KRIMINOLOGISCHES
FORSCHUNGSINSTITUT
NIEDERSACHSEN E.V.

Forschungsbericht Nr. 152

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

IT-Sicherheit
IN DER WIRTSCHAFT

Cyberangriffe gegen Unternehmen in Deutschland

Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019

Zusatzförderung durch: pwc VHV STIFTUNG

Arne Dreißigacker, Bennet von Skarczinski, Gina Rosa Wollinger

2020

FORSCHUNGSBERICHT Nr. 152

Cyberangriffe gegen Unternehmen in Deutschland

Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019

Arne Dreißigacker, Bennet von Skarczinski, Gina Rosa Wollinger

2020

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.de abrufbar.

Diese Publikation wurde vom Kriminologischen Forschungsinstitut Niedersachsen e. V. innerhalb des Projektes „Cyberangriffe gegen Unternehmen“ im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie (BMWi) erstellt und ist unter https://kfn.de/publikationen/kfn-forschungsberichte/ eingestellt.

Förderkennzeichen: BMWi-VID5-090168623-01-1/2017

Projektlaufzeit: Dez. 2017 – Nov. 2020

Initiative „IT-Sicherheit in der Wirtschaft“

Die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittelständische Unternehmen beim sicheren Einsatz von IKT-Systemen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter www.it-sicherheit-in-der-wirtschaft.de abrufbar.

ISBN: 978-3-948647-00-1

Druck: DruckTeam Druckgesellschaft mbH, Hannover.

Lützerodestraße 9, 30161 Hannover
Tel. +49 (0)511 34836-0, Fax: +49 (0)511 34836-10
E-Mail: kfn@kfn.de, Internet: www.kfn.de

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

IT-Sicherheit IN DER WIRTSCHAFT

aufgrund eines Beschlusses des Deutschen Bundestages

Zusatzförderung durch:

pwc

VHV STIFTUNG

DANKSAGUNG

Ein solches Projekt, und insbesondere eine solche umfangreiche Unternehmensbefragung zum Thema Cyberangriffe gegen Unternehmen, kann nicht ohne die Unterstützung vieler Personen verschiedener Gremien und Organisationen durchgeführt werden. An dieser Stelle sprechen wir allen involvierten Akteuren unseren Dank für die Unterstützung aus! Ein besonderer Dank gilt dem Bundesministerium für Wirtschaft und Energie für die finanzielle Hauptförderung des Projektes im Rahmen der Initiative „IT-Sicherheit für die Wirtschaft“. Daneben danken wir der PricewaterhouseCoopers Wirtschaftsprüfungsgesellschaft mbH und der VHV-Stiftung für die Zusatzförderung in Form von Personalmitteln bzw. –ressourcen. Für anregende Diskussionen und Feedback rund um den Fragebogen und die Ergebnisse danken wir unseren Kooperationspartner*innen vom Forschungszentrum L3S und der Leibniz Universität Hannover, allen assoziierten Partnerorganisationen und deren Vertreter*innen sowie allen Beteiligten am Projektbeirat und am regionalen Unternehmensstammtisch bei PwC in Hannover. Danken möchten wir auch dem Umfrageinstitut Kantar EMNID für die Unterstützung bei der Finalisierung des Fragebogens und für die professionelle Durchführung der Unternehmensbefragung. Darüber hinaus gilt unser besonderer Dank den Unternehmen bzw. Institutionen und deren Vertreter*innen, die an den Experteninterviews im Vorfeld der Fragebogenkonzeption, am Pretest des Fragebogens sowie an der Unternehmensbefragung teilgenommen haben. Nur dadurch war es uns möglich, gesicherte und differenzierte Erkenntnisse zur Verbreitung und zu den Folgen von Cyberangriffen zu gewinnen sowie Risiko- und Schutzfaktoren zu identifizieren, die bei der Einschätzung des Phänomenbereichs und der Prävention von Cyberangriffen helfen sollen.

Hannover, Februar 2020
Die Autor*innen

ABKÜRZUNGEN

2FA	Zwei-Faktor-Authentifizierung
ADM	Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.
AG	Aktiengesellschaft
Besch.	Beschäftigte
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BMWi	Bundesministerium für Wirtschaft und Energie
BVMW	Bundesverband mittelständische Wirtschaft – Unternehmerverband Deutschlands e.V.
BYOD	Brind-your-own-device
BSI	Bundesamt für Sicherheit in der Informationstechnik
CATI	Computer Assisted Telephone Interview
CD	Compact Disc
DDos	Distributed Denial of Service
DsiN	Deutschland sicher im Netz e.V.
DoS	Denial of Service
eco	eco – Verband der Internetwirtschaft e.V.
ENISA	Europäischen Agentur für Netz- und Informationssicherheit
GDV	Gesamtverband der Deutschen Versicherungswirtschaft
Geschf.	Geschäftsführung
GmbH	Gesellschaft mit beschränkter Haftung
IfM	Institut für Mittelstandsforschung Bonn
IHK	Industrie- und Handelskammer
IKT	Informations- und Kommunikationstechnik
ISMS	Informationssicherheits-Managementsystem
ISO	Internationale Organisation für Normung
IT	Informationstechnik
KFN	Kriminologisches Forschungsinstitut Niedersachsen e.V.
k.A.	keine Angabe
Kfz	Kraftfahrzeug
KG	Kommanditgesellschaft
KI	Konfidenzintervall
KMU	Kleine und mittlere Unternehmen
L3S	Forschungszentrum L3S der Leibniz Universität Hannover

n.r.	nicht relevant
NIST	National Institute of Standards and Technology
OHG	Offene Handelsgesellschaft
PKS	Polizeiliche Kriminalstatistik
PwC	PricewaterhouseCoopers Wirtschaftsprüfungsgesellschaft mbH
SD-Card	Secure Digital Memory Card
SVB	Sozialversicherungspflichtig Beschäftigte
URS	Unternehmensregistersystem
USB	Universal Serial Bus
WIK	Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH
WZ	Wirtschaftszweig
ZAC	Zentrale Ansprechstelle Cybercrime für die Wirtschaft

INHALT

1 EINLEITUNG

Digitalisierung lässt sich ganz allgemein als Verbreitung digitaler Technologien beschreiben, die Auswirkung auf viele Lebensbereiche hat.[1] Auch Organisationen wie Unternehmen sind mit dieser Entwicklung in vielfältiger Weise konfrontiert. Allerdings sind sie nicht nur einseitig der Digitalisierung und einem Handlungsdruck generierenden Digitalisierungs-Diskurs[2] ausgesetzt, sondern nehmen selbst Einfluss auf den Prozess.[3] Vor dem Hintergrund der wahrgenommenen Potentiale der Optimierung und Wertschöpfung (z.B. Vereinfachung und Beschleunigung von Prozessabläufen, grenzüberschreitende Kooperationen, Erschließung datenbasierter Geschäftsmodelle) treffen Unternehmen organisationale Entscheidungen zur Nutzung digitale Technologien/ Daten/ Dienstleistungen sowie zu deren Entwicklung/ Generierung/ Vermarktung.[4]

Zu den nicht intendierten Nebenfolgen dieser Entscheidungen zählen z.B. die wachsenden Risiken von Cyberkriminalität und die damit verbundenen Schädigungen der Unternehmen sowie ihrer Kunden und Geschäftspartner, die Fragen zur Absicherung von IT-Systemen in mehr oder weniger digitalisierten Unternehmen aufwerfen.

Strafrechtlich gesehen umfasst Cyberkriminalität einen weitreichenden Deliktsbereich. Hierzu zählen im Kontext von Unternehmen z.B. Straftaten wie Betrug (§ 263 StGB), Erpressung (§ 253 StGB) oder Mobbing-Handlungen,[5] die mittels des Internets begangen werden. Diese werden häufig unter „Cyberkriminalität im weiteren Sinn“[6] gefasst, da das Internet und darüber verbundene IT-Systeme lediglich als „Tatmittel“ dienen und nicht das eigentliche Ziel des Angriffs darstellen. Sie werden in der Regel unter schon lange bestehende Straftatbestände innerhalb des Strafgesetzbuches (StGB) subsumiert. Demgegenüber werden mit „Cyberkriminalität im engeren Sinn“ Straftaten umfasst, die erst mit der digitalen Vernetzung möglich wurden und sich primär gegen IT-Systeme bzw. digitale Daten richten. Für diese Delikte wurden neue Straftatbestände im StGB geschaffen. Dazu gehören z.B. das Ausspähen oder Abfangen von Daten (§§ 202a, 202b und 202c StGB), die Datenhehlerei (§ 202d StGB), die Datenveränderung, die Computersabotage (§§ 303a und 303b StGB) und die Fälschung beweiserheblicher Daten (§ 269 StGB).

Die kriminologische Forschung, die sich mit Cyberkriminalität befasst, fokussiert vergleichsweise häufig Delikte aus dem Bereich „Cyberkriminalität im weiteren Sinne“, die sich gegen

---

1 Vgl. Büchner (2018b: 333f.).

2 Vgl. Büchner (2018a); Pfeiffer (2015).

3 Vgl. Büchner (2018b).

4 Dabei unterscheiden sich die Unternehmen hinsichtlich ihrer „Datenkompetenz“, die nach Büchner (2018b: 339) nicht selten in einem „Spannungsverhältnis“ zu den „eingesetzten Möglichkeiten der Datengenerierung“ steht.

5 Bspw. Beleidigung nach § 185 StGB, üble Nachrede nach § 186 StGB oder Verleumdung nach § 187 StGB

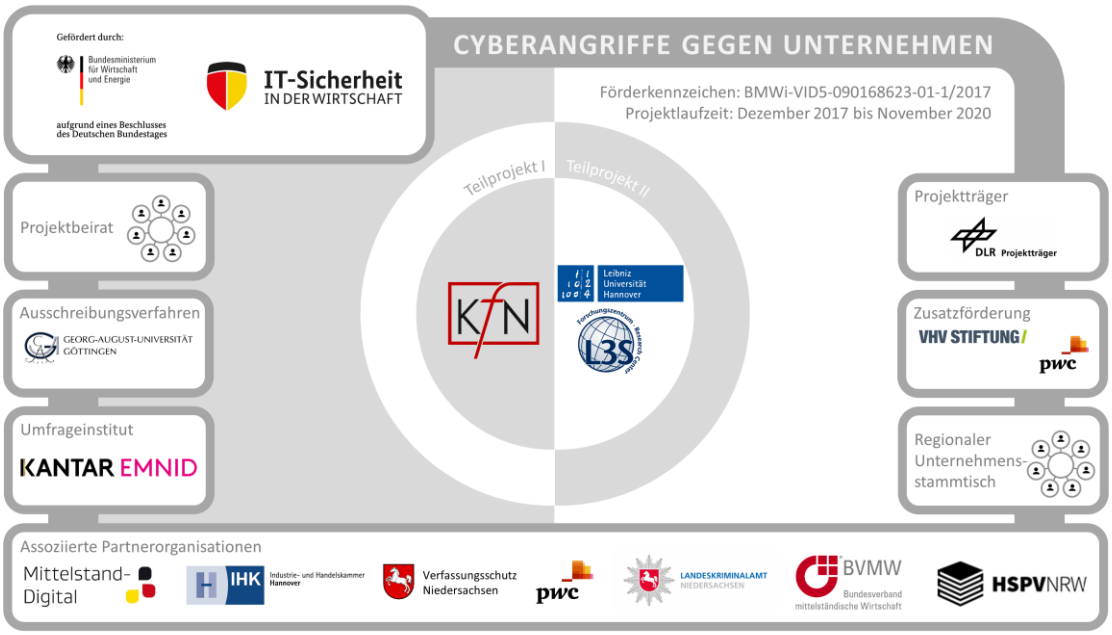
6 Zur Unterscheidung zwischen Cyberkriminalität im weiteren und im engeren Sinn siehe z.B. Council of Europe (2001); Eisele (2016: 255); Robertz, Oksanen und Räsänen (2016: 2); Seidl und Starnecker (2017: 338); Wall (2004: 20); Bundeskriminalamt (2018).

Privatpersonen richten,[7] wobei allgemein immer noch relativ wenig kriminologische Forschungen vorliegen.[8] Dies gilt besonders für Cyberkriminalität im Bereich der Wirtschaft. Vor allem fehlen Studien, die über eine beschreibende Darstellung der Verbreitung von Cyberkriminalität hinausgehen und Einflussfaktoren auf das Viktimisierungsrisiko untersuchen.[9]

Eine vom Bundesministerium für Wirtschaft und Energie (BMWi) bei der WIK-Consult in Auftrag gegebene Erhebung zur IT-Sicherheit von KMU in Deutschland hat ergeben, dass für kleine und mittlere Unternehmen auf dem Gebiet Cybersicherheit sehr viel Handlungsbedarf besteht.[10] Aber auch für größere Unternehmen und andere Bereiche der Wirtschaft, wie der Finanzbranche, haben Studien der Jahre 2015 und 2016 gezeigt, dass im Verlauf von zwei Jahren 40 bis 50 % der Unternehmen von Cyberkriminalität im Sinne von Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen waren (Bitkom 2015; KPMG 2015; PwC/Universität Halle 2016).

Sowohl für die kriminologische Forschung als auch für die deutsche Wirtschaft muss es angesichts dieser Ausgangssituation ein zentrales Anliegen sein, auf die Bedrohungslage durch Cyberkriminalität angemessen zu reagieren und sich mit dem Thema der IT-Sicherheit gezielter auseinanderzusetzen. Dazu bedarf es valider Ergebnisse möglichst unabhängiger wissenschaftlicher Forschung, um insbesondere Risiken, Verbreitung und Ausmaß von Cyberkriminalität abschätzen und mögliche Schutzmaßnahmen, z.B. in Hinblick auf das Kosten-Nutzen-Verhältnis beurteilen zu können.

Abbildung 1 **Projektbeteiligte**



[7] Z.B. Chen et al. (2016), Fansher & Randa (2018), Näsi et al. (2017), Tsitsika et al. (2015), Henson et al. (2016) oder Wegge et al. (2016).

[8] Vgl. Meier (2012). Einen Überblick über die Dunkelfeldforschung zum Thema Cybercrime gegen Privatpersonen in Europa geben Reep-van den Bergh und Junger (2018).

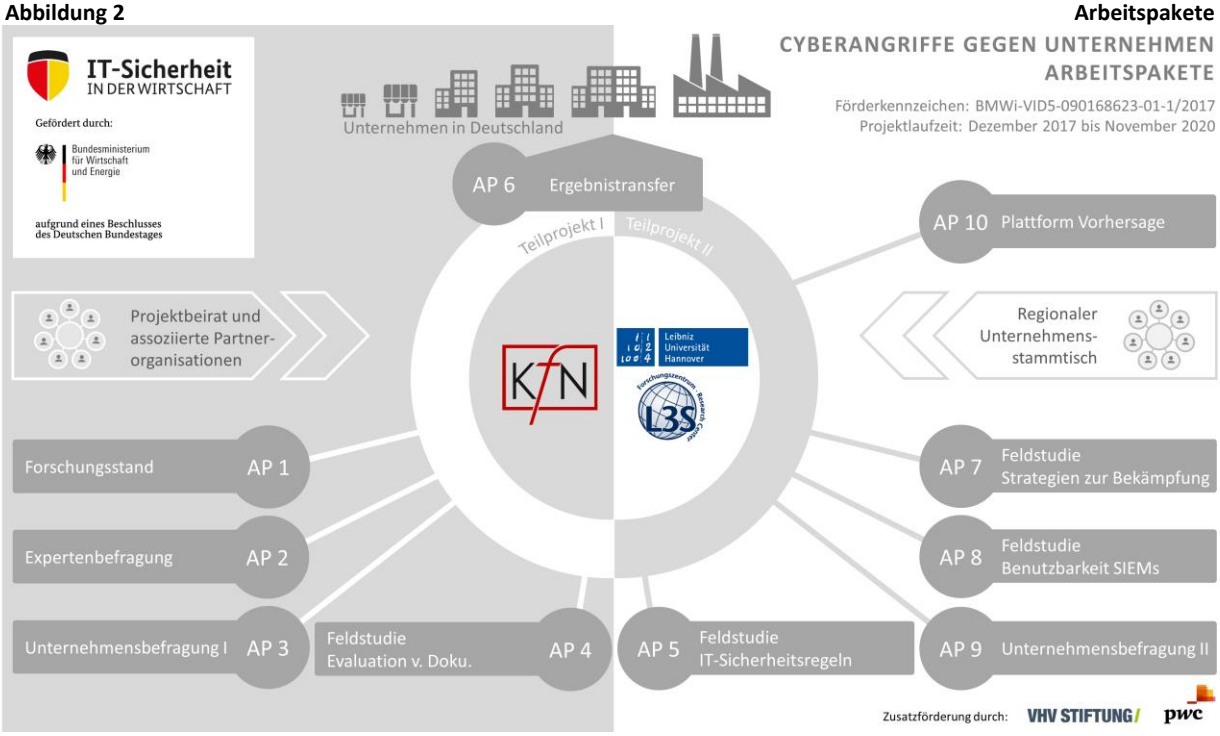
[9] Vgl. Meško (2018).

[10] Vgl. Bundesministerium für Wirtschaft und Energie (2012).

Das Kriminologische Forschungsinstitut Niedersachsen e.V. (KFN) hat sich deswegen zusammen mit dem Forschungszentrum L3S der Leibniz Universität Hannover dazu entschlossen, eine breit angelegte Untersuchung durchzuführen, die differenziertes Wissen zu den Angriffsarten und zur Häufigkeit der Cyberangriffe liefern soll. Zudem ist beabsichtigt, die Verbreitung von Präventionsmaßnahmen und von IT-Sicherheitsstandards zu ermitteln. Aufbauend auf diesen Ergebnissen soll zudem der Transfer der wissenschaftlichen Erkenntnisse in die Praxis sichergestellt werden. Hierfür sollen Präventionsstrategien und konkrete Handlungsempfehlungen erarbeitet werden.

Das Projekt „Cyberangriffe gegen Unternehmen“ wird im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie gefördert, erhält eine zusätzliche Förderung durch die VHV-Stiftung sowie von der Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers und wird durch einen beratenden Projektbeirat[11] unterstützt (Abbildung 1).[12] Es ist Modular aufgebaut und nutzt für die Beantwortung der jeweiligen Forschungsfragen unterschiedliche Erhebungsmethoden (Abbildung 2). Bisher wurden Interviews mit IT-Verantwortlichen in Unternehmen sowie mit Experten der Strafverfolgungsbehörden, des Verfassungsschutzes, des Bundesamtes für Sicherheit in der Informationstechnik und der Versicherungswirtschaft geführt,[13] gefolgt von Feldstudien mit IT-Beschäftigten in Unternehmen zu den Themen „Evaluation von Dokumentation im Kontext kleiner und mittlerer Unternehmen“ und „IT-Sicherheitsregeln im Arbeitsalltag“.

Abbildung 2 **Arbeitspakete**



[11] Darin sind neben den Förderern des Projektes der Bundesverband mittelständischer Wirtschaft, Mittelstand-Digital, die Industrie- und Handelskammer Hannover, das Landeskriminalamt Niedersachsen, der Verfassungsschutz Niedersachsen, der Lehrstuhl für Unternehmensrechnung und Wirtschaftsinformatik der Universität Osnabrück, der Lehrstuhl für Kriminologie und Soziologie der Hochschule für Polizei und öffentliche Verwaltung NRW in Köln, die VHV Versicherung und das IT-Sicherheits-Unternehmen CIPHRON vertreten.

[12] Weitere Informationen zum Gesamtprojekt und allen Beteiligten findet sich unter https://cybercrime-forschung.de.

[13] Ergebnisse zu den Experteninterviews finden sich bei Stiller et al. (2020).

Daneben wurde eine Befragung von 5.000 Unternehmen in Deutschland mit besonderem Fokus auf kleine und mittlere Unternehmen durchgeführt, die die Grundlage für diesen Bericht bildet. Die Laufzeit des Projektes ist auf drei Jahre von Dezember 2017 bis November 2020 angelegt.

1.1 Forschungsgegenstand

1.1.1 Cyberangriffe

Im Vergleich zu anderen kriminologischen Untersuchungsgegenständen, wie z.B. klassische Eigentumskriminalität, ist die Forschung zum Thema „Cyberkriminalität im engeren Sinne" mit Besonderheiten verbunden: Die Variations- und Kombinationsmöglichkeiten von Angriffsvektoren[14], Schadsoftware und Vorgehensweisen der Täter*innen sind aufgrund schneller technologischer Entwicklungen kaum zu überschauen.[15] Hinzu kommt, dass das sogenannte absolute Dunkelfeld[16] als sehr groß eingeschätzt werden kann.[17] Bestimmte Angriffe oder einzelne Schritte zusammenhängender Angriffe, wie das unbefugte Kopieren und Weitergeben von persönlichen Daten, werden durch die Betroffenen unter Umständen gar nicht erkannt. Möglicherweise werden erst deren Folgen zu einem späteren Zeitpunkt offensichtlich, wenn ein konkreter Schaden für das Unternehmen (z.B. der verlorene Wettbewerbsvorsprung infolge eines Spyware-Angriffs) oder Dritte eingetreten ist. Das Beratungsunternehmen Pascual & Marchini gibt in einer Studie zum Thema Identitätsdiebstahl beispielweise an, dass Betroffene, deren Kreditkartendaten durch Vorfälle bei Banken oder Handelsunternehmen im Vorjahr entwendet wurden, ein fast dreimal höheres Risiko aufweisen, Betroffene von Identitätsdiebstahl zu werden.[18] Die Intentionen der Täter*innen, z.B. zu welchem Zweck Daten unbefugt kopiert, manipuliert oder zerstört werden, ist für Privatanwender*innen wie für Unternehmen in vielen Fällen ebenfalls nicht unmittelbar zu erkennen. Selbst die Frage, ob es sich um einen gezielten Angriff handelt oder einen, von dem eine Vielzahl von Unternehmen betroffen ist, dürfte nur recht vage beantwortet werden können. Vor diesem Hintergrund wird in dieser Studie, unabhängig von ihrer strafrechtlichen Bewertung, auf Cyberangriffe abgestellt, die einerseits bemerkt wurden und die andererseits eine aktive Reaktion des Unternehmens notwendig machten, um Schäden zu verhindern oder zu begrenzen. Das kann z.B. vom manuellen Verschieben malware-infizierter Daten in einen Quarantänebereich bis zur Systemwiederherstellung eines ganzen Netzwerkes reichen. Die polizeiliche Anzeige eines laufenden CEO-Fraud wäre ebenfalls eine entspre-

[14] Als Angriffsvektoren werden Kombinationen von Angriffswegen und –techniken bezeichnet, mit denen sich Angreifer*innen unerlaubt Zugang zu IT-Systemen verschaffen (vgl. Bundesamt für Sicherheit in der Informationstechnik , 2017: 78).

[15] Die Herangehensweisen und Perspektiven bei der Differenzierung und Klassifikation von Cyberangriffen unterscheiden sich in der kriminologischen Forschung z.T. relativ stark. Je nach Fokus (Vorgehensweise oder Ziele der Täter*innen, Konsequenzen für die Betroffenen u.a.) werden Cyberangriffe in Kategorien geordnet und untersucht, die mehr oder weniger trennscharfe sind (vgl. Meško, 2018).

[16] Zum Dunkelfeld der Kriminalität gehören alle Straftaten, von denen die Polizei keine Kenntnis erlangt und die daher nicht in die offizielle Kriminalitätsstatistik eingehen. Dabei kann zwischen dem *relativen Dunkelfeld*, das sich mit Dunkelfeldforschung zumindest teilweise „erhellen" lässt, und dem *absoluten Dunkelfeld* unterschieden werden. Zum *absoluten Dunkelfeld* gehören strafrechtlich relevante Handlungen, die von den Beteiligten z.B. nicht erinnert oder nicht erkannt werden (vgl. Prätor 2014).

[17] Bayerl & Rüdiger (2018) weisen darauf hin, dass die Polizeiliche Kriminalstatistik (PKS) in Hinblick auf Cybercrime-Delikte aufgrund des vermutlich sehr großen Dunkelfeldes kaum aussagekräftig ist.

[18] Vgl. Pascual & Marchini (2015).

chende Reaktion. Zwischen folgenden Cyberangriffsarten wurde in der Befragung differenziert: Ransomware-Angriff, Spyware-Angriff, Angriff mit sonstiger Schadsoftware (Malware), manuelles Hacking, (D)DoS-Angriff, Defacing, CEO-Fraud und Phishing.[19]

1.1.2 Unternehmen

Als zumindest potentiell Betroffene von diesen Cyberangriffen stehen Unternehmen im Mittelpunkt dieser Studie. Nach dem Statistischen Bundesamt werden Unternehmen „als kleinste rechtlich selbstständige Einheit definiert, die aus handels- bzw. steuerrechtlichen Gründen Bücher führt. Ferner muss das Unternehmen eine jährliche Feststellung des Vermögensbestandes bzw. des Erfolgs der wirtschaftlichen Tätigkeit vornehmen. Hierzu zählen auch Einrichtungen zur Ausübung einer freiberuflichen Tätigkeit.“[20]

Ein besonderer Fokus liegt dabei auf den kleinen und mittleren Unternehmen (KMU). Nach einer gängigen KMU-Definition des Instituts für Mittelstandforschung (IfM) Bonn vom 01.01.2016 werden Unternehmen unter Verwendung der Beschäftigtengrößenklasse und des Jahresumsatzes folgendermaßen klassifiziert: Unternehmen bis 9 Beschäftigte und bis 2 Mio. EUR Jahresumsatz bilden die Gruppe der Kleinstunternehmen, bis 49 Beschäftigten und einem Umsatz bis 10 Mio. EUR/Jahr zählen zu der Gruppe der kleinen und bis 499 Beschäftigte und 50 Mio. EUR Jahresumsatz zu der Gruppe der mittleren Unternehmen.[21] Diese KMU werden wiederum von den Großunternehmen ab 500 Beschäftigten bzw. und mehr als 50 Mio. EUR Jahresumsatz abgegrenzt. In dieser Studie wird insofern davon abgewichen, als dass für die Schichtung und Ziehung der Stichprobe sowie für die Darstellung der Ergebnisse lediglich das Merkmal der Beschäftigtengrößenklasse herangezogen wurde. Der Jahresumsatz wurde separat erhoben und betrachtet. Daneben wurde die Gruppe der Kleinstunternehmen (bis 9 Beschäftigte) unberücksichtigt gelassen, da es sich um die Unternehmensgruppe handelt, die in den für die Stichprobenziehung genutzten Datenbanken nur lückenhaft vorhanden ist und damit nur schwer zu erreichen gewesen wären. Ihr Einbezug hätte daher den Zeit- und Kostenrahmen dieser Befragung überstiegen.

Die in diese Studie einbezogenen Befragten von Unternehmen wurden gebeten, jeweils für ihr Unternehmen als rechtlich selbstständige Einheit zu sprechen. Dies bedeutet, dass z.B. mehrere Betriebsstätten des Unternehmens einbezogen wurden, jedoch keine Tochter- oder Mutterunternehmen, da diese unter einer eigenen Rechtsform firmieren.

1.2 Forschungsfragen

Ziel der Unternehmensbefragung ist es, differenzierte Informationen über die Verbreitung von Cyberangriffen, auf die Unternehmen reagieren mussten, zu erlangen und die Folgen (System-

[19] Eine Erläuterung der Cyberangriffsarten und deren Operationalisierung findet sich in Kapitel 7. Nicht als Angriffsart, sondern als Folge bzw. Zweck eines Cyberangriffes wurden z.B. Identitätsdiebstahl oder Kreditkartenbetrug gewertet.

[20] Statistisches Bundesamt (2018: 5) Siehe dazu auch Hartmann (2017: 188f.).

[21] Quelle: https://www.ifm-bonn.org/definitionen/kmu-definition-des-ifm-bonn/ (aufgerufen am 07.06.2019). Eine hinsichtlich der Beschäftigtengrößenklasse abweichende KMU-Definition wird von der Europäischen Kommission verwendet: zu den mittleren Unternehmen werden nur solche mit bis zu 249 Beschäftigten und 50 Mio. EUR Jahresumsatz bzw. 43 Mio. EUR Jahresbilanzsumme gezählt (Quelle: http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/ (aufgerufen am 07.06.2019)).

ausfälle. Kosten etc.) und Reaktionen (Anzeigeverhalten, Hinzuziehen von IT-Sicherheitsdienstlern etc.) zu erheben. Ferner soll analysiert werden, welche Faktoren das Risiko eines erfolgreichen Angriffs erhöhen und welche IT-Sicherheitsmaßnahmen bestehen. Bezüglich der Reaktion auf Angriffe ist von Interesse, welche Erfahrungen ggf. mit den Strafverfolgungsbehörden und Versicherern gemacht wurden und welche Gründe dafür vorliegen, den Vorfall nicht anzuzeigen bzw. über keinen Versicherungsschutz für Informationssicherheitsverletzungen zu verfügen. Hieraus sollen auch Ableitungen dafür gewonnen werden, wie eine Strafverfolgung gestaltet sein muss, damit Unternehmen sie vermehrt nutzen. Ferner soll die Erhebung von spezifischen Unternehmensmerkmalen helfen, sinnvolle Differenzierungen zwischen Unternehmen treffen zu können, die von bestimmten Angriffsarten betroffen waren.

Bei der ersten Unternehmensbefragung innerhalb des Projektes „Cyberangriffe gegen Unternehmen“ sind vor allem folgende Forschungsfragen zentral:

- Welche IT-Sicherheitsmaßnahmen gegen Cyberangriffe haben die Unternehmen eingerichtet?
    - Verfügen die Unternehmen über schriftlich fixierte Richtlinien? Wird diese laufend den Veränderungen von Cyberangriffen angepasst?
    - Gibt es im Unternehmen spezialisierte Mitarbeiter*innen, denen explizit die Aufgabe übertragen wird, Cyberangriffe abzuwehren bzw. zu verhüten? Werden stattdessen oder ergänzend externe Fachkräfte herangezogen?
    - Wie kontrollieren die Unternehmen die eigene IT-Sicherheit? Wird insbesondere eine Sicherheitsüberprüfung des IT-Systems mit Methoden durchgeführt, die Angreifer*innen verwenden könnten, um unautorisiert in das System einzudringen (Penetration-Testing)? Gibt es eine förmliche Zertifizierung des IT-Sicherheitssystems?
- Auf welche Cyberangriffsarten mussten Unternehmen in den letzten zwölf Monaten reagieren?
    - Welche Unterschiede zu Art und Häufigkeit von Cyberangriffen zeigen sich, wenn man nach Beschäftigtengrößenklasse und Branchenzugehörigkeit der Unternehmen differenziert?
    - Wie lange benötigen die Firmen, um das befallene System zu substituieren oder in einen betriebsbereiten Zustand zu versetzen?
    - Gibt es Vermutungen über die Täter*innen?
    - Wie haben die Unternehmen auf Angriffe reagiert?
    - Haben sie insbesondere bei Angriffen, die mit einer Erpressung verknüpft waren, die geforderte Leistung ganz oder teilweise erbracht?
    - Wie hoch ist der Schaden, der aus wahrgenommenen Cyberangriffen entstanden ist?
    - Sind die befragten Unternehmen gegen Schäden versichert, die aus Cyberangriffen entstehen? Welche Leistungen haben versicherte Unternehmen nach einem Cyberangriff erhalten und wie zufrieden sind sie hiermit?

- Wie ist das Anzeigeverhalten von betroffenen Unternehmen?
    - Was sind die Gründe einer Nichtanzeige?
    - Welche Erfahrungen machten die anzeigenden Unternehmen mit der Polizei?
    - In wie vielen Fällen konnten Täter*innen ermittelt werden?
- Gibt es einen Zusammenhang zwischen der Häufigkeit von Cyberangriffen mit dem Vorhandensein bestimmter IT-Sicherheitsmaßnahmen?
    - Lässt sich der Nachweis führen, dass derartige Investitionen in die IT-Sicherheit die Wahrscheinlichkeit von erfolgreichen Cyberangriffen reduzieren?
    - Welche IT-Sicherheitsmaßnahmen wirken sich gegebenenfalls besonders aus?

Vor der Beantwortung dieser Fragen mit den Ergebnissen der Unternehmensbefragung in den Kapiteln 5 bis 10 werden in Kapitel 2 der Forschungstand bezogen auf Cyberangriffe gegen Unternehmen detailliert dargestellt sowie in Kapitel 3 die Methode und das Auswahlverfahren der Datenerhebung erläutert. Anschließend wird die Stichprobe anhand bestimmter Unternehmensmerkmale und deren Verteilung in der Grundgesamtheit beschrieben, wonach auf weitere Unternehmensmerkmale in Kapitel 4 übergeleitet wird.

Nach den Ergebnissen zur IT-Sicherheitsstruktur von Unternehmen, deren Einschätzungen zu IT-Risiken, erlebten Cyberangriffen in den letzten zwölf Monaten, den Details zum schwerwiegendsten Angriff und zur Wirksamkeit von IT-Sicherheitsmaßnahmen erfolgt in Kapitel 11 ein zusammenfassendes Fazit mit Hinweisen auf methodisch bedingte Restriktionen sowie ein Ausblick auf folgende Analysen und anstehende Forschungsmodule innerhalb der Projektes „Cyberangriffe gegen Unternehmen“.

2 FORSCHUNGSSTAND

2.1 Charakterisierung des Forschungstandes

Der Literaturstand zum Thema „Cyberangriffe gegen Unternehmen“ wächst aufgrund der weltweiten Aktualität und Brisanz des Phänomens stetig an und ist durch eine hohe Heterogenität sowohl hinsichtlich der jeweiligen Forschungsschwerpunkte als auch der Autorengruppen und deren Motivationen gekennzeichnet. So variieren die Forschungsschwerpunkte beispielweise in der Opferperspektive (Organisation oder Individuum), der Täterperspektive (Externer Angreifer, Insider), einem technischen oder nicht-technischen Fokus auf IT-Sicherheitsmaßnahmen, in der Behandlung angrenzender Themengebiete (Digitalisierung, Industrie 4.0, Kosten von Cyberangriffen, Cyberversicherungen etc.), den zugrundeliegenden Daten (Umfrage oder Analyse technischer Sekundärdaten, Größe und Zusammensetzung der Stichprobe) oder der Gültigkeit der Ergebnisse für die zugrundliegende Population (international, national, regional). Hinsichtlich der Autoren- und Herausgeberschaften ist es beispielweise möglich, die folgenden drei Gruppen zu unterscheiden: a) behördliche, politiknahe und andere nicht-kommerzielle Institutionen, b) kommerzielle bzw. unternehmerische Organisationen und c) akademische Forschungseinrichtungen. Jedoch ist diese Unterscheidung aufgrund der fließenden Grenzen zueinander nicht immer möglich.

Behörden und andere nicht-kommerzielle Stellen veröffentlichen regelmäßig Informationen zu Fallzahlen des Phänomens „Cyberangriffe gegen Unternehmen“. Diese fokussieren in möglichst neutraler Art und Weise zumeist das primäre Tätigkeitsfeld der entsprechenden Institution, geben ergänzend Hinweise oder Handlungsvorschläge an betroffene Unternehmen, steigen zumeist jedoch weniger in die Ursachenforschung und vertiefte Analyse ein. Gerade Erkenntnisse behördlicher Veröffentlichungen basieren häufig auf dem sogenannte Hellfeld, beispielweise der polizeilichen Kriminalstatistik, und umfassen somit lediglich offiziell gemeldete Vorfälle, jedoch nicht das sogenannte Dunkelfeld.

Eine zweite Gruppe von Autoren*innen verfolgt einen geschäftlichen bzw. kommerziellen Hintergrund mit der Veröffentlichung von Umfragen und Berichten. Dies ist beispielweise die Steigerung des eigenen Bekanntheitsgrades, die Darbietung eigener Kompetenzen, Interessensvertretungen oder Auftragsforschung. Solche Literatur ist ebenfalls sehr heterogen, verwendet teilweise emotionale Inhalte aber auch wissenschaftliche Methoden und Vorgehensweisen. Sie ist gegebenenfalls nicht unabhängig und beinhaltet mitunter subjektive, mit dem eigenen geschäftlichen Hintergrund harmonierende Aussagen und Ergebnisse. Berichte, Studien und Umfragen dieser Autorengruppe stellen den überwiegenden Teil der öffentlich verfügbaren Literatur zum Thema „Cyberangriffe gegen Unternehmen“ dar[22] und prägen daher maßgeblich die Wahrnehmung des Phänomens in der Öffentlichkeit.[23]

[22] Vgl. Gehem et al. (2015).

[23] Vgl. Paoli et al. (2018).

Die dritte Gruppe weist einen forschungsspezifischen bzw. akademischen Hintergrund auf. Ziel dieser Literatur ist in der Regel ein auf wissenschaftlichen Methoden basierender Erkenntnisgewinn und eine möglichst unabhängige Verbreitung dieser Erkenntnisse an einen weiten Adressatenkreis. Literatur dieser Autorenschaft weist in der Regel eine sachgerechte und transparente Beschreibung der verwendeten Stichprobe, Daten und Methoden auf und nennt Gütekriterien und Limitierungen, die zur Evaluation der Erkenntnisse dienen. Literatur dieser Gruppe, vor allem empirische Forschung, ist obwohl das Phänomen „Cyberangriffe gegen Unternehmen“ nicht neu ist, stark unterrepräsentiert und bedarf einer faktenbasierten Ausweitung.[24]

Trotz der hohen Anzahl und Vielfalt der öffentlich verfügbaren Literatur zum Thema „Cyberangriffe gegen Unternehmen“ wird immer wieder die fragmentierte, nicht vergleichbare, teils widersprüchliche oder fehlende Fundierung der Datenbasis der Forschung kritisiert.[25] Dies reicht bis hin zum Vorwurf, dass kaum verlässliche Daten zum Phänomen „Cyberangriffe gegen Unternehmen“ existieren, gar viele Akteure zuverlässige nicht mehr von unzuverlässigen Daten unterscheiden können und darum schlecht informierte Entscheidungen treffen.[26] Die vorherrschende Literatur scheint daher dem Informationsbedürfnis der Akteure, sei es von Unternehmen, Behörden, Forschern und Privatpersonen, nicht vollständig gerecht zu werden.

2.2 Vorgehen zur Auswahl und Aufarbeitung der betrachteten Literatur

Zu Beginn der Aufarbeitung des Forschungsstandes wurde eine umfassende Online-Recherche durchgeführt, die zum Ziel hatte, relevante empirische Studien und Berichte zum Thema „Cyberangriffe gegen Unternehmen“ zu identifizieren.[27] Im Rahmen der Aufarbeitung des Forschungsstandes wurden über 350 Titel in einem Literaturverwaltungsprogramm systematisch erfasst, innerhalb von über 150 Gruppen kategorisiert sowie mit ca. 1.700 Wissenselementen (Kommentaren, Schlagwörtern etc.) versehen. Die Schriften stammen von unterschiedlichsten Autoren aus dem In- und Ausland und haben nicht notwendiger Weise einen Fokus auf kleine- und mittlere Unternehmen, da davon auszugehen ist, dass das Phänomen „Cyberangriffe gegen Unternehmen“ keine Landesgrenzen[28] oder Größenklassen kennt und daher relevante Erkenntnisse auch außerhalb dieser Literatur anzutreffen sind. Da eine vollständige Wiedergabe dieser Literatur nicht möglich ist, beschränkt sich dieser Literaturstand auf eine Auswahl der relevantesten Quellen, die sich beispielweise durch neue, besonders erstaunliche sowie widersprüchli-

[24] Vgl. Organisation for Economic Co-operation and Development (2015); McGuire & Dowling (2013); Agrafiotis et al. (2018); Ngo & K. Jaishankar (2017); Gehem et al. (2015); Cobb (2015); Paoli et al. (2018).

[25] Vgl. Gehem et al. (2015); Florencio & Herley (2012); McGuire & Dowling (2013); Hillebrand et al. (2017); Cobb (2015); Ryan & Jefferson (2003).

[26] Vgl. Ryan & Jefferson (2003).

[27] Die Online-Recherche umfasste verschiedene Datenbanken und Suchmaschinen (z.B. DuckDuckGo, Google, Google Scholar, AISeLibrary, Springer, Elsevier, etc.) sowie Vor- und Rückwärtssuchen nach Schlagworten (z.B. Cybercrime, Online Crime, Internetkriminalität, Cyber Attacks etc.) mit dem Fokus auf Organisationen und Unternehmen. Ausgewertet wurden deutsch- und englischsprachige Quellen ohne Einschränkungen auf bestimmte Regionen, Unternehmensbranchen oder Unternehmensgrößen. Im Fokus stand vor allem primärdatenerhebende und -auswertende Literatur. Die Online-Recherche verlief projektbegleitend im Zeitraum vom Dezember 2017 bis April 2019.

[28] Vgl. Böhme (2013); Kigerl (2012).

che Erkenntnisse auszeichnen oder nach Meinung der Autoren ein gutes Abbild für die Mehrheit der gesichteten Literatur darstellen. Ein Fokus liegt zudem auf quantitativen Studien, die eigene Primärdaten erheben und auswerten.[29]

Ein Beispiel für eine beschränkte Auswahl des Forschungsstandes zum Vorteil einer systematischen und zusammenfassenden Darstellung der jeweiligen Erkenntnisse bietet die Studie „Aktuelle Lage der IT-Sicherheit in KMU“ des Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste (WIK GmbH)[30], welcher die Ausgangsbasis für den im Folgenden beschriebenen Literaturstand bildet. Ergänzt in Inhalt und Umfang stellt der Forschungstand nun 32 Studien bzw. Berichte dar, die zwischen den Jahren 2006 und 2019 veröffentlicht wurden.

Eine tabellarische Zusammenfassung der für diesen Forschungsbericht relevanten Literatur ist in Tabelle 53[31] enthalten. Dort können, sofern von den Autoren angegeben, Hintergrundinformationen zu Stichprobengrößen, Stichprobenzusammensetzungen, verwendeten Methoden etc. nachgeschlagen werden. Dies ist dringend geboten, um vermeintliche Gemeinsamkeiten oder Widersprüche der betrachteten Literatur in einen größeren Kontext zu rücken. Eine Erläuterung ausgewählter Erkenntnisse der genannten Literatur folgt in Abschnitt 2.4.

2.3 Limitationen der betrachteten Literatur

Im Rahmen der Aufarbeitung des Literaturstandes und der damit einhergehenden Sichtung zahlreicher verschiedener Studien und Berichte zum Themenkomplex „Cyberangriffe gegen Unternehmen“, sollen in diesem Abschnitt die häufigsten Limitationen genannt und kurz diskutiert werden. Dadurch soll eine gewisse Sensibilisierung des Lesers erreicht werden, die nötig ist, um die Interpretation des nachfolgenden Forschungsstandes zu vereinfachen. Die genannten Limitationen in den Bereichen a) Stichprobenart, Stichprobengröße und Stichprobenziehung, b) Operationalisierung und c) Ergebnisdarstellung und Transparenz können dazu führen, dass die Ergebnisse der aufgeführten Studien untereinander, als auch in der direkten Gegenüberstellung zu dieser Studie, zum Teil nur sehr eingeschränkt vergleichbar sind.

a) Stichprobenart, Stichprobengröße und Stichprobenziehung

Die Zusammensetzung der teilnehmenden Unternehmen in einigen Studien ist in Hinblick auf die Verteilung bestimmter Merkmale der jeweiligen Grundgesamtheit, wie beispielsweise die Beschäftigtengrößenklasse oder die Branche, stark verzerrt. Die Erkenntnisse der untersuchten Stichprobe können daher nicht oder nur stark eingeschränkt auf die Grundgesamtheit übertragen werden. Die Gewichtung von Antworten gemäß geeigneten Schätzern für die Grundgesamtheit, beispielsweise Angaben des Unternehmensregisters für Befragungen deutscher Unternehmen, kann helfen, Aussagen der Stichprobe gegenüber der Grundgesamtheit zu „re-proportionalisieren“. Problematisch kann, im Vergleich zu einer echten Zufallsstichprobe, zudem die Selbstrekrutierung teilnehmender Unternehmen in Studien sein. Je nach Verbreitungsgrad der Möglichkeit zur Umfrageteilnahme, kann es sein, dass sich nur bestimmte Unternehmen auf eine Teilnahme einlassen bzw. nur bestimmte Unternehmen von einer Umfrage erfahren.

[29] Folgende kürzlich erschienene Studien konnten in der Darstellung des Forschungsstandes nicht mehr mit einbezogen werden: Verband der TÜV e.V. (2019); Berg & Niemeier (2019).

[30] Vgl. Hillebrand et al. (2017).

[31] S. 183ff. (Anhang 1: Zusatztabellen).

Dies ist beispielsweise der Fall, wenn Web-Links zu den Fragebögen nur an eigene Kunden oder die Mitglieder des eigenen Verbandes versendet werden, welche bereits eine gewisse Sensibilisierung für das Thema „IT-Sicherheit“ aufweisen. Unternehmen ohne diese Netzwerke bzw. einschlägiges Vorwissen werden hingegen nicht auf diese Umfragen aufmerksam. Des Weiteren können durch die Selbstrekrutierung in Verbindung mit anonymen Umfragen Mehrfachteilnahmen eines Unternehmens kaum ausgeschlossen werden.

Eine weitere Limitation kann sich durch die Verwendung geringer Stichprobenzahlen ergeben, die in Studien häufig durch Budget- oder Zeitrestriktionen begründet sind. Je größer eine Stichprobe ist, desto genauere Aussagen zur Grundgesamtheit lassen sich treffen. Insbesondere Filterfragen und granulare Antwortkategorien können die jeweiligen Stichprobenzahlen einer Gruppe so weit reduzieren, dass eine statistische Aussagefähigkeit kaum noch gegeben ist.

Um die Erkenntnisse einer Studie auf eine Grundgesamtheit übertragen zu können ist es wichtig, die Grund- und Auswahlgesamtheit zunächst zu definieren und transparent zu beschreiben. Einige Studien schließen teilnehmende Unternehmen bestimmter Branchen oder Größen explizit ein oder aus, während dies andere Studien nicht tun. Auch werden Branchendefinitionen selbst erstellt, ohne eine Überleitung zu einem gängigen Standard (z.B. WZ08, NACE, NAICS) zu erlauben. Anschließend wird die Einordnung in dieses Branchenschema der befragten Person überlassen, was dazu führen kann, dass zwischen zwei Studien sprichwörtlich *Äpfel mit Birnen* verglichen werden.

b) Operationalisierung

Im Rahmen der Umsetzung einer Studie wird festgelegt, wie die zu untersuchenden und theoretischen Merkmale konkret messbar gemacht werden sollen (sogenannte Operationalisierung). Im Rahmen der Literaturrecherche fielen hier insbesondere eine Großzahl uneinheitlicher und mitunter intransparenter Definitionen zum Themenkomplex „Cyberangriffe gegen Unternehmen“ auf, die einen direkten Vergleich mehrerer Studien stark einschränken. Der Begriff „Cyberangriff“ wurde z.B. technisch oder rechtlich definiert, schon als bloßer Versuch oder erst nach erfolgtem Schadenseintritt gewertet. Des Weiteren wurde ein „Unternehmen“ als selbstständige juristische Einheit, als Konzern-Verbund oder in einzelne Betriebsstätten mit Standorten im Inland oder auch im Ausland unterteilt. Risiko-Wahrnehmungen wurden nicht unterschieden nach der Wahrnehmung für das eigene Unternehmen oder eine Vergleichsgruppe, als allgemeine Bedrohungslage oder konkrete Bedrohungen durch bestimmte Angriffsarten oder Angreifer*innen. Heterogene Definitionen und Operationalisierungen werden schon aufgrund der zahlreichen Akteure auf dem „IT-Sicherheits-Markt“ immer bestehen, sollten jedoch bewusst bei der eigenen Interpretation der Ergebnisse berücksichtigt werden.

Weitere Einschränkungen können sich durch die Datenerhebung ergeben. So ist der Untersuchungsgegenstand zu Cyberangriffen gegen Unternehmen zwar die Organisation, Daten werden jedoch in den meisten Fällen schriftlich oder mündlich durch Individuen mit begrenztem Wissen und eigenen Prägungen, Vorstellungen und Motivationen zur Verfügung gestellt (sogenannte Self-Reporting-Bias). Die Datenbasis beinhaltet dadurch ein gewisses Maß an Subjektivität. Neben Unwissenheit und Verständnisschwierigkeiten kann auch die soziale Erwünschtheit dazu führen, dass befragte Personen Angaben machen, die nicht der Realität ent-

sprechen. Um dies zu kontrollieren, ist es möglich, das Antwortverhalten verschiedener Befragtengruppen zu vergleichen (z.B.: Antworten Geschäftsführer*innen anders auf die Frage nach der Einschätzung des Betriebsklimas als IT-Mitarbeiter*innen?). Selbstverständlich können Befragte nur Auskunft über Geschehnisse geben, die ihnen selbst bekannt sind. Von der Organisation oder der befragten Person unbemerkte Cyberangriffe, das sogenannte absolute Dunkelfeld, können durch diese Studienformen nicht untersucht werden.

c) Ergebnisdarstellung und Transparenz

Weitere Einschränkungen innerhalb der gesichteten Literatur ergeben sich durch fehlende Angaben oder mangelnde Transparenz. So wird bei manchen Antwortmöglichkeiten nicht erhoben, ob Unternehmen Antworten nicht kennen, nicht antworten möchten oder die Frage gar nicht auf die Situation des Unternehmens zutrifft. Auch präzisieren Fragen nach IT-Sicherheitsmaßnahmen häufig nicht, ob diese bereits vor oder erst nach einem relevanten Cyberangriff vorlagen. Des Weiteren fehlen mitunter Standardangaben zur Grund- und Auswahlgesamtheit, zur Stichprobenzusammensetzungen sowie zur Struktur und Funktionen von befragten Personen. Auch Erhebungs- und Betrachtungszeiträume (z.B. das Jahr 2017 oder die letzten 12 Monate) werden nicht klar abgegrenzt und dargestellt. Dabei liegen sogar Studien vor, die Aussagen zu Betrachtungsjahren treffen, obwohl diese zum Zeitpunkt der Datenerhebung noch gar nicht abgeschlossen waren.[32] Nicht zuletzt besteht generell die Gefahr von Fehlinterpretationen durch die Leser*innen infolge mangelnder Transparenz über die zugrundeliegende konkrete Fragestellung, da einige Studien lediglich ihre Schlussfolgerungen veröffentlichen, nicht jedoch die ursprünglich gestellte Frage.

Die dargestellten Limitierungen sollen Leser*innen sensibilisieren und helfen, den im folgenden Abschnitt zusammengefassten Literaturstand sachgerechter interpretieren zu können.

2.4 Zentrale Ergebnisse bisheriger Forschung

In diesem Abschnitt werden die im Anhang 1 in Tabelle 53[33] aufgeführten Studien zusammengefasst und erläutert. Um die inhaltliche Würdigung für den Leser zu vereinfachen, werden die Inhalte thematisch[34] und nicht Titel nach Titel zusammengefasst. Direkte Vergleiche der in der Literatur vorliegenden Erkenntnisse mit den Erkenntnissen dieser Unternehmensbefragung werden, sofern möglich und sinnvoll, innerhalb der Kapitel 5 bis 10 diskutiert.

