Bundeskriminalamt

KRIMINALISTISCHES INSTITUT

Aktuelles aus der kriminalistisch-kriminologischen Forschung

FORSCHUNGSBERICHT

Kosten und Schäden durch Cyber-Kriminalität in Deutschland

Referat IZ 36 - Cybercrimeforschung
Christine Weber

2024
1

Inhaltsverzeichnis

Wesentliche Ergebnisse

- Aus der wissenschaftlichen Literatur zu Schäden durch (Cyber-)Kriminalität wird ein Modell abgeleitet. Dieses Modell dient der übersichtlichen Erfassung und Systematisierung von Kosten, d.h. finanziell messbaren Schäden, und weiteren, finanziell nicht messbaren oder nicht schätzbaren Schäden, die durch Cyber-Kriminalität verursacht werden.
- Das Modell unterscheidet zwischen 3 Ebenen:
    - Anhand der Schadensart: (1) Finanziell messbare Schäden (Kosten), (2) finanziell nicht messbare oder nicht schätzbare Schäden
    - Anhand der Betroffenen: (1) Privatpersonen, (2) Unternehmen, (3) Staat und Gesellschaft
    - Anhand des Zeitpunktes des Schadens: (1) durch Präventionsbemühungen, (2) als direkte Konsequenz der Straftat, (3) als Reaktion auf die Straftat
- In Anknüpfung an das Modell wurde eine Schätzung der Kosten sowie eine Einordnung der weiteren Schäden durch Cybercrime auf allen Ebenen vorgenommen.
- Im Hinblick auf die finanziellen Kosten durch Cyber-Kriminalität zeigt sich, dass die Kosten durch Präventionsbemühungen um ein Vielfaches höher ausfallen als die Kosten in direkter oder mittelbarer Folge der Straftat.
- Die Kosten, die auf Ebene von Privatpersonen und auf Unternehmensebene als Konsequenz der Straftat entstehen, können für das Jahr 2022 auf **mindestens 3,1 bis 3,7 Mrd. Euro** geschätzt werden.
- Zu den Kosten und Schäden auf staatlicher Ebene liegen bislang keine empirischen Daten vor, weshalb hierzu keine Schätzung vorgenommen werden kann.
- Im Allgemeinen besteht großer Bedarf an regelmäßigen, validen Erhebungen zu den Kosten und Schäden von Cyber-Kriminalität in Deutschland.

1 EINLEITUNG

Spätestens seitdem namhafte Schadsoftware wie „WannaCry“, „NotPetya“ oder „Emotet“ zahlreiche Unternehmen und Teile der kritischen Infrastruktur angriffen und lahmlegten, ist das immense Schadenspotential von derartigen Cyber-Phänomenen im öffentlichen und fachlichen Bewusstsein präsent (Scherschel, 2020; Windeck, 2017; Wölbert, 2020). Neben Unternehmen und staatlichen Einrichtungen sind auch Privatpersonen zunehmend von Cyber-Kriminalität (synonym „Cybercrime“) betroffen. Laut einer aktuellen Studie, die zwischen Oktober 2020 und Januar 2021 durchgeführt wurde, gaben 13,5 % der befragten Personen an, innerhalb der letzten zwölf Monate Opfer von Cyber-Kriminalität geworden zu sein (Birkel et al., 2022). Auch im Hellfeld, in der Polizeilichen Kriminalstatistik (PKS), werden seit 2010 kontinuierlich steigende Fallzahlen im Bereich der Cyber-Kriminalität verzeichnet (Bundeskriminalamt, 2022c). Für das Jahr 2021 wurde erneut ein Höchstwert erreicht, der einer 14-prozentigen Steigerung der Fallzahlen gegenüber dem Vorjahr entsprach (Bundeskriminalamt, 2022c). Einige Expertinnen und Experten vermuten außerdem, dass eine Verlagerung der Kriminalität vom analogen in den digitalen Raum stattfindet (Rüdiger, 2021). Da immer mehr Prozesse von digitaler Infrastruktur abhängig sind (Wölbert, 2020), geht die zunehmende Verbreitung von Cyber-Kriminalität folglich mit einem großen Schadenspotential für Privatpersonen, Firmen und die Gesellschaft einher.

Doch in welchem Umfang entstehen der Gesellschaft konkrete, benennbare und möglichst auch bezifferbare Schäden durch Cyber-Kriminalität? Bislang haben sich nur wenige wissenschaftliche Arbeiten dieser Thematik gewidmet. Die Studien, die zur Schätzung von Schäden bzw. Kosten der Cyberkriminalität herangezogen werden, stammen in der Regel von privaten Firmen oder Versicherungen (Accenture Security, 2019; Bitkom e.V., 2020; GDV, 2018; Hiscox, 2021; KPMG AG, 2019), die häufig ihre Kundschaft zur Erfassung nutzen. Dadurch ist die Stichprobe in diesen Studien meist sehr selektiv, weshalb die Ergebnisse in Bezug auf ihre Generalisierbarkeit kritisch zu betrachten sind. In der medialen Berichterstattung, die sich an den genannten privatwirtschaftlichen Untersuchungen orientiert, ist oftmals die Rede von immens hohen Schadenssummen – zum Teil in mehrstelliger Milliardenhöhe (Bitkom, 2020) – die die Wirtschaft durch Cyber-Kriminalität erleidet. In Deutschland hat sich die Wissenschaft bis dato jedoch nur unzureichend mit der Frage befasst, wie Schäden durch Cybercrime verlässlich und aussagekräftig geschätzt werden können. Eine Ausnahme stellt eine Studie von Dreißigacker et al. (2020) am Kriminologischen Forschungsinstitut Niedersachsen (KFN) dar, die sich allerdings ausschließlich mit der Erfassung von Cyber-Kriminalität gegen Unternehmen beschäftigt.

Um die Schäden durch Cyber-Kriminalität möglichst breit zu erfassen, sind jedoch mehr Perspektiven als nur die Unternehmensperspektive von Bedeutung. Abgesehen von unternehmensseitigen Schäden gibt es Schäden, die Privatpersonen erleiden, sowie Schäden, die Staat und Gesellschaft zu tragen haben. Für eine möglichst umfassende Betrachtung der Schäden, die durch Cyber-Kriminalität entstehen, sollen diese drei Ebenen daher im Folgenden getrennt voneinander analysiert werden. So wird ein möglichst umfassendes Modell zur Darstellung der Schäden, die durch Cybercrime entstehen, vorgeschlagen, das aus wissenschaftlicher Literatur abgeleitet wurde. Dieses Modell soll als Grundlage dienen, um eine Kalkulation der Kosten sowie eine Einordnung der Schäden durch Cybercrime auf allen drei Ebenen vorzunehmen. Basierend auf der Analyse bisheriger, empirischer Studien zum Thema wird letztlich weiterer Forschungsbedarf aufgezeigt, der in Zukunft adressiert werden sollte.

2 THEORETISCHER HINTERGRUND

2.1 Definition

Das Internet und digitale Kommunikationsmittel können bei zahlreichen Straftaten eine Rolle spielen. In diesem Bericht soll es jedoch hauptsächlich um Cybercrime im engeren Sinne (CCieS) gehen. Unter Cybercrime im engeren Sinne werden Straftaten gefasst, die sich gegen das Internet als Dateninfrastruktur, gegen andere Datennetze oder gegen Daten richten, die über das Internet bzw. andere Netze abrufbar sind (Bundeskriminalamt, 2019). Im Gegensatz dazu bezeichnet Cybercrime im weiteren Sinne (CCiwS) Straftaten, die sich *nicht* gegen das Internet oder informationstechnische Systeme richten, sondern *mithilfe* des Internets bzw. mithilfe informationstechnischer Systeme begangen werden, wie beispielsweise Cyberstalking oder Cybergrooming[1] (Bundeskriminalamt, 2019).

Wie in den Bundeslagebildern zu Cybercrime orientiert sich der vorliegende Bericht zunächst an der gesetzlichen Definition von Cyberdelikten, die auch Grundlage für die Erfassung der Delikte in der PKS darstellt. Folgende Tatbestände des Strafgesetzbuches sind hierfür relevant:

- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung gemäß §§ 269, 270 StGB
- Datenveränderung, Computersabotage gemäß §§ 303a, 303b StGB
- Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen gemäß §§ 202a, 202b, 202c StGB
- Computerbetrug gemäß § 263a StGB

Allerdings werden viele Straftaten, die auch die genannten juristischen Voraussetzungen erfüllen, in der PKS nicht unter Cybercrime geführt, da sie gleichzeitig einen schwereren Straftatbestand erfüllen. Beispielhaft hierfür werden Erpressungshandlungen im Zusammenhang mit DDoS[2]-Attacken oder Ransomware genannt (Bundeskriminalamt, 2019). Diese werden in der PKS in der Regel nicht als Cybercrime-Delikt, sondern als die schwerwiegendere Tat erfasst, in diesem Fall als Erpressung mit Tatmittel Internet (Bundeskriminalamt, 2019). Ransomware-Attacken zählen jedoch in der Regel zu CCieS, da die Erpressungshandlung auf einer Manipulation von Daten im Sinne des § 303 StGB basiert (Bundeskriminalamt, 2019). Im vorliegenden Bericht werden im Gegensatz zur PKS auch solche Straftaten in die Betrachtung eingeschlossen. Darüber hinaus werden zum Teil auch Delikte aus dem Bereich Online-Warenbetrug berücksichtigt, die im streng definitorischen Sinne zu CCiwS gehören. Insbesondere bei Bevölkerungsbefragungen zu Cyber-Kriminalität werden diese Delikte häufig unter Cyber-Delikten gefasst.

Eine weitere definitorische Unterscheidung bezieht sich auf die Terminologie von Kosten und Schäden. Während viele Autorinnen und Autoren diese Begriffe zum Teil fast austauschbar nutzen, werden sie durch andere Autorinnen und Autoren explizit unterschieden (Paoli et al., 2018a). In der vorliegenden Arbeit werden die Kosten in Anlehnung an Paoli et al. (2018a) definiert als der rein monetäre, in Geldwert messbare Verlust, der durch die Cyber-Kriminalität entsteht. „Schäden“ wird hingegen als Überbegriff verwendet und umfasst zusätzlich zu den monetären Verlusten noch weitere, nicht unmittelbar als Geldwert messbare Konsequenzen, wie z. B. psychologische Auswirkungen der

[1] Cybergrooming bezeichnet die Einwirkung auf ein Kind mithilfe digitaler Kommunikationstechnologien zum Zwecke der Anbahnung eines sexuellen Missbrauchs (siehe § 176b StGB).
[2] Distributed Denial of Service

Opferwerdung, Schäden für die Sicherheitswahrnehmung in der Bevölkerung und das Vertrauen in staatliche Einrichtungen oder Reputationsverluste[3].

Im vorliegenden Bericht werden verschiedene, wissenschaftliche Studien herangezogen, die sich mit der Darstellung der Kosten und Schäden durch Cybercrime bzw. mit Kriminalität im Allgemeinen befasst haben. Die Studien stammen aus Großbritannien, Belgien und den USA.

2.2 Bisherige Studien zu Modellen für Schäden durch (Cyber-)Kriminalität

Basierend auf den im Folgenden dargestellten, bereits existierenden Modellen und den jeweiligen Abwägungen ihrer Vor- und Nachteile wurde ein eigenes Modell für die Systematisierung der Schäden durch Cyber-Kriminalität entwickelt. Dieses soll dazu dienen, die Schäden durch Cybercrime möglichst übersichtlich, vollständig und transparent darzustellen, und damit eine Grundlage bieten, um die finanziell messbaren Schäden bzw. Kosten, die eine Unterkategorie der allgemeinen Schäden sind, zu errechnen bzw. zu schätzen und eine Einordnung weiterer, finanziell nicht messbarer Schäden vorzunehmen.

2.2.1 Anderson et al. (2013): The Changing Cost of Cybercrime (GB)

Ein erster Versuch, die Schäden durch Cybercrime systematisch zu erfassen, wurde von Anderson und Kollegen im Jahr 2013 vorgelegt. Die Autoren unterscheiden im Rahmen ihrer Studie und ihres Modells Schadenstypen und versuchen dabei, jedem Schadenstypus (bspw. auch psychischen Schäden) einen monetären Wert zuzuschreiben. Im Resultat führt dieser Ansatz zu einer rein monetären Schadensschätzung. Die Autoren unterteilen die Schäden in drei große Kategorien, deren Summe die gesellschaftlichen Gesamtschäden, ausgedrückt in monetären Schäden, also in Kosten, wiederspiegelt (siehe Abbildung 1):

1. Direkte Kosten (direct losses)
2. Indirekte Kosten (indirect losses)
3. Präventionskosten (defensive costs)

Direkte (opferseitige) Kosten (Direct losses) sind monetäre Werte von Verlusten, Schäden oder anderen Leiden, die das *individuelle* Opfer als Folge einer Cyber-Straftat erleidet. Die Autoren verdeutlichen das anhand des Beispiels des Online-Banking-Betrugs. Die direkten Kosten beinhalten dabei einerseits direkt messbare Verluste, wie z. B. das Geld, das von den Konten der Opfer abgehoben wurde. Andererseits summieren die Autoren zu den direkten Kosten auch weitere Schäden, wie beispielsweise den Verlust von Zeit für das Zurücksetzen der Kontodaten (bspw. bei Banken), psychische Konsequenzen des Opfers (wie z. B. erlittener Stress), sekundäre Kosten (z. B. durch überzogene Konten, aufgeschobene Einkäufe, fehlenden Zugriff auf Geld etc.) sowie individuelle Zeit- und Aufmerksamkeitsverluste aufgrund von Spam-Nachrichten.

Indirekte (nicht opferseitige) Kosten (Indirect losses) wiederum sind monetäre Verluste und Opportunitätskosten, die die Gesellschaft betreffen – nicht das Individuum. Exemplarisch hierfür ist ein Verlust von Technikvertrauen, der für Unternehmen zu finanziellen Einbußen führen kann[4]. Auch

[3] Reputationsverluste können bei Unternehmen zum Teil auch immens hohe Auswirkungen, z. B. auf den Aktienkurs, haben. Diese Verluste sind jedoch kaum operationalisierbar (siehe Dreißigacker et al., 2020; Paoli et al., 2018b), da nicht bestimmt werden kann, über welchen Zeitraum hinweg derartige Verluste auftreten und wie sie durch weitere Faktoren beeinflusst werden. Verluste im Aktienwert können daher kaum auf Reputationsverluste, basierend auf einem spezifischen Cyber-Vorfall, zurückgeführt werden. Daher sind auch diese Verluste nicht unmittelbar als Geldwert messbar.

[4] Ein Vertrauensverlust in Funktionen des Online-Bankings führt beispielsweise dazu, dass Kunden Online-Banking weniger nutzen. Das wiederum bedingt geringere Einnahmen aus elektronischen Transaktionsgebühren und höheren Kosten für die Aufrechterhaltung von Filialpersonal und Überweisungsbearbeitung.

der Personal- und Zeitaufwand, der für die Bereinigung betroffener Hardware (z. B. durch Malware) zu leisten ist, fällt unter die indirekten Verluste.

Präventionskosten *(Defensive Costs)* umfassen alle Kosten, die mit Präventionsbemühungen verknüpft sind. Anderson et al. (2013) unterscheiden dabei *direkte* Präventionskosten (z. B. Ausgaben für Entwicklung, Einsatz und Instandhaltung von Sicherheitsprodukten, Sicherheitsschulungen), sowie *indirekte* Präventionskosten (z. B. Unannehmlichkeiten, die durch die Präventionsmaßnahmen verursacht werden[5]). Die Präventionskosten werden – genau wie die indirekten Verluste – nicht auf individueller Ebene, sondern auf gesellschaftlicher Ebene betrachtet.

Basierend auf diesem Modell gehen die Autoren auf verschiedene Cyber-Delikte ein (wie z. B. Online-Zahlungskarten-Betrug oder Online-Banking-Betrug) und beschreiben auf der Basis unterschiedlich zusammengetragener Daten und Schätzungen, wie hoch die jährlichen Kosten für Großbritannien im jeweiligen Deliktbereich in etwa ausfallen. Die Autoren selbst betonen, dass diese Schätzungen mit Vorsicht zu interpretieren sind. Sie generieren zudem bewusst keine Summe der gesamtgesellschaftlichen Schäden, um zu vermeiden, dass eine derartige Gesamtzahl aus dem Kontext genommen und allzu wörtlich als Schadenssumme in den öffentlichen Diskurs einfließen würde.

Bewertung

Stärken
Das Modell von Anderson et al. (2013) stellt den ersten wissenschaftlichen Versuch dar, die Kosten, die durch Cyberkriminalität entstehen, systematisch aufzuarbeiten und messbar zu machen und stellte daher eine wertvolle Grundlage für die Forschung dar. Die Autoren waren hiermit Vorreiter, da sie zum ersten Mal einen Ansatz präsentierten, mit dem eine wissenschaftliche Einschätzung der durch Cyber-Kriminalität entstandenen Schäden ermöglicht werden kann.

Schwächen
Die Terminologie der Kostenkategorien ist sehr breit gefasst. So werden alle Kosten, die unmittelbar dem Opfer entstehen, als *direkte* Kosten bezeichnet, während alle weiteren Kosten, die nicht dem Opfer, sondern weiteren Betroffenen entstehen, als *indirekte* Kosten bezeichnet werden. In Anbetracht der Komplexität der Schäden durch Cyber-Kriminalität könnte daher in Frage gestellt werden, inwieweit diese sehr allgemeine Unterscheidung eine wirklich praktikable Vereinfachung der Thematik darstellt.
Auch der Ansatz, der versucht, jeder Schadensart einen monetären Wert beizumessen, kann prinzipiell kritisch betrachtet werden. Im Gegensatz zu der Studie von Anderson et al. (2013), geht der vorliegende Bericht, wie auch andere Autorinnen und Autoren (Greenfield & Paoli, 2015; Paoli et al., 2018a; Wickramaseker et al., 2015) davon aus, dass Schätzungen zu konkreten Kosten nicht für jede Schadensart möglich sind, da es schlichtweg Schadensarten gibt, deren Konsequenzen ohne spekulative Vorannahmen nicht monetär erfassbar sind (wie beispielsweise psychische Schäden).
Auch die Zahlen, die in der Studie generiert werden, basieren auf unterschiedlichen Schätzungen und Berichten. Die Methode der Erfassung ist nicht hinreichend systematisch, daher nicht objektivierbar und nicht ohne Weiteres auf andere Kontexte oder Länder übertragbar und wird deswegen auch hier nicht weiterausgeführt.

[5] Hierfür wird beispielhaft das Verpassen relevanter E-Mails genannt, die fälschlicherweise im Spam-Ordner landen.

Es wird außerdem nicht deutlich, auf welcher Basis die Autoren die jeweiligen Delikte ausgewählt haben, die sie in dem Artikel näher analysieren. Einige beschriebene Deliktarten (wie z. B. „Fake Escrow Scams“[6]) dürften in ihrer spezifischen Form heute kaum noch von Bedeutung sein.

