Kanäle genannt. Auch klassische Medien wie Zeitung und Radio werden als wichtig eingeschätzt. Jüngere Menschen bevorzugen Informationen in sozialen Medien. Bezüglich der Themenwünsche ist ein breites Bild zu verzeichnen. Diese sind in Abbildung 3.30 dargestellt. Am meisten gefragt sind Hinweise, um Internetkriminalität zu erkennen (57 %). Auch Informationen zu Schutzmaßnahmen, insbesondere zum Schutz sensibler Daten, geeignete Software dafür und Handlungsempfehlungen für Opfer, sind mit 48 % attraktive Themen. Als nicht so relevant und informativ werden Hinweise zu sicheren Passwörtern eingeschätzt. Diese wünschen sich lediglich 24 % der Befragten, die den Wunsch nach unterstützenden Informationen haben. [35, S.12–13]

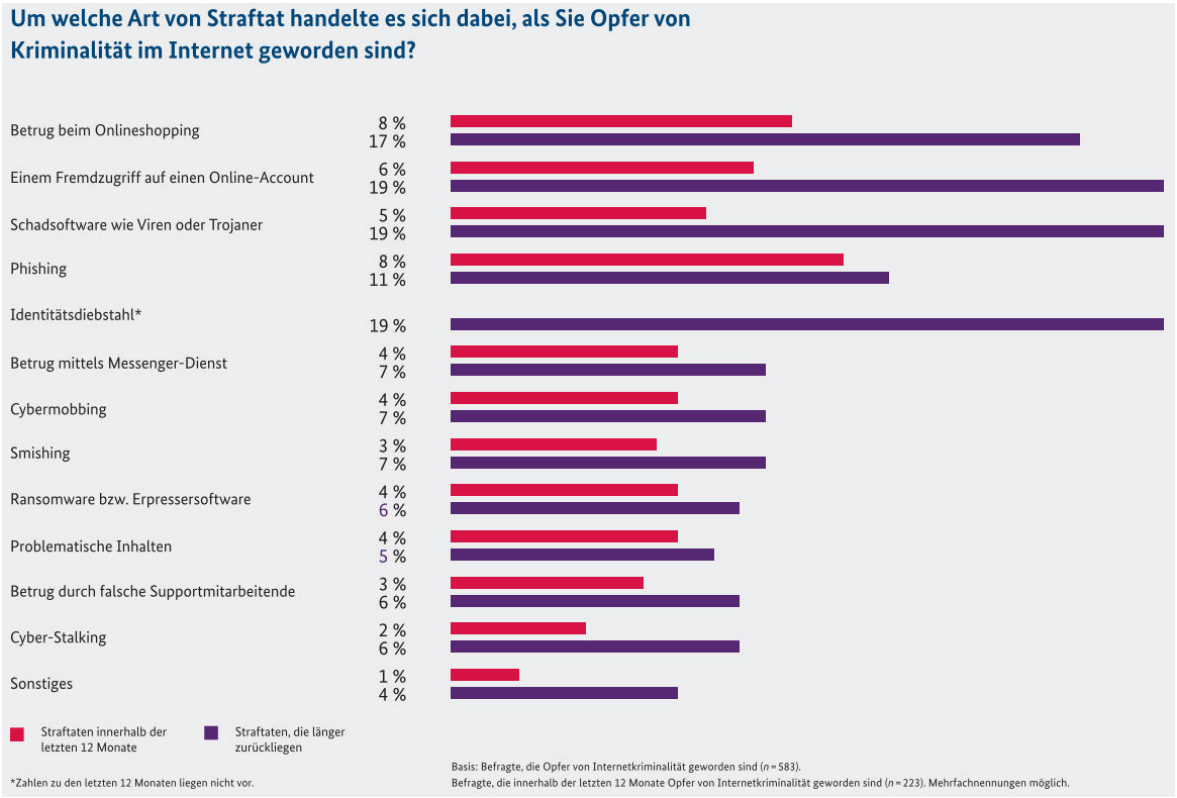


Abbildung 3.31: Straftaten 2021 [36, S. 9]

Die Zahlen und Informationen zu den persönlichen Erfahrungen mit Kriminalität im Internet im Digitalbarometer 2022 beziehen sich auf das hier fokussierte Jahr 2021. Die Statistik zeigt Abbildung 3.31. 29 % der Befragten geben an, schon einmal Opfer gewesen zu sein, 39 % davon erlebten dies innerhalb der vergangenen zwölf Monate. Die häufigsten Vorfälle sind Betrug beim Onlineshopping, Fremdzugriff auf Online-Accounts und Einschleusen von Schadsoftware. Dabei wurden von den Angreifenden verschiedene Betrugsarten eingesetzt: betrügerische E-Mails (19 %), gefälschte

Messengernachrichten (11 %), SMS (10 %) oder Anrufe vorgeblicher Support-Mitarbeitenden (9 %). Außerdem geben 62 % der Befragten an, schon einmal Phishing-Mails erhalten zu haben, ohne darauf eingegangen zu sein. In den vergangenen zwölf Monaten sind die von Angriffen Betroffenen besonders Opfer von Onlineshoppingbetrug (8 %) und Phishing (8 %) geworden. Mit sechs Prozent schließen sich daran Fremdzugriffe auf Online-Accounts und mit fünf Prozent Schadsoftware an. [36, S. 8–9]

Wie in Abbildung 3.32 zu sehen ist, geben 79 % der Befragten, die bereits Opfer von Internetkriminalität geworden sind, an, durch Cyber-Angriffe im vergangenen Jahr Schäden erlitten zu haben. Am meisten wurde zeitlicher Schaden (29 %) und Datenverlust (25 %) verursacht. Finanzielle Schäden erlitten 13 %. Der größte finanzielle Schaden wurde durch Betrugsmaschen verursacht. Der durchschnittliche Verlust hierbei beträgt 674€. Bei Schadsoftware belaufen sich Schäden meist unter 500€ und bei Datendiebstahl üblicherweise unter 600€. [36, S. 10]

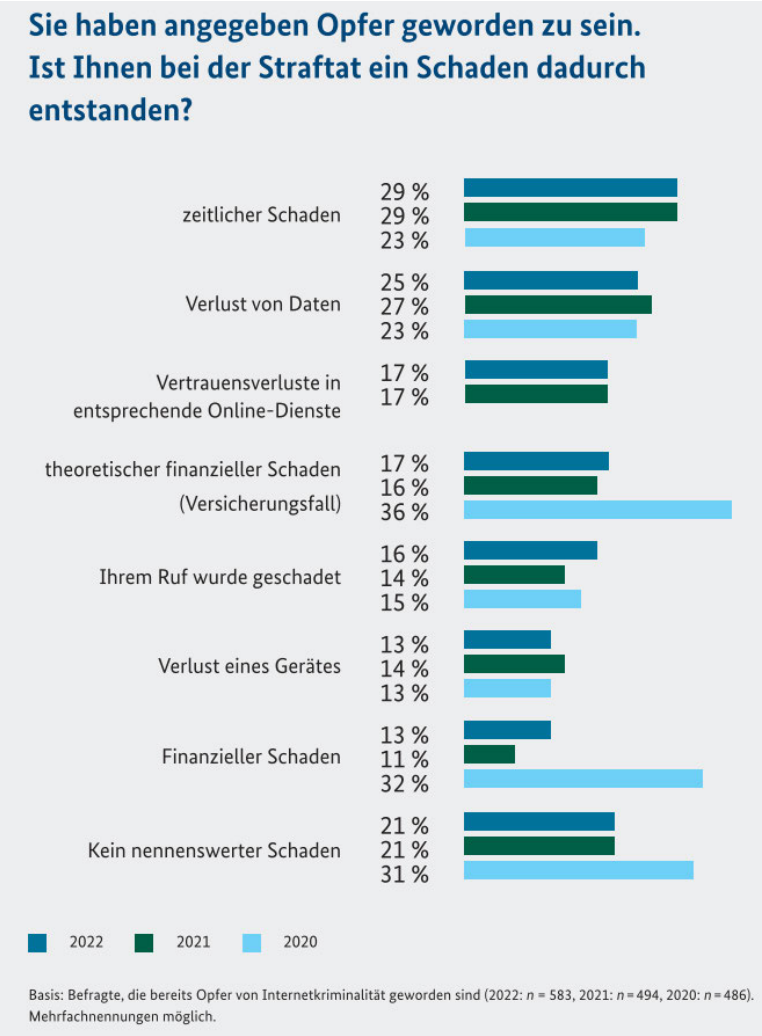


Abbildung 3.32: Entstandene Schäden [36, S. 10]

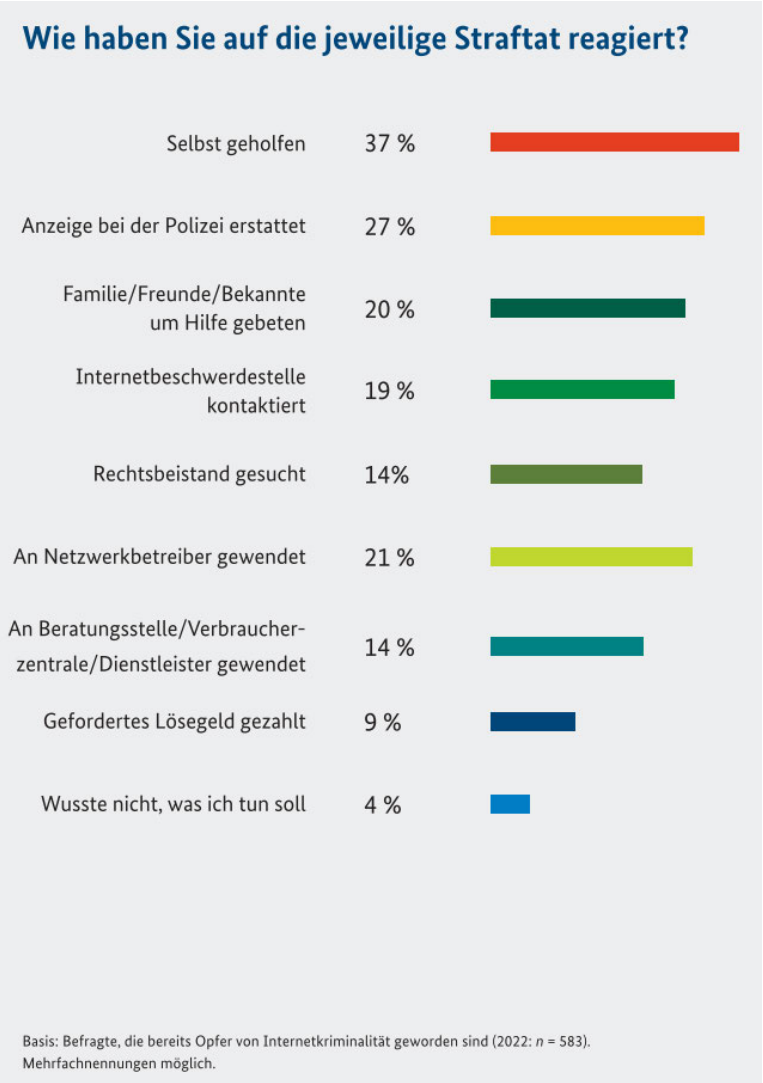


Abbildung 3.33: Reaktionen auf Straftaten [36, S. 11]

Die Reaktionen auf Straftaten im Internet gestalten sich sehr unterschiedlich, wie in Abbildung 3.33 erkennbar ist. Lediglich vier Prozent der Befragten, die bereits Erfahrungen mit Internetkriminalität gemacht haben, wussten nicht, was sie tun sollen. Ein großer Teil mit 37 % half sich selbst und 20 % fragten Menschen in ihrem Umfeld nach Hilfe. 27 % erstatteten Anzeige bei der Polizei. [36, S. 11]

3.10 Vergleich der Berichte

Nachdem für die Studien und Berichte der theoretische Hintergrund und die Inhalte detailliert dargestellt wurden, werden diese im folgendem Teil unter verschiedenen Aspekten miteinander verglichen und die Unterschiede und Gemeinsamkeiten aufgezeigt. Der Vergleich erfolgt jeweils getrennt nach dem Befragungsgebiet in Wirtschaft und Gesellschaft.

3.10.1 Bedrohungslage

Die Einschätzungen der Bedrohungslage Cybercrime in Deutschland kommen in den betrachteten Berichten zu ähnlichen Ergebnissen. So schätzen die Lageberichte des BSI die Lage als angespannt und kritisch ein. Dadurch ist die Bedrohung an ihrem bisherigen Höhepunkt. [23, S. 11] [5, S. 9]
Der Bericht zum Wirtschaftsschutz der Bitkom e.V. zeigt, dass vor allem KRITIS-Sektoren eine starke Zunahme der Bedrohung wahrnehmen. [29, S. 6]
In der Umfrage des Internetverbands eco wird die Bedrohungslage durch Cybercrime von 93,8 % als mindestens wachsend eingeschätzt. 80 % der Befragten sehen eine Verschärfung der Lage durch die Corona-Pandemie. [30, S. 12]
Laut dem Bericht IT- und Cybersicherheit 2021 machen sich Menschen die meisten Sorgen um illegale Datennutzung und Schadprogramminfektionen. [34, S. 5–6] Zudem stimmen 48 % der Aussage zu, mehr Angst vor Internetkriminalität als vor Kriminalität im analogen Raum zu haben und die Bedrohung durch Internetkriminalität nimmt in der Wahrnehmung der Befragten immer mehr zu. Das zeigt eine Zustimmung von 98 % zu dieser Aussage. Hingegen sehen sechs Prozent das Thema Internetkriminalität als in den Medien übertrieben dargestellt. [34, S. 12]
Im Digitalbarometer 2021 geben vor allem jüngere Menschen an, sich vorwiegend sicher zu fühlen. Vier Prozent halten eine Gefahr durch Cybercrime sogar für ganz ausgeschlossen und mehr als die Hälfte sieht eine geringe Gefahr. [35, S. 9]
Schlussfolgernd zeigt sich, dass sich Menschen vor Internetkriminalität im Allgemeinen fürchten und diese als Bedrohung sehen. Das wird sowohl im wirtschaftlichen Bereich als auch im privaten gesehen. Jüngere Menschen nehmen die Bedrohung tendenziell weniger wahr. Ein Grund dafür kann das Aufwachsen in einer bereits stark digitalisierten Welt und damit von Anfang an mehr Vertrauen in Technik sein.

3.10.2 Angriffe

Auch im Bezug auf stattgefundene Angriffe resultieren die Berichte im ähnlichen Ergebnis, dass von einer Zunahme der Cybercrime-Delikte auszugehen ist. Die Ausprägung der stattgefundenen Angriffe kann jedoch nicht genau quantifiziert werden. Die in der PKS aufgenommenen Fälle stellen das Hellfeld dar, welches der Polizei gemeldet wurde. Es wird jedoch von einem großen Dunkelfeld ausgegangen. [10, S. 9] Das Bundeslagebild Cybercrime stellt in den Cybercrime-Zahlen einen deutliche Anstieg fest. Als Grund dafür wird die zunehmende Digitalisierung in Folge der Corona-Pandemie gesehen. Außerdem ist eine Verlagerung der Angriffe vom analogen in den digitalen Raum festzustellen. [29, S. 3] Dieses Ergebnis korreliert mit der Feststellung, dass die Anzahl der erfassten Straftaten in der PKS abgenommen hat, die Zahl der Cybercrime-Delikte jedoch um 12 % gestiegen ist. [10, S. 4–7]
Im Bericht zum Wirtschaftsschutz 2022 des Bitkom e.V. geben 84 % der Befragten an, innerhalb der letzten zwölf Monate angegriffen worden zu sein. Im Vorjahr liegt dieser Prozentwert bei 88 %, ist also geringfügig gesunken. [29, S. 2] Auch bei der Bewertung, inwiefern sich Cyberangriffe 2021 verändert haben, stimmt der Großteil der Befragten (84 %) für mindestens zugenommen. Besonders KRITIS-Unternehmen unterstützen diese Aussage. [29, S. 6]
Die Frage nach mindestens einem gravierenden Sicherheitsvorfall im vergangenen Jahr, also 2021, beantworten 17 % in der Umfrage von eco mit ja. Im Vergleich dazu lag dieser Prozentwert im Vorjahr bei 20 %, also ist eine geringe Verringerung zu verzeichnen. Auch die Zahl der vermutlich Betroffenen ist gesunken. [30, S. 6]

In der Befragung durch DsiN machen 27 % der befragten KMU die Angabe, im vergangenen Jahr einige Probleme durch Schadsoftware gehabt zu haben. Außerdem waren 10 % mindestens einmal durch einen gezielten Angriff betroffen und fünf Prozent sogar ständig. Für stattgefundene Angriffe ergibt sich daraus insgesamt 42 %. Mehr als die Hälfte wurde noch nie angegriffen. [31, S. 10]
In der IT- und Cybersicherheitsstudie antworten auf die Frage, von welchen Angriffen sie 2021 betroffen waren, 21 % der Befragten, dass sie keine Erfahrungen damit gemacht haben. Bei der Betrachtung des Prozentwertes im Vergleich mit den Werten der vergangenen Jahre wird deutlich, dass der Wert sinkt, also mehr Menschen mit Internetkriminalität in Berührung kommen. 2020 waren immerhin noch 34 % nicht betroffen und 2019 sogar 40 %. [34, S. 7–8] Da 2021 21 % keine Internetkriminalitätserfahrungen gemacht haben, ergibt sich ein Prozentwert von 79 %, die im vergangenen Jahr von Angriffen betroffen waren.
Im Digitalbarometer 2022 geben jeder und jede vierte (29 %) der Befragten an, bereits angegriffen worden zu sein. Davon waren 39 % innerhalb der letzten zwölf Monate betroffen, also waren 11 % der Befragten 2021 betroffen. [36, S. 8–9] Zum Vergleich: im Vorjahr waren 9 % der Befragten innerhalb der letzten zwölf Monate betroffen und insgesamt waren 24 % der Befragten bereits von Cyberkriminalität betroffen. [35, S. 7]

Für eine bessere Übersicht sind diese Prozentwerte in der folgenden Tabelle 3.1 dargestellt.

Tabelle 3.1: Stattgefundene Angriffe 2021 in Prozent [29, S. 2], [30, S. 6], [31, S. 10], [34, S. 7–8], [36, S. 8–9]

Umfrage	stattgefundene Angriffe
Wirtschaftsschutz 2022	84 %
DsiN-Praxisreport 2021/22	42 %
eco Umfrage 2022	17 %
IT- & Cybersicherheit 2021	79 %
Digitalbarometer 2022	11 %

Bei dieser Gegenüberstellung der Prozentwerte gilt es zu beachten, dass die IT- und Cybersicherheitsstudie und das Digitalbarometer nicht die Wirtschaft umfassen, sondern allgemein Internetnutzende befragt wurden. Diese Umfragen bilden daher die Gesellschaft ab, während die drei weiteren die Wirtschaft umfassen. Im Wirtschaftsbereich zeigen sich deutliche Unterschiede in den Werten. Als ein weiteres Unterscheidungsmerkmal ist der unterschiedliche Umfang der Befragungen zu nennen. Besonders herausragend dabei ist die Umfrage des Internetverbands eco, denn diese umfasst nur 145 Befragungen. Als Gemeinsamkeit der Umfrage von eco und dem Wirtschaftsschutzbericht stellt sich die geringfügige Verringerung des Prozentwertes der stattgefundene Angriffe im Vergleich zum Vorjahr dar. Es gilt zu untersuchen, ob für diese Entwicklung möglicherweise eine verstärkte Umsetzung von Sicherheitsmaßnahmen ursächlich ist. Im Bezug auf die Entwicklung von Cybercrime in der Gesellschaft ist festzustellen, dass sich die Zahl der Betroffenen innerhalb der letzten zwölf Monate zwischen den Umfragen stark unterscheidet. Eine Gemeinsamkeit ist die Entwicklung im Vergleich zum Vorjahr. Beide Berichte des gesellschaftlichen Bereichs kommen zu dem Ergebnis, dass Cybercrime, wenn auch unterschiedlich stark, zunimmt. Möglicherweise ist als Grund dafür die fehlende oder mangelhafte Umsetzung von Sicherheitsmaßnahmen zu nennen.

Auch bei der genaueren Untersuchung der Angriffsarten fallen Gemeinsamkeiten und Unterschiede der verschiedenen Berichte auf. Das Bundeslagebild Cybercrime des BKA enthält eine Aufschlüsse-

lung der Cybercrime-Delikte nach ihrem Straftatbestand. Eine Darstellung befindet sich in Abbildung 3.2. Demnach macht Computerbetrug den größten Teil mit 77 % aus.
Im Bereich der Wirtschaft liefern die Wirtschaftsschutzstudie und die Umfrage von eco Ergebnisse. Nach der Wirtschaftsschutzstudie sind Angriffe auf Passwörter, Phishing und Schadsoftwareinfektionen mit jeweils 25 % am meisten vorgekommen. Auf dem zweiten Platz folgen mit 21 % DDoS-Angriffe. CEO-Fraud machen nur einen sehr geringen Teil von fünf Prozent aus. Diese Werte sind in Abbildung 3.13 zu finden. [29, S. 7]
Auf dem ersten Platz mit dem meisten Vorkommen befindet sich in der Umfrage von eco Ransomware mit 21 %. Webseiten-Hacking und Datendiebstahl folgen dicht dahinter mit jeweils 18 %. Den dritten Platz mit jeweils 14 % belegen DDoS und sonstige Angriffe. CEO Fraud macht 11 % und Wirtschaftsspionage einen Anteil von vier Prozent aus. Eine Abbildung 3.18 dieser Werte befindet sich weiter vorn. [30, S. 10]
Für die Betrachtung der Angriffsarten im Gesellschaftsbereich eignen sich die IT- und Cybersicherheitsstudie des Bitkom e.V. und das Digitalbarometer des BSI.
Die IT-und Cybersicherheitsstudie liefert das Ergebnis, dass Schadprogramminfektionen mit 47 % am meisten vorgekommen sind. Eine weitere große Gefahr geht von ungefragter Datenweitergabe an Dritte mit 39 % aus. Keine Erfahrungen mit Internetkriminalität haben lediglich 21 % der Befragten gemacht. Diese Werte sind in Abbildung 3.26 nachzulesen. [34, S. 7]
Die Angriffswerte im Digitalbarometer 2022 in Abbildung 3.31 beziehen sich auf die Befragten, die innerhalb der vergangenen zwölf Monate von Internetkriminalität betroffen waren. Wie bereits erwähnt, sind das 29 % der Befragten. Deshalb müssen alle Prozentwerte noch auf diese 29 % berechnet werden, um Aussagen darüber treffen zu können, wie viele Prozent der Befragten 2021 von einer Angriffsart betroffen waren. An erster Stelle mit jeweils 2,3 Prozent der Befragten befindet sich Online-Shopping-Betrug und Phishing. Fremdzugriffe auf Online-Accounts folgen mit 1,7 Prozent und Schadsoftwareinfektionen mit 1,5 Prozent. [36, S. 9]
Als Übersicht für den Vergleich der vorgekommenen Angriffsarten dienen die folgenden Tabellen 3.2 im wirtschaftlichen Bereich und 3.3 für Privatpersonen.