2.4.1 Strukturelle Merkmale

Von den 32 ausgewählten Studien stammen 18 von kommerziellen bzw. unternehmerischen Autorengruppen, neun von Behörden, politiknahen und anderen nicht-kommerziellen Organisationen und fünf von akademischen Forschungseinrichtungen. Veröffentlicht wurden sie in den Jahren 2006 bis 2019, wobei rund zwei Drittel aus den Jahren 2017 bis 2019 stammt. Die Studien unterscheiden sich sehr stark in ihrem Umfang (12 – 110 Seiten, Median 33 Seiten)

[32] Hier wurden anscheinend Jahreszahlen in Grafiken verwendet ohne darauf hinzuweisen, dass sich die Jahreszahl nicht auf die Verteilung des Merkmals im gesamten Jahr bezieht, sondern das bestimmte Merkmal lediglich in diesem Jahr erhoben wurde.

[33] Anhang 1: Zusatztabellen, S. 183ff.

[34] Siehe „Inhaltliche Merkmale“ in Tabelle 53.

und betreffen in 16 Fällen ausschließlich deutsche, in sechs Fällen ausschließlich eine andere Nation und in zehn Fällen Unternehmen/ Organisationen aus mehreren Ländern. Sofern die zugrundeliegenden Daten durch Interviews oder Fragebögen erhoben wurden (26 Fälle) lagen die Stichprobenumfänge zwischen 254 und 9.500 Befragten (Median 679). Dabei gaben zehn Studien nicht an, welche Personen bzw. Funktionen befragt wurden.

Angaben zur Grund- und Auswahlgesamtheit der Stichprobenziehung wurden in rund zwei Dritteln der Fälle nicht gemacht. Angaben zur Stichprobenart und -ziehung wurden in 17 Fällen nicht gegeben. Die Zusammensetzung der Stichprobe wurde von den meisten Unternehmen beschrieben, zumeist mittels der Angabe der befragten Branchen und Unternehmensgrößen.[35] Eine Reflektion über die Möglichkeit, die Ergebnisse zu verallgemeinern, fehlt häufig und wird im schlechtesten Fall stillschweigend angenommen. Vier der Studien gehen über eine rein deskriptive Darstellung der Ergebnisse hinaus und wenden Instrumente der schließenden Statistik an.

2.4.2 Risikoeinschätzung und Bedrohungslage

Untersuchungen zur Einschätzung des Risikos und der Bedrohung durch Cyberangriffe gegen sich und die eigene Organisation oder gegen andere Vergleichsgruppen (z.B. andere Branchen) beruhen auf Selbsteinschätzungen. Angaben hierzu wurden in 17 der 32 Studien identifiziert.

Nach einer Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sahen im Jahr 2017 92 % der befragten Unternehmen Cyberangriffe als relevante Gefährdung für die Betriebsfähigkeit an.[36] Ein Jahr später hingegen sinkt dieser Wert um 14 % auf 76 %, während der Anteil der Unternehmen, die eine zunehmende Bedrohungslage erwarten, im selben Zeitraum um 22% von 66 % auf 88 %[37] anstieg.[38] Dem entgegengesetzt hat der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) in einer Umfrage festgestellt, dass lediglich 32 % bis 43 % der befragten Unternehmen das Risiko der eigenen Viktimisierung als hoch oder sehr hoch wahrnehmen.[39] Auch eine Studie der Industrie- und Handelskammer Nord (IHK Nord) aus 2013 kommt zu ähnlichen Ergebnissen (38 % der Befragten schätzen die Lage als bedrohlich ein).[40] Eine Studie von PwC sieht die Bedrohungslage sehr ähnlich zur Umfrage des BSI 2017 als erhöht bzw. stark erhöht (66 %, sogar 85 % für Industrie 4.0-Unternehmen), sieht aber auch Anzeichen dafür, dass die allgemein wahrgenommene Bedrohungslage und das Bewusstsein für das eigene Risiko auseinanderklaffen.[41] In einer weiteren PwC-Studie wird dargestellt, dass die allgemein wahrgenommene Bedrohungslage stärker empfunden wird, als die eigene

---

35 In der Regel wurden hier eigene Gruppen gebildet, nur wenige bezogene sich auf offizielle Klassifikationen (z.B. WZ-Klassen, ISIC, NACE, NAICS etc.).

36 Vgl. Bundesamt für Sicherheit in der Informationstechnik .

37 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2019a).

38 In der ersten Fassung des Berichtes vom Bundesamt für Sicherheit in der Informationstechnik (2019b) stimmten 87 % der Befragten dieser Aussage nicht zu. Nach einem Hinweis zu diesem und anderen auffälligen Ergebnissen wurde am 18.04.2019 eine korrigierte Fassung des Berichtes veröffentlicht, bei der sämtliche Ergebnisse zum Abschnitt „Meinung“ korrigiert wurde. In einer dazu gehörigen Pressemitteilung („BSI korrigiert Ergebnisse der Cyber-Sicherheitsumfrage“ Quelle: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Cyber-Sicherheitsumfrage-180419.html) heißt es, dass „ein technisch bedingter Auswertungsfehler, [..] zu einer Verfälschung einiger weniger Ergebnisse der Umfrage geführt hat“.

39 Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

40 Vgl. Industrie- und Handelskammer Nord e.V. (2013).

41 Vgl. PricewaterhouseCoopers AG WPG (2017).

Bedrohungslage.[42] Diesen Unterschied in der eigenen Wahrnehmung stellt auch der GDV fest: 72 % sehen das Risiko von Cyberkriminalität für KMU, jedoch nur 34 % das eigene Risiko durch Cyberkriminalität betroffen zu sein.[43] Die IHK Nord gibt zudem an, dass bereits angegriffene Unternehmen die Lage bedrohlicher einschätzen als andere.[44] Weitere Umfragen berichten von hohen wahrgenommen Bedrohungen, jedoch ohne zwischen der Bedrohungswahrnehmung für die Allgemeinheit und der individuellen zu unterscheiden.[45] Einer Umfrage von Hiscox zufolge, geben 66 % der Befragten an, dass Cyber-Bedrohungen neben Betrug zu den stärksten Bedrohungen des Unternehmens zählen.[46]

Daneben gehen nur wenige Studien darauf ein, wovon sich Unternehmen konkret bedroht fühlen bzw. wie sich dieses äußert. Nach einer Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht fühlen sich Unternehmen vor allem von sonstigen IT-Angriffen (44 %), physischer Spionage (34 %), Daten-Spionage (31 %) und Social Engineering (16 %) gefährdet.[47] Cisco nennt Targeted Attacks (78 %), Advanced Persistent Threats (76 %) und die Ausweitung von Bring your own device (BYOD)-Praktiken als größte Sorgen von IT-Security-Entscheider*innen.[48] Dabei hat PwC festgestellt, dass sich die erhöhte Bedrohungslage vor allem durch das generelle Vorhandensein neuer Angriffsarten, die steigende Anzahl der Cyberangriffe und zusätzliche gesetzliche Vorgaben bemerkbar macht.[49] Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) hingegen hat die wahrgenommene Bedrohungslage u.a. durch den zunehmenden Schutzbedarf von Unternehmensdaten in 2012 und 2017 dargestellt. Hier werden insbesondere den Kunden-, Rechnungs-, Personal- und Prozessdaten in 2017 höhere Schutzbedarfe als noch in 2012 zugemessen.[50]

Insgesamt ergibt sich eine breite Spanne der durch Studien aufgezeigten Risikoeinschätzungen. Gründe hierfür können neben den in Abschnitt 2.2 genannten Einschränkungen auch Unterschiede in den jeweiligen Betrachtungszeiträumen, der Regionalität sowie nicht repräsentative Stichprobenziehungen sein.

2.4.3 Prävalenzen

In diesem Abschnitt werden die im Literaturstand identifizierten Häufigkeiten der Viktimisierung zusammenfassend dargestellt. Diese Prävalenzen beziehen sich stets auf einen definierten Zeitraum (z.B. Lebenszeitprävalenz, Jahresprävalenz, etc.) in dem die jeweiligen Unternehmen oder definierte Gruppen von Unternehmen (z.B. in Branchen, in Regionen) durch verschiedene Arten von Cyberangriffen im relevanten Maße getroffen wurden. Angaben hierzu wurden in 17

42 Vgl. PwC Strategy& GmbH (2016).

43 Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

44 Vgl. Industrie- und Handelskammer Nord e.V. (2013).

45 Siehe z.B. eco - Verband der Internetwirtschaft e.V. (2017). 95% der Unternehmen sehen eine (stark) wachsende Bedrohung; Vgl. auch techconsult (2017) Die Aussagen und Ergebnisse der Umfrage von Techconsult hinterlassen viele methodischen und inhaltliche Fragen. So wird beispielsweise angegeben, dass die gefühlte Bedrohung der IT- und Informationssicherheit zwischen 2014 und 2017 stetig zugenommen hat und der auf der eigenen Umfrage basierende Gefährdungsindex in dieser Zeit von 46 auf 50 anstieg, jedoch ohne auf die zugrundeliegende Operationalisierung einzugehen oder eine Orientierung zur Einschätzung der Höhe zu geben

46 Vgl. Hiscox (2018).

47 Vgl. Bollhöfer & Jäger (2018).

48 Vgl. Cisco (2017).

49 Vgl. PricewaterhouseCoopers AG WPG (2017).

50 Vgl. Hillebrand et al. (2017).

der 31 Studien identifiziert.[51] Sie wurden jeweils als Anteil der Unternehmen, die Opfer von Cyberangriffen wurden, in Prozent angegeben (%).

a) Angriffsarten

Eine der ersten und repräsentativen Umfragen in den Vereinigten Staaten befragte im Jahr 2005 fast 8.000 Unternehmen zu Cyberangriffen. Über alle Branchen und Angriffsarten gaben 67 % der befragten Unternehmen an, im Jahr 2005 mindestens einmal Opfer von Cyberangriffen geworden zu sein, wobei darunter sinngemäß zwischen den Angriffsarten Cyberkriminalität im engeren Sinne (z.B. Virus, Denial of Service, Sabotage: 44 % aller Unternehmen), Cyberkriminalität im weiteren Sinne (z.B. Betrug, Personal Data Breach: 8 % aller Unternehmen) und sonstige Vorfälle (z.B. Hacking, Phishing, Spyware: 15 % aller Unternehmen) unterschieden wurde.[52] Zu einer ähnlich hohen 12-Monatsprävalenz (66,5 %) kommen zehn Jahre später auch Paoli et al., allerdings für belgische Unternehmen. Sie unterscheiden zwischen den fünf nicht technischen Cyberkriminalitätsarten Illegaler Zugang (50 %), Data/System Interference (44 %), Cyber Extortion (24 %), Internet Fraud (13 %) und Cyber Espionage (4 %).[53] Gehem et al. haben in ihrer qualitativen Meta-Analyse von 65 Cybersecurity-Reports sehr unterschiedliche Ergebnisse festgestellt.[54] Je nach Autor der zugrundliegenden Studie unterschieden sich die vorkommenden Angriffsarten für 2013 und 2014 mitunter stark: Malware wurde beispielsweise von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) als die Top-Bedrohung eingestuft, während das russische Softwareunternehmen Kaspersky die Prävalenzrate bezüglich Malware mit rund 61 % (nach Spam mit ca. 65 %), die Internetseite Hackmageddon mit ca. 21 % und der US-Kommunikationskonzern Verizon mit ca. 12 % beziffert.[55]

Die Unternehmensberatung und Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers (PwC) kommt in zwei deutschen Studien zu folgenden Ergebnissen: in 2015 registrierten 56 % der befragten Unternehmen mindestens eine Cyber-Attacke[56], in 10 % (2015) bzw. 19 % (2016) der Fälle waren die Angriffe erfolgreich.[57] Nach einer Studie vom Bitkom aus 2018 gaben 68 % der Unternehmen an, dass sie in den letzten 24 Monaten von Vorfällen im Bereich Digitaler Wirtschaftsschutz betroffen waren, wobei der Diebstahl von IT- und Telekommunikationsgeräten (32 %), Diebstahl von sensiblen digitalen Daten (23 %) und analoger Diebstahl von Daten und Maschinen (21%) sowie digitale Sabotage von Systemen (19 %) die häufigsten Angriffsarten waren. Andere klassische Formen von Cyberangriffen wie beispielsweise digitales Social Engineering oder die Ausspähung digitaler Kommunikation waren hingegen nur mit 11 % vertreten.[58] Bei einigen Antwortkategorien fallen die schwierige Unterscheidbarkeit und Abgrenzung der zur Verfügung gestellten Antwortkategorien auf: So kann z.B. ein Diebstahl digitaler

[51] Offizielle Angaben zu Angriffen gegen Unternehmen sind schwierig aus der Polizeilichen Kriminalstatistik zu entnehmen, da nicht zwischen den Opfergruppen Unternehmen und Privatpersonen unterschieden wird. So greift das Bundeskriminalamt beispielweise auf externe Dunkelfelddaten, z.B. des Bitkoms, zurück um das Bundeslagebild Cybercrime darzustellen; Vgl. Bundeskriminalamt (2018).

[52] Vgl. Rantala (2008).

[53] Vgl. Paoli et al. (2018).

[54] Vgl. Gehem et al. (2015).

[55] Vgl. ebd.

[56] Vgl. PwC Strategy& GmbH (2016).

[57] Vgl. PricewaterhouseCoopers AG WPG (2017).; Eine Definition, was ein erfolgreicher Angriff sei, wurde nicht gegeben.

[58] Vgl. Bitkom e.V. (2018).

Daten auch durch den Diebstahl physischer Geräte bedingt sein. Unklar bleibt in vielen Studien auch, was genau unter einem Vorfall verstanden wird: Dies könnte aufgrund fehlender Definitionen sowohl ein registrierter Angriffsversuch ohne Folgen, ein abgewendeter Cyberangriff, ein tatsächlich eingetretener Schadensfall als auch lediglich eine IT-Störung sein.

Die Bitkom-Studie unterscheidet zwischen Betroffenheit und tatsächlichem Schadensanfall: Ein Anteil von 47 % der Industrieunternehmen haben in den letzten beiden Jahren einen Schaden durch digitale Angriffe erlitten. Die häufigsten drei Angriffsarten waren demnach Schadsoftware (24 %), das Ausnutzen von Software-Schwachstellen (16 %) und Phishing (16 %).[59]

Der GDV berichtet von einer Gesamt-Viktimisierungsrate von 30 %, wobei nicht weiter definierte Angriffe durch E-Mails (59 %) und Hackerangriffe (26 %) zu den häufigsten Angriffsarten gehören.[60] Hierbei ist zu beachten, dass die Betroffenheit mit dem Entstehen eines Schadens definiert wurde und generell kein Zeitraum angegeben wurde, in dem ein Schaden entstand. Zudem wurde nicht erläutert, welche Angriffsarten sich hinter den genannten „E-Mails" verbergen (z.B. Spam, Social-Engineering, etc.). Mit 33 % ist nach Angaben des (BSI) die Betroffenheit der befragten Unternehmen durch Cyber-Sicherheits-Vorfälle in 2018 ähnlich gering. Auch hier wurde die Betroffenheit nicht genauer definiert, allerdings wurde angegeben, dass in rund der Hälfte der Fälle die Angriffe erfolgreich waren, z.B. Zugang zu IT-Systemen hatten oder Funktionsweisen beeinflussten.[61] Auch die IHK Nord berichtet von einer nicht genauer definierten 12-Monats-Prävalenz von 33 %, allerdings für das Jahr 2013.[62] Stark nach oben abweichende Prävalenzen nennt das Ponemon-Institut für das Geschäftsjahr 2017. Demnach haben 98 % der befragten Unternehmen mit Malware, 69 % Phishing/ Social Engineering, 63 % Botnets, 43 % mit gestohlenen Geräten, 53 % mit Denial-of-Services-Angriffen, 40 % mit Insiderangriffen und 27 % der befragten Unternehmen mit Ransomware-Angriffen Erfahrungen gemacht.[63]

Der US-Kommunikationskonzern Verizon unterscheidet zwischen „Incident" und „Data Breaches",[64] nennt für die sogenannten Incidents aber vor allem Denial-of-Service-Angriffe (DoS) mit über 70 %, Losses due to errors mit ca. 15 % und Phishing mit unter 10 %.[65] Das amerikanische IT-Unternehmen IBM nimmt durch seine Dienstleistungen zur Überwachung von Kundeninfrastruktur einen eher technischen Fokus ein und nennt Unexprected Injections (79 %), Information Collection/Analysis (8 %) und Employment of Probabilistic Techniques (5 %) als wesentliche Angriffsmechanismen.[66] Das britische Versicherungsunternehmen Hiscox gab an, dass 45 % der Befragtem in den letzten 12 Monaten einen Cyberangriff erlitten, ohne jedoch die zugrundeliegenden Angriffsarten zu nennen oder genauer zu definieren, was

[59] Vgl. ebd.

[60] Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

[61] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2019a).

[62] Vgl. Industrie- und Handelskammer Nord e.V. (2013).

[63] Vgl. Ponemon Institute (2017b).

[64] Incident = Ein Sicherheitsevent, dass die Integrität, Verfügbarkeit oder Vertraulichkeit eines Informations-Vermögenswertes kompromittiert. Breach = Ein Incident, dass zu einer bestätigten Veröffentlichung der Informationen an unautorisierte Dritte führt.

[65] Vgl. Verizon (2018).; Alle Incidents wurden den Gruppen Error, Hacking, Malware, Misuse, Physical und Social zugeordnet.

[66] Vgl. IBM Cooperation (2018).

als Angriff gewertet wurde.[67] Klahr et al. nennen neben der 12-Monats-Prävalenz auch die Angriffsart, die den größten Schaden angerichtet hat (12 Mon. Prävalenz/Größter Schaden).[68] Dies waren vor allem betrügerische E-Mails oder Weiterleitungen auf betrügerische Webseiten (72 %/ 43 %), Malware oder Spyware (33 %/ 20 %), Others impersonating organisation in emails or online (27 %/ 12 %) und Ransomware (17 %/ 8 %).[69] Das Ponemon-Institut sieht in General Malware (77 %), Exploit of existing software vulnerability (75 %) und Web-borne malware attacks (64 %) die drei häufigsten Angriffsarten. Auffällig ist hier, dass Advanced Persistent Threats mit 51 % bereits an fünfter von elf genannten Stellen steht, was für solche hoch individualisierten und aufwandsintensiven Angriffe sehr viel erscheint.[70]

b) Branchen

Auch bei der Betroffenheit der Unternehmensbranchen zeigt sich ein heterogenes Bild. Während nach Rantala die Branchen Telekommunikation (82 %), Computer System Design (79 %) und die Herstellung langlebiger Güter (75 %) am stärksten sowie die Branchen Forst/Fischerei (44 %), Landwirtschaft (51 %) und Gastronomie (54 %) am wenigsten betroffen waren[71], nennen andere Studien abweichende Ergebnisse. Nach den Ergebnissen des UK Commercial Victimisation Surveys waren auf Basis unterschiedlicher Datensätze zwischen 2014 und 2017 die Branchen Administration und Support (36 %), Information/Kommunikation (23 %) und das produzierende Gewerbe (7,5 %) von „Online Crime“ am stärksten betroffen.[72]

Nach Angaben des Bitkom waren die am stärksten betroffenen Branchen Chemie und Pharma (74 %) sowie Automobilbau (68 %), wobei der Studienfokus hier auf Industrieunternehmen lag.[73] Das britische Versicherungsunternehmen Hiscox sieht bei den Branchen Finanzdienstleistungen, Energie, Telekommunikation und Regierungseinrichtungen die höchste Betroffenheit, ohne jedoch genauere Zahlen zu nennen.[74] Verizon fasst vor allem die Branchen Gesundheit (24 %), Hotel- und Gastronomie (15 %) sowie den öffentlichen Sektor (14 %) als Opfer zusammen,[75] und IBM nennt vor allem die Branchen Information- und Kommunikationstechnologie (33 %), produzierendes Gewerbe (18 %) und Finanzdienstleistungen (17 %) als Hauptziel von Angriffen.[76] Bei der Unterscheidung der Prävalenzen nach Branchen fällt auf, dass kaum einheitliche Branchendefinitionen, z.B. nach WZ08, NACE oder ISIC genutzt werden, was den direkten Vergleich dieser Studien so gut wie unmöglich macht.

c) Unternehmensgrößen

Die Prävalenzen nach Unternehmensgrößen zeigen ein vergleichsweise homogenes Bild: Größere Unternehmen werden häufiger angegriffen als kleinere Unternehmen. Das BSI gibt für 2018 an, dass 43 % der großen (>250 Mitarbeiter) und lediglich 26 % der kleinen und mittleren

67 Vgl. Hiscox (2018)..
68 Vgl. Klahr et al. (2017).
69 Vgl. ebd.
70 Vgl. Ponemon Institute (2016).
71 Vgl. Rantala (2008).
72 Vgl. Osborne et al. (2018).
73 Vgl. Bitkom (2018).
74 Vgl. Hiscox (2018).
75 Vgl. Verizon (2018).
76 Vgl. IBM Cooperation (2018).

Unternehmen (<250 Mitarbeiter) durch Cyber-Sicherheitsvorfälle betroffen waren, ohne jedoch genauer zu definieren, was ein Cyber-Sicherheitsvorfall konkret bedeutet.[77] Auch nach Rantala sind über alle Angriffsarten hinweg größere Unternehmen stärker betroffen als kleinere.[78] Hiscox stützt ebenfalls diese Beobachtung, macht aber auch deutlich, dass kein linearer Zusammenhang (je größer die Unternehmen, desto größer das Risiko) vorliegt. Vielmehr zeigen sich auch innerhalb der Gruppen große Unterschiede. So weisen Unternehmen mit bis zu 250 Mitarbeitern Prävalenzen zwischen 15 % und 55 % auf und Unternehmen mit über 250 Mitarbeitern Prävalenzen zwischen 60 % und 85 %.[79] Abweichend von der geteilten Beobachtung höherer Prävalenzraten bei größeren Unternehmen berichtet Bitkom, dass Industrieunternehmen mit mehr als 500 Mitarbeitern mit einem Anteil von 60 % weniger von Cyberangriffen betroffen sind als kleinere Unternehmen (10 bis 99 Mitarbeiter: 68 %; 100 bis 499 Mitarbeiter 73 %).[80] Das Mobilfunkunternehmen Verizon stellt dar, dass der überwiegende Teil (58 %) der betrachteten Data Breaches über alle Branchen hinweg bei den kleinen Unternehmen auftritt.[81] Die IHK Nord hingegen sieht keinen wesentlich Unterschied zwischen den beiden Richtungen und gibt an, dass „die Unternehmensgröße relativ wenig Einfluss auf die Angriffsrate hat“.[82]

d) Regionale Verteilung

Von vergleichsweise wenigen Studien werden regionale Unterschiede der Prävalenzen von Cyberangriffen gegen Unternehmen untersucht. Hiscox stellte in seinem Report 2018 fest, dass Unternehmen in Spanien am häufigsten betroffen waren (57 % der Vorfälle). Danach folgten die Niederlande (50 %), Deutschland (48 %), UK (40 %) und die USA (38 %).[83] Dies unterscheidet sich stark von dem Vorjahres-Report, in dem lediglich größere Unternehmen aus drei Ländern verglichen wurden: Danach waren US-amerikanische Unternehmen mit 72 % am stärksten betroffen, deutsche mit 65 % am zweitstärksten und britische mit 59 % am geringsten betroffen.[84] Auch Gehem et al. nennen in ihrer Meta-Untersuchung basierend auf Daten der Onlineplattform Hackmageddon für 2013 die USA als von Cyberangriffen am stärksten betroffenes Land (ca. 58 %), gefolgt von Großbritannien (ca. 14 %).[85]

Mit Blick auf die dargestellten Erkenntnisse des Forschungsstandes, lassen sich hinsichtlich der Prävalenzen, also der Betroffenheit von Unternehmen durch Cyberangriffe, kaum eindeutige Tendenzen erkennen. Vielmehr scheint, womöglich aufgrund verschiedener Definitionen, Vorgehensweisen und Stichproben, nahezu jede Aussage möglich.

77 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2019b).

78 Vgl. Rantala (2008): Viktimisierung von Unternehmen in 2005 über alle Angriffsarten: 2-24 Mitarbeiter (50%), 25-99 (59%), 100-999 (70%) und >1.000 Mitarbeiter (82%).

79 Vgl. Hiscox (2018).

80 Vgl. Bitkom e.V. (2018).

81 Vgl. Verizon (2018).

82 Vgl. Industrie- und Handelskammer Nord e.V. (2013).

83 Vgl. Hiscox (2018). Lediglich die fünf genannten Länder wurden betrachtet.

84 Vgl. Hiscox (2017). Lediglich die drei genannten Länder wurden betrachtet.

85 Vgl. Gehem et al. (2015).

2.4.4 IT-Sicherheitsstrukturen

Unter IT-Sicherheitsstrukturen werden alle technischen und organisatorischen Maßnahmen einer Organisation verstanden, um sich präventiv, kompensatorisch oder detektiv vor Cyberangriffen zu schützen. Angaben zu IT-Sicherheitsstrukturen finden sich in 25 der 31 Studien.

a) Generelle Selbsteinschätzung

Nach einer Umfrage des US-Telekommunikationsunternehmens Cisco unter mehr als 2.900 IT-Spezialist*innen, schätzen 58 % ihre Security Infrastruktur auf einem aktuellen Sicherheitsstand ein.[86] Auf ähnlichem Niveau, mit 54 %, schätzen die befragten Unternehmen nach Angaben des Ponemon Instituts ihre Cyber-Widerstandsfähigkeit als hoch bzw. sehr hoch ein.[87] Die Angaben des GDV liegen darüber: Demzufolge geben 74% der kleinen (10 bis 49 Mitarbeiter) und 63 % der mittleren Unternehmen (50 bis 249 Mitarbeiter) an, dass sie ausreichend gegen Cyberkriminalität geschützt sind.[88]

b) Technische Maßnahmen

Fast alle befragten Unternehmen nutzen nach Angaben des GDV Virenscanner und Firewalls (97 %), (automatische) Sicherheits-Updates (94 %) und systematische Datensicherungen (84 %).[89] Auch Hillebrand et al. sowie die IHK Nord kommen hier zu ähnlichen Ergebnissen.[90] Passwortgeschütze Zugänge für alle Mitarbeiter*innen (68 %), die Verschlüsselung sensibler Daten (54%) und das Verbot der Nutzung privater Geräte (41 %) sind hingegen weniger häufig implementierte Maßnahmen.[91] Auch nach Angaben einer Bitkom-Studie nutzen alle befragten Unternehmen Passwortschutz auf allen Geräten (100 %), Firewalls (100 %), Virenscanner (100 %) und regelmäßige Datensicherungen (100 %). Weniger häufig kommen u.a. Verschlüsselung von Datenträgern (47 %), verschlüsselter E-Mail-Verkehr (36 %), Penetrationstests (24 %) und Intrusion Detection Systeme (20 %) zum Einsatz.[92] Bollhöfer et al. sehen hier insbesondere bei der Verwendung von Penetrationtests und Krisensimulationen Abweichungen zur Bitkom-Studie. Diese liegen bei Unternehmen mit mehr als 50 Mitarbeiter*innen nur bei rund 16 %, bei weniger als 50 Mitarbeiter*innen sogar nur bei 5 % der befragten Unternehmen.[93] Nach Angaben von Cisco (2016) nutzten befragte Unternehmen lediglich zu 58 % Firewalls, 44 % Encryption/Data Protection, 42 % E-Mail/Messaging Security, 41 % Anti-Malware/ Endpoint Security, 40 % Access Control und 35 % Identity Administration.[94] Insbesondere die Angaben zur Nutzung von Firewalls und Anti-Virus-Lösungen weichen hier von den vorher genannten Studien ab. Das britische Marktforschungsinstitut Vanson Bourne sieht hingegen den

---

86 Vgl. Cisco (2017).

87 Vgl. Ponemon Institute (2016) Cyber-Widerstandsfähigkeit besteht hier aus den Einzel-Items Ability to contain a cyber-attack, Ability to quickly detect a cyber-attack, Ability to recover from a cyber-attack, Ability to prevent a cyber-attack und wurde auf einer Zehnerskala erfasst. Für diese Aussage wurden alle Angaben höher als sechs zusammengefasst.

88 Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

89 Vgl. ebd.

90 Vgl. Hillebrand et al. (2017).; Industrie- und Handelskammer Nord e.V. (2013).

91 Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

92 Vgl. Bitkom e.V. (2018).

93 Vgl. Bollhöfer & Jäger (2018).

94 Vgl. Cisco (2017).

Einsatz von Intrusion Detection/Prevention Systemen mit der Nutzung durch 56 % der befragten Unternehmen deutlich höher als Bitkom, wohingegen Anti-Virus (71 %) und E-Mail-Security Lösungen (70 %) unter den Angaben anderer Studien liegen.[95] Hinsichtlich der Nutzung von Multifaktor-Authentifizierung gibt Vanson Bourne einen Anteil von 43 % an, welchen PwC mit rund 51 % beziffert.[96] Osborne et al. stellen fest, dass die Nutzung von IT-Sicherheitsmaßnahmen nach Branche und Unternehmensgröße variieren können. Während die Nutzung von Anti-Virus Lösungen über alle Branchen und Unternehmensgrößen zwischen 80 % und 88 % liegt, werden Verschlüsselungssoftware (1-9 Mitarbeiter*innen: 40 %; >50 Mitarbeiter*innen: 66 %), Restriktionen von E-Mail- und Web-Nutzung (1-9 Mitarbeiter*innen: 33 %; >50 Mitarbeiter*innen: 80 %) und Restriktionen von Speichermedien (1-9 Mitarbeiter*innen: 26 %; >50 Mitarbeiter*innen: 63 %) im Groß- und Einzelhandelssektor von größeren Unternehmen deutlich häufiger eingesetzt als von kleinen Unternehmen. Über alle Unternehmensgrößen fällt insbesondere auf, dass Unternehmen der Land-, Forstwirtschaft und Fischerei weniger häufig über Data Security Richtlinien (13 %) verfügen, als beispielweise Unternehmen des Groß- und Einzelhandels (47 %). Auch bei den Maßnahmen Restriktionen von E-Mail- und Web-Nutzung sowie Restriktionen von Speichermedien unterscheiden sich diese beide Branchen mindestens um den Faktor zwei.[97] Der Sicherheitsmonitor 2016 von Deutschland sicher im Netz e.V. (DsiN) fasst für kleine und mittlere Unternehmen zusammen, dass zur Erlangung von IT-Sicherheit nach wie vor technische Einzellösungen überwiegen und es an ganzheitlichen Ansätzen mangelt.[98]

c) Organisatorische Maßnahmen

Rantala fragt in ihrer Studie nicht das Vorhandensein von IT-Sicherheitsmaßnahmen, sondern die Aufdeckung von Vorfällen durch diese Maßnahmen in den befragten Unternehmen ab. Alle abgefragten internen Maßnahmen die Vorfälle aufgedeckt haben, wie z.B. Richtlinien für Mitarbeiter*innen (60 %), Network Watch-Center (71 %), Intrusion Testing (63 %), Mitarbeiter Training (59 %) und Business Continuity Plan (60 %), lagen zwischen 59 % und 71 % relativ nah beieinander. Die scheinbar einzige Maßnahme, die zu weniger Entdeckungen bzw. Wahrnehmungen von Vorfällen führte, ist „Other“ (34 %), welche die Limitierung von Systemzugängen, automatisches Patch-Management und Maßnahmen zur Erfüllung des Sorbanes-Oxley-Acts beinhaltet.[99] Kritisch hieran ist vor allem die Zuordnung einer konkreten Maßnahme zu einer Aufdeckung durch die befragte Person sowie der Umstand zu sehen, dass nicht alle Maßnahmen darauf ausgelegt sind, Vorfälle aufzudecken, sondern insbesondere im Falle von Patch-Management und der Limitierung von Zugängen, Vorfälle zu verhindern. Bitkom gibt an, dass die befragten Industrieunternehmen u.a. folgende organisatorische Maßnahmen umsetzen: Festlegung von Zugriffsrechten für bestimmte Informationen (100 %), eindeutige Klassifizierung von Betriebsgeheimnissen (84 %), Regelungen für die Mitnahme von IT-Geräten auf Geschäftsreisen (66 %), Clean-Desk-Policy (50 %), Sicherheitszertifizierungen z.B.

95 Vgl. Vanson Bourne (2014).

96 Vgl. PricewaterhouseCoopers Network (2018).

97 Vgl. Osborne et al. (2018).

98 Vgl. Brandl et al. (2016).

99 Vgl. Rantala (2008).

nach ISO 27001 oder BSI Grundschutz (49 %), Einführung eines Informationssicherheits-Managementsystems (35 %)[100] und regelmäßige Sicherheits-Audits (34 %). Sicherheitsvorkehrungen im Bereich Personal sind u.a. Background-Checks zur Besetzung sensibler Positionen (59 %), Schulungen zu Sicherheitsthemen (59 %) und Hinweis-Geber-Systeme (22 %).[101] Die Nutzung von Audits/Reporting gibt Vansom Bourne abweichend vom Bitkom mit 56 % an, wohingegen Schulungen der Benutzer ähnlich hoch mit 56 % Nutzung unter den befragten Unternehmen angegeben werden.[102] Klahr et al. beziffern die Teilnahme von Mitarbeitern an Trainings für die letzten 12 Monate auf lediglich 20 % insgesamt, wobei sich hier sowohl zwischen Branchen und Unternehmensgrößen mitunter deutliche Unterschiede ergeben. Über diese Maßnahmen hinaus nennen Klahr et al. u.a. noch die Restriktion von Benutzerzugängen (alle Unternehmen: 79 %; große Unternehmen 96 %), die Überwachung von Benutzeraktivitäten (alle Unternehmen: 42 %; große Unternehmen 80 %) und das Vorhandensein formaler Cyber Security Richtlinien (alle Unternehmen: 33 %; große Unternehmen 71 %).[103]

Wie bereits unter den Einschränkungen im Abschnitt 2.2 erläutert, können auch in diesem Abschnitt nicht immer eindeutige Unterscheidungen der genannten Sicherheitsmaßnahmen vorgenommen werden. So fassen manche Studien beispielsweise die Maßnahme „Verschlüsselung" zu einem Oberbegriff zusammen,[104] während andere hierunter die Verschlüsselung von Netzwerkverbindungen (80 %), Verschlüsselung von Datenträgern (54 %) und E-Mailverschlüsselung (45 %) unterscheiden, deren Ausprägungen wie in diesem Beispiel aufgezeigt sehr unterschiedlich ausfallen können.[105] Zudem fällt auf, dass die bestehenden Studien die genannten Sicherheitsmerkmale sehr selten in einen direkten Zusammenhang mit den Prävalenzen setzen, sondern beides unabhängig voneinander darstellen.

2.4.5 Investitionen und Budgets

In diesem Abschnitt wird dargestellt welche Investitionen in Informations- und Cyber-Sicherheit die befragten Unternehmen bereits getätigt haben bzw. noch tätigen wollen und welche finanziellen Mittel dafür zur Verfügung stehen bzw. zur Verfügung standen. Angaben zu Investitionen und Budgets wurden in 13 der 31 Studien identifiziert.

Ebenso weisen die einbezogenen Studien bezüglich der Thematik Investitionen in Informations- und Cyber-Sicherheit unterschiedliche Ergebnisse auf. Für 2016 berichtet PwC, dass 51 % der befragten Unternehmen steigende und 35 % unveränderte Investitionen für Informationssicherheit im aktuellen Jahr erwarten,[106] während in einer weiteren PwC Studie 67 % der

[100] Nach Angaben des Bundesamt für Sicherheit in der Informationstechnik (2019a) verfügen 47% der Befragten über ein Informationssicherheits-Managementsystem (ISMS), davon 61% der großen und 37% der kleinen und mittleren Unternehmen.

[101] Vgl. Bitkom e.V. (2018).

[102] Vgl. Vanson Bourne (2014).

[103] Vgl. Klahr et al. (2017).

[104] Siehe z.B. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018)., Cisco (2017), eco - Verband der Internetwirtschaft e.V. (2017).

[105] Vgl. Bundesdruckerei GmbH (2017). Unter anderem auch Hillebrand et al. (2017) und Bitkom e.V. (2018) unterscheiden ähnliche Verschlüsselungsarten.

[106] Vgl. PricewaterhouseCoopers AG WPG (2017) Die der Umfrage zugrundeliegende Stichprobe enthält Unternehmen von 200 bis 1.000 Mitarbeitern.

Unternehmen von steigenden und 24 % von gleichbleibenden Investitionen ausgehen.[107] Eine Definition, was solche Investitionen umfassen, erfolgt hingegen nicht. Der eco – Verband der Internetwirtschaft e. V. berichtet für 2017 ebenfalls von überwiegend steigenden Investitionen (61 %) ohne jedoch anzugeben, ob dies erwartete oder tatsächliche Entwicklungen sind.[108] Allerdings stellte PwC fest, dass die tatsächlichen Investitionen den von Unternehmen geäußerten höheren Investitionserwartungen mitunter deutlich unterlagen. Als Gründe für Investitionen äußerten die befragten Unternehmen der PwC-Studie vor allem regulatorische Anforderungen (76 %), die Digitalisierung (74 %) und Kundenanforderungen (66 %), während aktuelle Sicherheitsvorfälle im eigenen Unternehmen (46 %) und der eigenen Branche (37 %) die letzten Plätze belegten.[109] Klahr et al. haben hiervon abweichende Ergebnisse zu den Gründen für Investitionen festgestellt. Die anteilig am häufigsten genannten Gründe waren demnach der Schutz von Kundendaten (51 %), der Schutz von geistlichem Eigentum bzw. Geschäftsgeheimnissen (28 %) und Business Continuity (19 %). Erst auf Platz sieben folgten Compliance Gründe mit einem Anteil von 7 %.[110] Demgegenüber berichtet das Ponemon Institut, dass 66 % der befragten Unternehmen Investitionen in IT-Sicherheit vor allem zur Aufrechterhaltung der Verfügbarkeit von Systemen und 46 % aus Compliance-Gründen tätigen, aber nur 35 % aus Angst vor Datenverlust- oder Diebstahl und nur 6 % aufgrund von befürchteten Umsatzrückgängen.[111]

Klahr et al. merken diesbezüglich an, dass Investitionen sowie deren Begründungen nach Unternehmensgröße und Branche variieren. So gaben beispielsweise die Branchen Information/ Kommunikation/ Versorgung durchschnittlich 19.500 Britische Pfund (GBP), das Gastgewerbe jedoch nur 620 GBP im letzten Geschäftsjahr für Hardware, Software, Gehälter, Training und Outsourcing mit Bezug zu Cybersecurity aus.[112] Auch die Bundesdruckerei berichtet, dass die Mehrheit (56 %) der deutschen Unternehmen höhere Investitionen in IT-Sicherheit tätigen wird. Rund ein Drittel der Unternehmen mit mehr als 2.000 Mitarbeitern gaben an, Investitionen sogar stark auszubauen, wohingegen Unternehmen mit weniger als 100 Mitarbeitern dies nur zu 18% tun. Vor allem die Branchen Energie/Versorgung (75 %), Transport/Logistik (75 %) und Banken/ Versicherungen (62 %) berichten von zunehmenden Investitionen, während dies lediglich von 40 % der Unternehmen der Branche Maschinen- und Anlagenbau angeben wird.[113] Ungeklärt bleibt, ob und welche Branchen womöglich bereits ein höheres Sicherheitsniveau aufweisen und daher weniger stark investieren. Zudem werden bestimmte Branchen vermutlich stärker durch regulatorische Anforderungen zur Investition bewegt als andere (z.B. durch das IT-Sicherheitsgesetz oder ausländische Äquivalente).

Hillebrand et al. nennen konkrete Zahlen in EUR, merken jedoch an, dass die Ergebnisse aufgrund der geringen Auskunftsbereitschaft der befragten KMU zurückhaltend zu bewerten sind. Für 2017 planten die KMU durchschnittlich 2.600 EUR für Ausgaben im Bereich IT-Sicherheit, wobei mit der Unternehmensgröße auch die Investitionshöhe steigt. Insgesamt planten nur ca.

[107] Vgl. PwC Strategy& GmbH (2016). Die der Umfrage zugrundeliegende Stichprobe enthält Unternehmen mit einem bis >10.000 Mitarbeitern.

[108] Vgl. eco - Verband der Internetwirtschaft e.V. (2017).

[109] Vgl. PricewaterhouseCoopers AG WPG (2017).

[110] Vgl. Klahr et al. (2017).

[111] Vgl. Ponemon Institute (2016).

[112] Vgl. Klahr et al. (2017).

[113] Vgl. Bundesdruckerei GmbH (2017).

2 % der KMU Investitionen von über 10.000 EUR im Geschäftsjahr 2017.[114] Klahr et al. nennen höhere Investitionen, allerdings in Britischen Pfund. Demnach gaben britische Unternehmen im Durchschnitt 4.590 GBP (Median 200 GBP) im letzten Geschäftsjahr aus, wobei rund ein Drittel der Unternehmen gar keine Investments in Cybersecurity tätigten.[115]

Nach Angaben von Hillebrand et al. machen IT-Sicherheitsausgaben rund 11 % des IT-Budgets von KMU aus.[116] Einem Bericht des britischen Marktforschungsinstituts Vanson Bourne zufolge liegt dieser Anteil für große Unternehmen bei durchschnittlich 12 %, wenn das Unternehmen noch keine Datenpanne erfahren hat. Nach einer solchen Datenpanne liegt der Anteil des IT-Sicherheitsbudgets bei 18 % des IT-Budgets. Insgesamt macht das IT-Budget der befragten Unternehmen rund ein Fünftel des Jahresumsatzes aus.[117] Diese Aufteilung des IT-Sicherheitsbudgets ist aber nicht bei allen Unternehmen gegeben. Bei 55 % der befragten Unternehmen ist das Budget für Sicherheit zwar im IT-Budget enthalten, jedoch berichten 36 % der Unternehmen, dass dies nur zum Teil der Fall ist. Immerhin 9 % der Unternehmen trennen das Sicherheits- und das IT-Budget vollständig.[118]

Auf die Frage wofür Unternehmen, deren Investitionen in den letzten 12 Monaten zunahmen, Geld ausgaben, nannten die befragten Unternehmen der Vanson Bourne-Studie vor allem Training der Mitarbeiter*innen (67 %), Cloud Security (58 %) und Monitoring Services (54 %). Die Investitionen Outsourcing Software (40 %), Outsourcing Infrastructure (39 %), Outsourcing Services (39 %) und Outsourcing Staff (35 %) wurden hingegen zuletzt genannt.[119] Das Ponemon Institut geht noch einen Schritt weiter und hat für neun abgefragte Investitionen einen geschätzten Return-On-Investment (ROI) berechnet. Demnach waren Investitionen in Security Intelligence Systeme (ROI: 21,5 %), Advanced Identity and Access-Lösungen (ROI: 19,7 %) und Automation, Orchestration und Machine-Learning (ROI: 17,1 %) besonders rentabel, während Enterprise Deployment of Governance, Risk and Compliance (ROI: 9,4 %) und Automated Policy Management (ROI: 6,9 %) auf den letzten Plätzen landeten.[120] Interessanterweise scheinen sich alle Investitionen in die neun genannten Technologien, vorbehaltlich des Vergleiches mit einem unternehmensinternen Zinssatz, für die Unternehmen zu lohnen.

Auch für die dargestellten Budgets und Investitionen zeigt der Literaturstand ein uneinheitliches Bild. Zwar könnte man tendenziell steigende Investitionen erkennen, allerdings bleibt offen, auf welchem Niveau und in welchen Bereichen dies der Fall ist.

2.4.6 Schäden und Konsequenzen

In diesem Abschnitt wird dargestellt, welche negativen, direkten oder indirekten Auswirkungen Cyberangriffe gegen Unternehmen haben, die nicht in Geldeinheiten (z.B. EUR, GBP oder

[114] Vgl. Hillebrand et al. (2017).

[115] Vgl. Klahr et al. (2017) Unterschiede nach Größenklassen (Mittelwert/Median in GBP): 2-49 Mitarbeiter 2.600/200; 50-249 Mitarbeiter 15.500/5.000; >250 Mitarbeiter 387.000/21.200.

[116] Vgl. Hillebrand et al. (2017).

[117] Vgl. Vanson Bourne (2014).

[118] Vgl. Cisco (2017).

[119] Vgl. Vanson Bourne (2014).

[120] Vgl. Ponemon Institute (2017b). Für die Ermittlung des ROI wurden die Erträge durch die Kosten des Investments geteilt. Zudem wurde eine Laufzeit von 3 Jahren, ein Discount-Zins von 2% p.a. und kein Residualwert unterstellt. Kosten für Betrieb und Wartung wurden aussagegemäß konservativ berücksichtigt.

USD) ausgedrückt werden. Angaben hierzu finden sich in 17 der 31 Studien. Auch im Bereich der Schäden und Konsequenzen von Cyberangriffen fallen häufig uneinheitliche Definitionen und Antwortmöglichkeiten der betrachteten Studien auf, was einen direkten Vergleich der vorliegenden Erkenntnisse erschwert oder sogar verhindert.

Nach Angaben des GDV nannten die befragten Unternehmen als wirtschaftliche Schäden durch Cyberangriffe vor allem Kosten für Wiederherstellung und Aufklärung (59 %), Betriebsunterbrechungen (43 %), Reputationsschäden (14 %), Diebstahl von Kundendaten (11 %) und Diebstahl von eigenen Daten/Betriebsgeheimnissen (8 %).[121] Abweichend dazu berichtet das BSI an erster Stelle von Betriebsstörungen, die bei 87 % zu Kosten geführt haben und erst danach von Kosten für Wiederherstellung (65 %).[122] Nach Angaben von Cisco hat ca. ein Fünftel der Unternehmen einen Kunden- und fast 30 % einen Umsatzverlust infolge eines Cyberangriffes erlitten.[123] Hiscox gibt hingegen an, dass nur 7 % der von einem Data Breach betroffenen Unternehmen Kund*innen verloren haben.[124] Von den Unternehmen die Kund*innen verloren, waren es nach Angaben von Cisco in 60 % der Fälle weniger als 20 % der Kund*innen, wobei rund 5 % der Unternehmen angaben, zwischen 80-100 % der Kund*innen verloren zu haben. Dieselben Größenordnungen (± 2 %) gelten für verlorene Umsätze.[125] Bitkom nennt, allerdings mit Fokus auf Wirtschaftsschutz, abweichende aufgetretene Schadensfälle. Imageschäden bei Kund*innen und Lieferant*innen (41 %) werden am häufigsten genannt, gefolgt von nicht weiter definierten, datenschutzrechtlichen Maßnahmen (40 %) und dem Ausfall/Diebstahl/Schädigung von Informationssystemen (27 %). Auch die Kosten für Ermittlungen und Ersatzmaßnahmen (16 %) werden deutlich seltener genannt als z.B. beim GDV.[126] Ebenfalls abweichend zu den Studien vom GDV und Bitkom, allerdings mit dem Fokus auf die teuersten Konsequenzen, nennt das Ponemon-Institut Informationsverlust (43 %), Betriebsunterbrechungen (33 %), Umsatzverlust (21 %) und Schäden an Equipment (3 %) als Schäden, die bei den befragten Unternehmen auftraten.[127] Neben den bereits genannten, durchaus häufiger auftretenden Folgen durch Cybervorfälle, geben Klahr et al. an, dass der Diebstahl von Geld (6 %) und der Verlust bzw. Diebstahl von Vermögenswerten, Betriebsgeheimnissen oder geistlichem Eigentum (1 %) relativ selten bei den befragten Unternehmen vorkamen. Auch der Einfluss durch Cybervorfälle der letzten 12 Monate auf die Gesamtorganisation in Bezug auf Kundenbeschwerden (5 %), Reputationsschäden (4 %), Umsatz- oder Aktienkursverluste (4 %) und Strafen oder Rechtskosten (<1 %) wurden eher selten genannt.[128] Allerdings geben Klahr et al. auch an, dass die angegebenen Folgen nach Unternehmensgröße variieren.[129]

[121] Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

[122] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2019a).

[123] Vgl. Cisco (2017).

[124] Vgl. Hiscox (2018).

[125] Vgl. Cisco (2017).

[126] Vgl. Bitkom e.V. (2018).

[127] Vgl. Ponemon Institute (2017b).

[128] Vgl. Klahr et al. (2017).

[129] Vgl. ebd.

Rantala berichtet in ihrer repräsentativen Befragung von US-Unternehmen für 2005,[130] dass in Unternehmen über alle Branchen und Größenklassen hinweg im Median eine System-Ausfallzeit von 16 Stunden bestand, der durch Sicherheitsvorfälle verursacht wurde. Bei 40 % der Unternehmen betrug der Ausfall 25 Stunden oder länger. Die längsten Ausfallzeiten wies die Branche Herstellung von Gebrauchsgütern mit einem Median von 32 Stunden auf.[131] Insgesamt wurde weder ausgewiesen, welche Angriffsarten zu diesen Ausfällen führten, noch wie sich die Ausfallzeiten auf die entsprechenden Unternehmensgrößen verteilen oder welche Art von Systemen ausfielen.

Das US-Telekommunikationsunternehmen Cisco gibt an, dass 13 % der befragten Unternehmen durch Sicherheitsverstöße weniger als eine Stunde Systemausfallzeiten hatten. Rund 45 % der Unternehmen meldeten Ausfallzeiten zwischen einer und acht Stunden und bei 9 % der befragten Unternehmen überstieg die Ausfallzeit 24 Stunden. Zum überwiegenden Teil (60 %) waren nicht mehr als rund ein Drittel der Systeme eines Unternehmens durch einen Vorfall betroffen, in 15 % der Fälle fielen hingegen mehr als die Hälfte der Systeme des Unternehmens aus.[132]

Das Ponemon-Institut zeigt auf, wie viele Tage es durchschnittlich dauerte, Cyberangriffe bestimmter Angriffsarten zu überwinden. Demnach dauerten Konsequenzen durch einen bösartigen Code (55,2 Tage), böswillige Innentäter*innen (50 Tage) und Ransomware (23,1 Tage) am längsten an, wohingegen Angriffe durch Malware (6,4 Tage) und Botnets (2,5 Tage) verhältnismäßig schnell gelöst werden konnten.[133] Nach Angaben von Klahr et al.[134] haben 57 % der britischen Unternehmen nach dem schwerwiegendsten Vorfall der vergangenen 12 Monate überhaupt keine Zeit gebraucht, um eine normale Betriebsfähigkeit wiederherzustellen. Weitere 23 % der befragten Unternehmen konnten diese innerhalb eines Tages und weitere 13 % innerhalb einer Woche wiederherstellen. Nur bei 2 % der Unternehmen dauerte es einen Monat oder länger. Ähnlich wie Klahr et al. stellen Paoli et al. fest, dass die Unternehmen die Mehrheit der Cyberangriffe (Illegaler Zugang: 81,7 %; Daten/System-Beeinträchtigung: 79,6 %; Cyber-Erpressung: 68,2 %) innerhalb eines Arbeitstages bewältigen konnten.[135] Mit dem Fokus auf Wirtschaftsspionage und Konkurrenzausspähung sagen Bollhöfer et al. aus, dass die Auswirkungen von Vorfällen bei 39 % der befragten Unternehmen keine Einschränkungen mit sich führten bzw. kurzfristig behebbar waren (38 %).[136] Insgesamt 5 % der betroffenen Unternehmen berichten hier von existenzbedrohlichen Auswirkungen. Bezogen auf KMU geben Hillebrand et al. an, dass Beeinträchtigungen durch IT-Sicherheitsprobleme entweder nicht vorhanden bzw. geringfügig waren (31 %) oder weniger als einen Tag betrugen (41 %).[137]

Wie der Literaturstand zum Thema Schäden und Konsequenzen aufzeigt, existiert eine Vielzahl negativer Folgen für Unternehmen, mit unterschiedlichen Ausprägungen. Obwohl die gefühlte

[130] Vgl. Rantala (2008).