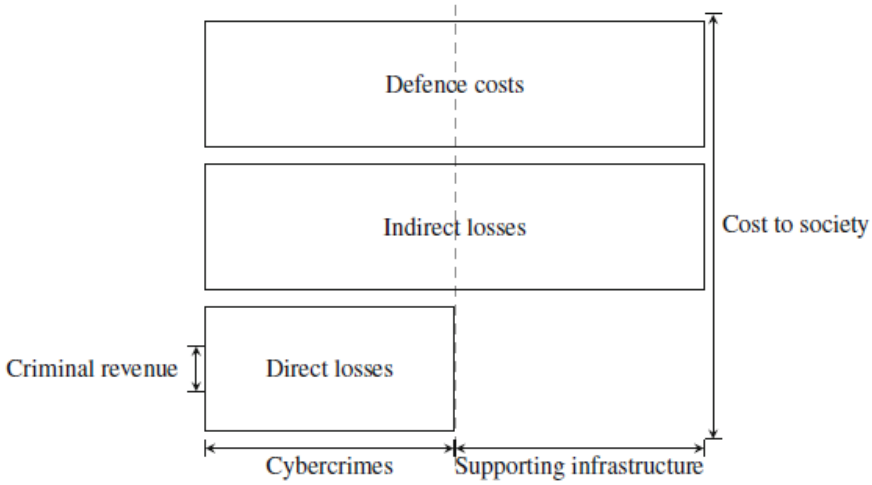


Abbildung 1. Die Darstellung der Schäden durch Cybercrime in der Studie von Anderson et al. (2013).

2.2.2 United States Government Accountability Office (2017): The cost of crime

Im Jahr 2017 legte das US Government Accountability Office (GAO), der Rechnungshof der Vereinigten Staaten, einen Bericht zu den Gesamtschäden der Kriminalität des Landes vor. Das Modell sollte zur Erfassung verschiedener Kriminalitätsarten, nicht nur von Cyber-Kriminalität, dienen. Für den Bericht wurden 17 Expertinnen und Experten aus den Bereichen Wirtschaft, Kriminologie, Demografie, Soziologie, öffentliche Gesundheit und Computerwissenschaften befragt, die über Expertise in der Erfassung von Schäden durch Kriminalität verfügen. Darüber hinaus führten die Autorinnen und Autoren eine Literaturrecherche durch und analysierten 27 Fachartikel, die seit dem Jahr 1996 zu der Thematik publiziert wurden.

Aufbauend auf den Erkenntnissen aus den Expertinnen- und Experteninterviews sowie der Literaturanalyse präsentieren die Autorinnen und Autoren in dem Bericht ein Modell, das die Schäden durch Kriminalität in zwei Hauptkategorien einteilt: Die *materiellen* Schäden (tangible costs) und die *nicht-materiellen* Schäden (intangible costs). Diese Kategorien werden jeweils unterteilt nach dem *Zeitpunkt*, zu dem sie auftreten: 1. Schäden durch Antizipation der Straftat, 2. Schäden als direkte Konsequenz der Straftat, 3. Schäden als Reaktion auf die Straftat (siehe Abbildung 2). Darüber hinaus wird hinsichtlich der *Träger* des Schadens differenziert. Hierbei kommen das Opfer, potentielle Opfer, die Opfer-Familie, die Gesellschaft, die Tatbegehenden, die Familien der Tatbegehenden, Unternehmen sowie „unschuldige Individuen“[7] in Frage.

Als materielle Kosten (tangible costs) in *Antizipation einer Straftat* werden beispielsweise Ausgaben zur Verringerung der Viktimisierungswahrscheinlichkeit aufgeführt (Träger: potentielle Opfer) oder auch Kosten durch Kriminalpräventionsprogramme von Regierungs- oder Nicht-Regierungsorganisationen, z. B. für Sensibilisierungsprogramme (Träger: Gesellschaft; siehe Abbildung 2). Materielle Kosten als *direkte Kosequenz der Straftat* sind beispielsweise Kosten durch verlorene Produktivität aufgrund von Fehltagen des Opfers (Träger: Gesellschaft und Unternehmen) oder auch Kosten für die medizinische und/oder psychische Gesundheitsversorgung des Opfers

[6] Das Opfer glaubt, eine Online-Auktion für ein Auto oder Motorrad gewonnen zu haben. Für die Abwicklung der Übergabe wird ein vom Verkäufer vorgeschlagener Treuhändler eingeschaltet – Hierbei handelt es sich um einen Betrug.
[7] Gemeint sind hier zu Unrecht Beschuldigte.

(Träger: Opfer, Familie des Opfers, Gesellschaft). Materielle Kosten als *Reaktion auf die Straftat* können beispielsweise Kosten zur Verteidigung des Angeklagten beinhalten (Träger: Tatausübende, Gesellschaft) sowie der Verlust von Steuereinnahmen durch fehlende Erwerbstätigkeit des Tatausübenden aufgrund deren Inhaftierung (Träger: Gesellschaft).
Immaterielle Schäden (intangible costs) können in *Antizipation der Straftat* beispielsweise durch Vermeidungsverhalten (von Personen, Orten etc.) oder Angst entstehen (Träger jeweils potentielle Opfer). Als *direkte Konsequenz der Straftat* können weiterhin immaterielle Schäden wie Schmerz, Leid, oder der Verlust von Lebensqualität auftreten (Träger: Opfer). In der Kategorie „Schäden *als Reaktion auf die Straftat*" werden beispielhaft Schäden durch „übermäßige Abschreckung" (overdeterrence) genannt, z. B. wenn als Konsequenz unschuldige Personen einer Straftat beschuldigt oder legitime Tätigkeiten der Gesellschaft beeinträchtigt werden (Träger: unschuldige Individuen, Gesellschaft).

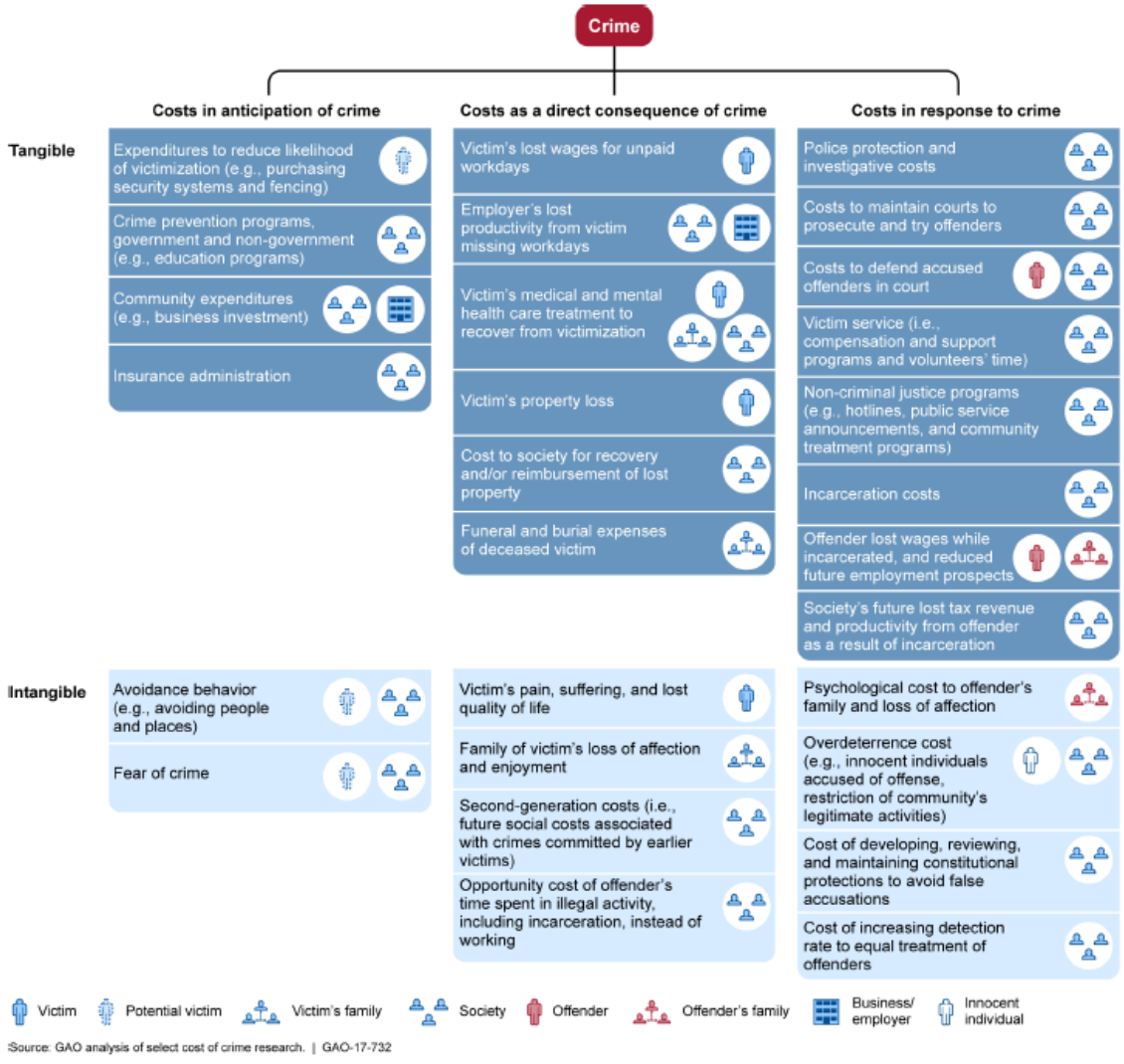


Abbildung 2. Modell zur Erfassung der Gesamtschäden der Kriminalität (United States Government Accountability Office, 2017).

Bewertung

Stärken

Das von dem US GAO (2017) erarbeitete Modell bietet eine gut recherchierte, umfassende Grundlage für die Erfassung der Schäden durch Kriminalität. Die Ebenen, die dabei betrachtet werden (Materiell vs. Nicht-materiell, Zeitpunkte des Auftretens sowie Träger des Schadens) liefern eine hilfreiche Kategorisierung, die z.T. auch in anderen Studien ähnlich angewandt wurde (Greenfield & Paoli, 2013;

Wickramasekera et al., 2015). Auch wenn Einzelaspekte des Modells womöglich nicht unmittelbar auf Deutschland oder den Phänomenbereich Cybercrime übertragbar sind, so bietet das Modell im Allgemeinen dennoch eine gute Grundlage für einen möglichen internationalen Vergleich von Schadenslagen sowie für eine Einordnung der Schäden, die auch durch Kriminalitätsformen wie Cybercrime entstehen können.

Schwächen
Einige konkret benannte Schäden, wie z. B. die medizinische Versorgung des Opfers oder für die Beerdigung anfallende Kosten, sind im Phänomenbereich Cybercrime womöglich eher zu vernachlässigen. Einige Aspekte sind außerdem möglicherweise schwer auf Deutschland übertragbar, wie z. B. die Verluste des Opfers aufgrund unbezahlter Arbeitstage[8], da in Deutschland andere Arbeitsschutzmaßnahmen gelten als in den USA. Eine weitere zentrale Limitation der Studie ist, dass keine Aussage zur Generierung der im Rahmen des Modells relevanten Daten getroffen wird. Das Modell bietet somit einen guten Überblick über verschiedene Schadensarten, geht aber nicht darauf ein, wie diese erfassbar gemacht werden können und ob sich auf Basis des Modells eine Schätzung der Kosten vornehmen lässt.

2.2.3 Agrafiotis et al. (2016): Cyber Harm Model

Im Rahmen einer Studie von Agrafiotis et al. (2016) wurde eine Taxonomie der Schadensarten durch Cyber-Vorfälle erstellt, um ein „universelles" Cyber-Schadensmodell daraus abzuleiten. Laut der Autorinnen und Autoren soll die Studie eine „Grundlage zur Erarbeitung umfassender Messinstrumente für die Bewertung von Cyberschäden und die Entwicklung eines Modells sein, das zukünftig als Instrument für politische Entscheidungen dienen soll"[9]. Für die Entwicklung des Modells wurden Interviews geführt sowie Fokusgruppen gebildet mit Cybersicherheits-Expertinnen und -Experten aus Regierungen, dem Privatsektor, der Wissenschaft und anderen Bereichen.

Für das Modell wurde zunächst die Perspektive der Betroffenen analysiert. Hier wurden vier zentrale Ebenen herausgearbeitet:

1. Individuum
2. Organisation
3. Infrastruktur/Eigentum
4. Staat

Als Schadensarten, die auf unterschiedlichen Ebenen auftreten können, wurden sechs zentrale Kategorien ausgearbeitet:

1. **physikalisch/digital** (z. B. Körperverletzungen oder Sachschäden an Geräten, Datenbeständen/Systemen oder Gebäuden)
2. **psychologisch** (auf individueller Ebene, z. B. durch Gefühle von Scham, Frustration, Sorge, Schuld etc.)

[8] Ausgenommen bei Selbstständigen oder Freiberuflern, für die unbezahlte Arbeitstage durchaus eine Rolle spielen.
[9] Wörtlich: […], this article lays the *groundwork* for establishing comprehensive measurements for cyber harm assessment and creating a model that will serve as a policy-making tool through future work and conversion of the research results into an operational framework (Agrafiotis et al., 2016; S. 5).

3. **ökonomisch** (entspricht finanziellen Verlusten von Individuen, Unternehmen oder Staaten.; auf individueller Ebene z. B durch entstandene Kosten, auf Unternehmensebene z. B. durch reduziertes Wachstum, fallende Aktienkurse, Ermittlungskosten, Kompensationszahlungen, Erpressungsgelder; auf staatlicher Ebene z. B durch Steuereinbußen aufgrund von „Schattenwirtschaft“ im DarkNet etc..)

4. **rufschädigend** kann Individuen, Unternehmen oder Staaten betreffen z. B. auf individueller Ebene durch die Verbreitung von falschen, persönlichen oder kompromittierenden Informationen; auf Unternehmensebene z. B. durch Schädigung von Zulieferer- oder Kunden-Beziehungen, Einbußen in der Personalrekrutierung, Verlust von Fachpersonal.; auf staatlicher Ebene z. B. durch eine Verschlechterung internationaler Beziehungen etc.)

5. **kulturell** (entspricht einer erheblichen Störung der sozialen Stabilität und Sicherheit einer Gesellschaft, z. B. durch beschädigte Kommunikationsnetze, die Verbreitung von Falschinformation oder Hassreden etc.)

6. **politisch/gesellschaftlich** (z. B. durch einen Verlust an öffentlichem Einfluss, Unterbrechung politischer Prozesse, Verschlechterung der internationalen Beziehungen etc.)

Abbildung 3 gibt einen Überblick über die Arten von Schäden, die auf den unterschiedlichen Ebenen der Betroffenen auftreten können.

Subject	Physical	Psychological	Economic	Reputational	Cultural	Political
Individual	✓	✓	✓	✓	✓	✓
Organisational			✓	✓	✓	✓
Property/ infrastructure	✓					
National		✓	✓	✓	✓	✓

Figure 4.4: Relationship between subjects und nature of harm

Abbildung 3. Zusammenhänge zwischen den Betroffenen und der Schadensart (Agrafiotis et al., 2016).

Letztlich gibt die Studie auch einen Ausblick auf verschiedene qualitative und quantitative Metriken, die für die Bewertung von Cyberschäden und -kosten herangezogen werden könnten. Beispielhaft für quantitative Metriken werden hierbei Statistiken zu direkten finanziellen Verlusten, Kriminalitäts- und medizinische Statistiken, Sentiment-Analysen[10] oder die Analyse von Unternehmenswerten genannt. Als qualitative Metriken werden Dunkelfeldstudien sowie Konsumentenbefragungen genannt.

Bewertung

Stärken

Das Modell liefert eine Taxonomie zur Einordnung von Cyberschäden auf Betroffenenebene anhand einer differenzierten Kategorisierung der Schadensart. Dabei werden exemplarisch auch qualitative und quantitative Metriken zur Erfassung des Schadens vorgeschlagen.

Schwächen

Die Studie greift in nur geringem Umfang auf bereits vorhandene Literatur zurück. Das Modell wurde (fast) ausschließlich auf Basis der Ergebnisse qualitativer Interviews und Fokusgruppen entwickelt. Die konkrete Umsetzung dieser Interviews/Fokusgruppen wird jedoch nicht näher erläutert, d. h. es

[10] Z. B. durch die automatisierte Analyse positiver oder negativer Äußerungen in diversen Medien oder in sozialen Netzwerken bezüglich eines bestimmten Unternehmens, das von einem Cyber-Angriff betroffen war. Das könnte beispielsweise dazu dienen, Schäden der Rufschädigung zu quantifizieren.

bleibt unklar, wie viele Expertinnen und Experten aus welchen Bereichen oder welchen Ländern und nach welchen Kriterien diese befragt wurden.
Auch das Modell selbst weist einige Schwächen auf. So ist nicht klar, weshalb Infrastruktur/Eigentum als separate Betroffenheits-Ebene aufgeführt wird, wo doch erstens Infrastruktur bzw. Eigentum *immer* in die Ebenen der Individuen, Organisation oder des Staates eingebettet sind und zweitens – wie in Abbildung 3 dargestellt – *nur* physikalische Schäden in Bezug auf Infrastruktur/Eigentum auftreten, was konzeptionell redundant wirkt. Zudem widerspricht diese Einteilung gängiger Literatur zu Schadensmodellen (United States Government Accountability Office, 2017; Paoli et al., 2018a; Wickramasekera et al., 2015).
Auch die Taxonomie der Schadensarten wirkt in sich nicht schlüssig. So wird nicht deutlich, inwieweit sich politische/gesellschaftliche Schäden von kulturellen Schäden abgrenzen bzw. unterscheiden lassen.[11] Die dargestellten Zusammenhänge zwischen Betroffenen und Schadensarten bleiben ebenfalls fraglich. So erscheint es beispielsweise nicht schlüssig, dass politische/gesellschaftliche und kulturelle Schäden auch auf individueller Ebene angesiedelt sind.
Die Studie gibt zwar einen Überblick über mögliche qualitative und quantitative Metriken, nutzt diese Metriken allerdings nicht, um (beispielhaft) darzustellen, wie diese im Rahmen des Modells Anwendung finden können. Außerdem wird nicht klar, weshalb Dunkelfeldstudien und Konsumentenbefragungen – klassische quantitative Messmethoden – als qualitative Metriken aufgeführt werden.
Darüber hinaus wird nicht deutlich, welche Arten von Cyberangriffen bzw. welche Definition von Cybercrime dem Artikel zugrunde gelegt wurde. Anhand der Beispiele lässt sich ableiten, dass das Modell sowohl für Cybercrime im engeren Sinne als auch im weiteren Sinne[12] gelten soll, dies wird im Rahmen der Studie aber nicht näher ausgeführt oder erläutert.

2.2.4 Paoli et al. (2018a): Belgian Cost of Cybercrime: Measuring Cost and Impact of Cybercrime in Belgium

In Belgien wurden 2018 die Ergebnisse eines vier Jahre andauernden Forschungsprojektes der Universitäten Leuven und Gent zur Erfassung der Schäden und Kosten durch Cybercrime veröffentlicht. Ziele des Projekts waren (1) die Auswirkungen von Cyberkriminalität auf Privatpersonen, Unternehmen und die Regierung zu erfassen, (2) die Präventions- und Reaktionskosten von Einzelpersonen, Unternehmen und der Regierung einzuschätzen, sowie (3) politische Empfehlungen für belgische und europäische Entscheidungsträger zu entwickeln. In das interdisziplinäre Forschungsprojekt waren verschiedene Lehrstühle aus den Bereichen Computer Science, Kriminologie, Kommunikationswissenschaft und IT-Recht eingebunden.