Tabelle 3.2: Angriffsarten in der Wirtschaft 2021 [29, S. 7], [30, S. 10]

Wirtschaftsschutz 2022		eco Umfrage 2022	
Angriffe auf Passwörter	25 %	Ransomware	21 %
Phishing	25 %		
Schadsoftwareinfektion	25 %	Webseiten-Hacking	18 %
		Datendiebstahl	18 %
DDoS	21 %		
		DDoS	14 %
Spoofing	15 %	Sonstiges	14 %
Cross-Site-Scripting	14 %	CEO Fraud	11 %
SQL-Injektion	14 %		
		Wirtschaftsspionage	4 %
Ransomware	12 %		
Man-in-the-middle-Angriff	10 %		
CEO Fraud	5 %		

Tabelle 3.3: Angriffsarten in der Gesellschaft 2021 [34, S. 7], [36, S. 9]

IT- & Cybersicherheit 2021		Digitalbarometer 2022	
Schadprogramminfektion	47 %	Betrug beim Onlineshopping	2,3 %
		Phishing	2,3 %
ungefragte Datenweitergabe	39 %		
		Fremdzugriff auf Online-Accounts	1,7 %
keine Erfahrung	21 %		
		Schadsoftwareinfektion	1,5 %
Betrug bei privaten Einkäufen	19 %		
		Betrug mittels Messenger-Dienst	1 %
Betrug beim Online-Banking	15 %	Cybermobbing	1 %
		Ransomware	1 %
Ausspionieren von Zugangsdaten	14 %	Problematische Inhalte	1 %
		Smishing	0,9 %
		Betrug durch falsche Supportmitarbeitende	0,9 %
		Cyber-Stalking	0,6 %
		Sonstiges	0,3 %

Bei der Betrachtung dieser Werte fallen deutliche Unterschiede auf. Daher ist es sinnvoll, die beiden Tabellen mit ihren Werten getrennt voneinander zu analysieren.
Im Wirtschaftsbereich sind als Gemeinsamkeit geringe Vorkommen von CEO Fraud zu verzeichnen. Außerdem ist die Angriffsart DDoS in beiden Umfragen auf den vorderen Plätzen, also mit erhöhtem Vorkommen, vertreten. Die Unterschiede sind vielfältig. Es ist zu beobachten, dass die Angriffsarten in beiden Berichten sehr unterschiedlich sind und damit schwer miteinander vergleichbar sind. Außerdem variiert die Anzahl der Angriffsarten in den Berichten. Die Wirtschaftsschutzstudie nimmt eine Unterscheidung zwischen Schadprogramminfektion und Ransomware vor, die Umfrage von eco nicht. Dabei ist festzustellen, dass sich im Bericht zum Wirtschaftsschutz Schadsoftwareinfektion mit 25 % ganz vorn befindet, hingegen Ransomware mit 12 % weiter hinten. Im Bericht von eco ist Ransomware ganz vorn mit 21 % festzustellen. Schadsoftwareinfektionen und speziell Ransomware sind demnach eine vorherrschende Bedrohung in der Wirtschaft. Weiterhin können Cross-Site-Scripting und SQL-Injektion im Wirtschaftsschutzbericht als Kategorien von Webseiten-Hacking in der eco Umfrage verstanden werden. Diese unterscheiden sich in den konkreten Prozentwerten nur gering, aber in der Platzierung mit den anderen Angriffsarten stark. Die Kategorien Angriffe auf Passwörter und Phishing mit jeweils 25 % und Man-in-the-middle-Angriffe können der Kategorie Datendiebstahl mit 18 % zugeordnet werden. Dabei geht es um mögliche Angriffsvektoren, die Datendiebstahl ermöglichen. Mit der Ausnahme von Man-in-the-middle-Angriffen, einem sehr speziellen Angriffsvektor, sind diese weit verbreitet und auf den vorderen Plätzen zu finden. Hinsichtlich der Unterschiede ist zudem erkennbar, dass die Prozentwerte der eco-Umfrage zu 100 % summiert werden können. Dieser Sachverhalt legt nahe, dass keine Mehrfachnennung in dieser Frage der Umfrage möglich

war. Dazu sind keine Informationen in der Umfrage zu finden. Weiterhin ist anzumerken, dass der Umfang der Befragten sich deutlich unterscheidet. Die Wirtschaftsschutzumfrage umfasst 1066 Unternehmen, während die Umfrage von eco lediglich 145 umfasst.
Bei der Betrachtung des gesellschaftlichen Bereichs fällt auf, dass Schadprogramminfektionen weit verbreitet sind. Außerdem gehen Gefahren von Betrug bei Einkäufen, Online-Banking, mittels Messenger-Dienste und durch falsche Supportmitarbeitende aus. Im Allgemeinen ist zu beobachten, dass sich die Prozentwerte deutlich unterscheiden. Auffällig ist, dass im Digitalbarometer alle Werte sehr klein sind. Auch hier ist anzumerken, dass die Zahl der Befragten unterschiedlich ist. Für die IT- und Cybersicherheitsumfrage wurden 1011 Internetnutzende und für das Digitalbarometer wurde ungefähr die doppelte Anzahl befragt. Zudem unterscheiden sich die Antwortmöglichkeiten sehr stark, nicht nur in der Anzahl, und sind damit schwer zu vergleichen.

3.10.3 Malware

Das Bundeslagebild Cybercrime 2021 beschreibt Malware als eines der primären Werkzeuge um Cybercrime-Straftaten zu begehen. Die bedeutendsten Malware-Typen sind demnach Ransomware, RAT und Info-Stealer. Dabei wird der Zugang zu Systemen mit der Malware eröffnet, um Daten abzuleiten und diese anschließend für nachgelagerte Angriffe zu verkaufen. [10, S. 18] Außerdem wird auf die Abwehr-Indizes des BSI zum Aufkommen von Malware-Angriffen auf die Netze des Bundes und präventive Sperrungen von maliziösen Webseiten verwiesen. Abgewehrte Schadprogramm-Angriffe haben demnach besondere Höhepunkte im März und November 2021, Sperrungen maliziöser Webseiten im März und August 2021. Jedoch ist ein Rückgang im Vergleich zum Vorjahr in den Zahlen der abgewehrten Malware-Angriffe um 40 % und um 12 % bei den Sperrungen von Webseiten zu verzeichnen. [10, S. 14–15]
Die Lageberichte des BSI beinhalten eine Beschreibung der Entwicklung der Produktion von neuen Schadprogrammen. Eine grafische Darstellung des Verlaufs ist in Abbildung 3.3 zu finden. Der tägliche Zuwachs im Zwölf-Monatsdurchschnitt lag bei 409 500 neuen Malwarevarianten. Der höchste bisher gemessene Wert mit 553 000 neue Varianten pro Tag war im Monat Februar. [23, S. 11–12]
Ein bedeutendes Ereignis in diesem Bereich war die Zerschlagung der Infrastruktur der Schadsoftware Emotet im Januar 2021. [5, S. 54]
Im Cyber Security Report 2021 sehen 76 % eine große Bedrohung durch Schadsoftware oder Computerviren. Damit belegen diese Angriffsarten den zweiten Platz in der Aufstellung der größten Cyber-Risiken, wie Abbildung 3.10 darstellt. [28, S. 6–7]
Schadsoftwareinfektionen sind im Wirtschaftsschutzbericht mit 25 % neben zwei weiteren Angriffsarten am meisten verbreitet. Anzumerken ist dabei, dass dieser Prozentwert um sechs Prozentpunkte im Vergleich zum Vorjahr abgenommen hat. Schadsoftwareinfektionen sind also leicht zurückgegangen. [29, S. 7]
Auf die Frage nach stattgefundenen Angriffen 2021 antworten 27 % der befragten KMU, dass sie einige Probleme mit Schadsoftware hatten. [31, S. 10]
Im Bericht zur IT- und Cybersicherheit zeigt sich, dass stattgefundene Infizierungen mit Schadprogrammen im Vergleich der vergangenen zwei Jahre immer ähnliche Prozentwerte haben und am meisten verbreitet sind. Knapp die Hälfte der Befragten war von derartigen Angriffen betroffen. [34, S. 7–8]
Auch im Digitalbarometer wird deutlich, dass unter den im Jahr 2021 stattgefundenen Straftaten Schadsoftwareinfektionen weit vorn zu finden sind. Unter den Straftaten, die schon länger zurückliegen, befindet sich diese Angriffsart auf dem ersten Platz. [36, S. 9]

Allgemein ist festzustellen, dass Malware-Angriffe sowohl im Privatbereich als auch in der Wirtschaft mehr geworden sind oder auf einem ähnlichen Niveau geblieben sind. Als Ausnahme sticht hierbei die Studie zum Wirtschaftsschutz hervor. Demnach sind stattgefundene Schadsoftwareinfektionen im Vergleich zum Vorjahr weniger geworden. Zudem sind rückläufige Zahlen in den Netzen des Bundes bei abgewehrten Malware-Angriffen und der Sperrung maliziöser Webseiten festzustellen. Weiterhin ist anzumerken, dass die konkreten Prozentwerte deutlich variieren. Das ändert jedoch nichts an der Feststellung, dass diese Angriffsart häufig vorkommt. Besonders im Betrachtungsjahr 2021 ist die Produktion neuer Malware-Varianten deutlich gestiegen.

3.10.4 Ransomware

Ein bekannter Malwaretyp ist Ransomware. Das Bundeslagebild Cybercrime fokussiert 2021 Ransomware als primäre, gesamtgesellschaftliche Bedrohung im Cybercrime-Bereich. Das Bedrohungs- und Schadenspotenzial ist erneut deutlich angestiegen. [10, S. 2] Ransomware ist nicht nur in Fachkreisen bekannt, sondern auch in den Medien ein populäres Thema. Die Erpressungsvariante Double Extortion etablierte sich als Standard-Modus-Operandi. Im Fokus der Angreifenden standen im Berichtsjahr besonders das Finanzwesen, der Einzelhandel, öffentliche Einrichtungen und das verarbeitende Gewerbe. Tendenziell fokussieren Angreifende eher größere Unternehmen, aber auch Angriffe auf KRITIS und öffentliche Verwaltungen stehen ab dem Sommer 2021 zunehmend im Fokus. [10, S. 20]
Der Lagebericht 2022 des BSI sieht Ransomware als größte Cyber-Bedrohung für Staat, Wirtschaft und Gesellschaft. [5, S. 14] Die im Lagebericht 2021 als neue Entwicklung dargestellte Double Extortion ist im darauffolgendem Lagebericht zum Regelfall geworden. [5, S. 14] Außerdem fokussieren sich Angreifende auf finanzstarke Opfer, um möglichst hohe Lösegelder zu erpressen. [23, S. 12] Weiterhin wird vermehrt RaaS beobachtet. [5, S. 14] Herausragende Ereignisse waren ein Ransomware-Angriff im Juni 2021 auf eine deutsche Kreisverwaltung und im November auf ein Handelsunternehmen. Außerdem gab das BSI eine Warnung vor vermehrten Ransomware-Angriffe zur Weihnachtszeit heraus. [5, S. 54–55]
Bei stattgefundenen Angriffen im Bericht zum Wirtschaftsschutz befindet sich Ransomware mit 12 % im hinteren Mittelfeld. Außerdem ist der Wert verglichen mit dem Vorjahr um sechs Prozentpunkte gesunken. [29, S. 7] Dafür sieht mehr als die Hälfte (59 %) der Befragten diese Angriffsart als sehr bedrohlich in der Zukunft. Damit stellt das in dieser Umfrage die größte Bedrohung dar. [29, S. 14]
In der Umfrage von eco ist Ransomware die am meisten stattgefundene Angriffsart 2021 mit 21 %. [30, S. 7] Im Vergleich mit den Vorjahren ist festzustellen, dass Ransomware zwar weiterhin die größte Bedrohung darstellt, jedoch weniger signifikant als in den Vorjahren. Im Vorjahr betrug der Prozentwert 35 %, also ist eine deutliche Verringerung zu verzeichnen. [30, S. 10]
Beim Vergleich dieser Punkte fällt als Gemeinsamkeit auf, dass nach dem Wirtschaftsschutzbericht und dem Bericht von eco Ransomware-Angriffe 2021 leicht abgenommen haben. Ransomware als am meisten stattgefundene Angriffsart im eco-Bericht korreliert mit den Aussagen des Bundeslageberichts vom BKA und den Lageberichten vom BSI über Ransomware als Hauptbedrohung. Im Bericht zum Wirtschaftsschutz wird ähnlich dazu Ransomware als sehr starke Bedrohung für die Zukunft wahrgenommen. Unterschiedlich sind die Prozentwerte im Vergleich der Angriffsarten. Auch befindet sich Ransomware im Wirtschaftsschutzbericht nicht an erster Stelle der verbreitetsten Angriffe. Im gesellschaftlichen Bereich der Studien sind keine Angaben speziell zu Ransomware zu finden. Daher lässt sich dafür keine Aussage treffen. Allgemein lässt sich jedoch sagen, dass der Konsens, Ransomware als starke Bedrohung für alle, von allen Berichten dargestellt wird.

3.10.5 Data-Leaks und Datensicherheit

Das Bundeslagebild Cybercrime 2021 berichtet zum Thema Data-Leaks und Datensicherheit von externen Quellen, in diesem Fall vom Identity Leak Checker des HPI [15]. Dieses System erfasst jeden Monat Millionen von Data-Leaks kompromittierter Konten. Insgesamt wurden 2021 ca. 184,65 Millionen kompromittierte Nutzerkonten festgestellt. [10, S. 12]
Im Lagebericht 2021 wird von einer Steigerung um fast 360 % im Bereich der monatlich aktiven Data-Leak-Seiten berichtet. [23, S. 13] Ursächlich ist demnach die Entwicklung im Ransomware-Bereich hin zu Double Extortion. Es wird nicht nur mit der Veröffentlichung der Daten gedroht, sondern diese in einzelnen kleinen Teildatensätzen tatsächlich veröffentlicht. [5, S. 14] Zudem erwähnt der Lagebericht 2022 eine Rückgang von Data-Leaks im Januar mit anschließender Zunahme und erneutem Rückgang im Mai 2021. Dies ist demnach auf die Abschaltung einer Reihe von RaaS-Angeboten zurückzuführen. [5, S. 16–17]
Bei den größten Cyber-Risiken für Menschen in Deutschland 2021 in der Umfrage von Deloitte in Abbildung 3.10 befindet sich Datenbetrug im Internet mit 77 % auf Platz eins. [28, S. 6–7]
Im Wirtschaftsschutzbericht geben bei der Betrachtung der Verschiebung von Angriffen in den digitalen Raum 36 % der Befragten an, innerhalb der letzten zwölf Monate von Diebstahl sensibler digitaler Daten oder Informationen betroffen gewesen zu sein und 27 % waren vermutlich betroffen. [29, S. 3] Außerdem wird in diesem Bericht Datendiebstahl genauer untersucht. Es wird die Frage gestellt, welche Arten von digitalen Daten gestohlen wurden. In Abbildung 3.12 befindet sich die dazugehörige Grafik. Am meisten wurden mit 68 % Kommunikationsdaten wie beispielsweise E-Mails gestohlen. An zweiter Stelle folgen Kundendaten mit 45 %. Auffällig ist, dass im Vergleich über die vergangene Jahre hinweg immer Kommunikationsdaten Diebstahlobjekt Nummer eins darstellen. Jedoch schwankt die Reihenfolge der weiteren Datenarten. [29, S. 4]
Die Umfrage von eco ergibt, dass Datendiebstahl am zweithäufigsten mit 18 % stattgefunden hat. [30, S. 7]
Die Umfrage zur IT- und Cybersicherheit thematisiert das Vertrauen für persönliche Daten im Internet allgemein. Dabei ist ein Anstieg von neun Prozentpunkten auf 77 % bei den Befragten, die ihre Daten für unsicher halten, festzustellen. [34, S. 2] Zusammenfassend lässt sich sagen, dass in jeder Kategorie das Misstrauen überwiegt und von einem großen Misstrauen gegenüber Netzwerken, Verwaltung und Polizei ausgegangen werden kann. Am größten ist das Vertrauen in Online-Händler (47 %), bei denen Befragte bestellten, und den eigenen E-Mail-Anbietern (46 %). Das Misstrauen ist in die selbst genutzten sozialen Netzwerke (68 %) am größten. [34, S. 3] Außerdem wird die Frage nach der Zuständigkeit für den Schutz persönlicher Daten gestellt. Der größte Teil (88 %) sieht sich dafür selbst in der Verantwortung, acht Prozent den Staat und zwei Prozent wirtschaftliche Akteure wie etwa Dienstleister. Mit Blick auf die Vorjahre wird eine Verlagerung dieser Zuständigkeit hin zur Selbstverantwortung deutlich. [34, S. 4] Bei der Frage nach stattgefundenen Angriffen 2021 zeigt sich, dass ein großer Teil (39 %) Opfer von ungefragter Datenweitergabe wurde. Damit befindet sich diese Angriffsart, nach ihrem Vorkommen sortiert, auf Platz zwei. [34, S. 7–8]
Schlussfolgernd ist festzustellen, dass die steigenden Zahlen in diesem Bereich auf das große Risiko des Datenbetrugs hindeuten. In diesem Zusammenhang erklärt sich das große Misstrauen in Institutionen und das Internet, was den Schutz persönlicher Daten angeht. In der Wirtschaft kommen zwei Berichte zum gleichen Ergebnis, dass Datendiebstahl und -betrug 2021 am zweithäufigsten stattgefunden haben. Beim Thema Datendiebstahl sind die Datenarten aufgrund fehlender Daten nicht vergleichbar.

3.10.6 Distributed Denial of Service (DDoS)-Angriffe

Wie das Bundeslagebild Cybercrime erklärt, entwickeln sich DDoS-Angriffe sowohl qualitativ als auch quantitativ steigernd. Besonders im ersten und dritten Quartal des Jahres 2021 wurden überdurchschnittlich hohe Angriffszahlen verzeichnet. [10, S. 23–24] Außerdem werden DDoS-Angriffe wegen der Angriffe im Zusammenhang mit Ransomware, sogenanntes Triple Extortion, weitaus relevanter gesehen als in den Vorjahren. [10, S. 25]
Laut dem Lagebericht des BSI stellt DDoS weiterhin eine der Hauptbedrohungen für die Cyber-Sicherheit dar. Trotz der größeren Angriffsfläche seit der verstärkten Umsetzung von Home-Office ist keine besondere Steigerung in der Angriffszahl in Deutschland zu beobachten. Jedoch wurden erstmals langanhaltende DDoS-Erpressungskampagnen als eine Art Schutzgelderpressung registriert. Der Maximalwert der gemessenen Bandbreite von DDoS-Angriffen trat am 02. Dezember 2021 mit über 290 000 Mbits und einer Dauer von 228 Minuten auf. Die durchschnittlichen Bandbreiten über alle Angriffe gemittelt sinken tendenziell. Das hängt mit der Veränderung der Angriffe zusammen. Es wird nicht mehr auf hohe Bandbreite gezielt, sondern zunehmend mit geringer Bandbreite auf Netzwerk- und Transportebene gearbeitet. Besonders in umsatzstarken Zeiten wie der Vorweihnachtszeit und vor Online-Events wie dem Black Friday wurden vermehrt DDoS-Attacken beobachtet. [5, S. 41–43] Das BSI warnte im Dezember 2021 vor vermehrten DDoS-Angriffen.
DDoS-Angriffe befinden sich in der Umfrage zum Wirtschaftsschutz mit 21 % auf dem zweiten Platz der stattgefundenen Angriffe. Sie sind somit eine ernstzunehmende Bedrohung. Jedoch ist anzumerken, dass dieser Prozentwert im Vergleich zum Vorjahr um sechs Prozentpunkte gesunken ist. [29, S. 7]
Auch in der eco-Umfrage wird deutlich, dass DDoS-Attacken weit verbreitet sind. Diese Angriffsart belegt mit 14 % den dritten Platz. Hinsichtlich der zeitlichen Entwicklung ist festzustellen, dass sich DDoS-Angriffe im Vergleich zum Vorjahr gesteigert haben. [30, S. 10]
Im Vergleich der Ergebnisse der Berichte ist zu bemerken, dass DDoS-Attacken im Allgemeinen zum einen qualitativ als auch quantitativ gestiegen sind. Das zeigt auch die Entwicklung in der Umfrage von eco. Hingegen fällt dazu der Widerspruch im Ergebnis der sinkenden Zahlen in der Wirtschaftsschutzstudie auf. Allgemein lässt sich jedoch feststellen, dass DDoS-Angriffe in beiden Umfrage im wirtschaftlichen Bereich ein hohes Vorkommen aufweisen.