[131] Vgl. ebd.

[132] Vgl. Cisco (2017).

[133] Vgl. Ponemon Institute (2017b).

[134] Vgl. Klahr et al. (2017).

[135] Vgl. Paoli et al. (2018).

[136] Vgl. Bollhöfer & Jäger (2018).

[137] Vgl. Hillebrand et al. (2017).

Bedrohung durch Cyberangriffe sehr akut sein mag, berichtet tendenziell die Mehrzahl der Unternehmen von verhältnismäßig überschaubaren Schäden, was die Brisanz des Phänomens, gerade aus Sicht stark betroffener Unternehmen, keinesfalls mindern sollte.

2.4.7 Entstandene Kosten

In diesem Abschnitt werden für den ausgewählten Literaturstand Kosten, ausgedrückt in Geldeinheiten (z.B. EUR, GBP oder USD), die im Zusammenhang mit Cyberangriffen gegen Unternehmen entstanden sind, dargestellt. Konkrete Angaben dazu werden in 13 von 32 Studien gemacht.

Die Bitkom-Studie sieht auf Basis einer Hochrechnung, allerdings mit Fokus auf digitale Wirtschaftsspionage, Sabotage und Datendiebstahl, Gesamtschäden bei Industrieunternehmen in den vergangenen zwei Jahren von rund 43 Mrd. EUR. [138] Davon machen Imageschäden (8,8 Mrd. EUR), Patentrechtsverletzungen (8,5 Mrd. EUR) und der Ausfall, Diebstahl, Schädigung von Systemen und Betriebsabläufen (6,7 Mrd. EUR) die größten sowie Datenschutzrechtliche Maßnahmen (1,4 Mrd. EUR), Erpressung mit gestohlenen/ verschlüsselten Daten (0,3 Mrd. EUR) und sonstige Schäden (0,3 Mrd. EUR) die kleinsten Positionen aus.[139] Die Schäden werden allerdings nicht für verschiedene Branchen, Unternehmensgrößen oder Angriffsarten, sondern lediglich als Gesamtschaden dargestellt. Zudem werden alle Kostenarten ohne Berücksichtigung von möglichen Kumulations- oder Verteilungseffekten addiert und mithilfe der Prävalenzrate für die Anzahl der deutschen Industrieunternehmen hochgerechnet. PwC berichtet für Unternehmen mit 200 bis 1.000 Mitarbeiter*innen, dass rund 36 % der Befragten finanzielle Auswirkungen erlitten. Dabei belief sich die Höhe des monetären Schadens auf durchschnittlich 41.000 EUR, wobei auch hier keine weiteren strukturellen Merkmale differenziert wurden.[140] Da insbesondere bei monetären Schäden von einer großen Spannweite ausgegangen werden kann, und der Mittelwert stark von Extremwerten abhängt, ist die Aussagekraft des berichteten Durchschnittsschadens ohne zusätzliche Angaben (z.B. Standardabweichung) sehr vorsichtig zu interpretieren.

Paoli et al. unterscheiden vier Kostenkomponenten sowie vier Cyberkriminalitätstypen, jeweils bezogen auf den letzten Vorfall, auf alle Vorfälle insgesamt und vereinzelnd auf den schwerwiegendsten Vorfall.[141] Für den letzten Vorfall von illegalem Zugang beliefen sich die internen Personalkosten in 44,2 % der Fälle auf weniger als 69 EUR, Hard- und Software-Ersatzkosten zu 55,6 % auf 0 EUR und zu 35,8 % der Fälle auf unter 10.000 EUR sowie Straf- und Ausgleichzahlungen zu 90,7 % auf 0 EUR und zu 4 % der Fälle auf unter 10.000 EUR.[142] Zusammenfassend kommen Paoli et al. zu dem Ergebnis, dass nur eine Minderheit der befragten Unternehmen von schwerwiegenden finanziellen Schäden berichten[143] und sich Unterschiede, insbesondere zu Studien kommerzieller Autor*innen bzw. Herausgeber*innen, ergeben.[144] Nach

[138] Vgl. Bitkom e.V. (2018).

[139] Vgl. ebd.

[140] Vgl. PricewaterhouseCoopers AG WPG (2017).

[141] Vgl. Paoli et al. (2018).

[142] Vgl. ebd.

[143] Dies berichten auch Klahr et al. (2017).

[144] Vgl. Paoli et al. (2018).

Angaben von Klahr et al. ist es für Unternehmen grundsätzlich eher unüblich finanzielle Schäden von Cybersecurity-Vorfällen systematisch zu erfassen, (nur rund 6 % der befragten Unternehmen täten dies),[145] was auch ein Grund für das eingeschränkte Antwortverhalten vieler Unternehmen sein könnte. In der Befragung von rund 1.500 britischen Unternehmen kommen Klahr et al. zu dem Ergebnis, dass für alle Vorfälle der letzten 12 Monate über alle Unternehmen durchschnittliche Kosten von 1.570 GBP sowie Kosten für große Unternehmen von 19.600 GBP anfielen. Der Median über alle Unternehmen liegt hingegen bei 0 GBP, was zeigt, dass eine Mehrheit der Unternehmen gar keine finanziellen Schäden meldete.[146] Deutlich höher gibt Vanson Bourne die Kosten der Sicherheitsverstöße des vergangenen Jahres für Unternehmen ab 500 Mitarbeiter*innen für den globalen Durchschnitt an. Demnach erlitten Unternehmen Schäden von über 917.000 USD.[147] Allerdings wird an dieser Stelle weder auf strukturelle Unterschiede, noch die genaue Zusammensetzung dieser Kosten eingegangen.

Rantala et al. geben für ihre Befragung aus 2005 an,[148] dass über alle Angriffs- bzw. Vorfallsarten und Unternehmensgrößen monetäre Verluste mit einem Median von ca. 6.000 USD entstanden. Insbesondere Cyber-Unterschlagung/Veruntreuung (Median 50.000 USD) und der Diebstahl geistigen Eigentums (Median 43.000 USD) wogen besonders schwer, während durch Computer-Viren (Median 5.000 USD) und Denial-of-Service-Angriffe (Median 5.000 USD) weniger finanzielle Schäden verursacht wurden. Rund 51 % der Unternehmen hatten finanzielle Schäden zwischen 1.000 und 9.000 USD zu verkraften, wobei nur 13 % mehr als 100.000 USD Schäden meldeten. Insbesondere die Branchen Finanzen (29 %) und Versicherungen (20 %) gaben relativ häufig an, finanzielle Schäden in Höhe von mindestens 100.000 USD erlitten zu haben.[149] Wie sich diese finanziellen Verluste zusammensetzen, wurde nicht dargestellt.

Das Ponemon Institut weist in seinem Bericht darauf hin, dass sich Kosten für Datenpannen[150] zwischen bestimmten Regionen und Branchen unterscheiden können. Auf Basis eines Vorfalls nachgelagerten Aktivitäten, die in direkte, indirekte und Opportunitätskosten unterschieden, jedoch leider nicht offengelegt werden, gibt das Institut an, dass in 2017 die durchschnittlichen Gesamtkosten pro Unternehmen 3,62 Mio. USD betrugen. Dabei sind Vorfälle in US-amerikanischen Unternehmen deutlich teurer (7,35 Mio. USD) als z.B. in Deutschland (3,68 Mio. USD) oder Brasilien (1,52 Mio USD). Die Kosten pro kompromittierten Datensatz werden für 2017 in den Branchen Gesundheit (380 USD), Finanzwesen (245 USD) und Dienstleistungen (223 USD) am höchsten und in den Bereichen Medien (119 USD), Forschung (101 USD) und dem öffentlichen Sektor (71 USD) am geringsten angegeben.[151] In einem weiteren Bericht stellt das Ponemon-Institut die durchschnittlichen Cyberkriminalitätskosten der letzten drei Jahre je Quartil der Anzahl der Arbeitsplätze mit Netzwerkzugang dar. Demnach entstanden den 254 befragten Unternehmen in 2017 hohe Kosten (Quartil 1(kleinste Unternehmen): USD 3,6 Mio.; Q2: USD 5,7 Mio.; Q3: USD 10 Mio.; Q4: Mio. 16,9 USD), die seit 2013 mit Ausnahme des

145 Vgl. Klahr et al. (2017).

146 Vgl. ebd.

147 Vgl. Vanson Bourne (2014).

148 Vgl. Rantala (2008)..

149 Vgl. ebd.

150 Ponemon definiert einen Data Breach sinngemäß als Ereignis, durch das personenbezogene Daten (z.B. medizinische Daten, Kreditkartendaten etc.) im elektronischen oder nicht-elektronischen Format möglicherweise gefährdet werden.

151 Vgl. Ponemon Institute (2017a).

vierten Quartils permanent zugenommen haben. Pro Arbeitsplatz mit Netzwerkzugang wird dargestellt, dass die durchschnittlichen Kosten in kleinen Unternehmen höher ausfallen, als in großen Unternehmen (Q1: 1.726 USD; Q2: 975 USD; Q3: 655 USD; Q4: 436 USD).[152] Neben den vom Institut genannten Einschränkungen dieser Umfrage (z.B. keine Repräsentativität, Sampling-Frame Bias, nicht berücksichtigte Faktoren, geschätzte Kosten/einfache Hochrechnungen) kann zudem die fehlende Transparenz der Kostenbestandteile sowie Kalkulationsschritte angeführt werden.

Der britische Versicherer Hiscox führt für deutsche Unternehmen geschätzte durchschnittliche Kosten der Cybersecurity-Vorfälle der letzten 12 Monate an. Darin zeigt sich, dass größere Unternehmen auch höhere Kosten melden (< 250 Mitarbeiter*innen: 55.067 USD; 250 bis 999 Mitarbeiter*innen: 406.653 USD; > 1.000 Mitarbeiter*innen: 640.408 USD). Auch die durchschnittlichen Kosten des schwersten Cybersecurity-Vorfalls der letzten 12 Monate weisen diese Tendenz auf (< 250 Mitarbeiter*innen: 11.918 USD; 250 bis 999 Mitarbeiter*innen: 86.834 USD; > 1.000 Mitarbeiter*innen: 150.891 USD).[153] Romanosky wählt ein anderes Vorgehen zur Erhebung der Kosten durch Cyberangriffe und wertet Fälle einer kommerziellen Datenbank zu öffentlich gemeldeten Cyber-Vorfällen aus, die er nach vier Angriffs- bzw. Vorfallsarten unterscheidet.[154] Im Durchschnitt entstanden durch Phishing die höchsten unternehmensinternen Kosten (USD 20 Mio.; Median: USD 0,3 Mio.), gefolgt von Privacy Violations (USD 10,1 Mio.; Median: USD 1,3 Mio.), Sicherheitsvorfällen (USD 9,1 Mio.; Median: USD 0,35 Mio.) und Data Breaches (USD 5,9 Mio.; Median: USD 0,1 Mio.). Mithilfe von Regressionsanalysen stellt er fest, dass die Unternehmensgröße gemessen in Umsatz und die Anzahl der betroffenen Datensätze signifikant mit der Höhe der entstandenen Schäden zusammenhängen. Insgesamt schätzt er, dass die Verluste im Durchschnitt nur 0,4 % des Jahresumsatzes betragen und damit deutlich hinter anderen Bedrohungen für das Unternehmen (z.B. Betrug, Korruption, Diebstahl und Forderungsausfälle) liegen.[155]

Verlässliche Daten, besonders unterschieden nach einzelnen Kostenbestandteilen zu verursachten Kosten durch Cyberangriffe, sind schwierig in der Literatur zu finden. Ähnlich zu den gemeldeten Schäden ergibt sich auch hier eine breite Spanne gemeldeter Kosten, wobei tendenziell die Mehrzahl der befragten Unternehmen von keinen oder geringen Kosten berichtet. Einige Autor*innen deuten Unterschiede zwischen akademischen und kommerziellen Studien an, die gegebenenfalls auch mit dem Aggregationsgrat der Daten einhergehen und gerade im Falle linearer Hochrechnungen zu hohen kalkulierten Kosten führen.

2.4.8 Anzeigeverhalten und Zusammenarbeit mit Behörden

Inhalt dieses Abschnitts sind Angaben des Literaturstandes, inwiefern Unternehmen im Falle eines Cyberangriffes mit offiziellen Stellen kooperieren bzw. Vorfälle anzeigen und welche

[152] Vgl. Ponemon Institute (2017b).

[153] Vgl. Hiscox (2018).

[154] i) Data Breaches: Nicht-authorisierte Veröffentlichung personenbezogener Daten; ii) Sicherheitsvorfälle: Böswillige Attacken auf Unternehmen; iii) Privacy Violations: Vermeintliche Verletzung der Privatsphäre von Kunden; iv) Phishing/Skimming: Individuelle finanzielle Verbrechen.

[155] Vgl. Romanosky (2016).

Gründe für oder gegen diese Zusammenarbeit sprechen. Lediglich in 7 von 32 Studien finden sich dazu Angaben.

Klahr et al. berichten von ihrer Umfrage unter britischen Unternehmen,[156] dass nur 26 % der Befragten den schwerwiegendsten Vorfall der letzten 12 Monate an Externe, mit Ausnahme von Security Providern, meldeten. Davon wurden Vorfälle meisten an Banken oder Kreditkartenfirmen (28 %), die Polizei (19 %) und Lieferant*innen (10 %) gemeldet. Als Gründe für die Unterlassung einer Meldung des Vorfalls, der Auswirkungen mit sich brachte, an Externe, werden vor allem die Unwichtigkeit der Vorfalls (52 %), die Unwissenheit, an wen zu berichten gewesen wäre (24 %), keine Verpflichtung zur Meldung (8 %) und keine Erfolgsaussichten (7 %) genannt.[157] Auch Bollhöfer et al. berichten mit Fokus auf Wirtschaftsspionage und Konkurrenzausspähung von ähnlich hohen Anzeigequoten bei der Polizei (22 %).[158] Die berichteten Anzeigequoten der IHK Nord liegen sogar noch darunter. Hier gaben lediglich 13,2 % der befragten Unternehmen an, mindestens einen Angriff der letzten zwölf Monate angezeigt zu haben. Ähnlich zur Studie von Klahr et al. wird die Unwissenheit über den richtigen Ansprechpartner von 22,1 % der befragten Unternehmen angegeben, während der mit einer Anzeige verbundene hohe Arbeitsaufwand (54,4 %) und negative Erfolgsaussichten (30,1 %) deutlich häufiger angegeben wurden. Daneben begründeten jeweils 3,7 % der Unternehmen die Nichtanzeige mit schlechten Vorerfahrungen sowie mit einem grundsätzlichen Misstrauen gegenüber Ermittlungsbehörden.[159]

Die Bitkom-Studie adressiert sehr ähnliche Fragestellungen,[160] kommt allerdings mit dem Fokus auf Wirtschaftsschutz in der Industrie, zu gegenteiligen Ergebnissen. So haben aussagegemäß nur 2 % der angegriffenen Unternehmen ihre Sicherheitsvorfälle nicht an staatliche Stellen gemeldet. 78 % der befragten Unternehmen haben eine Strafanzeige für Vorfälle innerhalb der letzten zwei Jahre gestellt und 29 % gaben eine freiwillige Meldung an Behörden ab. Auf die Frage, an wen Vorfälle gemeldet wurden, gaben 90 % der Unternehmen die Polizei, 70 % eine Staatsanwaltschaft, 14 % das Bundesamt für Sicherheit in der Informationstechnologie und nur wenige den Verfassungsschutz (7 %) oder Datenschutz-Aufsichtsbehörden (5 %) an. Als Gründe für den Verzicht zur Einbindung staatlicher Stellen zwecks Untersuchung nannten die Unternehmen vor allem Angst vor Imageschäden (38 %), keine Erfolgsaussichten (38 %), zu hohen Aufwand (37 %) und befürchtete negative Konsequenzen für das Unternehmen (36 %). Trotzdem wird anscheinend bei der Untersuchung der Vorfälle neben eigenen Ermittlungen (57 %) häufiger auf staatliche Stellen zurückgegriffen (38 %) als auf externe Spezialisten (31 %).[161] Eine weitere Bitkom-Umfrage mit Fokus auf Wirtschaftsschutz, allerdings nicht nur für Industrieunternehmen, gibt an, dass 31 % der Vorfälle durch staatliche Stellen untersucht wurden. Hiervon wurden zu 84 % die Polizei, 57 % die Staatsanwaltschaft, 15 % Datenschutzbehörden,

156 Vgl. Klahr et al. (2017).

157 Vgl. ebd.

158 Vgl. Bollhöfer & Jäger (2018).

159 Vgl. Industrie- und Handelskammer Nord e.V. (2013).

160 Vgl. Bitkom e.V. (2018).

161 Vgl. ebd.

15 % das BSI und zu 3 % der Verfassungsschutz involviert.[162] In einer Umfrage zur Betroffenheit durch Ransomware 2016 nennt das BSI eine Anzeigequote von 18 % der betroffenen Unternehmen, die allerdings nur für dieses Delikt erhoben wurde.[163]

Zu der Vorstellung, wie eine Zusammenarbeit zwischen Staat und Wirtschaft aussehen kann, befragten PwC und Strategy& im Jahr 2016 309 Unternehmen. Demnach gaben die befragten Unternehmen an, dass die Aufgaben Schadensbegrenzung, Forensik und Wiederherstellung vorwiegend als eigene Verantwortung gesehen werden, wohingegen die Durchführung von Forschungsprojekten und das Setzen von Standards als staatliche Aufgaben wahrgenommen werden. Die Themen Bildung, Sensibilisierung und Bedrohungsanalyse werden hingegen als gemeinsame Aufgabe betrachtet.[164]

Die dargestellten Anzeigequoten variieren je nach Studie. Vermisst wird an dieser Stelle vor allem Forschung dazu, welche Art von Angriffen durch welche Art von Unternehmen angezeigt wird. Möglich wäre, dass sich dadurch unterschiedlich berichtete Anzeigequoten erklären lassen würden.

2.4.9 Cyberversicherungen

In diesem Abschnitt werden Aussagen der betrachteten Literatur zur Verbreitung sowie Gründe, die für und gegen den Einsatz von Cyberversicherungen in Unternehmen sprechen, dargestellt. Angaben dazu waren lediglich in vier von 33 Studien zu finden.

Je nach Unternehmensgröße gab in einer Umfrage des GDV nur ein kleiner Teil der befragten Unternehmen an, eine Cyberversicherung abgeschlossen zu haben (Kleinste Unternehmen: 6 %; Kleine: 15 %; Mittlere: 9 %).[165] Einige weitere Unternehmen planen den Abschluss oder sind an einer Cyberversicherung interessiert (Kleinste Unternehmen: 15 %; Kleine: 15 %; Mittlere: 25%), wohingegen der Großteil der Befragten keine Versicherung hatte bzw. sich nicht dafür interessierte (Kleinste Unternehmen: 79 %; Kleine: 67 %; Mittlere: 63 %).[166] Bitkom spricht in einer Umfrage von einer Versicherung gegen digitale Wirtschaftsspionage, Sabotage oder Datendiebstahl und gibt an, dass 14 % der befragten Unternehmen eine solche vorweisen.[167] Auch hier gibt es unternehmensgrößenbezogene Unterschiede (10-99 Beschäftigte.: 10 %; 100-499 Beschäftigte: 23 %; >500 Beschäftigte: 32 %). Im Vergleich zum GDV gaben weniger Unternehmen an, dass eine solche Versicherung derzeit kein Thema im Unternehmen ist (10-99 Beschäftigte: 43 %; 100-499 Beschäftigte: 23 %; >500 Beschäftigte: 24 %). Lediglich 28 % der befragten Unternehmen, die mindestens einen Vorfall in den letzten zwei Jahren hatten, gaben an, dass sich der Abschluss einer entsprechenden Versicherung eher oder sehr gelohnt hat. Kleinere Unternehmen (10 bis 99 Beschäftigte) hingegen berichteten häufiger von einem lohnenswerten Einsatz (48 %) als größere Unternehmen (100 bis 499 Beschäftigte: 10 %; >500 Beschäftigte: 16 %).[168]

---

[162] Vgl. Bitkom e.V. (2017).

[163] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2016).

[164] Vgl. PwC Strategy& GmbH (2016).

[165] Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

[166] Vgl. ebd.

[167] Vgl. Bitkom e.V. (2018).

[168] Vgl. ebd.

Hiscox nennt in seinem Bericht deutlich höhere Anteile. Demnach gaben insgesamt 33 % der befragten Unternehmen in Deutschland, Spanien, UK, den Niederlanden und den USA an, eine Cyberversicherung zu haben.[169] Weitere 25 % planen einen Abschluss in den nächsten 12 Monaten. Auch hier zeigen sich starke Größenunterschiede. Während Unternehmen mit mehr als 250 Mitarbeitern je nach Nation Abschlussraten zwischen 49 % und 62 % aufweisen, ist dies für Unternehmen mit weniger als 250 Mitarbeitern nur zwischen 20 % und 33 % der Fall.[170]

Klahr et al. berichten, dass entgegen der Investitionen in Cybersicherheit, das Vorhandensein einer Cyberversicherung nicht positiv mit dem Umsatz korreliert.[171] Demnach ist in Unternehmen mit einem Umsatz zwischen Mio. 2 bis 10 GBP die Wahrscheinlichkeit am höchsten, eine Cyberversicherung anzutreffen (46 %), wohingegen dieser Anteil bei Unternehmen mit geringeren oder höheren Umsätzen jeweils bei 36 % liegt. Zudem sind Cyberversicherungen eher in den Branchen Bildung, Gesundheit, Soziales (57 %), Finanzwesen (53 %) und Verwaltung oder Immobilien (52 %) vertreten. Klahr et al. fragten die Unternehmen zusätzlich danach, inwiefern Kenntnisse darüber, welche Schäden durch die Versicherung abgedeckt sind und welche nicht, vorhanden sind. Ohne wesentliche Unterschiede in den Unternehmensgrößen, gaben durchschnittlich 59 % der Unternehmen an, dass diese Inhalte gut bzw. sehr gut verstanden wurden. Weitere 37 % gaben umgekehrt an, die Versicherungsumfänge gar nicht oder nicht gut zu kennen.[172]

Trotz divergierender Angaben scheint tendenziell der Großteil der Unternehmen bisher keine Versicherung gegen Cyber- und Informationssicherheitsverletzungen abgeschlossen zu haben. Ursachen für die unterschiedlichen Ergebnisse können neben den in Abschnitt 2.3 genannten Limitationen auch unterschiedliche Arten und Umfänge entsprechender Versicherungen sein. So wäre es möglich, dass Unternehmen das Vorhandensein einer umfangreichen Betriebsunterbrechungsversicherung, die auch bestimmte Schäden durch Cyberangriffe abdeckt, als Vorhandensein einer Cyberversicherung werten.

2.5 Zwischenresümee

Wie der dargestellte Auszug des Forschungsstandes zeigt, ist das Phänomen Cyberangriffe gegen Unternehmen sehr dynamisch und vielseitig. Aufgrund dessen existiert eine große Bandbreite an Literatur verschiedener Autorengruppen, deren Forschung starke Unterschiede im methodischen Vorgehen und der jeweiligen Operationalisierung aufweist. Neben den in Abschnitt 2.3 genannten Limitationen, die ursächlich für unterschiedliche Ergebnisse sein können, fehlen insbesondere erprobte standardisierte Instrumente zur Datenerhebung, wie dies in vielen Bereichen der quantitativen empirischen Forschung üblich ist. Dies schränkt u.a. die direkte Vergleichbarkeit verschiedener Studien sehr stark ein.

Neben den unterschiedlichen und teils widersprüchlichen Angaben zu den oben dargestellten Themengebieten fallen zudem offene Fragestellungen auf, die bisher nicht oder nur sehr selten

169 Vgl. Hiscox (2018).

170 Vgl. ebd.

171 Vgl. Klahr et al. (2017).

172 Vgl. ebd.

adressiert wurden. Dazu zählen insbesondere differenzierte Auswirkungen einzelner Angriffsarten auf Technik, Prozesse, Organisation und Beschäftigte von Unternehmen, Art und Höhe entstehender Kosten infolge von Cyberangriffen und nicht zuletzt Risiko- und Schutzfaktoren, die sich auf die Betroffenheit von Cyberangriffen auswirken.

3 ERHEBUNG

Neben der Aufbereitung und Darstellung des Forschungsstandes wurden im Vorfeld der Befragung und der Fragebogenkonzeption neun leitfadengestützte qualitative Interviews mit Vertretern der Strafverfolgungsbehörden (Zentrale Ansprechstellen Cybercrime (ZAC) und spezialisierte Staatsanwaltschaft), des Verfassungsschutzes, des Bundesamtes für Sicherheit in der Informationstechnik sowie von Versicherern durchgeführt, um einen Zugang in das Forschungsfeld zu erlangen und den Bedarf an Forschung zu eruieren. Die detaillierte Beschreibung des methodischen Vorgehens sowie die Dokumentation der Ergebnisse der qualitativen Inhaltsanalyse dieser Interviews werden in einem gesonderten Forschungsbericht veröffentlicht. [173]

Ein zentrales Resultat dieser Vorarbeiten ist, dass das Ausmaß und die Folgen von Cyberangriffen gegen Unternehmen durch die Strafverfolgungsbehörden nur sehr ungenau eingeschätzt werden können. Insbesondere das als sehr groß vermutete Dunkelfeld und eine als gering wahrgenommene Anzeigebereitschaft erschweren die Einschätzung des Phänomens und damit die Sensibilisierung der Unternehmen, der Öffentlichkeit sowie der Politik. Daneben wird eine große Diskrepanz zwischen kleinen und mittleren Unternehmen auf der einen Seite und Großunternehmen auf der anderen Seite von den Strafverfolgungsbehörden wahrgenommen, insofern KMU aufgrund geringerer Ressourcen und einer geringeren Sensibilisierung gegenüber dem Thema Cyberangriffe häufig nicht ausreichend geschützt zu sein scheinen.[174]

3.1 Methode

Um aussagekräftige Erkenntnisse insbesondere über das Ausmaß von Cyberangriffen, verursachte Schäden und geeignete Schutzmaßnahmen zu erheben, wurde die Erhebungsmethode computergestützter Telefoninterviews (Computer Assisted Telephone Interviews, kurz CATI) eingesetzt.

Für die Methode der CATI-Befragung sprach vor allem im Vergleich zur postalischen und Online-Befragung, dass sich die Erhebung in relativ kurzer Zeit durchführen lässt und die „richtige“ Zielpersonen in den Unternehmen schneller zu erreichen und gegebenenfalls für die Teilnahme an einer Befragung zu gewinnen sind. Dafür riefen professionelle Interviewer*innen ausgewählte Unternehmen an, warben für die Teilnahme an der Befragung und machten im Fall der Teilnahmebereitschaft einen Termin mit der Zielperson innerhalb des Unternehmens für die Befragung aus. Bei diesem Termin leitete eine Software durch den Fragebogen, sodass sich die Interviewer*innen ganz auf die Antworten der Teilnehmer*innen konzentrieren und diese direkt in elektronischer Form eingegeben konnten. Ein wesentlicher Vorteil der CATI-Befragung ist, dass die Datenqualität während der Erhebung kontrolliert werden kann. Fehler bei der Fragebogenkonstruktion hätten gegebenenfalls rechtzeitig erkannt und ausgebessert werden kön-

[173] Stiller et al. (2020).

[174] Vgl. Stiller et al. (2020).

nen. Teilnahmeverweigerungen und Abbrüche werden ebenfalls rechtzeitig registriert und können über eine Nachziehung kompensiert werden. Durch technische Validierungsregeln können direkt im Augenblick der Datenerfassung unrealistische Eingaben oder fehlerhafte Reihenfolgen von Filterfragen verhindert und ggf. nachgefragt werden. Dadurch ist es möglich, eine hohe Datenqualität, eine relativ hohe Teilnahmequote und damit einen in der zur Verfügung stehenden Zeit für die angestrebten Analysen ausreichend großen Datensatz zu erreichen.[175]

Zur Durchführung der CATI-Befragung von den anvisierten 5.000 Unternehmen wurde nach einer offiziellen europaweiten Ausschreibung das Umfrageinstitut Kantar EMNID beauftragt. Kantar EMNID ist Mitglied der Branchenverbände BVM (Berufsverband Deutscher Markt- und Sozialforscher e.V.) und ADM (Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.), den geltenden Datenschutz- und Standesbestimmungen verpflichtet und insbesondere nach der internationalen Norm für den Bereich der Meinungs- und Sozialforschung ISO 20252 zertifiziert. Zudem hält Kantar EMNID Zertifizierungen in den Bereichen Qualitätsmanagement (ISO 9001) und Informationssicherheitsmanagement (ISO/IEC 27001). Das Umfrageinstitut führte bereits verschiedene Befragungen zum Thema Wirtschaftskriminalität, Cyber Security und Informationssicherheit von kleinen und mittleren Unternehmen durch und ist somit auch in thematischer Hinsicht ein geeigneter Partner für die Umsetzung des Vorhabens.

Der standardisierte Fragebogen für diese quantitative Erhebung enthielt insgesamt 40 Fragen, die in vier Abschnitte gegliedert wurden. Abschnitt A enthielt eine kurze Einführung und Fragen zur Berufsfunktion der interviewten Person sowie eigene Risikoeinschätzungen. Anschließend wurden in Abschnitt B rund 21 Fragen zu erkannten Cyberangriffen in den letzten 12 Monaten oder auf Lebenszeit sowie detaillierter zum schwersten Cyberangriff der letzten 12 Monate gestellt. Das Vorhandensein technischer und organisatorischer Sicherheitsmaßnahmen wurde in Sektion C erhoben, woraufhin abschließend in Abschnitt D bestimmte strukturelle Merkmale der teilnehmenden Unternehmen erfragt wurden. Der Fragebogen wurde nach einer Aufarbeitung des Forschungsstandes, Diskussionen mit dem projektbegleitenden Unternehmensstammtisch[176] und unter Einbezug der Ergebnisse aus neun Experteninterviews innerhalb des Forschungsprojektes entwickelt und einem qualitativen Pretest unterzogen. Dazu wurden sechs IT-Mitarbeiter von Unternehmen unterschiedlicher Größe und Branche – überwiegend in der Situation eines telefonisch geführten Interviews – gebeten, die gestellten Fragen laut denkend,[177] d.h. unter Äußerung von Verständnisschwierigkeiten oder Überlegungen zur Antwortfindung etc., zu beantworten. Fragen und Begrifflichkeiten, die bereits im Vorfeld Schwierigkeiten erwarten ließen, wurden vom Testleiter gezielt angesprochen und hinterfragt.[178] Auf dieser Grundlage wurde der Fragebogen erneut überarbeitet und entsprechend angepasst.[179] Eine Kurzdarstellung des eingesetzten Fragebogens findet sich in Anhang 2.

---

[175] Bollhöfer & Jäger (2018) berichten für eine postalische Unternehmensbefragung zum Thema Wirtschaftsspionage eine Rücklaufquote von 9,3 %. Während der viermonatigen Befragungszeit sendeten lediglich 583 der 6284 angeschriebenen Unternehmen einen ausgefüllten Fragebogen zurück. Paoli et al. (2018) gaben für einen per E-Mail versendeten Fragebogen eine Rücklaufquote von 4,9 % an.

[176] Der projektbegleitende Unternehmensstammtisch setzt sich aus acht bis zwölf Unternehmen unterschiedlicher Branchen aus der Region Hannover zusammen, die regelmäßig inhaltliche Fragestellungen und Ergebnisse des Forschungsprojektes diskutieren, um die Praxisrelevanz für und den Wissenstransfer in die Wirtschaft zu fördern.

[177] Zur Methode des „Think-Aloud“ vgl. z.B. Blanke et al. (2011: 644) oder Willis (2005).

[178] Zur Methode des „Probing“ vgl. z.B. Prüfer & Rexroth (16).

[179] Neben der Anpassung von Formulierungen wurden zusätzliche Antwortmöglichkeiten bei den Fragen B18 zu den Nichtanzeigegründen („Wusste nicht, an wen man sich dafür wenden muss“) und D08 zur Onlinepräsenz sensibler Daten

Vor der Feldphase wurden zusammen mit den Befragungsleitern von Kantar EMNID Schulungen mit den 141 Interviewern*innen in den genutzten CATI-Studios Berlin und Bielefeld durchgeführt und der Fragebogen mit zusätzlichen Hinweisen für die Interviewer*innen versehen. Zur Erhöhung der Teilnahmebereitschaft bei den kontaktierten Unternehmen wurde ein offizielles Motivationsschreiben des Bundesministeriums für Wirtschaft und Energie während der Kontaktphase eingesetzt sowie die spätere Zusendung des Ergebnisberichtes angeboten.

Die Befragung fand in der Zeit von August 2018 bis Januar 2019 statt.

3.2 Untersuchungseinheit

Studien zu Organisationen als Untersuchungseinheit „stellen survey-methodologisch teilweise spezielle Anforderungen und unterscheiden sich deutlich von Personenbefragungen“[180], da in der Regel lediglich ein/e Vertreter*in der Organisation zu dieser befragt wird. Neben dem Problem der Erreichbarkeit innerhalb der Organisation, ist bereits die Auswahl eines/r entsprechenden Vertreters*in von entscheidender Bedeutung.

Wie bereits in Abschnitt 1.1.2 dargestellt, bilden rechtlich selbstständige Unternehmen die Untersuchungseinheit. Bei Unternehmen mit mehreren Betrieben[181] innerhalb einer rechtlich selbständigen Einheit, wurde jeweils nur die Unternehmenszentrale befragt.[182] Beschäftigte, die für den Bereich IT und Informationssicherheit verantwortlich sind, wurden als bevorzugte Zielpersonen definiert. Gab es im befragten Unternehmen keine derartige spezifische Position, wurde die Person befragt, in deren Zuständigkeitsbereich das Thema IT & Informationssicherheit innerhalb des Unternehmens fiel. Je nach Größe des Unternehmens kam dies mehr oder weniger häufig vor.[183]

3.2.1 Grundgesamtheit

Die Grundgesamtheit bildeten dementsprechend alle Unternehmen, d.h. rechtlich selbständige Einheiten (z.B. AG, GmbH, GbR etc.), die im Zeitraum der Befragung ihren Sitz in Deutschland und mehr als neun sozialversicherungspflichtig Beschäftigte hatten.[184]

Der Umfang und die Zusammensetzung dieser Grundgesamtheit kann über das Unternehmensregister-System (URS) des Statistischen Bundesamts eingeschätzt werden, das alle Unterneh-

(„teilweise“) ergänzt sowie zwei zusätzliche Fragen (B03: Wahrscheinlichkeitseinschätzung eines nicht bemerkten Cyberangriffs; C02: Art der eingesetzten Firewall) aufgenommen.

[180] Hartmann (2017: 186).

[181] „Ein Betrieb ist eine Niederlassung an einem bestimmten Ort, einschließlich örtlich und organisatorisch angegliederter Betriebsteile“ (Statistisches Bundesamt 2018: 5).

[182] Hartmann (2017: 189).

[183] Siehe dazu Abschnitt 3.4.3.

[184] Kleinstunternehmen bis neun Beschäftigte wurden in dieser Befragung ausgeschlossen, da deren Einbezug den zeitlichen und finanziellen Rahmen der geplanten Befragung gesprengt hätte. Ein wesentlicher Grund dafür ist, dass diese große Gruppe einer relativ starken Veränderung z.B. durch häufigere Gewerbean- und abmeldungen bzw. Neugründungen und Insolvenzen unterworfen ist (Vgl. Statistisches Bundesamt (2019a, 2019b)) und dadurch die Verfügbarkeit und Aktualität insbesondere von telefonischen Kontaktinformationen in den herangezogenen Firmendatenbanken nur sehr eingeschränkt gegeben ist.

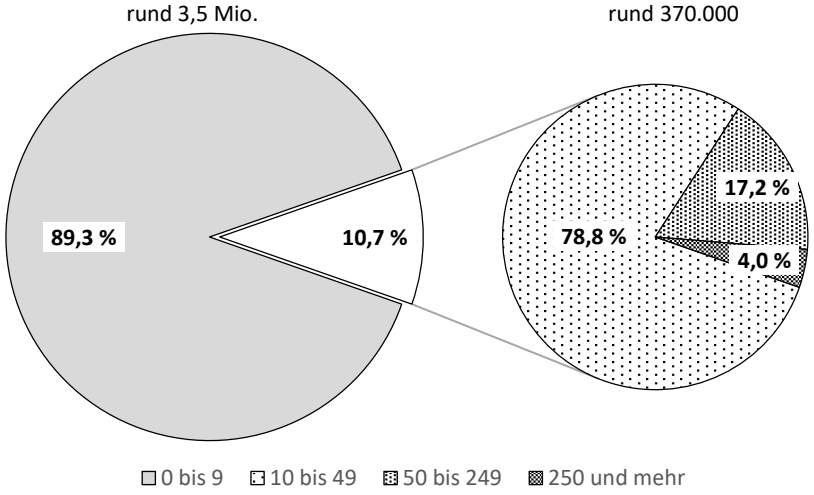
men enthält, die einen Beitrag zum Bruttoinlandsprodukt leisten, ihren Sitz in Deutschland haben und den Wirtschaftszweigen (nach WZ 2008 Klassifikation) der Abschnitte B bis N oder P bis S zugehören.[185]

Alternativ dazu bietet die „Statistik für kleine und mittlere Unternehmen" des statistischen Bundesamtes eine Einschätzung der Grundgesamtheit für alle Unternehmen mit Sitz in Deutschland, die nicht der Finanz- und Versicherungsdienstleistung (WZ08-K) zugeordnet sind. Wie beim URS werden auch hier die Beschäftigtengrößenklassen *0 bis 9*, *10 bis 49*, *50 bis 249* und *250 und mehr sozialversicherungspflichtigen Beschäftigte (SVB)* unterschieden. Ein Vergleich mit dem URS ist allerdings nicht sinnvoll, da andere Definitionen und die Methoden der Datengewinnung voneinander abweichen.[186]

Beide Statistiken bieten hinsichtlich der Beschäftigtengrößenklassen demnach nur eine grobe Kategorisierung und mit Bezug auf die WZ-Klassen kein umfassendes Bild über alle deutschen Unternehmen hinweg[187]. Da die verfügbaren Daten des URS aktueller sind und hinsichtlich der WZ-Klassen die größere Schnittmenge zu den untersuchten Unternehmen enthält, wurden diese zur Einschätzung der Grundgesamtheit herangezogen.

Gemäß URS-Daten (Stand 2017) haben lediglich 10,7 % (372.599) aller Unternehmen (3.481.860) mehr als neun Beschäftigte und zählen damit zur Grundgesamtheit der Befragung. Davon haben Unternehmen mit zehn bis 49 Beschäftigten mit 78,8 % den größten Anteil, gefolgt von Unternehmen mit 50 bis 249 Beschäftigten (17,2 %) und großen Unternehmen ab 250 Beschäftigten (4,0 %).

Abbildung 3 **Anteile der Unternehmen nach Beschäftigtengrößenklassen**
Quelle: URS, Statistisches Bundesamt, 2017; eigene Abbildung



Obwohl diese Grundgesamtheit nur 10,7 % der Unternehmen in Deutschland repräsentiert, stellen die darin enthaltenen Unternehmen ungefähr 81,5 % der Beschäftigten in Deutschland dar.[188]

185 Quelle: Statistisches Bundesamt, Wiesbaden 2015 (https://www-genesis.destatis.de).

186 Quelle: Statistisches Bundesamt, Wiesbaden 2018 (https://www-genesis.destatis.de).

187 Keine Unternehmen im Bereich WZ08-A: Land- und Forstwirtschaft, Fischerei.

188 In 2017 gab es in Unternehmen der Branchen WZ08-B bis N (außer K) rund 29,7 Mio. Beschäftigte (Kleinstunternehmen: 5,5 Mio.; Kleine Unternehmen: 6,9 Mio.; Mittlere Unternehmen: 5,7 Mio.; Großunternehmen: 11,6 Mio.). Unternehmen der WZ-Klassen A, K, O, P, Q, R, S sind allerdings nicht in dieser Statistik berücksichtigt, dafür aber in der

Tabelle 1 **Unternehmen in Deutschland nach Beschäftigtengrößenklassen und Wirtschaftszweigen ab 10 Besch.**
WZ 2008; Quelle: URS, Statistisches Bundesamt, 2017

		Beschäftigtengrößenklassen							
		10 bis 49		50 bis 249		250 und mehr		insgesamt	
WZ08 (Abschnitte): URS, 2017		Anzahl	Prozent	Anzahl	Prozent	Anzahl	Prozent	Anzahl	Prozent
B	Bergbau und Gewinnung von Steinen und Erden	487	0,2	113	0,2	18	0,1	618	0,2
C	Verarbeitendes Gewerbe	43.540	14,8	15.845	24,8	4.340	28,8	63.725	17,1
D	Energieversorgung	692	0,2	518	0,8	194	1,3	1.404	0,4
E	Wasserversorg., Entsorg., Beseitig. v. Umweltverschm.	2.517	0,9	829	1,3	157	1,0	3.503	0,9
F	Baugewerbe	37.002	12,6	3.397	5,3	280	1,9	40.679	10,9
G	Handel, Instandhaltung und Reparatur von Kfz	54.140	18,4	9.582	15,0	1.781	11,8	65.503	17,6
H	Verkehr und Lagerei	17.020	5,8	3.867	6,0	693	4,6	21.580	5,8
I	Gastgewerbe	17.493	6,0	2.123	3,3	213	1,4	19.829	5,3
J	Information und Kommunikation	10.352	3,5	2.812	4,4	523	3,5	13.687	3,7
K	Erbringung von Finanz- und Versicherungsleistungen	2.023	0,7	1.132	1,8	777	5,2	3.932	1,1
L	Grundstücks- und Wohnungswesen	3.722	1,3	510	0,8	64	0,4	4.296	1,2
M	Freiberufliche, wiss. u. techn. Dienstleistungen	28.041	9,6	4.037	6,3	703	4,7	32.781	8,8
N	Sonstige wirtschaftliche Dienstleistungen	16.552	5,6	5.617	8,8	1.553	10,3	23.722	6,4
P	Erziehung und Unterricht	11.360	3,9	2.022	3,2	441	2,9	13.823	3,7
Q	Gesundheits- und Sozialwesen	33.533	11,4	8.868	13,9	2.855	19,0	45.256	12,1
R	Kunst, Unterhaltung und Erholung	3.979	1,4	601	0,9	126	0,8	4.706	1,3
S	Erbringung von sonstigen Dienstleistungen	11.157	3,8	2.055	3,2	343	2,3	13.555	3,6
		293.610	100,0	63.928	100,0	15.061	100,0	372.599	100,0

3.2.2 Auswahlgesamtheit

Auch wenn mit den ausgeschlossenen Kleinstunternehmen (null bis neun Beschäftigte)[189] der größte Anteil aller in Deutschland ansässigen Unternehmen unberücksichtigt bleibt, ist eine Vollerhebung der inkludierten kleinen, mittleren und großen Unternehmen aufgrund ihrer immer noch großen Grundgesamtheit forschungsökonomisch nicht möglich. Alternativ dazu soll nur eine zufällig ausgewählte Teilmenge der Grundgesamtheit untersucht werden, die diese annähernd abbildet. Als Basis für die Stichprobenziehung (Auswahlgesamtheit) kommen neben amtlichen Unternehmensregistern kommerzielle Firmendatenbanken[190] in Betracht. Diese haben den großen Vorteil, dass neben der Adresse der Unternehmen auch Kontaktpersonen und Kontaktdaten verfügbar sind, die eine telefonische Befragung sehr erleichtern. Hinzu kommt, dass die Ziehung der Stichprobe im Vergleich zu amtlichen Quellen ohne großen Aufwand und deutlich schneller erfolgen kann. Der Nachteil an solchen kommerziellen Datenbanken ist, dass

Grundgesamtheit dieser Studie enthalten. Je nachdem wie sich Unternehmen dieser WZ-Klassen auf die Beschäftigtengrößenklassen verteilen, kann sich der angegebene Anteil von 81,5 % der durch die Unternehmen in der Grundgesamtheit repräsentierten Beschäftigten erhöhen oder verringern. Quelle: Statista.com (https://de.statista.com/statistik/daten/studie/731962/umfrage/beschaeftigte-in-unternehmen-in-deutschland-nach-unternehmensgroesse/)

189 Siehe dazu Fn. 184.

190 Vgl. Hartmann (2017: 193).

sie in der Regel nicht vollständig sind. Die nicht enthaltenen Unternehmen haben damit keine Chance, in die Stichprobe zu gelangen (undercoverage) und die Auswahlgesamtheit ist folglich nur eine mehr oder weniger gute Annäherung an die Grundgesamtheit,[191] bei der darauf zu achten ist, woher die Unternehmensinformationen stammen und ob die Datensätze selektiv zustande gekommen sind.[192]

Die vom Umfrageinstitut Kantar EMNID zur Stichprobenziehung verwendeten Datenbanken der Anbieter Bisnode (ehemals Hoppenstedt) und Heins & Partner enthalten nach telefonischer Auskunft nahezu alle Unternehmen mit Sitz in Deutschland und werden täglich aktualisiert. Dennoch sind die für die CATI-Befragung benötigten Kontaktdaten (insbesondere Telefonnummern) in beiden Datenbanken nicht lückenlos vorhanden. Da die Datenbank von Bisnode entsprechend der geschäftlichen Ausrichtung vor allem Kontaktinformationen von Unternehmen der beiden größten Beschäftigtengrößenklassen und die Datenbank von Heins & Partner insbesondere die der mittleren und kleinen Unternehmen enthält, konnte über eine gemeinsame Nutzung auf eine Datenbasis zurückgegriffen werden, „die alle Facetten des Quotengerüsts adäquat [abdeckt].“[193] Ein automatisierter Duplikate-Check verhinderte die Mehrfachbefragung von Unternehmen. Vor diesem Hintergrund und mit dem Ausschluss der volatilsten und damit am lückenhaftesten enthaltenen Gruppe der Kleinstunternehmen unter zehn Beschäftigten kann von einer guten Annäherung an die Grundgesamtheit ausgegangen werden.

3.3 Stichprobenziehung und -realisierung

Wie in Abbildung 3 und Tabelle 1 zu sehen, ist die Verteilung in Hinblick auf die Beschäftigtengrößenklassen sowie die Wirtschaftszweigzugehörigkeit sehr schief. Die in der Grundgesamtheit selten vorhandenen Teilgesamtheiten (z.B. große Unternehmen ab 500 Beschäftigten) würden demnach bei einer einfachen Zufallsauswahl wegen ihrer entsprechend geringeren Auswahlwahrscheinlichkeit kaum in der Stichprobe vertreten sein.

Tabelle 2 **Stratifizierungsplan der disproportional geschichteten Stichprobe**

	Zielgröße	Branchenverteilung
10-49 Besch.	1.000	proportional zur Auswahlgesamtheit; WZ08-A bis S (ohne WZ08-O,T,U)
50-99 Besch.	1.000	
100-249 Besch.	1.000	
250-499 Besch.	1.000	Best-Effort-Basis; WZ08-A bis S (ohne WZ08-O,T,U)
ab 500 Besch.	500	
Unternehmen der Daseinsvorsorge	500	Branchen- und Größenverteilung auf Best-Effort-Basis[194]
Gesamt	5.000	

[191] Schnell & Noack (2015: 9f.) Dieser Umstand ist aus inferenzstatistischer Sicht problematisch, da somit streng genommen die Auswahlwahrscheinlichkeit nicht mehr berechnet werden kann und keine „echte“ Zufallsauswahl besteht (vgl. Hartmann 2017: 194).

[192] Snijkers & Meyermann (2017: 252). Siehe dazu auch Smith (2013).

[193] Kantar Emnid (2019: 3).

[194] Im Bereich der wirtschaftlichen Leistungserbringung zählen folgende Sektoren zum Kanon der Daseinsvorsorge: Elektrizitätsversorgung, Gasversorgung, Gewerbliche Entsorgung / Kreislaufwirtschaft, Gesundheit (Krankenhäuser, ambulante Versorgung, Vor- und Nachsorge, Pflege), Post, Verkehrs- und Beförderungswesen (Schienen, Straßen, Wasserstraßen, Luftverkehr), Geld- und Kreditversorgung (mit dem verbindlichen Auftrag zur Leistungserbringung an die Sparkassen), Telekommunikation/Internet und Wohnungswirtschaft (vgl. Schäfer 2018). Die den Unternehmen der Daseinsvorsorge zugeordneten WZ08-Klassen finden sich im Anhang 1 in Tabelle 43.

Um auch für solche Gruppen genügend Aussagen bei der Befragung zu erzielen, wurde hinsichtlich der Beschäftigtengrößenklassen eine disproportional geschichtete Nettostichprobe nach einem vorgegebenen Stratifizierungsplan (Tabelle 2) anvisiert.[195]

Für die Durchführung von 5.000 Interviews nach diesem Stratifizierungsplan (Nettostichprobe) wurden 43.219 Unternehmen kontaktiert (Bruttostichprobe; Tabelle 3). Dies entspricht einer Teilnahmequote von 11,6 %.[196]

Tabelle 3 **Ausschöpfung**

		Anzahl	Prozent
Ausfall nach Kontakt mit Unternehmen	keine Zielperson im Unternehmen	6.160	14,3
	kein Interesse am Thema	7.156	16,6
	Verweigerung im Namen der Zielperson	3.634	8,4
	Verweigerung ohne Angabe von Gründen	14.582	33,7
	sonstiger Grund (z.B. Sprachprobleme, Datenschutz)	101	0,2
Ausfall im Kontakt mit Zielperson	Verweigerung aus Zeitgründen	1.006	2,3
	kein Interesse am Thema	2.136	4,9
	Verweigerung ohne Angabe von Gründen	3.266	7,6
	Abbruch im Interview	165	0,4
	sonstiger Grund (z.B. Sprachprobleme, Datenschutz)	13	0,0
	Nettostichprobe	5.000	11,6
	Bruttostichprobe	43.219	100,0

Die Ziehung der Bruttostichprobe erfolgte innerhalb der einzelnen Stratifikationszellen, die sich aus Beschäftigtengrößenklasse und Branchenzugehörigkeit (WZ08-Klasse) ergaben, nach dem Zufallsprinzip und unter Berücksichtigung der ADM-Sperrdatei.[197] Ein weiteres Merkmal, das bei der Stratifizierung berücksichtigt wurde, ist die Zugehörigkeit der Unternehmen zum Bereich der Daseinsvorsorge.[198]

Hinsichtlich des Teilnahmeausfalls können zwei Kontaktphasen unterschieden werden: Der größte Anteil an Ausfällen kam bereits in der ersten Phase zustande, in der die Unternehmen erstmalig kontaktiert wurde, um den Hintergrund der Befragung vorzustellen, geeignete Zielpersonen innerhalb der Unternehmen zu bestimmen und deren Kontaktinformationen zu erfragen. Etwa ein Drittel der Unternehmen waren in dieser Phase ohne Angabe von Gründen nicht zur Teilnahme bereit (33,7 %), weitere 16,6 % hatten kein Interesse am Befragungsthema, bei 14,3 % konnte keine Zielperson im Unternehmen bestimmt werden und bei einem Anteil von 8,4 % wurde die Teilnahme im Namen der Zielperson verweigert.