Im Rahmen des Projekts wurde eine Literaturanalyse zur Generierung von Cyber-Schadensmodellen für Privatpersonen, Unternehmen und die Regierung durchgeführt, welche anschließend als Framework für die empirischen Untersuchungen dienten. Cyber-Kriminalität wurde dabei relativ breit definiert als „alle computervermittelten Aktivitäten, die über elektronische Kommunikationsnetzwerke und Informationssysteme in einer elektronischen Umgebung begangen werden, die entweder illegal sind oder von bestimmten Parteien als illegal angesehen werden und die über alle globalen elektronischen Netzwerke und Medien durchgeführt werden können“ (Paoli et al., 2018a; S. 30). In der

[11] Den Autoren und Autorinnen selbst muss die fehlende Trennschärfe dieser beiden Kategorien auch aufgefallen sein, denn in einer späteren Studie, die sich insbesondere auf Unternehmen bezieht, nennen sie nur noch fünf Schadensarten, abzüglich der kulturellen Schäden (siehe Agrafiotis et al., 2018)
[12] z. B. ist auch die Rede von Hassrede, Verbreitung persönlicher Informationen etc.

Erfassung von Cyber-Kriminalität gegenüber Privatpersonen wurden außerdem vier verschiedene Angriffsarten unterschieden: Malware, Scam[13], Hacking und Monitoring[14].
Bei der Erfassung von Cyber-Kriminalität gegenüber Unternehmen wurden die Delikte Illegaler Zugriff auf IT-Systeme, Cyber-Spionage, Störung von Daten oder Systemen, Cyber-Erpressung und Internet-Betrug erfasst. Die Auswahl dieser Angriffsarten erfolgte in Anlehnung an das belgische Strafrecht sowie an das Übereinkommen des Europarats über Computerkriminalität.

Die Kosten, die Unternehmen und öffentliche Einrichtungen für Präventionszwecke ausgeben, wurden nicht in die Kosten der Kriminalität miteingerechnet. Die Autorinnen und Autoren nennen hierfür insbesondere methodische Gründe, da es nicht möglich ist, die präventiven Ausgaben für *einzelne* kriminelle Aktivitäten einzuschätzen und die Präventionsausgaben darüber hinaus nicht nur von der Bedrohungslage abhängen, sondern auch von der spezifischen Wahrnehmung der einzelnen Parteien. Auch Ermittlungskosten wurden ausgeschlossen, da es laut der Autorinnen und Autoren aufgrund der Studie sonst zu Verzerrungen der ohnehin bereits priorisierten Aktivitäten der Strafverfolgungsbehörden kommen könnte. Denn je nach Priorisierung durch Behörden weisen einige Ermittlungsbereiche höhere Ermittlungsraten auf, die wiederum mit höheren Ermittlungskosten verbunden sind. Würde man diese Ermittlungskosten in die Schadensschätzungen einbeziehen, könnte das dazu führen, dass die ohnehin bereits priorisierten Ermittlungsbereiche noch weiter priorisiert werden.

Die Schäden durch Cybercrime wurden anhand folgender empirischer Untersuchungen erfasst:

1. **Privatpersonen**: Durchführung von zwei Online-Befragungen[15] (2015, 2017)
2. **Unternehmen**: Durchführung von zwei Befragungen zur Untersuchung des Sicherheitsstands der belgischen Unternehmen[16]
3. **Regierung**: Zunächst Versuch der Erfassung verschiedener Regierungen in Belgien[17] anhand eines Online-Fragebogens. Allerdings war der Rücklauf unzureichend für die Analyse. Stattdessen wurden die Antworten der Regierung auf parlamentarische Anfragen analysiert sowie Interviews mit Regierungsvertreterinnen und -vertretern sowie Repräsentantinnen und Repräsentanten zweier belgischer Großstädte geführt.

Mithilfe der Ergebnisse der empirischen Untersuchungen leiten die Autorinnen und Autoren allgemeine sowie spezifische Handlungsempfehlungen für Privatpersonen, Unternehmen und Regierungsbehörden ab.

Bewertung

[13] Wurde im Rahmen der Studie als „Scam" definiert, konkret aber als Betrugsversuch mit dem Ziel an persönliche Informationen oder Geld zu gelangen, z. B. durch E-Mails (Phishing) oder falsche Webseiten (Pharming)
[14] Monitoring wurde dabei definiert als das Sammeln/Ausspähen von persönlichen Daten durch die Regierung oder ein privates Unternehmen.
[15] Es wurden Daten von 1033 Personen (2015) sowie 1181 Personen (2017) im Rahmen der Online-Befragungen erhoben und analysiert. Die Stichproben wurde aus dem Panel eines Forschungsunternehmens rekrutiert. Es wurden Quotenstichproben verwendet, sodass die Stichproben in Bezug auf Alter, Geschlecht und Wohnort für die internetnutzende, belgische Bevölkerung repräsentativ waren.
[16] Die Unternehmen wurden per E-Mail um Teilnahme an der Befragung gebeten. Kontaktiert wurden alle 9.249 Unternehmensvertreter, die im Verband der Unternehmen in Belgien (Federation of Enterprises in Belgium - FEB) gelistet waren. Die Rücklaufquote dieses Rekrutierungsprozesses war allerdings äußerst gering: 310 (erste Welle) und 277 (zweite Welle) Daten konnten für die Analysen genutzt werden, was Rücklaufquoten von 3,4% sowie 2,6% entspricht.
[17] Föderale Regierung, Flämische Regierung, Wallonische Regierung, Regierung der französischsprachigen Gemeinschaft, Brüsseler Regierung, IT-Organisation der flämischen Provinzen und Städte, IT-Organisation der wallonischen Provinzen und Städte.

Stärken
Die Belgische Studie stellt ein komplexes Forschungsprojekt zur Erfassung der Schäden durch Cybercrime in Belgien dar. Im Gegensatz zu den vorher dargestellten Studien wird hier das präsentierte theoretische Modell unmittelbar mit der Operationalisierung und empirischen Erfassung der Schäden verknüpft. Die Studie bietet damit ein konkretes Beispiel dafür, wie eine Erfassung der Kosten und Schäden auf unterschiedlichen Ebenen (Privatpersonen, Unternehmen, Staat bzw. Regierung) möglich sein kann.

Schwächen
Bei der Studie handelt es sich im Wesentlichen um eine ausführliche Darstellung der Art, empirische Daten zusammenzutragen und zu analysieren und weniger um eine Systematisierung spezifischer Schadensarten im Bereich Cyber-Kriminalität. Daher ist der Begriff „Modell", auch wenn die Autorinnen und Autoren ihn selbst nutzen (siehe Paoli et al., 2018, S. 16)[18], irreführend.
Diskutabel sind zudem einige Aspekte der theoretischen Herleitung. Einerseits erscheint die zugrundeliegende Definition von Cybercrime sehr breit gehalten. Trotz dieser übergeordneten Definition werden für Privatpersonen nur vier Angriffsarten beleuchtet, was in Anbetracht des Spektrums der Cyberkriminalität wenig erscheint. Darüber hinaus weist die belgische Rechtsprechung einige Unterschiede zum deutschen StGB auf, weshalb eine Übertragbarkeit der Angriffsarten und ihrer Erfassung auf Deutschland ggf. nur eingeschränkt möglich ist.
Eine weitere Limitation stellt die Auswahl unterschiedlicher Angriffsarten für Privatpersonen und Unternehmen dar. Aus strafrechtlicher Sicht ist diese Vorgehensweise – zumindest für Cybercrime im engeren Sinne – wenig nachvollziehbar. Zwar gibt es Delikte, bei denen in erster Linie Unternehmen betroffen sind (wie DDoS-Attacken, Defacing, Ransomware), aber viele Angriffsarten können sowohl Unternehmen als auch Privatpersonen betreffen (z. B. Malware, Phishing, Hacking). Darüber hinaus wäre zu diskutieren, ob Präventionsausgaben und Ermittlungskosten tatsächlich aus einer solchen Analyse zu den Kosten von Cybercrime ausgeschlossen werden sollten. Trotz legitimer methodischer und inhaltlicher Bedenken wäre es bei einer Gesamtbetrachtung der Schäden doch wünschenswert, diese nicht gänzlich auszuschließen und zumindest eine vergleichende Einordnung anzustreben. Im Allgemeinen lässt auch die geringe Rücklaufquote der kontaktierten Unternehmen hinterfragen, inwieweit die empirischen Ergebnisse der Studie tatsächlich verallgemeinerbar sind.

2.3 Zusammenfassung: Modell der Schäden durch Cyber-Kriminalität

In Anlehnung an die dargestellten Modelle, die zur Schätzung der Kosten und Schäden durch (Cyber-)Kriminalität bereits Anwendung gefunden haben, wird im Folgenden ein Modell skizziert, das als Grundlage für eine möglichst vollumfängliche Darstellung der Schäden durch Cybercrime in Deutschland dienen soll. Im Rahmen dieses Modells werden die Schäden zunächst in zwei zentrale Kategorien eingeteilt: Die *finanziell messbaren* Schäden (Kosten) und die *finanziell nicht messbaren oder nicht schätzbaren* Schäden. Diese Einteilung erfolgt in Anlehnung an das GAO-Modell (United States Government Accountability Office, 2017) sowie an andere wissenschaftliche Studien (Paoli et al., 2018a; Greenfield und Paoli, 2013). Das Modell unterscheidet außerdem hinsichtlich der Ebenen, auf denen die Schäden entstehen (Privatpersonen, Unternehmen, Staat) (siehe United States Government Accountability Office; 2017; Paoli et al., 2018a) sowie hinsichtlich des *Zeitpunktes:* Durch Antizipation der Straftat (sog. Präventionskosten bzw. -bemühungen), als direkte Konsequenz der Straftat oder als Reaktion auf die Straftat (United States Government Accountability Office, 2017). Hierbei ist zu beachten, dass diese Zeitpunkte nicht zeitlich distinkt voneinander oder getrennt zu verstehen

[18] „We conducted a literature review in order to develop cybercrime models for citizens based in Belgium on the one hand and Belgian businesses and the Belgian government on the other hand. These models were used as framework for the different empirical studies undertaken within this project." (Paoli et al., 2018; S. 16)

sind, sondern sich überlappen. Die Schäden als direkte Konsequenz auf die Straftat und als Reaktion auf die Straftat können beispielsweise unter Umständen bereits parallel auftreten.

2.3.1 Eigenes Modell zur Schätzung der Kosten (finanziell messbare Schäden)

	Präventionskosten	**Kosten als direkte Konsequenz der Straftat**	**Kosten als Reaktion auf die Straftat**
Privatpersonen	Ausgaben für Sicherheitssysteme, Antiviren-Software auf privaten Geräten	Verlust/Zerstörung von Eigentum	Anwaltskosten, evtl. Gerichtskosten
Unternehmen	Cybersicherheitspersonal Technische Schutzmaßnahmen (Cybersicherheit) Cyberversicherungen Mitarbeitenden-Schulungen	Direkte Kosten durch Verlust/Zerstörung von Daten/ Infrastruktur/Hardware Produktivitätsverlust durch Störungen im Betriebsablauf	Kosten für Untersuchungen und Ersatzmaßnahmen Kosten für Rechtsstreitigkeiten Zahlungen in Folge von Erpressung durch gestohlene/verschlüsselte Daten
Staat und Gesellschaft	Kosten für Kriminalpräventionsprogramme Staatliche Investitionen in Cybersicherheit (Staatliche Einrichtungen, Forschungsförderprogramme)	Zerstörung staatlicher Infrastrukturen durch Cyberangriffe	Polizei-/Ermittlungskosten Gerichtliche Kosten, Inhaftierungskosten

2.3.2 Eigenes Modell der finanziell nicht messbaren oder nicht schätzbaren Schäden

(Annäherung z. B. durch Studien und/oder ExpertInnen-Interviews möglich)

	Durch Präventionsbemühungen	**Schäden als direkte Konsequenz der Straftat**	**Schäden als Reaktion auf die Straftat**
Privatpersonen	Vermeidungsverhalten (z. B. von Online-Diensten)	Psychische Auswirkungen auf das Opfer, Verlust von Lebensqualität	Zeitaufwand/Stress durch Anzeige, ggf. Anklage, gesundheitliche Folgen, Folgen für Dritte (Familie…)
Unternehmen	Verzicht auf Digitalisierungsschritte, damit Verzicht auf Effizienzsteigerung	Image-Schaden bei Bekanntwerden des Cyberangriffs	Verlust von Kundschaft aufgrund von Image-Schaden Minderung des Unternehmenswertes (z. B. durch reduziertes Wachstum)[19]
Staat und Gesellschaft	Verzicht auf Einsatz geeigneter Infrastrukturkomponenten, denen höhere Angreifbarkeit durch Cyberkriminalität zugeschrieben wird	Durch Cybercrime erzwungenes Aussetzen staatlichen Handelns	Verlust von Vertrauen in staatliche Institutionen (Sicherheitsbehörden, Verwaltungen) und Prozesse (Meinungsbildung, Wahlen)

[19] Hierbei handelt es sich um einen Schaden, der sich in der Theorie zwar prinzipiell in finanziellen Geldwerten messen lässt, aber faktisch unmöglich schätzbar ist. Da der Börsenwert eines Unternehmens von sehr vielen Faktoren beeinflusst wird und die Auswirkungen eines Cyberangriffs z.T. sehr stark verzögert auftreten können, lassen sich Veränderungen des Unternehmenswertes sehr schwer auf einen einzelnen Angriff zurückführen. Daher wird dieser Schadenspunkt hier als „nicht schätzbarer Schaden“ mitaufgeführt.

3 Empirische Daten zur Schätzung der Kosten

Im Folgenden werden die Kosten des vorgeschlagenen Modells, die durch Cybercrime im engeren Sinne entstehen, separat für die Ebenen Privatpersonen, Unternehmen und Staat dargestellt. Es wird zurückgegriffen auf kommerzielle sowie wissenschaftliche Studien aus dem Bereich, die dezidierte Schätzungen für Deutschland liefern. Dabei wird im Einzelnen auch auf methodische Schwierigkeiten der jeweiligen Erhebungen hingewiesen.

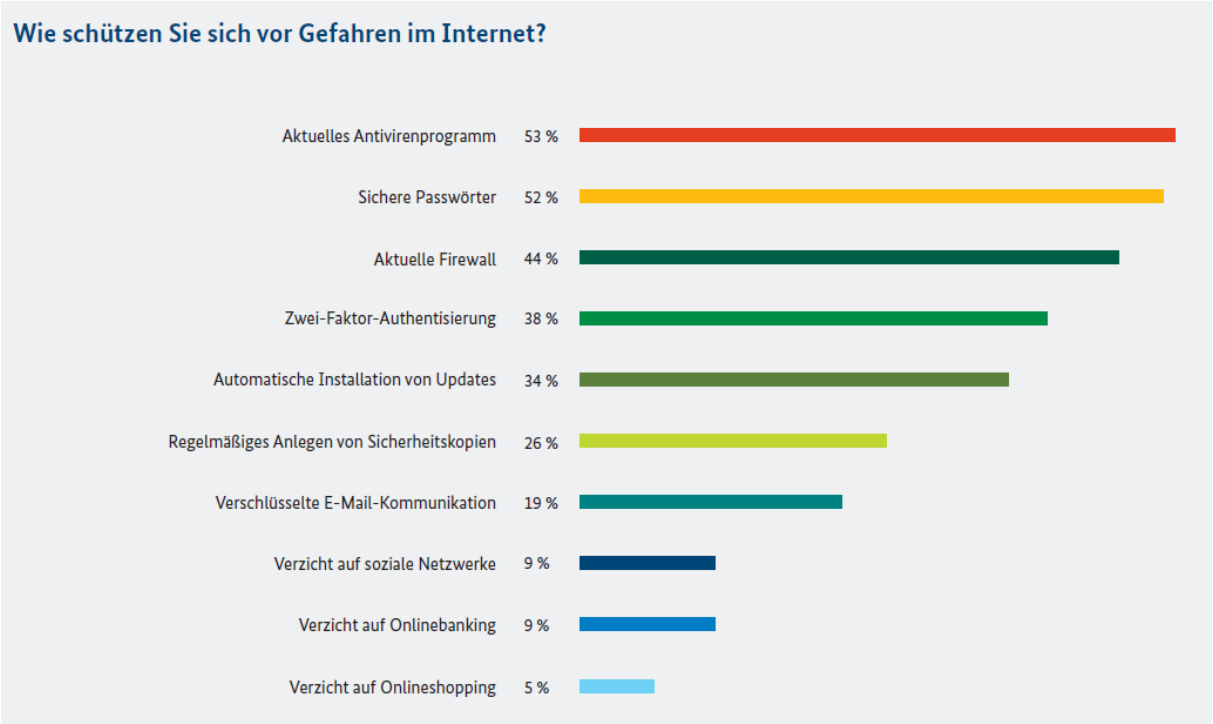
3.1 Privatpersonen

Im deutschsprachigen Raum gibt es kaum Studien, die die Kosten durch Cybercrime für Privatpersonen systematisch erfassen. Gängige Dunkelfeldstudien wie beispielsweise der Deutsche Viktimisierungssurvey (DVS; siehe Weber und Wührl, 2022), SKiD[20] (Birkel et al., 2022) oder das Digitalbarometer (Van Nek & Borz, 2022) erfassen zwar in der Regel die Prävalenz und die Anzeigequote einzelner Cyber-Delikte, geben aber keine oder kaum Auskunft über den durch die Viktimisierung entstandenen, materiellen Schaden oder über die privaten Ausgaben für Cybersicherheitsmaßnahmen. Angaben zu den materiellen Schäden, die Privatpersonen als Antizipation, Reaktion oder Konsequenz durch Cyber-Kriminalität erleiden, sind daher nur auf Basis ungefährer Schätzungen möglich. Es wird dennoch versucht, sich einer Zahl, die die Kosten für Privatpersonen abbildet, anzunähern. Hierbei ist jedoch zu betonen, dass die herangezogenen Studien Schwächen aufweisen, welche die Generalisierbarkeit der Ergebnisse einschränken.

3.1.1 Präventionskosten

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) geben seit 2019 jährlich eine Studie in Auftrag, die den Kenntnisstand der Bevölkerung zu den Themen IT-Sicherheit und Cyber-Kriminalität untersucht (Van Nek & Borz, 2022). Für die Studie wird eine deutschsprachige, repräsentative[21] Netto-Stichprobe von insgesamt 2.000 Personen[22] im Alter von 16 bis 69 Jahren mittels Online-Befragung untersucht (Van Nek & Borz, 2022). Von den 2022 befragten Personen gaben 53 % an, über ein aktuelles Antivirenprogramm und 44 % über eine aktuelle Firewall zu verfügen (Van Nek & Borz, 2022).