3.10.7 IT-Schwachstellen

IT-Schwachstellen stellen einen weiteren Eintrittsvektor für Cybercrime dar. Im Bundeslagebild Cybercrime wird auf eine Veröffentlichung des IT-Security-Dienstleisters Trend Micro [17] verwiesen. Aus dieser geht hervor, dass die Anzahl der entdeckten IT-Schwachstellen seit 2017 enorm ansteigt. Eine schwerwiegende Schwachstelle im Jahr 2021 bildet die im Dezember 2021 entdeckte Schwachstelle Log4Shell. [10, S. 15–17]
Der Lagebericht zur IT-Sicherheit 2021 berichtet von kritischen Schwachstellen in Microsoft Exchange, welche mit Sicherheitsupdates im März 2021 gepatcht wurden. [23, S. 26–29] Auch die Schwachstelle Log4Shell wird vorgestellt. Diese zog im Dezember 2021 eine Warnung des BSI mit der höchsten Warnstufe nach sich. [5, S. 37] Grundsätzlich steigt die Zahl bekannt gewordener Schwachstellen. Ein enormer Anstieg der Meldezahlen beim BSI auf das 5,5-fache ist mutmaßlich zum größten Teil auf die Einführung eines neue Online-Meldeformulars zurückzuführen. Die Lage wird als überdurchschnittlich bedrohlich eingeschätzt. Zudem wurden verschiedene Software- und Hardware-Schwachstellen entdeckt. [5, S. 35, 38]

Zero-Day-Exploits stellen für 55 % der Befragten der Wirtschaftsschutz-Umfrage eine sehr starke Bedrohung für die IT-Sicherheit in Zukunft dar. Damit sind sie auf dem zweiten Platz der Bedrohungen. [29, S. 14]
Alle weiteren Berichte enthalten keine Informationen zu diesem Eintrittsvektor von Cybercrime.
Zum Vergleich bleibt deshalb nicht viel zu sagen. Die Berichte von BKA und BSI beschreiben die steigende Anzahl neuer Schwachstellen und gehen auf besondere Entdeckungen in diesem Bereich wie Log4Shell und Schwachstellen in Microsoft Exchange ein. Die Bedrohlichkeit von Schwachstellen wird auch im wirtschaftlichen Bereich gesehen.

3.10.8 Phishing und Spam

Nach dem Bundeslagebild Cybercrime stellt Phishing einen der Haupteintrittsvektoren 2021 dar. Die APWG [16] stellt fest, dass die Zahl neu bekannt gewordener Phishing-Webseiten seit Beginn der Corona-Pandemie stark angestiegen ist. Bei der Beobachtung des Spam-Niveaus im Spam-Mail-Index des BSI fällt ein hohes Spam-Aufkommen bis zum Sommer 2021 auf. Die Sommer- und Herbstmonate über sank dieses und stieg gegen Ende des Jahres wieder graduell an. [10, S. 15]
Der Lagebericht 2021 berichtet von Sextortion-Kampagnen im Januar, März und Mai 2021. [23, S. 19]
Aus der Grafik im Lagebericht 2022 mit einer Aufteilung von Spam nach Kategorien geht hervor, dass Erpressungs-Spam mit 36 % den größten Teil ausmacht. Danach folgt mit geringem Abstand Betrug mit 33 % und mit größerem Abstand Werbungs-Spam mit 16 %. [5, S. 27] Den größten Teil von Erpressungs-Mail umfassen Sextortion-Mails mit 76 %. Phishing-Mails machen in der Kategorie Betrugs-Mails 90 % aus. [5, S. 27] Besondere Höhepunkte der Spam-Wellen in der Wirtschaft sind im Januar, März, Mai, Juli und besonders stark im Dezember zu beobachten. Das zeigt Abbildung 3.7. Dazu im Vergleich ist die Spam-Ratio der Bundesverwaltung in Abbildung 3.8 dargestellt. Die Kurve dieser beiden Diagramme verläuft ähnlich, jedoch unterscheiden sich die genauen Zahlen. Im Februar 2021 bewirkte die Zerschlagung des Botnetzes Emotet in beiden Bereichen eine Entspannung mit niedrigeren Zahlen. Die Sextortion-Kampagnen im Januar, März und Mai sind an den Peaks in beiden Grafiken erkennbar. Der besondere Anstieg im Dezember ist auf eine Sextortion-Kampagne und dem zunehmenden Wiederaufbau des Botnetzes Emotet zurückzuführen. [5, S. 84–86] Der deutlich höhere Wert im März bei der Spam-Ratio der Bundesverwaltung steht im Zusammenhang mit einer Spam-Mail-Angriffswelle mit Bounce-Mails. [23, S. 69–70]
Im Bericht zum Wirtschaftsschutz werden die Kommunikationswege beim Social Engineering betrachtet. Diese Untersuchung zeigt, dass die beliebtesten Wege per Telefon mit 38 % und per E-Mail mit 34 % sind. [29, S. 8] Zudem befindet sich Phishing mit 25 % mit an erster Stelle bei den stattgefundenen Angriffen 2021. [29, S. 7] Des Weiteren sehen 63 % der Befragten eine hohe Bedrohlichkeit von Social Engineering für die Zukunft. [29, S. 14]
Phishing meint das Ausspionieren von Zugangsdaten. In der Umfrage zur IT- und Cybersicherheit geben 14 % der Befragten an, 2021 davon betroffen gewesen zu sein. Diese Angriffsart befindet sich im Ranking der stattgefundenen Angriffe auf dem letzten Platz. [34, S. 7]
Im Digitalbarometer hingegen geben mit 2,3 Prozent die meisten der Befragten an, 2021 von Phishing betroffen gewesen zu sein. Angreifende setzten dabei verschiedene Betrugsarten ein. Dazu gehören betrügerische E-Mails (19 %), gefälschte Nachrichten über Messenger (11 %) oder SMS (10 %) sowie durch vermeintliche Support-Mitarbeitende (9 %). Mehr als die Hälfte (62 %) stimmt der Aussage zu, schon einmal betrügerische Phishing-Mails erhalten zu haben, ohne darauf eingegangen zu sein. Außerdem geben 0,9 Prozent der Befragten an, 2021 von Smishing betroffen gewesen zu sein. [36, S. 8]

Allgemein lässt sich sagen, dass Phishing und Spam 2021 zugenommen haben. Diese Aussage vertreten das Bundeslagebild Cybercrime 2021 und die Lageberichte des BSI 2021 und 2022. Weiterhin ist anzumerken, dass diese drei Berichte zu großen Teilen auf den selben Daten des BSI basieren und daher Überschneidungen zwangsläufig sind. Im wirtschaftlichen Bereich können keine weiteren Aussagen getroffen werden, da dieses Thema nur in einem Bericht thematisiert wird. Bei den stattgefundenen Angriffe im gesellschaftlichen Bereich ist festzustellen, dass die beiden Berichte IT- und Cybersicherheit und Digitalbarometer zu unterschiedlichen Ergebnissen kommen. Dies stellt jedoch keinen außergewöhnlichen Sachverhalt dar, denn wie bei anderen Vergleichsaspekten bereits erwähnt, unterscheiden sich die Umfragen in ihren Antwortmöglichkeiten sehr. Jedoch ist zu beobachten, dass sowohl im Wirtschaftsschutzbericht als auch im Digitalbarometer Phishing an erster Stelle bei den stattgefundenen Angriffen steht. Außerdem ist zu beobachten, dass E-Mails in diesen beiden Berichten als beliebtes Kommunikationsmittel für Phishing gelten.

3.10.9 Supply-Chain-Angriffe

Beim Thema Supply-Chain-Angriffe ist kein aussagekräftiger Vergleich möglich oder notwendig. Lediglich der Bericht des BKA und die Berichte des BSI gehen auf diese Themengebiet ein. Zusammenfassend ist zu sagen, dass von derartigen Angriffen aus verschiedenen, bereits genannten Gründen, eine große Bedrohung ausgeht. Außerdem berichten beide Berichte von dem Angriff auf das amerikanische Unternehmen Kasey Ltd. und seiner Software VSA im Sommer 2021. [10, S. 28–29]

3.10.10 Botnetze, Advanced Persistent Threats (APT) und hybride Bedrohungen

Das Thema Botnetze wird lediglich in den Lageberichten des BSI thematisiert und bietet daher keine Möglichkeit zum Vergleich.
Das gleiche gilt für APT und hybride Bedrohungen.

3.10.11 Täterkreis

Bei der Betrachtung des Täterkreises kommt das Bundeslagebild Cybercrime zu dem Ergebnis, dass eine klare Unterscheidung der Tätergruppierungen schwierig ist. Aufgrund der zunehmenden Professionalität und neuen Angeboten wie MaaS entwickeln sich die Gruppierungen auf ein ähnliches Niveau hin. Als Unterscheidungsmerkmal eignet sich lediglich die Motivationslage. Anhand dieses Merkmals lassen sich Tätergruppierungen in drei Bereiche kategorisieren: unabhängige Cyberkriminelle, staatliche Akteure und im Mittelfeld State-Sponsored-Gruppierungen. [10, S. 30–31]
Im Wirtschaftsschutzbericht konnte zum Ursprung von 35 % der Angriffe keine Aussage getroffen werden. Im Ländervergleich befindet sich China mit 43 % an erster Stelle. Russland mit 36 % wird dicht gefolgt von Deutschland mit 32 %. Osteuropäische Länder, Russland davon ausgenommen, sind mit 27 % noch vor den USA mit 21 %. EU-Ländern, ausgenommen von Deutschland, machen lediglich acht Prozent aus. Besonders bei Russland und China sind große Anstiege von jeweils 13 Prozentpunkten zu verzeichnen, wobei alle Gebiete zumindest leichte Anstiege verzeichnen. Die Untersuchung der Täterkreise in Abbildung 3.15 ergibt, dass besonders organisierte Kriminalität zugelegt hat. Damit befindet sich diese Gruppierung an erster Stelle und verzeichnet einen Anstieg von 22 Prozentpunkten im Vergleich zum Vorjahr. Danach reihen sich die bisherigen größten Bedrohungen Privatpersonen mit 38 % und unabsichtlich handelnde Beschäftigte mit 36 % ein. An vierter

Stelle befinden sich vorsätzlich handelnde Beschäftigte mit 26 %. Danach folgen konkurrierende Unternehmen mit 14 %, Kunden mit 11 % und ausländische Nachrichtendienste mit acht Prozent. Sehr wenig Vorfälle sind durch Lieferanten mit drei Prozent und externe Dienstleister mit ein Prozent zu verzeichnen. [29, S. 10–11]
In der Umfrage von eco stehen profitgetriebene Cyberkriminelle mit 83 % an erster Stelle. Einen weiteren großen Täterkreis stellen unbeabsichtigte Innentäter, sogenannte Cyber-Unfälle, mit 50 % dar. Weniger stark vertreten sind internationale Wirtschaftsspionage mit 25 % und absichtliche Innentäter mit 18 %. [30, S. 11]
Mit Tabelle 3.4 folgt eine Übersicht der genannten Tätergruppierungen.

Tabelle 3.4: Tätergruppierungen [29, S. 10–11], [30, S. 11]

Wirtschaftsschutz 2022		eco Umfrage 2022	
organisierte Kriminalität	51 %	profitgetriebenen Cyberkriminelle	83 %
Privatperson/Hobby-Hacker	38 %	unbeabsichtigte Innentäter (Cyber-Unfälle)	50 %
unabsichtlich handelnde (ehemalige) Beschäftigte	36 %	Internationale Wirtschaftsspionage	25 %
vorsätzlich handelnde (ehemalige) Beschäftigte	26 %	absichtliche Innentäter	18 %
Konkurrierende Unternehmen	14 %		
Kunden	11 %		
ausländischer Nachrichtendienst	8 %		
Lieferanten	3 %		
externe Dienstleister	–		

Beim Vergleich dieser Ergebnisse fällt auf, dass als Gemeinsamkeit in den beiden wirtschaftlichen Studien jeweils auf den vorderen Plätzen beim Täterkreis organisierte Kriminalität und Privatpersonen bzw. profitgetriebene Cyberkriminelle stehen. Dabei ist anzumerken, dass auch andere Täter profitorientiert handeln können. Des Weiteren finden häufig Cyberunfälle durch unbeabsichtigt handelnde Beschäftigte in beiden Umfragen statt. Zur internationalen Wirtschaftsspionage können konkurrierende Unternehmen und ausländische Nachrichtendienste zugeordnet werden. Diese befinden sich im hinteren Mittelfeld. Als Unterschiede stellen sich die Angaben zu absichtlichen Innentätern heraus. Als mögliche Gründe für die Unterschiede sind die unterschiedliche Anzahl der Befragten und die verschiedenen Antwortmöglichkeiten zu nennen. Außerdem ist in diesem Themengebiet von einer gewissen Ungenauigkeit auszugehen, da nicht alle Angriffe zurückverfolgt werden können. Zudem sind Tätergruppierungen nicht mehr eindeutig voneinander differenzierbar, wie das

Bundeslagebild Cybercrime 2021 verdeutlicht. Ein Ländervergleich ist durch fehlende Daten nicht möglich. Dazu lässt sich jedoch sagen, dass im Lagebericht 2021 des BSI von mindestens vier unterschiedlichen Ursprungsländern für Angriffe auf deutsche Regierungsbehörden berichtet wird [23, S. 28–29].

3.10.12 Schäden und Folgen von Angriffen

Allgemein ist zu sagen, dass der Phänomenbereich Cybercrime ein hohes Schadenspotenzial bietet. Das Schadensausmaß ist auf Grundlage der PKS nicht valide einschätzbar. Außerdem stellt die PKS lediglich das Hellfeld dar und Folgeschäden sind nicht abschätzbar. An dieser Stelle wird sich im Bundeslagebild Cybercrime auf externe Quellen gestützt. Demnach liegt die Schadenssumme, basierend auf Werten des Bitkom e.V., bei 223,5 Milliarden Euro im Berichtszeitraum 2020/2021. [10, S. 34–35]
Auch die Lageberichte des BSI liefern bezüglich der Schadenssummen keine absoluten Zahlen. Denn diese gestalten sich grundsätzlich schwierig, da von einer hohen Dunkelziffer ausgegangen wird und einzelne Statistiken von IT-Sicherheitsdienstleistenden lediglich den eigenen Kundenstamm einbeziehen. Grundsätzlich ist zu sagen, dass die erpressten Lösegelder zunehmen. [5, S. 16]
Im Wirtschaftsschutzbericht stimmen 45 % der Befragten der Aussage zu, dass Cyberattacken die Unternehmensexistenz bedrohen. Im Vorjahr taten dies nur neun Prozent. [29, S. 5] Bei der Schadensbetrachtung summiert sich ein Gesamtschaden von 202,7 Milliarden Euro pro Jahr. Eine Aufschlüsselung der Schäden ist in Abbildung 3.14 zu sehen. Es ist festzustellen, dass die Gesamtschadenssumme im Vergleich zum Vorjahr leicht gesunken ist. Den meisten Schaden bewirken Ausfall, Diebstahl oder Schädigung von Betriebsabläufen oder Systemen für die Produktion und Umsatzeinbußen als Folge vom Verlust von Wettbewerbgsvorteilen mit jeweils 20 %. Weiterhin entstehen durch negative Medienberichterstattung und damit einhergehenden Imageschäden 11 % und durch Umsatzeinbußen durch nachgemachte Produkte 10 % der Schäden. Fünf Prozent der Gesamtsumme machen zudem Erpressungen mit gestohlenen oder verschlüsselten Daten aus. [29, S. 9]
In der Umfrage von eco geben 30 % der Befragten an, nach Cyber-Angriffen leichte Schäden erlitten zu haben. Für fünf Prozent folgten erhebliche wirtschaftliche Schäden und mehr als die Hälfte erlitt keinerlei Schaden (55 %). Eine grafische Darstellung der Schäden ist in Abbildung 3.19 zu finden. In unter 10 % wurden zumindest Teile des Schadens von einer Cyberversicherung aufgenommen. [30, S. 8] Das Schadensniveau ist für 37 % etwa gleichbleibend im Vergleich zum vorherigen Jahr. 11 % sind der Meinung, die Schäden seien mindestens leicht gestiegen und sieben Prozent nehmen eher eine Verringerung der Schäden wahr. [30, S. 9]
Der DsiN-Praxisreport stellt ein eher geringes Schadenspotenzial in Abbildung 3.22 dar. Mehr als die Hälfte hatte nach Angriffen geringen Aufwand und keine nachhaltigen Schäden (59 %). Knapp ein Viertel hatte mit keinerlei Konsequenzen zu kämpfen (24 %). Hingegen war der Aufwand für 13 % erheblich, aber nicht existenzbedrohend und vier Prozent erlitten schwere Belastungen. Hinsichtlich der Branchenzugehörigkeit zeigen sich bei den entstandenen Schäden deutliche Unterschiede. Die Hälfte aller Angriffe im Gastgewerbe bewirkten erheblichen Aufwand oder existenzbedrohende Zustände. Der Anteil derartiger Angriffe beträgt im Handelsgewerbe 21 %. In der Industrie sind mit 14 % und im Gesundheitsbereich mit 11 % noch geringere Anteile solcher Angriffe zu verzeichnen. [31, S. 11]
Das Digitalbarometer konzentriert sich nicht nur auf finanzielle Schäden von Cyber-Angriffen, sondern betrachtet die Folgen ganzheitlich. Das ist in Abbildung 3.32 zu sehen. Demnach erlitten 79 % der Opfer von Cyberangriffen im Jahr 2021 Schäden. An erster Stelle steht hier zeitlicher Schaden

mit 29 %, dicht gefolgt von Datenverlust mit 25 %. 13 % erlitten finanzielle Schäden. Diese wurden größtenteils durch Betrugsmaschen verursacht. Dabei beträgt der durchschnittliche Verlust 674 Euro. Finanzielle Schäden bei Schadsoftware belaufen sich meist bei unter 500 Euro und bei Datendiebstahl etwas mehr, üblicherweise unter 600 Euro. [36, S. 10]
Grundsätzlich ist hervorzuheben, dass konkrete Schadenssummen schwer zu beziffern sind. In der Wirtschaftsschutzstudie erfolgt der Versuch, absolute Zahlen aufzustellen. Dabei ist zu beachten, dass die Summe im Bundeslagebild Cybercrime und dem Bericht zum Wirtschaftsschutz aufgrund der gleichen Datengrundlage gleich sein sollte, jedoch bezieht sich das Bundeslagebild auf die Werte des Vorjahres. Interessanter Weise machen die Schadenssummen für Erpressung mit gestohlenen oder verschlüsselten Daten nur einen geringen Teil aus. Allgemein ist bei den Werten eine leichte Verringerung der Schadenssummen im Vergleich zum vorherigen Jahr festzustellen. In der Umfrage von eco wird das Schadensniveau eher gleichbleibend eingeschätzt. Insgesamt hat die Bedrohung der Unternehmensexistenz nach dem Wirtschaftsschutzbericht jedoch zugenommen. Außerdem sind die Prozentwerte der Befragten der Umfragen von eco und DsiN, die keine Folgen durch Angriffe hatten, sehr unterschiedlich. Hingegen sind bei bedrohlichen Schäden bzw. schweren Belastungen ähnlich niedrige Werte zu verzeichnen. Außerdem ist in beiden Umfragen eine recht hohe Zustimmung bei wenig Aufwand nach Angriffen festzustellen. Das Digitalbarometer zeigt mit 13 % einen geringen Teil, der finanzielle Schäden erleiden musste, jedoch mit 79 % einen sehr großen Teil derer, die überhaupt Schäden verzeichneten. Die Unterschiedlichkeit der Ergebnisse der Umfragen und Berichte kann einerseits damit begründet werden, dass, wie die Umfrage von DsiN bereits zeigt, die Branchenzugehörigkeit einen großen Einflussfaktor ausmacht. Außerdem sind, wie bei den anderen Vergleichsaspekten, die Umfänge der Befragungen verschieden. Im Allgemeinen können keine validen Aussagen zu konkreten Schadenssummen gemacht werden.

3.10.13 Investitionen in die IT-Sicherheit

Der Wirtschaftsschutzbericht kommt zu dem Ergebnis, dass Investitionen in die IT-Sicherheit steigen. Dies ist in Abbildung 3.16 dargestellt. Durchschnittlich beträgt der Anteil des Budgets für IT-Sicherheit am gesamten IT-Budget eines Unternehmens neun Prozent. Damit ist dieser Wert um zwei Prozentpunkte gestiegen. Der Großteil der Unternehmen mit 38 % investiert fünf bis zehn Prozent und 36 % investieren 10 % bis unter 20 %. Ein geringer Teil von sieben Prozent investiert sogar 20 % und mehr. Jedoch setzen 17 % weniger als fünf Prozent ein. [29, S. 13]
In der Umfrage von eco geben 44 % der Befragten an, dass sich die Ausgaben für IT-Sicherheit im letzten Jahr leicht erhöht haben, 10 % sogar deutlich erhöht. Lediglich zwei Prozent stellen eine Verringerung fest und 22 % sind gleichbleibend. Dies ist in Abbildung 3.20 dargestellt. [30, S. 9]
Versicherungen gegen IT-Risiken stellen eine Möglichkeit zur Investition in IT-Sicherheit dar. Damit ist gewährleistet, dass bei entstandenen Schäden Hilfe gegeben ist. Im Bericht von DsiN kennt jedoch jedes vierte Unternehmen derartige Versicherungen nicht und die Hälfte der Unternehmen weiß zwar davon, hat sich aber noch nicht mit diesem Thema beschäftigt. Solche Versicherungen werden lediglich von 21 % der Unternehmen verwendet und vier Prozent der Unternehmen sind sogar dazu verpflichtet. [31, S. 34]
Bei diesem Thema sind wenige vergleichende Informationen zu nennen. Allgemein lässt sich sagen, dass Investitionen in die IT-Sicherheit zunehmen, was beide Umfragen des wirtschaftlichen Bereiches belegen. Um zumindest Teile von entstandenen Schäden durch Angriffe aufzufangen, eignen sich Cyber-Versicherungen. Diese Möglichkeit ist noch wenig verbreitet und Unternehmen sollten daher dahingehend informiert werden.