[195] Nicht mit einbezogen wurden die Wirtschaftszweigklassen WZ08-T (Private Haushalte mit Haushaltspersonal etc.) und WZ08-U (Exterritoriale Organisationen und Körperschaften), weil es sich dabei um keine privatwirtschaftlichen Unternehmen handelt und sie auch nicht der Daseinsvorsorge zuzuordnen sind.

[196] Nur wenige Studien berichten transparent über die Teilnahme- bzw. Rücklaufquoten: Beispiele sind Paoli et al. (2018) (4,9 %); Computer Security Institute (2011) (6,4 %); Rantala (2008) (23 %).

[197] Die Sperrdatei des Arbeitskreises Deutscher Markt- und Sozialforschungsinstitute e.V. (ADM) enthält Unternehmen, die für sozialwissenschaftliche Befragungen generell nicht zur Verfügung stehen.

[198] Siehe Fn. 194.

In der zweiten Phase, in der die vorher bestimmten Zielpersonen von den Interviewern*innen kontaktiert und zur Teilnahme an der Befragung unter Einsatz des Begleitschreibens vom BMWi gebeten wurden, kam es zu einem Ausfall von 7,6 % ohne Angabe von Gründen, 4,9 % hatte kein Interesse am Thema und 2,3 % nahmen aus zeitlichen Gründen nicht an der Befragung teil. Bei einem Anteil von 0,4 % erfolgte der Abbruch im Interview. Sonstige Gründe (z.B. sprachliche Probleme oder Datenschutzgründe) spielten in beiden Kontaktphasen eine untergeordnete Rolle (0,2 % bzw. 0,03 %).

3.4 Stichprobenbeschreibung

Bei der Darstellung der Stichprobenverteilung und anschließend der Befragungsergebnisse, beziehen sich die angegebenen Prozentwerte auf die jeweils gültigen Fälle, d.h. abzüglich der Fälle mit fehlenden Angaben. Da die Zahl dieser gültigen Fälle (N) variieren kann, wird sie jeweils mit ausgewiesen. Sollte die Anzahl der fehlenden Fälle auffällig hoch ausfallen, wird an entsprechender Stelle gesondert darauf hingewiesen.

Insbesondere für den späteren Vergleich der Ergebnisse zwischen bestimmten Unternehmensgruppen werden z.T. die 95%-Konfidenzintervalle (95%-KI)[199] in den Diagrammen mit Hilfe sogenannter Fehlerbalken ausgehend vom Ende der Säulen bzw. von den Punkten dargestellt.[200] Überschneiden sich die Konfidenzintervalle zweier Werte nicht, kann mit einer fünfprozentigen Irrtumswahrscheinlichkeit von einem signifikanten Unterschied ausgegangen werden. Eine Überschneidung weist hingegen darauf hin, dass der Unterschied zufällig zustande gekommen sein könnte. Darüber hinaus werden für alle weiteren Gruppenvergleiche zusätzlich Signifikanztests (Chi²-Tests) durchgeführt und gegebenenfalls signifikante Unterschiede fett dargestellt.[201]

Durch die disproportionale Schichtung der Stichprobe veränderte Auswahlwahrscheinlichkeit sind insbesondere große Unternehmen und Unternehmen der Daseinsvorsorge in der Nettostichprobe stärker vertreten als in der Grund- und Auswahlgesamtheit (oversampling). Damit können auch zu diesen Gruppen sinnvolle Aussagen getroffen werden.

Für Aussagen zu allen Unternehmen, d.h. über alle Beschäftigtengrößenklassen und Branchen hinweg, wird die Stichprobe mit einer nachträglichen Gewichtung re-proportionalisiert, so dass die Stichprobe entsprechend der Auswahlgesamtheit und damit näherungsweise der Grundgesamtheit verteilt ist und keine Hinweise für eine Verzerrung hinsichtlich dieser Unternehmensmerkmale mehr vorliegen.

---

[199] Das Konfidenzintervall ist ein Wertebereich (Erwartungsbereich), der mit einer bestimmten Wahrscheinlichkeit (hier 95 %) zu den Wertebereichen gehört, die den wahren Wert eines Parameters der Auswahlgesamtheit enthalten. Dabei handelt es sich um eine konservative Schätzung, d.h., im Vergleich zu anderen Signifikanztests gelangt man unter gleichen Voraussetzungen eher zu dem Schluss, dass kein Zusammenhang besteht.

[200] Die Spannweite des so umfassten Wertebereichs kann variieren; sie wird z.B. umso größer, je kleiner die Anzahl gültiger Angaben ist, auf der die Schätzung des wahren Anteilwertes der Auswahlgesamtheit beruht.

[201] Das zugrundeliegende Signifikanzniveau liegt auch hier bei mindestens 95 %, d.h., es gibt noch eine Restwahrscheinlichkeit von maximal 5 % ($p < .05$), dass in der Auswahlgesamtheit kein Unterschied zwischen den Vergleichsgruppen besteht und die beobachtete Differenz in der untersuchten Stichprobe zufällig zustande gekommen ist.

3.4.1 Beschäftigtengrößenklassen

In Tabelle 4 ist die Stichprobenverteilung hinsichtlich der Beschäftigtengrößenklassen zu erkennen. Während die Anteile der Unternehmen der einzelnen Beschäftigtengrößenklassen (mit Ausnahme der Unternehmen ab 500 sozialversicherungspflichtig Beschäftigte) in der ungewichteten Stichprobe etwa gleich groß sind, entsprechen deren Anteile in der gewichteten Stichprobe denen in der Auswahlgesamtheit. So haben z. B. Unternehmen mit zehn bis 49 Beschäftigte als auch Unternehmen mit 50 bis 99 Beschäftigte in der ungewichteten Stichprobe einen Anteil von rund 24 % und in der gewichteten Stichprobe einen Anteil von 79,1 % bzw. 10,5 %. Bei den Auswertungen über alle Unternehmen sämtlicher Beschäftigtengrößenklassen hinweg erhalten demnach kleine Unternehmen ein höheres und größere Unternehmen ein geringeres Gewicht.

Tabelle 4 Stichprobe nach Beschäftigtengrößenklassen und dem Merkmal Daseinsvorsorge

		disproportionale Stichprobe		
		ungewichtet		gewichtet
Beschäftigtengrößenklassen		Anzahl	Prozent	Prozent
	10-49 Besch.	1.190	23,8	79,1
	50-99 Besch.	1.181	23,6	10,5
	100-249 Besch.	1.120	22,4	6,5
	250-499 Besch.	1.005	20,1	2,2
	ab 500 Besch.	504	10,1	1,8
	Gesamt	5.000	100,0	100,0
Unternehmen der Daseinsvorsorge				
	ja	847	16,9	11,2
	nein	4.153	83,1	88,8
	Gesamt	5.000	100,0	100,0

Unternehmen der Daseinsvorsorge sind gemessen an ihrem Anteil in Auswahlgesamtheit in der ungewichteten Stichprobe mit 16,9 % etwas überrepräsentiert und werden daher auf 11,2 % heruntergewichtet.

3.4.2 Branchen

Die Branchenzugehörigkeit der Unternehmen ist bereits in Form der Klassifikation der Wirtschaftszweige des Statistischen Bundesamts von 2008 (WZ 2008)[202] in der Firmendatenbank, die zur Stichprobenziehung herangezogen wurde, bis zur zweiten Gliederungsebene enthalten und musste nicht gesondert erhoben werden. Die Klassifizierung auf der ersten Gliederungsebene (WZ08-A bis S) dient als weiteres Merkmal, das zur Gewichtung des Datensatzes verwendet wird, d. h., die Branchenverteilung wird für jede Beschäftigtengrößenklasse auf Basis der jeweiligen Branchenverteilung innerhalb der Auswahlgesamtheit gewichtet.

In Tabelle 5 sind die Verteilungen der 19 WZ-Klassen (Ebene 1) über alle Unternehmen hinweg in der ungewichteten und gewichteten Stichprobe zu erkennen. Größere Unterschiede lassen sich insbesondere beim verarbeitenden Gewerbe (WZ08-C), beim Baugewerbe (WZ08-F) und

[202] Vgl. Statistisches Bundesamt (2008).

beim Handel inkl. Instandhaltung und Reparatur von Kraftfahrzeugen (WZ08-G) erkennen. Diese sind vor allem auf Unterschiede zwischen den Beschäftigtengrößenklassen zurückzuführen. So ist z. B. der Anteil an Unternehmen des verarbeitenden Gewerbes in der Gruppe der kleinen Unternehmen (10-49 Besch.) mit 18,8 % deutlich kleiner als bei den größeren (50-99 Besch.: 26,0 %; 200-249 Besch.: 30,1 %; 250-499 Besch.: 30,1 %; ab 500 Besch.: 26,4 %). Da kleine Unternehmen bei Auswertungen zum Gesamtdatensatz ein höheres Gewicht erhalten, reduziert sich in diesem Fall der Anteil von WZ08-C-Unternehmen von 26,6 % in der ungewichteten Stichprobe auf 20,7 % in der gewichteten. Ähnlich aber genau andersherum verhält es sich bei den Anteilen der WZ08-F- und WZ08-G-Unternehmen, die in der Gruppe der kleinen Unternehmen (10-49 Besch.) deutlich häufiger auftreten als in den größeren. Daher sind hier im Vergleich zur ungewichteten Stichprobe größere Anteilswerte in der gewichteten Stichprobe zu erkennen.

Tabelle 5 **Stichprobe nach Branchen (WZ 2008)**

	disproportionale Stichprobe		
	ungewichtet		gewichtet
Branche (WZ08)	Anzahl	Prozent	Prozent
Land- und Forstwirtschaft, Fischerei (A)	39	0,8	1,4
Bergbau und Gewinnung von Steinen und Erden (B)	17	0,3	0,3
Verarbeitendes Gewerbe (C)	1.328	26,6	20,7
Energieversorgung (D)	68	1,4	0,5
Wasserversorgung; Abwasser- u. Abfallentsorgung u. Beseitigung v. Umweltverschmutzungen (E)	89	1,8	0,9
Baugewerbe (F)	310	6,2	12,9
Handel; Instandhaltung und Reparatur von Kraftfahrzeugen (G)	607	12,1	18,0
Verkehr und Lagerei (H)	329	6,6	4,7
Gastgewerbe (I)	130	2,6	4,2
Information und Kommunikation (J)	152	3,0	3,1
Erbringung von Finanz- und Versicherungsdienstleistungen (K)	209	4,2	2,1
Grundstücks- und Wohnungswesen (L)	105	2,1	1,6
Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen (M)	434	8,7	9,1
Erbringung von sonstigen wirtschaftl. Dienstleistungen (N)	235	4,7	4,3
Öffentliche Verwaltung, Verteidigung; Sozialversicherung (O)	19	0,4	0,4
Erziehung und Unterricht (P)	274	5,5	6,4
Gesundheits- und Sozialwesen (Q)	436	8,7	5,8
Kunst, Unterhaltung und Erholung (R)	64	1,3	1,2
Erbringung von sonstigen Dienstleistungen (S)	155	3,1	2,5
Gesamt	5.000	100,0	100,0

Die Klassifizierung der Unternehmen auf der zweiten Gliederungsebene der WZ-Kodierung wird insbesondere bei auffälligen Unterschieden für eine detailliertere Darstellung herangezogen. Die Verteilung und die Zuordnung der zweiten zur ersten Ebene kann im Anhang der Tabelle 44 entnommen werden.

3.4.3 Position der Interviewten innerhalb des Unternehmens

Wie bereits unter 3.1 beschrieben, liegt eine Schwierigkeit bei Unternehmensbefragungen in der Auswahl eines/r Unternehmensvertreters*in, der*die Auskunft zum Unternehmen gibt. Die bevorzugte Zielperson bestand in einem/r Beschäftigten, der*die für IT & Informationssicherheit zuständig ist. In den Fällen, in denen es eine solche spezifische Position nicht gibt, etwa weil dieser Bereich auf externe Dienstleistern ausgelagert oder von Beschäftigten anderer Bereiche mitübernommen wird, wurde ein/e Vertreter*in zur Teilnahme gebeten, in dessen/deren Zuständigkeitsbereich das Thema IT & Informationssicherheit fällt. Da sich der Tätigkeitsbereich der Befragten möglicherweise auf das Antwortverhalten auswirkt, wurde die Position innerhalb des Unternehmens erfragt und wird insbesondere in multivariaten Analysen als Kontrollvariable mit einbezogen.

Tabelle 6 **Stichprobe nach Position der Interviewten**
Mehrfachantworten möglich

	ungewichtet		gewichtet				
			Prozentanteile nach Beschäftigtengrößenklassen				
Position	Anzahl	Prozent	10-49	50-99	100-249	250-499	ab 500
IT & Informationssicherheit	3.484	69,8	38,8	67,3	78,6	86,7	91,9
Geschäftsführung, Vorstand	1.171	23,5	51,3	25,8	14,9	8,1	4,4
Datenschutz	342	6,8	8,7	8,0	5,6	5,9	5,0
Revision, Prüfung	104	2,1	2,8	2,9	1,9	1,4	0,4
Werkssicherheit	56	1,1	1,9	1,4	0,7	0,8	0,2
Sonstiges[203]	402	8,1	12,8	9,6	6,9	5,5	4,2

In Tabelle 6 ist zu erkennen, dass die Mehrzahl der befragten Vertreter*innen im Bereich der IT & Informationssicherheit arbeitet (69,8 %), dass es aber wie erwartet relevante Unterschiede zwischen den Unternehmen der verschiedenen Beschäftigtengrößenklassen gibt. Während fast alle Befragten der Unternehmen ab 500 Beschäftigten angaben, in diesem Bereich tätig zu sein (91,9 %), trifft dies in Unternehmen zwischen zehn und 49 Beschäftigten lediglich auf 38,8 % der Befragten zu. Befragte aus dem Bereich Geschäftsführung & Vorstand sind in kleinen Unternehmen entsprechend stärker vertreten.

Für die weitere Auswertung (insbesondere in Kapitel 6) wurden Mehrfachantworten aufgelöst und die Positionen folgendermaßen zusammengefasst: Befragte, die „Geschäftsführung, Vorstand“ und eine weitere Position angegeben haben, wurden lediglich der Geschäftsführung zugeordnet. Befragte, die „IT & Informationssicherheit“ und eine weitere Position mit Ausnahme von „Geschäftsführung, Vorstand“ angegeben haben, wurden ausschließlich der „IT & Informationssicherheit“ zugeordnet. Alle anderen wurden in der Kategorie „sonstige Position“ zusammengefasst (Tabelle 7).

[203] Dazu zählen insbesondere die Bereiche Finanz- und Rechnungswesen, Management, Einkauf und Vertrieb sowie Betrieb und Technik.

Tabelle 7 **Stichprobe nach zusammengefassten Positionen der Interviewten**

	ungewichtet		gewichtet				
			Prozentanteile nach Beschäftigtengrößenklassen				
Position	Anzahl	Prozent	10-49	50-99	100-249	250-499	ab 500
IT & Informationssicherheit	3.345	67,0	34,0	63,4	76,7	85,2	91,1
Geschäftsführung	1.171	23,5	51,3	25,8	14,9	8,1	4,4
Sonstige Position	477	9,6	14,7	10,8	8,4	6,8	4,6
Gesamt	4.993	100,0	100,0	100,0	100,0	100,0	100,0

3.5 Limitationen und Stärken

Zusammenfassend werden im Folgenden die methodischen Limitationen und Stärken dieser Studie dargestellt, auf die teilweise bereits in den vorgehenden Abschnitten hingewiesen wurden. Diese Zusammenstellung soll es dem Leser ermöglichen, die Aussagen der Studie auch im Vergleich zu anderen Studien sachgerechter zu interpretieren und letzten Endes besser informierte Entscheidungen zu treffen.

Die Stichprobenziehung erfolgte aus einer Auswahlgesamtheit (Unternehmensdatenbanken) und nicht direkt aus der Grundgesamtheit. Auch wenn die Stichprobe hinsichtlich der Verteilung aller kontrollierten Merkmale weitgehend der Grundgesamtheit entspricht und keine Hinweise auf eine systematische Verzerrung vorliegen, bleibt damit eine Unsicherheit hinsichtlich des Coverage-Problems bestehen, insofern nicht erfasste Unternehmen keine Chance hatten, in die Stichprobe zu gelangen. Obwohl der Untersuchungsgegenstand „Unternehmen“ eine Organisation und kein Individuum ist, sind derartige Unternehmensbefragungen darauf beschränkt, dass lediglich eine Person als Unternehmensvertreter*in befragt werden kann. Neben dem Problem der Auswahl geeigneter Repräsentanten*innen, spiegeln deren Antworten immer den jeweiligen Wissensstand sowie persönliche Motivationen und Einstellungen wider (sogenanntes Self-Reporting-Bias). Hinzu kommt, dass insbesondere die Fragen nach vorgefallenen Cyberangriffen retrospektiv gestellt wurden, was mit entsprechenden Verzerrungen verbunden sein kann, wenn erfragte Ereignisse z.B. gar nicht erinnert werden oder in Wahrheit länger zurückliegen als in der Erinnerung der Befragten. Selbstverständlich können Befragte auch nur Auskunft über Geschehnisse geben, die ihnen selbst bekannt sind. Von der Organisation oder der befragten Person unbemerkte Cyberangriffe, das sogenannte absolute Dunkelfeld, können durch diese Studienformen nicht untersucht werden. Neben Unwissenheit und Verständnisschwierigkeiten kann auch die sogenannte soziale Erwünschtheit dazu führen, dass befragte Personen Angaben machten, die nicht der Realität entsprechen. Um die soziale Erwünschtheit zumindest ansatzweise zu kontrollieren, wird hier das Antwortverhalten verschiedener Befragtengruppen verglichen (z.B. ob Geschäftsführer*innen anders auf die Frage nach der Einschätzung des Betriebsklimas antworten als IT-Mitarbeiter*innen). Hinsichtlich der mehrmonatigen Erhebungsphase ist es zudem möglich, dass Störereignisse, z.B. die mediale Berichterstattung zu einer neuen Cyberangriffswelle wie im Falle von Emotet, Einfluss auf das Antwortverhalten hatten. So könnten z.B. der Anteil der Unternehmen, die das Risiko von Cyberangriffen (eher) hoch bewerteten, überschätzt sein. Eine weitere Limitation liegt darin, dass aus forschungspragmatischen Gründen lediglich das Vorhandensein bestimmter Merkmale und Maßnahmen erfragt werden konnte und daher keine Aussagen zu qualitativen Unterschieden gemacht werden

können. Komplexe Fragekonstrukte und technisch-detaillierte Antwortmöglichkeiten sind durch die CATI-Methode nur im eigeschränkten Maße anwendbar.

Verglichen mit vielen anderen Studien, in denen das methodische Vorgehen und die Aussagekraft der Ergebnisse gar nicht oder nur oberflächlich berichtet und reflektiert wird und die teilweise auf Willkürstichproben zugrückgreifen, zählt insbesondere die transparent dokumentierte Ziehung einer geschichteten Zufallsstichprobe zu den Stärken dieser Studie. Unter Berücksichtigung der genannten Einschränkungen sind auf Basis der gewichteten Daten Rückschlüsse auf die Auswahlgesamtheit[204] und unter der Annahme, dass diese der Grundgesamtheit sehr nahe kommt, auch auf die Grundgesamtheit[205] möglich, was z.B. bei Willkürstichproben so gut wie ausgeschlossen ist. Die vergleichsweise große Nettostichprobe von 5.000 Unternehmen macht es zudem möglich, Ergebnisse und Zusammenhänge differenzierter darzustellen als in vielen Studien mit kleinerem Stichprobenumfang. Daneben ermöglicht die Nutzung von WZ08-Klassen zur Zuordnung der Branchenzugehörigkeit der Unternehmen zum einen die Vergleichbarkeit mit anderen offiziellen Unternehmensstatistiken, als auch die internationale Anschlussfähigkeit der Ergebnisse für bestimmte Branchen. Des Weiteren können durch die Erhebung zahlreicher struktureller Unternehmensmerkmale sowie IT-Sicherheitsmaßnahmen Zusammenhänge mit der Betroffenheit von Cyberangriffen analysiert und dargestellt werden.

[204] Unternehmen in Deutschland mit mehr als zehn Beschäftigten, die in den Firmendatenbanken von Bisnode und Heins & Partner erfasst sind.

[205] Unternehmen in Deutschland mit mehr als zehn Beschäftigten.

4 UNTERNEHMENSMERKMALE

Neben der bereits beschriebenen Beschäftigtengrößenklasse und der Branchenzugehörigkeit gibt es weitere Unternehmensmerkmale, die ebenfalls die Stichprobe beschreiben helfen, aber z.T. auch in einem späteren Schritt als Risiko- oder Schutzfaktoren in Zusammenhang mit der Betroffenheit von Cyberangriffen gebracht werden.

4.1 Bundesland

Das Bundesland, in dem sich der Unternehmensstandort befindet, wurde bei der Schichtung der Stichprobenziehung nicht einbezogen. Ein Vergleich der regionalen Verteilung der befragten Unternehmen in der gewichteten Stichprobe mit der regionalen Verteilung in der Grundgesamtheit (Tabelle 8) zeigt, dass sich diese sehr nahe kommen und damit auch diesbezüglich kein Hinweis auf eine systematische Verzerrung vorliegt.[206] Die größten Unterschiede finden sich bei Anteilen in Bayern, Nordrhein-Westfalen, Sachsen und Hessen, insofern, dass bayrische und sächsische Unternehmen im gewichteten Datensatz leicht überrepräsentiert und Unternehmen aus Nordrhein-Westfalen und Hessen leicht unterrepräsentiert sind.

Tabelle 8 **Stichprobe nach Bundesland**

	URS*		disproportionale Stichprobe		
	WZ08 (B-N, P-S)		ungewichtet		gewichtet
Standort	Anzahl	Prozent	Anzahl	Prozent	Prozent
Schleswig-Holstein	12.766	3,5	169	3,4	4,0
Hamburg	10.735	2,9	140	2,8	2,7
Niedersachsen	34.792	9,5	565	11,3	11,0
Bremen	3.625	1,0	46	0,9	0,4
Nordrhein-Westfalen	77.133	21,2	950	19,0	19,0
Hessen	27.588	7,6	304	6,1	5,8
Rheinland-Pfalz	16.393	4,5	196	3,9	4,4
Baden-Württemberg	49.458	13,6	712	14,2	12,6
Bayern	60.935	16,7	930	18,6	19,3
Saarland	3.920	1,1	59	1,2	1,1
Berlin	16.052	4,4	138	2,8	3,5
Brandenburg	9.465	2,6	144	2,9	2,6
Mecklenburg-Vorpommern	6.690	1,8	103	2,1	2,1
Sachsen	17.147	4,7	270	5,4	6,5
Sachsen-Anhalt	8.852	2,4	124	2,5	2,7
Thüringen	8.907	2,4	150	3,0	2,4
Gesamt	364.458	100,0	5.000	100,0	100,0

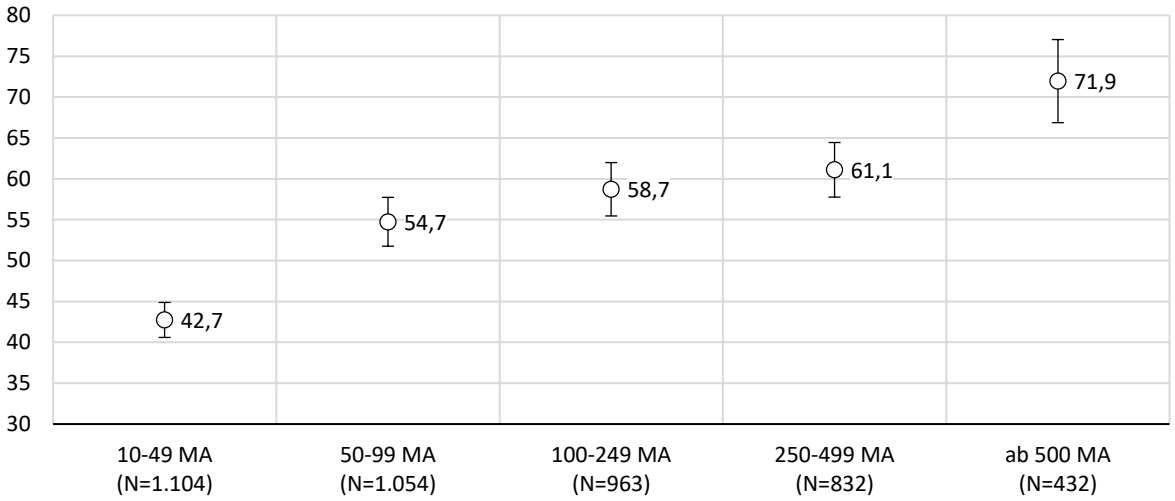
*) Quelle: Statistisches Bundesamt, 2017

[206] Den Vergleich einschränkend ist zu erwähnen, dass in Angaben aus dem URS keine Unternehmen der WZ08-A (Land- und Forstwirtschaft, Fischerei) und WZ08-O (Öffentliche Verwaltung, Verteidigung; Sozialversicherung) eingegangen sind.

4.2 Unternehmensalter

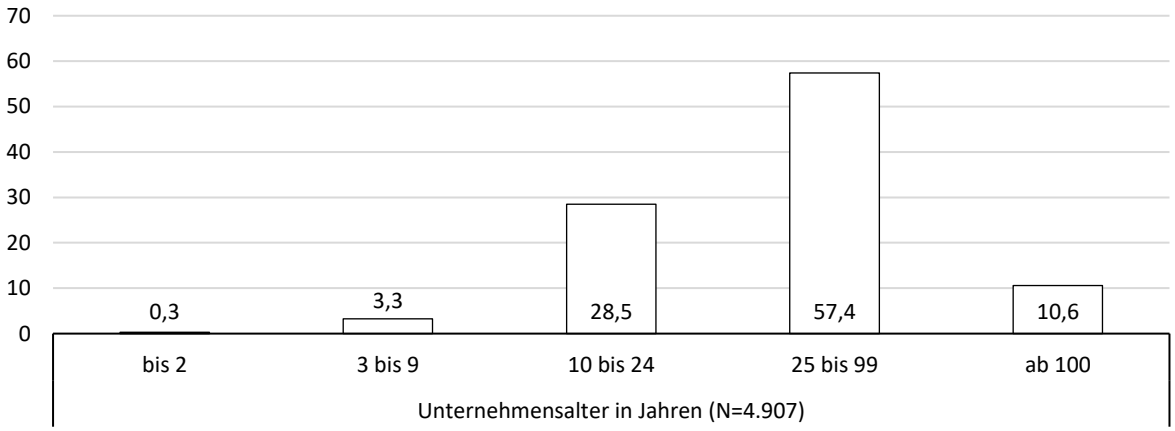
Das Alter des Unternehmens wurde anhand der konkreten Angaben zum Gründungsjahr berechnet und beträgt im Durchschnitt 56 und im Median 39 Jahre[207] (N=4.371). Dabei ergeben sich signifikante Unterschiede zwischen den verschiedenen Beschäftigtengrößenklassen (Abbildung 4) insofern, dass größere Unternehmen in Durchschnitt älter sind als kleinere.

Abbildung 4 **Durchschnittliches Unternehmensalter nach Beschäftigtengrößenklassen**
in Jahren, gewichtete Daten, 95%-KI



Befragte Vertreter*innen der Unternehmen, die das Gründungsjahr nicht genau angeben konnten (11,2 %), wurden gebeten das Unternehmensalter anhand einer vorgegebenen Skala zu schätzen.

Abbildung 5 **Anteil der Unternehmen nach Altersklassen**
in Prozent; gewichtete Daten



In Abbildung 5 sind die geschätzten und die anhand des Gründungsjahres berechneten Angaben zusammengefasst und klassiert dargestellt. Am stärksten ist die Klasse der 25 bis 99 Jahre alten Unternehmen vertreten (57,4 %) gefolgt von der Klasse der 10 bis 24 Jahre alten Unternehmen

[207] D.h., die Hälfte der befragten Unternehmen ist unter 39 Jahre und die andere Hälfte über 39 Jahre alt.

(28,5 %). Junge Unternehmen unter 10 Jahren haben nur einen sehr kleinen Anteil innerhalb der Stichprobe.[208]

4.3 Rechtsform

Die Rechtsform der teilnehmenden Unternehmen konnte den Firmendatenbanken entnommen und mussten somit nicht erfragt werden (Tabelle 9).

Tabelle 9 **Befragte Unternehmen nach Rechtsform**

	disproportionale Stichprobe		
	ungewichtet		gewichtet
Rechtsform	Anzahl	Prozent	Prozent
Gesellschaft mit beschränkter Haftung	2925	60,9	64,5
Gesellschaft mit beschränkter Haftung & Co. Kommanditgesellschaft	827	17,2	13,6
Eingetragene/r Kaufmann/Kauffrau	124	2,6	5,2
Aktiengesellschaft	139	2,9	1,9
Genossenschaft	177	3,7	4,7
Körperschaft/Anstalt des öffentlichen Rechts	224	4,7	1,9
Kommanditgesellschaft	48	1,0	0,7
Offene Handelsgesellschaft	31	0,6	1,4
Eingetragener Verein	224	4,7	5,0
Partnerschaftsgesellschaft	28	0,6	0,7
Stiftung	27	0,6	0,3
Gesamt	4.805	100,0	100,0

Die mit 64,5 % in der Stichprobe am häufigsten auftretende Rechtsform ist die Gesellschaft mit beschränkter Haftung (GmbH), gefolgt von der Gesellschaft mit beschränkter Haftung & Co. Kommanditgesellschaft (GmbH & Co. KG; 13,6 %).

Tabelle 10 **Verteilung der Unternehmen nach Rechtsform**

	URS[209]		disproportionale Stichprobe		
	WZ08 (B-N, P-S)		ungewichtet		gewichtet
Rechtsform	Anzahl	Prozent	Anzahl	Prozent	Prozent
Einzelunternehmer*innen	66.310	17,8	124	2,6	5,2
Personengesellschaften (zum Beispiel OHG, KG)	69.916	18,8	940	19,6	16,5
Kapitalgesellschaften (GmbH, AG)	200.328	53,8	3.076	64,0	66,3
Sonstige Rechtsformen	36.045	9,7	665	13,8	12,0
Gesamt	372.599	100,0	4.805	100,0	100,0

[208] Da die Stichprobe auf Basis einer Firmendatenbank gezogen wurde, ist es denkbar, dass insbesondere sehr junge Unternehmen noch nicht in diese aufgenommen wurden und damit möglicherweise unterrepräsentiert sind.

[209] Quelle: https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Unternehmensregister/Tabellen/unternehmen-rechtsformen-wzbefragunhtml (zuletzt geprüft am 06.05.2019).

Im Vergleich mit der Verteilung der Unternehmen ab zehn Beschäftigten nach Rechtsform im Unternehmensregistersystem des Statistischen Bundesamtes (Tabelle 10)[210] fällt auf, dass insbesondere die Einzelunternehmer innerhalb der Stichprobe unter- und die Kapitalgesellschaften überrepräsentiert sind.

4.4 Jahresumsatz

Der Jahresumsatz der Unternehmen stammt zu einem Teil aus der zugrunde liegenden Firmendatenbank und wurde zum anderen Teil erfragt.[211] Am stärksten sind Unternehmen mit einem Jahresumsatz von einer bis unter zwei Millionen EUR (25,0 %) und zwei bis unter zehn Millionen EUR (40,3 %) im gewichteten Datensatz vertreten (Tabelle 11).[212]

Tabelle 11 **Befragte Unternehmen nach Jahresumsatz**

		disproportionale Stichprobe		
		ungewichtet		gewichtet
Umsatzgrößenklasse		Anzahl	Prozent	Prozent
	unter 500.000 EUR	111	2,4	5,6
	500T bis unter 1 Mio. EUR	194	4,3	12,1
	1 bis unter 2 Mio. EUR	384	8,4	25,0
	2 bis unter 10 Mio. EUR	1.268	27,9	40,3
	10 bis unter 50 Mio. EUR	1.533	33,7	12,5
	50 bis unter 500 Mio. EUR	978	21,5	4,1
	500. Mio. EUR und mehr	83	1,8	0,3
	Gesamt	4.551	100,0	100,0

Da im Unternehmensregistersystem lediglich Angaben zu den Umsatzgrößenklassen über alle Unternehmen hinweg verfügbar sind, lässt sich die Verteilung in der Stichprobe der Unternehmen ab zehn Beschäftigten nicht mit einer entsprechenden Verteilung in der Grundgesamtheit vergleichen. Vor dem Hintergrund des Bias bei den Rechtsformen, wonach Einzelunternehmer*innen in der gewichteten Stichprobe schwächer vertreten sind als in der Grundgesamtheit, lässt sich vermuten, dass Unternehmen der unteren Umsatzgrößenklassen ebenfalls unterrepräsentiert sind.

Zusammen mit der Beschäftigtengrößenklasse lassen sich die befragten Unternehmen gemäß der KMU-Definition des Instituts für Mittelstandforschung (IfM) Bonn vom 01.01.2016 in kleine, mittlere und große Unternehmen einteilen. Demnach zählen Unternehmen bis 49 Beschäftigten und einem Umsatz bis 10 Mio. EUR/Jahr zu den kleinen[213] und bis 499 Beschäftigte

[210] Dazu wurden die im Sample vertretenen Rechtsformen folgendermaßen zusammengefasst: Einzelunternehmer (e. Kfm, e. Kfr), Personengesellschaften (GmbH & Co. KG, KG, OHG, AG & Co. KG, GbR, GmbH & Co OGH, PartG), Kapitalgesellschaften (GmbH, AG, Europa-AG, KGaA, Ltd.) und sonstige Rechtsformen (Gen., AdöR, KdöR, Stiftung, Eigenbetrieb, e.V., VVaG). Der Vergleich ist nur eingeschränkt möglich (siehe Fn. 206).

[211] Insbesondere dann, wenn Daten in der Firmendatenbank fehlten („Wie hoch war der Gesamtumsatz Ihres Unternehmens im letzten Geschäftsjahr?“).

[212] Bei einem Anteil von 9,0 % der Unternehmen lagen weder Angaben zum Jahresumsatz in der Firmendatenbank vor noch wurden dazu Angaben in der Befragung gemacht.

[213] Kleinstunternehmen (bis neun Beschäftigte und 2 Mio. EUR Jahresumsatz) bleiben in dieser unberücksichtigt.

und 50 Mio. EUR Jahresumsatz zu den mittleren Unternehmen.[214] Unternehmen ab 500 Beschäftigte zählen demzufolge zu den Großunternehmen.

Tabelle 12 **Befragte Unternehmen nach KMU-Zugehörigkeit**

	disproportionale Stichprobe		
	ungewichtet		gewichtet
	Anzahl	Prozent	Prozent
Kleinstunternehmen (bis 9 Besch. u. bis 2 Mio. EUR Jahresumsatz)	0	0,0	0,0
Kleine Unternehmen (bis 49 Besch. u. bis 10 Mio. EUR Jahresumsatz)*	1.103	22,1	74,4
Mittlere Unternehmen (bis 499 Besch. u. bis 50 Mio. EUR Jahresumsatz)**	2.749	55,0	21,0
Großunternehmen (ab 500 Besch.)	1.148	23,0	4,6
Gesamt	5.000	100,0	100,0

*) und kein Kleinstunternehmen
**) und kein Kleinst- oder Kleinunternehmen

In der gewichteten Stichprobe gehören etwa drei Viertel der Unternehmen (74,4 %) zu den kleinen, etwas über ein Fünftel (21,0 %) zu den mittleren und 4,6 % zu den großen Unternehmen (Tabelle 12).[215]

4.5 Anzahl der Standorte

Die teilnehmenden Unternehmensvertreter*innen wurden danach gefragt, wie viele Standorte ihr Unternehmen mit eigener IT-Infrastruktur in Deutschland und im Ausland hat. Ein Anteil von 71,5 % der befragten Unternehmen hat im gewichteten Datensatz nur einen Standort in Deutschland (Tabelle 13). Ein weiteres Viertel (26,0 %) hat zwischen zwei und neun Standorte im Inland. Bezogen auf Standorte im Ausland ist das Bild noch eindeutiger: 93,4 % gaben an, keinen Standort mit eigener IT-Infrastruktur im Ausland zu betreiben, 6,6 % berichten von mindestens einem Standort im Ausland.

[214] Quelle: https://www.ifm-bonn.org/definitionen/kmu-definition-des-ifm-bonn/ (aufgerufen am 07.06.2019). Eine hinsichtlich der Beschäftigtengrößenklasse abweichende KMU-Definition wird von der Europäischen Kommission verwendet: zu den mittleren Unternehmen werden nur solche mit bis zu 249 Beschäftigten und 50 Mio. EUR Jahresumsatz bzw. 43 Mio. EUR Jahresbilanzsumme gezählt (Quelle: http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/ (aufgerufen am 07.06.2019)).

[215] Unternehmen, bei denen Angaben zum Jahresumsatz fehlten, wurden allein auf Grundlage der Beschäftigtengrößenklasse zugeordnet.

Tabelle 13 **Befragte Unternehmen nach Anzahl der Standorte im In- und Ausland**

		disproportionale Stichprobe		
		ungewichtet		gewichtet
Anzahl der Standorte mit eigener IT-Infrastruktur		Anzahl	Prozent	Prozent
in Deutschland	1	2.826	57,6	71,5
	2 bis 9	1.735	35,4	26,0
	10 bis 24	203	4,1	1,4
	25 bis 99	113	2,3	0,9
	100 und mehr	26	0,5	0,1
	Gesamt	4.903	100,0	100,0
im Ausland	0	4.199	85,7	93,4
	1	255	5,2	3,7
	2 bis 9	318	6,5	2,3
	10 bis 24	60	1,2	0,2
	25 bis 99	41	0,8	0,2
	100 und mehr	25	0,5	0,2
	Gesamt	4.898	100,0	100,0

4.6 Exporttätigkeit

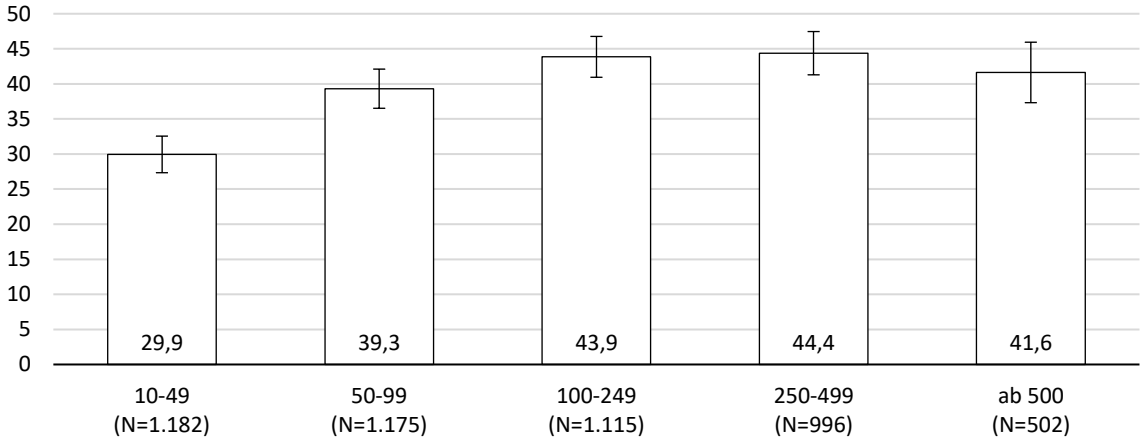
Die Frage, ob das Unternehmen Produkte oder Dienstleistungen in das Ausland exportiert, bejahten knapp ein Drittel der Unternehmensvertreter*innen (32,5 %) im gewichteten Datensatz.

Tabelle 14 **Befragte Unternehmen nach Exporttätigkeit**

		disproportionale Stichprobe		
		ungewichtet		gewichtet
Export von Produkten oder Dienstleistungen		Anzahl	Prozent	Prozent
	Ja	1.997	40,2	32,5
	Nein	2.972	59,8	67,5
	Gesamt	4.969	100,0	100,0

Im Vergleich der Beschäftigtengrößenklassen sind dabei statistisch signifikante Unterschiede zu erkennen (Abbildung 6). Insbesondere der Anteil der exportierenden kleinen Unternehmen liegt mit 29,9 % deutlich unter den Anteilen der größeren Unternehmen, von denen etwa zwei Fünftel im Exportgeschäft tätig sind.

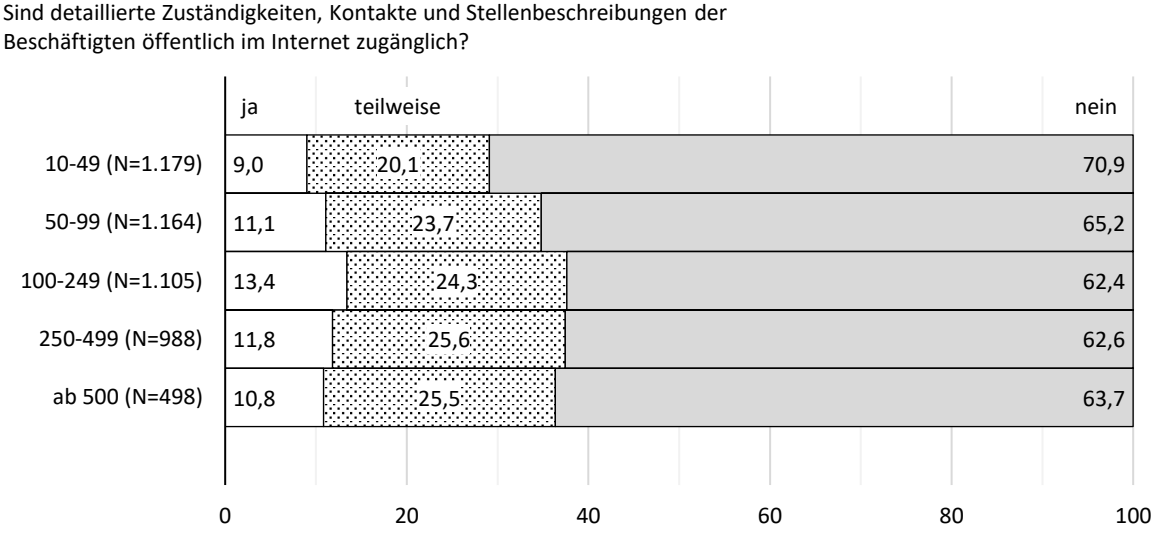
Abbildung 6 **Anteil exportierender Unternehmen nach Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI



4.7 Öffentlich zugängliche Informationen zu Beschäftigten

Die Verfügbarkeit von Informationen zu den Beschäftigten der Unternehmen könnte Angriffsarten wie Social Engineering und Phishing fördern und wurde mit der Frage erhoben: „Sind detaillierte Zuständigkeiten, Kontakte und Stellenbeschreibungen der Beschäftigten öffentlich im Internet zugänglich?“. Als Antwortmöglichkeiten standen „ja“, „teilweise“ und „nein“ zur Auswahl. Über zwei Drittel der befragten Unternehmen verneinte die Frage und macht demnach keine derartigen Informationen öffentlich online verfügbar (69,5 %; N=4.948). Etwa jedes zehnte Unternehmen bejahte die Frage und ein Fünftel veröffentlicht derartige Unternehmensinformationen zumindest teilweise im Internet (21,0 %). Auch dabei zeigen sich statistisch relevante Unterschiede zwischen den Beschäftigtengrößenklassen, wonach kleine Unternehmen seltener mit derartigen Informationen im Internet präsent sind als größere (Abbildung 7).

Abbildung 7 **Im Internet öffentl. zugängliche Beschäftigteninfos nach Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten



5 IT-SICHERHEITSSTRUKTUR IM UNTERNEHMEN

Die IT-Sicherheitsstrukturen von Unternehmen bieten einerseits weitere Merkmale zur Beschreibung der Stichprobe. Andererseits nehmen diese Merkmale auch eine zentrale Position bei der Erklärung von Unterschieden hinsichtlich der Betroffenheit von verschiedenen Formen von Cyberangriffen ein. Wie in Abschnitt 2.4.4 dargestellt, berichten verschiedene Studien über das Vorhandensein bestimmter IT-Sicherheitsmerkmalen. Jedoch werden diese i.d.R. rein deskriptiv und unabhängig von den Prävalenzen dargestellt.[216] Im Folgenden werden die Sicherheitsstrukturmerkmale zunächst ebenfalls alleinstehend beschrieben und in Kapitel 10 in Zusammenhang mit der Betroffenheit bzw. Nichtbetroffenheit von Cyberangriffen als potentielle Schutzfaktoren diskutiert.

5.1 IT-Beschäftigte

Ein erstes Merkmal betrifft die Anzahl von Beschäftigten im Unternehmen, die mit dem Betrieb der IT insgesamt und speziell mit der IT- & Informationssicherheit hauptsächlich beschäftigt sind.

Tabelle 15 **Befragte Unternehmen nach IT-Beschäftigten**

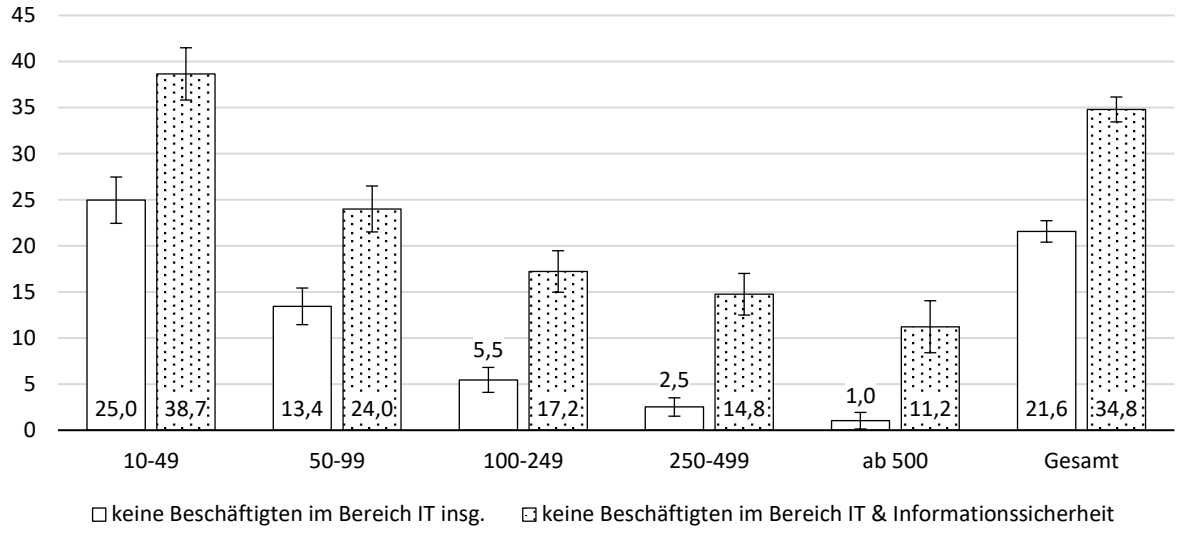
		disproportionale Stichprobe		
		ungewichtet		gewichtet
Beschäftigte im Bereich der IT insg.		Anzahl	Prozent	Prozent
	0	517	10,8	21,6
	1	1.091	22,8	30,0
	2 bis 9	2.375	49,7	39,4
	10 bis 24	405	8,5	5,1
	25 bis 99	280	5,9	2,9
	100 und mehr	111	2,3	1,0
	Gesamt	4.779	100,0	100,0
Davon sind … im Bereich der IT- & Informationssicherheit tätig.				
	0	562	13,2	16,8
	1	1.979	46,6	54,0
	2 bis 9	1.583	37,3	27,4
	10 bis 24	85	2,0	1,3
	25 bis 99	26	0,6	0,3
	100 und mehr	9	0,2	0,2
	Gesamt	4.244	100,0	100,0

[216] Eine Ausnahme hiervon bildet beispielsweise Rantala (2008), die Outsourcing von IT-Funktionen mit den Prävalenzen in Zusammenhang stellt.

Etwa ein Fünftel der Unternehmen ab zehn Beschäftigten (21,6 %) hat keine Beschäftigte, die den überwiegenden Teil ihrer Arbeitszeit in den Betrieb der IT investiert (Tabelle 15). Ein Anteil von 30,0 % beschäftigt in diesem Bereich eine/n Beschäftigte*n und die übrige Hälfte der Unternehmen mindestens zwei.

Bei den Unternehmen, die mindestens eine*n IT-Beschäftigte*n haben, ist in den meisten Fällen auch mindestens eine*r speziell für den Betrieb der IT- & Informationssicherheit zuständig (eine Person: 54,0 %; mindestens zwei Personen: 29,2 %).

Abbildung 8 **Befragte Unternehmen ohne IT-Beschäftigte nach Beschäftigtengrößenklassen**
in Prozent; gewichtete Daten; 95%-KI



Ob und wie viele Beschäftigte in den Unternehmen überwiegend im Bereich IT insgesamt und IT- & Informationssicherung arbeiten, steht im Zusammenhang mit der Beschäftigtengrößenklasse. In Abbildung 8 ist zu erkennen, dass knapp zwei Fünftel der kleinen Unternehmen (10-49 Besch.) keine Beschäftigten für den Bereich IT- & Informationssicherheit hat (38,7 %; N=1.133) und ein Viertel dieser Unternehmen beschäftigte auch keine Beschäftigten im Bereich der IT insgesamt (25,0 %). Je größer das Unternehmen ist, desto kleiner werden dies Anteile. Dennoch hat auch jedes neunte große Unternehmen (ab 500 Besch.) keine Beschäftigten für den Bereich IT- & Informationssicherheit (11,2 %; N=481). Die Nicht-Beschäftigung von Beschäftigten in diesen IT-Bereichen hängt damit zusammen, ob IT-Funktionen an externe Dienstleister ausgelagert wurden oder nicht. Klahr et al. beziffern für britische Unternehmen das Vorhandensein von Mitarbeiter*innen deren Stellenbeschreibungen Informationssicherheit oder Governance beinhaltet etwas geringer, und nennen einen Anteil von insgesamt 38% (10-49 Besch.: 46%; 50-249 Besch.: 61%: >250 Besch.: 73%).[217] Hingegen berichten Hillebrand et al. von höheren Anteilen an Mitarbeitern mit IT-Sicherheitskenntnissen (< 49 Besch. 54%, > 49 Besch. 85%).[218]

[217] Vgl. Klahr et al. (2017).

[218] Vgl. Hillebrand et al. (2017: 56).