[20] „Sicherheit und Kriminalität in Deutschland“
[21] Die repräsentative Stichprobe wurde anhand der Merkmale Alter, Geschlecht, Bildung und Bundesland aus dem Ipsos Online-Access-Panel gezogen. Die Ergebnisse der Befragung wurden anhand dieser Merkmale gewichtet.
[22] Die Personen leben weiterhin in einem Privathaushalt und verfügen über einen Internetzugang.



Quelle: Digitalbarometer 2022 (van Nek und Borz, 2022)

In einer aktuellen Verbraucherumfrage von Bitkom Research gaben 67 Prozent der Befragten an, kostenpflichtige Antiviren-Programme zu nutzen (Marwan, 2022). Von diesen haben 37 Prozent ein Abonnement abgeschlossen, das im Durchschnitt 29,70 Euro im Jahr kostet (Marwan, 2022). Die Übrigen haben eine Einmalzahlung von durchschnittlich 45,20 Euro geleistet (Marwan, 2022).

Angenommen die Ergebnisse ließen sich auf die deutsche Allgemeinbevölkerung übertragen, sodass von 66,6 Mio. Internetnutzenden[23] 53 % über ein aktuelles Antivirenprogramm verfügen (~ 35,3 Mio.) und von diesen wiederum 67 % ein *kostenpflichtiges* Programm besitzen. Das würde bedeuten, dass etwa 23,7 Mio. Personen in Deutschland finanzielle Ausgaben für Antivirenprogramme haben. Wenn von diesen wiederum 37 % ein Abonnement besitzen (~ 8,8 Mio.), das im Durchschnitt 29,70 Euro pro Jahr kostet, würde das **jährliche** Ausgaben in Höhe von rund **259 Mio. Euro** durch Privatpersonen für Präventionszwecke bedeuten. Darüber hinaus wäre davon auszugehen, dass in der Vergangenheit zusätzlich noch **Einmalzahlungen** in Höhe von insgesamt **rund 675 Mio. Euro** geleistet wurden.[24] Hinzu kämen ggf. noch weitere finanzielle Kosten, wie z. B. für aktuelle Firewalls. Hierzu liegen aber leider keine empirischen Daten vor, die Aufschluss über entsprechend geleistete Kosten geben würden.

3.1.2 Kosten als direkte Konsequenz der Straftat

Die bundesweit in Kooperation mit dem Bundeskriminalamt und den Polizeien der Länder durchgeführte Bevölkerungsumfrage „Sicherheit und Kriminalität in Deutschland“ (SKiD) aus dem Jahr 2020 liefert aktuelle und repräsentative Daten im Hinblick auf Viktimisierungserfahrungen durch Cyber-Kriminalität (Birkel et al., 2022). Befragt wurde hierfür eine repräsentative Netto-Stichprobe der in Deutschland lebenden Personen ab 16 Jahren in Privathaushalten von rund 45 000 Personen (Birkel

[23] Laut Destatis für 2021, siehe: https://de.statista.com/statistik/daten/studie/36146/umfrage/anzahl-der-internetnutzer-in-deutschland-seit-1997/
[24] Von den 23,7 Mio. Personen, die finanzielle Ausgaben für Antivirenprogramme angaben, haben 63 % (~ 15 Mio.) Einmalzahlungen in Höhe von durchschnittlich 45,20 Euro geleitet (siehe Marwan, 2022).

et al., 2022). Die Befragung ergab, dass innerhalb eines Jahres insgesamt 13,5 % der Bevölkerung mindestens einmal Opfer einer Cyber-Straftat wurden (Birkel et al., 2022). Erfasst wurde eine Opferwerdung durch Waren- oder Dienstleistungsbetrug im Internet[25] (7,5 %), einen Missbrauch persönlicher Daten bei Nutzung des Internets (6,1 %), eine Infizierung mit Computerviren (3,4 %), einen Cyberangriff auf Online-Banking (2,0 %) sowie durch sonstigen Betrug im Internet (1,6 %) (Birkel et al., 2022). Die Dunkelfeldbefragung SKiD liefert allerdings keine weiteren Daten, die eine Schätzung des finanziellen Schadens ermöglichen würde (Birkel et al., 2022).
Im Digitalbarometer 2021 gaben sogar 38 % der Befragten an, in den letzten zwölf Monaten mindestens einmal Opfer einer Straftat im Cyber-Raum gewesen zu sein (Onemichl & Borz, 2021).[26] Von den Straftaten, die unter Cybercrime im engeren Sinne fallen, traten Schadsoftware (4%) und Ransomware (1%) innerhalb der letzten zwölf Monate am häufigsten auf (Onemichl & Borz, 2021). Von den betroffenen Personen gaben 79 % an, bereits einen Schaden durch Cybercrime erlitten zu haben, wobei vor allem ein zeitlicher Schaden (29%) und ein Verlust von Daten (27 %) berichtet wurde (Onemichl & Borz, 2021).[27] Einen finanziellen Schaden berichteten nur 11 % der Betroffenen, dieser lag zwischen 20 und 2.000 Euro (Onemichl & Borz, 2021). In absoluten Zahlen würde das bedeuten, dass von insgesamt 66,6 Mio. Internetnutzenden[28] in Deutschland rund 25,3 Mio. (38 %) innerhalb eines Jahres Opfer einer Cyber-Straftat werden und davon etwa 2,8 Mio. Personen in Deutschland (11 % der Opfer) einen finanziellen Schaden durch Cyber-Kriminalität erleiden.

Leider wird in der Studie keine Zahl für den durchschnittlichen, erlebten Schaden berichtet. Geht man jedoch von dem berichteten Minimum (= 20 Euro) aus, ergäbe das **mindestens** einen monetären Gesamtschaden von ca. **56 Mio. Euro** und einen **Maximalschaden** (Maximum = 2.000 Euro) von rund **5,6 Mrd. Euro** für Privatpersonen in Deutschland. Bemerkenswert ist hierbei, dass der berichtete finanzielle Schaden von Privatpersonen 2021 rückläufig war: Während im Digitalbarometer 2020 noch 32 % abgaben, einen finanziellen Schaden erlitten zu haben, waren es 2021 nur noch 11 % (Onemichl & Borz, 2021). Die Herausgebenden des Digitalbarometers erklären die Entwicklung dadurch, dass es weniger Opfer von Betrug beim Online-Shopping[29] gab als im Vorjahr (Onemichl & Borz, 2021, S. 6).

Eine andere Möglichkeit, sich der Schadenssumme für Privatpersonen anzunähern, wäre auf Basis der Polizeilichen Kriminalstatistik (PKS). Diese Strategie wurde auch von Journalisten aus Großbritannien gewählt, die exemplarisch polizeiliche Statistiken aus mehreren Ländern genutzt haben, um anhand dieser Zahlen eine weltweite Schadenssumme zu berechnen[30]. Auf Basis der in der PKS aufgetretenen Fälle und des dort berichteten Gesamtschadens wird ein durchschnittlicher Schaden pro angezeigtem Fall berechnet. Der durchschnittliche Schaden pro Fall wird wiederum mit der errechneten Gesamtzahl an Vorfällen[31] multipliziert, d. h. auf das Hell- und Dunkelfeld hochgerechnet, und ergibt den Gesamtschaden für Deutschland. Für das Jahr 2021 sähe das konkret folgendermaßen aus: 2021 wurden insgesamt 99.311 vollendete Fälle unter dem Schlüssel für Computerbetrug (§ 263a StGB)

[25] Bei dem Delikt handelt es sich um Cybercrime im weiteren Sinne. In Dunkelfeldstudien wird leider selten eine klare Trennung zwischen CCieS und CCiwS vorgenommen, sodass die Delikte häufig gemeinsam erfasst und ausgewertet werden (siehe Birkel et al., 2022; Onemichl & Borz, 2021; Van Nek & Borz, 2022).
[26] Die Diskrepanz gegenüber den SKiD-Ergebnissen kommt vermutlich dadurch zustande, dass im Rahmen der Digitalbarometer-Befragung auch Angriffsarten wie Smishing (=Phishing-Angriffe per SMS, 7%) und Phishing (5%) sowie der Fremdzugriff auf einen Online-Account (9%) erfasst wurden. Bei diesen Delikten werden in der Regel persönliche Daten abgegriffen oder kompromittiert, von einem unmittelbaren finanziellen Schaden ist jedoch nicht auszugehen. Im Rahmen der Befragung wurden außerdem auch Delikte, die zu Cybercrime im weiteren Sinne zählen, erfasst (wie Cybermobbing, Problematische Inhalte, Cyberstalking).
[27] Auf nicht-finanzielle Schäden wird inhaltlich unter 6.1.3 näher eingegangen.
[28] Laut Destatis für 2021, siehe: https://de.statista.com/statistik/daten/studie/36146/umfrage/anzahl-der-internetnutzer-in-deutschland-seit-1997/
[29] Entspricht dem Delikt Waren- und Dienstleistungsbetrug im Internet und ist daher CCiwS.
[30] Siehe https://www.comparitech.com/blog/vpn-privacy/cybercrime-cost/
[31] Hell- und Dunkelfeld, hierfür wird die Hellfeld-Zahl mit der Anzeigequote verrechnet.

in der PKS registriert (Bundeskriminalamt, 2022b).[32] Für diese Delikte wurde eine Schadenssumme von insgesamt 125.003.465 Euro erhoben (Bundeskriminalamt, 2022b). Verrechnet man zunächst die Zahl der angezeigten, vollendeten Fälle in der PKS mit der Anzeigequote bei Cyber-Delikten (17,9 %, siehe Birkel et al., 2022), ergibt das eine geschätzt absolute Fallzahl (Hellfeld und Dunkelfeld) von insgesamt 554 810 Fällen des Computerbetrugs in Deutschland. Auf Basis der Zahlen der PKS (Bundeskriminalamt, 2022b) berechnet sich außerdem der durchschnittliche Schaden pro Fall (Schadenssumme durch Anzahl vollendeter Fälle), dieser liegt 2021 bei 1.259 Euro.

Das heißt in der Folge: Für insgesamt 554 810 Cybercrime-Fälle in Deutschland, bei denen ein durchschnittlicher Schaden von 1.259 Euro entstanden ist, lässt sich von einem **Gesamtschaden von rund 700 Mio. Euro**[33] ausgehen.
Diese Schätzung ist etwa 13-mal höher als der Minimalschaden und entspricht etwa einem Achtel des Maximalschadens, basierend auf den Daten des Digitalbarometers. Die Schätzung von 700 Mio. Euro erscheint daher eine durchaus plausible Annäherung an den Gesamtschaden. An dieser Stelle sei dennoch erneut darauf hingewiesen, dass in der PKS viele Cyber-Delikte (wie bspw. Ransomware) nicht unter dem Summenschlüssel Cybercrime, sondern anderweitig erfasst werden (siehe 2.1) und die Berechnung anhand der PKS-Daten daher ebenfalls Schwächen aufweist.

3.1.3 Kosten als Reaktion auf die Straftat

Zu den Kosten als Reaktion auf die Cyber-Straftat für Privatpersonen liegen bislang keine wissenschaftlichen Erkenntnisse vor. Zwar sind in Tabelle 1 Anwaltskosten und damit verknüpft gegebenenfalls anfallende Gerichtskosten beispielhaft aufgeführt, doch es liegen bislang keine empirischen Daten dazu vor, inwieweit diese Kosten bei Cybercrime-Delikten gegenüber Privatpersonen eine Rolle spielen und wie sich diese finanziell einschätzen lassen. Da im Allgemeinen nur ein geringer Anteil an erlebten Cybercrime-Delikten von der Bevölkerung zur Anzeige gebracht wird und Cybercrime-Delikte noch dazu von Privatpersonen als „weniger schlimm“ eingeschätzt werden (Weber & Wührl, 2022), ist im Allgemeinen eher zu vermuten, dass Anwalts- oder Gerichtskosten für Privatpersonen bei Cyber-Delikten eine geringe Rolle spielen.

Finanziell messbare Schäden (Kosten)

	Präventionskosten	**Kosten als direkte Konsequenz der Straftat**	**Kosten als Reaktion auf die Straftat**
Privatpersonen	259 Mio. Euro jährlich für Abonnements (Antivirenprogramme) ~ 675 Mio. Euro für Einmalzahlungen (Antivirenprogramme)	Ca. 700 Mio. Euro Min. 56 Mio., Max. 5,6 Mrd.	Keine Datengrundlage, vmtl. vernachlässigbar

[32] Für die Schlüssel 543000 (Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB), 674200 (Datenveränderung, Computersabotage §§ 303a, 303b StGB) und 678000 (Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen gemäß §§ 202a, 202b, 202c StGB), die ebenfalls unter den Summenschlüssel Cybercrime fallen, werden keine Daten zum entstandenen Schaden erhoben.
[33] Konkret sind es 689.343.309 Euro.

3.2 Unternehmen

Im Gegensatz zu den Schäden gegen Privatpersonen gibt es im Bereich der Schäden gegen Unternehmen eine Vielzahl unterschiedlicher Studien, die aber häufig durch kommerzielle Firmen oder Verbände (Accenture Security, 2019; Bitkom e.V., 2020; GDV, 2018; Hiscox, 2021; KPMG AG, 2019) in Auftrag gegeben werden. Die angewandte Methodik zur Schätzung der Kosten unterscheidet sich in diesen Studien zum Teil sehr stark, sodass die Ergebnisse in Bezug auf den errechneten Gesamtschaden für Unternehmen ebenfalls sehr variieren. So kommt die Firma Accenture in ihrer „Cost of Cybercrime"-Studie aus dem Jahr 2019 auf einen durchschnittlichen, jährlichen Gesamtschaden von etwa 13 Mio. USD pro (Groß-)Unternehmen in Deutschland (Accenture Security, 2019).[34] Der Verband Bitkom wiederum nennt anhand seines Schadensberechnungsmodells eine Summe von 100 Milliarden Euro Gesamtschaden jährlich für die deutsche Wirtschaft in den Jahren 2018 und 2019 (Bitkom e.V. 2020).

Anhand dieser Beispiele zeigt sich eindrücklich, wie unterschiedlich mit der Fragestellung umgegangen wird. Dieser Unterschied liegt häufig einerseits in der Stichprobenziehung, d. h. in der konkreten Auswahl von Firmen, die zu der Fragestellung befragt werden. Während in der Bitkom-Studie eine Stichprobe von 1.007 nach Branchen- und Größenklassen repräsentativ ausgewählter Unternehmen zu den entstandenen Schäden innerhalb der letzten zwei Jahre befragt wurden (Bitkom e.V., 2020), wurde im Rahmen der Accenture-Studie nur eine hochselektive Stichprobe von insgesamt 355 Großunternehmen mit mehr als 5.000 Beschäftigten zu den entstandenen Schäden innerhalb der letzten vier Wochen[35] befragt (Accenture Security, 2019; siehe Tabelle 1).

Doch nicht nur die Stichprobenziehung unterscheidet sich in den jeweiligen Studien, es werden auch unterschiedliche, statistische Maße berichtet. So wurde in den Studien von Bitkom e.V. (2020) und Accenture Security (2019) das arithmetische Mittel zur Schätzung verwendet, wohingegen z. B. der Versicherer Hiscox (2021) den Median (siehe Infobox) und das 95-Prozent Perzentil[36] als statistisches Schadensmaß pro Unternehmen berichtet (Tabelle 1). Laut Hiscox (2021) liegt der Median bei Cyberangriffen in Deutschland bei 24.000 $, der wirtschaftliche Gesamtschaden für Deutschland wird auf knapp 50 Millionen Dollar geschätzt (Tabelle 1). Die Wirtschaftsprüfungsgesellschaft KPMG AG (2019) verzichtet bewusst auf die Angabe eines Durchschnittswerts und nutzt stattdessen Verteilungsmaße: Im Ergebnis bedeutet das, dass die mittleren 50 Prozent der Unternehmen, d. h. ausgenommen der 25 Prozent der Unternehmen mit den geringsten sowie der 25 Prozent der Unternehmen mit den höchsten Schäden, einen Schaden zwischen 20.000 und 150.000 Euro erlitten haben (KPMG AG, 2019). Die sehr unterschiedliche, statistische Herangehensweise erschwert letztlich eine Vergleichbarkeit der Studienergebnisse.

[34] Befragt wurden allerdings nur Großunternehmen mit mehr als 5.000 Beschäftigten; siehe Tabelle 1.
[35] Auf Basis der Angaben bezogen auf die Zeitspanne von vier Wochen wurden die Hochrechnung der jährlichen Kosten vollzogen.
[36] Das 95-Prozent Perzentil gibt an, in welchem Bereich 95 % der erfassten Werte liegen. Genauer gesagt liegen 95 % der Werte unterhalb des Perzentils und 5 % der Werte oberhalb des Perzentils.

Median und Mittelwert

*Der **Median** ist das statistische Maß, das eine Verteilung von Messwerten in genau zwei Hälften teilt. Das bedeutet, 50 % der Messwerte liegen unterhalb des Medians und 50% der Messwerte oberhalb des Medians. Der Vorteil des Medians gegenüber dem Mittelwert liegt darin, dass er eine klarere Auskunft über die Verteilung der Daten gibt und weniger anfällig für Ausreißer ist.*

*Der **Mittelwert** wird berechnet, indem die Summe einer Wertereihe durch die Anzahl der Wertereihe geteilt wird. Er ist anfällig für extreme Ausreißer, die den Mittelwert nach oben oder unten verzerren könne.*

Am Kriminologischen Forschungsinstitut Niedersachen (KFN) wurde 2020 der Ergebnisbericht zu einer Studie von Dreißigacker et al. (2020)., die auf der Befragung von 5.000 Unternehmen in Deutschland basierte, veröffentlicht. Im Rahmen der Studie wurden umfängliche Analysen der durch Cyberkriminalität verursachten Kostenpositionen vorgenommen, wobei jeweils der Median sowie das arithmetische Mittel der Ergebnisse berichtet wurde. Die Autorinnen und Autoren berichten Gesamtkosten zwischen 10 Euro und 2 Mio. Euro je Unternehmen, wobei ein einzelner Cyber-Angriff im Durchschnitt 16.900 Euro kostete (Dreißigacker et al., 2020). Der Durchschnitt wird allerdings durch wenige Extremwerte stark beeinflusst. Im Vergleich lag nämlich der Median bei nur 1.000 Euro (Dreißigacker et al., 2020). Das bedeutet, dass 50 Prozent der Unternehmen einen Schaden von 1.000 Euro oder weniger hinnehmen mussten. Darüber hinaus zeigte sich, dass die Kosten infolge eines Cyberangriffs höher ausfallen, je größer das betroffene Unternehmen ist (Dreißigacker et al., 2020; Hiscox, 2021).