3.10.14 Umgang mit Angriffen und Notfallmanagement

Im Bezug auf die Vorsorge von Angriffen geben in der eco-Umfrage 63 % der befragten Unternehmen an, mit einem Notfallplan oder anderen internen Prozessen auf mögliche Cyber-Angriffe vorbereitet zu sein. Außerdem planen weitere 24 % solche Systeme. [30, S. 14] Außerdem geben die meisten der Befragten an, aus Sicherheitsvorfällen entstandene Probleme intern gelöst zu haben. Externe Hilfe wurde in einigen Fällen in Anspruch genommen und in noch weniger Fällen wurden Kunden darüber informiert und die Polizei zur Strafverfolgung eingeschaltet. [30, S. 7]
Dem Umgang mit Angriffe geht die Angriffserkennung voran. Jedoch sind im Praxisbericht von DsiN 32 % der Befragten der Meinung, nicht von Angriffen betroffen zu sein oder diese nicht zu bemerken. In ebenso vielen Unternehmen wird die Angriffserkennung den Mitarbeitenden überlassen und 15 % haben spezialisierte Dienstleistende dafür beauftragt. In 21 % der Unternehmen werden Sensoren in der Infrastruktur eingesetzt, um Angriffs-Anzeichen zu erkennen und diese dann an Spezialisten zu übermitteln. [31, S. 26] Außerdem werden verschiedene Möglichkeiten der Reaktion auf Angriffe vorgestellt. 34 % der Unternehmen beschäftigen sich zunächst mit der Entwicklung geeigneter Maßnahmen und deren Umsetzung. Die Verantwortung wird in 44 % in die Hände der Mitarbeitenden gegeben, weil diese entsprechend geschult sind und in 11 % kommen digitale Ersthelfende zum Einsatz. Über spezielle Notfallpläne verfügen 11 % der Unternehmen und testen diese auch regelmäßig. [31, S. 28]
In der Umfrage zu den Sicherheitsmaßnahmen geben mehr als die Hälfte (51 %) der befragten Unternehmen an, über ein Notfallmanagement zu verfügen. Es zeigt sich, dass solche Sicherheitsmaßnahmen in größeren Unternehmen mit mehr als 500 Beschäftigten mehr etabliert sind. Außerdem ist ein solches Regelsystem besonders in KRITIS-Sektoren existent. [33, S. 2]
Das Digitalbarometer 2022 enthält eine Auflistung der Reaktionen auf Cyberangriffe. Das ist in Abbildung 3.33 zu sehen. Demnach wussten lediglich vier Prozent der Betroffenen nicht, was sie tun sollen. Ein großer Teil half sich selbst (37 %), 20 % der Betroffenen fragten Menschen in ihrem Umfeld nach Hilfe und 19 % kontaktierten eine Internetbeschwerdestelle. Nur 27 % erstatteten Anzeige bei der Polizei. [36, S. 11]
Der Vergleich dieser Ergebnisse stellt dar, dass der DsiN-Praxisbericht mit seinen Zahlen deutlich hervorsticht. Die beiden anderen Umfragen kommen zum Ergebnis, dass mehr als die Hälfte der Unternehmen über ein Notfallmanagement verfügt, während im Bericht von DsiN lediglich 11 % darüber verfügen. Zudem zeigt sowohl der wirtschaftliche Bereich als auch die Privathaushalte, dass Probleme in Folge von Sicherheitsvorfällen meist intern und selbst gelöst werden. Nur in wenigen Fällen wird die Polizei informiert. Allgemein lässt sich sagen, dass auch dieser Bereich der Sicherheitsmaßnahmen noch ausbaufähig ist. Ein gutes Zeichen ist, dass im privaten Bereich lediglich vier Prozent der Betroffenen nicht wussten, was zu tun war. Jedoch geben im DsiN-Praxisbericht knapp zwei Drittel der Unternehmen an, keine Angriffe zu bemerken oder nicht davon betroffen zu sein. Aber auch unbemerkte Angriffe können nachhaltige Schäden verursachen, weshalb Angriffserkennung ein relevanter Bestandteil von Sicherheitsmanagement ist.

3.10.15 Sicherheitsmaßnahmen

In der eco-Umfrage wird die Lage der deutschen Wirtschaft gegenüber Cybercrime im Allgemeinen von 71 % der Befragten als unzureichend aufgestellt eingeschätzt. Diese Einschätzung sieht hingegen bezüglich des eigenen Unternehmens deutlich anders aus. Dort nehmen nur 12,4 % unzureichende Maßnahmen wahr. [30, S. 5] In der Umfrage wird auch die Bedeutung von Sicherheitsthemen

beleuchtet. [30, S. 13] Das Ergebnis ist in Abbildung 3.21 dargestellt. Die Sicherheitsthemen aus der Abbildung werden im weiteren Verlauf dieses Abschnitts nach den Kategorien technisch, organisatorisch und personell sortiert.
Der DsiN-Praxisreport befasst sich mit der Frage, ob der Erfolg des Unternehmens von der IT-Sicherheit abhängt. Für knapp die Hälfte (49 %) besteht dieser direkte Zusammenhang und 37 % sehen die Wichtigkeit, aber nicht essenziell. Für sieben Prozent sind Integrität, Vertraulichkeit und Verfügbarkeit von Informationen nicht wichtig und weitere sieben Prozent sagen, dass Betriebsabläufe nicht darauf angewiesen sind. Hervorzuheben ist, dass den direkten Zusammenhang besonders KMU mit weniger als zehn Beschäftigten sehen und größere Unternehmen diese Abhängigkeit weniger stark wahrnehmen. Auch die Branchenzugehörigkeit spielt in dieser Frage eine große Rolle. So sieht insbesondere der Dienstleistungsbereich den direkten Zusammenhang mit 29 %. Dabei ist als möglicher Grund die Verlagerung und Ausweitung der Angebote dieser Branche im Zuge der Digitalisierung aufgrund der Corona-Pandemie in den digitalen Raum zu nennen. [31, S. 8] Bei der Betrachtung der Sicherheitsmaßnahmen fällt auf, dass die Ermittlung von Risikosituationen nicht ausreichend berücksichtigt wird. 37 % verzichten auf diesen Sicherheitsaspekt und 29 % ermitteln dies nur einmalig. In 18 % der befragten Unternehmen werden Risikosituationen einmal jährlich ermittelt und 16 % führen kontinuierliche Risikoermittlungen durch. [31, S. 11–12] Ein weiterer nicht zu vernachlässigender Sicherheitsaspekt ist neben der Umsetzung von Schutzmaßnahmen die Überprüfung von deren Wirksamkeit. Jedes dritte Unternehmen setzt Schutzmaßnahmen ein, überprüft deren Wirksamkeit jedoch nicht. 27 % der Unternehmen überprüfen die Wirksamkeit der eingesetzten Schutzmaßnahmen erst im Verdachtsfall und bei 19 % erfolgt diese Überprüfung regelmäßig. 27 % der Unternehmen kommen ohne spezielle Schutzmaßnahmen aus. [31, S. 26]
Gemeinsam ist den beiden Umfragen, dass sich die schlecht aufgestellte deutsche Wirtschaft auch in den einzelnen Aspekten der Sicherheitsmaßnahmen und -vorkehrungen mit niedrige Zahlen der Umsetzung widerspiegelt.
Es folgen Unterkapitel zu den verschiedenen Formen von Sicherheitsmaßnahmen, aufgeteilt nach Wirtschaft und Gesellschaft.

3.10.15.1 Technische Sicherheitsmaßnahmen Wirtschaft

Im Wirtschaftsschutz-Bericht schätzen 58 % der Befragten fehlkonfigurierte Cloud-Umgebungen als Bedrohung für die IT-Sicherheit ein. [29, S. 14]
In die Kategorie technische Maßnahmen lassen sich folgende Maßnahmen der eco-Umfrage einordnen. Die Wichtigkeit von E-Mail-Schutz vor Spam, Schadprogrammen und Phishing wird von 65 % gesehen. Eine Relevanz von Patchmanagement sehen 59 % der befragten Unternehmen. In einem ähnlichen Bereich befindet sich die Verschlüsselung von Daten und Kommunikation mit einer Wichtigkeit für 58 % der Befragten. Auch Schadsoftware wird von 57 % der Befragten für ein mindestens wichtiges Sicherheitsthema gesehen. Nur gering weniger wichtig erfolgt die Einschätzung für Cloud Security mit 51 %. Eine geringere Wichtigkeit ordnen die Befragten der Mobile Device Security mit 42 % zu. Die Absicherung von Produktions- und Industrieanlagen in technischer Hinsicht ist für 32 % wichtig. Noch geringer ist die Wichtigkeit von Smart Device Security mit jeweils 15 % sehr wichtig und wichtig. [30, S. 13]
Zum Thema technische Sicherheitsmaßnahmen gehören Möglichkeiten beim Versand elektronischer Nachrichten und Datenaustausch. Im DsiN-Praxisbericht wird festgestellt, dass nur jedes zweite Unternehmen übertragene Daten in Anhängen absichert und nur 18 % E-Mail-Verschlüsselung oder elektronische Signaturen einsetzen. Mit einem Passwort sichern 21 % der Unternehmen Dateianhänge ab und bei 12 % erfolgt Datenaustausch nur über dedizierte Austauschplattformen. [31, S. 25]

Ein weiteres bedeutungsvolles Thema ist die Privatnutzung firmeneigener Geräte, die durch das vermehrte Home-Office zugenommen hat. Demnach lässt jedes vierte Unternehmen die Nutzung geschäftlicher Endgeräte zusätzlich für private Angelegenheiten ohne Richtlinien zu und in 22 % der Unternehmen sind für diesen Gebrauch Nutzungsrichtlinien festgelegt. Zudem wird das Prinzip BYOD in 23 % der Unternehmen eingesetzt. 30 % hingegen trennen private und geschäftliche Anwendungen strikt. [31, S. 25] Der Umgang mit Schwachstellen in Standardsoftware ist ein weiteres Risiko. 17 % der befragten Unternehmen haben keine Kenntnis über mögliche Schwachstellen. 26 % reagieren auf Hinweise durch die Presse oder die Hersteller unmittelbar mit Softwareupdates und regelmäßige und sofortige Updates werden in nahezu jedem zweiten Unternehmen durchgeführt. Informationen dazu beziehen acht Prozent von einem Informationsdienst, um dessen Empfehlungen zu folgen. [31, S. 27]
Weiterhin ist Ransomware als eine der gefährlichsten Bedrohungen bekannt und Datendiebstahl ein häufiges Phänomen. Als Möglichkeit, um Schäden durch Verschlüsselung oder Verlust der Daten zu begrenzen, werden regelmäßige Backups angesehen. Dennoch wird in neun Prozent der Unternehmen gänzlich darauf verzichtet und 16 % führen nur unregelmäßig Datensicherungen durch. In 46 % der Unternehmen existieren Konzepte dafür, welche regelmäßig umgesetzt werden und 29 % verfügen über ein qualifiziertes Backup-Konzept. [31, S. 28] Im Hinblick auf die Nutzung von Cloud-Computing haben 44 % der Unternehmen, die diese technische Möglichkeit nutzen, kein Wissen über IT-Sicherheitsanforderungen oder rechtliche Rahmenbedingungen diesbezüglich. Eine externe Beratung diesbezüglich wird von 31 % der Cloud-nutzenden Unternehmen und klare Regeln für den Einsatz und die Verwendung haben 25 % definiert. [31, S. 33]
Im Bericht zum Thema Sicherheitsmaßnahmen des Bitkom wird auf die einzelnen Kategorien wie den technischen Bereich gesondert eingegangen. Beim diesem Thema ist eine Zunahme im Vergleich zu den Vorjahren in Abbildung 3.23 festzustellen. Am meisten etabliert sind Mindestanforderungen an Passwörter mit 72 % und einer konkreten Planung von 16 %. Mit wenig Abstand folgt Zugriffsprotokollierung mit 71 % Umsetzung und 10 % konkreter Planung. Mit 70 % Umsetzung und 13 % konkreter Planung befindet sich elektronische Zugangskontrollen zu Gebäuden und Maschinen direkt folgend. Die Verschlüsselung von Daten auf Datenträgern ist auch eine wichtige Maßnahme mit einer Umsetzung von 67 % und konkrete Planung von 12 %. Wie bereits erwähnt, bergen auch Cloud-Anwendungen ein Risiko für Angriffe. Schutzmaßnahmen zur Absicherung diesbezüglich werden von 63 % der Unternehmen eingesetzt und von 25 % zumindest konkret geplant. Auf abhörsichere Sprachkommunikation setzen 60 % der Unternehmen und erweiterte Verfahren zur Benutzeridentifikation setzen 46 % ein. In 43 % der Unternehmen wird auf Absicherung gegen Datenabfluss von innen geachtet und 42 % verfügen über separate Netzwerkzugänge für Kunden und Geschäftspartner. Verschlüsselter E-Mail-Verkehr wird lediglich von 41 % der Unternehmen eingesetzt und von 17 % konkret geplant. Ebenso gering ist der Einsatz von Penetrationstests mit 40 % Umsetzung und 16 % Planung. Noch weniger eingesetzt werden Intrusion Detection Systeme mit 28 % und 19 % in Planung und Security-by-Design-Produkte mit 19 % Umsetzung und 12 % Planung. Ein leichter Rückgang ist beim Einsatz von Sicherheitssystemen, die auf KI basieren, erkennbar. Der ohnehin niedrige Wert des Vorjahres ist um wenige Prozentpunkte auf acht Prozent Umsetzung und neun Prozent Planung abgestiegen. Alle weiteren Maßnahmen, für die Vergleichswerte der vergangenen Jahre existieren, verzeichnen Anstiege. Dieser Anstieg ist bei der Verschlüsselung von Datenträgern mit 15 Prozentpunkten am stärksten ausgeprägt. [33, S. 3-–5]

3.10.15.2 Organisatorische Sicherheitsmaßnahmen Wirtschaft

Zu den organisatorischen Maßnahmen in der eco-Umfrage gehören die folgenden. Zum einen die Absicherung von mobilen Arbeitsplätzen, besonders im Home-Office. Deren Wichtigkeit ist für 28 % sehr stark und für 35 % mittel ausgeprägt. Weiterhin umfasst diese Kategorie die Konzeption und den Einsatz eines Information Security Management Systems (ISMS) mit einer Wichtigkeit von 58 %. Auch Compliance mit Datenschutz, IT-Sicherheitsgesetz und weiteren zählt mit 53 % wichtig in diese Kategorie. Die Sicherheit von Lieferanten und Dienstleistern ist für knapp die Hälfte der Befragten (49 %) wichtig. Mit geringster Relevanz in dieser Kategorie schätzen die Befragten Identitätsdiebstahl mit 47 % wichtig ein. [30, S 13]
Der Bericht zu den Sicherheitsmaßnahmen enthält speziell auch organisatorische Maßnahmen, wie in Abbildung 3.24 zu sehen ist. Dabei fällt auf, dass Zugriffsrechte für bestimmte Informationen in jedem befragten Unternehmen umgesetzt werden. Auch klare Regeln für den Umgang mit schützenswerten Informationen sind in fast allen Unternehmen (97 %) etabliert. Weniger verbreitet sind Zutrittsrechte für bestimmte Unternehmensräume mit 83 % Umsetzung und 13 % konkreter Planung. Mit ein wenig Abstand folgt die eindeutige Kennzeichnung von Betriebsgeheimnissen mit einer Umsetzung von 81 % und Planung von sieben Prozent. Eine Clean-Desk-Policy ist in 68 % der Unternehmen etabliert und in 10 % geplant. Außerdem sind Sicherheits-Zertifizierungen und darin enthaltene ISMS nur mäßig verbreitet. Dazu gehören zudem regelmäßige Sicherheits-Audits durch Spezialisten von außerhalb. Grundsätzlich ist zu sagen, dass, mit der Ausnahme von gültigen Sicherheits-Zertifizierungen und in vorherigen Umfragen nicht abgefragte Maßnahmen, alle Sicherheitsmaßnahmen im Vergleich zum Vorjahr an Bedeutung gewonnen haben. Ein starker Anstieg um 13 Prozentpunkte ist bei Clean-Desk-Policy zu beobachten. [33, S. 6–7]

3.10.15.3 Personelle Sicherheitsmaßnahmen Wirtschaft

In der Wirtschaftsschutz-Umfrage sehen insgesamt 72 % eine Bedrohung durch den Mangel an qualifizierten IT-Sicherheitskräften. [29, S. 14]
In der Umfrage von eco wird in der Übersicht der Sicherheitsthemen Mitarbeitersensibilisierung beleuchtet. Zugleich befindet sich diese an erster Stelle mit 51-prozentiger Zustimmung bei sehr wichtig. Weitere 22 % finden diese Maßnahme wichtig und nur fünf Prozent weniger wichtig und ein Prozent gar nicht wichtig. [30, S. 13] In einer spezifischen Frage geben 62 % der befragten Unternehmen an, regelmäßig Mitarbeiterschulungen und Sensibilisierungen durchzuführen. In 35 % der Unternehmen finden solche Schulungen unregelmäßig statt und in drei Prozent gar nicht. [30, S. 14]
Der Praxisbericht von DsiN stellt heraus, dass in Sachen Sicherheitsmaßnahmen im personellen Bereich Veränderungen notwendig sind. So ist in 35 % der befragten Unternehmen allein die Geschäftsleitung für IT-Sicherheit zuständig. Unterstützung durch Informationssicherheitsbeauftragte erfährt diese in weiteren 27 %. [31, S. 16] Dieser Zustand besteht vor allem in kleinen Unternehmen. In jedem zweiten kleinen Unternehmen mit weniger als zehn Beschäftigten ist die Geschäftsleitung zugleich die verantwortliche Person für IT-Sicherheit. [31, S. 17] Dazu gehört zudem, dass in jedem zweiten Unternehmen die Geschäftsleitung über den konkreten Risikoumgang entscheidet. In 34 % der Unternehmen ist dafür die IT-Abteilung oder externe IT-Dienstleister zuständig, in 10 % Leitungspersonen der Abteilungen und in fünf Prozent die Beschäftigten selbst. [31, S. 18] Weiterhin ist zu beobachten, dass je größer ein Unternehmen ist, desto weniger fällt die Geschäftsleitung Entscheidungen in einer akuten Bedrohungslage. [31, S. 18] In Sachen Mitarbeiterschulungen haben 16 % der Unternehmen ein verpflichtendes Sicherheitsschulungsprogramm und sechs Prozent

ein solches, das auf verschiedene Profile der Mitarbeitenden angepasst ist und regelmäßige Tests enthält. In 34 % der Unternehmen werden gelegentlich Informationen über kostenlos stattfindende Online-Schulungen verteilt. 44 % der Unternehmen vertreten die Meinung, dass ihre Mitarbeitenden hinsichtlich IT-Sicherheit ausreichend informiert sind und deshalb keine weiteren Maßnahmen erforderlich sind. [31, S. 19]
Der Bericht Sicherheitsmaßnahmen 2021 enthält eine Aufstellung personeller Sicherheitsmaßnahmen, in Abbildung 3.25 zu sehen. An der ersten Stelle befindet sich die Bestellung von Sicherheitsverantwortlichen mit einer Umsetzung von 59 % und konkreten Planung von 22 %. Schulungen der Mitarbeitenden zu Sicherheitsthemen liegen auf dem zweiten Platz mit 56 % Umsetzung und 19 % Planung. In diesem zahlenmäßigen Bereich befinden sich auch Background-Checks des Personals vor der Besetzung sensibler Positionen mit 55 % Umsetzung und 18 % konkrete Planung. Ein anonymes Hinweis-System auf verdächtige Beschäftigte ist weniger verbreitet. Lediglich 32 % der Unternehmen haben ein solches im Einsatz und 11 % planen ein solches. Im Allgemeinen ist zu beobachten, dass Mitarbeiterschulungen und Background-Checks im Vergleich zum Vorjahr ein wenig an Bedeutung verloren haben. Die beiden weiteren Maßnahmen verzeichnen Anstiege. [33, S. 8]

3.10.15.4 Vergleich der Sicherheitsmaßnahmen Wirtschaft

Ein bemerkenswerter Sachverhalt, der beim Vergleich dieser Ergebnisse auffällt, ist im Bericht zu den Sicherheitsmaßnahmen 2021 die höhere Umsetzung der abhörsicheren Sprachkommunikation als der Einsatz verschlüsselter E-Mail-Kommunikation. Das lässt darauf schließen, dass Unternehmen sichere E-Mail-Kommunikation weniger wichtig ist als abgesicherte Sprachkommunikation [33, S. 3–5]. Als Gemeinsamkeit der Berichte ist der Aspekt Benutzeridentifikation zu nennen. Erweiterte Verfahren dafür werden laut der Sicherheitsmaßnahmen-Umfrage von 46 % der Unternehmen umgesetzt [33, S. 3–5]. Dem wird das Sicherheitsthema Identitätsdiebstahl in der eco-Umfrage mit einer Wichtigkeit von 47 % und einem somit sehr ähnlichen Prozentwert zugeordnet [30, S. 13]. Eine weitere Gemeinsamkeit ist bei der Sicherheit von Lieferanten, Kunden, Dienstleistern und Geschäftspartnern festzustellen. 42 % der Unternehmen geben in der Umfrage zu den Sicherheitsmaßnahmen an, separate Netzwerkzugänge für diese Personengruppe anzubieten [33, S. 3–5] und 49 % der Befragten der eco-Umfrage finden diesen Sicherheitsaspekt mindestens wichtig [30, S. 13]. Auch der Umgang mit Cloud-Security stellt sich als Gemeinsamkeit heraus. Laut der eco-Umfrage halten 51 % dieses Thema für mindestens wichtig und in der Umfrage zu den Sicherheitsmaßnahmen setzen 63 % der Befragten derartige Maßnahmen um und 25 % planen diese konkret [33, S. 3–5]. Außerdem sehen mehr als die Hälfte der Befragten (58 %) eine Bedrohung in fehlerhafter Cloud-Konfiguration für die IT-Sicherheit des eigenen Unternehmens [29, S. 14]. 56 % der Cloud-nutzenden Befragten des DsiN-Praxisberichts setzen Maßnahmen in diesem Bereich um [31, S. 25]. Ähnliche Tendenzen sind auch beim Vergleich des Patchmanagements und des Umgangs mit Schwachstellen feststellbar. In der eco-Umfrage geben 59 % der Befragten an, Patchmanagement als mindestens wichtig zu sehen [30, S. 13]. In der Umfrage von DsiN zeigt sich, dass nahezu jedes zweite Unternehmen regelmäßig sofortige Updates durchführt und 26 % zumindest auf Hinweise zu Schwachstellen sofort mit Updates reagiert [31, S. 27]. Unterschiede weisen die Angaben zum Einsatz von E-Mail-Verschlüsselung auf. In der Umfrage von eco gibt es zwei Sicherheitsthemen, die diesem Aspekt zugeordnet werden können. Zum einen E-Mail-Schutz mit 65 % mindestens wichtig und zum anderen Verschlüsselung von Daten und Kommunikation mit 58 % mindestens wichtig [30, S. 13]. Im DsiN-Praxisbericht geben