5.2 Ausgelagerte IT-Funktionen

Insgesamt betrachtet, nutzt lediglich ein relativ kleiner Anteil von 18,6 % der Unternehmen ab zehn Beschäftigte keine externen Dienstleister für ausgelagerte IT-Funktionen (Tabelle 16). Ein großer Anteil (81,4 %) hat mindestens eine IT-Funktion an externe Dienstleister ausgelagert. Mit 76,0 % am häufigsten wird dabei der Webauftritt der Unternehmen von externen Dienstleistern übernommen, gefolgt von der Netzwerk-Administration und Wartung (63,0 %), der IT-Security (49,3 %) und dem Betrieb von E-Mail und Kommunikation (48,8 %). Vergleichsweise selten werden Cloud-Software und Cloud-Speicher von externen Dienstleistern genutzt (36,8 %) oder sonstige IT-Funktionen ausgelagert (10,8 %).[219] Der Anteil ausgelagerter IT-Sicherheit wurde auch von Klahr et al. erhoben und wird ebenfalls mit insgesamt 49% (10-49 Besch.: 58%; 50-249 Besch.: 64%; >500 Besch.: 49%) der befragten Unternehmen beziffert, wobei mit zunehmender Unternehmensgröße die Angaben beider Studien weiter auseinandergehen (vgl. Abbildung 9).[220]

Tabelle 16 **Befragte Unternehmen nach ausgelagerten IT-Funktionen**
Mehrfachantworten hinsichtlich der IT-Funktionen möglich

		disproportionale Stichprobe		
		ungewichtet		gewichtet
IT-Funktion(en) ausgelagert?		Anzahl	Prozent	Prozent
	Nein	817	16,6	18,6
	Ja	4.116	83,4	81,4
	Gesamt	4.933	100,0	100,0
Wenn „Ja“, in welchem Bereich?				
	E-Mail & Kommunikation	1.876	45,6	48,8
	Netzwerk-Administration & Wartung	2.267	55,1	63,0
	Webauftritt	3.297	80,1	76,0
	Cloud-Software & Cloud-Speicher	1.597	38,8	36,8
	IT-Security	1.872	45,5	49,3
	Sonstiges	550	13,4	10,8

Im Vergleich der Unternehmen nach Beschäftigtengrößenklassen hinsichtlich der Frage, ob externe Dienstleister bestimmte IT-Funktionen übernehmen, fallen lediglich kleine Unterschiede auf. Am seltensten bejahten diese Frage Unternehmen mit zehn bis 49 Beschäftigten (80,5 %) und am häufigsten Unternehmen mit 50 bis 99 bzw. 250 bis 499 Beschäftigten (jeweils 85,7 %).[221]

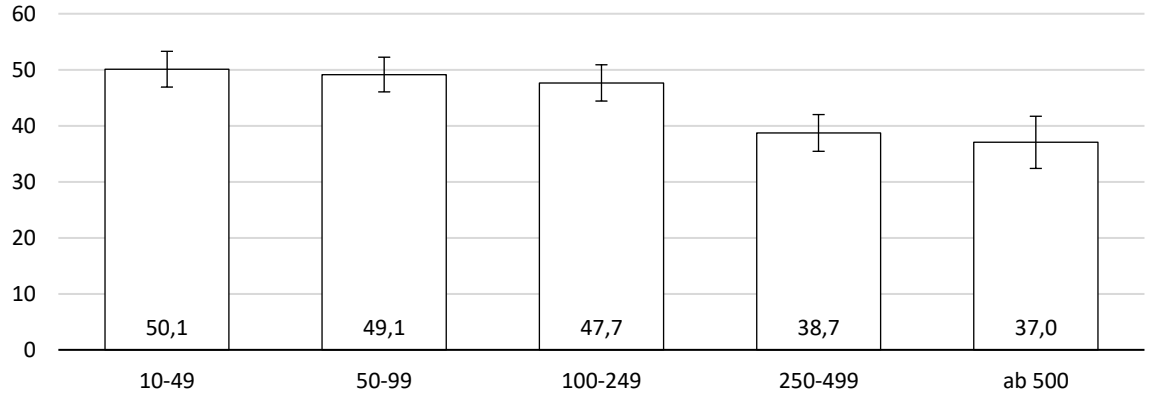
Bezogen auf die Auslagerung der IT-Security finden sich hingegen signifikante Unterschiede zwischen den Beschäftigtengrößenklassen: Kleine Unternehmen beauftragen in diesem Bereich häufiger Dienstleister als große Unternehmen (Abbildung 9).

[219] Die Kategorie „Sonstiges“ kann bei dieser Frage nicht aufgelöst werden, da aus zeitökonomischen Gründen bei den Interviews nicht immer freitextliche Angaben erhoben werden konnten.

[220] Vgl. Klahr et al. (2017).

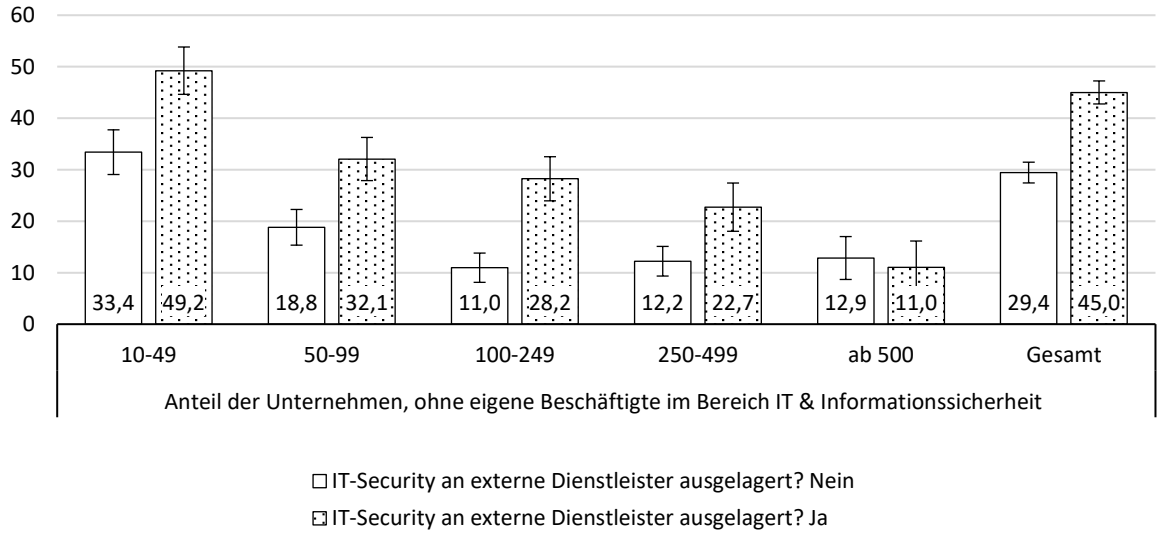
[221] Unternehmen mit 100-249 Besch.: 83,0 %; Unternehmen ab 500 Besch.: 82,3 %.

Abbildung 9 **Anteil der Unternehmen mit ausgelagerter IT-Security nach Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten, 95%-KI



Wird die Information, ob externe IT-Dienstleister genutzt werden oder nicht, in Zusammenhang mit den Informationen zur Beschäftigung von internen Mitarbeiter*innen im IT-Bereich gesetzt, dann zeigt sich erwartungsgemäß, dass Unternehmen, die externe IT-Dienstleister nutzen, signifikant häufiger keine eigenen Mitarbeiter*innen im Bereich IT insgesamt (23,1 %) und für die IT und Informationssicherheit (37,1 %) beschäftigen als Unternehmen, die keine IT-Funktionen ausgelagert haben (14,8 % bzw. 24,9 %). Unter zusätzlichem Einbezug der Beschäftigtengrößenklasse zeigt sich weiter, dass dies bezogen auf die IT insgesamt nur für kleine und mittlere Unternehmen (bis 249 Besch.) zutrifft. Große Unternehmen (ab 250 Besch.) haben mit wenigen Ausnahmen in jedem Fall eigene IT-Beschäftigte, ob sie auf externe IT-Dienstleister zurückgreifen oder nicht.

Abbildung 10 **Befragte Unternehmen ohne Beschäftigte im Bereich IT & Informationssicherheit**
in Prozent; gewichtete Daten, 95%-KI



Mit Blick auf den Zusammenhang von ausgelagerter IT-Security und Beschäftigung eigener Mitarbeiter*innen im Bereich IT & Informationssicherheit ist in Abbildung 10 einerseits zu erkennen, dass mit Ausnahme der großen Unternehmen (ab 500 Besch.) die Anteile von Unternehmen ohne eigene Beschäftigte im Bereich IT & Informationssicherheit bei denjenigen signifikant größer sind, die externe Dienstleister mit der IT-Security betraut haben. Zum anderen zeigt sich, dass es gerade bei den kleinen Unternehmen (10-49 Besch. und 50-99 Besch.) relativ

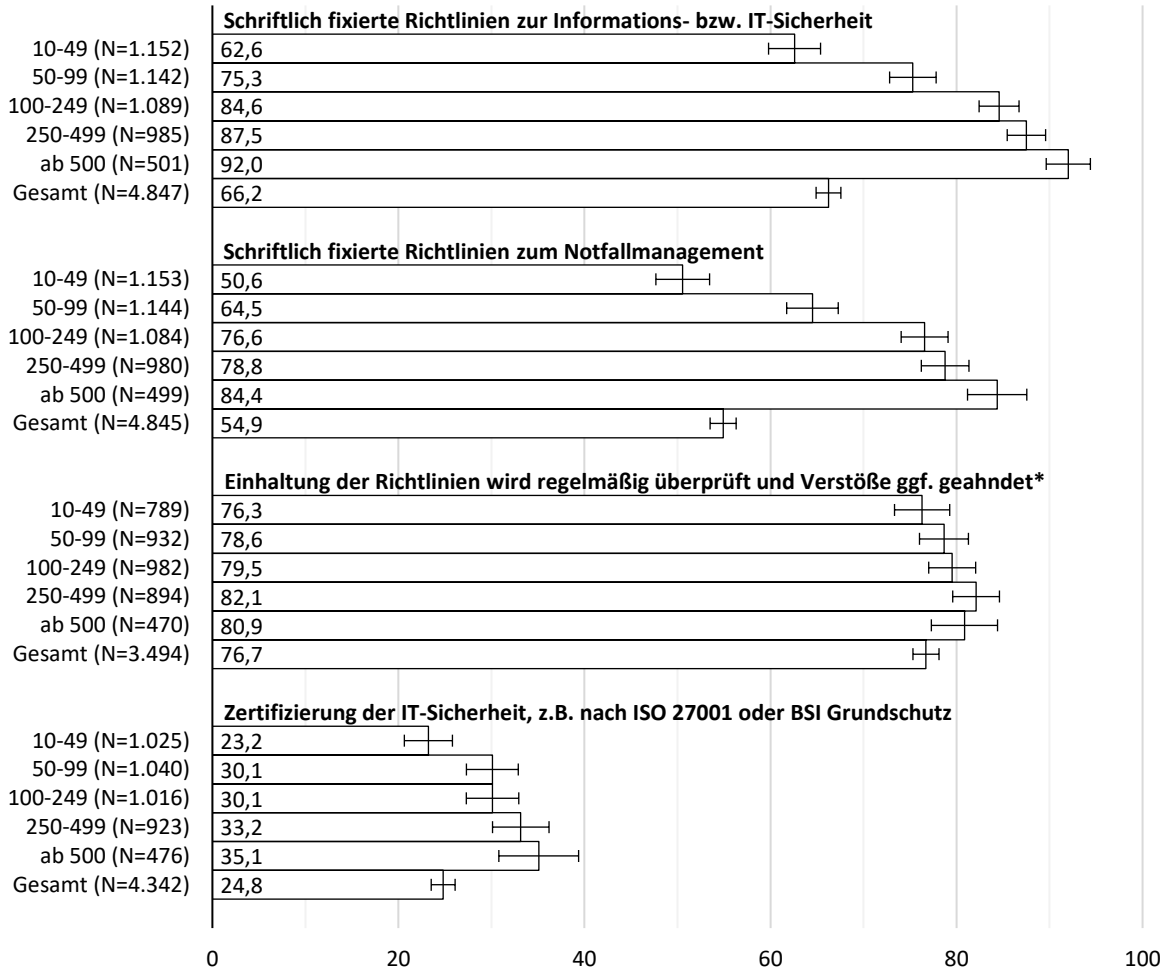
große Anteile gibt, die weder eigene spezialisierte IT-Beschäftigte noch externe Dienstleister für die IT-Security haben (33,4 % bzw. 18,8 %; N=455 bzw. 489).

5.3 IT-Sicherheitsmaßnahmen

5.3.1 Organisatorische Maßnahmen

Organisatorische Maßnahmen, wie schriftlich fixierte Richtlinien zur Informations- bzw. IT-Sicherheit oder zum Notfallmanagement sind in vielen Unternehmen ab zehn Beschäftigte vorhanden (66,2 % bzw. 54,9 %; N=4.847; Abbildung 11).[222]

Abbildung 11 **Unternehmen mit Richtlinien und Zertifizierungen nach Beschäftigtengrößenklassen**
in Prozent; gewichtete Daten, 95%-KI



*) Nur Unternehmen, die schriftlich fixierte Richtlinien haben

Davon überprüfen drei Viertel (76,7 %; N=3.494) deren Einhaltung regelmäßig und ahnden ggf. Verstöße. Mit Blick auf ähnliche Erhebungen weisen Hillebrand et al. den Anteil der Unternehmen mit schriftlichen Regelungen zur IT-Sicherheit (> 49 Besch.: 22 %; < 49 Besch.: 68 %) und Notfallmanagement (> 49 Besch.: 29 %; < 49 Besch.: 71 %) geringer aus,[223] was

[222] Angaben zum Umfang und Inhalt solcher Richtlinien wurden nicht erhoben.

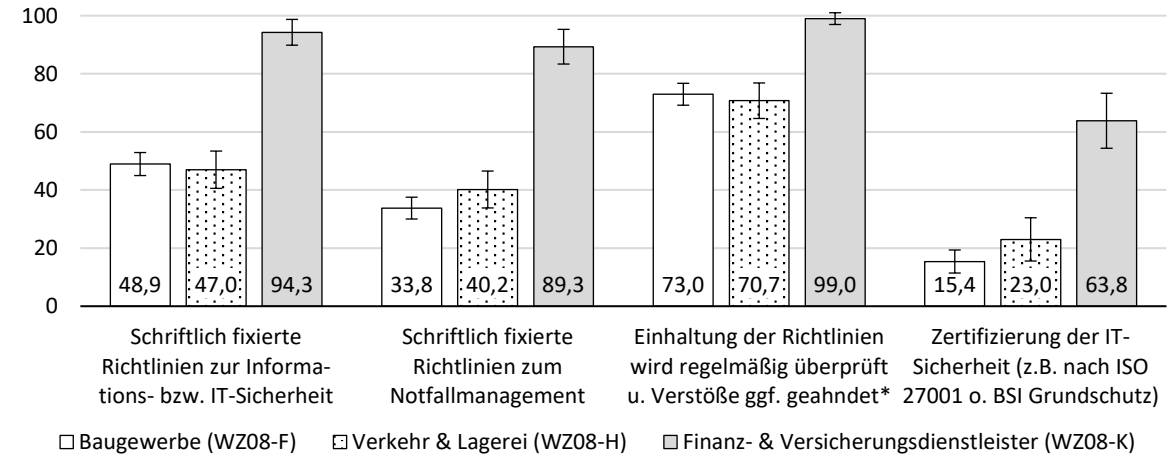
[223] Vgl. Hillebrand et al. (2017).

allerdings auch daran liegen kann, dass dort auch Unternehmen mit 0-9 Mitarbeitern berücksichtigt wurden. Gerade im Hinblick auf größere Unternehmen nähern sich die Ergebnisse beider Studien an. Auch Klahr et al. beziffern die Anteile der Unternehmen mit formalen Richtlinien die Cybersicherheitsrisiken betreffen insgesamt deutlich geringer (10-49 Besch.: 39%; 50-249 Besch.: 59%; >500 Besch.: 71%).[224]

Die Zertifizierung der IT-Sicherheit (z.B. nach ISO 27001[225] oder dem BSI Grundschutz[226]) ist vergleichsweise selten aber dennoch überraschend weit verbreitet; etwa ein Viertel der Unternehmen ab zehn Beschäftigten gibt eine zertifizierte IT-Sicherheit an. Hierzu ist allerdings anzumerken, dass diese Frage von 12,1 % der Unternehmensvertreter*innen aufgrund fehlender Kenntnis nicht beantwortet werden konnte und sich die Anzahl der gültigen Fälle dadurch reduziert. Die Bitkom-Studie beziffert den Anteil der Befragten, die eine Sicherheits-Zertifizierung (z.B. nach ISO 27001, BSI Grundschutz o.ä.) haben, allerdings mit Fokus auf Industrieunternehmen, mit rund 49 % deutlich höher.[227] Auch die Bundesdruckerei nennt in ihrer Umfrage einen Anteil an Unternehmen mit Sicherheits-Zertifizierungen in Höhe von 45 %.[228]

Im Vergleich der Unternehmen nach Beschäftigtengrößenklassen ist, wie erwartet, zu erkennen, dass in kleineren Unternehmen die Verbreitung dieser Maßnahmen z.T. signifikant geringer ist als in den großen. Beispielweise existiert in etwa zwei Dritteln der kleinen Unternehmen (10-49 Besch.) eine Richtlinie zur Informations- bzw. IT-Sicherheit (62,6 %; N=1.152) aber fast in jedem großen Unternehmen (ab 500 Besch.: 92,0 %; N=501).

Abbildung 12 **Unternehmen mit Richtlinien und Zertifizierungen nach WZ08-Klassen (F, H, K)**
in Prozent; gewichtete Daten; 95%-KI



*) Nur Unternehmen, die schriftlich fixierte Richtlinien haben

[224] Vgl. Klahr et al. (2017).

[225] Die internationale Norm ISO 27001 bezieht sich auf verschiedene Bereiche von Informationssicherheits-Managementsystemen. Dabei ist zu berücksichtigen, dass die Internationale Organisation für Normung (ISO) selbst keine Zertifizierungen durchführt, sondern diese lediglich erstellt. Dass ein Unternehmen ISO-Konformität erlangt hat, kann es selbst verkünden, von Geschäftspartnern und Kunden bestätigen lassen oder über ein externes Auditverfahren feststellen und zertifizieren lassen (Kersten et al. 2016).

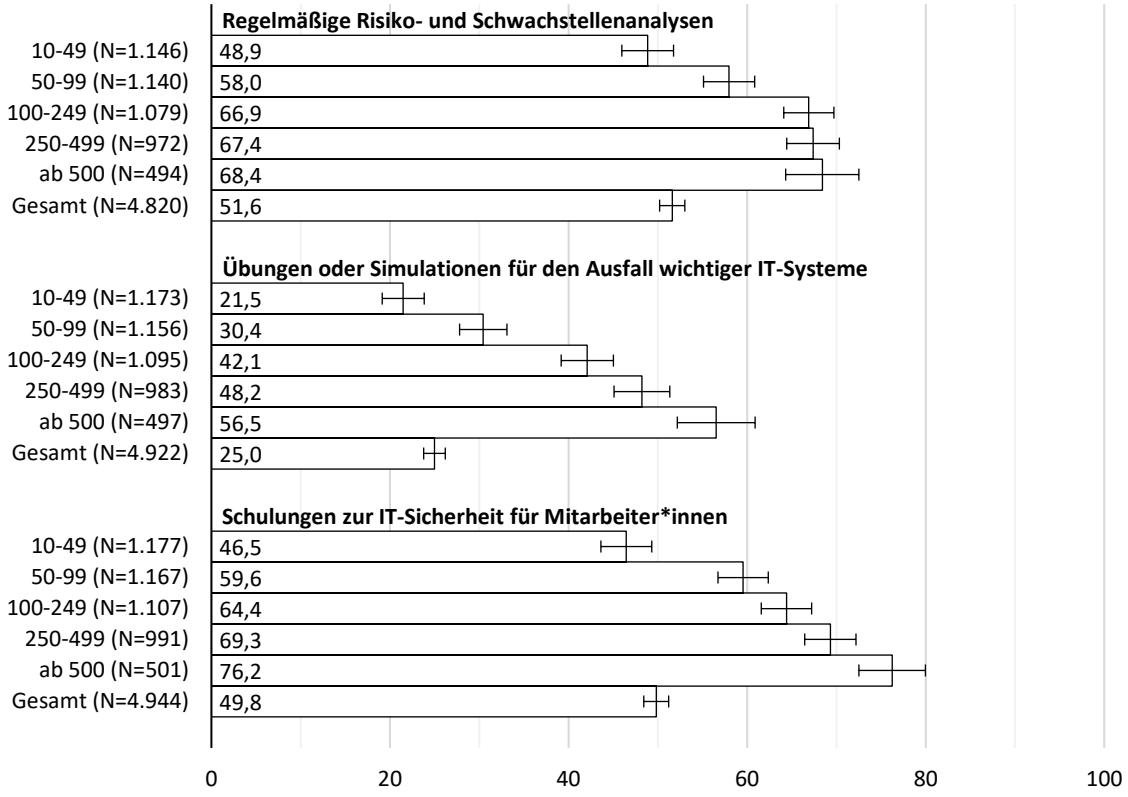
[226] Die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zielen auf die Informationssicherheit von Organisationen sowie den Aufbau eines Managementsystems für Informationssicherheit (ISMS) und sollen dabei ISO 27001-kompatibel sein (Quelle: https://www.bsi.bund.de). Siehe dazu auch (Kersten et al. 2016).

[227] Vgl. Bitkom e.V. (2018).

[228] Vgl. Bundesdruckerei GmbH (2017)..

Mit Blick auf die Branchenzugehörigkeit der Unternehmen sind ebenfalls deutliche Unterschiede feststellbar. Exemplarisch dafür werden in Abbildung 12 die Wirtschaftszweige F, H und K miteinander verglichen.[229] WZ08-F und H (Baugewerbe und Verkehr & Lagerei) haben insgesamt betrachtet die kleinsten Anteile hinsichtlich vorhandener organisatorischer und technischer IT-Sicherheitsmaßnahmen, während WZ08-K (Finanz- u. Versicherungsdienstleister) mit einer Ausnahme[230] durchgehend die größten Anteile aufweist und hierbei als Positivbeispiel dient. So haben fast alle Finanz- und Versicherungsdienstleister schriftlich fixierte Richtlinien zur Informations- bzw. IT-Sicherheit (94,3 %; N=105) sowie zum Notfallmanagement (89,3 %; N=103) und überprüfen diese auch regelmäßig (99,0 %; N=94). Demgegenüber liegen diese Anteile der anderen beiden Wirtschaftszweige signifikant und deutlich erkennbar darunter. Dabei muss allerdings beachtet werden, dass z.B. der Anteil an kleinen Unternehmen (10-49 Besch.) in der Gruppe der Finanz- und Versicherungsdienstleister kleiner ist als in den anderen beiden WZ-Klassen.

Abbildung 13 Unternehmen mit Analysen, Übungen u. Schulungen z. IT-Sicherheit nach Beschäftigtengrößenklassen
in Prozent; gewichtete Daten; 95%-KI



Etwa die Hälfte der Unternehmen ab zehn Beschäftigten führt regelmäßige Risiko- und Schwachstellenanalysen durch (51,6 %) und schult seine Beschäftigten zur IT-Sicherheit (49,8 %). Für britische Unternehmen berichten Klahr et al. von geringeren Schulungsquoten innerhalb der letzten 12 Monate (10-49 Besch.: 25 %; 50-249 Besch.: 43 %; >250 Besch.: 63 %).[231] Auch das aktive technische Testing (z.B. Penetrationstests) wird geringer angegeben

[229] Die Anteile vorhandener IT-Sicherheitsmaßnahmen nach den WZ-Klassen der ersten und zweiten Ebene findet sich im Anhang in Tabelle 45 bis Tabelle 48.

[230] Die Ausnahme betrifft das Vorhandensein physisch getrennter Backups, wobei der Unterschied zu den WZ08-Klassen mit höheren Anteilen statistisch nicht signifikant ist.

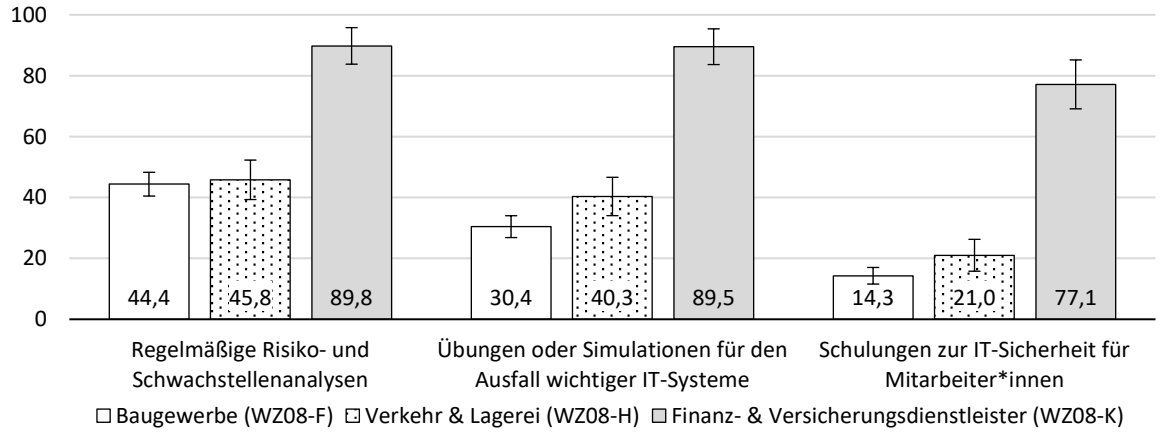
[231] Vgl. Klahr et al. (2017).

(25 %). Hinsichtlich der Schulungsquoten nennt die Bundesdruckerei mit 46 % jedoch ähnliche Ergebnisse wie diese Studie.[232]

Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme werden von einem Viertel (25,0 %) durchgeführt (Abbildung 13). Auch hierbei ist der Zusammenhang mit der Beschäftigtengrößenklasse der Unternehmen deutlich zu erkennen, insofern die Anteile der größeren Unternehmen, die diese IT-Sicherheitsmaßnahmen durchführen, größer ist als bei den Kleineren. So führt etwa lediglich ein Fünftel der kleinen Unternehmen (10-49 Besch.) Übungen oder Simulationen zum Ausfall von IT-Systemen durch (21,5 %), während diese Maßnahme von über der Hälfte der großen Unternehmen (ab 500 Besch.) eingesetzt wird (56,5 %).

Neben Unterschieden im Vergleich der Beschäftigtengrößenklasse der Unternehmen sind wiederum auch Unterschiede bezüglich der Branchenzugehörigkeit zu erkennen (Abbildung 14). Während neun von zehn Unternehmen der Finanz- und Versicherungsbranche (WZ08-K) regelmäßiges Risiko- und Schwachstellenanalysen sowie Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme durchführen, werden diese Maßnahmen lediglich von vier bzw. drei von zehn Unternehmen des Baugewerbes (WZ08-F) eingesetzt. Noch deutlicher fällt der Unterschied in Hinblick auf die Durchführung von Schulungen zur IT-Sicherheit aus: Knapp acht von zehn Unternehmen der Finanz- und Versicherungsdienstleister stehen einem bis zwei von zehn Unternehmen des Baugewerbes gegenüber, die auf Schulungen setzen.

Abbildung 14 **Unternehmen mit Analysen, Übungen und Schulungen nach WZ08-Klassen (F, H, K)**
in Prozent; gewichtete Daten; 95%-KI



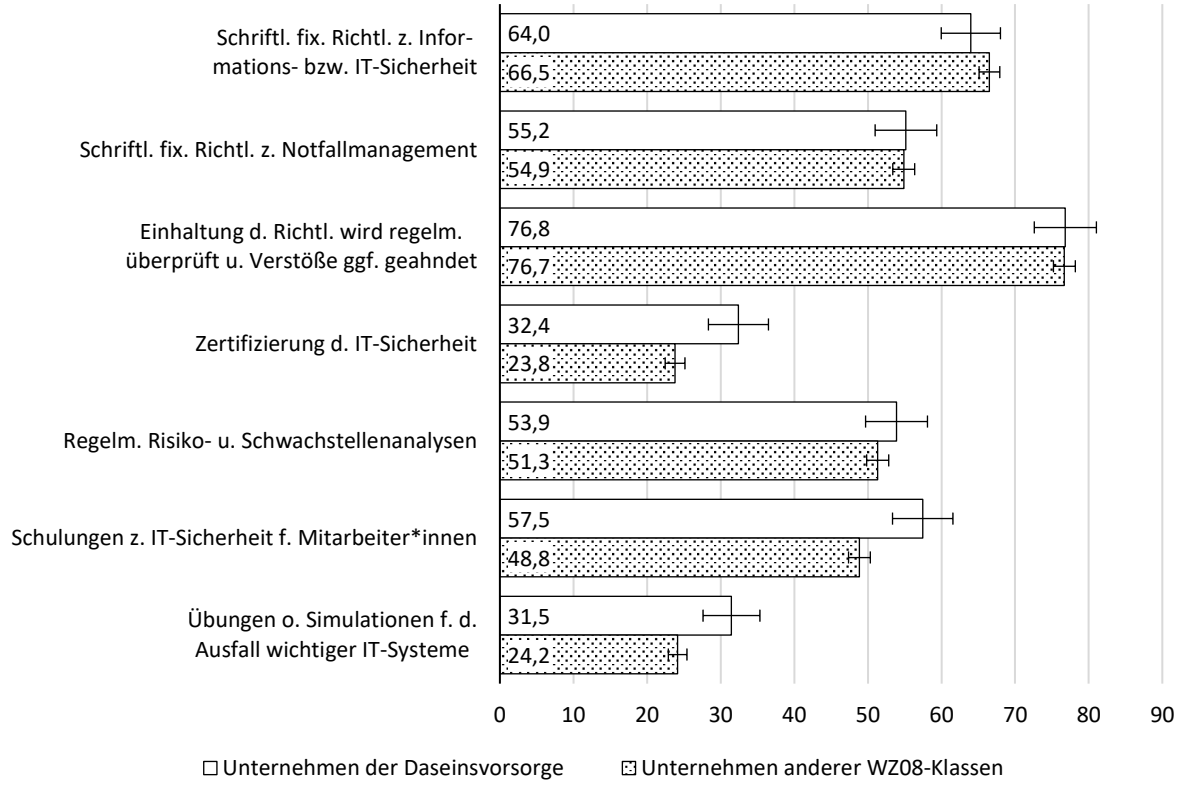
Auf der zweiten Ebene der WZ08-Klassen fallen folgende Wirtschaftszweige mit relativ niedrigen Anteilen bei den organisatorischen IT-Sicherheitsmaßnahmen auf[233]: WZ08-16 (Herstellung von Holz-, Flecht-, Korb- und Korkwaren (ohne Möbel), WZ08-23 (Herstellung von Glaswaren, Keramik, Verarbeitung von Steinen und Erden) sowie WZ08-31 (Herstellung von Möbeln). Demgegenüber liegen die Anteile von WZ08-64 (Finanzdienstleistung), WZ08-62 (Dienstleistungen der Informationstechnologie) und WZ08-79 (Reisebüros, -veranstalter und sonstige Reservierungen) im oberen Bereich.

232 Vgl. Bundesdruckerei GmbH (2017).

233 Siehe Tabelle 47 im Anhang 1.

Im Vergleich von Unternehmen nach Zugehörigkeit zur Daseinsvorsorge[234] (Abbildung 15) zeigt sich, dass Zertifizierungen im Bereich der IT-Sicherheit, Schulungen zur IT-Sicherheit für Beschäftigten sowie Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme anteilig häufiger bei Unternehmen der Daseinsvorsorge zu finden sind (32,4 %, 57,5 % bzw. 31,5 %) als bei Unternehmen der anderen WZ08-Klassen (23,8 %, 48,8 % bzw. 24,2 %). Bezüglich der übrigen organisatorischen Maßnahmen finden sich keine statistisch relevanten Unterschiede.

Abbildung 15 **Organisatorische IT-Sicherheitsmaßnahmen nach Zugehörigkeit zur Daseinsvorsorge**
in Prozent; gewichtete Daten; 95%-KI



5.3.2 Technische Maßnahmen

In Hinblick auf die Verbreitung technischer Maßnahmen zur Erhöhung der IT-Sicherheit fällt auf, dass diese allgemein relativ hoch ist (Abbildung 16 und Abbildung 19) und sich die Anteile der Beschäftigtengrößenklassen nicht mehr so deutlich unterscheiden wie bei den organisatorischen Sicherheitsmaßnahmen. Diesbezüglich scheint es inzwischen gewisse Standards zu geben, die von den meisten Unternehmen ab zehn Beschäftigten umgesetzt werden. Aussagen dazu, wie wirksam und effizient die Umsetzung der einzelnen Maßnahmen ist, können hingegen nicht getroffen werden. Die größten signifikanten Unterschiede finden sich in Hinblick auf Mindestanforderungen an Passwörter[235] und die individuelle Vergabe von Zugangs- und Nut-

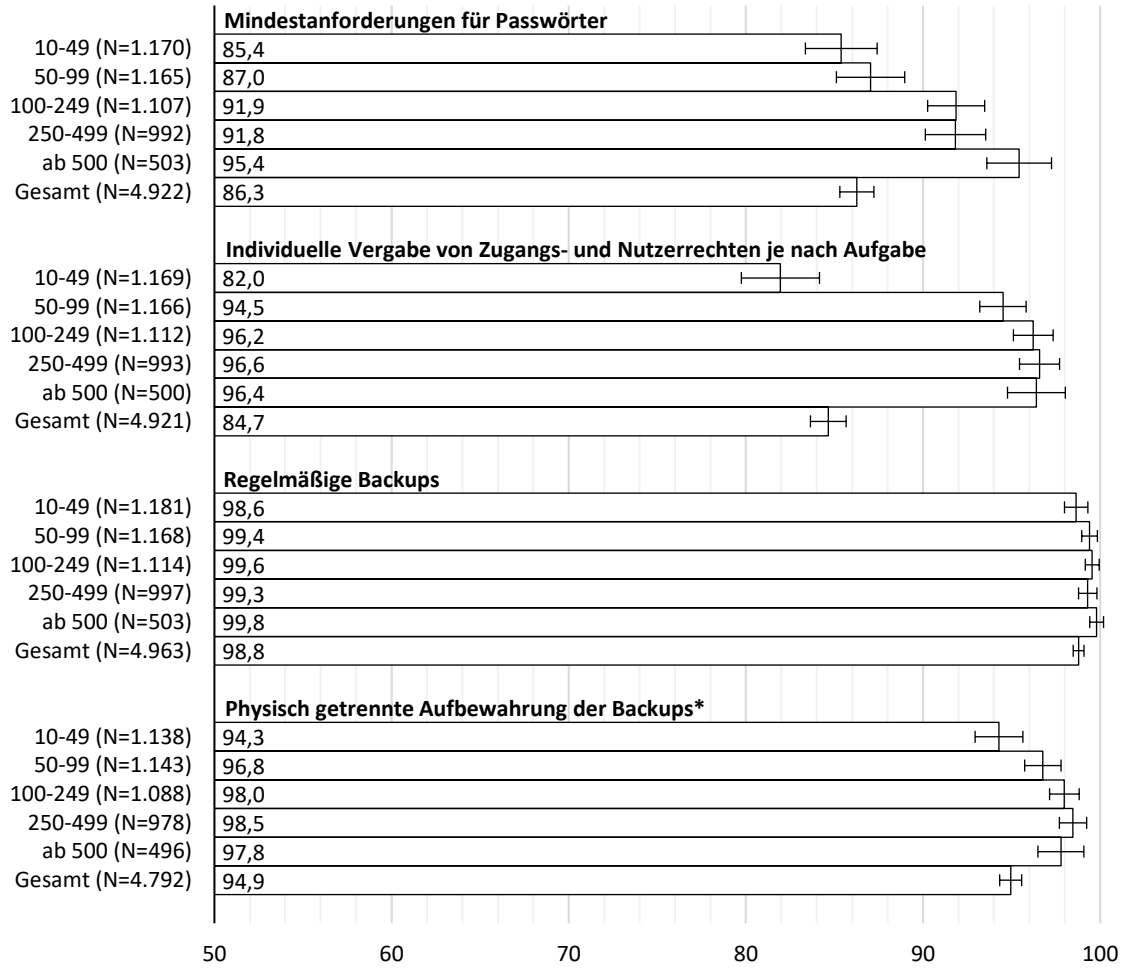
[234] Siehe dazu Fn. 194 sowie Tabelle 4 in Abschnitt 3.4.1. Eine Auflistung aller zur Daseinsvorsorge zugehörigen WZ-Klassen findet sich in Tabelle 43 im Anhang 1.

[235] Bei der Frage, ob es im Unternehmen Mindestanforderungen für Passwörter gibt, gab es keine weitere Spezifizierung. Es bleibt also offen, welche Anforderungen an Passwörter in den Unternehmen gestellt werden (z.B. Passwortlänge, Wechselhäufigkeit etc.). Diesbezüglich vollzieht sich in den letzten Jahren ein Paradigmenwechsel. Die seit dem Jahr 2003 existierende und einflussreiche Passwortrichtlinie der US-Technologie-Standardbehörde NIST (6 bis 8 Zeichen, Klein-

zerrechten je nach Aufgabe. So gibt es in jedem siebten Unternehmen mit zehn bis 49 Beschäftigten (14,6 %) keine Mindestanforderungen für Passwörter und etwa in jedem sechsten (18,0 %) keine individuellen, aufgabenspezifisch vergebenen Zugangs- und Nutzerrechte, während dies lediglich auf jedes 22. bzw. 28. Unternehmen ab 500 Beschäftigten (4,6 % bzw. 3,6 %) zutrifft.

So gut wie alle Unternehmen führen regelmäßige Backups ihrer Daten durch und auch wenn es hinsichtlich der physisch getrennten Aufbewahrung der Backups kleinere zum Teil signifikante Unterschiede zwischen den Beschäftigtengrößenklassen gibt (z.B. 10-49 Besch.: 94,3 % vs. 250-499 Besch.: 98,5 %), liegen die Anteile jeweils über 90,0 %.

Abbildung 16 **Unternehmen mit technischen IT-Sicherheitsmaßnahmen nach Beschäftigtengrößenklassen**
in Prozent; gewichtete Daten; 95%-KI



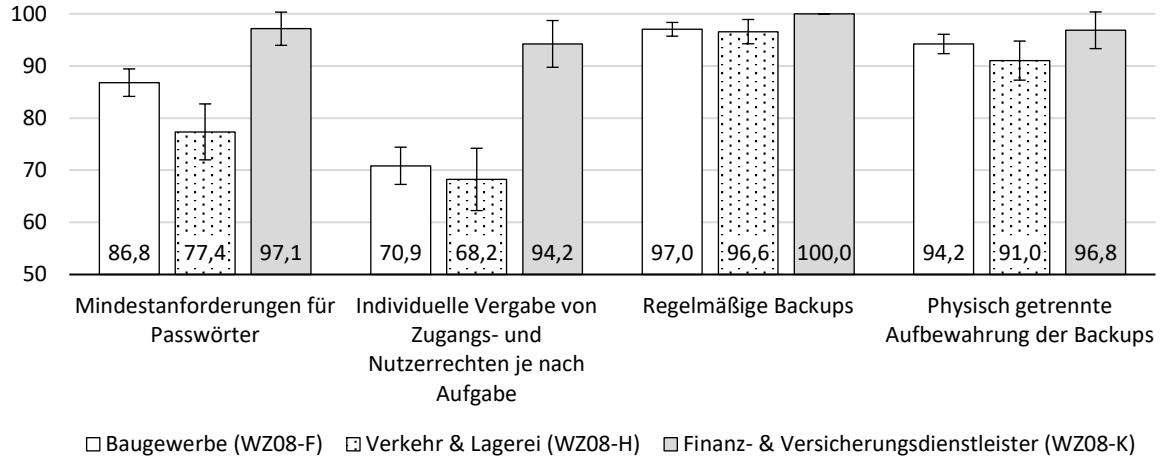
*) Nur Unternehmen, die regelmäßige Backups durchführen

Auch andere Studien berichten von der weiten Verbreitung oben genannter Sicherheitsmaßnahmen. So berichten Klahr et al., dass insgesamt 69 % der befragten britischen Unternehmen

und Großbuchstaben, Zahlen und Sonderzeichen verwenden und das Passwort nach 90 Tagen wechseln) von Burr et al. (2003) wurde im Jahr 2017 grundlegend überarbeitet. Gemäß Grassi et al. (2017: 67f.) ist verglichen mit der Passwortkomplexität die Passwortlänge das entscheidendere Kriterium für die Passwortsicherheit. Passwörter (memorized secrets) sollten so lang wie möglich (mindestens 8 Zeichen) und ohne Wörter aus dem Wörterbuch oder von der „schwarzen Liste" gestaltet werden. Die geforderte Komplexität (Verwendung von Klein- und Großbuchstaben, Zahlen und Sonderzeichen) könnte mit zunehmender Passwortlänge reduziert werden. Insbesondere zum Schutz sensibler Daten und Systeme ist zudem eine Zwei-Faktor-Authentifizierung (2FA) eine sinnvolle Ergänzung.

Mindestanforderungen für Passwörter haben, wobei dieser Anteil für größere Unternehmen auf 91 % steigt.[236] Nach Erkenntnissen von Hillebrand et al. nutzen zwischen 96 % – 98 % der befragten Unternehmen Passwörter, allerdings wurde hier nicht auf Mindestanforderungen eingegangen. Mit Blick auf regelmäßige Datensicherungen nennen sie Verbreitungen von 89 % für kleine KMU und 99 % für größere KMU.[237] Brandl et al. geben ebenfalls eine Verbreitung von 96 % an,[238] die die Bikom-Studie mit 100 % für Industrieunternehmen sogar noch übertrifft.[239] Die individuelle Vergabe von Zugangs- und Nutzerrechten bemisst der Gesamtverband der Deutschen Versicherungen (GDV) mit 68 % hingegen geringer als diese Studie, [240] wohingegen Klahr et al. diesen Anteil ähnlich hoch mit insgesamt 79 % beziffern.[241]

Abbildung 17 **Unternehmen mit PW-Anforderungen, indiv. Rechtevergabe und Backup nach WZ08-Klassen (F, H, K)**
in Prozent; gewichtete Daten; 95%-KI



Beim Vergleich der WZ08-Klassen F, H und K sind erneut signifikante Unterschiede erkennbar (Abbildung 17).[242] Die Anteile der Unternehmen, die Mindestanforderungen für Passwörter einsetzt, ist bei den Unternehmen im Bereich Verkehr und Lagerei mit 77,4 % signifikant niedriger als der Anteil der Unternehmen des Baugewerbes (86,8 %), der wiederum signifikant unter dem Anteil der Finanz- und Versicherungsdienstleister liegt (97,1 %). Die Anteile der Unternehmen mit individueller und aufgabengemäßer Vergabe von Zugangs- und Nutzerrechten sind im Baugewerbe sowie bei Verkehrs- und Lagereiunternehmen deutlich niedriger als bei den Finanz- und Versicherungsdienstleistern (70,9 % bzw. 68,2 % vs. 94,2 %). In Hinblick auf die Durchführung regelmäßiger Backups und deren physisch getrennten Aufbewahrung gibt es zwischen diesen Wirtschaftszweigen keine statistisch relevanten Unterschiede.

236 Vgl. Klahr et al. (2017).

237 Vgl. Hillebrand et al. (2017).

238 Vgl. Brandl et al. (2016).

239 Vgl. Bitkom e.V. (2018).

240 Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

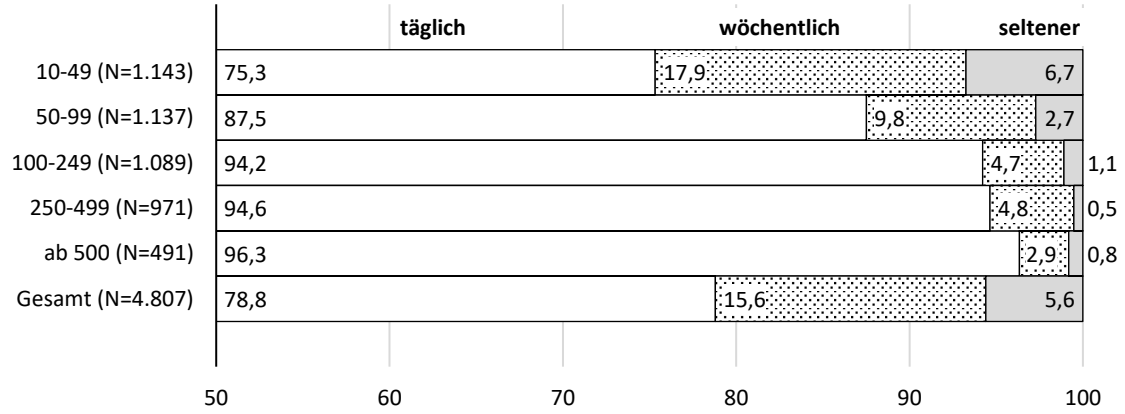
241 Vgl. Klahr et al. (2017)

242 Siehe dazu auch Tabelle 46 im Anhang 1.

Tabelle 17 **Befragte Unternehmen nach Durchführung und Häufigkeit von Backups**

		disproportionale Stichprobe		
		ungewichtet		gewichtet
Regelmäßige Backups?		Anzahl	Prozent	Prozent
	Nein	37	0,7	1,2
	Ja	4.928	99,3	98,8
	Gesamt	4.965	100,0	100,0
Wenn „Ja“, wie häufig?				
	Täglich	4.262	88,4	78,8
	Wöchentlich	425	8,8	15,6
	Seltener	136	2,8	5,6
	Gesamt	4.823	100,0	100,0

Abbildung 18 **Unternehmen mit regelmäßigen Backups nach Backup-Häufigkeit und Beschäftigtengrößenklassen**
in Prozent; gewichtete Daten



Größere Unterschiede treten erst bei der Frage nach der Backupfrequenz auf: Insgesamt führt über ein Fünftel aller Unternehmen (21,2 %) die Datensicherung lediglich wöchentlich oder noch seltener durch (Tabelle 17), wobei dieser Anteil bei großen Unternehmen z.T. signifikant kleiner ist als bei kleineren. Immerhin ein Viertel der Unternehmen mit zehn bis 49 Beschäftigten (24,7 %) führt keine täglichen Backups durch, wohingegen dieser Anteil bei Unternehmen ab 500 Beschäftigten mit 3,7 % deutlich kleiner ausfällt (Abbildung 18). Brandl et al. berichten von permanenten oder täglichen Datensicherungen zwischen 76 % und 85 % der befragten Unternehmen, die kein bzw. ein Datensicherungskonzept implementiert haben und liegen damit genau um die Ergebnisse dieser Studie.[243]

Aktuelle Antivirensoftware und der Schutz der IT-Systeme mittels Firewalls werden insgesamt gesehen von so gut wie allen Unternehmen (98,8 % bzw. 98,0 %) eingesetzt,[244] was durch andere Studien des Literaturstandes gestützt wird.[245] Beim Vergleich der Beschäftigtengrößenklassen sind nur sehr kleine, wenn auch z.T. statistisch signifikante, Unterschiede erkennbar

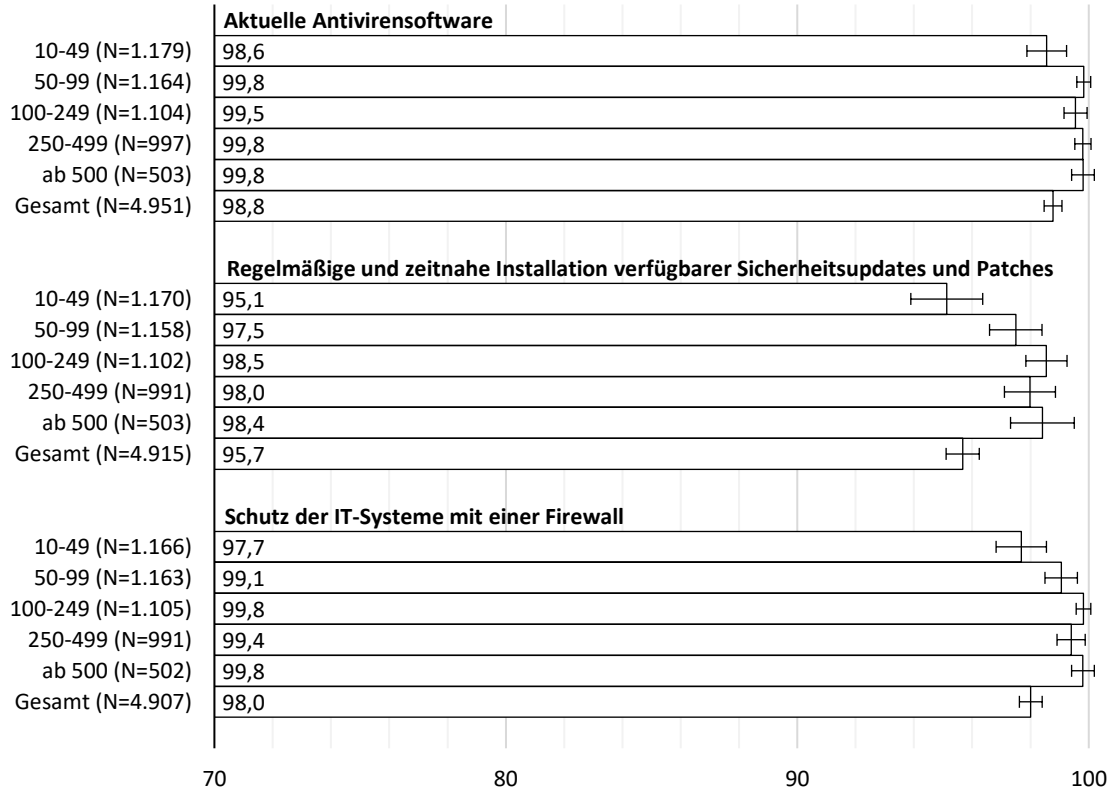
[243] Vgl. Brandl et al. (2016).

[244] Aussagen über Hersteller, Umfang und Effektivität der eingesetzten Software können nicht getroffen werden. Die hohen Anteile könnten sich darüber erklären, dass Antivirensoftware vielfach bereits im Betriebssystem enthalten ist (z.B. Windows Defender Antivirus in Windows 10) und dass es kostenlose Software gibt. Zur Frage, ob Antivirensoftware Schutz vor Schadsoftware bietet, siehe z.B. Sukwong et al. 2011 oder Min et al. 2014.

[245] Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018); Hillebrand et al. (2017); Bitkom e.V. (2018).