Eine Schätzung der tatsächlichen Kosten, die Unternehmen als Folge von Cyberangriffen innerhalb eines Jahres erleiden, ist demnach methodisch herausfordernd. Nicht nur die Stichprobe der in der Untersuchung berücksichtigten Unternehmen, auch die Auswahl der statistischen Maße und die Frage, welche Unternehmenscharakteristika in der Analyse berücksichtigt werden (hinsichtlich Größe, Branche etc.), können die Ergebnisse beeinflussen. Weitere Probleme der Erfassung liegen in der oftmals „mäßigen Auskunftsbereitschaft“ der Unternehmen sowie dem Umstand, dass „nur wenige Unternehmen die entstanden direkten Kostenpositionen tatsächlich ermitteln und nachhalten“ (Dreißigacker et al., 2020, S. 140). Trotz dieser Limitationen wird im Folgenden versucht, die Kosten für Unternehmen, die (1) durch Präventionsbemühungen, (2) als direkte Konsequenz der Straftat und (3) als Reaktion auf die Straftat entstehen, soweit möglich anhand bisheriger, empirischer Erhebungen zu analysieren und eine Schätzung der Kostenhöhe vorzunehmen.

Tabelle 1. Übersicht über bisherige Studien anhand ihrer Stichproben, Erhebungszeiträume und statistisch verwendeten Maße zur Darstellung des Schadens

Studie (Jahr)	Stichprobe	Erhebungszeitraum	Statistische Maße zur Darstellung des Schadens
Accenture Security (2019)	355 Großunternehmen mit mehr als 5.000 Beschäftigten aus elf Ländern[37], davon 40 aus Deutschland	Mehrere Monate im Jahr 2018	Jährlicher Durchschnittsschaden (arithmetisches Mittel) pro Unternehmen[38]
Bitkom e.V. (2020)	1007 nach Branchen- und Größenklassen repräsentativ ausgewählte Unternehmen mit mind. 10 Beschäftigten, geschichtete Zufallsstichprobe	Mai und Juni 2019	Darstellung der Gesamt-Schadenssumme für die deutsche Wirtschaft, basierend auf Hochrechnungen[39] der durchschnittlichen Schadenssumme pro Unternehmen[40]
Dreißigacker et al. (2020)	5.000 Unternehmen ab 10 Beschäftigten, geschichtete Zufallsstichprobe aus kommerziellen Unternehmensdatenbanken[41]	August 2018 bis Januar 2019	Durchschnittskosten (arithmetisches Mittel) und Median der Kosten für schwerwiegendsten Angriff sowie prozentuale Angaben zu klassifizierten[42] Gesamtkosten nach Cyberangriffsart
GDV (2018)	3000 Vertreter/innen von kleinen und mittleren Unternehmen (bis 249 Beschäftigte bzw. 50 Mio. Euro Jahresumsatz)	März/April 2018	Keine Angaben zu Kostenpositionen, nur prozentuale Angaben zu Schadensarten
Hiscox (2021)	Vertreter/innen von 6.042 repräsentativ nach Branche und Größe ausgewählte Unternehmen aus acht Ländern (UK, Belgien, Irland, USA, den Niederlanden, Deutschland, Frankreich und Spanien)	November 2020 bis Januar 2021	Median und 95%-Perzentil der Kostensumme (in 1T $) je Beschäftigtengrößenklasse Für Deutschland: Zusätzlich Median der Kosten pro Unternehmen und wirtschaftlicher Gesamtschaden[43]

[37] USA, UK, Deutschland, Japan, Frankreich, Brasilien, Kanada, Australien, Spanien, Italien, Singapur
[38] Dieser bezieht sich auf alle in der Stichprobe enthaltenen Länder bezieht.
[39] Die Hochrechnungen erfolgten auf der Grundlage der Umsatzsteuerstatistik des Statistischen Bundesamts.
[40] Bei der Hochrechnung wurde die Stichprobe um Ausreißer bereinigt. Daher sprechen die Herausgebenden von einer eher konservativen Berechnung der Schadenssumme.
[41] Umfasste Unternehmen aus nahezu allen Branchen der offiziellen Klassifikation der Wirtschaftszweige (WZ08-A bis S)
[42] Je Cyberangriffsart (Ransomware, Spyware etc.) wird der prozentuale Anteil der klassifizierten Gesamtkosten (Klassen in Tausend Euro: < 1T, 1T < 5T, 5T<10T, 10T<50T, ab 50T) dargestellt.
[43] Diese Daten wurden für Deutschland zusätzlich angegeben, da sie im internationalen Vergleich besonders hoch ausfielen. Der wirtschaftliche Gesamtschaden in Deutschland betrug dabei mehr als ein Drittel des im Rahmen der Studie erfassten, internationalen Gesamtschadens über alle acht Länder hinweg.

KPMG AG (2019)	1.001 Vertreter/innen von repräsentativ nach Branche und Umsatz ausgewählten Unternehmen	September 2018 bis Januar 2019 (Folgestudie zu vorherigen Studien aus den Jahren 2015 und 2017)	Verzicht auf Angabe eines Durchschnittswerts. Stattdessen prozentual gestaffelte Angabe des Gesamtschadens nach Unternehmensgröße, gemessen am Umsatz (z. B. einen Schaden von mehr als 1 Mio. Euro hatten 22 % der Großunternehmen mit einem Umsatz über 3 Mrd. Euro)

3.2.1 Präventionskosten

In Anlehnung an das unter Punkt 2.2.1 dargestellte Modell werden zunächst die Kosten durch Antizipation der Straftat erfasst. Darunter sind verschiedene Ausgaben für Präventions-Zwecke zu verstehen. Im Rahmen des Modells werden dabei drei zentrale Kostenpunkte genannt: (1) IT-Sicherheitspersonal, (2) Technische Schutzmaßnahmen (Cybersicherheit), (3) Cyberversicherungen sowie (4) Mitarbeitenden-Schulungen (z. B. gegen Phishing-Angriffe). Dies ist keine abschließende Auflistung, sie umfasst aber die wesentlichen durch Präventionsbemühungen entstehenden Kosten.
Über die Datenbank des Deutschen Statistischen Bundesamts GENESIS werden die Daten der Unternehmen aus dem Unternehmensregister für das Jahr 2021[44] abgerufen. Dort waren für das Jahr 2021 insgesamt etwa 3,68 Mio. Unternehmen in unterschiedlichen Beschäftigtenklassen[45] registriert, wobei mit großem Abstand die meisten Unternehmen in die die kleinste Klasse mit 0 bis 9 sozialversicherungspflichtig Beschäftigten fallen (N = 3.130.446).

In der Studie von Dreißigacker et al. (2020) wurden allerdings Unternehmen mit weniger als 10 Beschäftigten nicht in die Analysen einbezogen, weshalb für diese Klasse keine Daten (hinsichtlich Prävalenz, Schadensberechnung etc.) vorliegen. Da für die folgenden Kostenberechnungen die Ergebnisse der KFN-Studie zugrunde gelegt werden, wird diese Unternehmensklasse daher zunächst aus der folgenden Berechnung ausgeklammert. In der genannten Studie wurde zunächst die Anzahl der Beschäftigten im Bereich der IT- und Informationssicherheit erfasst (siehe Tabelle 2). So gaben 97,2 % der befragten Unternehmen an, weniger als 10 Beschäftigte in diesem Bereich zu haben, 59,8 % hatten sogar weniger als zwei Beschäftigte und 13,2 % der Unternehmen gaben an, keine Beschäftigten im Bereich IT- und Informationssicherheit zu haben. Aufgrund der gestaffelten Angaben ist es nicht möglich, einen Durchschnittswert zu berechnen. Zum Zwecke der weiteren Berechnungen wird angenommen, dass der Durchschnitt bei etwa zwei IT-Sicherheitsangestellten pro Unternehmen liegt – wohl wissend, dass leichte Abweichungen nach unten oder oben hierbei möglich sind.

[44] Siehe https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Unternehmensregister/Tabellen/betriebe-beschaeftigtengroessenklassen-wz08.html
[45] Anzahl der Unternehmen mit 0 bis 9 sozialversicherungspflichtigen Beschäftigten: 3.130.446, 10 bis 49 sozialversicherungspflichtigen Beschäftigten: 433.028, 50 bis 249 sozialversicherungspflichtigen Beschäftigten: 95.847, mehr als 250 sozialversicherungspflichtigen Beschäftigten: 16.464.

Tabelle 2. Anzahl der Beschäftigten im Bereich der IT- und Informationssicherheit anhand der Anzahl befragter Unternehmen (siehe Dreißigacker et al., 2020)

Anzahl der Beschäftigten im Bereich der IT- und Informationssicherheit	Anzahl der befragten Unternehmen (N = 4.244)
0	562
1	1.979
2 bis 9	1.583
10 bis 24	85
25 bis 99	26
100 und mehr	9

Eine Internet-Recherche auf Berufsinformationsportalen hat ergeben, dass das Durchschnittsgehalt eines IT-Sicherheitsbeschäftigten bei ca. 65.000 Euro brutto jährlich liegt (durchschnittliche Angaben zwischen 58.100 Euro und 76.335 Euro)[46]. Das entspricht Arbeitgeber-Bruttokosten von ca. 80.000 Euro[47] pro IT-Fachkraft jährlich.
Geht man folglich davon aus, dass jedes Unternehmen mit mehr als 10 Beschäftigten für durchschnittlich zwei IT-Sicherheitsfachkräfte etwa 160.000 Euro jährlich ausgibt, bedeutet das: Hochgerechnet auf die 545.339 im Unternehmensregister registrierten Unternehmen mit mehr als 10 Beschäftigten entstehen **Kosten von rund 87 Mrd. Euro** für deutsche Unternehmen, die allein in das **IT-Sicherheitspersonal** investiert werden.

In einer weiteren Quelle[48] wurde die Anzahl der Angestellten im Bereich Cybersicherheit in Deutschland mit 464.749 beziffert ((ISC)², 2022). Hier ist allerdings nicht ersichtlich, wie die Zahl zustande kam, die Autorinnen und Autoren weisen lediglich darauf hin, dass sie „eine Vielzahl an primären und sekundären Datenquellen" verwendet haben ((ISC)², 2022, S. 5).[49] Verwendet man nun diese Zahl zur Hochrechnung und geht weiterhin von Arbeitgeber-Bruttokosten in Höhe von durchschnittlich 80.000 Euro aus, ergäbe das Kosten von rund **37. Mrd. Euro** durch IT-Sicherheitspersonal.

Das sind erhebliche Summen, die deutlich über den unter 6.2.2 berechneten Schäden als direkte Konsequenz für Unternehmen liegt. In diesem Zusammenhang sei auf eine Feststellung der Studie von Hillebrand et al. (2018, S. 55) verwiesen, die angeben, dass „Experten zufolge [...] das Gehalt eines IT-Sicherheitsspezialisten erheblich über den jährlich (vermutlich) verursachten Schäden [liegt]"[50]. Nichtsdestotrotz ist hier darauf hinzuweisen, dass die durch Cyber-Kriminalität entstehenden Kosten und die weiteren, nicht-finanziellen Schäden (siehe 4.2) voraussichtlich noch um Einiges höher ausfallen würden, wenn es keine Sicherheitsmaßnahmen in Unternehmen gäbe, die durch IT-Sicherheitsbeschäftigte implementiert würden. Die Investitionen, die im Bereich IT-Sicherheit getätigt werden, geben daher auch Aufschluss darüber, welch erheblicher Wert der IT-Sicherheit besonders in großen Unternehmen (mittlerweile) zugemessen wird.

[46] https://www.karrieresprung.de/jobprofil/it-sicherheitsbeauftragte/
https://www.stepstone.de/gehalt/IT-Security-Engineer.html
https://www.gehalt.de/beruf/it-sicherheit
[47] Inklusive der für den Arbeitgeber anfallenden Versicherungskosten (Rentenversicherung, Arbeitslosenversicherung, Pflegeversicherung, Krankenversicherung) und Umlagen.
[48] Bei dem Herausgeber der Studie handelt es sich um eine internationale Nonprofit-Organisation, die „International Information System Security Certification Consortium, Inc"
[49] Wörtlich: "This proprietary methodology integrates a wide array of primary and secondary data source..." ((ISC)², 2022, S. 5) wie Erkenntnisse aus Befragungen, die statistische Schätzung des U.S. Bureau of Labor und Daten aus Trendanalysen (siehe (ISC)², 2022, S. 80).
[50] Gemeint sind hier vermutlich die zu erwartenden Schäden durch Cyberangriffe.

Einige Befragungen geben außerdem Auskunft darüber, dass viele Unternehmen großen Wert auf die Implementierung technischer Schutzmaßnahmen legen, um die Firma vor Angriffen zu schützen. So ergab eine Studie des GDV (2018), dass eine überwiegende Mehrheit der Unternehmen technische Schutzmaßnahmen wie Virenscanner und Firewalls (97%), automatische Sicherheitsupdates (94 %) und systematische Backups (84 %) nutzt, allerdings weniger Unternehmen auch weitere, organisatorische Schutzmaßnahmen implementieren, z. B. indem für jeden Mitarbeitenden ein eigener, passwortgeschützter Zugang generiert wird (68 %), sensible Daten verschlüsselt werden (54 %) oder die Nutzung privater Geräte in der Unternehmens-IT verboten wird (41 %).

Des Weiteren zeigt sich eine große Diskrepanz zwischen großen und kleinen Unternehmen, da große Unternehmen über deutlich mehr Schutzmaßnahmen verfügen als kleinere Unternehmen (siehe Abbildung 4). So ergab die KFN-Studie, dass Großunternehmen ab 500 Beschäftigten häufiger regelmäßige Risiko- und Schwachstellenanalysen, Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme, sowie Schulungen zur IT-Sicherheit ihrer Mitarbeitenden durchführen als kleine Unternehmen mit zehn bis 49 Beschäftigten (Dreißigacker et al., 2020).

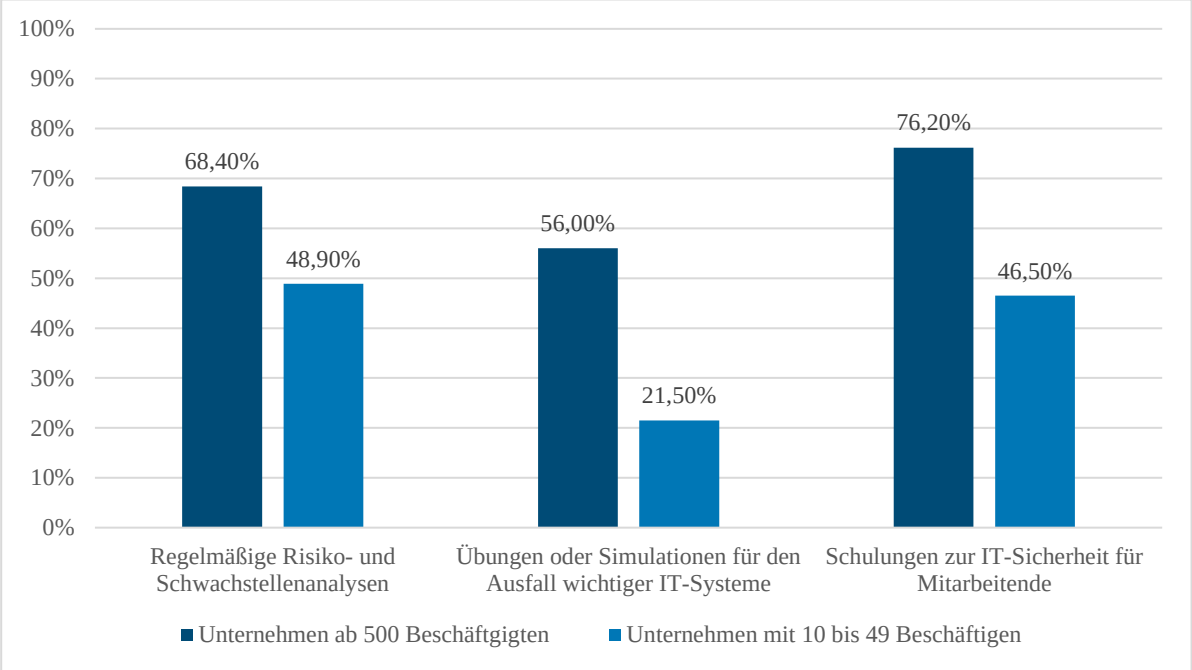


Abbildung 4. Anteil der Unternehmen mit technischen Schutzmaßnahmen nach Beschäftigtengrößenklasse.

Zu dem Ergebnis, dass große Unternehmen mehr in technische und auch in organisatorische Schutzmaßnahmen investieren, kam auch die Studie von Hillebrand et al. (2018) sowie die Cybersicherheits-Umfrage des BSI (2019).

Es zeigt sich also insgesamt, dass Unternehmen im Schnitt über mehr technische Schutzmaßnahmen (Virenschutz, Firewall, Software-Patches, Spamfilter, Verschlüsselungen, Datensicherung) als organisatorische Schutzmaßnahmen (Schulungen, Protokoll-Auswertungen, Regeln, Kontrollen) verfügen und große Unternehmen darüber hinaus insgesamt besser gerüstet sind als kleine Unternehmen. Kleinere Unternehmen schätzen ihr Risiko bezüglich eines Cyber-Angriffs als geringer ein, investieren weniger in die IT-Sicherheit und in Versicherungsschutz und sind dadurch anfälliger für wiederholte Angriffe (GDV, 2018).

In Bezug auf Versicherungsausgaben gaben in der KFN-Studie insgesamt 27,4 % der Unternehmen an, eine Cyberversicherung abgeschlossen zu haben (Dreißigacker et al., 2020). Ähnliche Zahlen wurden auch in anderen Studien berichtet (Bitkom e.V., 2020: 17 %, KPMG AG, 2019: 27%, Hiscox, 2021: 34 %). Es ist allerdings kaum möglich, die hierfür jeweils anfallenden Kostenpositionen zu berechnen, da diese abhängig sind von der festgelegten Versicherungssumme, dem Jahresumsatz des Unternehmens sowie der evtl. gewünschten Zusatzleistungen im Rahmen der Versicherung. Bei einer Versicherungssumme von 50.000 Euro (250 Euro Selbstbeteiligung) zahlt ein Unternehmen mit 100.000 Euro Jahresumsatz ca. 240 Euro jährlich, ein Unternehmen mit 900.000 Euro Jahresumsatz ca. 350 Euro jährlich und ein Unternehmen mit 2 Mio. Euro ca. 960 Euro jährlich[51].

Zusammenfassend zeigen die hier untersuchten Studien, dass große Unternehmen deutlich mehr IT-Sicherheitsmaßnahmen implementieren als kleinere Unternehmen und im Allgemeinen nur etwa jedes zweite Unternehmen angibt, über weitergehende Präventionsmaßnahmen wie Risikoanalysen, Mitarbeitenden-Schulungen oder Managementsysteme für Informationssicherheit zu verfügen. Während zwar etwa jedes vierte Unternehmen angibt, eine Cyber-Versicherung abgeschlossen zu haben, gibt es auch hierzu kaum Zahlen, die eine Schätzung der Kosten zulassen.