18 % der befragten Unternehmen an, E-Mail-Verschlüsselung einzusetzen [31, S. 25] und in der Umfrage zu den Sicherheitsmaßnahmen sind es 41 % und bei 17 % konkret geplant [33, S. 3–5]. Damit zeigen sich deutliche Unterschiede in der Einschätzung der Wichtigkeit und der Umsetzung solcher Sicherheitsmaßnahmen. Auch die Verschlüsselung von Daten auf Datenträgern stellt sich im Vergleich verschieden dar. Wie bereits erwähnt, umfasst dieses Sicherheitsthema in der eco-Umfrage neben der Verschlüsselung von Daten auch E-Mail-Verschlüsselung und zeigt eine Wichtigkeit von 58 % [30, S. 13]. Datenverschlüsselung auf Datenträgern wird von der Umfrage zu den Sicherheitsmaßnahmen hingegen mit 67 % Umsetzung und 12 % konkreter Planung beziffert [33, S. 3–5]. Als Grund für den starken Unterschied ist hierbei der erweiterte Umfang dieses Sicherheitsaspekts in der Umfrage von eco zu nennen. Wie zuvor dargelegt, ist die Verschlüsselung von E-Mails weniger beliebt und es ist daher möglich, dass dieser Aspekt zu einem niedrigeren Gesamtprozentwert führt. Zugangskontrolle zu Gebäuden und Maschinen wird laut dem Sicherheitsmaßnahmen-Bericht von 70 % umgesetzt, von 13 % konkret geplant und ist damit die am dritt-häufigsten umgesetzte Sicherheitsmaßnahme in diesem Bericht [33, S. 3–5]. Im weiteren Sinne kann dieser Maßnahme das Sicherheitsthema der Absicherung von Produktions- und Industrieanlagen in der eco-Umfrage mit einer Wichtigkeit von 32 % zugeordnet werden, welches sich an vorletzter Stelle im Ranking der Sicherheitsthemen befindet [30, S. 13]. Als Grund für diese starke Differenz ist hier die erfolgte Zuordnung im weiteren Sinne anzuführen, die auch mehr den organisatorischen Bereich umfassen kann. In diesem Bereich sind noch ISMS zu nennen. Die Umfrage zu den Sicherheitsmaßnahmen differenziert zwischen verschiedenen Zertifizierungen, wie z.B. ISO 27001. Daher ist ein Vergleich mit den Angaben zur Wichtigkeit in der eco-Umfrage schwierig. Diese Wichtigkeit liegt bei 58 % [30, S. 13], während die einzelnen ISMS jeweils bei unter 50 % Umsetzung liegen [33, S. 3–5].
Beim Vergleich der personellen Sicherheitsmaßnahmen sind zwei Unterschiede zu nennen. Bei der Bestellung eines Sicherheitsverantwortlichen ist das Ergebnis von DsiN, dass in 35 % der Unternehmen die Geschäftsleitung allein diese Position innehat. Diese Situation ist besonders in kleinen Unternehmen wahrzunehmen. [31, S. 16] Die Umfrage zu den Sicherheitsmaßnahmen liefert bei diesem Thema nur, dass in 59 % der Unternehmen Sicherheitsverantwortliche bestellt werden und diese Maßnahme damit im personellen Bereich am meisten umgesetzt wird [33, S. 3–5]. Ein Mangel an IT-Sicherheitskräften wird von dreiviertel der Befragten der Wirtschaftsschutz-Umfrage als Bedrohung für die IT-Sicherheit gesehen [29, S. 14]. Mitarbeitersensibilisierung ist an erster Stelle der Sicherheitsthemen der eco-Umfrage mit 73 % wichtig platziert [30, S. 13]. Außerdem finden regelmäßige Mitarbeiterschulungen in 62 % der Unternehmen statt und in weiteren 35 % unregelmäßig [30, S. 14]. Der DsiN-Praxisbericht gibt an, dass 22 %, teilweise verpflichtend, Mitarbeiterschulungen durchführen, und in 34 % der Unternehmen die Mitarbeitenden über kostenlos stattfindende Online-Schulungen informiert werden [31, S. 19]. Im Sicherheitsmaßnahmen-Bericht wird eine Umsetzung von Mitarbeiterschulungen von 56 % und 19 % konkrete Planung dargestellt [33, S. 3–5]. Bei diesem Vergleich fällt auf, dass die niedrigen Zahlen von DsiN hervorstechen, während die beiden anderen Berichte Prozentwerte im ähnlichen Bereich beschreiben. Zusammenfassend ist zu sagen, dass in allen drei Kategorien technisch, organisatorisch und personell Maßnahmen vorhanden sind, die sehr häufig umgesetzt werden oder geplant sind, aber auch Maßnahmen, die weniger beliebt sind. Eine 100-prozentige Umsetzung ist lediglich im Bericht zu den Sicherheitsmaßnahmen bei Zugriffsrechten für bestimmte Informationen zu finden. Gründe für die Unterschiede, besonders zwischen der eco-Umfrage und den beiden weiteren, sind, dass Sicherheitsthemen für wichtig empfunden werden können, aber dennoch nicht zwangsläufig umgesetzt werden müssen. Außerdem sind die Aspekte teilweise nicht gut oder gar nicht vergleichbar.
Eingesetzte Sicherheitsmaßnahmen können sich im gesellschaftlichen Bereich deutlich von der Wirt-

schaft unterscheiden. Das wird im folgenden Abschnitt analysiert und im anschließenden Vergleich gegenübergestellt.

3.10.15.5 Sicherheitsmaßnahmen Privat

In der Umfrage zur IT- und Cybersicherheit des Bitkom schätzt weniger als die Hälfte (41 %) sich selbst so gut über Sicherheitsmaßnahmen informiert ein, dass die eigenen Geräte ausreichend geschützt werden können. Dazu kommt, dass 69 % der Befragten angeben, es vermutlich nicht zu bemerken, wenn sie über das Internet ausspioniert werden würden. [34, S. 12] Grundsätzlich ist zu sagen, dass fast alle in Tabelle 3.5 genannten Maßnahmen im Vergleich zum Vorjahr mehr eingesetzt werden. [34, S. 9–11]
Im Digitalbarometer geben zwei Drittel der Befragten an, Schutzempfehlungen zu kennen. Jedoch setzen nur 12 % diese vollständig um. Als Gründe werden zu hoher Aufwand und Kompliziertheit der Sicherheitsmaßnahmen genannt. Hingegen schätzen Personen, die Sicherheitsmaßnahmen umsetzen, den Aufwand geringer ein. [35, S. 4] Im Allgemeinen werden mehr Sicherheitsmaßnahmen als in den Vorjahren eingesetzt. So ist in nahezu allen aufgelisteten Maßnahmen in Abbildung 3.29 ein Anstieg zu erkennen. [35, S. 4–5] Zudem ist zu beobachten, dass jüngere Menschen durchschnittlich lediglich drei Maßnahmen umsetzen und damit unter dem Gesamtdurchschnitt von vier eingesetzten Maßnahmen liegen. Allgemein fühlt sich knapp ein Drittel der Befragten diesbezüglich mindestens gut informiert. Hingegen schätzen 18 % ihren Informationsstand als schlecht ein und 45 % fühlen sich nur teilweise informiert. 57 % der Befragten wünschen sich mehr Informationen über Cybersicherheit. Der ältere Teil der Befragten von 40 bis 69 Jahren nennt vor allem Webseiten und E-Mail-Newsletter als gewünschte Informationskanäle. Außerdem werden klassische Medien wie Zeitung und Radio als wichtig eingeschätzt. Jüngere Menschen hingegen bevorzugen Informationen über die sozialen Medien. Die Themenwünsche sind breit aufgestellt und in Abbildung 3.30 dargestellt. Am meisten gefragt sind Hinweise, wie Internetkriminalität erkannt werden kann (57 %). Hinweise zum Schutz sensibler Daten und welche Software zum Schutz geeignet ist sowie Handlungsempfehlungen für Opfer sind mit jeweils 48 % beliebte Themen. Auffallend gering ist der Wunsch nach Informationen über sichere Passwörter mit 24 % und zur sicheren Nutzung von Cloud-Diensten mit 28 %. [31, S. 12–13]
Beim Vergleich dieser Ergebnisse ist eine Gemeinsamkeit zu nennen. Beide Umfrage kommen zu dem Ergebnis, dass im Allgemeinen mehr Maßnahmen als in den Vorjahren eingesetzt werden. Jedoch fühlen sich nach dem IT- und Cybersicherheitsbericht 41 % gut über mögliche Maßnahmen zum Schutz informiert, während im Digitalbarometer nur 33 % angeben, gut informiert zu sein. Beides sind jedoch nur geringe Werte, die auf Informationsbedarf schließen lassen. Wie unterschiedlich dieser bei den verschiedenen Sicherheitsthemen aussieht, zeigt das Digitalbarometer.
In Tabelle 3.5 sind die Schutzmaßnahmen für Computer und Smartphone aus den Abbildungen 3.27 und 3.28 aus der Studie des Bitkom zur IT- und Cybersicherheit 2021 aufgelistet. Dabei ist bei Maßnahmen auf privaten Computern zu beobachten, dass mit den Ausnahmen der Virenschutzprogramme und regelmäßigen Backups auf externen Speichern alle Maßnahmen leicht oder stärker an Bedeutung gewonnen haben. Der größte Anstieg ist bei Passwort-Safes mit einer Zunahme von 15 Prozentpunkten zu verzeichnen. Smartphones werden allgemein weniger geschützt. Vermehrter Einsatz im Vergleich zum Vorjahr ist hier jedoch bei allen Maßnahmen außer Abdeckungen auf Smartphone-Kameras festzustellen. Regelmäßige Backups in der Cloud erfahren die größte Steigerung. [34, S. 9–11] Beim Einsatz von Zwei-Faktor-Authentifizierung ist eine deutliche Ausbaufähigkeit

zu erkennen. Lediglich 37 % der Befragten geben an, diese Zugangsmöglichkeit, zumindest für einige Online-Dienste zu nutzen. Am meisten werden dabei Codes per SMS mit 35 % oder per E-Mail mit 32 % eingesetzt oder mit 31 % ein TAN-Generator verwendet. 64 % der Befragten stimmen der Aussage zu, Sicherheits-Updates immer sofort zu installieren. [34, S. 12]

Tabelle 3.5: Technische Sicherheitsmaßnahmen IT- und Cybersicherheit 2021 [34, S. 9–11]

auf privaten Computern		auf privaten Smartphones	
Virenschutzprogramm	86 %	Lokalisierungsfunktion bei Verlust	65 %
Firewall	71 %	Virenschutzprogramm	43 %
Abdeckung der Webcam	39 %	Regelmäßige Backups in der Cloud	38 %
Regelmäßige Backups in der Cloud	35 %	Regelmäßige Backups auf externen Speichern	31 %
VPN-Verbindung	28 %	Passwort-Safe	18 %
Anonymisierungsdienste	25 %	Abdeckung der Smartphone-Kamera	14 %
Passwort-Safe	23 %		
Regelmäßige Backups auf externen Speichern	22 %		
Meta-Suchmaschinen ohne Nutzerdaten-Speicherung	4 %		

Eine vergleichende Betrachtung von Sicherheitsmaßnahmen auf Computern und auf Smartphones zeigt den hohen Einsatz von Virenschutzprogrammen auf beiden Gerätetypen, jedoch mit deutlich unterschiedlichen Prozentwerten. Ähnliche Prozentwerte haben hingegen Backups in der Cloud, wobei bei beiden festzustellen ist, dass diese häufiger umgesetzt werden als Backups auf externen Speichern. In der Cloud sind Backups deutlich komfortabler, da der Zugriff von jedem Ort möglich ist, wenig Aufwand notwendig ist und diese Funktion von vielen Anbietern direkt angeboten wird und mit wenigen Klicks umgesetzt werden kann. Das Digitalbarometer zeigt, dass auch der Informationsbedarf bei diesem Thema gering ist. Passwortsafes kommen bei beiden Geräten weniger häufig zum Einsatz. Als Unterschied ist zu nennen, dass Abdeckungen auf Webcams deutlich beliebter sind als auf Smartphone-Kameras. Einige Sicherheitsmaßnahmen sind gerätespezifischer und können daher nicht verglichen werden. Dazu gehört, dass Lokalisierungsfunktionen bei Smartphones sehr beliebt sind. Diese sind in vielen Geräten standardmäßig installiert oder durch wenig Aufwand einsatzbereit. Außerdem kommen Smartphones mobil zum Einsatz und damit ist die Wahrscheinlichkeit des Verlustes höher.
In der Tabelle 3.6 befindet sich eine Auflistung der Schutzmaßnahmen des Digitalbarometers 2021 aus Abbildung 3.29. Am häufigsten eingesetzt werden Virenschutzprogramme mit 62 %, sichere Passwörter mit 60 % und aktuelle Firewalls mit 53 %. [35, S. 4–5]

Tabelle 3.6: Sicherheitsmaßnahmen Digitalbarometer 2021 [35, S. 4–5]

Sicherheitsmaßnahmen	
aktuelles Virenschutzprogramm	62 %
Sichere Passwörter	60 %
Aktuelle Firewall	53 %
Sichere https-Verbindung bei der Übertragung persönlicher Daten	41 %
Zwei-Faktor-Authentisierung	40 %
Einstellung der automatischen Installation von Updates	32 %
Regelmäßiges Anlegen von Sicherheitskopien	28 %
Verschlüsselte E-Mail-Kommunikation	23 %
Verzicht auf soziale Medien	13 %
Verzicht auf Online-Banking	9 %

Beim Vergleich der beiden Umfragen zeigt sich deutlich, dass Virenschutzprogramme und Firewalls in beiden Umfragen angesagt sind und häufig verwendet werden. Zwei-Faktor-Authentisierung wird ungefähr gleich häufig eingesetzt und regelmäßige Backups bzw. Sicherungskopien befinden sich im Mittelfeld der häufigen Umsetzung. Anzumerken ist, dass sichere Passwörter häufig in Passwort-Safes gespeichert werden und der prozentuale Unterschied zwischen der Nutzung von Passwort-Safes und sicheren Passwörtern eine deutliche Differenz aufweist. Ein weiterer Unterschied besteht bei der Installation von Updates. Im Digitalbarometer geben 32 % der Befragten an, Updates automatisch zu installieren [35, S. 4–5] während 64 % der Befragten in der Umfrage zur IT- und Cybersicherheit angeben, Updates sofort zu installieren [34, S. 9–11]. Dabei besteht eine Differenz um die doppelten Prozentpunkte. Weiterhin stellt der Verzicht auf Online-Banking keine für jeden umsetzbare Sicherheitsmaßnahme dar, weil diese Funktion häufig notwendig ist. Der Verzicht auf soziale Medien ist hingegen durchaus möglich. Im Allgemeinen wird deutlich, dass einfache, schnell umsetzbare Sicherheitsmaßnahmen häufiger eingesetzt werden. Dazu gehört die einmalige Installation eines Virenschutzprogrammes mit automatischen Updates und eine Firewall, die keine weiteren Aktionen benötigt. Zwei-Faktor-Authentisierung ist hingegen recht aufwendig, da nach der Konfiguration jedes Mal bei der Verwendung ein, wenn auch geringer, Mehraufwand entsteht. Als Grund für die Steigerung beim Einsatz von Backups in der Cloud und dem Abstieg von Backups auf externen Medien gelten die bereits genannten Gründe für die häufigere Verwendung des ersteren.
Die beiden Berichte betrachten lediglich technische Sicherheitsmaßnahmen, weil organisatorische und personelle Maßnahmen im Bereich der Privathaushalte keine Relevanz haben.

3.10.15.6 Vergleich der Sicherheitsmaßnahmen in der Wirtschaft und Privat

Allgemein lässt sich feststellen, dass grundsätzlich mehr Maßnahmen als in den Vorjahren umgesetzt werden, da nahezu alle Umfragen zu diesem Ergebnis kommen. Eine weitere Gemeinsamkeit ist die Umsetzung von sicheren Passwörtern. Im Wirtschafts-Bereich setzen laut der Umfrage zu den Sicherheitsmaßnahmen 72 % der befragten Unternehmen Mindestanforderungen an Passwörter um und 16 % planen dies konkret [33, S. 3–5]. Damit ist das die am häufigsten umgesetzte technische Maßnahme. Im Digitalbarometer wird angegeben, dass sichere Passwörter von 60 % der Befragten verwendet werden [35, S. 4–5] und dies damit die am zweithäufigsten verwendete Maßnahme ist. Damit sind in diesem Aspekt ähnliche Ergebnisse zu verzeichnen und es kann die These aufgestellt werden, dass sichere Passwörter sowohl in der Wirtschaft als auch im Privaten eine große Rolle spielen. Außerdem ist bei diesem Thema anzumerken, dass der im Digitalbarometer angegebene Informationswunsch über sichere Passwörter verhältnismäßig gering ist. Offenbar besteht bei diesem Thema wenig Bedarf, weil es schon viel umgesetzt wird. Zu den Unterschieden gehört das Ergebnis, dass im privaten Bereich nur technische Sicherheitsmaßnahmen beleuchtet werden, weil nur diese Relevanz haben. Daher sind insgesamt nur drei Maßnahmen zwischen den verschiedenen Bereichen vergleichbar. Es ist nicht erklärbar, warum beispielsweise Firewall, Virenschutzprogramm und weitere in den Umfragen der Wirtschaft nicht vorkommen. Ein weiterer Unterschied besteht in der Umsetzung von regelmäßigen Backups. Gemäß der Angaben der Befragten des DsiN-Praxisberichts führen 16 % unregelmäßig Backups durch, 46 % regelmäßig und 29 % nach einen qualifizierten Backup-Konzept [31, S. 28]. Somit ergibt sich ein Wert von 75 % der Befragten, die regelmäßig Backups durchführen. In der Umfrage zur Internet- und Cybersicherheit geben in der Kategorie Computer 35 % der Befragten an, regelmäßig Backups in der Cloud durchzuführen und 22 % auf externen Speichergeräten. Leicht unterschiedlich gestalten sich diese Werte für Smartphones. 38 % machen Backups in der Cloud und 31 % auf externen Speichergeräte. [34, S. ß–11] Im Digitalbarometer machen 28 % die Angabe, regelmäßig Sicherheitskopien zu erstellen [35, S. 4–5]. Damit ist anzunehmen, dass Backups in der Wirtschaft mehr Bedeutung als im Privaten zugemessen wird. Hinsichtlich verschlüsselter E-Mail-Kommunikation werden stark unterschiedliche Angaben gemacht. So halten in der eco-Umfrage 58 % der Befragten diese Sicherheitsmaßnahme für mindestens wichtig [30, S. 13], während aus dem DsiN-Praxisbericht hervorgeht, dass lediglich 18 % diese Maßnahme umsetzen [31, S. 25]. Im Sicherheitsmaßnahmen-Bericht zeigt sich, dass 41 % Verschlüsselung für E-Mail-Kommunikation einsetzen [33, S. 3–5]. Das Digitalbarometer liefert einen Prozentwert von 23 % der Befragten, die solche Maßnahmen im privaten Bereich umsetzen [35, S. 4–5]. Aufgrund der starken Differenzen dieser Werte kann keine gültige Aussage beim Vergleich getroffen werden. Zusammenfassend ist zu sagen, dass die Verwendung sicherer Passwörter als Sicherheitsmaßnahme hervorgeht, dass diese in Wirtschaft und Privathaushalten gleich bedeutend ist. Hingegen kann bei der Untersuchung von regelmäßigen Backups darauf geschlossen werden, dass diese im wirtschaftlichen Bereich mehr Relevanz haben. Zu allen weiteren Maßnahmen kann, teilweise aufgrund fehlender Vergleichswerte, keine Aussage getroffen werden.

3.10.16 Zukunft und Prognose

Im Bezug auf die Zukunft liefert der Wirtschaftsschutz-Bericht ein eher düsteres Bild. 42 % der Befragten erwarten eine starke Zunahme von Cyber-Attacken und 18 % stimmen eher der Zunahme zu. Nur 18 % erwarten eine gleichbleibende Entwicklung. Mit einer stärkeren Zunahme rechnen

besonders KRITIS-Sektoren mit 51 %. Im Nicht-KRITIS-Bereich sieht diese Einschätzung anders aus. Dort prognostizieren nur 40 % einen starken Anstieg. [29, S. 12]
In der Umfrage von eco wird eine Einschätzung der stärksten Veränderungstreiber hinsichtlich der nächsten fünf Jahre erfragt. Besonders dem Anstieg von Cyberkriminalität wird eine große Rolle zugesprochen. Weitere starke Einflussfaktoren sind vernetzte kritische Infrastrukturen und Cloud Computing. [30, S. 15]
Aus beiden Umfragen geht hervor, dass Cybercrime in Zukunft weiterhin einen großen Einfluss hat und eine ernst zu nehmende Bedrohung darstellt.