(Abbildung 19). Ein ähnliches Bild zeigt sich bezogen auf die regelmäßige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches.[246] Für deutsche Unternehmen berichten Hillebrand et al. von vergleichbaren Patch- und Updatequoten (kleine KMU: 90 %; größere KMU: 97 %).[247] Auch Klahr et al. stellten fest, dass ein Großteil der britischen Unternehmen (92 %) angaben, Software-Updates zeitnah zu installieren.[248]

Abbildung 19 **Unternehmen mit technischen IT-Sicherheitsmaßnahmen nach Beschäftigtengrößenklassen**
in Prozent; gewichtete Daten; 95%-KI



Bei diesen drei technischen IT-Sicherheitsmaßnahmen (siehe Abbildung 20) finden sich nur kleine Unterschiede zwischen den Unternehmen der WZ08-Klassen F, H und K. Der Anteil der Verkehrs- und Lagereiunternehmen, der regelmäßig und zeitnah verfügbare Sicherheitsupdates und Patches installiert (89,3 %), ist signifikant kleiner als bei den bei den anderen beiden WZ08-Klassen (F: 94,4 %; K: 100 %). Der Anteil mit aktueller Antivirensoftware und Firewall-Schutz ist ebenfalls bei Verkehrs- und Lagereiunternehmen geringfügig aber signifikant kleiner (97,8 % bzw. 94,3 %) als bei den Finanz- und Versicherungsdienstleistern (jeweils 100 %).

Zu den Wirtschaftszweigen der zweiten Ebene, die hinsichtlich der technischen IT-Sicherheitsmaßnahmen mit kleineren Anteilswerten auffallen[249], gehören insbesondere WZ08-10 (Herstellung von Nahrungs- und Futtermitteln), WZ08-24 (Metallerzeugung und –bearbeitung) und WZ08-49 (Landverkehr; Transport in Rohrleitungen). Demgegenüber liegen erneut die Anteile

[246] Offen bleibt dabei die Frage, ob Software zum Einsatz kommt, für die keine Sicherheitsupdates bzw. Patches mehr angeboten werden.

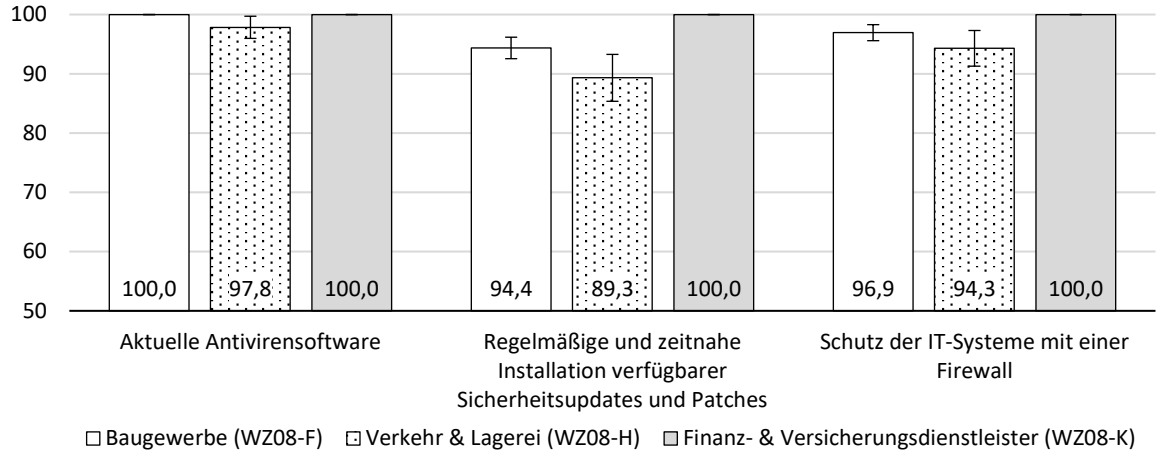
[247] Vgl. Hillebrand et al. (2017)

[248] Vgl. Klahr et al. (2017).

[249] Siehe Tabelle 48 im Anhang 1.

von WZ08-64 (Finanzdienstleistung) und WZ08-62 (Dienstleistungen der Informationstechnologie) sowie WZ08-26 (Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen) im oberen Bereich.

Abbildung 20 **Unternehmen mit Antivirensoftware, Sicherheitsupdates und Firewall nach WZ08-Klassen (F, H, K)**
in Prozent; gewichtete Daten; 95%-KI



Auf die Nachfrage, ob eine einfache Firewall (Paketfilterung nach Quell- und Zieladresse durch Software-Firewall oder Router auf Netzwerkebene) oder eine erweiterte Firewall (zusätzliche Überwachung und Filterung nach Paketinhalt auf Anwendungsebene) zum Einsatz kommt, konnte über ein Fünftel (22,4 %) der befragten Unternehmensvertreter*innen keine Antwort geben (Tabelle 18). Bezieht man die Antwortkategorie „Weiß nicht“ mit ein, dann nutzt etwa die Hälfte der Unternehmen mit Firewall-Schutz eine erweiterte Firewall und über ein Viertel (28,5 %) eine einfache.

Tabelle 18 **Befragte Unternehmen nach Firewall-Schutz**

	disproportionale Stichprobe		
	ungewichtet		gewichtet
Firewall-Schutz?	Anzahl	Prozent	Prozent
Nein	48	1,0	2,0
Ja	4.882	99,0	98,0
Gesamt	4.930	100,0	100,0
Wenn „Ja“, welche Firewall-Art?			
einfache Firewall, d.h. Paketfilterung nach Quell- und Zieladresse durch Software-Firewall oder Router auf Netzwerkebene	981	20,6	28,5
erweiterte Firewall, d.h. zusätzliche Überwachung und Filterung nach Paketinhalt auf Anwendungsebene	3.120	65,5	49,1
Weiß nicht	665	14,0	22,4
Gesamt	4.101	100,0	100,0

Im Vergleich der Unternehmen nach Beschäftigtengrößenklassen (Abbildung 21) ist erkennbar, dass vor allem kleinere Unternehmen häufiger auf den Schutz durch eine einfache Firewall zurückgreifen (z.B. 10-49 Besch.: 30,9 % vs. ab 500 Besch.: 14,5 %) und das diese signifikant seltener Angaben zum Reifegrad der Firewall machen können (z.B. 10-49 Besch.: 24,9 % vs. ab 500 Besch.: 6,5 %). Ein möglicher Grund dafür kann die Komplexität und der hohe Konfigurationsaufwand sein, den größere Unternehmen vermutlich eher bewerkstelligen können als

kleinere Unternehmen. Der Anteil der Unternehmen, die angegeben haben, über eine erweiterte Firewall zu verfügen, scheint in Anbetracht des Zeit- und Kostaufwands zum wirksamen Betreiben einer solchen Firewall zudem relativ hoch zu sein. Unter Umständen liegen diese technischen Sicherheitsmaßnahmen in den Unternehmen zwar vor, ob und inwiefern sie aber effizient betrieben und tatsächlich wirksam sind, kann in dieser Studie nicht vollständig beantwortet werden.

Abbildung 21 **Unternehmen mit Firewall-Schutz nach Art der Firewall**
in Prozent; gewichtete Daten

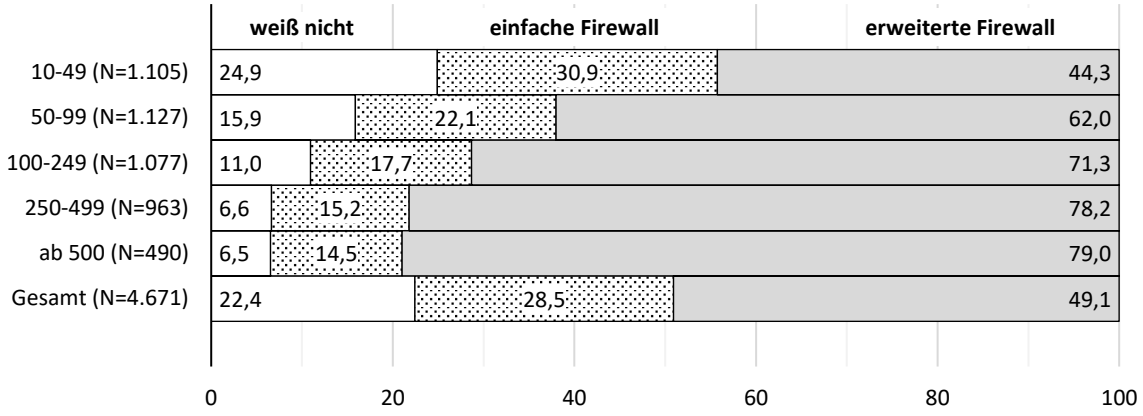
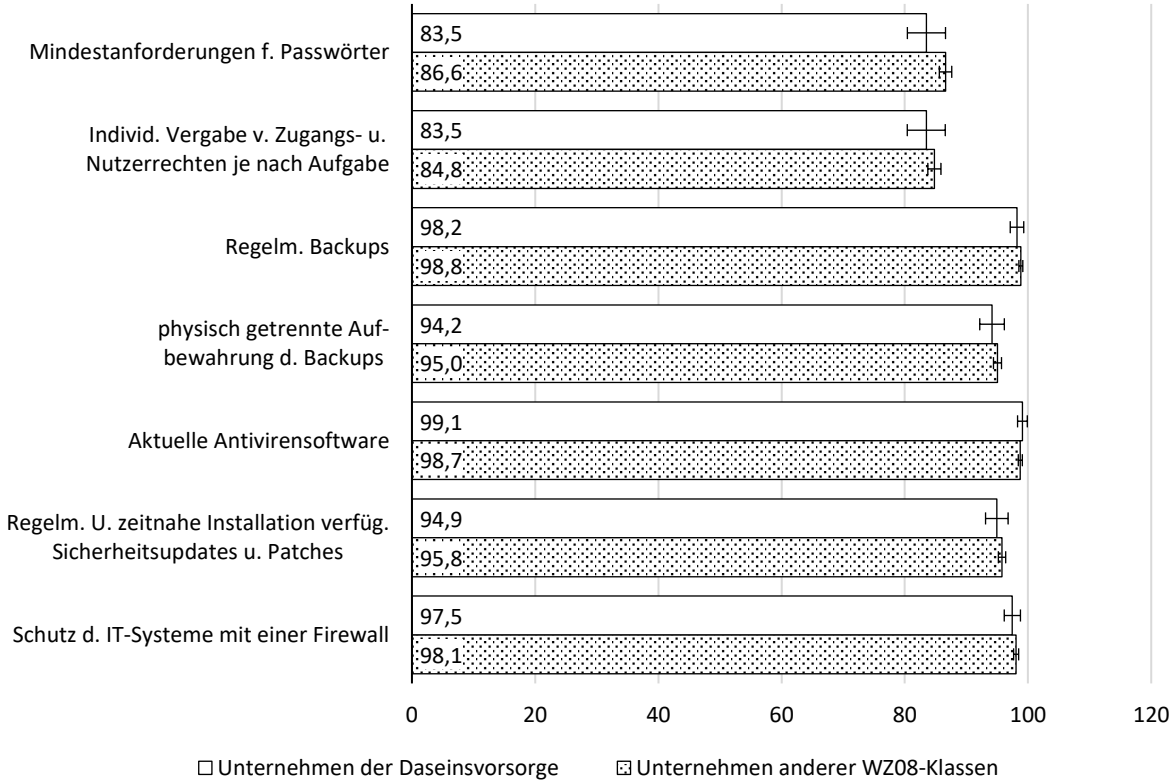


Abbildung 22 **Technische IT-Sicherheitsmaßnahmen nach Zugehörigkeit zur Daseinsvorsorge**
in Prozent; gewichtete Daten; 95%-KI



Wie bei den organisatorischen IT-Sicherheitsmaßnahmen werden auch die Anteile der Unternehmen mit vorhandenen technischen Maßnahmen nach Zugehörigkeit zur Daseinsvorsorge[250] miteinander verglichen (Abbildung 22). Anders als bei den organisatorischen Maßnahmen zeigen sich hierbei keine statistisch relevanten Unterschiede.

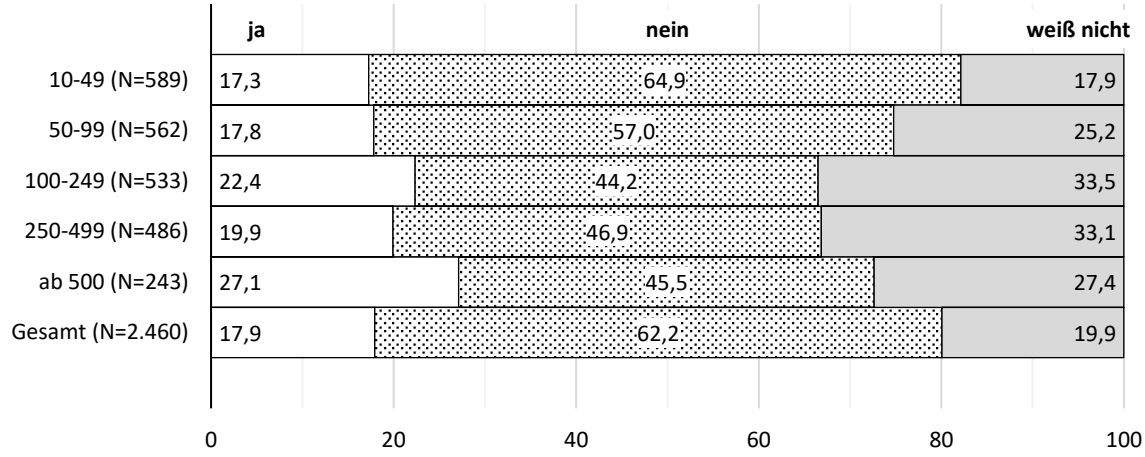
5.4 Versicherung gegen Informationssicherheitsverletzungen

Die Fragen zum Thema Cyberversicherung wurden aus zeitökonomischen Gründen in einem Split-Half-Verfahren nur der Hälfte der Unternehmensvertreter*innen gestellt. Somit konnten zusätzliche Fragen zu einem weiteren Thema in den Fragebogen aufgenommen werden, die von der anderen Hälfte beantwortet wurden und die vorgesehene durchschnittliche Interviewdauer nicht erhöhten.[251] Um systematische Verzerrungen zu vermeiden, erfolgte die Auswahl der Unternehmen zur einen oder anderen Gruppe nach dem Zufallsprinzip.

Danach gefragt, ob das Unternehmen eine Versicherung gegen Informationssicherheitsverletzungen (Cyberversicherung) abgeschlossen hat, antwortete über ein Fünftel (27,4 %; N=1.767) mit „ja“. Dazu ist allerdings anzumerken, dass der aus den gültigen Angaben ausgeklammerte Anteil aller Befragten, der dies nicht wusste, bei 26,8 % (N=2.483) liegt. Unter Einbezug der Antwortkategorie „weiß nicht“ haben 17,9 % (N=2.460) der Unternehmen eine Cyberversicherung, 62,2 % haben keine und bei 19,9 % wussten es die befragten Unternehmensvertreter*innen nicht (Abbildung 23).

Abbildung 23 **Unternehmen mit Cyberversicherung nach Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; Split-Half-Gruppe B

Hat Ihr Unternehmen eine Versicherung gegen Informationssicherheitsverletzungen?



Differenziert nach Beschäftigtengrößenklassen fällt auf, dass der Anteil ohne Kenntnis über das Vorhandensein einer Cyberversicherung in kleinen Unternehmen kleiner ist als in den mittleren und großen. Auf der anderen Seite ist auch der Anteil der kleinen Unternehmen mit Cyberversicherung signifikant kleiner (10-49 Besch.: 17,3 %) als bei den großen (ab 500 Besch.: 27,1 %). Der GDV nennt geringere Anteile. So verfügen nur rund 6 % der Kleinst-, 15 % der

[250] Siehe dazu Fn. 194 sowie Tabelle 4 in Abschnitt 3.4.1. Eine Auflistung aller zur Daseinsvorsorge zugehörigen WZ-Klassen findet sich in Tabelle 43 im Anhang 1.

[251] Bei einer weiteren Erhöhung der durchschnittlichen Interviewdauer von 20 Minuten wäre gemäß bisheriger Erfahrungen des Umfrageinstituts mit höheren Abbruchquoten zu rechnen gewesen.

kleinen und 9 % der mittleren Unternehmen über eine Cyberversicherung.[252] Entsprechende Ergebnisse einer Bitkom-Studie liegen in einem ähnlich hohem Bereich und für Unternehmen ab 100 Mitarbeiter*innen sogar darüber (10-99 Besch.: 10 %; 100-499 Besch.: 23 %; >500 Besch.: 32 %).[253] Zu beachten ist an dieser Stelle der Fokus des Bitkom auf Industrieunternehmen. Das britische Versicherungsunternehmen Hiscox gibt in seiner Umfrage unter 4.100 Unternehmen aus fünf verschiedenen Ländern sogar einen Anteil von 33 % der Unternehmen an, die eine Cyberversicherung abgeschlossen haben. Den im berichteten Forschungsstand höchsten Anteil an Versicherungen, die Cybervorfälle abdecken, beziffern Klahr et al. mit insgesamt 38 % der britischen Unternehmen.[254] Neben den in Abschnitt 2.3 beschrieben Limitationen ist es denkbar, dass unterschiedliche Angaben zu den Abschlussquoten von Versicherungen gegen Informationssicherheitsverletzungen darin liegen, dass bestimmte Betriebsunterbrechungsversicherungen auch Schäden durch Cyberangriffe abdecken, die dann von den befragten Unternehmen genannt wurden. Zudem dürfte der Anteil der gegen Informationssicherheitsverletzungen versicherten Unternehmen in den letzten Jahren gewachsen sein und auch weiter wachsen.

Aufgeschlüsselt nach Branchenzugehörigkeit (Abbildung 24) liegen Unternehmen der WZ08-Klasse K (Finanz- und Versicherungsdienstleistungen) mit einem Anteil von 61,5 % gegen Informationssicherheitsverletzungen Versicherten mit Abstand vor allen anderen WZ08-Klassen. Danach folgen Unternehmen des Gesundheits- und Sozialwesens (WZ08-Q: 32,7 %) und sonstige Dienstleister (WZ08-S: 24,1 %). Kaum entsprechend versicherte Unternehmen finden sich in der Land- u. Forstwirtschaft bzw. Fischerei (WZ08-A: 0,0 %). Bei der Interpretation dieser Ergebnisse sind allerdings die unterschiedlichen und z.T. sehr großen Anteile der diesbezüglich Unwissenden zu beachten. Zu den WZ08-Klassen der zweiten Ebene, deren Unternehmen vergleichsweise selten eine Cyberversicherung angegeben haben gehören WZ08-01 (Landwirtschaft, Jagd und damit verbundene Tätigkeiten: 0,0 %), WZ08-16 (Herstellung von Holz-, Flecht-, Korb- und Korkwaren; ohne Möbel: 0,0 %) sowie WZ08-42 (Tiefbau: 5,3 %). Die Finanzdienstleistung (WZ08-64: 69,0 %) und das Gesundheitswesen (WZ08-86: 46,9 %) sind dagegen anteilig häufiger versichert, wobei bei Unternehmen des Gesundheitswesens der Anteil, der nicht wusste, ob eine Cyberversicherung besteht oder nicht, vergleichsweise groß ist (24,5 %).[255]

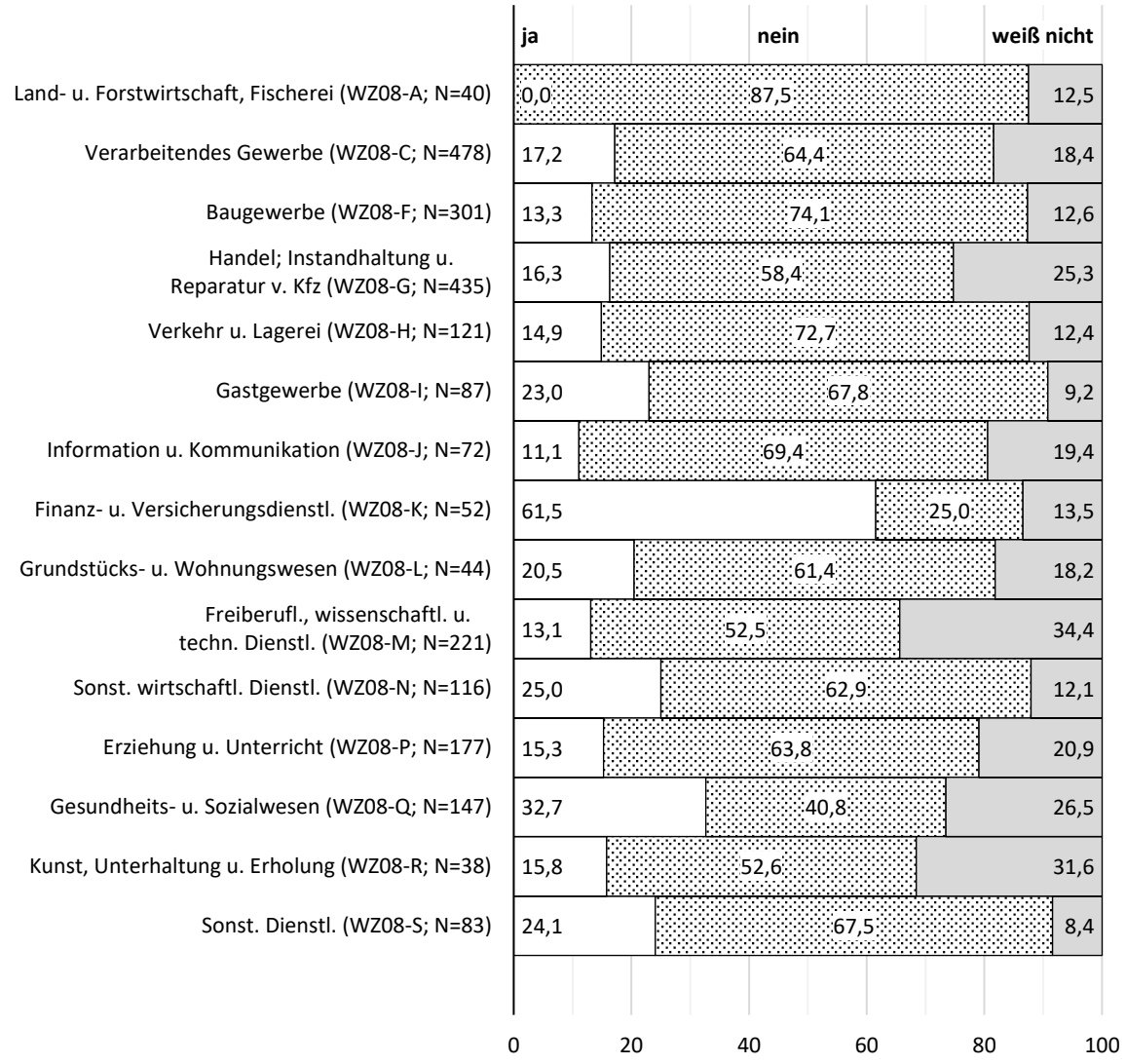
[252] Vgl. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

[253] Vgl. Bitkom e.V. (2018). Die Cyberversicherung wird folgendermaßen definiert: Versicherung für den Fall des Auftretens von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl.

[254] Vgl. Klahr et al. (2017).

[255] Eine Aufschlüsselung dieser Anteile nach WZ08-Klassen der zweiten Ebene findet sich in Tabelle 49 im Anhang 1.

Abbildung 24 **Unternehmen mit Cyberversicherung nach WZ08-Klassen der ersten Ebene**

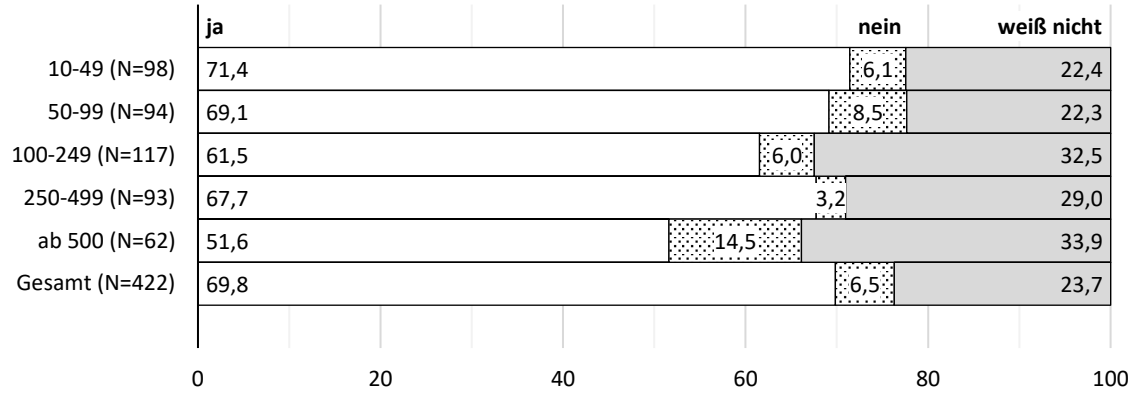


Wenn eine Cyberversicherung vorhanden war, wurde danach gefragt, ob der Abschluss einer solchen Versicherung weiterempfohlen wird und ob bereits versucht wurde, die Versicherung in Anspruch zu nehmen. Insgesamt betrachtet würde die Mehrheit von 69,8 % die Cyberversicherung weiterempfehlen, wobei weitere 23,7 % dies noch nicht wissen und nur ein sehr kleiner Anteil von 6,5 % keine Empfehlung geben würde (Abbildung 25). Zwischen den Beschäftigtengrößenklassen sind lediglich tendenzielle aber keine statistisch abgesicherten Unterschiede zu erkennen: Demnach würden kleine Unternehmen häufiger den Abschluss einer Cyberversicherung empfehlen als große (10-49 Besch.: 71,4 % vs. ab 500 Besch.: 51,6 %), allerdings ist der Anteil derjenigen, die dies nicht noch nicht wissen, bei den großen Unternehmen größer als bei den kleinen (ab 500 Besch.:33,9 % vs. 10-49 Besch.: 22,4 %). In eine ähnliche Richtung, allerdings mit der Fragestellung ob sich der Abschluss einer Cyberversicherung bisher für das Industrieunternehmen gelohnt habe, gibt Bitkom an, dass dies für 61 % der Unternehmen nicht bzw. überhaupt nicht der Fall sei und nur 28 % das Gegenteil berichten. Allerdings stellt die Bitkom-Studie auch fest, dass Unternehmen mit zehn bis 99 Mitarbeiter*innen hier positiver

eingestellt sind (48 % sehr/eher gelohnt; 44 % kaum/überhaupt nicht gelohnt) als Unternehmen anderer Beschäftigtengrößenklassen.[256]

Abbildung 25 **Weiterempfehlung von Cyberversicherungen nach Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; Split-Half-Gruppe B mit Cyberversicherung

Würden Sie die Cyberversicherung weiterempfehlen?



Die relativ großen Anteile der Unentschlossenen dürften mit der mangelnden Erfahrung beim Thema Cyberversicherung zusammenhängen. Lediglich 5,7 % der versicherten Unternehmen (N=424) hat jemals versucht, Leistungen der Cyberversicherung in Anspruch zu nehmen.[257] 18 von 20 Unternehmen gaben an, daraufhin auch Leistungen erhalten zu haben und 13 von 18 berichten davon, dass damit der gesamte Schaden abgedeckt wurde. Aufgrund der geringen Fallzahlen ist die Aussagekraft dieser Ergebnisse zu den Leistungen von Cyberversicherungen jedoch sehr beschränkt.

Tabelle 19 **Gründe der Nichtversicherung**
in Prozent; gewichtete Daten; Mehrfachantworten möglich; fett: signifikant bei p<.05 (Chi²-Test)

		Beschäftigtengrößenklasse				
Warum hat Ihr Unternehmen keine Cyberversicherung?	Gesamt	10-49	50-99	100-249	250-499	ab 500
Wir haben uns damit noch nicht beschäftigt	63,0	**63,8**	**59,4**	**60,3**	**57,6**	**41,6**
Das Preis-Leistungs-Verhältnis stimmt nicht	11,0	10,4	14,2	16,5	14,3	20,8
Sonstiger Grund	27,6	27,4	27,7	24,7	29,5	39,6
N	1.461	366	310	224	217	101

Die Unternehmen, die keine Cyberversicherung hatten, wurden nach den Gründen dafür gefragt (Tabelle 19). Fast zwei Drittel gaben an, sich mit dem Thema Cyberversicherung noch nicht beschäftigt zu haben (63,0 %), für jedes neunte Unternehmen stimmt das Preis-Leistungs-Verhältnis von geprüften Produkten nicht (11,0 %) und über ein Viertel gab an, einen sonstigen Grund dafür zu haben (27,6 %). Der Anteil der großen Unternehmen (ab 500 Besch.), die sich bisher noch nicht mit Cyberversicherungen beschäftigt haben, ist mit 41,6 % signifikant kleiner als bei den kleinen (10-49 Besch.). Auf der anderen Seite kamen die großen Unternehmen zumindest tendenziell häufiger zu dem Ergebnis, dass das Preis-Leistungs-Verhältnis nicht stimme (ab 500 Besch.: 20,8 % vs. 10-49 Besch.: 10,4 %).

256 Vgl. Bitkom e.V. (2018).

257 Auch Klahr et al. (2017) nennen hier nur zwei von insgesamt über 1.500 befragten Unternehmen.

5.5 Zwischenresümee

Die betrachteten Unternehmen weisen Unterschiede in den IT-Sicherheitsstrukturen auf. Etwa ein Fünftel der Unternehmen ab zehn Beschäftigten (21,6 %) hat keine eigenen IT-Mitarbeiter*innen. Je größer das Unternehmen ist, desto kleiner werden diese Anteile. Knapp zwei Fünftel der kleinen Unternehmen (10-49 Besch.) haben darüber hinaus keine Beschäftigten im Bereich IT- & Informationssicherheit (38,7 %; N=1.133). Sofern dieses fehlende Know-how nicht anderweitig, z.B. durch externe Dienstleister, ausgeglichen werden kann, können dem Unternehmen erhöhte Risiken durch Cyberangriffe drohen. Auf das Mittel der Auslagerung bestimmter IT-Funktionen scheint jedoch ein Großteil (81,4 %) der deutschen Unternehmen mit mehr als zehn Beschäftigten zurückzugreifen. Für IT-Sicherheitsfunktionen liegt dieser Anteil bei rund 49 %. Der Einsatz externer IT-Dienstleister steht wie erwartet mit einer geringen Anzahl eigener IT-Mitarbeiter*innen im Zusammenhang. Größere Unternehmen verfügen jedoch unabhängig der Auslagerung bestimmter IT-Funktionen in der Regel über eigene IT-Mitarbeiter*innen.

Hinsichtlich der IT-Sicherheitsstrukturen in den betrachteten Unternehmen fällt auf, dass organisatorische Sicherheitsmaßnahmen in kleineren Unternehmen weniger verbreitet sind, als in größeren. Zudem bestehen signifikante Unterschiede innerhalb verschiedener Branchen. Unternehmen der Daseinsvorsorge haben anteilig häufiger Zertifizierungen im Bereich der IT-Sicherheit und führen häufiger Schulungen zur IT-Sicherheit für Beschäftigten sowie Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme durch als anderen Unternehmen. Unbeantwortet bleiben Fragen nach der genauen Umsetzung solcher organisatorischer Maßnahmen, d.h., ob es z.B. zyklische Prozesse der Wiederholung, Auffrischung und Kontrolle u.ä. gibt.

Mit Blick auf die technischen Sicherheitsmaßnahmen besteht weniger Varianz in den Beschäftigtengrößenklassen als bei organisatorischen Sicherheitsmaßnahmen. Diesbezüglich scheint es inzwischen gewisse Standards zu geben, die von den meisten Unternehmen ab zehn Beschäftigte zumindest vorhanden sind. Auch Unternehmen der Daseinsvorsorge zeigen anders als bei den organisatorischen Maßnahmen keine statistisch relevanten Unterschiede im Vergleich zu anderen Unternehmen. Offen bleibt an dieser Stelle in welcher Qualität bzw. mit welchem Reifegrad diese technischen Maßnahmen implementiert wurden, ob eine sachgemäße Konfiguration und Wartung stattfindet und ob die Endanwender*innen die damit verbundenen Verhaltensregeln einhalten.

Neben organisatorischen und technischen Sicherheitsmaßnahmen setzt ein Teil der Unternehmen auch auf Versicherungsschutz. Unter Einbezug der Antwortkategorie „weiß nicht“ haben 17,9 % (N=2.460) der Unternehmen eine Versicherung gegen Informationssicherheitsverletzungen, 62,2 % haben keine und bei 19,9 % der Fälle wussten es die Befragten nicht. Lediglich 5,7 % der versicherten Unternehmen (N=424) hat jemals versucht, Leistungen der Cyberversicherung in Anspruch zu nehmen. Unternehmen ohne eine solche Versicherung, gaben überwiegend an, sich mit dem Thema noch nicht beschäftigt zu haben (63,0 %)

Da das reine Vorhandensein von IT-Sicherheitsmaßnahmen ohne entsprechende Verhaltensweisen bzw. das nötige Risikobewusstsein der Betroffenen wenig effektiv sein dürfte, wurden die Befragten diesbezüglich um eine Einschätzung für die jeweiligen Unternehmen gebeten. Die Ergebnisse dieser Einschätzungen werden im folgenden Kapitel dargestellt.

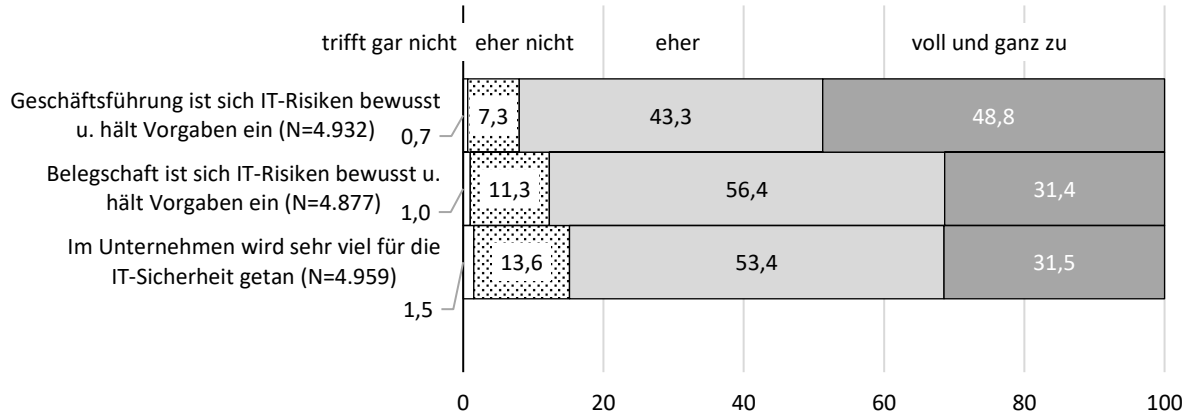
6 EINSCHÄTZUNGEN ZU IT-RISIKEN

Neben dem Vorhandensein von IT-Sicherheitsmaßnahmen spielt das Risikobewusstsein innerhalb der Unternehmen eine zentrale Rolle, denn vor allem Richtlinien und andere vorhandene präventive und schützende Maßnahmen müssen von der Geschäftsführung und den Beschäftigten umgesetzt und gelebt werden, damit sie eine Wirkung entfalten können. Die teilnehmenden Unternehmensvertreter*innen wurden gebeten, sowohl das Risikobewusstsein innerhalb des Unternehmens als auch das Risiko für das Unternehmen, einen schädigenden Cyberangriff zu erleiden, einzuschätzen. Daneben wurde eine Einschätzung zur Frage erhoben, warum das jeweilige Unternehmen zum Ziel eines Cyberangriffs werden könnte. Diese Ergebnisse können dabei einen Hinweis auf das Risikobewusstsein innerhalb des Unternehmens geben, wenn es auch die Einschätzung des/der einzelnen Befragten bleibt.

6.1 Risikobewusstsein innerhalb des Unternehmens

Zum Thema Risikobewusstsein konnten die befragten Unternehmensvertreter*innen auf einer vierstufigen Skala von 1 „Trifft gar nicht zu“ bis 4 „Trifft voll und ganz zu“ ihre Einschätzung zu folgenden Aussagen treffen: „Die Geschäftsführung ist sich der IT-Risiken bewusst und hält die Vorgaben ein.“, „Die Belegschaft ist sich der IT-Risiken bewusst und hält die Vorgaben ein.“ und „Im Unternehmen wird sehr viel für die IT-Sicherheit getan (‚mehr als klassische Schutzmaßnahmen‘).“

Abbildung 26 **Einschätzung zum Risikobewusstsein im Unternehmen**
in Prozent; gewichtete Daten



Die Anteile der Befragten, die den drei Aussagen, gar nicht oder eher nicht zustimmen konnten, ist mit 8,0 % hinsichtlich des Risikobewusstseins der Geschäftsführung, 12,3 % hinsichtlich des Risikobewusstseins der Belegschaft und 15,2 % bezogen auf IT-Sicherheitsmaßnahmen im Unternehmen relativ klein (Abbildung 26). Die größte Zustimmung (43,3 %: „trifft eher zu“ und 48,8 %: „trifft voll und ganz zu“) erhielt die Aussage, dass die Geschäftsführung sich der IT-Risiken bewusst ist und entsprechende Vorgaben einhält. Dies ist vor allem vor dem Hintergrund interessant, dass in der Literatur bemängelt wird, dass Cybersicherheit immer noch

keine bzw. in zu geringem Maße „Chefsache“ sei und daher eine stärkere Einbindung der Geschäftsführung gefordert wird.[258] Womöglich sind sich Geschäftsführer der IT-Risiken bewusst, delegieren oder vernachlässigen die Behandlung des Themas aber trotz dessen.

Für die weitere Auswertung wurde aus diesen drei Einzelaspekten ein Mittelwertindex gebildet.[259]

Tabelle 20 **Einschätzung zum Risikobewusstsein im Unternehmen**
in Prozent; gewichtete Daten; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)

		Position innerhalb des Unternehmens			Beschäftigtengrößenklasse				
	Gesamt	Gschf.	IT	Sonst.	10-49	50-99	100-249	250-499	ab 500
(eher) geringes Risikobewusstsein im Unternehmen (N=4.797)	8,2	**9,6**	**7,1**	**7,3**	8,4	8,3	7,4	8,1	8,7
Wie sehr trifft Folgendes auf Ihr Unternehmen zu?	Anteile der Antworten "trifft gar nicht/eher nicht zu"								
Geschäftsführung ist sich der IT-Risiken bewusst und hält Vorgaben ein (N=4.932)	8,0	**7,0**	**9,2**	**7,3**	7,6	9,5	9,2	10,0	11,2
Belegschaft ist sich der IT-Risiken bewusst und hält Vorgaben ein (N=4.877)	12,3	**13,0**	**13,1**	**7,2**	**11,6**	**14,4**	**12,8**	**16,7**	**23,3**
Im Unternehmen wird viel für IT-Sicherheit getan (N=4.959)	15,2	**17,7**	**11,3**	**19,0**	**16,4**	**11,1**	**9,5**	**8,4**	**8,0**

Beim Vergleich des eingeschätzten Risikobewusstseins innerhalb des Unternehmens zwischen den Positionen der antwortenden Unternehmensvertreter*innen[260] fallen relativ kleine aber signifikante Unterschiede auf (Tabelle 20). Befragte aus der Geschäftsführung bzw. dem Vorstand geben anteilig häufiger ein (eher) geringes Risikobewusstsein im Unternehmen (9,6 %) an als Befragte aus dem Bereich IT und Informationssicherheit (7,1 %) oder aus sonstigen Bereichen (7,3 %) und scheinen demnach kritischer zu sein. Dies trifft allerdings nicht auf alle Einzelaspekte des Mittelwertindexes zu: So stimmt z.B. ein signifikant größerer Anteil der Befragten aus dem Bereich IT & Informationssicherheit eher nicht/gar nicht zu, dass sich die Geschäftsführung der Risiken bewusst ist und Vorgaben einhält (9,2 %), als Befragte der Geschäftsführung selbst (7,0 %). Demnach schätzen Geschäftsführer*innen das eigene IT-Risikobewusstsein selbst höher ein, als ihre IT-Mitarbeiter*innen ihnen beimessen würden. Bezogen auf die Belegschaft äußern sich Befragte in sonstigen Positionen signifikant seltener kritisch (7,2 %) als die anderen beiden Gruppen (Gschf.: 13,0 %; IT: 13,1 %). Dies könnte z.B. daran liegen, dass diese inhaltlich weiter vom Thema IT-Sicherheit entfernt sind und so ggf. zu einem milderen Urteil kommen. Der Aussage, dass im Unternehmen viel für die IT-Sicherheit getan wird,

[258] Vgl. Hillebrand et al. (2017); Georgia Institute of Technology (2016); Bundesamt für Sicherheit in der Informationstechnik (2015); Bitkom e.V. (2018); Nach Angaben von PwC steigt allerdings das Risikobewusstsein der Chefetage zu diesem Thema (PricewaterhouseCoopers AG WPG (2017)).

[259] Die Maßzahl Cronbachs Alpha beziffert das Ausmaß der Beziehung der enthaltenen Einzelaspekte (Items), kann Werte zwischen minus unendlich und 1 annehmen und diente der Einschätzung der interne Konsistenz des Indexes. Cronbachs Alpha liegt in diesem Fall bei 0,72 und deutet auf eine relativ gute Konsistenz hin. Die über die drei Items errechneten Mittelwerte wurden anschließend wie folgt kategorisiert: „gering“ (1,000-1,749), „eher gering“ (1,750-2,499), „eher hoch“ (2,500-3,249) und „hoch“ (3,250-4,000).

[260] Zur zusammengefassten Zuordnung der Unternehmensvertreter siehe Abschnitt 3.4.3.

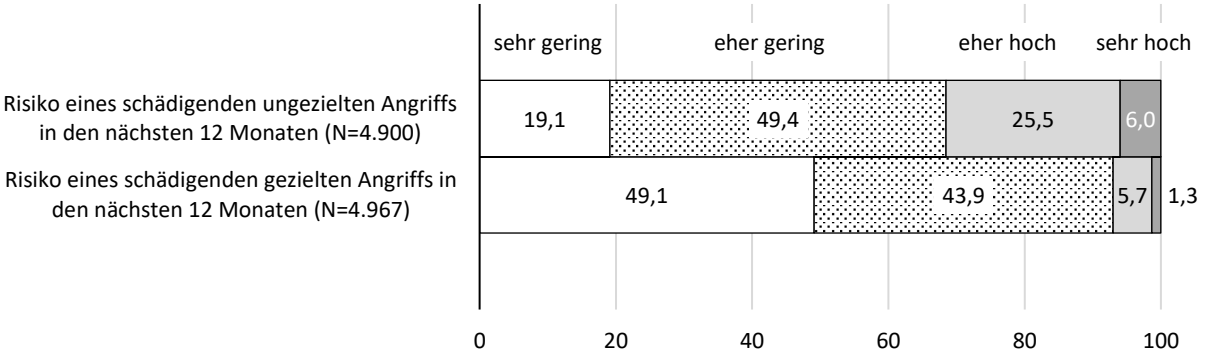
stehen mehr Befragte in sonstigen Positionen (19,0 %) und der Geschäftsführung (17,7 %) (eher) ablehnend gegenüber als Befragte der IT und Informationssicherheit (11,3 %). Vermutet werden kann an dieser Stelle, dass Befragte der IT und Informationssicherheit hier ihre eigene Arbeit bewerten und diese verständlicherweise sehr präsent ist bzw. andere Beschäftigtengruppen kein vollständiges Bild aller Sicherheitsbemühungen im Unternehmen haben. Gegebenenfalls könnte eine höhere Transparenz von bereits bestehenden Sicherheitsmaßnahmen dazu beitragen, die kritischeren Einschätzungen von Geschäftsführern und sonstigen Beschäftigen abzumildern und dadurch insgesamt eine höhere Sensibilisierung und Widerstandsfähigkeit zu erreichen.

Differenziert nach Beschäftigtengrößenklassen fallen bei zwei Einzelaspekten signifikante Unterschiede im Antwortverhalten auf, was zumindest teilweise dadurch zu erklären ist, dass in größeren Unternehmen eher Beschäftigte aus dem Bereich der IT und Informationssicherheit und in kleineren Unternehmen häufiger die Geschäftsführung befragt wurden. Dennoch zeigt sich, dass der Anteil der kritischen Stimmen bei den großen Unternehmen in Hinblick auf das Risikobewusstsein der Belegschaft deutlich größer ausfällt als bei den kleinen (ab 500: 23,3 % vs. 10-49 Besch.: 11,6 %). Bezüglich der Aussage, „im Unternehmen wird viel für die IT-Sicherheit getan“, ist es genau anders herum ist: Hier sind in den kleinen Unternehmen deutlich mehr kritische Stimmen als in den großen (10-49 Besch.: 16,4 % vs. ab 500: 8,0 %). Dies steht im Einklang mit dem allgemeinen Ergebnis in Abschnitt 5.3, dass in größeren Unternehmen mehr IT-Sicherheitsmaßnahmen umgesetzt werden, und deutet gleichzeitig darauf hin, dass der Faktor Mensch mit zunehmender Beschäftigtenzahl an Bedeutung gewinnt.

6.2 Einschätzung des Unternehmensrisikos

Neben dem Risikobewusstsein in ihrem Unternehmen sollten die Befragten das Risiko für ihr Unternehmen einschätzen, dass es in den nächsten zwölf Monaten von einem Cyberangriff geschädigt wird, der a) gleichzeitig auch viele andere Unternehmen trifft (ungezielter Angriff) und b) der ausschließlich des eigene Unternehmen trifft (gezielter Angriff). Diese Einschätzung konnten die Befragten ebenfalls auf einer vierstufigen Skala von 1 „sehr gering“ bis 4 „sehr hoch“ treffen.

Abbildung 27 **Risikoeinschätzung für die Schädigung des Unternehmens durch (un)gezielte Cyberangriffe**
in Prozent; gewichtete Daten



Das Risiko eines gezielten Cyberangriffs in den nächsten zwölf Monaten, der das Unternehmen schädigt, wird noch deutlich geringer eingeschätzt als das eines schädigenden ungezielten Angriffs (Abbildung 27): Mit einem Anteil von 93,0 % erachtet der größte Teil der Unternehmen

das Risiko in Hinblick auf gezielte Angriffe als sehr/eher gering. Hinsichtlich ungezielter Angriffe sehen dies lediglich 68,5 % so. Fast die Hälfte (49,1 %) hält das Risiko einer Schädigung durch gezielte Angriffe sogar für sehr gering, während dieser Anteil bezüglich ungezielter Angriffe mit 19,1 % deutlich tiefer liegt.

Tabelle 21 **Risikoeinschätzung für die Schädigung des Unternehmens durch (un)gezielte Cyberangriffe**
in Prozent; gewichtete Daten; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)

Wie hoch schätzen Sie das Risiko für Ihr Unternehmen ein, in den nächsten 12 Monaten von einem Cyberangriff geschädigt zu werden, der …	Gesamt	Position innerhalb des Unternehmens			Beschäftigtengrößenklasse				
		Gschf.	IT	Sonst.	10-49	50-99	100-249	250-499	ab 500
	Anteile der Antworten "sehr/eher hoch"								
… gleichzeitig auch viele andere Unternehmen trifft (N=4.900)	31,5	**31,9**	**34,1**	**22,6**	**30,3**	**35,3**	**36,1**	**37,8**	**41,7**
… ausschließlich das eigene Unternehmen trifft (N=4.967)	7,0	**6,3**	**9,0**	**3,6**	**6,6**	**7,7**	**9,4**	**8,6**	**12,4**

Im Vergleich der Risikoeinschätzungen nach Position der Befragten innerhalb der Unternehmen (Tabelle 21) ist zu erkennen, dass sich vor allem Beschäftigte im Bereich IT und Informationssicherheit von den Beschäftigten in sonstigen Positionen signifikant unterscheiden: Die Anteile derjenigen, die das Risiko einer Schädigung durch einen Cyberangriff in den nächsten zwölf Monaten sehr oder eher hoch einschätzten, liegen in Hinblick auf ungezielte und gezielte Angriffe bei Beschäftigten im Bereich IT- und Informationssicherheit am höchsten (34,1 % bzw. 9,0 %; N=2.043 bzw. 2.067) und bei Beschäftigten in sonstigen Positionen am niedrigsten (22,6 % bzw. 3,6 %; N=660 bzw. 676). Ein Erklärungsansatz könnte hier wieder die stärkere Präsenz des Themas bei Beschäftigten der IT- und Informationssicherheit sein. Gleichzeitig spiegelt das Antwortverhalten aber auch die geringere Einschätzung des Risikobewusstseins der IT-Beschäftigten gegenüber ihrer Geschäftsführung wider.

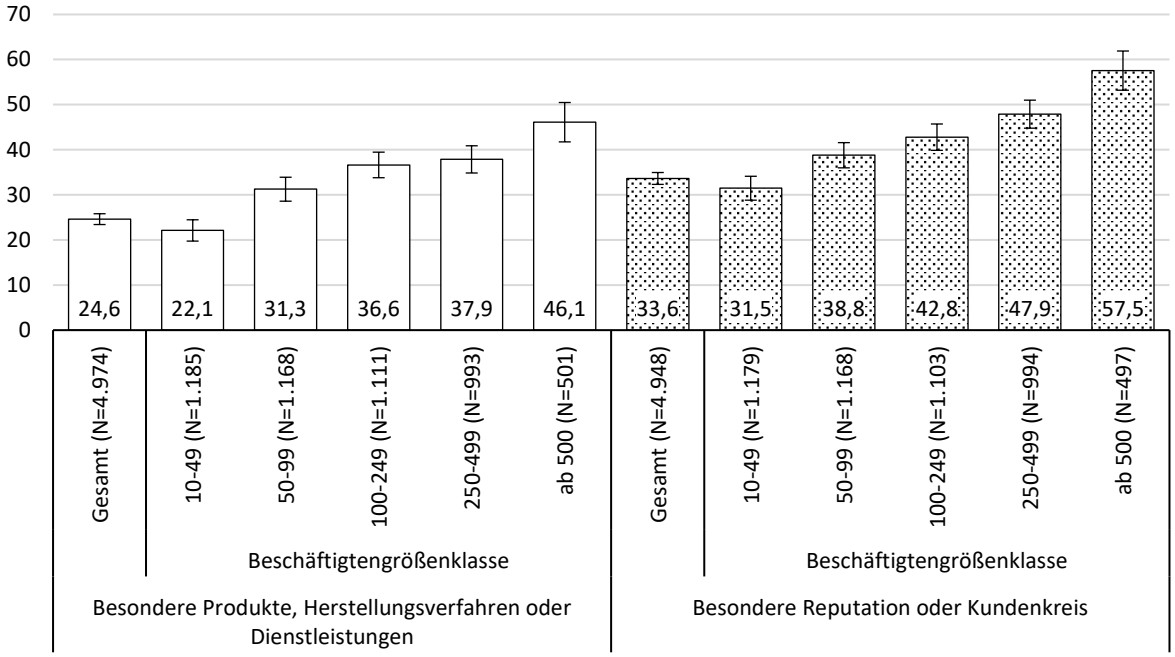
Die Anteile der verschiedenen Beschäftigtengrößenklassen unterscheiden sich ebenfalls: Befragte aus kleinen Unternehmen kamen signifikant seltener zu dem Schluss, dass das Risiko für ungezielte und gezielte Angriffe sehr/eher hoch ist (10-49 Besch.: 30,3 % bzw. 6,6 %; N=1.167 bzw. 1.184), als Befragte großer Unternehmen (ab 500 Besch.: 41,7 % bzw. 12,4 %; N=494 bzw. 499). Dies kann wiederum zumindest teilweise mit dem höheren Anteil an IT und Informationssicherheitsbeschäftigten unter den Befragten großer Unternehmen zusammenhängen. Nichts desto trotz, sollte diese Einschätzung für kleinere Unternehmen nicht zu dem Trugschluss führen, dass sie sich weniger schützen sollten bzw. uninteressantere Angriffsziele darstellen würden.