Insgesamt gibt es zu dem konkreten Budget, das Unternehmen in technische und organisatorische IT-Sicherheitsmaßnahmen investieren, kaum verlässliche Angaben. In einer Bitkom-Umfrage aus 2017 gaben zwar 74 % der Unternehmen an, dass sie beabsichtigen, ihre Investitionen für das Jahr 2018 zu erhöhen (Bitkom e.V., 2018) – es gibt allerdings kaum Erkenntnisse dazu, in welcher Höhe oder in welcher Relation zum Gesamtbudget des Unternehmens die Investitionen liegen. In der Studie von Hillebrand et al. (2018) gaben die befragten kleinen und mittleren Unternehmen an, für das Jahr 2017 Ausgaben von durchschnittlich 2.600 Euro für die IT-Sicherheit zu planen. Für die rund 545 Tsd. registrierten Unternehmen mit mehr als zehn Beschäftigten im Unternehmensregister würde das bedeuten, dass eine Summe von **insgesamt ca. 1,4 Mrd. Euro** jährlich in **IT-Sicherheit** investiert wird – wobei es nicht unwahrscheinlich ist, dass die Investitionsbereitschaft seit 2017 noch gestiegen ist.

3.2.2 Kosten als direkte Konsequenz der Straftat

Empirisch konnte gezeigt werden, dass die Prävalenzrate für Cybercrime mit der Unternehmensgröße zusammenhängt (GDV, 2018; Paoli et al., 2018b). Daher werden den unterschiedlichen Unternehmensklassen (10-49 Beschäftigte, 50 – 249 Beschäftigte, mehr als 250 Beschäftigte) entsprechend unterschiedliche Prävalenzen zugrunde gelegt, um die absolute Anzahl betroffener Unternehmen zu schätzen (siehe Tabelle 3).

Tabelle 3. Schätzung der Anzahl betroffener Unternehmen auf Basis empirischer Ergebnisse aus der Studie von Dreißigacker et al. (2020)

Beschäftigtengrößenklasse	Anzahl registrierter Unternehmen im Unternehmensregister 2021	Ermittelte Prävalenz je Beschäftigtengrößenklasse (Dreißigacker et al., 2020)	Geschätzte Anzahl absolut betroffener Unternehmen	Anteil der Unternehmen mit Schaden infolge des Angriffs (Dreißigacker et al., 2020)	Geschätzte absolute Anzahl der Unternehmen mit Schaden infolge des Angriffs

[51] Das Beispiel stammt von der Internetseite eines Vergleichsportals für Versicherungsanbieter: https://www.transparent-beraten.de/cyber-versicherung/#Kosten-und-Preise

10 – 49	433.028	39,4 %	170.613	72,3 %	123.353
50 – 249	95.847	46,3 %	44.377	63,1 %	28.002
>250	16.464	53,1 %	8.742	63,6 %	5.560
Summe	545.339		223.733		**156.915**

Auf Basis der erhobenen Zahlen kann in Deutschland eine absolute Anzahl von umgerechnet etwa 157.000 durch Cybercrime geschädigten Unternehmen mit mehr als 10 Beschäftigten angenommen werden (siehe Tabelle 3). Für diese Gesamtzahl an geschädigten Unternehmen wird anhand der Prävalenzen für die Delikte Ransomware (12,5 %), Spyware (11,3 %), sonstige Schadsoftware (21,3 %), manuelles Hacking (2,8 %), DDOS (6,4 %) Defacing (3,1 %) CEO-Fraud[52] (8,1 %) und Phishing (22,0 %) berechnet, wie viele Unternehmen von den jeweiligen Deliktarten betroffen waren. Hieraus ergibt sich je Delikt die geschätzte, absolute Anzahl betroffener Unternehmen (siehe Tabelle 4).

Methodisch ist hier zu beachten, dass in der Studie von Dreißigacker et al. (2020) nur die Kosten infolge des schwerwiegendsten Angriffs erhoben wurden; daher können in unserem Beispiel auch nur diese berücksichtigt werden. Das bedeutet allerdings, dass es sich bei dieser Berechnung um eine äußerst konservative Schätzung der Kosten handelt, denn mehr als die Hälfte der befragten Unternehmen (57,2 %) gaben an, innerhalb des Befragungszeitraums von *mehr* als einem Cyberangriff betroffen gewesen zu sein (Dreißigacker et al., 2020). Es ist daher durchaus wahrscheinlich, dass auch in Folge der weiteren Cyberangriffe Kosten für die Unternehmen entstanden sein können, die in den erfassten Daten jedoch nicht wiedergespiegelt werden.

Nichtsdestotrotz kann die folgende Berechnung als Annäherung an den tatsächlichen Schaden verstanden werden. Denn auf Basis weiterer Studien (Paoli et al., 2018b) ist bekannt, dass die absolute Mehrheit der Cybervorfälle bei Unternehmen keinen oder nur einen geringen Schaden verursachen. So lag beispielsweise auch in der Studie von Dreißigacker et al. (2020) der Median des Schadens bei nur 1.000 Euro jährlich, was bedeutet, dass die Hälfte aller geschädigten Unternehmen mit Kosten bis max. 1.000 Euro konfrontiert waren. Das deutlich höher ausfallende arithmetische Mittel der Gesamtkosten (je Angriff: 16.900 Euro) kommt daher insbesondere auf Basis einiger, besonders teurer Vorfälle zustande (Maximalkosten je Angriff: 2 Mio. Euro; siehe Dreißigacker et al., 2020).
Im Folgenden wird somit die geschätzte, absolute Anzahl jährlich geschädigter Unternehmen verrechnet mit dem durchschnittlichen Schaden des schwerwiegendsten Angriffs[53] je Deliktart (in Anlehnung an Dreißigacker et al., 2020; siehe Tabelle 4). Die Summe des berechneten Schadens pro Angriffsart ergibt wiederum den geschätzten **Gesamtschaden für alle Unternehmen mit mehr als 10 Beschäftigten** in Deutschland. Dieser läge – auf Basis der dargestellten Berechnungen und der Daten von Dreißigacker et al. (2020) – bei insgesamt etwa **1,9 Milliarden Euro** in Deutschland.
Alternativ und weniger aufwändig wäre darüber hinaus die Möglichkeit, den allgemeinen Durchschnittsschaden von 16.900 Euro pro Unternehmen mit der geschätzten, absoluten Anzahl geschädigter Unternehmen zu verrechnen (129.204, siehe Tabelle 3). Das ergibt eine geschätzte **Gesamtschadenssumme** von rund **2,65 Mrd. Euro**. Wie zu erwarten liegt dieser Wert höher als die differenziert errechnete Schadenssumme von 1,9 Mrd. Euro in Tabelle 4. Es ist aber auch nicht auszuschließen, dass dieser Wert durch die wenigen Extremwerte in der Stichprobe etwas nach oben verzerrt ist.

[52] Unter Punkt 2 wurde dargelegt, dass sich dieser Bericht in erster Linie auf Cybercrime im engeren Sinne bezieht. Im Rahmen der KFN-Studie wurde allerdings auch das Delikt CEO-Fraud miterfasst, obwohl dieses definitorisch zu Cybercrime im weiteren Sinne zählt. Da sich die Miterfassung des Delikts nur schwer aus den Gesamtergebnissen der Studie herausrechnen lässt, wurde daher das Delikt CEO-Fraud in die Schätzung mitaufgenommen.
[53] Je erfasstem Angriff wurden folgende Kostenpositionen erfasst: Externe Beratung, Sofortmaßnahmen zur Abwehr und Aufklärung, Schadensersatz/Strafen, abgeflossene Gelder, Betriebsunterbrechung, Wiederherstellung/Wiederbeschaffung. Auf Basis des unter Punkt 4 dargestellten Modells können diese Kostenpositionen dem Bereich „Kosten als direkte Konsequenz der Straftat“ zugeordnet werden und dienen daher im Folgenden als Berechnungsgrundlage.

Tabelle 4. Schätzung der jährlichen Gesamtkosten für alle Unternehmen mit mehr als 10 Beschäftigten anhand empirischer Prävalenzraten der Cyberangriffe (Dreißigacker et al., 2020)

	Absolute Anzahl geschädigter Unternehmen[54]	Durchschnittskosten je Unternehmen	Jährliche Gesamtkosten anhand des Durchschnitts
Ransomware	19.614	32.200 €	631.584.352 €
Spyware	17.731	4.700 €	83.337.751 €
Sonst. Schadsoftware	33.423	8.200 €	274.068.380 €
Manuelles Hacking	4.394	43.700 €	192.001.643 €
DDOS	10.043	25.600 €	257.090.137 €
Defacing	4.864	2.600 €	12.647.379 €
CEO-Fraud	12.710	8.600 €	109.307.245 €
Phishing	34.521	9.300 €	321.048.841 €
Summe			**1.881.085.727 €**

In diesen Schadenssummen sind allerdings noch nicht die Vielzahl an Kleinst-Unternehmen enthalten, die ebenfalls von Cyberangriffen betroffen sein können. Da die Studie von Dreißigacker et al. (2020) hierzu keine Daten liefert, ist es lediglich möglich, hierzu Schätzungen vorzunehmen. Im Allgemeinen zeigen die Ergebnisse verschiedener Studien, dass kleinere Unternehmen weniger von Cyberangriffen betroffen sind als größere Unternehmen (BSI, 2019; Dreißigacker et al., 2020; Paoli et al., 2018b). Allerdings kommt es bei kleinen Unternehmen mit einer größeren Wahrscheinlichkeit zu einem Schaden, *sofern* diese von einem Cyberangriff betroffen sind (Dreißigacker et al., 2020). Das lässt sich vermutlich auf die schlechtere IT-Sicherheitsausstattung in Kleinstunternehmen zurückführen. Die entsprechende Schadenshöhe fällt dann jedoch geringer aus als für große Unternehmen (Dreißigacker et al., 2020). Wenn man beispielsweise davon ausgeht, dass von den ca. 3,1 Mio. registrierten Kleinst-Unternehmen unter 10 Beschäftigten nur etwa jedes fünfte[55] im Jahr von einem Cyberangriff betroffen ist und davon wiederum etwa 80 Prozent[56] einen Schaden erleiden, der im Durchschnitt bei ca. 1.000 Euro[57] liegt, ergibt das in der Schätzung einen zusätzlichen Gesamtschaden von **rund 500 Mio. Euro** für die kleinste Unternehmensklasse.

Auch wenn diese Rechnung lediglich beispielhaft ist und nicht ausreichend Evidenz für die Unternehmensklasse vorliegt, ist es nicht unwahrscheinlich, dass eine Schadenssumme in dieser Größenordnung noch zusätzlich anfallen könnte. Außerdem ist hier noch darauf hinzuweisen, dass kleine Unternehmen zwar *absolut* den finanziell geringsten Schaden erleiden, sie *relativ* jedoch die höchsten

[54] Basierend auf den Schätzungen anhand der Jahresprävalenzen.
[55] Der Wert orientiert sich an dem von Dreißigacker et al. (2020) berichteten Anteil betroffener Unternehmen von 39,4 % bei einer Beschäftigtengröße von 10 bis 249. Da Kleinstunternehmen in der Regel noch seltener betroffen sind (siehe BSI, 2019; Dreißigacker et al., 2020; Paoli et al., 2018b) und wir von einer eher konservativen Schätzung statt einer zu liberalen Schätzung ausgehen möchten, wird hier eine Betroffenheitsrate von 20 % angenommen.
[56] Auch dieser Wert orientiert sich an den von Dreißigacker et al. (2020) berichteten empirischen Daten. Der Schadensanteil für Unternehmen mit einer Beschäftigtengröße von 10 bis 249 lag bei 72,3 % (siehe Tabelle 1). Da Kleinstunternehmen voraussichtlich noch häufiger von einem Schaden betroffen sein sollten, da sie im Vergleich zu größeren Unternehmen in der Regel über weniger Präventionsmaßnahmen verfügen (siehe GDV, 2018), wird in der Schätzung von einem etwas höheren Schadensanteil (80 %) ausgegangen.
[57] Zur durchschnittlichen Kostenhöhe bei Kleinstunternehmen liegen bislang keine Daten vor. Bekannt ist jedoch, dass kleine Unternehmen *absolut* betrachtet von geringeren Kosten betroffen sind als größere Unternehmen (siehe Hiscox, 2021). Zum Zwecke einer konservativen Schätzung wird daher in diesem Beispiel von einem (verhältnismäßig) niedrigen Durchschnittschaden ausgegangen, auch wenn dieser *relativ* betrachtet im Verhältnis zum deutlichen geringeren Umsatz von Kleinstunternehmen ebenfalls von einiger Bedeutung sein dürfte.

Kosten tragen, in Anbetracht ihres deutlich geringeren Umsatzes (Hiscox, 2021). Daher sind auch diese Kosten gegenüber Kleinstunternehmen bezüglich ihres Schadenspotentials nicht zu vernachlässigen. Auf jeden Fall ist davon auszugehen, dass die oben dargestellten 1,9 Mrd. Euro Gesamtschaden für Unternehmen ab 10 Beschäftigten *nicht* als abschließende Schadenssumme für Unternehmen in Deutschland zu betrachten sind. Vielmehr handelt es sich um eine Art Untergrenze, die anhand der Daten der KFN-Studie empirisch fundiert ist. Es gelten jedoch weiterhin die Einschränkungen, dass es sich bei den Kosten (1) nur um die Kosten für den schwerwiegendsten Cyberangriff handelt und weitere Schäden (durch weitere Cyberangriffe im gleichen Jahr) nicht miterhoben wurden sowie (2) dass die numerisch größte Unternehmensklasse mit weniger als 10 Beschäftigten nicht in die Analysen miteinbezogen wurde.

Im Vergleich zu den anfangs berichteten Angaben durch Bitkom e.V. (2020) und Hiscox (2021) liegt die hier dargestellte Schätzung im mittleren Bereich. Geht man von einem Minimalschaden von ca. 1,9 Mrd. Euro aus, liegt diese Schätzung ca. um ein vierzigfaches höher als die Schätzung durch Hiscox (50 Mio. USD), wobei die Schätzung durch Bitkom wiederum um ein fünfzigfaches höher liegt (ca. 100 Mrd. Euro).

3.2.3 Kosten als Reaktion auf die Straftat

Angaben zu Kosten, die im Nachgang der Straftat und damit im Rahmen von Ersatzmaßnahmen, Ermittlungen oder Rechtsstreitigkeiten entstehen, gibt es in der Literatur kaum. Und wenn, dann werden diese häufig – wie bei Dreißigacker et al. (2020) – gemeinsam mit den allgemeinen Kostenpositionen im Rahmen des Angriffs erfasst. In der KFN-Studie wurden beispielsweise die Kosten für Wiederherstellung und Wiederbeschaffung erfasst und mit durchschnittlich 13.100 Euro je schwerwiegendstem Angriff beziffert (Dreißigacker et al., 2020). Diese Kostenposition ist jedoch bereits im gesamtheitlich errechneten Durchschnittsschaden unter 3.2.2 enthalten und stellt knapp 78 % des durchschnittlichen Gesamtschadens dar. Kosten, die durch Ermittlungen oder Rechtsstreitigkeiten entstehen, wurden im Rahmen der Studie nicht erfasst.
In der Bitkom-Studie (2020) wiederum wurden die „Kosten für Ermittlungen und Ersatzmaßnahmen“ sowie die „Kosten für Rechtsstreitigkeiten“ separat erfasst und insgesamt mit 36,5 Mrd. Euro für ersteres und mit 31,2 Mrd. Euro für letzteres beziffert, bezogen auf den Erhebungszeitraum von zwei Jahren. Damit liegen die Kosten für diese Positionen deutlich höher als die übrigen, erfassten Kostenpositionen im Rahmen der Studie. Auch in der KPMG-Studie (2019) wird berichtet, dass Ermittlungs- und Folgekosten etwa ein Drittel des Gesamtschadens ausmachten und damit eine hohe Kostenposition darstellen. Da in der Studie jedoch keine Durchschnittswerte berichtet werden, kann hierzu keine absolute Schätzung vorgenommen werden.
Im Allgemeinen geben diese Angaben dennoch Auskunft darüber, dass die Kosten, die als Reaktion auf die Straftat entstehen, vermutlich auch von erheblicher Bedeutung sind. Leider liegen hierzu bislang nicht genügend empirische Erkenntnisse vor, um eine konkretere Aussage zuzulassen.

Finanziell messbare Schäden (Kosten)

	Präventionskosten	Kosten als direkte Konsequenz der Straftat	Kosten als Reaktion auf die Straftat
Unternehmen	Mind. 87 Mrd. Euro Personal Mind. 1,4 Mrd. Euro IT-Sicherheitstechnik	Mind. 1,9 Mrd. – 2,65 Mrd. Euro Mind. 500 Mio.	Ca. 30 – 80 % der Gesamtkosten

Summe hier: mind. 88,4 Mrd. Euro durch Präventionskosten, mind. 2,4 Mrd. Euro als direkte Konsequenz der Straftat.

3.3 Staat und Gesellschaft

Empirische Daten, die die Kosten für Staat und Gesellschaft durch Cyber-Kriminalität erfassen, liegen in Deutschland nicht vor. Es ist daher besonders schwierig, valide Daten zur Kostenschätzung zu finden.
In Bezug auf Präventionskosten lässt sich darauf hinweisen, dass der Bund Institutionen wie das „Bundesamt für Sicherheit in der Informationstechnik" (BSI) sowie die 2020 neu eingerichtete „Agentur für Innovation in der Cybersicherheit" (Cyberagentur) finanziert. Das BSI verfügt aktuell über 1.441 Mitarbeitende[58] (Informatiker, Physiker, Mathematiker und andere Mitarbeitende), die Cyberagentur über 53 Mitarbeitende[59], langfristiges Ziel ist jedoch ein Aufwuchs auf 100 Mitarbeitende. Es ist somit davon auszugehen, dass allein die laufenden Kosten dieser Institutionen auf eine beträchtliche Summe hinauslaufen. Im Bundeshaushalt 2022 ist beispielsweise festgehalten, dass sich die Gesamtausgaben durch das BSI auf rund 217 Mio. Euro belaufen sollen (Bundesamt für Finanzen, 2022). Theoretisch wäre es auch eine Möglichkeit, die Ausgaben für Cybersicherheit in den einzelnen Bundes- und Landesministerien anhand der Bundes- sowie Landeshaushalte, die jährlich offengelegt werden müssen, nachzuvollziehen. Allerdings wäre eine derartige Analyse extrem zeitaufwändig und komplex, da jedes einzelne Ministerium über diverse Kostentitel verfügt, die sich nur sehr selten eindeutig dem Bereich „Cybersicherheit" zuordnen lassen.

Zu den Präventionskosten zählen weiterhin auch staatliche Ausgaben für Forschungsprogramme im Bereich der Cybersicherheit. Das BMBF[60] macht in seinem Bericht „Forschung in Zahlen" aus dem Jahr 2021 zwar transparent, welche Gelder in verschiedene Forschungsschwerpunkte investiert werden (z. B. in Informations- und Kommunikationstechnologien sowie in die zivile Sicherheitsforschung), allerdings werden keine konkreten Angaben für den Bereich der Cyber-Sicherheitsforschung gemacht (BMBF, 2021). Es fließen zusätzlich auch Gelder in Kriminalpräventionsprogramme, wie z. B. in das „Programm Polizeiliche Kriminalprävention" (ProPK), die zum Teil wiederum in Präventionsmaßnahmen für Cyber-Kriminalität investiert werden. Beispielsweise ist das aktuelle Schwerpunktthema der Projektgruppe Mediensicherheit „Messenger-Betrug". Allerdings liegen auch hier keine Daten zu konkreten Ausgaben im Phänomenbereich vor.