3.10.17 Einfluss der Corona-Pandemie

Der Lagebericht 2021 beschäftigt sich in einem Kapitel explizit mit den Gefährdungen der Cybersicherheit durch die Corona-Pandemie. Aufgrund dieser gesellschaftlichen Entwicklungen erfolgte ein Digitalisierungs-Boom, was dazu führte, dass mehr Dienstleistungen und Geschäftstätigkeiten online angeboten werden. Mit der schlagartigen Einführung digitaler Arbeitsmittel und Home-Office entstanden neue Angriffsmöglichkeiten für Cyber-Angreifende. Dennoch stellt das BSI keine signifikante Steigerung der Angriffszahlen fest. [23, S. 38–41]
In der Umfrage von eco wird die Frage gestellt, inwieweit sich die Sicherheitslage durch die Corona-Pandemie verändert hat. Dabei nehmen 80 % der Befragten eine Verschärfung wahr. Allerdings beobachten nur 16 % in ihrem Unternehmen mehr erfolgreiche Angriffe durch das vermehrt stattfindende Home-Office. [30, S. 12]
Das Digitalbarometer 2021 fokussiert das Thema Online-Aktivitäten in der Corona-Pandemie. Es wird eine deutliche Steigerung in der Internetnutzung seit Beginn der Pandemie beobachtet. Je nach Altersklasse nennen die Befragten, deren Internetnutzung aufgrund der Pandemie gestiegen ist, dazu verschiedene Gründe. Für die Jüngeren stehen besonders Streaming-Dienste im Fokus und Onlinekauf wird von 40- bis 59-Jährigen bevorzugt. Der ältere Teil der Befragten nutzt das Internet mit seinen Möglichkeiten vor allem zur Kontaktaufrechterhaltung und Kommunikation. Insgesamt geben 80 % der Befragten an, ein sicheres Gefühl bei der Nutzung zu haben. [35, S. 9]
Der Vergleich bei diesem Thema zeigt, dass Internetnutzung und Digitalisierung seit Beginn der Corona-Pandemie zugenommen haben, jedoch die detektierten Angriffszahlen keine signifikante Steigerung zeigen. In der Wirtschaft wird eine Verschärfung der Bedrohungslage durch Cybercrime wahrgenommen, im privaten Bereich fühlen sich jedoch viele sicher.

3.10.18 Erwartungen an Politik und Polizei

In der Wirtschaftsschutz-Umfrage werden die Teilnehmenden zu ihren Wünschen bezüglich politischer Maßnahmen im Umgang mit Cybercrime befragt. 98 % wünschen sich, dass sich die Politik stärker um eine EU-weite Zusammenarbeit im Bereich der Cybercrime einsetzen soll. 97 % stimmen dem Wunsch zu, dass die Politik auch verstärkt gegen Cyberattacken aus dem Ausland vorgehen soll, erweiterte Ermittlungsbefugnisse zur Aufklärung von Cyberangriffe befürworten jedoch nur 77 %. 77 % stimmen der Aussage zu, dass der bürokratische Aufwand zur Meldung von Vorfällen zu hoch ist. [29, S. 15]
91 % der Befragten der Umfrage zur IT- und Cybersicherheit des Bitkom sehen mehr Präsenz der Polizei im digitalen Raum als geeignete Maßnahme. Außerdem halten 92 % finanzielle staatliche Förderung von speziell auf Internetkriminalität spezialisierte Polizeieinheiten für sinnvoll. [34, S. 12–13]

Zusammenfassend ist bei diesem Thema zu sagen, dass die meisten Menschen sich mehr Engagement der Politik und Polizei wünschen. Das soll jedoch nicht zwangsläufig mit mehr Befugnissen der Polizei in ihrer Arbeit einhergehen. Außerdem sollen bürokratische Hürden bei der Meldung von Vorfällen vereinfacht werden.

3.10.19 Zusammenfassung

Alle genannten Berichte liefern den Grundkonsens, dass Cybercrime-Delikte zunehmen und daher ein ausreichender Schutz mit verschiedenen Maßnahmen notwendig ist. Innerhalb einzelner Aspekte und besonders bei der Betrachtung der stattgefundenen Angriffe liegen deutliche, nicht nur zahlenmäßige, Unterschiede vor. Aufgrund verschiedener Gründe ist ein direkter Vergleich teilweise nicht möglich.

4 Awareness-Trainings

Der zweite Themenkomplex der vorliegenden Arbeit sind Awareness-Schulungen. Einige angebotene Schulungen und Seminare werden in diesem Kapitel exemplarisch vorgestellt und miteinander verglichen. Im Anschluss erfolgt der Vergleich mit der Bedrohungslage Cybercrime.

4.1 Vergleich verschiedener Awareness-Trainings

Eines der Ziele dieser Arbeit ist es, Aussagen darüber zu treffen, ob aktuelle Awareness-Schulungen an den richtigen Punkten ansetzen und damit die notwendigen Inhalte haben. Die Angriffe wurden im vorherigen Kapitel untersucht. Nun ist es zunächst erforderlich, Aussagen über aktuellen Inhalte von Awareness-Trainings zu treffen, bevor der Vergleich erfolgt.
Grundlegend ist zu sagen, dass die ausgewählten Awareness-Schulungen nur einen Ausschnitt des vielfältigen Gesamtangebots darstellen. Bei der sonst willkürlichen Auswahl wurde darauf geachtet, dass verschiedene Anbieter enthalten sind und bei der Vorstellung des Angebots auf die Inhalte der jeweiligen Schulung eingegangen wird. Neben neun Angeboten für Angestellte im Allgemeinen, richtet sich ein weiteres Training speziell an Mitarbeitende in der Produktion und Fertigung. Dieses wird gesondert den anderen gegenübergestellt. Tabelle 4.1 stellt eine Übersicht dar.

Tabelle 4.1: Vergleich der Inhalte der Angebote von Awareness-Schulungen [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48]

	Is-fox	Fraunh.	TÜV Süd E-L.	TÜV Süd	Skyt. Ac.	IT-Sch.	secunet	DGC	TÜV Thü. Anw.	TÜV Thü. Fert.	Is-fox Anw.	12 Kernth.
Phishing	x	x	x		x			x	x	x	x	x
Passwort	x	x	x		x	x			x	x	x	x
Social Engineering	x	x			x	x	x	x			x	x
E-Mail	x	x	x		x		x		x	x		x
Mobiles Arbeiten/HO	x		x				x		x		x	x
Malware & Ransomware	x	x	x		x						x	x
Internet	x	x			x	x	x					x
sicherer Arbeitsplatz	x		x			x	x				x	
Bedrohungslage	x	x	x	x		x						
Cloud	x	x	x								x	x
Methoden und Angriffe	x	x		x				x				
soziale Medien	x		x			x						x
Schutz mobile Geräte	x								x		x	x
Viren	x								x	x	x	
Schutz sensibler Daten	x	x									x	
Informationsklassifizierung	x						x				x	
USB-Stick/Datenspeicher					x				x			x
Grundlage IT-Sicherheit							x	x		x		
Verschlüsselung	x								x			
Sicherheitsmaßnahmen				x					x			
Bedeutung Informationssicherheit			x	x								
Spam									x	x		
Schutz v. Anlagen & Maschinen							x			x		
Reaktionen										x	x	
Netzwerksicherheit									x	x		
Umgang mit Besuchern											x	
Signaturen									x			
IT-Security Awareness								x				
Identitätsmissbrauch									x			
Datenschutz & DSGVO									x			
Dateiendungen	x											
Cyber Awareness Audit								x				
öffentliches WLAN												x
physische Sicherheit												x
Vermeidung Schatten-IT										x		
Umgang mit Updates										x		
Sicherheitsbewusstes Arbeiten										x		
Fernwartung										x		

Die HvS-Consulting AG bietet mit IS-FOX ein breites Angebot von Kursen zum Thema Cybersicherheit an. Angeboten werden modulare Online E-Learning-Kurse mit Abschlusstests und Zertifikat. Bei der Themenauswahl ist eine individuelle Zusammenstellung möglich. Ausgewählt werden können Module zur aktuellen Bedrohungslage, zur Rolle der Angreifenden, E-Mail und Phishing, Ransomware, Viren und Schadsoftware, sichere Passwörter und Passwortmanagement, Social Engineering, sicherer Arbeitsplatz, Geschäftsreise und Home-Office, soziale Medien und Internet sowie die sichere Handhabung von technischen Geräten. [37]
Das Fraunhofer Lernlabor Cybersicherheit bietet ein dreistündiges Online-Seminar mit dem Thema „Security Awareness – Bewusstsein schaffen, Sicherheit gewinnen“ an. Zur Zielgruppe gehören alle öffentlich wirksamen Personen, Arbeitnehmer und -geber sowie Selbstständige. Inhaltlich behandelt dieses Seminar die großen Themengebiete Passwortsicherheit, Social Engineering, E-Mail-Sicherheit, Schutz sensibler Daten und sichere Internetnutzung. [38]
Ein Angebot von TÜV Süd ist ein 60-minütiges E-Learning zum Thema Cybersecurity Awareness. Inhaltlich geht es um die Gründe für Cybersecurity, die Sicherheit von E-Mail, Phishing, Ransomware, Passwörter, sicherer Arbeitsplatz und Home-Office, Internet und Cloud sowie den Umgang mit sozialen Medien. [39]
Neben der E-Learning-Schulung wird von TÜV Süd ein eintägiges firmeninternes Inhouse-Seminar zum Thema Information Security Awareness Training angeboten, um Cyberrisiken im Büroalltag zu erkennen. Als grobe Inhalte werden die Bedeutung von Informationssicherheit, aktuelle Bedrohungslage, Fallbeispiele und praktische Darstellung von Sicherheitslücken und der gängigsten Cybersicherheitsbedrohungen sowie Sicherheitsmaßnahmen genannt. [40]
SKYTALE, die Online Akademie für IT-Sicherheit der Audiocation GmbH, verfügt über ein Angebot über die Grundlagen der IT-Sicherheit in Form eines Security Awareness Trainings. Dieses kann online und zeitlich flexibel durchgeführt werden. Die vier Module werden jeweils mit einem Abschlusstest beendet. Inhaltlich behandeln die Module die vier großen Themen Sicherheit von Internet und Webseiten, E-Mail-Sicherheit, USB-Stick-Sicherheit und Passwort-Sicherheit. [41]
Der Seminaranbieter IT-Schulungen.com bietet eine eintägige Schulung unter dem Titel „IT-Security Awareness – Mitarbeitersensibilisierung“ an. Die Zielgruppe umfasst Angestellte von kleinen und großen Betrieben und Behörden sowie Benutzerbetreuende und IT-Supportmitarbeitende. Zu den Inhalten gehören aktuelle Trends und Gefahren, Social Engineering, sicherer Arbeitsplatz, Kennwörter, Internetgefahren und Gefahren der soziale Medien. Es stehen verschiedene Formen des Seminars wie firmeninterne Schulungen als Inhouse, Einzelcoaching oder auch öffentliche Schulungen mit anderen Unternehmen gemeinsam zur Verfügung. Diese können jeweils auch online durchgeführt werden. [42]
Secunet hat ebenfalls ein Security Awareness Training im Angebot. Die Trainings können individuell zusammengestellt werden und Evaluationsmaßnahmen ermöglichen eine Fortschrittsverfolgung der Ergebnisse und einen Abschlussbericht. Bei der Themenzusammenstellung kann auf verschiedene Zielgruppen wie z.B. Führungskräfte eingegangen werden. Die Themen umfassen Basissicherheit, mobiles Arbeiten und sicherer Arbeitsplatz, E-Mail-Sicherheit, Social Engineering, Internetgefahren, Informationsklassifizierung und industrielle Anlagensicherheit. [43]
Die Deutsche Gesellschaft für Cybersicherheit mbH & Co. KG verfügt über ein vielseitiges E-Learning-Programm auf einer interaktiven Plattform in Zusammenarbeit mit SoSafe zum Thema Security Awareness. Diese Schulungsmodule können individuell zusammengestellt werden und mit Hilfe des Monitorings können die Ergebnisse evaluiert werden. Zusätzlich werden auch persönliche Schulungen angeboten. Die Inhalte des Programms reichen über Grundlagen der IT-Sicherheit, Social Engineering, Securiy Awareness, Angriffsziele, Top zehn Phishing Trends und Schutzmechanismen bis hin zu praxisnahen Übungen. [44]

Ein Angebot der TÜV Akademie Thüringen ist ein 16-stündiges Live-Webinar mit dem Titel „Security Awareness – IT-Sicherheit für Anwender“. Zu den Inhalten gehören sicherheitsbewusstes und mobiles Arbeiten, Passwortsicherheit, Netzwerksicherheit, Datenspeicher und -schutz, E-Mail-Sicherheit, Phishing, Spam, Signaturen, Verschlüsselungen, Computerviren, Identitätsmissbrauch, Schutz von mobilen Geräten und allgemein die Gefahrenabwehr. [45]
Ein weiteres Angebot der TÜV Akademie Thüringen ist ein spezielles Security Awareness Training für Beschäftigte in Produktion und Fertigung. Das achtstündige Live-Webinar behandelt die Themen sicherheitsbewusstes Arbeiten in Produktion und Fertigung, Fernwartung, Vermeidung von Schatten-IT, Umgang mit Updates, Passwort-, E-Mail- und Netzwerksicherheit, Schutz von Anlagen und Maschinen, Computerviren sowie allgemeine Grundlagen der IT-Sicherheit. [46]
Im linken Abschnitt von Tabelle 4.1 ist ein Überblick der vorgestellten Awareness-Trainings mit einer Auflistung der jeweiligen Themen zu finden. Beim Vergleich fallen viele gleiche Inhalte, aber auch Unterschiede darin auf. Als eine Gemeinsamkeit, die alle Anbieter aufweisen, sind Zertifikate oder Teilnahmebescheinigungen beim Besuch der Veranstaltungen oder bei der erfolgreichen Durchführung des Lernprogramms zu nennen. Gemeinsam ist einigen der vorgestellten Schulungen das Angebot über eine interaktive Lernplattform, zur flexiblen Gestaltung und Durchführung der Schulungen. Einige Trainings sind hingegen „klassische“ Seminare, die von Dozierenden durchgeführt werden. Inhaltlich befassen sich sieben der zehn Schulungen mit den Themen Passwort- und E-Mail-Sicherheit und Phishing. Social Engineering wird in sechs der zehn Trainings behandelt. Die Hälfte der Schulungen beinhaltet Internetgefahren und die aktuelle Bedrohungslage. Mit vier von zehn Schulungen knapp unter der Hälfte werden die Themen mobiles Arbeiten, Malware und Ransomware, sicherer Arbeitsplatz und Methoden und Angriffe behandelt. Einige Spezialthemen wie Dateiendungen, Umgang mit Besuchern und weitere werden jeweils nur von einem Anbieter als Schulungsinhalt genannt. Eine besondere Rolle stellt die Schulung von TÜV Thüringen für Beschäftigte in der Fertigung und Produktion dar. Sie beinhaltet wegen der speziellen Zielgruppe einige Sonderthemen. Aber auch einige der häufigsten Themen wie Phishing, Passwort- und E-Mail-Sicherheit sind enthalten. Es wird deutlich, dass neben speziellem Sicherheits-Wissen auch in diesem Bereich das Grundlagenwissen relevant ist. Allgemein ist zu beachten, dass viele Themen miteinander in Verbindung stehen, sich sehr stark ähneln oder Kategorien eines gelisteten Themas darstellen. Beispielsweise gehört das Thema Spam zur E-Mail-Sicherheit, wird aber von einem Anbieter explizit als Inhalt genannt. In einem derartigen Zusammenhang stehen auch die Themen aktuelle Bedrohungslage sowie Methoden und Angriffe. Hier ist eine Differenzierung schwierig. Auffällig ist die Schulung von TÜV Süd, denn in der Tabelle wird deutlich, dass diese keins der häufigsten Themen beinhaltet. Das ist jedoch eine falsche Annahme, weil für diese Schulung lediglich große und verallgemeinernde Themenkomplexe genannt werden. Deshalb werden Inhalte wie Phishing oder Passwort-Sicherheit zwar nicht explizit genannt, aber sind in der Kategorie Sicherheitsmaßnahmen vermutlich doch enthalten. Zur Darstellung dieses Sachverhaltes, wird auch auf diese Schulung hier eingegangen. Dieser Aspekt gilt ebenso für alle weiteren Schulungen. Auch wenn Themen nicht explizit genannt werden, kann dennoch darauf eingegangen werden. Der Vergleich stellt deshalb nur eine Annäherung dar.
Der rechte Abschnitt der Tabelle 4.1 enthält eine Reihe von Themen für Awareness-Schulungen, die von den zwei Dienstleistenden IS-FOX und Security-Insider empfohlen werden.
Auf der Webseite von IS-FOX gibt es einen Leitfaden, der die richtigen Security-Awareness-Themen für die jeweilige Zielgruppe enthält. Die Basis richtet sich speziell an Anwender und kann thematisch jeweils für Führungskräfte, IT-Administratoren und Software-Entwickler erweitert werden. Zentrale Themen sind auch hier Phishing und Ransomware, Social Engineering, Viren und Trojaner, Passwörter, mobile Geräte, Cloud-Dienste, Umgang mit sensiblen Informationen und mit Besuchern, sicherer Arbeitsplatz und Home-Office sowie Meldewege bei Vorfällen. Führungskräfte sind zugleich auch

Anwender. Daher werden auch sie in den Grundlagen geschult. Zusätzlich haben Führungskräfte eine Vorbildfunktion und sind Entscheidungsträger in vielerlei Hinsicht. Deshalb benötigen sie zusätzliche Schulungsthemen, die sich mit diesen Funktionen beschäftigen. Dazu gehört Grundsätzliches, wie die Funktionsweise von Cyber Security im Unternehmen und ISMS sowie der Einfluss der Vorbildfunktion auf das Verhalten der Angestellten und damit auf die Sicherheit des Unternehmens. IT-Administratoren sind enorm wichtig für die Cyber Security eines Unternehmens. Fokussierte Inhalte sind bei dieser Zielgruppe technische Maßnahmen wie Patching, Vulnerability Management und technische Angriffserkennung sowie Hilfsmittel dafür. Eine große Verantwortung für die IT-Sicherheit haben auch Software-Entwickler. Es geht darum, geeignete Maßnahmen und Sicherheitsmittel schon früh zu implementieren. Stichworte hierbei sind Autorisierung und Authentisierung sowie Logging. [47]
In einem Artikel des Nachrichtenportals Security-Insider wird beschrieben, wie ein gutes Schulungsprogramm entwickelt werden kann. Als beste Schulungsprogramme werden ganzheitliche Angebote mit intuitiver Oberfläche, zum Entwerfen und Verwalten von Kampagnen genannt. Außerdem ist eine Möglichkeit zur Beobachtung des Fortschritts der Teilnehmenden wichtig, auch um am Ende Berichte zu erstellen. Das Portal für die Teilnehmenden sollte aus Lernmodulen, kurzen Videos und Wiederholungsübungen bestehen. Um ein gutes Trainingsprogramm zu entwickeln werden sechs Schritte genannt. Als erstes muss die Bestandsaufnahmen erfolgen. Darauf folgt der Entwurf und die Entwicklung und darauf die Implementierung. Nach oder während der Durchführung soll diese beobachtet und kontrolliert werden. Im fünften Schritt geht es weiter mit Auffrischung und Vertiefung sowie im Anschluss daran Evaluation und Verbesserung. Des Weiteren werden zwölf Kernthemen für Awareness-Schulungen genannt. Diese sind Phishing-Angriffe, Ransomware, Social Engineering, soziale Medien, Nutzung von Internet und E-Mail, Schutz mobiler Geräte, Wechseldatenträger, Passwörter, physische Sicherheit, mobiles Arbeiten, öffentliches WLAN und Cloud-Sicherheit. Des Weiteren ist es wichtig, die Schulungsinhalte immer auf dem aktuellen Stand zu halten und neueste Entwicklungen im Bereich Cybercrime zu beachten. [48]
Für einen besseren Vergleich dieser Leitlinien für Inhalte von Awareness-Trainings mit tatsächlichen Angeboten von Dienstleistern und Organisationen sind diese in der Tabelle im rechten Abschnitt 4.1 abgebildet. Beim Vergleich dieser beiden Leitlinien fallen viele gemeinsame Themen auf. Beide enthalten nahezu alle der häufigsten genannten Inhalte. Das ist ein gutes Zeichen für eine gute Aufstellung der betrachteten Angebote. Die meisten Unterschiede sind auf den bereits genannten Grund zurückzuführen, dass manche Themengebiete sehr umfangreich sind und andere Themen miteinbeziehen und daher nicht extra genannt werden.