6.3 Potentielle Angriffsziele

In Zusammenhang mit der Frage, warum das Unternehmen zum Ziel eines Cyberangriffs werden könnte, hatten die Unternehmensvertreter*innen die Möglichkeiten anzugeben, ob „besondere Produkte, Herstellungsverfahren oder Dienstleistungen (z.B. aufgrund spezieller Technik, Designs, Materialien, Innovationen)“ und/oder eine „besondere Reputation/ Kundenkreis (z.B. hoher Bekanntheitsgrad, hohe Sicherheitsstandards, besondere Verschwiegenheit)“ vorhanden

sind oder nicht. Die Einschätzung der „Besonderheit“ wurde bewusst den Befragten überlassen, da eine objektivierte Definition über die Vielzahl verschiedener Unternehmen und Branchen nahezu unmöglich festzulegen ist. Vielmehr konnten so die Befragten im Vergleich zu anderen Unternehmen diese Einschätzung frei treffen.

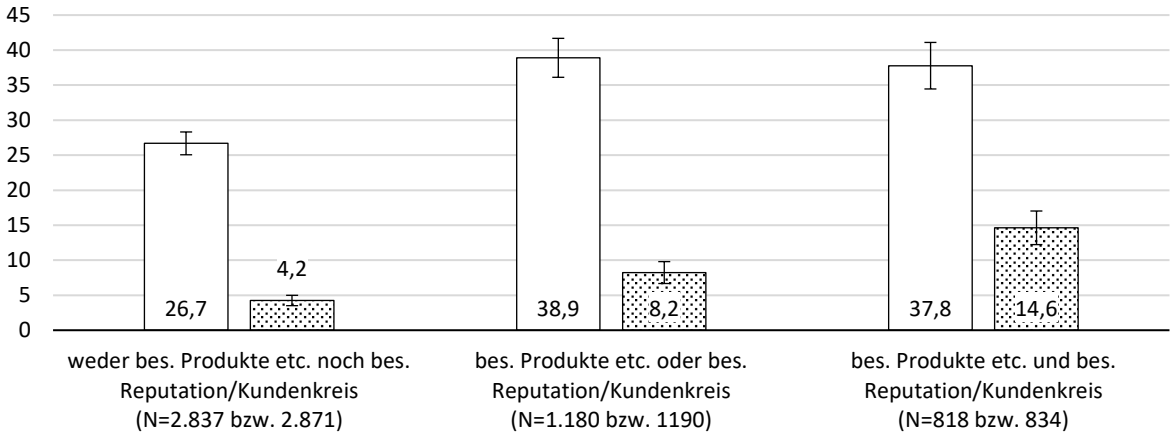
Abbildung 28 **Potentielle Gründe für einen gezielten Cyberangriff nach Beschäftigtengrößenklassen**
in Prozent; gewichtete Daten; 95%-KI



Etwa ein Viertel der Unternehmen hat demnach besondere Produkte, Herstellungsverfahren oder Dienstleistungen (24,6 %) und ein Drittel eine besondere Reputation oder einen besonderen Kundenkreis (33,6 %), die/der das Unternehmen zum Ziel von individuellen Cyberangriffen machen könnte (Abbildung 28). Dabei sind signifikante Unterschiede zwischen den Beschäftigtengrößenklassen erkennbar, demzufolge vor allem bei großen Unternehmen deutlich häufiger besondere Produkte etc. sowie besondere Reputation/ Kundenkreis (ab 500: 46,1 % bzw. 57,5 %) vorhanden sind als bei kleineren (10-49 Besch.: 22,1 % bzw. 33,6 %). Der Anteil der Unternehmen, die weder besondere Produkte, Herstellungsverfahren oder Dienstleistungen noch eine besondere Reputation oder einen besonderen Kundenkreis haben, beträgt insgesamt 58,6 % (N=4.927) und ist bei kleinen Unternehmen deutlich größer als bei den großen (10-49 Besch.: 61,1 % ; ab 500 Besch.: 33,8 %).

In Abbildung 29 sind die Anteile der Befragten dargestellt, die das Risiko einer Schädigung des Unternehmens durch ungezielte bzw. gezielte Cyberangriffe in den nächsten zwölf Monaten als (eher) hoch einschätzen, differenziert nach dem Vorhandensein von potentiellen Angriffszielen. Die Anteile liegen bei Unternehmen, die weder über besondere Produkte etc. noch über besondere Reputation/ Kundenkreis verfügen, signifikant niedriger (26,7 % bzw. 4,2 %) als bei Unternehmen, die entweder besondere Produkte etc. oder eine besondere Reputation/Kundenkreis (38,9 % bzw. 8,2 %) oder sogar beides haben (37,8 % bzw. 14,6 %). D.h., Unternehmen mit potentiellen Angriffszielen schätzen das Risiko eines schädigenden Angriffs in den nächsten zwölf Monaten signifikant häufiger (eher) hoch ein. Das spricht zum einen für eine gesteigerte Awareness dieser besonders exponierten Unternehmen und ist andererseits problematisch, wenn sich Unternehmen ohne diese Besonderheiten auf der sicheren Seite wiegen.

Abbildung 29 **Risikoeinschätzung für die Schädigung nach Vorhandensein potentieller Angriffsziele**
in Prozent; gewichtete Daten; 95%-KI



6.4 Informationsquellen zum Thema IT- und Informationssicherheit

Informationen zum Thema IT- und Informationssicherheit werden von diversen Quellen angeboten. Neben staatlichen Institutionen wie dem Verfassungsschutz, der Polizei oder dem BSI, und den Berufsverbänden und Kammern (z.B. IHK, BVMW) bieten z.B. Beratungsdienstleister und IT-Softwarehersteller entsprechende Informationen an. Zudem können über eigene Internetrecherchen, über Fachliteratur bzw. Fachzeitschriften oder auf sonstigem Wege (denkbar wären z.B. persönliche Gespräche mit Geschäftspartnern etc.) Informationen eingeholt werden.

Tabelle 22 **Informationsquellen zum Thema IT- und Informationssicherheit**
in Prozent; gewichtete Daten; Mehrfachantworten möglich; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)

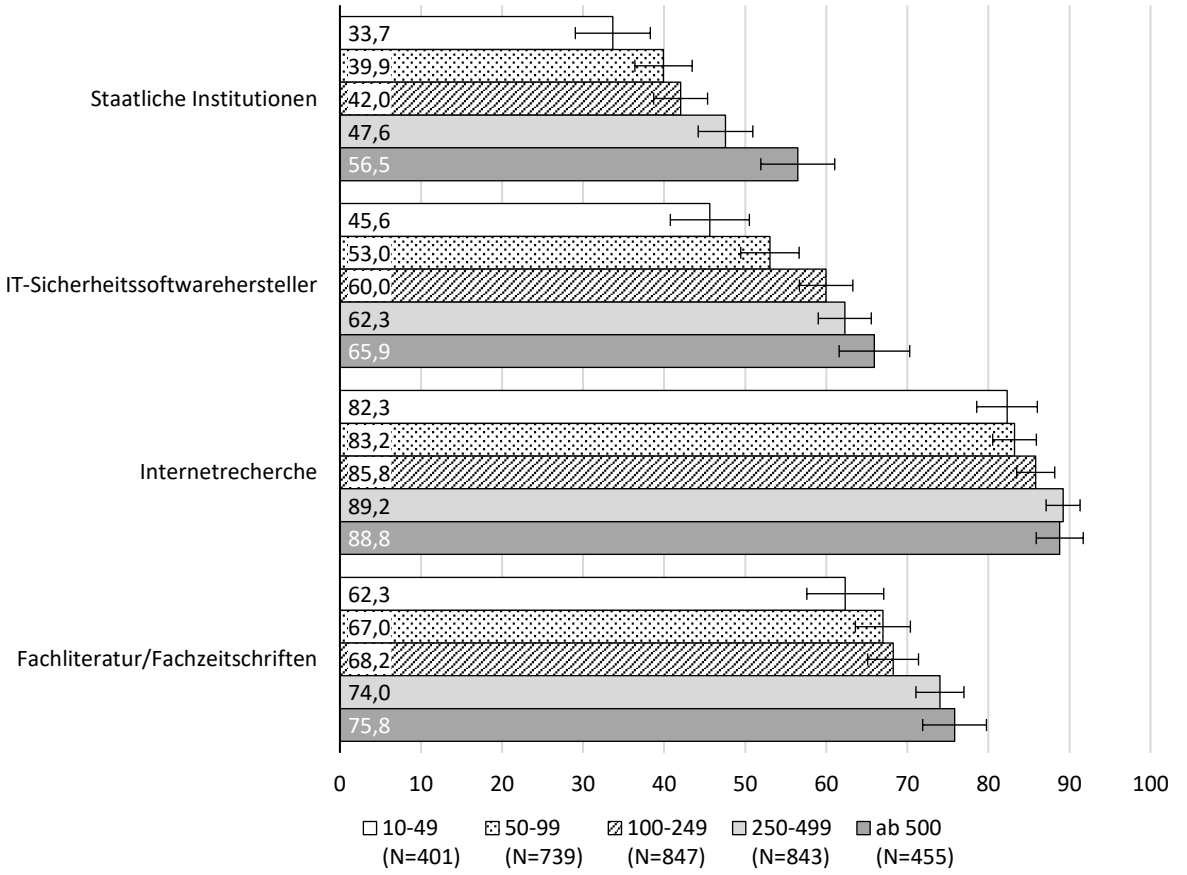
An wen wenden Sie sich, um Informationen zur IT- und Informationssicherheit einzuholen? An …	Gesamt	Position innerhalb des Unternehmens			Beschäftigtengrößenklasse				
		Gschf.	IT	Sonst.	10-49	50-99	100-249	250-499	ab 500
Staatliche Institutionen (z.B. Verfassungsschutz, Polizei, BSI)	23,3	**13,9**	**36,9**	**11,0**	**19,8**	**33,1**	**36,7**	**43,9**	**55,0**
IT-Sicherheitssoftwarehersteller	40,0	**33,9**	**49,7**	**29,2**	**37,1**	**46,5**	**54,8**	**59,2**	**64,9**
Beratungsdienstleister	73,6	**75,1**	**71,0**	**76,9**	73,1	74,7	74,6	75,5	74,9
Berufsverbände, Kammern (z.B. IHK, BVMW)	28,9	**32,7**	**26,7**	**23,7**	29,0	28,7	27,6	28,8	30,4
Internetrecherche	63,3	**49,9**	**83,4**	**44,3**	**59,6**	**73,4**	**79,1**	**84,8**	**87,7**
Fachliteratur bzw. Fachzeitschriften	44,7	**30,5**	**64,8**	**27,9**	**40,7**	**54,9**	**60,7**	**67,7**	**74,7**
Sonstige	12,0	**13,0**	**10,4**	**13,8**	11,9	12,6	12,1	11,5	14,3
N	4.882	2.156	2.067	654	1.159	1.165	1.099	986	500

Beratungsdienstleister sind, insgesamt betrachtet, mit 73,6 % die am häufigsten genannte Informationsquelle (Tabelle 22), gefolgt von eigenen Internetrecherchen (63,3 %), Fachliteratur

bzw. Fachzeitschriften (44,7 %) und IT-Sicherheitssoftwarehersteller (40,0 %). Seltener wurden dazu Berufsverbände und Kammern (28,9 %) sowie staatliche Institutionen (23,3 %) angelaufen.

Bei allen Antwortmöglichkeiten gibt es statistisch signifikante Unterschiede zwischen den Positionen der antwortenden Unternehmensvertreter*innen: IT-Beschäftigte informieren sich zunächst häufiger über mehrere Quellen und nutzen neben der eigenen Internetrecherche oder den Informationen in der Fachliteratur und in Fachzeitschriften das Informationsangebot von IT-Sicherheitssoftwareherstellern aber auch von staatlichen Institutionen signifikant häufiger als z.B. die Geschäftsführung, die sich demgegenüber häufiger an Berufsverbände und Kammern sowie vor allem an Beratungsdienstleister wendet. Interessant ist zudem, dass sich Geschäftsführungen zur Informationseinholung vergleichsweise selten an staatliche Stellen wenden. Dies deutet darauf hin, dass sie staatliche Stellen häufig nicht als kompetente Ansprechpartner wahrnehmen, was sich im Schadensfall auch auf das Anzeigeverhalten auswirken könnte.

Abbildung 30 **Ausgewählte Informationsquellen von IT-Beschäftigten nach Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; Mehrfachantworten möglich



Im Vergleich der Unternehmen nach Beschäftigtengrößenklassen fallen signifikante Unterschiede hinsichtlich der staatlichen Institutionen, der IT-Sicherheitssoftwarehersteller, der Internetrecherche sowie der Fachliteratur/ Fachzeitschriften als Informationsquellen auf (Abbildung 30). Große Unternehmen (ab 500 Besch.) nutzen diese deutlich häufiger als die kleinen (10-49 Besch.). Vor dem Hintergrund, dass in großen Unternehmen vor allem IT-Beschäftigte geantwortet haben, sind diese Unterschiede erwartungskonform. Doch auch unter Kontrolle der Position der antwortenden Unternehmensvertreter*innen bleiben diese Unterschiede zwischen

den Beschäftigtengrößenklassen zumindest in der Gruppe der IT-Beschäftigten bestehen (Abbildung 30): IT-Beschäftigte in kleinen Unternehmen (10-49 Besch.) nutzen staatliche Institutionen, IT-Sicherheitssoftwarehersteller, Internetquellen und Fachliteratur/ Fachzeitschriften signifikant seltener zur Information zum Thema IT- und Informationssicherheit als IT-Beschäftigte großer Unternehmen (ab 500 Besch.). Besonders deutlich ist dieser Unterschied in Hinblick auf staatliche Institutionen: Während diese von einem Drittel der IT-Beschäftigten kleiner Unternehmen (10-49 Besch.: 33,7 %) genannt werden, liegt der Anteil der IT-Beschäftigten großer Unternehmen, die dies ebenfalls tun, bei über der Hälfte (ab 500 Besch.: 56,5 %). Vermutet werden könnte hier, dass sich das Informations- und Unterstützungsangebot staatlicher Stellen inhaltlich eher an größere Unternehmen richtet und kleinere Unternehmen weniger erreicht werden. Dominierend ist bei allen Unternehmensgrößenklassen die Internetrecherche als Informationsmedium.

Insgesamt ist zu erkennen, dass das Informationsgewinnungsverhalten der Unternehmen zum Thema IT-Sicherheit differenziert ist. Die adressatengerechte Wahl des Informationsmediums zukünftigen Wissens scheint daher eine wichtige Rolle zu spielen.

6.5 Zwischenresümee

In diesem Kapitel konnte gezeigt werden, dass Unternehmen IT-Risiken unterschiedlich einschätzen und sich unterschiedlich über das Thema IT-Sicherheit informieren. Wichtig ist zu beachten, welche Person mit welcher Funktion als Individuum Auskünfte über die Untersuchungseinheit „Unternehmen“ gibt. So schätzen Geschäftsführer das eigene IT-Risikobewusstsein selbst höher ein, als ihre IT-Mitarbeiter ihnen beimessen würden. Andersrum sind Geschäftsführer kritischer als IT-Mitarbeiter, wenn es darum geht, ob im Unternehmen viel für IT-Sicherheit getan wird. Dieses differenzierte Antwortverhalten sollte in zukünftigen Studien kontrolliert werden. Auch die Unternehmensgröße spielt eine Rolle. Der Anteil der kritischen Stimmen bei den großen Unternehmen in Hinblick auf das Risikobewusstsein der Belegschaft fällt deutlich größer aus, als bei den kleinen Unternehmen.

Bezüglich der Aussage, „im Unternehmen wird viel für die IT-Sicherheit getan“, ist es genau anders herum: Hier sind in den kleinen Unternehmen deutlich mehr kritische Stimmen als in den großen.

Risiken für die Unternehmen durch ungezielte bzw. gezielte Cyberangriffe in den nächsten 12 Monaten werden sehr unterschiedlich eingeschätzt. Fast alle Unternehmen (93,0 %) erachten das Risiko in Hinblick auf gezielte Angriffe als sehr/eher gering, während dieser Anteil für ungezielte Angriffe deutlich kleiner ist (68,5 %). Fast die Hälfte (49,1 %) hält das Risiko einer Schädigung durch gezielte Angriffe sogar für sehr gering. Für ungezielte Angriffe sind es nur 19,1 %. Auch hier zeigen sich Unterschiede in den Beschäftigtengrößenklassen. Je größer das Unternehmen, desto häufiger werden beide Angriffsvarianten eingeschätzt. Befragte aus kleinen Unternehmen kamen signifikant seltener zu dem Schluss, dass das Risiko für ungezielte und gezielte Angriffe sehr/eher hoch ist.

Mit Blick darauf, warum ein Unternehmen gezielt angegriffen werden könnte, wurden Besonderheiten erfragt. Etwa ein Viertel der Unternehmen hat demnach besondere Produkte, Herstellungsverfahren oder Dienstleistungen (24,6 %) und ein Drittel eine besondere Reputation oder

einen besonderen Kundenkreis (33,6 %), die/der das Unternehmen zum Ziel von individuellen Cyberangriffen machen könnte. Je größer das Unternehmen ist, desto höher sind die Anteile dieser Besonderheiten. Werden die Aussagen zur Einschätzung des Unternehmensrisikos und den potenziellen Angriffszielen verknüpft, zeigt sich folgerichtig, dass Unternehmen mit potentiellen Angriffszielen das Risiko eines schädigenden Angriffs in den nächsten zwölf Monaten signifikant häufiger (eher) hoch einschätzen. Das spricht zum einen für eine funktionierende Awareness dieser besonders exponierten Unternehmen, darf aber im Umkehrschluss nicht bedeuten, dass sich Unternehmen ohne diese Besonderheiten auf der sicheren Seite wiegen können.

Hinsichtlich der Frage, wie sich Unternehmen über IT-Sicherheit informieren, könnten sowohl Unterschiede zwischen den Unternehmensgrößen, als auch den Funktionen der antwortenden Personen gezeigt werden. Geschäftsführer weisen die höchsten Anteile bei der Informationsgewinnung durch Beratungsdienstleister auf, während sich IT-Mitarbeiter zum höchsten Anteil im Internet informieren. Größere Unternehmen greifen beispielsweise signifikant häufiger auf durch staatliche Stellen bereitgestellte Informationen zurück, als kleinere. Insgesamt ist zu erkennen, dass das Informationsgewinnungsverhalten der Unternehmen zum Thema IT-Sicherheit differenziert ist und bei zukünftigen Publikationskampagnen berücksichtigt werden sollte.

7 CYBERANGRIFFE GEGEN UNTERNEHMEN

Die Schwierigkeit, die Betroffenheit von Cyberangriffen zu erheben, besteht u.a. darin, dass sich ein Cyberangriff auf vielfältige Art und Weise sowie als Kombination verschiedener Angriffsarten, gezielt auf ein spezielles Unternehmen oder ungezielt, z.B. über massenhaft verbreitete Schadprogramme, durchführen lässt. Daneben ist bei vielen Cyberangriffen eine Schädigung des betroffenen Unternehmens auch schon vor Zielerreichung der Täter*innen möglich, etwa wenn IT-Arbeitsplätze ausfallen, Arbeitszeit zur Abwehr eines akuten Angriffs investiert werden muss etc.

Ohne Anspruch auf eine vollständige Erfassung aller Möglichkeiten wurden folgende Angriffsarten innerhalb der Befragung unterschieden:[261] Ransomware-Angriff, Spyware-Angriff, Angriff mit sonstiger Schadsoftware (Malware), manuelles Hacking, (D)DoS-Angriff, Defacing, CEO-Fraud und Phishing. Diese weniger technische und relativ breite Klassifikation wurde aus zwei Gründen gewählt. Zum einen, um unabhängig von bestimmten Angriffsvektoren, Techniken und Tools sowie betroffenen Domänen bzw. Systemen oder Daten[262] zu sein, die sich im Zeitverlauf ändern können.[263] Zum anderen, um die Verständlichkeit und Akzeptanz bei den Befragten zu fördern sowie der eingeschränkten Möglichkeit zur Komplexität eines Telefoninterviews gerecht zu werden.

1) Bei einem Ransomware-Angriff wird ein Schadprogramm eingesetzt, das die Daten infizierter Computer oder Netzwerke verschlüsselt und somit für die Nutzer*innen unbrauchbar macht. Damit ist häufig eine Erpressung von Lösegeld (engl. ransom) verbunden, insofern die Entschlüsselung an die Zahlung des geforderten Betrages (meist in Form einer Kryptowährung wie Bitcoin oder Monero) geknüpft wird. Ob die Zusendung des Freigabecodes nach der Bezahlung des Lösegeldes erfolgt, bleibt dabei ungewiss.
2) Als Spyware werden Programme bezeichnet, die zur Spionage (engl. spying) eingesetzt werden und möglichst unerkannt interne Daten von Unternehmen identifizieren und ausschleusen sollen. Diese Angriffsart kann z.B. zur Produktspionage oder zur Vorbereitung anderer Cyberangriffe dienen (siehe z.B. CEO-Fraud-Angriff).
3) Unter sonstigen Malware-Angriffen werden Angriffe mit schädigender bzw. „bösartiger“ (engl. malicious) Software, wie Viren, Würmer, Trojaner, Rootkits, Scareware etc. verstanden. Da die Bandbreite der Schadprogramme, deren mögliche Variation und

[261] Die Klassifikation der Angriffsarten wurde unter Beachtung der Güterkriterien der Erschöpfung (jede Angriffsart kann einer Kategorie zugeordnet werden) und Exklusivität (jede Angriffsart kann nur einer Kategorie zugeordnet werden) durch das Projektteam nach Sichtung des Literaturstandes sowie Diskussionen mit dem projekteigenen regionalem Unternehmensstammtisch erstellt.

[262] Die Betroffenheit von Systemen und Daten stellen aus Sicht dieser Studie keine Angriffsart, sondern die Konsequenz eines Angriffes dar und werden daher im Kapitel 9 als Folgen dargestellt. Zum Beispiel stellt demnach „Identitätsdiebstahl“ keine Angriffsart, sondern das Ergebnis eines erfolgreichen Angriffes z.B. mithilfe einer Spyware-Software dar.

[263] Ein ähnliches Vorgehen wählten auch Paoli et al. (2018).

Kombination permanent zunimmt und eine sinnvolle Abgrenzung kaum möglich erscheinen, erfassen wir Malware-Angriffe mit Ausnahme von Ransomware- und Spyware-Angriffen lediglich gesammelt.

4) Manuelles Hacking steht für eine nicht autorisierte Manipulation bzw. Konfiguration von Hard- und Softwareeinstellungen von Computern ohne den Einsatz von Schadprogrammen (Malware). Ziel eines unautorisierten Hackers (z.T. auch Cracker oder Blackhat bezeichnet) könnte es z.B. sein, illegitime Einsicht in Unternehmensdaten zu erlangen, diese zu entwenden, Unternehmen zu sabotieren oder einen anderen Cyberangriff vorzubereiten.
5) Ein Denial-of-Service- oder kurz DoS-Angriff zielt auf Web- oder E-Mail-Server von Unternehmen, die mit massenhaften Anfragen oder E-Mail-Sendungen überlastet werden sollen und somit für den regulären Betrieb nicht mehr zur Verfügung stehen. Wird dieser Angriff durch den Zusammenschluss der Rechenleistung mehrerer verteilter IT-Systeme durchgeführt, um Schutzmaßnahmen zu überwinden, wird dies als Distributed Denial-of-Service- oder kurz DDoS-Angriff bezeichnet. Ein solcher Angriff kann z.B. auf die Sabotage von Unternehmen durch temporäre Betriebsunterbrechung abzielen und/oder mit einer Erpressung verbunden sein.
6) Unter Defacing-Angriffen werden unautorisierte Manipulationen von Inhalten der Webpräsenz oder ganzer Webseiten von Unternehmen gefasst. Diese können z.B. der Sabotage sowie der Erlangung von Aufmerksamkeit aus politischen oder religiösen Gründen dienen oder eine öffentlich sichtbare Demonstration der Fähigkeiten der Angreifer*innen darstellen. Auch die Einschleusung von Schadprogrammen oder Täuschung der Besucher*innen der Webseite, zum Zweck des Abfangens persönlicher Daten ist möglich.
7) Der CEO-Fraud ist eine Form des Betruges (engl. Fraud) bei der unter Verwendung einer falschen Identität einer weisungsbefugten Person des Unternehmens, z.B. der des CEO (Chief Executive Officer), andere Beschäftigten meist mit fingierten E-Mails zu bestimmten Handlungen verleitet werden sollen. Diese Angriffsart hat das Ziel Menschen zu täuschen bzw. zu manipulieren und wird auch häufig als Social-Engineering bezeichnet. Dabei kann es z.B. um eine vermeintlich dringende finanzielle Transaktion zum Abschluss eines geheimen Geschäftes oder die Umleitung einer regulären Transaktion auf ein anderes Konto gehen. Daneben kann durch Social-Engineering auch die Herausgabe von sensiblen Informationen erreicht werden. Diese Angriffsart ist häufig gut vorbereitet und nutzt interne Informationen des Unternehmens, z.B. über bestimmte Geschäfts- und Kommunikationsabläufe, beteiligte Personen und deren Abwesenheitszeiten, aus, die möglicherweise auch aus anderen Cyberangriffen stammen.
8) Phishing-Angriffe gegen Unternehmen zielen insbesondere darauf ab, an sensible Unternehmensdaten, z.B. Zugangsdaten, Passwörter, Daten von Bankkonten oder Kreditkartendaten, zu gelangen. Dazu werden häufig manipulierte oder gefälschte E-Mails eingesetzt, um Beschäftigten so zu täuschen, dass sie diese preisgeben. Die Kenntnis solcher Daten eröffnet Täter*innen viele andere Angriffsmöglichkeiten, z.B. Manipulation und Umleitung von Transaktionsvorgängen oder Identitätsdiebstahl zur Täuschung Dritter (siehe CEO-Fraud-Angriff).
9) Sonstige Angriffsarten wurden in den Fragen zur Lebenszeitprävalenz und zum schwerwiegendsten Angriff der letzten 12 Monate als Freitext erfasst und anschließend, sofern

möglich, den oben genannten Angriffsarten zugeteilt bzw. als fehlende Antwort gewertet.

Wie bereits angedeutet, lassen sich diese Angriffsarten innerhalb eines Angriffs miteinander kombinieren oder schrittweise durchführen. Zum Beispiel können Informationen aus einem Phishing- oder Spyware-Angriff zur Vorbereitung und Durchführung eines CEO-Fraud-Angriffs verwendet werden. Wenn ein erlebter Cyberangriff aus mehreren Angriffsarten bestand und Erkenntnisse dazu vorlagen, sollten die miteinander kombinierten bzw. verknüpften Angriffsarten dennoch gesondert angegeben werden. Die im Folgenden berichteten Ergebnisse beziehen sich demnach auf die erlebten Angriffsarten unabhängig davon, ob sie in irgendeiner Form miteinander zusammenhingen oder nicht.[264]

7.1 Prävalenzrate

Zu den jeweiligen Angriffsarten wurde zunächst gefragt, wie oft das Unternehmen betroffen war. Dazu sollten alle Angriffe gezählt werden, auf die das Unternehmen aktiv reagieren musste, z.B. durch die Einleitung von Maßnahmen. Angriffe, die aufgrund vorhandener IT-Sicherheitsstrukturen automatisiert vereitelt wurden, beispielsweise durch das herausfiltern von E-Mails mit schädigender Software, blieben unberücksichtigt.[265] Die anhand dieser Angaben berechnete Prävalenzrate gibt den Anteil der Unternehmen an, die innerhalb eines definierten Zeitraumes (in den letzten zwölf Monate bzw. jemals) Erfahrungen mit mindestens einem Cyberangriff gemacht haben, auf den reagiert werden mussten.

7.1.1 Cyberangriffe insgesamt

Insgesamt gaben zwei Fünftel (41,1 %; N=4.981) der Unternehmen an, dass sie in den letzten zwölf Monaten von mindestens einer der erfragten Angriffsarten betroffen gewesen waren (Abbildung 31). Davon hat über die Hälfte (57,2 %) mehrere unterschiedliche Angriffsarten erlebt. Der direkte Vergleich mit entsprechenden Ergebnissen anderer Studien ist schwer möglich. Neben anderen in Abschnitt 2.4.3 dargestellten Ergebnissen liegen die Jahresprävalenzen zum Teil unter und zum Teil über den Angaben dieser Studie (z.B. für belgische Unternehmen in 2018: 66,5 %[266] und für deutsche Unternehmen in 2018 33 %.[267] Gründe dafür können, wie in Abschnitt 2.3 erwähnt, neben unterschiedlichen Stichproben insbesondere die unterschiedlichen Definitionen eines Cyber-Angriffes sein.

---

[264] Ob verschiedene Angriffsarten Bestandteil eines zusammenhängenden Cyberangriffs sind, ließe sich allenfalls mit forensischer Untersuchung feststellen.

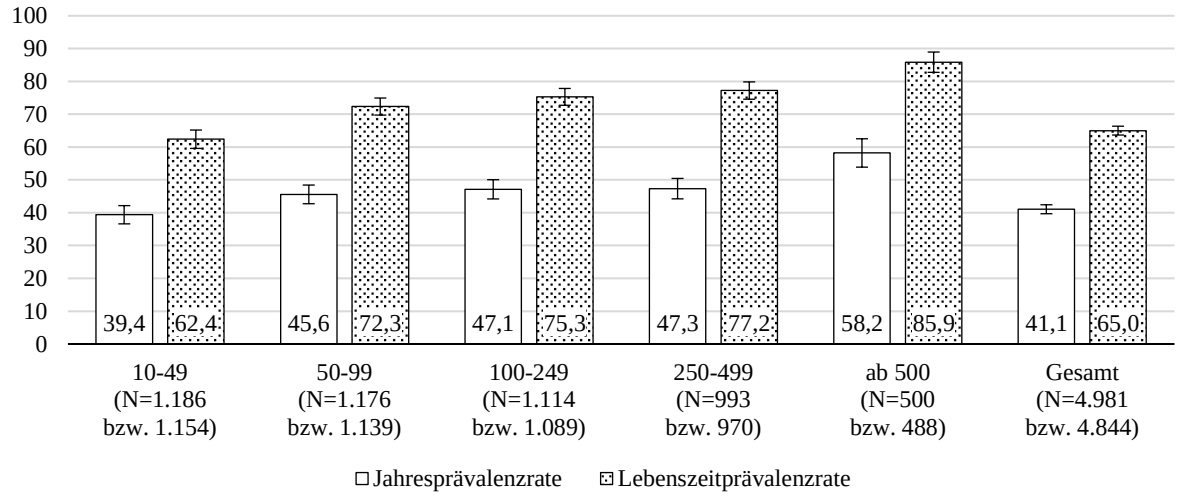
[265] Die Frage lautete: „Immer bezogen auf die letzten 12 Monate: Wie oft war Ihr Unternehmen von folgenden Angriffsarten betroffen und musste reagieren?“ Neben der Nennung der Angriffsart wurde diese kurz erläutert: „Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln“, „Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen“, „Sonstige Schadsoftware – z.B. Viren, Würmer oder Trojaner“, „Manuelles Hacking, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware“, Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten“, „Defacing-Attacken, die das Ziel hatten, unbefugt Webinhalte des Unternehmens zu verändern“, „CEO-Fraud, wobei eine Führungspersönlichkeit des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Beschäftigten zu bewirken“ und „Phishing, wobei Beschäftigte mit echt aussehenden E-Mails oder Webseiten getäuscht wurden, um z.B. sensible Unternehmensdaten zu erlangen“.

[266] Vgl. Paoli et al. (2018).

[267] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2019b).

Die Unternehmen, die im letzten Jahr keine der erfragten Cyberangriffsarten erlebt haben, wurden gefragt, ob sie von diesen jemals betroffen gewesen waren. Zusammen mit den Angaben zur Jahresprävalenz lässt sich eine „Lebenszeitprävalenz“ für Unternehmen[268] berechnen, wonach etwa zwei Drittel der Unternehmen (65,0 %) jemals von mindestens einem Cyberangriff getroffen wurden, auf den reagiert werden musste.

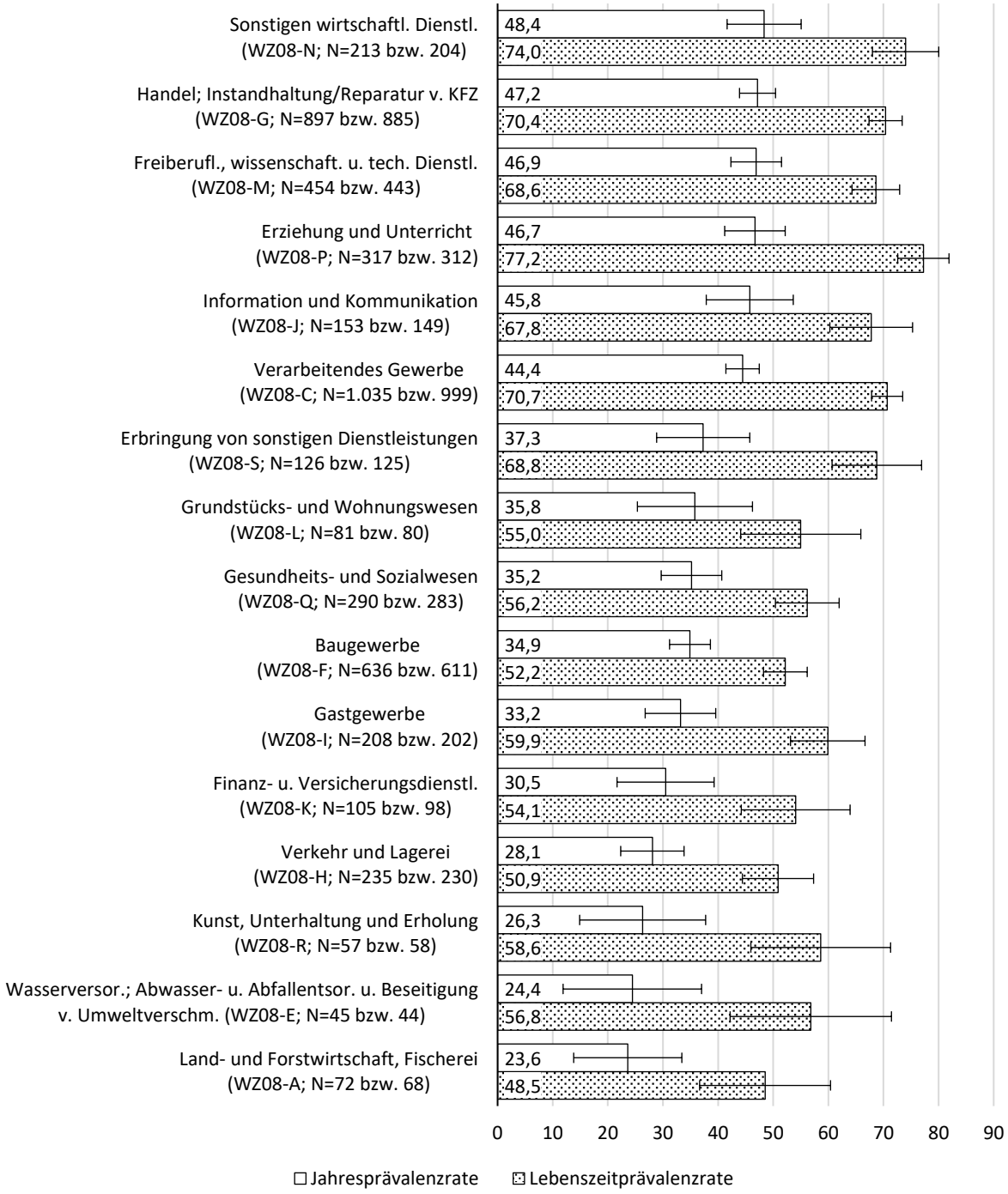
Abbildung 31 **Prävalenzraten für Cyberangriffe insgesamt nach Beschäftigtengrößenklassen**
in Prozent; gewichtete Daten; 95%-KI



Differenziert nach Beschäftigtengrößenklassen der Unternehmen (Abbildung 31) zeigt sich, dass Unternehmen mit zehn bis 49 Beschäftigten insgesamt betrachtet eine statistisch signifikant kleinere Jahresprävalenzrate aufweisen (39,4 %) als alle anderen. Demgegenüber haben Unternehmen ab 500 Besch. eine signifikant größere Prävalenzrate als alle anderen (58,2 %). Die Unterschiede zwischen den Unternehmen der übrigen Beschäftigtengrößenklassen (50-99, 100-249 und 250-499) sind statistisch nicht bedeutsam und könnten zufällig entstanden sein. Ein ähnliches Bild zeigt sich in Hinblick auf die „Lebenszeitprävalenz“ von Unternehmen. Auch hier ist ein tendenzieller Anstieg mit zunehmender Beschäftigtenzahl zu erkennen, wobei sich die Anteile von kleinen und sehr großen Unternehmen statistisch signifikant voneinander (10-49 Besch.: 62,4 % vs. ab 500 Besch.: 85,9) sowie von den Unternehmen der übrigen Beschäftigtengrößenklassen unterscheiden. Eine Hypothese für diese Beobachtung wäre, dass größere Unternehmen aufgrund eines höheren Reifegrades im Bereich IT-Sicherheit und des größeren Ressourceneinsatzes Angriffe vermeintlich zuverlässiger erkennen und anschließend auch berichten können als kleinere Unternehmen, die Cyberangriffe seltener entdecken. Das sogenannte „doppelte“ oder „absolute“ Dunkelfeld, das auch durch Dunkelfeldbefragungen nicht aufgehellt werden kann, ist nach dieser Hypothese bei kleinen Unternehmen größer als bei den großen. Diese Erklärung kann jedoch nicht für alle Angriffsarten gleichermaßen herangezogen werden, da beispielsweise Ransomware-, Defacing- und CEO-Fraud-Angriffe (letztere zumindest nach einer gewissen Zeit) aufgrund ihrer offensichtlichen Folgen i.d.R. fast immer erkannt werden.

[268] Das Ergebnis der Lebenszeitprävalenz wird hier vermutlich noch unterschätzt, da insbesondere länger zurückliegende Ereignisse, die das Unternehmen betreffen, von den befragten Vertreter*innen, die zudem unterschiedlich lange im Unternehmen tätig sind, möglicherweise weniger gut oder gar nicht erinnert werden (können) als z.B. persönliche Ereignisse.

Abbildung 32 **Prävalenzraten für Cyberangriffe insgesamt nach WZ08-Klassen der ersten Ebene**
in Prozent; gewichtete Daten; 95%-KI; nur wenn N≥30



Im Vergleich der Jahres- und Lebenszeitprävalenzen einzelner Branchen auf der ersten Ebene der WZ08-Klassifikation (Abbildung 32) sind stärker belastete Wirtschaftszweige wie Handel; Instandhaltung/Reparatur von KFZ (WZ08-G: 47,2 % Jahresprävalenz bzw. 70,4 % Lebenszeitprävalenz), freiberufliche, wissenschaftliche und technische Dienstleistungen (WZ08-M: 46,9 % bzw. 68,6 %), Erziehung und Unterricht (WZ08-P: 46,7 % bzw. 77,2 %) oder das verarbeitende Gewerbe (WZ08-C: 44,4 % bzw. 70,7 %) zu erkennen und demgegenüber weniger stark belastete Wirtschaftszweige wie Gesundheits- und Sozialwesen (WZ08-Q: 35,2 % bzw. 56,2 %), Baugewerbe (WZ08-F: 34,9 % bzw. 52,2 %), Gastgewerbe (WZ08-I: 33,2 % bzw. 59,9 %) und Verkehr und Lagerei (WZ08-H: 28,1 % bzw. 50,9 %).

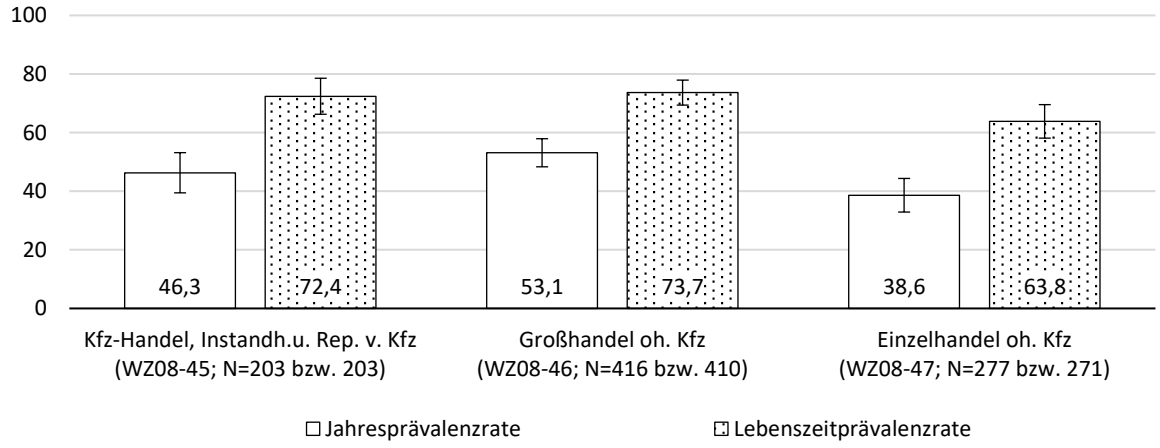
Die Unterschiede zwischen den WZ08-Klassen könnten z.T. mit unterschiedlichen Verteilungen nach Beschäftigtengrößenklassen erklärt werden, insofern z.B. Branchen mit tendenziell eher kleineren Unternehmen weniger stark von Cyberangriffen betroffen sind als Branchen in denen es eher größere Unternehmen gibt. Um dies zu überprüfen, werden in Tabelle 23 die Prävalenzen von Unternehmen des Baugewerbes (WZ08-F) und des Handels, Instandhaltung/Reparatur von Kfz (WZ08-G) in den jeweiligen Beschäftigtengrößenklassen verglichen.

Tabelle 23 **Prävalenzraten für Cyberangriffe insgesamt nach Beschäftigtengrößenklasse und Branche**
in Prozent; fett: signifikant bei p<.05 (Chi²-Test)

	Jahresprävalenzrate		Lebenszeitprävalenzrate	
Beschäftigtengrößenklasse	Baugewerbe (WZ08-F)	Handel; Instandhaltung/Reparatur v. KFZ (WZ08-G)	Baugewerbe (WZ08-F)	Handel; Instandhaltung/Reparatur v. Kfz (WZ08-G)
10-49	**34,2** (N=120)	**46,0** (N=163)	**51,3** (N=115)	**68,9** (N=161)
50-99	43,1 (N=72)	53,2 (N=173)	**59,2** (N=71)	**77,8** (N=167)
100-249	**35,4** (N=65)	**53,3** (N=137)	**62,5** (N=64)	**78,8** (N=137)
250-499	45,9 (N=37)	50,5 (N=91)	62,9 (N=35)	77,3 (N=88)
ab 500	9/13	55,3 (N=38)	13/13	79,5 (N=39)

Dabei zeigt sich, dass die Unterschiede sowohl bezüglich der Jahresprävalenzrate als auch der Lebenszeitprävalenzrate zumindest tendenziell zwischen den beiden Wirtschaftszweigen in den jeweiligen Beschäftigtengrößenklassen erhalten bleiben. Statistisch signifikant sind die Unterschiede zwischen den beiden Wirtschaftszweigen bei Unternehmen von zehn bis 49 Beschäftigten, von 100 bis 249 Beschäftigten und hinsichtlich der Lebenszeitprävalenz auch von 50 bis 99 Beschäftigten. Das Ergebnis, dass Unternehmen des Baugewerbes (WZ08-F) weniger stark von Cyberangriffen insg. betroffen sind als Unternehmen des Handels, Instandhaltung/Reparatur von Kfz (WZ08-G) lässt sich zumindest nicht vollständig durch unterschiedlich vertretene Unternehmensgrößen in den Wirtschaftszweigen erklären.

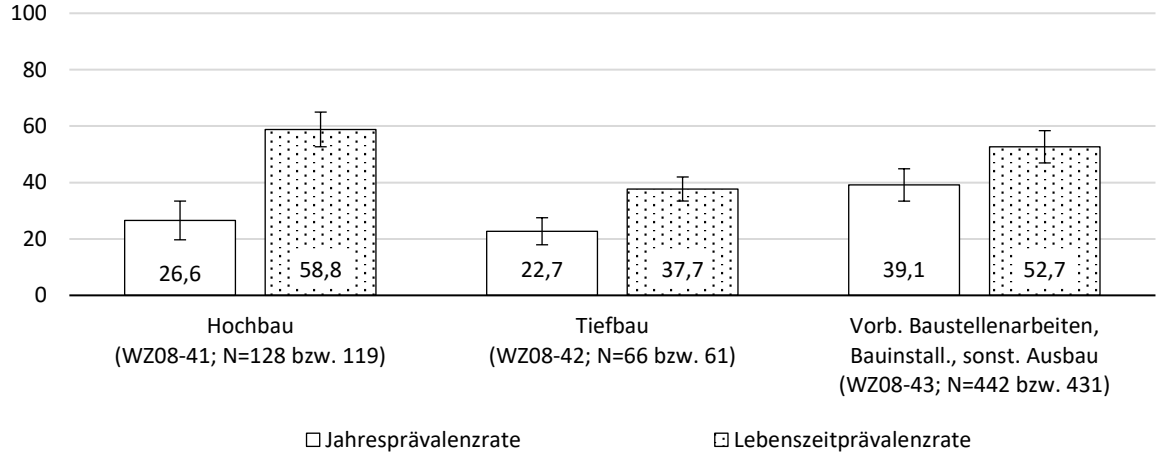
Abbildung 33 **Prävalenzraten für Cyberangriffe insg. innerhalb des Handels, Instandhaltung/Reparatur von Kfz (WZ08-G)**
in Prozent; gewichtete Daten; 95%-KI



Am Beispiel von Unternehmen des Handels, Instandhaltung/Reparatur von Kfz (WZ08-G) kann gezeigt werden, dass es auch innerhalb eines Wirtschaftszweiges, d.h. der ersten Ebene der WZ08-Klassifikation, Unterschiede gibt (Abbildung 33): So ist der Einzelhandel (WZ08-47) sowohl in den vergangenen zwölf Monaten (38,6 %) als auch darüber hinaus (63,8 %) signifikant weniger stark durch Cyberangriffe insgesamt betroffen als der Großhandel (WZ08-46:

53,1 % bzw. 73,7 %), der sich nur tendenziell vom Kfz-Handel, Instandhaltung und Reparatur von Kfz (WZ08-45: 46,3 % bzw. 72,4 %) unterscheidet.

Abbildung 34 **Prävalenzraten für Cyberangriffe insg. innerhalb des Baugewerbes (WZ08-F)**
in Prozent; gewichtete Daten; 95%-KI

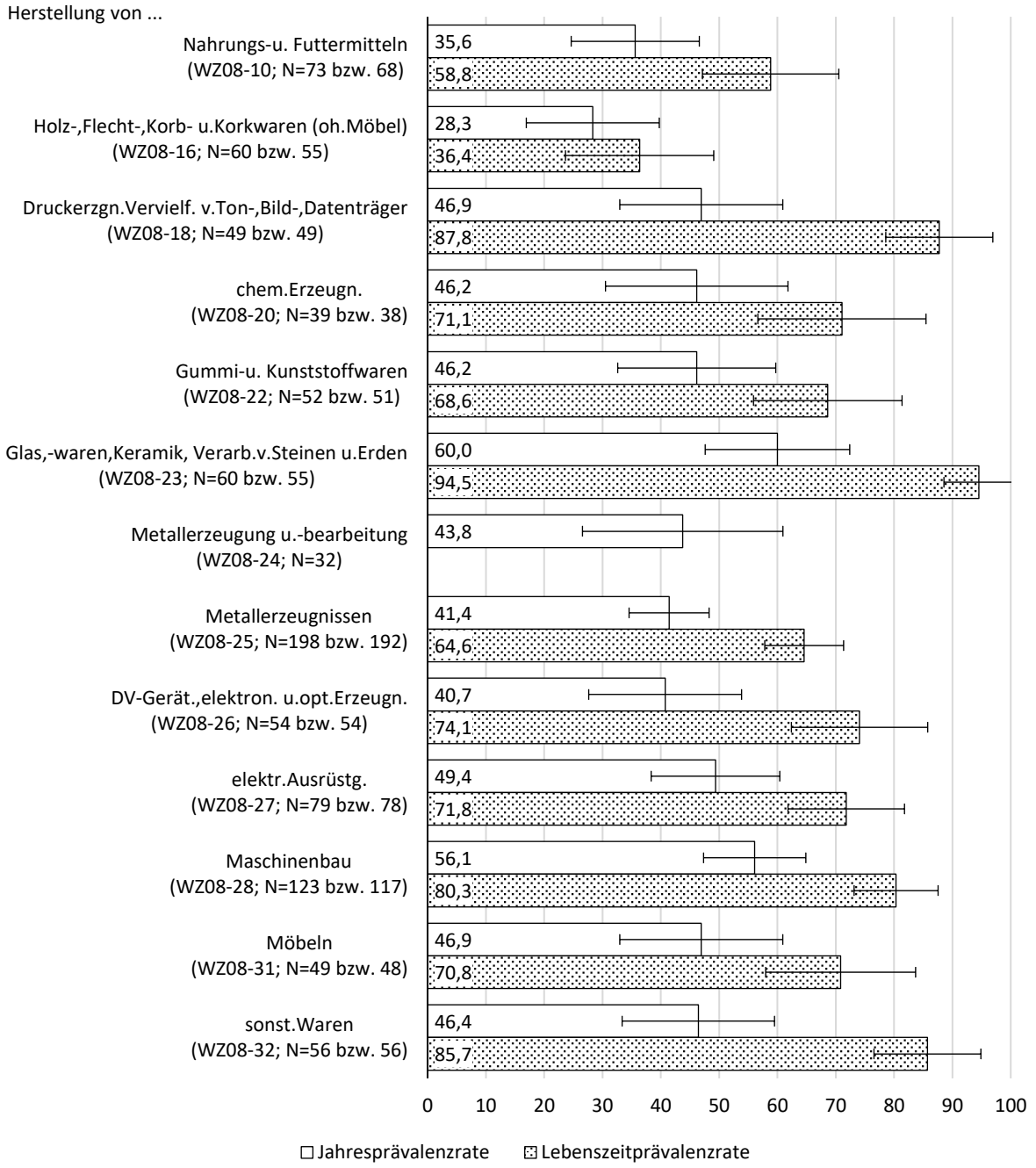


Statistisch signifikante Unterschiede zeigen sich ebenfalls innerhalb des Baugewerbes (WZ08-C) in Abbildung 34: Unternehmen für vorbereitende Baustellenarbeiten, Bauinstallationen und sonstigen Ausbau haben eine statistisch bedeutsam höhere Jahresprävalenz (39,1 %) als Tief- und Hochbauunternehmen (22,7 % bzw. 26,6 %). Verglichen mit Tiefbauunternehmen trifft dies ebenfalls auf die „Lebenszeitprävalenz“ (52,7 % vs. 37,7 %) zu.