Empirische Daten zu Kosten, die durch die konkrete Zerstörung staatlicher Infrastrukturen entstehen, liegen bislang ebenfalls nicht vor. Erkenntnisse, die vorliegen, basieren in der Regel auf anekdotischen

[58] Siehe https://www.bsi.bund.de/DE/Das-BSI/Organisation-und-Aufbau/Abteilungen-inkl-Organigramm/abteilungen-inkl-organigramm.html#:~:text=Das%20BSI%20ist%20eine%20unabh%C3%A4ngige,Mathematiker%20und%20andere%20Mitarbeiter%20besch%C3%A4ftigt, abgerufen am 08.02.2023
[59] Siehe https://www.faz.net/aktuell/wirtschaft/cyberagentur-sucht-weiter-mitarbeiter-18572894.html, abgerufen am 08.02.2023
[60] Bundesministerium für Bildung und Forschung

Medienberichten, die keine wissenschaftlich validen Aussagen im Hinblick auf konkrete entstandene Kosten ermöglichen. Berichtet wird in der Regel von erheblichen Arbeitsausfällen und einem hohen Zeitaufwand zur Wiederherstellung der Systeme, was dazu führen kann, dass betroffene Einrichtungen über eine längere Zeit nur eingeschränkt oder kaum funktionsfähig sind (Von Westernhagen, 2019; Wölbert, 2020). Erkenntnisse zu konkreten finanziellen Schäden liegen jedoch nicht vor.

Auch Kosten, die durch polizeiliche Ermittlungen, Gerichtsverhandlungen oder Inhaftierungen entstehen, sind nicht ohne Weiteres zu schätzen, da auch hier eine valide Datengrundlage fehlt. Zwar ist davon auszugehen, dass die entsprechenden staatlichen Kosten immer weiter ansteigen, da die Zahlen in der polizeilichen Kriminalstatistik (Bundeskriminalamt, 2022c) zeigen, dass die Anzahl von zur Anzeige gebrachten Cyber-Delikten über die letzten Jahre stark gestiegen ist und Experten sowie Expertinnen davon ausgehen, dass sich dieser Trend auch weiter fortsetzen wird (Rüdiger, 2021). Es liegen jedoch keine Daten dazu vor, wie hoch die Kosten sind, die durch Ermittlungen in einem Cyber-Fall entstehen. Ebenso liegen keine Daten zu den Kosten durch Gerichtsverhandlungen oder Inhaftierungen vor.

4 Empirische Daten zu weiteren Schäden

Zusätzlich zu Kosten, die durch Cyber-Delikte entstehen, können auch Schäden auftreten, die nicht finanziell messbar sind und daher nicht in Geldwerten erfasst werden können (siehe 2.2.2). Im folgenden Gliederungspunkt werden daher bisherige Erkenntnisse aus Dunkelfeldstudien und internationaler, wissenschaftlicher Literatur zusammengetragen, die Aufschluss darüber geben, welche weiteren, nicht-finanziellen Schäden auf Personen-, Unternehmens- und auf staatlicher Ebene durch Cyber-Angriffe entstehen können. Da es bisher kaum quantitative, empirische Daten zu den weiteren Schäden durch Cyber-Kriminalität gibt, wird vor allem auf qualitative Studien sowie auf exemplarische Berichte aus der Medienberichterstattung zurückgegriffen.

4.1 Privatpersonen

Das Modell umfasst nicht-finanzielle Schäden durch Cybercrime auf Personenebene zunächst hinsichtlich der Präventionsbemühungen. Hierunter ist Vermeidungsverhalten zu verstehen, z. B. im Sinne eines Verzichts auf verschiedene Online-Dienste, die Prozesse beschleunigen oder erleichtern können, aber aufgrund der Angst vor einer Opferwerdung nicht mehr genutzt werden.
Auf die Frage, wie sie sich im Internet vor Gefahren schützen, gaben im Digitalbarometer 2022 9 % der Personen an, auf soziale Medien, 9 % auf Online-Banking und 5 % auf Online-Shopping zu verzichten (siehe Abbildung unter 3.1.1) (Van Nek & Bolz, 2022). 26 % gaben außerdem an, regelmäßige Sicherheitskopien anzulegen, was zumindest mit einem gewissen zeitlichen Aufwand einhergehen kann (Van Nek & Bolz, 2022).

Nicht-finanzielle Schäden in direkter Konsequenz der Cyber-Straftat können sowohl auf psychischer, physischer als auch auf Verhaltensebene auftreten, wobei sich diese Ebenen überschneiden können (Borwell et al., 2021). In einer niederländischen Studie von Jansen und Leukfeldt (2018) wurden qualitative Interviews mit Personen durchgeführt, die Opfer von Phishing- oder Malware Angriffen auf ihren Online-Banking-Account geworden sind. Viele Opfer berichteten von negativen emotionalen Auswirkungen, wie z. B. einem verminderten Selbstwertgefühl („sich dumm fühlen“), Stress und Angst. Sie gaben außerdem an, dass das Vertrauen in Banken und das Online-Banking, aber auch generell in Menschen und in sich selbst durch den Vorfall beeinträchtigt wurde (Jansen & Leukfeldt, 2018). Zum Teil wurden auch körperliche Auswirkungen wie Schlaflosigkeit, Herzklopfen, Ohnmachtsanfälle und Zittern bei der erneuten Nutzung von Online-Banking berichtet (Jansen & Leukfeldt, 2018). Es gab jedoch auch Personen, die von keinen psychischen Konsequenzen berichteten. Von Bedeutung ist hier allerdings, dass ein Großteil der Personen, die durch den Vorfall einen erheblichen finanziellen Schaden erlitten hatten, Kompensationszahlungen ihrer Bank erhalten haben, was die negativen psychischen/physischen Auswirkungen in der Regel minderte (Jansen & Leukfeldt, 2018).
In einer australischen Studie von Cross et al. (2016) wurden hingegen nur Personen befragt, die Opfer eines Online-Betrugs geworden waren, bei dem sie einen finanziellen Schaden von mindestens 10.000 $ erlitten hatten. Die berichteten psychologischen und körperlichen Konsequenzen der Geschädigten waren in der Studie entsprechend stärker ausgeprägt: Viele berichteten von starken Scham- und Schuldgefühlen, sowie von Gefühlen wie Verzweiflung, Traurigkeit und Wut (Cross et al., 2016). Auf körperlicher Ebene wurden Auswirkungen wie Schlaflosigkeit, Übelkeit und Gewichtsverlust berichtet (Cross et al., 2016).

Schäden, die im Nachgang, als Reaktion auf die Straftat entstehen, sind in der Regel zeitlicher Natur. Solche Schäden wurden im Digitalbarometer (2021) von 29 % der betroffenen Personen, die einen Schaden erlitten haben, berichtet. Ein zeitlicher Schaden entsteht durch die weitere Abwicklung des

Vorfalls, die zeitliche Ressourcen der Betroffenen in Anspruch nimmt. In der Studie von Jansen und Leukfeldt (2018) wurden beispielsweise zeitliche Verluste durch die Meldung des Online-Banking Vorfalls bei der Bank und der Polizei sowie durch ein gesperrtes Bankkonto und somit fehlende Verfügbarkeit des eigenen Geldes berichtet.

Leider existieren jedoch bislang nur wenige wissenschaftliche Studien, die die Auswirkungen und Konsequenzen einer Viktimisierung durch Cyber-Kriminalität untersucht haben. Auch Borwell et al. (2021, S. 95) weisen in einem aktuellen Literatur-Review darauf hin, dass Cyber-Kriminalität zwar derzeit als wichtiges Forschungsfeld anerkannt ist, aber eine „fundierte, nuancierte Sichtweise auf die Auswirkungen der Cyber-Kriminalität fehlt". Insbesondere fehlt es an quantitativen Studien, die einen Überblick über verschiedene Viktimisierungsarten ermöglichen; vorhandene Studien basieren in der Regel auf qualitativen Daten und konzentrieren sich auf eine oder wenige, spezifische Arten von Cyberkriminalität, die keine Übertragbarkeit der Ergebnisse ermöglichen (Borwell et al., 2021).

4.2 Unternehmen

Auch auf Unternehmensebene können nicht bezifferbare Schäden durch Präventionsbemühungen entstehen, z B. wenn auf Digitalisierungsschritte verzichtet wird. Ein solcher Digitalisierungsverzicht kann auch erhebliche Konsequenzen haben: So gibt es Unternehmen, die Insolvenz anmelden mussten, weil sie es verpasst haben, ihr Angebot um digitale Alternativen zu erweitern. Ein bekanntes Beispiel hierfür ist die Insolvenz der Firma Kodak (SPIEGEL, 2012). Auch im Manager Magazin wurde bereits 2015 beklagt, dass die „Risikoaversion der Deutschen" ein „Fortschrittskiller" sei und Gefahren wie „Datendiebstahl, Cyberkriminalität und Hackerangriffe hierzulande die Digitaldebatten beherrschen" (Müller, 2015). Und auch Expertinnen und Experten im Bereich Digitalisierung im Gesundheitswesen warnen immer wieder davor, dass „das Potenzial der Digitalisierung nicht ausgeschöpft wird" (Cornelsen, 2018).

Weitere Schäden, die Unternehmen als direkte Konsequenz oder als Reaktion auf die Cyber-Straftat betreffen können, sind Image-Schäden und damit verknüpft ein Verlust von Kundschaft und eine Minderung des Unternehmenswertes. Laut Dreißigacker et al. (2020, S. 140) sind derartige, „indirekte Kosten", die durch „Reputationsschäden, Auftragsausfälle oder Wettbewerbsnachteile" entstehen „kaum realistisch [...] zu beziffern", da sie zeitlich stark versetzt vom Cyberangriff auftreten können. Auch in der belgischen Studie von Paoli et al. (2018b) wurden Schäden wie Reputationsverluste von Unternehmen als nicht quantifizierbar bewertet. Die Autorinnen und Autoren erkennen zwar an, dass es monetäre Indikatoren für die Image-Schäden eines Unternehmens geben kann (z. B. den Börsenkurs), aber sie argumentieren, dass diese Daten einerseits nicht für alle Unternehmen verfügbar sind und es andererseits nicht möglich ist, die Auswirkungen eines einzelnen Cyber-Angriffs auf sie zu schätzen (Paoli et al., 2018b). Daher ließen die Autorinnen und Autoren die Schwere der nichtmateriellen Schäden für verschiedene Cyber-Angriffsarten[61] in ihrer Studie anhand einer sechsstufigen Skala bewerten (Paoli et al., 2018b). Reputationsschäden wurden in 7 % bis 9 % der Fälle als ernst, schwer oder sogar katastrophal eingeschätzt. Ein Großteil der befragten Unternehmen gab aber auch an, dass keine Reputationsschäden durch Cyber-Vorfälle entstanden sind (48 % bis 58 %). Die Ergebnisse deuten folglich darauf hin, dass eine Vielzahl betroffener Unternehmen keine Image-Schäden erleidet, was möglicherweise auch damit zusammenhängt, dass Cyber-Angriffe gegen Unternehmen nur selten und vermutlich eher bei Großunternehmen medial bekannt werden (Paoli et al., 2018b). Nur in wenigen Fällen wurden schwere Image-Schäden berichtet.
In einer Befragung des GDV (2018) gaben wiederum 14 % der Unternehmen an, wirtschaftliche Schäden durch Reputationsschäden, 11 % durch den Diebstahl von Kundendaten und 8 % durch den

[61] Erfasst wurden in der Studie Cyber-Vorfälle wie der Illegale Zugriff auf Daten/Informationen, eine Daten-/Systemstörung, Ransomware, Cyber-Spionage und Betrugsfälle.

Diebstahl von eigenen Daten/Betriebsgeheimnissen erlitten zu haben. In der Bitkom-Studie zu Datendiebstahl, Industriespionage oder Sabotage wurden die Unternehmen sogar zu einer Schätzung der Kosten durch Imageschäden und Umsatzeinbußen befragt: Die berechnete Summe der Kosten durch Imageschaden bei Kunden oder Lieferanten sowie durch negative Berichterstattung lag bei 18,6 Mrd. Euro, die Kosten durch Umsatzeinbußen bei insgesamt 44,4 Mrd. Euro[62] (Bitkom e.V., 2020). Damit lagen die Kosten, die durch Imageschäden und Umsatzeinbußen entstanden, bei etwa 30 % der insgesamt entstanden Gesamtkosten (= 205,7 Mrd. Euro). Wie unter 3.2 bereits erläutert wurde, sind die hier berechneten Kosten aufgrund der Methodik der Studie jedoch mit Vorsicht zu interpretieren.[63]

Der hier vorgelegte Bericht folgt der Bewertung anderer Wissenschaftlerinnen und Wissenschaftler (Dreißigacker et al., 2020; Paoli et al., 2018b) und unterlässt es, eine Schätzung der Kosten für Image-Schäden und ihre Konsequenzen (Verlust von Kundschaft, Marktwerten) vorzunehmen. Es sei allerdings darauf hingewiesen, dass empirische Erkenntnisse darauf hindeuten, dass Imageschäden – sofern sie auftreten – einen erheblichen weiteren, finanziellen Schaden mit sich ziehen können.

4.3 Staat und Gesellschaft

Analog zu den Schäden für Unternehmen, die durch Präventionsbemühungen entstehen können, kann auch für staatliche Institutionen ein Verzicht auf den Einsatz digitalisierter Infrastrukturkomponenten, denen eine höhere Angreifbarkeit durch Cyberkriminalität zugeschrieben wird, zu Verlusten führen. Ein Beispiel hierfür ist die bislang nur geringe Digitalisierung der öffentlichen Verwaltung (Welchering, 2021), deren Realisierung für den einzelnen Bürger und die einzelne Bürgerin eine deutliche Erleichterung des Alltags bedeuten könnte.

Schäden, die auf staatlicher Ebene als direkte Konsequenz einer Cyber-Straftat auftreten können, betreffen in erster Linie das erzwungene Aussetzen staatlichen Handelns, wenn Systeme z. B. aufgrund von Schädigungen durch Schadsoftware nicht mehr nutzbar sind. In der jüngeren Vergangenheit finden sich viele Beispiel für solche Situationen: Allein die Schadsoftware Emotet schädigte in der Vergangenheit diverse Verwaltungen, Behörden und Universitäten und schränkte so die Handlungsmöglichkeiten der Institutionen sehr stark ein (Wölbert, 2020). Beispielhaft sei die Stadtverwaltung Neustadt aufgeführt, deren Systeme mindestens eine Woche vom Netz genommen werden mussten (von Westernhagen, 2019). Als Konsequenz blieb in dieser Zeit die Zulassungsstelle für Kraftfahrzeuge geschlossen und auch Reisepässe sowie Personalausweise konnten von den Bürgerinnen und Bürgern nicht beantragt werden (von Westernhagen, 2019). Auch Zahlungen, wie z. B. des Elterngeldes, konnten nicht mehr erfolgen (Wölbert, 2020). Daher mussten viele Familien vorerst auf einen Teil ihres Einkommens verzichten (Wölbert, 2020).
Derartige Einschränkungen der staatlichen Handlungsfähigkeit können längerfristig auch zur Folge haben, dass das Vertrauen der Bevölkerung in die Sicherheit staatlicher Institutionen sinkt. Aus aktuellen Dunkelfeldstudien ist bekannt, dass nur etwa 18 % der Cyber-Vorfälle zur Anzeige gebracht werden (Birkel et al., 2022). Besonders niedrig ist die Anzeigequote bei Cyber-Delikten im engeren Sinne, d. h. bei Opferwerdung durch Missbrauch persönlicher Daten bei Nutzung des Internets (15,7 %) und einer Infizierung mit Computerviren (11,6 %) (Birkel et al., 2022). Ein Großteil der Cyber-Straftaten wird folglich nicht zur Anzeige gebracht und bleibt im Dunkelfeld. Als Gründe gegen eine Anzeige wurde von den befragten Personen häufig genannt, „die Polizei hätte [den] Fall nicht aufklären können“ (Birkel et al., 2022, S. 201). 39,9 % der Betroffenen durch Computerviren und sogar 43,8 % der

[62] 22,2 Mrd. Euro Umsatzeinbußen durch nachgemachte Produkte (Plagiate) sowie 22,2 Mrd. Euro Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen
[63] Darüber hinaus sei hier auch darauf hingewiesen, dass ebenfalls nicht nachvollzogen werden kann, auf welcher Basis die durch Imageschäden errechneten Kosten zustande kommen.

Betroffenen von persönlichem Datenmissbrauch gaben dies als Grund gegen eine Anzeige an (Birkel et al., 2022). Die Ergebnisse zeigen, dass fast jede/r zweite Betroffene kein Vertrauen in die Strafverfolgungskompetenz bei Cyber-Delikten hat und die Straftaten daher nicht zur Anzeige bringt.

5 Zusammenfassung und Fazit

Ziel des vorliegenden Berichts war es, ein Modell zu entwickeln, das eine Schätzung der Kosten und Schäden durch Cyber-Kriminalität ermöglicht. Das unter 2.3 dargestellte Modell unterscheidet zunächst grundsätzlich zwischen finanziell messbaren Kosten und weiteren, finanziell nicht messbaren oder nicht schätzbaren Schäden. Die Kosten bzw. Schäden werden separat für die Ebenen der Betroffenen (Privatpersonen, Unternehmen, Staat), sowie anhand des auftretenden Zeitpunktes (durch Antizipation der Straftat, als direkte Konsequenz der Straftat, oder als Reaktion auf die Straftat) betrachtet. Anschließend wurde versucht, empirische Daten anhand bisheriger Studien zusammenzutragen, die eine Einschätzung der Kosten und weiteren Schäden in Anlehnung an das dargestellte Modell ermöglichen.

Für den Themenbereich „Kosten und Schäden durch Cyber-Kriminalität" gibt es in Deutschland bislang zwar nur wenige, empirisch fundierte Studien, die zuverlässige Aussagen über die Kosten und Schäden von Privatpersonen, Unternehmen und Staat erlauben. Das liegt nicht zuletzt an der immensen Komplexität des Themas und den damit verknüpften methodischen Herausforderungen. Im hier vorgelegten Bericht wurde dennoch versucht, auf Basis verschiedener, empirischer Daten eine Schätzung der Kosten und Schäden durch Cyber-Kriminalität vorzunehmen.

Für die Ebene der Privatpersonen werden die Kosten durch Antizipation der Straftat auf 259 Mio. Euro jährlich für Abonnements von Antiviren-Programmen sowie auf zusätzliche rund 675 Mio. Euro für Einmalzahlungen über mehrere Jahre geschätzt. Die Kosten als direkte Konsequenz der Straftat können je nach herangezogener Datengrundlage auf ca. 700 Mio. Euro[64] oder grob auf einen Bereich zwischen 56 Mio. und 5,6 Mrd. Euro[65] jährlich eingegrenzt werden. Zu den Kosten als nachgelagerte Reaktion auf die Straftat liegen für Privatpersonen keine Daten vor, sie werden aber auch als eher vernachlässigbar eingeschätzt.