4.2 Weitere Angebote und Informationen

Auf der Webseite des BSI [49] werden zu diesem Thema weitere Hinweise und Empfehlungen gegeben. Dort sind Materialien zum Schutz vor Spam, Passwortdiebstahl durch Phishing, IT-Sicherheit am Arbeitsplatz und weitere Informationen zu finden.
Weiterhin werden drei Tipps für mehr IT-Sicherheits-Awareness erläutert. So ist erstens auf eine verständliche Sprache, auch im Bezug auf Fachausdrücke, und praktische Beispiele zu achten. Die Beschäftigten sollen an ihrem individuellen Wissensstand abgeholt werden. Ein zweiter Tipp ist die Information, dass jede Arbeitskraft eine Kontaktstelle hat, an die sich bei Fragen und verdächtigen Vorkommnissen gewendet werden kann. Dabei ist es wichtig zu vermitteln, dass solches Nachfragen erwünscht und nicht als zusätzliche Belastung gesehen wird. Drittens sind Awareness-Maßnahmen besonders effektiv, wenn sie praxisnah durchgeführt werden. Dabei kann ein Gamification-Ansatz,

beispielsweise als Quiz oder Escape Room, ein gutes Motivationsmittel sein. [50]
In einer Veröffentlichung von Security-Insider zum Thema Security Awareness wird deutlich auf die Notwendigkeit nicht nur zielgruppenspezifischer, sondern auch altersgruppenspezifischer Angebote hingewiesen. Zielgruppenspezifisch meint, dass in einem Unternehmen verschiedene Rollen existieren und es unterschiedliche Aufgabengebiete und damit verschiedene Zugänge und Verantwortungen hinsichtlich IT-Sicherheit gibt. Zu den altergruppenspezifischen Inhalten gehört es, dass beispielsweise für jüngere Menschen bestimmte Themenbereiche besonders wichtig sind, weil sie dort aktiver sind. In diesem Zusammenhang sind Datensparsamkeit im Internet, Phishing durch persönliche Angaben in sozialen Medien und freizügiger Umgang mit Fotos und Videos vom Arbeitsplatz zu nennen. In anderen Themenfeldern ist der Wissensstand dieser Altersgruppe jedoch vermutlich höher. Dazu gehören die vorsichtige Nutzung von WLAN-Hotspots, Webcams, Online-Meeting-Dienste und Chatprogramme. Neben verschiedenen fokussierten Themen wird vorgeschlagen, auch die Schulungsinhalte anders zu lehren. So sollen mediale Inhalte wie Audioelemente, Videos und Fotos eingesetzt werden. Auch der Gaming-Ansatz wird als geeignetes Mittel vorgestellt, um jüngeren Menschen IT-Sicherheitsinformationen zu vermitteln. [51]

4.3 Vergleich von Cybercrime-Bedrohungslage und Awareness-Schulungen

Beim Vergleich der Berichte im Bezug auf die Bedrohungslage durch Cybercrime fällt auf, dass keine eindeutigen Aussagen darüber getroffen werden können, welche Angriffe am häufigsten aufgetreten sind. Das konkrete Auftreten der einzelnen Angriffe kann nicht so gut abgeschätzt werden, weil die Berichte verschiedene und sich teilweise widersprechende Ergebnisse liefern. Grundsätzlich ist zu sagen, dass von Malware und speziell von Ransomware eine große Bedrohung ausgeht und die mutmaßlichen Schäden gravierender sind als beispielsweise bei DDoS-Attacken. Außerdem scheint eine Unterscheidung der Eintrittsvektoren Phishing bzw. Social Engineering und IT-Schwachstellen von anderen Angriffen wichtig. Dadurch wird sich erst Zugang zum System verschafft, um weitere Angriffe durchführen zu können. Phishing bietet den Vorteil, dass es geräteunabhängig ist und stattdessen auf die geschickte Täuschung des Benutzenden angewiesen ist. IT-Schwachstellen setzen hingegen an den Geräten oder der eingesetzten Software an. Eine logische Konsequenz ist es, die Eintrittsvektoren besonders zu schützen. Dafür sind Mitarbeitersensibilisierung durch Awareness-Trainings und regelmäßige Sicherheitsupdates der Software notwendig. Der menschliche Faktor sollte nicht nur als mögliches Einfallstor, sondern auch als Schutzmechanismus gesehen werden. Dieser benötigt entsprechende Schulungen, um einen guten Wissensstand vorweisen zu können. Um mögliche Schäden durch Ransomware einzugrenzen, sind regelmäßige Backups erforderlich. Allgemein ist es wichtig, in den Schulungen zu thematisieren, welche Sicherheitsmaßnahmen existieren und sinnvoll sind und wie deren gezielte Umsetzung funktioniert. Denn trotz der Betrachtung des menschlichen Faktors als Schutzfaktor ist es relevant, auch technische Möglichkeiten zu betrachten und umzusetzen. Im Vergleich der Schutzmaßnahmen wird deutlich, dass dort teilweise starke Defizite bestehen. Das umfasst auch organisatorische und personelle Sicherheitsmaßnahmen. Auch wenn der Trend der Angriffe vermehrt hin zu Cybercrime-Delikten, also in den digitalen Raum geht, dürfen Sicherheitsmaßnahmen für die analoge Welt nicht außer Acht gelassen werden. Diese können zudem ebenfalls Angriffsmöglichkeiten für Cybercrime-Delikte darstellen.
Wie der Autor des Security-Insider-Artikels „Security Awareness ist auch eine Frage des Alters“Oliver Schonschek, schreibt, sollen Awareness-Maßnahmen nicht nur zielgruppenspezifisch sondern auch

altersspezifisch ausgerichtet sein [51, S. 7–10]. Im Digitalbarometer 2021 wird festgestellt, dass sich jüngere Menschen vorwiegend sicher fühlen und durchschnittlich nur drei Sicherheitsmaßnahmen einsetzen. Das liegt unter dem Gesamtdurchschnitt von vier Maßnahmen. [35, S. 12–13] Damit zeigt sich ein spezielles Informationsbedürfnis dieser Altersgruppe, das auch in Awareness-Kampagnen berücksichtigt werden sollte.
Bei der Themenwahl der Awareness-Schulungen bietet sich ein Vergleich mit dem Informationswunsch der Befragten im Digitalbarometer 2021 an. Dort zeigt sich, dass die Themen sichere Passwörter und Cloud-Sicherheit im Vergleich mit den anderen Themen unattraktiv sind. Die meisten wünschen sich Hinweise, um Internetkriminalität zu erkennen. Auch der Schutz sensibler Daten ist ein beliebtes Thema. [35, S. 12–13] Die Inhalte der Awareness-Schulungen deuten darauf hin, dass sichere Passwörter, die Bedrohungslage und Methoden und Angriffen wichtige Themengebiete sind. Der Schutz sensibler Daten befindet sich im Mittelfeld, ebenso wie Cloud-Sicherheit. Damit zeigt sich ein widersprüchliches Bild. Doch auch wenn ein Thema weniger gewünscht ist, kann nicht automatisch davon ausgegangen werden, dass alle über Wissen dazu verfügen oder dieses sogar einsetzen. Außerdem ist zu beachten, dass Awareness-Schulungen sich an Unternehmen richten, während das Digitalbarometer allgemein Internetnutzende befragt.
Bei der Untersuchung der Inhalte von Awareness-Schulungen ist ein breites Themenspektrum festzustellen. Dieses zeigt sich auch in den möglichen Angriffsarten. Daher sind die Themen grundsätzlich passend gewählt. Weiterhin scheinen altersspezifische und besonders an das Unternehmen angepasste Inhalte sinnvoll. Besonderer Wert sollte außerdem auf gut nachvollziehbare und realitätsnahe Beispiele gelegt werden. Schwerpunkte für Awareness-Seminare sollten definitiv Phishing und Social Engineering sowie andere Eintrittsvektoren wie Malware in E-Mail-Anhängen oder manipulierte Speichermedien sein. Grundsätzlich sind alle Inhalte wichtig und keins der genannten Themen kann ausgeschlossen werden.

5 Diskussion

Nachdem die Ergebnisse im vorherigen Teil beschrieben, interpretiert und einander gegenübergestellt wurden, beschäftigt sich dieses Kapitel nun mit der Einordnung dieser Erkenntnisse. Dafür werden diese kritisch hinterfragt, die Erwartungen dieser Arbeit eingeschätzt und ein Ausblick auf weitere Forschungsmöglichkeiten gegeben.

5.1 Ergebnisse

Zusammenfassend ist zu sagen, dass die Bedrohung durch Cybercrime zunimmt und Menschen sich vor Internetkriminalität im Allgemeinen fürchten. Zu den 2021 stattgefundenen Cyber-Angriffen können keine genauen Zahlen genannt werden. Von mehreren Berichten werden Ransomware und DDoS-Attacken als Hauptbedrohungen für Staat, Gesellschaft und Wirtschaft genannt. Im Zuge der Corona-Pandemie mit der verstärkten Digitalisierung ist keine signifikante Steigerung der Angriffszahlen festzustellen. Es lässt sich sagen, dass eine steigende Bedrohlichkeit der entstandenen Schäden wahrgenommen wird. Um dies einzuschränken wird zunehmend mehr in IT-Sicherheit investiert und es werden mehr Sicherheitsmaßnahmen eingesetzt. Jedoch besteht in dieser Hinsicht noch Nachholbedarf. In Zukunft wird weiterhin ein großer Einfluss von Cybercrime auf das Sicherheitsgefühl der Menschen gesehen und eine wachsende Bedrohung erwartet. Von der Politik wird sich mehr Unterstützung in verschiedenen Formen im Kampf gegen Internetkriminalität gewünscht. Die inhaltlichen Schwerpunkte von Awareness-Maßnahmen werden aus dem Vergleich heraus als geeignet und passend eingeschätzt. Dabei ist zu beachten, dass Praxisnähe mit vielen anschaulichen Beispielen ein wichtiger Aspekt einer guten Mitarbeitersensibilisierung darstellt. Außerdem kommen zielgruppenorientierten und altersspezifischen Schulungen eine große Bedeutung zu.
Die erwarteten Ergebnisse dieser Bachelorarbeit wurden nur teilweise erfüllt. Das Ausmaß der verschiedenen Angriffe, also welche Angriffsart am häufigsten und welche am wenigsten auftritt, ist nicht eindeutig bestimmbar. Im Allgemeinen wurde eine höhere Übereinstimmung der Werte der verschiedenen Studien und Berichte erwartet. Daraus sollte dann geschlussfolgert werden, welche die meisten Angriffe sind und Empfehlungen ausgesprochen werden, dass auf diese besonderer Fokus in Awareness-Maßnahmen gelegt werden sollte. Zu den Inhalten von Awareness-Schulungen bleibt zu sagen, dass diese sich an der aktuellen Bedrohungslage orientieren sollten, um auf dem neuesten Stand zu bleiben und auf mögliche neue Entwicklungen schnell reagieren zu können. Wie die Berichte zeigen, finden sowohl im wirtschaftlichen als auch im privatem Bereich Angriffe statt und es besteht Handlungsbedarf in der Abwehr dieser Attacken. Das lässt die Schlussfolgerung zu, dass Awareness-Schulungen so ausgelegt sein sollten, dass sie nicht nur für die Unternehmen einen Mehrwert bringen, sondern auch für das Privatleben mit technischen Geräten und Internet nützlich sind. Dem schließt sich an, dass in verschiedenen Aspekten ein Zusammenhang zwischen privat und Unternehmen besteht. So können beispielsweise in Sozialen Netzwerken veröffentlichte Medien aus dem Alltag möglicherweise von Angreifenden für gezieltes Social Engineering oder Phishing (Spear-Phishing) genutzt werden und damit neue Angriffspunkte darstellen. Deshalb scheint es wichtig, nicht nur das Verhalten der Mitarbeitenden im Unternehmen zu schulen, sondern darüber hinaus allgemeine Hinweise für sicheres Verhalten im Internet zu geben. Die Frage nach einer tieferen Erforschung des Dunkelfeldes zu beantworten und Aussagen darüber durch den Vergleich

der Berichte und Studien zu treffen, kann nicht erfolgen. Dafür unterscheiden sich die Ergebnisse der einzelnen Berichte zu stark. Zur Cybercrime-Entwicklung der letzten Jahre ist festzustellen, dass die Bedrohungslage zwar weiter zunimmt, jedoch keine signifikanten Steigerungen seit Beginn der Corona-Pandemie erkennbar sind. Ein möglicher Grund dafür kann die ebenfalls wachsende Entwicklung im Bereich der Sicherheitsmaßnahmen und Investitionen in die IT-Sicherheit sein. Bei der Untersuchung der stattgefundenen Angriffe 2021 entwickelten sich zwei Thesen oder Fragestellungen, die es zu analysieren galt. Dafür wurde nach den Gründen für die geringer gewordene Anzahl an Angriffen in der Wirtschaft [29, S. 2] [30, S. 6] gefragt, speziell, ob dafür die verstärkte Umsetzung von Sicherheitsmaßnahmen ursächlich sein kann. Dafür liefert die Studie zu den Sicherheitsmaßnahmen 2021 des Bitkom das Ergebnis, dass fast alle Maßnahmen im Vergleich zum Vorjahr Anstiege aufweisen [33, S. 3–5]. Somit ist dies als Grund denkbar. Bei der Analyse der Angriffszahlen in Privathaushalten wird deutlich, dass die Anzahl zugenommen hat [34, S. 7–8] [35, S. 6–9]. Doch auch der Einsatz von Sicherheitsmaßnahmen ist beliebter geworden [34, S. 9–11] [35, S. 4–5]. Somit kann die aufgestellte These, dass Angriffe aufgrund weniger eingesetzter Sicherheitsmaßnahmen gestiegen sind, nicht gestützt werden.

5.2 Vergleich mit der Studie des Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste (WIK)

Die in der Einleitung erwähnte Studie des WIK aus dem Jahr 2017 hatte es sich zum Ziel gesetzt, KMU hinsichtlich IT-Sicherheit zu untersuchen, diese Ergebnisse auszuwerten und danach Empfehlungen dafür auszusprechen. Neben einer eigenen Befragung von 1508 Unternehmen wurden Experteninterviews durchgeführt und Studien mit hoher Relevanz für das Thema gesichtet und ausgewertet. [1, S. 11–12] Bei der Betrachtung der Studien ergaben sich folgende Ergebnisse [1, S. 35–36]: die meisten Menschen nahmen eine wachsende Bedrohungslage war. Außerdem wird insgesamt der Eindruck der Ergebnissen bestätigt, den die Studie auch während ihrer eigenen durchgeführten Umfrage erhielt. Demnach ist ein Basisschutz im technischen Bereich wie Firewall oder Virenscanner in der Mehrheit der Unternehmen im Einsatz.
Es folgt ein kurzer Vergleich einiger Hauptaspekte der vom WIK selbst durchgeführten Umfrage mit den Ergebnissen der Studien zum Jahr 2021. Als hauptsächliche Ursachen für IT-Probleme nannten Unternehmen in der Umfrage des WIK am häufigsten Fehler von Angestellten durch Irrtum oder Nachlässigkeit sowie Technikausfall. Mehr als die Hälfte gab an, dass die Systeme häufig durch Außentäter absichtlich manipuliert wurden. Deutlich geringer ist die Zahl derer, die von Spionage durch Nachrichtendienste oder konkurrierenden Unternehmen oder absichtlicher Manipulation von Innentätern betroffen waren. [1, S. 49] Ähnlich zu dieser Auflistung der Täterkreise sind die des Wirtschaftsschutzberichts 2022 [29, S. 10–11] und des Internetverbands eco [30, S. 11], wie genauer in der Gegenüberstellung dieser beiden Berichte auf Seite 56 dieser Bachelorarbeit zu lesen ist. Als Gemeinsamkeit erweisen sich die häufigen Angriffe durch Außentäter, profitgetriebene Cyberkriminelle, sowie organisierte Kriminalität und Privatpersonen, welche alle eine ähnliche Tätergruppierung bezeichnen. Außerdem sind die niedrigen Vorkommen von Spionage durch Nachrichtendienste und konkurrierende Unternehmen ähnlich. Gering unterschiedlich ist das Aufkommen von absichtlichen Innentätern. Der Bericht des WIK und die eco-Umfrage verorten diese als weniger vorkommend, während die Wirtschaftsschutzstudie zu dem Ergebnis kommt, dass diese mittelhäufig vorkommen. Deutlich unterschiedlich werden unbeabsichtigte Vorfälle durch Innentäter, sogenannte Cyberunfälle

wahrgenommen. Diese machten laut WIK den größten Teil der Vorfälle aus, jedoch in den Berichten von 2021 nicht. Daraus ergibt sich die Feststellung, dass im Bereich der Täterkreise wenig Veränderungen im Verlauf der letzten vier Jahre stattgefunden haben. Lediglich absichtlich Vorfälle durch Innentäter sind zurückgegangen. Im Bezug auf die Umsetzung von Sicherheitsmaßnahmen ist zu beobachten, dass die durchgeführte Befragung des WIK 2017 insgesamt höhere Prozentwerte bei der Umsetzung der Sicherheitsmaßnahmen feststellte [1, S. 51–55], als in dieser Arbeit über das Jahr 2021. Das betrifft sowohl technische, organisatorische als auch personelle Maßnahmen. Jedoch ist bei diesem Vergleich anzumerken, dass die hier betrachteten Werte von 2021 sich in den verschiedenen Umfragen teilweise deutlich unterscheiden. Ebenso wie in dieser Arbeit wurde in der Umfrage 2017 festgestellt, dass Mitarbeiterschulungen noch ausbaufähig sind [1, S. 72]. Kostenlose Schulungen liegen vorn und werden dicht von kostenpflichtigen Schulungen gefolgt. In diesem Bereich liegt auch die Beauftragung eines Beraters für IT-Sicherheit. Auffallend ist die in allen Antwortmöglichkeiten höhere Zustimmung von größeren KMU als von kleineren KMU. Das zeigt die starke Abhängigkeit von der Unternehmensgröße. [1, S. 72–73] Die WIK-Studie lieferte die folgenden zusammenfassenden Informationen und Handlungsempfehlungen [1, S. 88–91]. Wie festgestellt wurde, ist der technische Schutz bereits ausreichend vorhanden und es sollte sich deshalb auf andere Maßnahmen fokussiert werden, z.B. organisatorische und personelle. Trotz einer steigenden Awareness werden noch zu wenig konkrete Maßnahmen umgesetzt. Diese Ergebnisse stimmen mit den in dieser Arbeit entwickelten Erkenntnissen in großen Teilen überein. Somit bestehen keine großen Unterschiede im Bereich der IT-Sicherheit von 2017 zu 2021. Die Unterschiedlichkeit der konkreten Zahlenwerte zeigt das Auf und Ab der Werte, dass auch bei der Betrachtung anderer Studien im Vergleich der Jahre auffällt. Das Thema bleibt weiterhin relevant und darf nicht vernachlässigt werden. Die Relevanz des Themas wird durch das hohe Schadenspotenzial von Cybercrime unterstützt. Außerdem ist dieser Deliktbereich von einer mutmaßlich hohen Dunkelziffer geprägt und Cyber-Angriffe werden zudem teilweise nicht oder stark verzögert bemerkt. Daher gilt es die Sensibilisierung für das Thema zu erhöhen.

5.3 Herausforderungen und Beschränkungen

Einige Beschränkungen der in dieser Arbeit entwickelten Ergebnisse wurden bereits genannt. Dazu gehört die Unterschiedlichkeit der Berichte und Studien. Ein Unterscheidungsmerkmal, welches in den meisten Abschnitten berücksichtigt wurde, ist der Bezug der Berichte zur Wirtschaft, allgemein zur Gesellschaft in Privathaushalten oder einer Mischung daraus. Weiterhin ist anzumerken, dass die PKS nicht zwischen Privatpersonen und Unternehmen unterscheidet. Zudem werden einige Angriffsarten erläutert und betrachtet, die speziell für Staaten wichtig sind und sich auf Privathaushalte oder Unternehmen nur bedingt auswirken. Im wirtschaftlichen Sektor hat zusätzlich die Unternehmensgröße einen Einfluss auf die Ergebnisse, welche in den Berichten unterschiedlich berücksichtigt wird. Dazu gehört auch die Definition von KMU, denn darunter können je nach betrachteter Studie teilweise unterschiedliche Mitarbeiterzahlen verstanden werden. Außerdem variiert die Stichprobengröße der einzelnen Umfragen sehr stark. Auch die Inhalte weichen teilweise stark voneinander ab. Manche Themengebiete werden in nahezu allen Berichten thematisiert, andere nur in einem einzigen. Dieser Umstand wirkt sich negativ auf die Vergleichbarkeit aus, sodass vereinzelt keine Vergleiche möglich sind oder daraus weniger wertvolle Aussagen oder ganz allgemein keine eindeutige Aussagen generiert werden können. Im Allgemeinen sollten die Zahlen der Berichte und Studien nur vorsichtig bewertet und nicht als eindeutig eingeschätzt werden. Die Umfragen repräsentieren teilweise nur die

eigenen Kunden und somit existiert keine vollumfängliche und eindeutige Statistik. Das zeigen die zum Teil stark unterschiedlichen Werte. Zudem wird von einem großen Dunkelfeld ausgegangen. Ein weiteres Problem stellt die geringe Beachtung des Unterschieds zwischen Angriffs- oder Eintrittsvektor und den Folge-Angriffen daraus dar. Bei der Betrachtung der stattgefundenen Angriffe wird dies in den meisten Studien nicht berücksichtigt und erschwert dadurch den Vergleich. Denn Angriffsvektoren kommen zwangsläufig häufiger vor als Folge-Angriffe. Jedoch ist eine Differenzierung aufgrund verschiedener Überschneidungen der Angriffe schwierig. Als weitere Beschränkung der Ergebnisse ist die Tatsache zu nennen, dass sich in dieser Arbeit auf das Jahr 2021 bezogen wird, weil der Lagebericht des BSI immer erst im Mai des Folgejahres erscheint. Damit ist die Aktualität der Ergebnisse eingeschränkt. Eine Herausforderung und sogleich ein Kritikpunkt in der zeitlichen Komponente der Arbeit sind die verschiedenen Zeitpunkte der Durchführung der Umfragen. Dabei wurde versucht darauf zu achten, dass sich bei der Betrachtung der Angriffe rückwirkend auf das 2021 bezogen wird und Sicherheitsmaßnahmen während des Jahres 2021 betrachtet werden. Dieses Handeln war jedoch nicht bei allen Berichten möglich. Des Weiteren ist die Auswahl der Awareness-Schulungen für den Vergleich der Inhalte willkürlich ausgefallen und ist deshalb nur begrenzt repräsentativ. Zu diesem Themenbereich gehört außerdem, dass Awareness-Trainings mit sinnvollen Inhalten und guter Lehre nicht grundsätzlich darauf schließen lassen, dass Mitarbeitende sich diese zu Herzen nehmen und danach handeln. Es werden lediglich gute Voraussetzungen geschaffen. Grundsätzlich bleibt zu sagen, dass die vollumfängliche und tiefgehende Untersuchung des gesamten komplexen Themas den Umfang dieser Bachelorarbeit überschreiten würde.