Auf Unternehmensebene werden die Antizipationskosten bzw. Präventionskosten auf insgesamt etwa 89,3 Mrd. Euro geschätzt, wobei in dieser Schätzung die mit Abstand größte Kostenposition durch die geschätzten Personalausgaben von Unternehmen (~ 87 Mrd. Euro) zustande kommt. Geschätzt wird außerdem, dass Kosten von mindestens 1,4 Mrd. Euro durch Ausgaben für IT-Sicherheitstechnik hinzukommen. Bezüglich weiterer Ausgaben, die durch Cyber-Versicherungen oder Mitarbeitenden-Schulungen entstehen, liegen bislang keine empirischen Daten vor. Unternehmenskosten, die als direkte Konsequenz der Straftat entstehen, wurden auf Basis der Studie von Dreißigacker et al. (2020) auf mindestens 1,9 Mrd. – 2,65 Mrd. Euro für Unternehmen mit mehr als 10 Beschäftigten geschätzt. Außerdem wird angenommen, dass für Kleinstunternehmen mit maximal zehn Mitarbeitenden ebenfalls noch Kosten von mindestens 500 Mio. Euro hinzukommen. Kosten, die als nachgelagerte Reaktion auf einen Cyber-Angriff entstehen, werden in der Regel nicht separat, sondern gemeinsam mit den Gesamtkosten infolge eines Angriffs erfasst. Es wird jedoch geschätzt, dass diese Kosten einen erheblichen Anteil von etwa 30 bis 80 Prozent an den Gesamtkosten für Unternehmen haben.
Für die Ebene Staat und Gesellschaft liegen bislang die wenigsten empirischen Daten vor, sodass eine Schätzung der Kosten hier nicht möglich erschien.

Im Ergebnis hieße das, dass man für das Jahr 2022 auf **direkte oder nachgelagerte Kosten in Höhe von 3,1 bis 3,7 Mrd. Euro für Privatpersonen und Unternehmen** kommt, wobei man davon ausgehen kann, dass es sich hierbei um eine eher konservative Schätzung handelt und die tatsächlichen Kosten

[64] Grundlage für die Schätzung stellt die erfasste Schadenssumme in der PKS sowie die Anzeigequote bei Cyber-Delikten dar (siehe Birkel et al., 2022).
[65] Auf Basis des „Digitalbarometers" (Van Nek & Bolz, 2021).

wahrscheinlich noch höher ausfallen könnten. Kosten, die durch Präventionsbemühungen entstehen, werden mit insgesamt rund 90 Mrd. Euro sogar noch um ein Vielfaches höher geschätzt als Kosten, die als direkte Konsequenz oder als Reaktion auf die Straftat entstehen. Dieses Ergebnis steht in Einklang mit früheren empirischen Erkenntnissen (Hillebrand et al., 2018). Nichtsdestotrotz ist gleichzeitig davon auszugehen, dass die durch Cyber-Kriminalität entstehenden Kosten und die weiteren, nicht-finanziellen Schäden entsprechend höher ausfallen würden, wenn es keine oder weniger Präventionsmaßnahmen gäbe.

Im Bericht werden darüber hinaus auch weitere, nicht finanziell messbare bzw. nicht schätzbare Schäden durch Cyber-Kriminalität skizziert, die ebenfalls von erheblicher Bedeutung sein können. Auf individueller Ebene kann es beispielsweise zu psychischen sowie physischen Leiden der Betroffenen kommen sowie zu einem erheblichen Zeitaufwand und Stress, z. B. durch einen vorübergehend fehlenden Zugriff auf das persönliche Online-Banking. Auch auf Unternehmensebene können erhebliche Schäden, z.B. durch einen Image-Verlust und in der Konsequenz durch einen Verlust von Kundschaft und eine Minderung des Unternehmenswertes entstehen (Paoli et al., 2018a). Diese Schäden können auch erhebliche, nachgelagerte finanzielle Auswirkungen auf ein Unternehmen haben, die sich jedoch kaum valide in ihrem Ausmaß schätzen lassen.
Auf staatlicher Ebene können Cyber-Angriffe dazu führen, dass staatliches Handeln eingeschränkt wird und letztlich Bürgerinnen und Bürger das Vertrauen in staatliche Institutionen verlieren. Diese Schäden lassen sich zwar nicht in Geldwerten erfassen, sie können aber auch von erheblicher Bedeutung sein, z. B. wenn Cyber-Delikte aufgrund von fehlendem Vertrauen in die Strafverfolgungskompetenz nicht zur Anzeige gebracht werden.

Zukünftiger Forschungsbedarf liegt folglich vor allem in der Erfassung von Kosten und Schäden staatlicher Einrichtungen, da es hierzu bislang noch keine empirische Untersuchung für Deutschland gibt. Möchte man dazu valide Daten erhalten, wäre es sinnvoll, eine Studie mit Vertreterinnen und Vertretern staatlicher Institutionen durchzuführen und diese zu ihrer Betroffenheit zu befragen. Allerdings ist eine derartige Befragung oftmals mit besonderen Hürden wie beispielsweise einer fehlenden Aussagebereitschaft verknüpft (siehe Paoli et al., 2018a).

Der vorliegende Bericht weist natürlich auch einige Limitationen auf. Viele der in Gliederungspunkt 3 exemplarischen Berechnungen haben deutliche Schwächen, auf die entsprechend hingewiesen wurde. Die vorgenommenen Hochrechnungen können und sollten daher nur als grobe Schätzwerte für die Kosten und Schäden durch Cyber-Kriminalität verstanden werden. Für eine tatsächlich valide Schätzung der gesamtheitlichen Kosten und Schäden durch Cyber-Kriminalität bedarf es weiterer, umfassender Studien. Darüber hinaus wurde versucht, Cybercrime im engeren Sinne (CCieS) in den Fokus zu nehmen und Cybercrime im weiteren Sinne (CCiwS) nicht in die Schätzungen miteinzubeziehen. Das konnte zum Teil jedoch nicht umgesetzt werden, da Delikte aus den Bereichen CCieS und CCiwS oft gemeinsam erhoben und analysiert werden und eine nachträgliche Trennung anhand der berichteten Daten oft nicht möglich war. Gleichzeitig ist davon auszugehen, dass man insbesondere für die Ebene der Privatpersonen die Kosten durch Cyber-Kriminalität unterschätzt, wenn man CCiwS ausklammert, da auf dieser Ebene insbesondere viele Kosten durch Online-Betrugsdelikte entstehen können (siehe Onemichl & Borz, 2021). Insofern lässt sich auch grundsätzlich infrage stellen, inwieweit ein Ausklammern von CCiwS auf Privatpersonenebene überhaupt wünschenswert ist.
Auch das unter 2.3 vorgestellte Modell verfügt über Schwächen, insbesondere im Hinblick auf die dritte Ebene von Staat und Gesellschaft. Hier ließe sich argumentieren, dass diese Ebene auch geteilt werden könnte in die Ebenen „öffentlicher Sektor“ (zur Betrachtung der Kosten und Schäden von öffentlichen Einrichtungen und Institutionen) und der gesamtstaatlichen, nationalökonomischen Perspektive, in der der gesamte Wirtschaftskreislauf des Staates betrachtet werden könnte. Eine derartige Trennung überstieg den Anspruch dieses Berichts, wäre aber in zukünftigen Studien erwägenswert.

Letztendlich wäre es notwendig, regelmäßige, repräsentative Erhebungen von Privatpersonen, Unternehmen und staatlichen Institutionen durchzuführen, um wirklich valide und aktualisierte Daten zu Kosten und Schäden durch Cyber-Kriminalität zu erhalten, die gleichzeitig ein Abbilden von Entwicklungen ermöglichen. Derartige, regelmäßige Erhebungen wären mit einem erheblichen Kosten- und Ressourcenaufwand verbunden. Sie wären jedoch notwendig, wenn man konkrete Erkenntnisse für Lagebeurteilungen erhalten oder langfristige Entwicklungen im Phänomenbereich verfolgen möchte. Aufgrund der immensen Komplexität des Themas könnte es zunächst ein Ansatz sein, sich spezifische, einzelne Delikte mit großem Schadenspotential (wie z.B. Ransomware, DDOS-Attacken, Malware) auf Unternehmensebene vorzunehmen und für diese Delikte regelmäßige Erhebungen durchzuführen.

6 Literaturverzeichnis

Accenture Security (2019). The cost of cybercrime: Ninth annual cost of cybercrime study. Ponemon Institute LLC: Michigan.

Agrafiotis, I., Bada, M., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, E., ... & Upton, D. M. (2016). Cyber harm: concepts, taxonomy and measurement. Saïd Business School.

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S. & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity 4(1), 1–15. **https://doi.org/10.1093/cybsec/tyy006**.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J.G., Levi, M., Moore, T. & Savage, S. (2013). Measuring the Cost of Cybercrime. The economics of information security and privacy, 265–300. **https://doi.org/10.1007/978-3-642-39498-0_12**.

Birkel, C., Church, D., Erdmann, A., Hager, A., Leitgöb-Guzy, N. (2022). Sicherheit und Kriminalität in Deutschland – SKiD 2020. Bundesweite Kernbefunde des Viktimisierungssurvey des Bundeskriminalamts und der Polizeien der Länder. Bundeskriminalamt (Hrsg.): Wiesbaden.

Bitkom e.V. (2020). Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der vernetzten Welt. Bitkom e.V.: Berlin. Online abrufbar unter: **https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf** (zuletzt abgerufen am 15.02.2023).

Bitkom (2018). Live Security Studie 2017/2018. Bitkom Research GmbH: Berlin. Online abrufbar unter: **https://www.bitkom-research.de/de/Live-Security-Studie-2017/2018** (zuletzt abgerufen am 15.02.2023).

Borwell, J., Jansen, J., & Stol, W. (2021). Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions. Journal of Digital Social Research, 3(3), 85-110.

Bundesamt für Finanzen (2022). Bundeshaushalt 2022. Online abrufbar unter: **https://www.bundeshaushalt.de/static/daten/2022/soll/BHH%202022%20gesamt.pdf**. (zuletzt abgerufen am 03.03.2022).

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2019). Cyber-Sicherheits-Umfrage – Cyber-Risiken & Schutzmaßnahmen in Unternehmen: Betrachtungszeitraum 2018. Geschäftsstelle der Allianz für Cybersicherheit: Bonn. Online abrufbar unter: **https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/cyber-sicherheits-umfrage_2018.pdf?__blob=publicationFile&v=1** (zuletzt abgerufen am 15.02.2023).

Bundeskriminalamt. (2019). Cybercrime: Bundeslagebild 2018. Bundeskriminalamt: Wiesbaden. Online abrufbar unter: **https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.html?nn=28110** (zuletzt abgerufen am 15.02.2023).

Bundeskriminalamt. (2022a). Cybercrime: Bundeslagebild 2021. Bundeskriminalamt: Wiesbaden. Online abrufbar unter:

https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html?nn=28110 (zuletzt abgerufen am 15.02.2023)

Bundeskriminalamt. (2022b). PKS 2021 – Bund-Falltabellen: T07 Aufgliederung der Straftaten nach Schadenshöhe. Online abrufbar unter: **https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2021/PKSTabellen/BundFalltabellen/bundfalltabellen.html?nn=194208** (zuletzt abgerufen am 13.02.2023).

Bundeskriminalamt. (2022c). PKS 2021 – Zeitreihen: T01 Grundtabelle – Fälle ab 1987. Online abrufbar unter: **https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2021/PKSTabellen/Zeitreihen/zeitreihen_node.html** (zuletzt abgerufen am 13.02.2023).

Bundesministerium für Bildung und Forschung (BMBF) (2021). Bildung und Forschung in Zahlen 2021. BMBF: Rostock. Online abrufbar unter: **https://www.bmbf.de/SharedDocs/Publikationen/de/bmbf/1/31689_Bildung_und_Forschung_in_Zahlen_2021.html** (zuletzt abgerufen am 05.03.2023).

Cornelsen, J. (2018). Patienten und Zahnärzte als Opfer digitaler Skepsis. dwz Online. Online abrufbar unter: **https://dzw.de/prof-dr-david-matusiewicz-patienten-und-zahnaerzte-als-opfer-digitaler-skepsis** (zuletzt abgerufen am 14.02.2023).

Dreißigacker, A., Skarczinski, B. von & Wollinger, G. R. (2020). Cyberangriffe gegen Unternehmen in Deutschland: Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019 (Forschungsbericht Nr. 152). Kriminologisches Forschungsinstitut Niedersachsen e.V: Hannover.

Gesamtverband der Deutschen Versicherungswirtschaft (GDV) e.V. (2018). Cyberrisiken im Mittelstand: Ergebnisse einer Forsa-Befragung. Berlin.

Greenfield, V. A. & Paoli, L. (2013). A framework to assess the harms of crimes. British Journal of Criminology, 53(3), 864–885.

Hillebrand, A., Niederprüm, A., Schäfer, S., Thiele S., & Henseler-Ungar, I. (2018). Aktuelle Lage der IT-Sicherheit in KMU. Bad Honnef. Online abrufbar unter: **https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Redaktion/DE/PDF-Anlagen/Studien/aktuelle-lage-der-it-sicherheit-in-kmu-langfassung.pdf?__blob=publicationFile&v=3** (zuletzt abgerufen am 15.02.2023).

Hiscox. (2021). Hiscox Cyber Readiness Report 2021. Pembroke, Bermuda.

(ISC)² (2022). (ISC)² Cybersecurity Workforce Study 2022. Online abrufbar unter: **https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx**. (zuletzt abgerufen am 01.03.2023).

Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. Journal of Qualitative Criminal Justice and Criminology, 6(2), 205-228.

KPMG AG. (2019). e-Crime in der deutschen Wirtschaft: Computerkriminalität im Blick.

Marwan, P. (2022). Erhebung des Bitkom: So viel zahlen Verbraucher für Virenschutz auf PC, Notebook und Smartphone. ChannelPartner. Online abrufbar unter:

https://www.channelpartner.de/a/so-viel-zahlen-verbraucher-fuer-virenschutz-auf-pc-notebook-und-smartphone,3340580. (zuletzt abgerufen am 01.03.2023).

McAfee. (2018). Economic Impact of Cybercrime - No Slowing Down. Santa Clara, USA.

Müller, E. (2015). Republik der Angsthasen - Risikoscheu als Fortschrittskiller. Manager Magazin Online. Online abrufbar unter: **https://www.manager-magazin.de/magazin/artikel/die-risikoaversion-der-deutschen-wird-zum-fortschrittskiller-a-1055045.html** (zuletzt abgerufen am 13.02.2023).

Onemichl, A., & Bolz, C. (2022). Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit 2022. Bundesamt für Sicherheit in der Informationstechnik (BSI) und Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) (Hrsg.): Bonn. Online abrufbar unter: **https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Leistungen-und-Kooperationen/Digitaler-Verbraucherschutz/Digitalbarometer/digitalbarometer_node.html** (zuletzt abgerufen am 13.02.2023).

Paoli, L., van Hellemont, E., Verstraete, C., Visschers, J., Wolf, R. d., Martens, M., Marez, L. de, Verdegem, P., Teerlinck, E., Chen, P., Huygens, C., Cnudde, T. d., Rijmen, V., Janssens, M.-C. & Marquenie, T. (2018a). Belgian Cost of Cybercrime: Measuring cost and impact of cybercrime in Belgium. Final Report: Brussels. Online abrufbar unter: **https://www.belspo.be/belspo/brain-be/projects/FinalReports/BCC_Final%20Report.pdf** (zuletzt abgerufen am 15.02.2023).

Paoli, L., Visschers, J. & Verstraete, C. (2018b). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. Crime, Law and Social Change, 70(4), 397–420.

Ponemon Institute. (2019). The cost of cybercrime: Ninth annual cost of cybercrime study: Unlocking the value of improved cybersecurity protection. Michigan, USA.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity 2(2), 121–135. **https://doi.org/10.1093/cybsec/tyw001**.

Rüdiger, T.-G. (2021). Digitale Kriminalitätstransparenz: Von der Durchbrechung der "Präventivwirkung des Nichtwissens. Kriminalistik 2/2021, 72–76.

Scherschel, F. A. (2020). 3 Jahre NotPetya: Der Erpressungstrojaner, der keiner war. Heise Online. Online abrufbar unter: **https://www.heise.de/hintergrund/3-Jahre-NotPetya-Der-Erpressungstrojaner-der-keiner-war-4797250.html** (zuletzt abgerufen am 21.02.2023).

SPIEGEL Online (2012). Ende einer Traditionsfirma: Kodak ist pleite. Online abrufbar unter: **https://www.spiegel.de/wirtschaft/unternehmen/ende-einer-traditionsfirma-kodak-ist-pleite-a-809979.html** (zuletzt abgerufen am 14.02.2023).

United States Government Accountability Office (GAO) (2017). Costs of Crime: Experts Report Challenges Estimating Costs and Suggest Improvement to Better Inform Policy Decisions. Online abrufbar unter: **https://www.gao.gov/assets/gao-17-732.pdf** (zuletzt abgerufen am 17.02.2023).

Van Nek, L., & Bolz, C. (2021). Digitalbarometer 2021: Bürgerbefragung zur Cyber-Sicherheit. Bundesamt für Sicherheit in der Informationstechnik (BSI) und Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) (Hrsg.): Bonn. Online abrufbar unter:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Leistungen-und-Kooperationen/Digitaler-Verbraucherschutz/Digitalbarometer/digitalbarometer_node.html (zuletzt abgerufen am 13.02.2023).

Von Westernhagen, O. (2019). Trojaner-Befall: Neue Emotet-Welle legt Neustädter Stadtverwaltung lahm. Heise online. Online abrufbar unter: **https://www.heise.de/security/meldung/Ransomware-Neue-Emotet-Welle-legt-Neustaedter-Stadtverwaltung-lahm-4518819.html** (zuletzt abgerufen am 13.02.2023).

Weber, C. & Wührl, J. M., (2022). Opfererfahrungen im Internet – Ergebnisse des Deutschen Viktimisierungssurvey (DVS). In: Rüdiger, TG., Bayerl, P.S. (eds) Handbuch Cyberkriminologie. Springer VS: Wiesbaden. **https://doi.org/10.1007/978-3-658-35450-3_44-1.**

Wickramasekera, N., Wright, J. & Elsey, H. (2015). Cost of Crime: A Systematic Review. Journal of Criminal Justice 43 (3), 218–228. **https://doi.org/10.1016/j.jcrimjus.2015.04.009**.

Windeck, C. (2017). WannaCry: Gewaltiger Schaden, geringer Erlös. Heise Online. Online abrufbar unter: **https://www.heise.de/security/meldung/WannaCry-Gewaltiger-Schaden-geringer-Erloes-3713689.html** (zuletzt abgerufen am 21.02.2023).

Wölbert, C. (2020). Was Emotet anrichtet – und welche Lehren die Opfer daraus ziehen. Heise Online. Online abrufbar unter: **https://www.heise.de/hintergrund/Was-Emotet-anrichtet-und-welche-Lehren-die-Opfer-daraus-ziehen-4665958.html** (zuletzt abgerufen am 21.02.2023).

Impressum

Herausgeber
Bundeskriminalamt
Kriminalistisches Institut
65173 Wiesbaden

Stand
August 2023 (redaktionelle Überarbeitung März 2024)

Gestaltung & Bildnachweis
Bundeskriminalamt