5.4 Ausblick und weiterführende Forschungsideen

Das führt zum nächsten Aspekt, der Empfehlung für weiterführende Forschungsmöglichkeiten. In einem größerem Umfang und bei genauerer Analyse kann das Thema besser erforscht werden. Außerdem ist der zeitliche Fokus auf das vergangene Jahr 2022 ein neuer thematischer Schwerpunkt und bietet aktuelle Ergebnisse. Weiterhin können durch einen größeren Vergleich mit mehr Studien und Berichten möglicherweise besser Aussagen zu den genannten Themen und zur Erforschung des Dunkelfelds getroffen werden. Die WIK-Studie von 2017 zeigt außerdem das Potenzial einer eigenen durchgeführten Umfrage. Dabei kann auf fokussierte Themen eingegangen werden, der Umfang selbst bestimmt werden und Fragen nach eigenem Ermessen formuliert und Antwortmöglichkeiten entwickelt werden. Durch die Untersuchung einer möglichen Differenzierung von Angriffs- oder Eintrittsvektoren und Folge-Angriffen daraus und der Betrachtung der zahlenmäßig stattgefundenen Angriffe können möglicherweise Empfehlungen dazu gegeben werden, ob es Chancen bietet, diese Angiffe in zukünftigen Befragungen getrennt voneinander zu betrachten. Die Fokussierung in einer weiteren Forschung auf die Wirtschaft, staatliche Behörden oder Privathaushalte ermöglicht eine tiefer gehende Untersuchung. Aber auch der Vergleich dieser drei Bereiche bietet neue Forschungsmöglichkeiten. Als weiterer möglicher neuer Untersuchungsgegenstand sind die Gründe zu nennen, aus denen Maßnahmen nicht oder noch nicht umgesetzt werden. Auch die genauere Betrachtung der verschiedenen Altersgruppen bietet Forschungspotenzial. Aus diesen Ergebnissen können mögliche neue Ansätze für der Empfehlung von Sicherheitsmaßnahmen und Inhalte von Awareness-Schulungen entwickelt werden.

6 Fazit

Das Ziel der vorliegenden Bachelorarbeit war es, Aussagen darüber zu treffen, welche Angriffsarten häufig und welche weniger häufig im Jahr 2021 stattfanden. Zu diesem Aspekt sind jedoch keine eindeutigen Aussagen möglich.
Mehrere Berichte stellen Ransomware und DDoS als Hauptbedrohungen dar. Ransomware, oder Malware im Allgemeinen, spielt besonders in der Wirtschaft eine große Rolle. Zudem ist die Produktion neuer Malware-Varianten weiter angestiegen. DDoS-Angriffe sind qualitativ und quantitativ angestiegen. Außerdem sind Cyber-Erpressungen ein häufig vorkommendes Phänomen. Ein Indiz auf vermehrten Datenbetrug und Diebstahl sind die steigenden Zahlen von Data-Leaks. IT-Schwachstellen, sowohl in Hardware als auch in Software, bilden Eintrittsvektoren für weitere Angriffe. Phishing stellt einen weiteren Eintrittsvektor dar und findet zumeist über E-Mail-Kommunikation statt. Eine große Bedrohung geht auch von Supply-Chain-Angriffen aus. Bei der Betrachtung der Täterkreise gestaltet sich die Differenzierung der einzelnen Akteure zunehmend schwieriger, weil sich das Niveau der Angriffe angleicht. Unterschiede sind nunmehr lediglich anhand der Motivationslage gegeben. Beim Umgang mit Cyber-Angriffen zeigt sich, dass diese meist selbst und intern gelöst werden. Zu konkreten Schadenssummen in Folge von Cyber-Angriffen können keine validen Aussagen getroffen werden. Es ist zu beachten, dass sich Schäden nicht nur finanziell auswirken können. Die Investitionen in IT-Sicherheit im Allgemeinen steigen und es werden mehr Sicherheitsmaßnahmen umgesetzt. Cybercrime wird auch in Zukunft als starke Bedrohung eingeschätzt und sich mehr Unterstützung durch Polizei und Politik gewünscht.
Aus den erwarteten Ergebnissen zur Anzahl der Angriffe sollte auf sinnvolle und notwendige Inhalte von Awareness-Schulungen geschlossen werden. Dazu lässt sich sagen, dass die analysierten Awareness-Trainings ein breites Spektrum an Themen beinhalten und damit die Vielfalt der möglichen Angriffe umfassen. Eine Priorisierung der Themen scheint nicht relevant zu sein. Ein wichtiger Aspekt bei diesem Thema ist der Fokus auf zielgruppenspezifische und altersspezifische Sensibilisierungsmaßnahmen. Außerdem werden anschauliche Beispiele und allgemein ein hoher Praxisbezug der Schulungen zum Erfolg förderlich gesehen.
Eine weitere Erwartung in diese Arbeit war es, durch den Vergleich der verschiedenen Berichte und Umfrageergebnisse Eindrücke über das mutmaßlich große Dunkelfeld zu gewinnen und darüber Aussagen treffen zu können. Aufgrund der Unterschiedlichkeit der einzelnen Berichte ist dies nicht möglich.
Trotz dieser Umstände ist es möglich, Erkenntnisse zur Entwicklung von Cybercrime im Laufe der Zeit zu gewinnen. Demnach nimmt die Bedrohungslage immer weiter zu, wobei keine signifikante Steigerung im Zuge der Corona-Pandemie festzustellen ist. Im Vergleich mit der Studie des WIK zeigt sich die weiterhin relevante Sachlage und die Schwierigkeiten beim Vergleich. Außerdem wird die Bedeutung einer eigenen durchgeführten Umfrage deutlich. Die Beschränkung, dass die Ergebnisse von 2021 nun nicht mehr aktuell sind, wird durch den Beginn des Ukraine-Kriegs und der damit einhergehenden zunehmenden Bedrohung und Wahrnehmung von Cyberangriffen bestätigt und verstärkt. Es besteht die Schwierigkeit, aktuelle Berichte zu analysieren und dennoch zeitnah Erkenntnisse aus dem Vergleich zu liefern. Dies kann Schwerpunkt in weiteren Untersuchungen sein.

Anhang A: Übersicht der betrachteten Studien

Tabelle A.1: Übersicht der betrachteten Studien [10], [23], [5], [28], [29], [30], [31], [33], [34], [35], [36]

	Bundeslagebild Cybercr.	Lage der IT-Sicherheit	Cyber Security Report	Wirtschaftsschutz	eco Umfrage Internets.	DsiN-Praxisreport	Sicherheitsmaßnahmen	IT- und Cybersicherheit	Digitalbarometer
Herausgeber	BKA	BSI	Deloitte	Bitkom e.V.	eco – Verband der Internetwirtschaft e.V.	DsiN	Bitkom e.V.	Bitkom e.V.	BSI & Polizeiliche Kriminalprävention der Länder und des Bundes
Veröffentlichung	Mai 2022	2021: September 2021 2022: Oktober 2022	August 2021	31. August 2022	17. Februar 2022	keine Angabe	14. Oktober 2021	14. Dezember 2021	2021: September 2021 2022: November 2022
Methode bzw. Basis	PKS & externe Quellen	BSI-Quellen & externe Quellen	Befragung	Computer Assisted Telephone Interview (CATI)	Online-Umfrage	Fragebögen	keine Angabe	telefonische Befragung	Computer Assisted Web Interviewing (CAWI)
Befragungszeitraum	keine Befragung	keine Befragung	keine Angabe	10. Januar bis 13. März 2022	Ende 2021	Mai 2020 bis Januar 2022	keine Angabe	November 2021	2021: April bis Mai 2021 2022: April bis Mai 2022
Befragungsgruppe	keine Befragung	keine Befragung	Politik und Wirtschaft	Wirtschaft	Wirtschaft	Wirtschaft	Wirtschaft	allg. Internetnutzende	allg. Internetnutzende
Umfang	keine Befragung	keine Befragung	508	1066	145	1339	1067	1011	2021: 2025 2022: 2000
Inhalte:									
Bedrohungslage	Entwicklung Fallzahlen	x		x	x	x		x	
stattgefundene Angriffe				x	x	x		x	x
Malware, Ransomware	x	x							
Data-Leaks	x	x							
DDoS	x	x							
IT-Schwachstellen	x	x							
Phishing	x	x							
Spam	x	x							
Supply-Chain-Angriffe	x	x							
Cloud-Anwendungen		x				x			
Täterkreise	x			x	x				
Schäden	Wirtschaftsschutz 2021			x	x	x			x
Investitionen IT-Sicherheit				x	x				
Umgang mit Angriffen					x				x
IT-Sicherheit Unternehmen					x	x			
techn. Sicherheitsmaßn.						x	x	x	x
pers. Sicherheitsmaßn.						x	x		
org. Sicherheitsmaßn.							x		
Gefährdungen d. C.-Pandemie		x			x				
Politische Maßnahmen				x				x	
Sonderthemen	• Underground Economy	• Botnetze • APT • Hybride Bedrohungen • Ergebnisse Digitalbarometer • Mediale Identitäten • Wirtschaft • Gefährdungslage der Bundesverwaltung	• Cyber-Risiken in Deutschland 2021	• Datendiebstahl • Social-Engineering • Zukünftige Bedrohungen	• Bedeutung von Sicherheitsthemen • Zukünftige Veränderungstreiber			• Sicherheitsgefühl für persönliche Daten	• internetfähige Geräte • Internetnutzung • Online-Aktivitäten in Corona-Pandemie • Informationswünsche

Literaturverzeichnis

[1] A. Hillebrand, A. Niederprüm, S. Schäfer, S. Thiele und I. Dr. Henseler-Unger, *Aktuelle Lage der IT-Sicherheit in KMU*, WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH (Hrsg.), Bad Honnef, Dez. 2017. Adresse: https://www.wik.org/fileadmin/files/_migrated/news_files/WIK-Studie_Aktuelle_Lage_der_IT-Sicherheit_in_KMU_Langfassung__2_.pdf.

[2] Bundeskriminalamt (Hrsg.), *Cybercrime*. Adresse: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html (besucht am 12. Jan. 2023).

[3] Bundeskriminalamt (Hrsg.), *Lageprodukte aus dem Bereich Cybercrime - QR Code 1: Die Polizeiliche Kriminalstatistik (PKS)*. Adresse: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2021/Code1.html (besucht am 15. Jan. 2023).

[4] Cornelsen Verlag GmbH (Hrsg.), *Cyberattacke*. Adresse: https://www.duden.de/rechtschreibung/Cyberattacke (besucht am 1. Apr. 2023).

[5] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), *Die Lage der IT-Sicherheit in Deutschland 2022*, Bonn, Okt. 2022. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=8.

[6] Bundeskriminalamt (Hrsg.), *Lageprodukte aus dem Bereich Cybercrime - QR Code 4: Eintrittsvektoren*. Adresse: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2021/Code4.html (besucht am 15. Jan. 2023).

[7] Bundeskriminalamt (Hrsg.), *Lageprodukte aus dem Bereich Cybercrime - QR Code 5: Schadprogramme*. Adresse: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2021/Code5.html (besucht am 15. Jan. 2023).

[8] Bundeskriminalamt (Hrsg.), *Lageprodukte aus dem Bereich Cybercrime - QR Code 6: DDoS - Distributed Denial of Service*. Adresse: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2021/Code6.html (besucht am 15. Jan. 2023).

[9] Bundeskriminalamt (Hrsg.), *Lageprodukte aus dem Bereich Cybercrime - QR Code 7: Täter*. Adresse: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2021/Code7.html (besucht am 15. Jan. 2023).

[10] Bundeskriminalamt (Hrsg.), *Bundeslagebild Cybercrime 2021*, Mai 2022. Adresse: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.pdf?__blob=publicationFile&v=6.

[11] Bundeskriminalamt (Hrsg.), *Lageprodukte aus dem Bereich Cybercrime - QR Code 2: Die Underground Economy*. Adresse: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2021/Code2.html (besucht am 15. Jan. 2023).

[12] K. Weber, A. Schütz und T. Fertig, *Grundlagen und Anwendung von Information Security Awareness: Mitarbeiter zielgerichtet für Informationssicherheit sensibilisieren* (Essentials). Wiesbaden: Springer Vieweg, 2019, ISBN: 9783658262587. Adresse: https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=5771304.

[13] S. Richter, T. Straub und C. Lucke, „Information Security Awareness – eine konzeptionelle Neubetrachtung“, *Multikonferenz Wirtschaftsinformatik 2018*, S. 1369–1380, Adresse: https://wwwlehre.dhbw-stuttgart.de/~tstraub/download.php?file=MKWIpaper.

[14] Bundeskriminalamt (Hrsg.), *Bundeslagebild Cybercrime 2020*, Apr. 2021. Adresse: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.pdf?__blob=publicationFile&v=5.

[15] Hasso-Plattner-Institut für Digital Engineering gGmbH (Hrsg.), *Identity Leak Checker*. Adresse: https://sec.hpi.de/ilc/statistics (besucht am 16. März 2023).

[16] Anti-Phishing Working Group (Hrsg.), *Phishing Activity Trends Reports*. Adresse: https://apwg.org/trendsreports/ (besucht am 16. März 2023).

[17] Trend Micro Research (Hrsg.), *Attacks From All Angles: 2021 Midyear Cybersecurity Report*. Adresse: https://documents.trendmicro.com/assets/rpt/rpt-attacks-from-all-angles.pdf.

[18] Coveware (Hrsg.), *Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority*. Adresse: https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority (besucht am 16. März 2023).

[19] SonicWall (Hrsg.), *SONICWALL CYBER THREAT REPORT*. Adresse: https://www.sonicwall.com/medialibrary/de/infographic/2021-mid-year-update-sonicwall-cyber-threat-report.pdf.

[20] Coveware (Hrsg.), *Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021*. Adresse: https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021 (besucht am 16. März 2023).

[21] Link11 GmbH (Hrsg.), *DDOS-REPORT für das Jahr 2021*, Frankfurt, 9. Dez. 2021. Adresse: https://www.link11.com/de/downloads/ddos-report-2021/.

[22] A. Malatras, V. Valeros, I. Lella, E. Tsekmezoglou, M. Theocharidou und S. Garcia, *ENISA threat landscape for supply chain attacks*, European Union Agency for Cybersecurity (Hrsg.), 2. Aug. 2021. DOI: 10.2824/168593. Adresse: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

[23] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), *Die Lage der IT-Sicherheit in Deutschland 2021*, Bonn, Sep. 2021. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf?__blob=publicationFile&v=4.

[24] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), *Ausgabe 10/2022: Neue Malware- und PUA-Varianten*, Bonn. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Statistikberichte/Bedrohungslage-allgemein/Malware/xls-csv/Malware-Statistik2210.html (besucht am 12. Apr. 2023).

[25] The Record (Hrsg.), *Ransomware tracker: the latest figures*. Adresse: https://therecord.media/ransomware-tracker-the-latest-figures (besucht am 16. März 2023).

[26] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), *Ausgabe 12/2021: E-Mails und Spam-E-Mails in der Wirtschaft in Deutschland*. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Statistikberichte/Bedrohungslage-allgemein/Spam/xls-csv/Spam-W2112.html (besucht am 12. Apr. 2023).

[27] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), *Ausgabe 09/2022: E-Mails und Spam-E-Mails an die Bundesverwaltung*. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Statistikberichte/Bundesverwaltung/Spam/xls-csv/Spam-BV2210.html (besucht am 12. Apr. 2023).

[28] Deloitte (Hrsg.), *Cyber Security Report 2021: Wahljahr 2021 – digitale Meinungsbildung ein Risiko*, Aug. 2021. Adresse: https://www2.deloitte.com/de/de/pages/risk/articles/cyber-security-report.html.

[29] Achim Berg, *Wirtschaftsschutz 2022*, Bitkom e.V. (Hrsg.), Berlin, 31. Aug. 2022. Adresse: https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf.

[30] eco - Verband der Internetwirtschaft e.V. (Hrsg.), *eco Umfrage Internetsicherheit 2022*, 17. Feb. 2022. Adresse: https://www.eco.de/presse/eco-it-sicherheitsumfrage-2022-unternehmen-reagieren-auf-angespannte-cybersicherheitslage/.

[31] Deutschland sicher im Netz e.V. (Hrsg.), *DsiN-Praxisreport 2021/22 Mittelstand@IT-Sicherheit*, Berlin, Juni 2022. Adresse: https://www.sicher-im-netz.de/file/13823/download?token=Z4uX0d1v.

[32] Deutschland sicher im Netz e.V. (Hrsg.), *DsiN-Sicherheitscheck*. Adresse: https://www.sicher-im-netz.de/dsin-sicherheitscheck (besucht am 19. Jan. 2023).

[33] Bitkom e.V. (Hrsg.), *Sicherheitsmaßnahmen 2021: Wie sich Deutschlands Unternehmen gegen Diebstahl, Spionage und Sabotage schützen*, Berlin, 14. Okt. 2021. Adresse: https://www.bitkom.org/sites/main/files/2021-10/bitkom-charts-sicherheit-in-der-dt.-wirtschaft-14-10-2021_0.pdf.

[34] Achim Berg, *IT- und Cybersicherheit 2021*, Bitkom e.V. (Hrsg.), Berlin, 14. Dez. 2021. Adresse: https://www.bitkom.org/sites/main/files/2021-12/bitkom-charts-it-und-cybersicherheit-14-12-2021.pdf.

[35] Bundesamt für Sicherheit in der Informationstechnik und Polizeiliche Kriminalprävention der Länder und des Bundes (Hrsg.), *Digitalbarometer 2021: Bürgerbefragung zur Cyber-Sicherheit*, Bonn. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2021.pdf?__blob=publicationFile&v=2.

[36] Bundesamt für Sicherheit in der Informationstechnik und Polizeiliche Kriminalprävention der Länder und des Bundes (Hrsg.), *Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit 2022*, Bonn. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2022.pdf?__blob=publicationFile&v=3.

[37] HvS-Consulting AG (Hrsg.), *Cyber und IT Security Training für Mitarbeiter*. Adresse: https://www.is-fox.com/de/cyber-security-training-fur-mitarbeiter/ (besucht am 23. März 2023).

[38] Fraunhofer Academy (Hrsg.), *Security Awareness - Bewusstsein schaffen, Sicherheit gewinnen*. Adresse: https://www.cybersicherheit.fraunhofer.de/de/kursangebote/organisatorische-it-sicherheit/security-awareness.html (besucht am 19. März 2023).

[39] TÜV SÜD Akademie GmbH (Hrsg.), *Cybersecurity Awareness - E-Learning*. Adresse: https://www.tuvsud.com/de-de/store/akademie/seminare-management/informationssicherheit/it-sicherheit/1712003 (besucht am 20. März 2023).

[40] TÜV SÜD Akademie GmbH (Hrsg.), *Information Security Awareness Training | TÜV SÜD Akademie*. Adresse: https://www.tuvsud.com/de-de/store/akademie/themenwelt/informationssicherheit/information-security-awareness-training (besucht am 21. März 2023).

[41] SKYTALE Online-Akademie für IT-Sicherheit (Hrsg.), *Security Awareness Training - SKYTALE Akademie für IT-Sicherheit*. Adresse: https://skytale.academy/security-awareness-online-training/ (besucht am 20. März 2023).

[42] IT-Schulungen.com (Hrsg.), *IT-Security Awareness – Mitarbeitersensibilisierung*. Adresse: https://www.it-schulungen.com/seminare/security/it-grundschutz-u-gstool/it-security-awareness-mitarbeitersensibilisierung.html (besucht am 21. März 2023).

[43] secunet Security Networks AG (Hrsg.), *Security Awareness Training zur Prävention*. Adresse: https://www.secunet.com/loesungen/security-awareness/awareness-training (besucht am 21. März 2023).

[44] Deutsche Gesellschaft für Cybersicherheit mbH & Co. KG (Hrsg.), *Security Awareness Trainings | DGC*. Adresse: https://dgc.org/security-awareness-trainings/ (besucht am 21. März 2023).

[45] TÜV Akademie GmbH (Hrsg.), *Security Awareness - IT-Sicherheit für Anwender*. Adresse: https://die-tuev-akademie.de/security-awareness-it-sicherheit-fuer-anwender-didi011 (besucht am 21. März 2023).

[46] TÜV Akademie GmbH (Hrsg.), *Security Awareness - IT-Sicherheit für Produktion/Fertigung*. Adresse: https://die-tuev-akademie.de/security-awareness-it-sicherheit-fuer-mitarbeiter-in-produktion-und-fertigung-didi012 (besucht am 21. März 2023).

[47] HvS-Consulting AG (Hrsg.), *Security Awareness Training*. Adresse: https://www.is-fox.com/de/know-how/security-awareness-training-im-uberblick/ (besucht am 21. März 2023).

[48] F. Barthel, „Geschulte Mitarbeiter fördern die Cybersicherheit“, *Security-Insider*, 2022-12-29. Adresse: https://www.security-insider.de/geschulte-mitarbeiter-foerdern-die-cybersicherheit-a-0bb1a9c1bb0bef4985a660cae2cd811a/?cmp=nl-36&uuid=70250c6037e2b54a3d4c2c56ac8e22a5 (besucht am 22. März 2023).

[49] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), *Awareness*. Adresse: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/awareness_node.html (besucht am 22. März 2023).

[50] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), *3 Tipps für mehr IT-Sicherheits-Awareness*. Adresse: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/3-Tipps-fuer-mehr-IT-Sicherheits-Awareness/3-tipps-fuer-mehr-it-sicherheits-awareness_node.html (besucht am 22. März 2023).

[51] O. Schonschek, *Security Awareness*, Vogel IT-Medien GmbH (Hrsg.) Adresse: https://www.security-insider.de/security-awareness-braucht-ein-upgrade-d-6213a1e2ab00d/ (besucht am 4. Apr. 2023).

Eidesstattliche Erklärung

Hiermit versichere ich – Sophie Matschke – an Eides statt, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinn nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht.

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

Mittweida, 16. April 2023	[redacted]
Ort, Datum	Sophie Matschke