Der Wirtschaftszweig des verarbeitenden Gewerbes gliedert sich auf der zweiten Ebene der WZ-Klassifikation in 24 Unterklassen auf, die zum Teil nicht in der für einen Vergleich nötigen Anzahl von Fällen besetzt sind. Es werden daher in Abbildung 35 nur Unterklassen mit mindestens 30 gültigen Antworten zur Betroffenheit dargestellt: Die Jahresprävalenz für Cyberangriffe insgesamt reicht von 28,3 % bei Unternehmen der Herstellung von Holz-, Korb- und Korkwaren (ohne Möbel; WZ08-16) bis zu einem Anteil von 60,0 % bei Unternehmen der Herstellung von Glaswaren, Keramik sowie Verarbeitung von Steinen und Erden (WZ08-23). Diese beiden Unterklassen haben auch die niedrigste bzw. höchste „Lebenszeitprävalenz“ (36,4 % vs. 94,5 %). Zu den stärker belasteten Unterklassen gehören Maschinenbauunternehmen (WZ08-28: 56,1 % bzw. 80,3 %) und Hersteller elektronischer Ausrüstung (WZ08-27: 49,4 % bzw. 71,8 %).[269]

[269] Aufgrund sehr unterschiedlicher Branchendefinitionen zusammen mit uneinheitlichen Definitionen zu Cyberangriffen in den betrachteten Studien des Literaturstandes sind an dieser Stelle kaum sinnvolle Vergleiche möglich.

Abbildung 35 **Prävalenzraten für Cyberangriffe insg. innerhalb des verarbeitenden Gewerbes (WZ08-C)**
in Prozent[270]; gewichtete Daten; 95%-KI



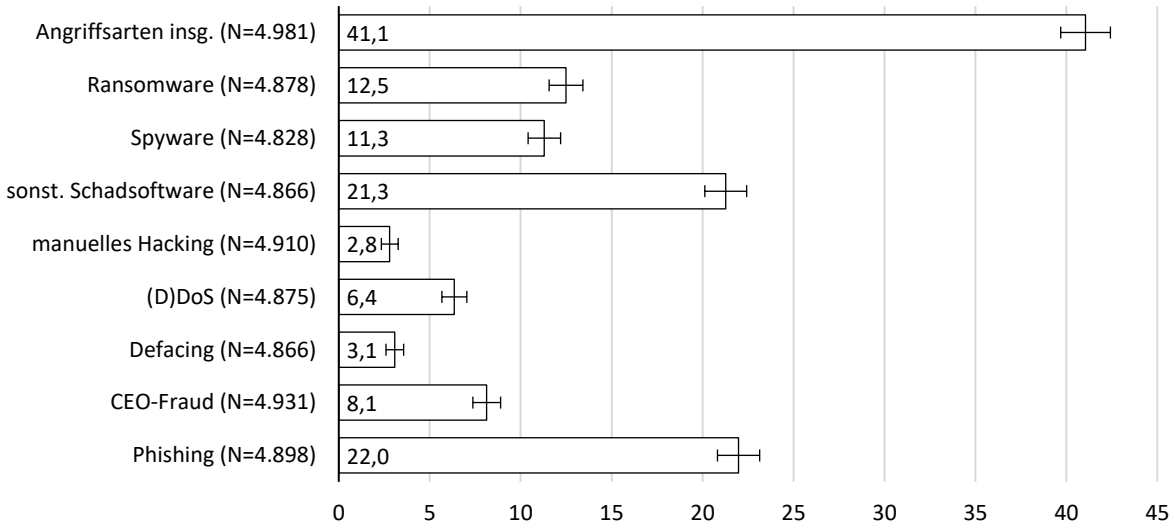
7.1.2 Cyberangriffe nach Angriffsart

Neben der Differenzierung der Betroffenheit nach Beschäftigtengrößenklassen und Branchenzugehörigkeit, lassen sich die Prävalenzen[271] hinsichtlich der Angriffsart miteinander vergleichen (Abbildung 36).

[270] Unterkategorien mit einer Fallzahl kleiner 30 werden nicht dargestellt. Die Ergebnisse zu weiteren WZ-Unterkategorien, die dieses Kriterium erfüllen, finden sich in Tabelle 50 im Anhang 1.

[271] Im Folgenden werden nur die Jahresprävalenzen dargestellt, da die „Lebenszeitprävalenz“ nicht nach Angriffsart differenziert erhoben wurde.

Abbildung 36 **Jahresprävalenzraten nach Angriffsart**
in Prozent; gewichtete Daten; 95%-KI



Ein großer Teil der Unternehmen wurde von Angriffen mittels Schadsoftware getroffen: 12,5 % gaben an, in den letzten zwölf Monaten mindestens einen Ransomware-Angriff, 11,3 % einen Spyware-Angriff und 21,3 % einen sonstigen Schadsoftware-Angriff erlebt zu haben. Auf mindestens einen Phishing-Angriff musste über ein Fünftel der Unternehmen reagieren. Jedes zwölfte Unternehmen (8,1 %) war von CEO-Fraud, jedes sechzehnte Unternehmen (6,4 %) von (D)DoS-Angriffen betroffen. Mit Anteilen von 3,1 % bzw. 2,8 % betroffenen Unternehmen spielten die Angriffsarten Defacing und manuelles Hacking hinsichtlich der Verbreitung eine vergleichsweise geringe Rolle.

Der Vergleich mit Ergebnissen anderer Studien ist nur sehr eingeschränkt möglich. Trotz möglicher Spielräume in der Definition der Betroffenheit können z.B. Ransomware-, (D)DoS- und Schadsoftware-Angriffe aufgrund ihrer i.d.R. klareren Abgrenzungen näherungsweise verglichen werden. So berichtet das BSI in einer Umfrage aus 2016, dass in den letzten sechs Monaten 32 % der befragten Unternehmen durch Ransomware infiziert wurden.[272] Gründe für diese hohen Abweichungen können neben unterschiedlichen methodischen Vorgehensweisen bei der Stichprobenziehung[273] auch die technologische Entwicklung sein, die in den letzten Jahren Unternehmen ggf. zuverlässiger von Ransomware-Angriffen geschützt hat. Ebenfalls hohe Abweichungen zur aktuellen Cyber-Sicherheits-Umfrage des BSI finden sich in Bezug auf (D)DoS-Angriffe. Hier berichtet das BSI von Anteilen in Höhe von 18 %, rund dreimal höher als in der vorliegenden Studie.[274] Gründe dafür dürften auch hierbei vor allem in der Art der Stichprobenziehung liegen. Klahr et al. kommen in ihrer repräsentativen Studie für britische Unternehmen hingegen zu ähnlichen Ergebnissen. So werden Mal- oder Spyware-Angriffe mit insgesamt 33 % angegeben (hier zusammen 32,6 %) sowie Ransomware-Angriffe mit 17 % (hier 12,5 %) beziffert.[275]

[272] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2016).

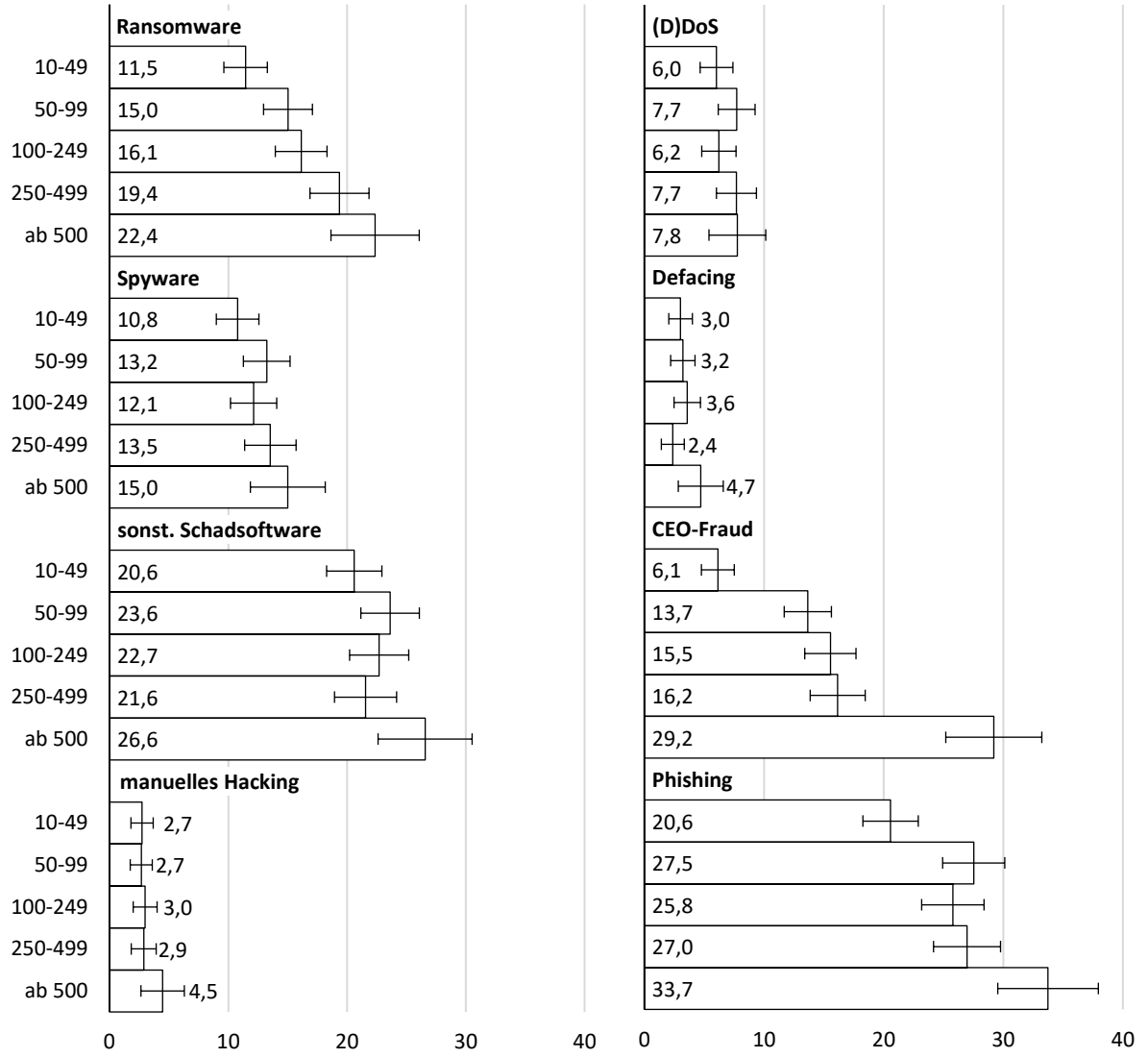
[273] Z.B. erlauben Stichproben, bei denen sich die Teilnehmer*innen selbst rekrutieren, keine Rückschlüsse auf die Grundgesamtheit und schließen den Vergleich mit anderen Studien weitgehend aus.

[274] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2019b).

[275] Vgl. Klahr et al. (2017).

Wie bereits in Abbildung 31 gezeigt, sind bezogen auf Cyberangriffe insgesamt große Unternehmen (ab 500 Besch.) deutlich stärker betroffen als kleine (10-49 Besch.). Bei der Differenzierung zwischen den einzelnen Angriffsarten wird erkennbar, dass es nicht in jedem Fall signifikante Unterschiede zwischen den Beschäftigtengrößenklassen gibt (Abbildung 37).

Abbildung 37 **Jahresprävalenzraten nach Angriffsart und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI; Mehrfachantworten möglich



In Hinblick auf manuelles Hacking, (D)DoS-Angriffe und Defacing sind allenfalls tendenzielle Unterschiede zwischen kleinen und großen Unternehmen zu erkennen. Hingegen unterscheiden sich die Prävalenzen bezogen auf Ransomware-Angriffe, CEO-Fraud und Phishing sehr deutlich. Dies ist insofern überraschend, weil es sich um Angriffsarten handelt, die anders als z.B. Spyware-Angriffe oder manuelles Hacking in ihrer Konsequenz schnell offensichtlich werden. Eine naheliegende Erklärung, dass große Unternehmen aufgrund größerer Ressourceneinsätze im Bereich der IT-Sicherheit möglicherweise mehr Angriffe erkennen als kleinere Unternehmen, greift bei diesen Angriffsarten kaum. Stattdessen deutet sich hierbei an, dass große Unternehmen vermutlich aufgrund ihrer höheren Präsenz im Internet und ihrer umfangreicheren IT-Infrastruktur sowie höheren Anzahl von IT-Nutzer*innen eine größere Angriffsfläche insbesondere für ungezielte Cyberangriffe bieten.

Bei Ransomware-Angriffen ist ein linearer Anstieg der Prävalenzrate mit zunehmender Unternehmensgröße zu erkennen. Während nur etwa jedes neunte kleine Unternehmen (10-49 Besch.: 11,5 %; N=1.161) in den vergangenen zwölf Monaten von mindestens einem Ransomware-Angriff betroffen war, betraf es jedes vierte bis fünfte große Unternehmen (ab 500 Besch.: 22,4 %; N=483). Eine denkbare Erklärung ist hier, dass E-Mails als typische Infektionswege für Ransomware (z.B. Bewerbungen, Einladungen etc.) bei kleineren Unternehmen rein quantitativ weniger eingehen, die Zahl der potenziellen Absender überschaubarer und deren Bekanntheit größer ist. Deshalb dürften fingierten E-Mails in kleinen Unternehmen ggf. besser als solche identifiziert werden können.

Ein noch deutlicherer Unterschied zwischen kleinen und großen Unternehmen zeigt sich beim CEO-Fraud: 6,1 % der kleinen (10-49 Besch.) aber 29,2 % der großen Unternehmen (ab 500 Besch.) musste innerhalb eines Jahres auf einen oder mehrere solcher Angriff reagieren. Neben der größeren Internetpräsenz und Angriffsfläche könnten komplexere Organisationsstrukturen als Erklärung für die deutlich stärkere Betroffenheit großer Unternehmen angeführt werden, insofern damit verbundene unübersichtlichere Arbeitsabläufe, unklarere Zuständigkeiten und größere Kommunikationsprobleme sowie eine mit der Unternehmensgröße zunehmende Anonymität unter den Beschäftigten von den Täter*innen gezielt ausgenutzt werden können.

Von Phishing-Angriffen in den vorangegangenen zwölf Monaten ist ein Fünftel der kleinen Unternehmen (10-49 Besch.: 20,6 %) und ein Drittel der großen Unternehmen (ab 500 Besch.: 33,7 %) betroffen.

Neben der Beschäftigtengrößenklasse könnte auch die WZ-Klassenzugehörigkeit im Zusammenhang mit der Belastung durch verschiedene Angriffsarten stehen. In Tabelle 24 ist diesbezüglich anhand der Schattierung zu erkennen, dass einzelne WZ08-Klassen auf der ersten Ebene stärker durch bestimmte Angriffsarten belastet sind als andere: So ist z.B. das verarbeitende Gewerbe (WZ08-C) am stärksten von Phishing (28,0 %) aber vor allem auch von Ransomware (14,5 %), Spyware (12,8 %) und sonstige Schadsoftware (22,6 %) betroffenen.

Tabelle 24 zeigt, dass innerhalb der WZ08-Klassen tendenziell Unterschiede in der Betroffenheit durch bestimmte Angriffsarten bestehen. Während ein überwiegender Teil der WZ08-Klassen am stärksten durch sonst. Schadsoftware und Phishing betroffen ist, wurden Land- u. Forstwirtschaft, Fischerei sowie Kunst, Unterhaltung und Erholung am häufigsten durch Ransomware-Angriffe getroffen.

Des Weiteren fällt auf, dass in den WZ08-Klassen P: Erziehung u. Unterricht sowie M: Freiberufl., wissenschaftl. u. techn. Dienstleist. jeweils zwei Angriffsarten anteilmäßig am häufigsten auftraten. Hinzu kommt, dass in diesen beiden WZ08-Klassen auch relativ viele grau schattierte Zellen (fünf größten Anteile je Angriffsart) vorhanden sind, was auf eine vergleichsweise hohe allgemeine Vulnerabilität diese Wirtschaftszweige gegenüber Cyberangriffen hindeutet.

Tabelle 24 **Jahresprävalenzraten für Cyberangriffe nach Angriffsart und WZ08-Klassen**
in Prozent; gewichtete Daten

	Cyberangriffsart							
WZ08-Klasse (Ebene 1)[276]	1	2	3	4	5	6	7	8
Land- u. Forstwirtschaft, Fischerei (WZ08-A)	13,7	6,8	8,3	0,0	7,4	0,0	1,4	8,3
Verarbeitendes Gewerbe (WZ08-C)	14,5	12,8	22,6	2,1	6,5	3,4	8,3	**28,0**
Wasserversor.; Abwasser- u. Abfallentsor. u. Beseitigung v. Umweltverschm. (WZ08-E)	8,9	7,0	13,3	0,0	4,7	2,3	6,8	11,4
Baugewerbe (WZ08-F)	9,9	9,8	20,9	1,7	3,4	0,8	4,9	18,1
Handel; Instandhaltung u. Reparatur von Kfz (WZ08-G)	14,5	13,3	24,2	5,2	5,0	3,1	9,5	22,8
Verkehr und Lagerei (WZ08-H)	8,7	6,6	13,5	1,7	4,3	3,0	6,9	13,9
Gastgewerbe (WZ08-I)	10,6	12,6	20,6	3,4	7,0	3,4	3,9	19,3
Information u. Kommunikation (WZ08-J)	6,7	6,7	25,0	1,3	**18,8**	4,0	5,3	24,3
Finanz- u. Versicherungsdienstleistungen (WZ08-K)	4,8	8,7	16,5	0,0	2,9	1,0	5,8	22,0
Grundstücks- u. Wohnungswesen (WZ08-L)	12,5	8,8	15,2	1,2	8,8	3,7	12,2	25,0
Freiberufl., wissenschaftl. u. techn. Dienstleist. (WZ08-M)	15,7	10,5	**25,2**	**5,3**	10,0	4,3	7,3	23,5
Sonst. wirtschaftl. Dienstleist. (WZ08-N)	9,1	12,4	20,7	2,9	5,8	2,5	**17,0**	27,8
Erziehung u. Unterricht (WZ08-P)	**16,4**	**14,8**	21,7	2,6	8,3	5,0	7,4	16,8
Gesundheits- u. Sozialwesen (WZ08-Q)	11,8	11,7	20,9	2,1	4,2	**6,0**	12,5	23,0
Kunst, Unterhaltung u. Erholung (WZ08-R)	14,5	7,0	13,8	0,0	1,7	1,8	3,4	6,9
Sonstige Dienstleist. (WZ08-S)	3,2	5,9	16,5	0,8	8,3	0,0	12,0	19,0

Cyberangriffsart: 1: Ransomware, 2: Spyware, 3: sonst. Schadsoftware, 4: manuelles Hacking, 5: (D)DoS, 6: Defacing, 7: CEO-Fraud, 8: Phishing
Hervorhebung: fett: größter Anteil je Angriffsart; grau hinterlegt: die fünf größten Anteile je Angriffsart; unterstrichen: größter Anteil je WZ08-Klasse

7.1.3 Androhung von Cyberangriffen

Die betroffenen wie nicht betroffenen Unternehmen wurden danach gefragt, ob ihnen in den letzten zwölf Monaten eine der angeführten Angriffsarten zumindest angedroht wurde. Dies bejahte ein Anteil von 3,9 % (N=4.982). Bei 44,1 % der Unternehmen, denen ein Cyberangriff angedroht wurde (N=197) blieb es bei der Drohung, sie erlebten im gleichen Zeitraum keinen Cyberangriff.[277]

7.1.4 Nichtbetroffene Unternehmen

Unternehmen, die in den letzten zwölf Monaten keinen Cyberangriff erlebten, wurden gefragt, für wie wahrscheinlich sie es halten, dass ein Cyberangriff erfolgt ist, der nur nicht bemerkt wurde. Etwa ein Drittel (31,1 %, N=2.876) hält dies für sehr und über die Hälfte (57,3 %) für eher unwahrscheinlich. Demgegenüber hält jedes zehnte Unternehmen (9,8 %) dieses Szenario für eher und ein sehr kleiner Anteil von 1,9 % für sehr wahrscheinlich. Der Anteil der Unternehmen, die dies für eher/sehr wahrscheinlich halten ist bei denjenigen signifikant geringer, die

[276] Klassen mit einer Fallzahl kleiner 30 werden nicht aufgeführt.

[277] Ein Anteil von 55,9 % (N=197) erlebte mindestens einen Cyberangriff, wobei aufgrund der Erhebung unklar bleibt, ob der angedrohte Angriff umgesetzt wurde oder im selben Zeitraum ein anderer Angriff ohne vorherige Androhung erlebt wurde. Bezüglich des schwerwiegendsten Angriffes wurde die Frage nach der Androhung jedoch erneut gestellt.

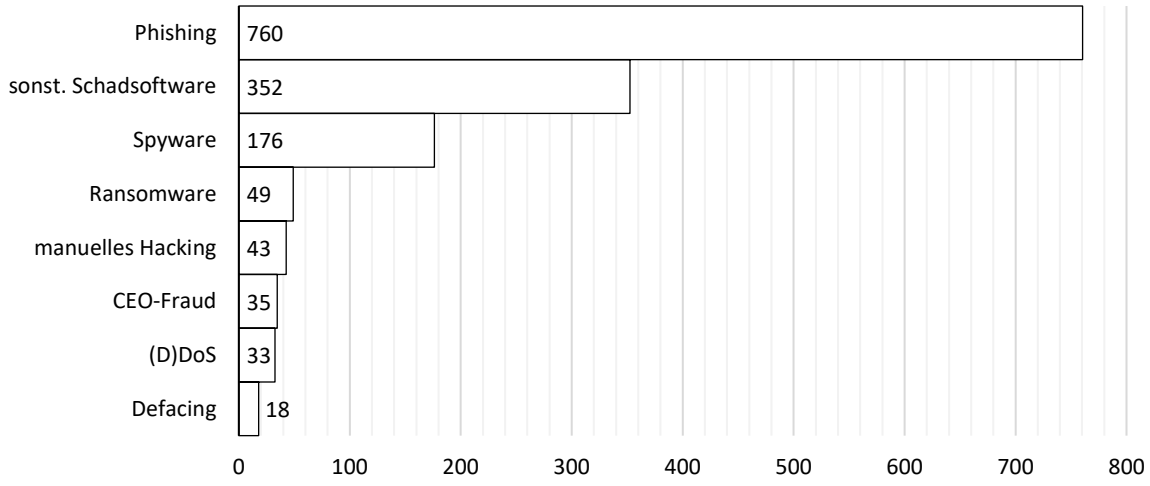
noch nie einen Cyberangriff erlebt haben (7,8 %, N=1.643) als bei denjenigen, die vor den letzten zwölf Monaten mindestens einmal angegriffen wurden (17,4 %, N=1.092). Dies deutet darauf hin, dass das Risikobewusstsein bei bereits betroffenen Unternehmen höher ist, als bei noch nicht betroffenen. Weitere statistisch bedeutsame Unterschiede hinsichtlich dieser Einschätzung sind weder in Hinblick auf die Positionen der antwortenden Unternehmensvertreter*innen noch zwischen Unternehmen verschiedener Beschäftigtengrößenklassen zu erkennen.

7.2 Inzidenzrate

Neben der Angabe, ob die befragten Unternehmen in den vorangegangenen zwölf Monaten mindestens einmal von der jeweiligen Angriffsart betroffen waren (Prävalenz), wurde auch die Anzahl der Cyberangriffe, auf die in diesem Zeitraum reagiert werden musste, erhoben.[278] Die summierten Ereignisse, von denen die Unternehmen für diesen Zeitraum berichteten, bilden die sogenannte Inzidenz und die relativierte Anzahl der Ereignisse je 100 Unternehmen die Inzidenzrate. Danach erlebten 100 Unternehmen in den letzten zwölf Monaten z.B. 760 Phishing-Angriffe, 352 Angriffe mit sonstiger Schadsoftware und 176 Spyware-Angriffe aber lediglich 49 Ransomware-Angriffe auf die sie reagieren mussten (Abbildung 38).

Abbildung 38 **Inzidenzraten nach Angriffsart**

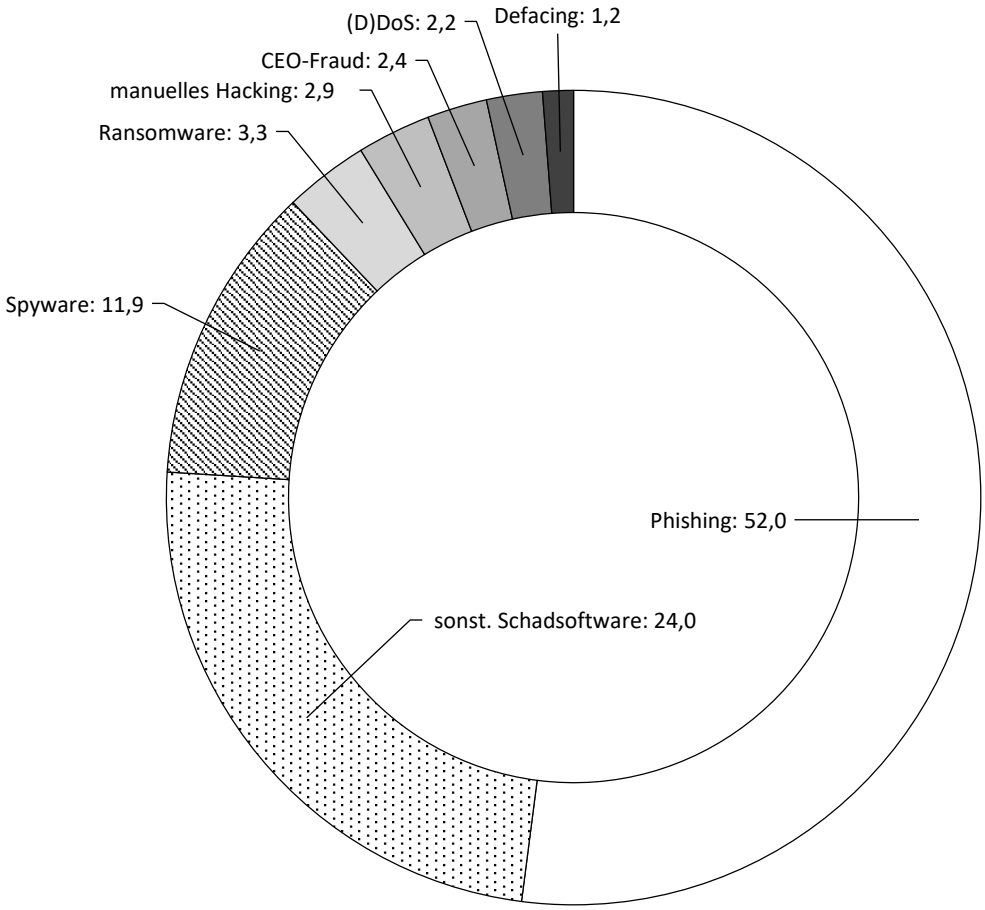
Anzahl der Cyberangriffe in den letzten 12 Monaten je 100 Unternehmen; gewichtete Daten



Daneben lassen sich die für jede Angriffsart summierten Ereignisse ins Verhältnis zur Gesamtzahl aller berichteten Cyberangriffe setzen (Abbildung 39). Sowohl anhand der Inzidenzraten als auch an den Anteilen der jeweiligen Angriffsarten an allen berichteten Cyberangriffen lässt sich gegenüber den Jahresprävalenzraten (Abbildung 36) eine veränderte Rangfolge feststellen.

[278] Um den Einfluss von Extremwerten bei der folgenden Auswertung zu reduzieren, wurden diese bei der jeweiligen Angriffsart auf einen Wert zurückgesetzt, der aus dem Mittelwert addiert mit drei Standardabweichungen (bei Unternehmen ab 500 Besch.: Mittelwert addiert mit vier Standardabweichungen) berechnet wurde. Der Unterschied in der Berechnung des oberen Grenzwertes zwischen großen Unternehmen (ab 500 Besch.) und allen anderen begründet sich in der höheren theoretisch möglichen Anzahl an Vorfällen bei sehr großen Unternehmen.

Abbildung 39 **Anteile der erlebten Cyberangriffe nach Angriffsart**
in Prozent; gewichtete Daten



Phishing- und sonstige Schadsoftware-Vorfälle (52,0 % bzw. 24,0 %) machen zusammen über drei Viertel aller erlebten Cyberangriffe aus und bleiben auf den vorderen Rängen. Anders als bei den Jahresprävalenzraten liegt der Anteil von Spyware-Angriffen (11,9 %) an allen Cyberangriffen über dem von Ransomware-Angriffen (3,3 %). D.h., im Vergleich zu Ransomware-Angriffen wurden Spyware-Angriffe zwar tendenziell von weniger Unternehmen erlebt (11,3 % vs. 12,5 %), dafür aber in einer deutlich höheren Anzahl. Ähnlich verhält es sich hinsichtlich manuellem Hacking: die Zahl der Unternehmen, die einen solchen Angriff innerhalb eines Jahres erlebte, ist zwar geringer als bei allen anderen Angriffsarten, die Zahl der berichteten Vorfälle liegt hingegen anteilig über der von CEO-Fraud, (D)DoS und Defacing (2,9 % vs. 2,4 %, 2,2 % bzw. 1,2 %). Dies deutet darauf hin, dass Spyware-Angriffe und manuelles Hacking gezielter auf bestimmte Unternehmen erfolgen als die anderen Angriffsarten.

Zwischen den Beschäftigtengrößenklassen sind ebenfalls tendenziell Unterschiede hinsichtlich der Fallanteile je Angriffsart zu erkennen (Tabelle 25). Interessant dabei ist, dass diese Unterschiede keinem linearen Trend folgen (z.B. je größer das Unternehmen, desto größer der Anteil von Phishing).

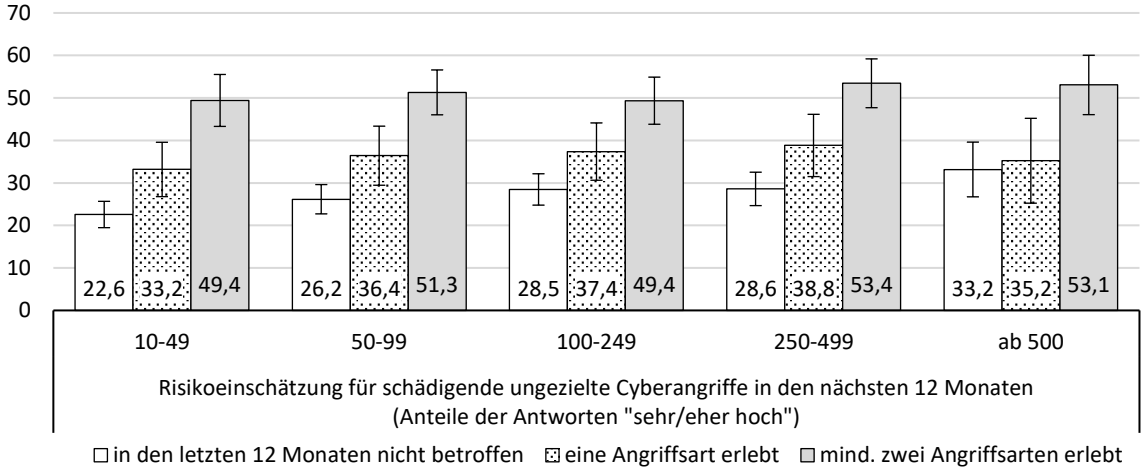
Tabelle 25 **Anteile der erlebten Cyberangriffe nach Angriffsart und Beschäftigtengrößenklassen**
in Prozent; gewichtete Daten

	Beschäftigtengrößenklasse				
Cyberangriffsart	10-49	50-99	100-249	250-499	ab 500
Phishing	57,1	43,7	38,7	51,1	36,0
sonst. Schadsoftware	19,0	32,5	38,0	25,4	36,5
Spyware	12,4	10,4	7,0	11,9	18,1
Ransomware	2,6	6,3	4,4	4,7	3,1
manuelles Hacking	4,0	0,4	1,8	0,3	0,7
CEO-Fraud	1,3	4,2	5,6	3,0	4,2
(D)DoS	2,2	1,6	3,5	3,2	0,6
Defacing	1,4	1,0	1,1	0,5	0,7
Gesamt	100,0	100,0	100,0	100,0	100,0

7.3 Risikoeinschätzung nach erlebten Cyberangriffen

Es ist ein allgemeiner Befund der Dunkelfeldforschung, dass die Erfahrung, Opfer einer Straftat geworden zu sein, im Zusammenhang mit einer erhöhten Kriminalitätsfurcht steht, wozu auch eine höhere Risikoeinschätzung bezüglich einer zukünftigen Viktimisierung gehört.[279] Von diesem Befund ausgehend, kann auch für den Unternehmenskontext ein ähnliche Beziehung zwischen erlebten Cyberangriffen und der Risikoeinschätzung für das Unternehmen erwartet werden.

Abbildung 40 **Risikoeinschätzung für ungezielte Cyberangriffe nach Betroffenheit und Beschäftigtengrößenklasse**
Anteile der Antworten „sehr/eher hoch“ in Prozent; gewichtete Daten



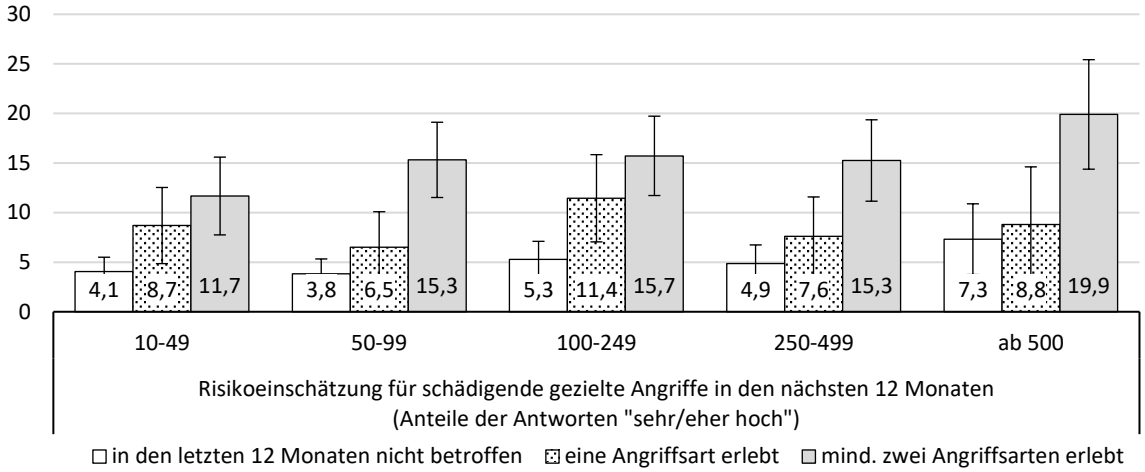
In Abbildung 40 sind die Anteile der Unternehmen dargestellt, für die das Risiko, in den nächsten zwölf Monaten einen schädigenden ungezielten Cyberangriff zu erleiden, als „sehr“ oder „eher hoch“ eingeschätzt wurde. Diese wurden neben der Beschäftigtengrößenklasse zusätzlich danach differenziert, ob sie in den letzten zwölf Monaten von keiner, einer oder mehreren An-

[279] Zu den Folgen von computerbezogener Kriminalität bei Privatpersonen siehe z.B. Dreißigacker & Riesner (2018).

griffsarten betroffen waren. Wie vermutet, wurde das Risiko bezüglich ungezielter Cyberangriffe signifikant seltener „sehr/eher hoch“ eingeschätzt, je weniger Erfahrungen in den letzten zwölf Monaten mit Cyberangriffen gemacht wurden.

Ein ähnliches Bild zeigt sich auch in Bezug auf die Risikoeinschätzungen für Unternehmen zu gezielten schädigenden Cyberangriffen (Abbildung 41). Für Unternehmen, die im Vorjahr auf einen oder mehrere Angriffsarten reagieren mussten, wurde das Risiko erneuter schädigender Angriffe im Folgejahr zumindest tendenziell höher eingeschätzt als für nichtbetroffene Unternehmen.

Abbildung 41 **Risikoeinschätzung für gezielte Cyberangriffe nach Betroffenheit und Beschäftigtengrößenklasse**
Anteile der Antworten „sehr/eher hoch“ in Prozent; gewichtete Daten



7.4 Zwischenresümee

In diesem Kapitel wurde dargestellt, in welchem Umfang Unternehmen durch Cyberangriffe betroffen waren. Insgesamt gaben 41,1 % der Unternehmen an, in den letzten zwölf Monaten von mindestens einer der erfragten Angriffsarten betroffen gewesen zu sein. Davon haben 57,2 % der Unternehmen mehrere unterschiedliche Angriffsarten erlebt. Hinsichtlich der sog. „Lebenszeitprävalenz“ gaben zwei Drittel der Unternehmen an, in der Vergangenheit Cyberangriffe erlebt zu haben. Insgesamt zeigt sich, dass kleinere Unternehmen geringere Prävalenzraten aufweisen als größere.

Neben der Beschäftigtengrößenklasse steht die Branchenzugehörigkeit im Zusammenhang mit der Prävalenzrate, die von 23,6 % bei Unternehmen der Land- und Forstwirtschaft und Fischerei (WZ08-A) bis 48,4 % bei Unternehmen sonstiger wirtschaftlichen Dienstleistungen (WZ08-N) reicht. Diese Varianz besteht auch unabhängig von den Beschäftigtengrößenklassen und ist darüber hinaus z.T. auch auf der zweiten Ebene einzelner WZ-Klassen zu finden.

Ein großer Teil der Unternehmen wurde von Angriffen mittels Schadsoftware getroffen: 12,5 % durch mindestens einen Ransomware-Angriff, 11,3 % durch einen Spyware-Angriff und 21,3 % durch einen sonstigen Schadsoftware-Angriff. Auf mindestens einen Phishing-Angriff musste über ein Fünftel der Unternehmen reagieren. Jedes zwölfte Unternehmen war von CEO-Fraud, jedes sechzehnte Unternehmen von (D)DoS-Angriffen betroffen. Mit Anteilen von 3,1 % bzw. 2,8 % betroffenen Unternehmen spielten die Angriffsarten Defacing und manuelles Hacking hinsichtlich der Verbreitung eine vergleichsweise geringe Rolle.

Hinsichtlich der jeweiligen Angriffsarten finden sich weitere Unterschiede zwischen den Beschäftigtengrößenklassen der Unternehmen: In Hinblick auf manuelles Hacking, (D)DoS-Angriffe und Defacing sind lediglich tendenzielle Unterschiede zwischen kleinen und großen Unternehmen zu erkennen. Demgegenüber unterscheiden sich die Prävalenzen bezogen auf Ransomware-Angriffe, CEO-Fraud und Phishing sehr deutlich. Dies ist insofern überraschend, weil es sich um Angriffsarten handelt, die anders als z.B. Spyware-Angriffe oder manuelles Hacking in ihrer Konsequenz schnell offensichtlich werden. Eine naheliegende Erklärung, dass große Unternehmen aufgrund größerer Ressourceneinsätze im Bereich der IT-Sicherheit möglicherweise mehr Angriffe erkennen als kleinere Unternehmen, greift bei diesen Angriffsarten weniger. Stattdessen deutet sich hierbei an, dass große Unternehmen vermutlich aufgrund ihrer höheren Präsenz im Internet und ihrer umfangreicheren IT-Infrastruktur sowie höheren Anzahl von IT-Nutzer*innen eine größere Angriffsfläche insbesondere für ungezielte Cyberangriffe bieten.

Mit Blick auf die Anteile der Angriffsarten an allen berichteten Cyberangriffen in den letzten 12 Monaten, machen Phishing- und sonstige Schadsoftware-Vorfälle (52,0 % bzw. 24,0 %) zusammen über drei Viertel aus. Interessant ist zudem, dass diese Anteile von Spyware und manuellem Hacking höher sind, als die Jahresprävalenzraten. Das bedeutet, dass diese Angriffsarten zwar insgesamt von weniger Unternehmen erlebt wurden, aber wenn, dann meist mehrfach.

Wie erwartet, steht die Betroffenheit von Cyberangriffe in den letzten zwölf Monaten auch im Zusammenhang mit der Einschätzung des Risikos für das Unternehmen, in den nächsten zwölf Monaten (erneut) einen schädigenden Cyberangriff zu erleben. Dies zeigte sich sowohl bezogen auf ungezielte Cyberangriffe, die gleichzeitig auch viele andere Unternehmen treffen, als auch auf gezielte Cyberangriffe, die nur das eigene Unternehmen treffen.

Im folgenden Kapitel wird dargestellt, welche Unternehmensmerkmale in einem positiven Zusammenhang mit der Prävalenzrate für Cyberangriffe insgesamt stehen und somit als potentielle Risikofaktoren anzusehen sind.

8 MÖGLICHE RISIKOFAKTOREN

Wie bereits bei der Darstellung der Prävalenzraten gezeigt wurde, gibt es statistisch bedeutsame Unterschiede der Betroffenheit von Cyberangriffen zwischen den Beschäftigtengrößenklassen und den Branchen (WZ08-Klassen): Größere Unternehmen und bestimmte Branchen (z.B. WZ08-G: Handel; Instandhaltung/Reparatur von KFZ oder WZ08-M: freiberufliche, wissenschaftliche und technische Dienstleistungen) sind häufiger von Cyberangriffen betroffen als andere.[280] Warum dies so ist, bleibt dabei ersteinmal offen.

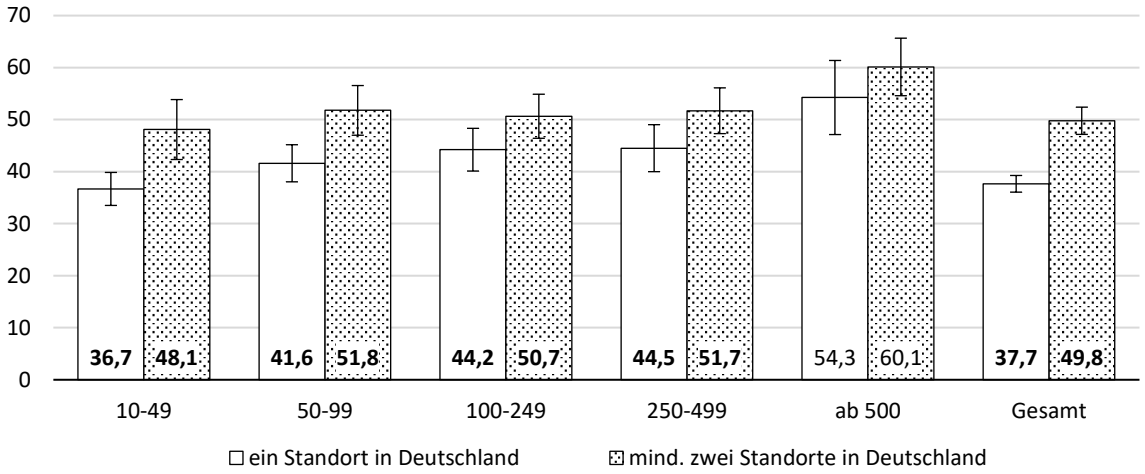
Im Folgenden werden weitere ausgewählte Unternehmensmerkmale mit der Jahresprävalenzrate für Cyberangriffe insgesamt in Beziehung gesetzt, um Hinweise darauf zu erhalten, welche weiteren Faktoren das Risiko für Cyberangriffe erhöhen. Daneben kann über die Kontrolle der Beschäftigtengrößenklassen überprüft werden, ob ein Zusammenhang ggf. in allen oder nur in einzelnen Größenklassen besteht. Über die Kontrolle des betrachteten Merkmals kann andererseits geprüft werden, ob die oben gezeigten Prävalenzunterschiede zwischen den Beschäftigtengrößenklassen innerhalb der jeweiligen Merkmalsgruppen stabil bleiben oder aufgelöst werden. Unterscheiden sich die Prävalenzraten innerhalb einer dieser Merkmalsgruppen nicht mehr zwischen den Beschäftigtengrößenklassen, kann das entsprechnde Merkmal als mögliche Erklärung für diesen Unterschied herangezogen werden.

8.1 Anzahl der Standorte

Die Anzahl der Standorte mit eigener IT-Infrastruktur könnte sich über eine damit verbundene komplexere und dezentralere IT-Struktur positiv auf das Risiko von Cyberangriffen auswirken. Bei einem Vergleich der Jahresprävalenzraten von Unternehmen mit einem (37,7 %; N=3.523) und Unternehmen mit mindestens zwei Standorten in Deutschland (49,8 %; N=1.400) zeigt sich dieser erwartete Zusammenhang als statistisch hoch signifikant ($p<.000$; Chi^2-Test). Auch wenn die Beschäftigtengrößenklasse der Unternehmen kontrolliert wird, bleibt dieser Zusammenhang bestehen (Abbildung 42). Lediglich bei Unternehmen ab 500 Beschäftigten kann bei einer fünfprozentigen Irrtumswahrscheinlichkeit nicht ausgeschlossen werden, dass dieser zufällig zustande gekommen ist.

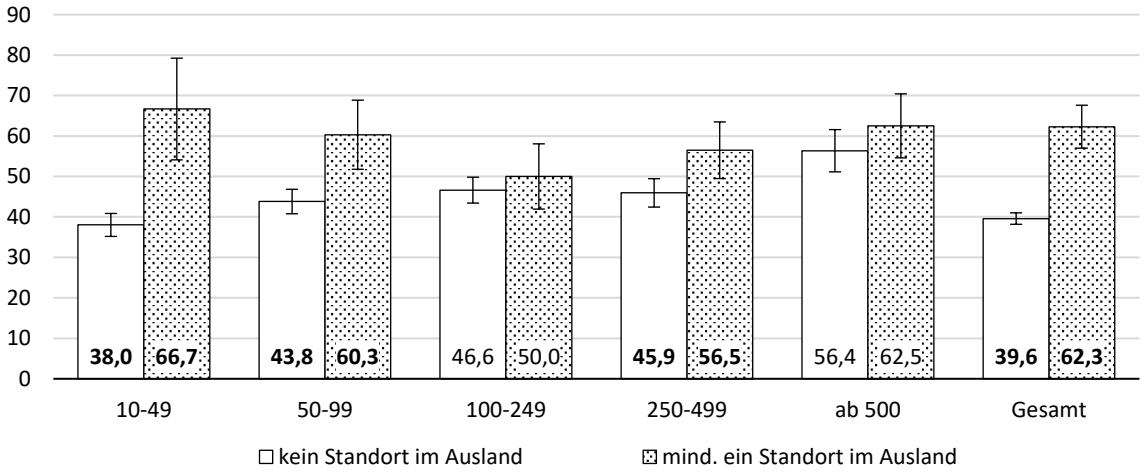
[280] Siehe Abschnitt 7.1.1.

Abbildung 42 **Jahresprävalenz insg. nach Anzahl der Standorte in Dtl. und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



Daneben ist zu erkennen, dass sich die Prävalenzraten der Unternehmen mit mindestens zwei Standorten in Deutschland hinsichtlich ihrer Beschäftigtengrößenklasse mit Ausnahme der Großunternehmen (ab 500 Besch.) nicht signifikant unterscheiden. D.h., mit der Anzahl der Standorte kann ein Teil des Zusammenhangs zwischen Unternehmensgröße und Prävalenzrate erklärt werden.

Abbildung 43 **Jahresprävalenz insg. nach Auslandsstandort und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



Bezogen auf das Vorhandensein mindestens eines Standortes im Ausland lässt sich ebenfalls ein Zusammenhang zur Jahresprävalenz erkennen. Unternehmen mit mindestens einem Auslandsstandort waren deutlich häufiger von Cyberangriffen in den letzten zwölf Monaten betroffen (62,3 %; N=321) als Unternehmen ohne Standorte im Ausland (39,6 %; N=4.609). Dies trifft tendenziell auf alle Beschäftigtengrößenklassen (Abbildung 43), am deutlichsten aber auf die kleinen Unternehmen zu (10-49 Besch.: 66,7 % vs. 38,0 %; N=54 bzw. 1.123).

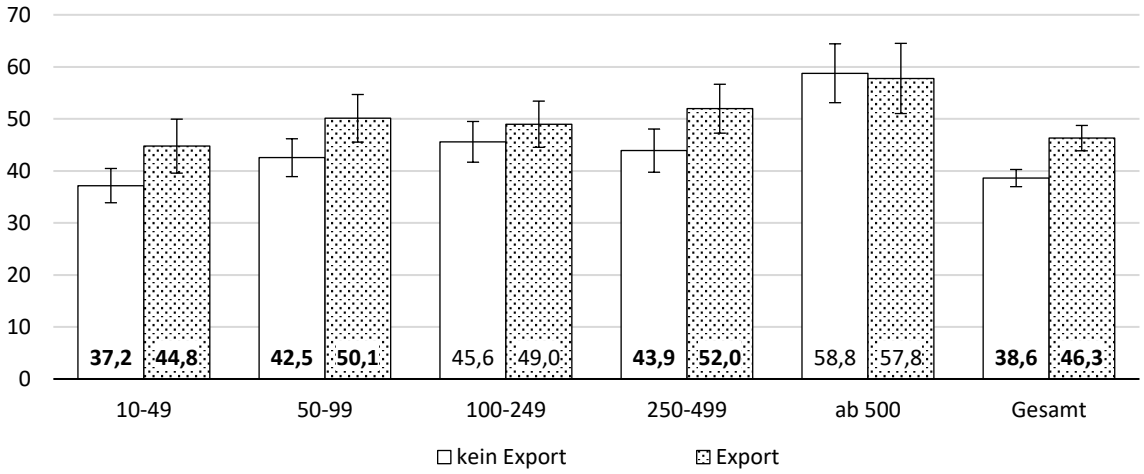
Die Prävalenzunterschiede in der Gruppe der Unternehmen mit Auslandsstandort(en) nach Beschäftigtengrößenklasse, sind statistisch gesehen nicht mehr bedeutsam. D.h., auch über das Vorhandensein mindestens eines Auslandsstandortes können Prävalenzunterschiede zwischen den Beschäftigtengrößenklassen erklärt werden.

8.2 Exporttätigkeit

Die Exporttätigkeit könnte sich ebenfalls auf das Risiko von Cyberangriffen auswirken, weil damit eine höhere internationale Vernetzung und Sichtbarkeit verbunden sein dürfte.

Insgesamt betrachtet zeigt sich der erwartete Unterschied bei der Jahresprävalenz zwischen Unternehmen, die Produkte oder Dienstleistungen ins Ausland exportieren (46,3 %; N=1.607) und Unternehmen, die dies nicht tun (38,6 %; N=3.343). Im Vergleich zu den Differenzen beim Auslandsstandort fällt dieser Unterschied nicht so deutlich aus (Abbildung 44), ist aber mit einer Ausnahme bei den kleinen und mittleren Unternehmen signifikant (bei Unternehmen mit 100 bis 249 Beschäftigten lässt sich dies nicht mit der nötigen Sicherheit sagen). Bei großen Unternehmen scheint sich die Exporttätigkeit hingegen nicht auf die Betroffenheit durch Cyberangriffe auszuwirken.

Abbildung 44 **Jahresprävalenz insg. nach Exporttätigkeit und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)

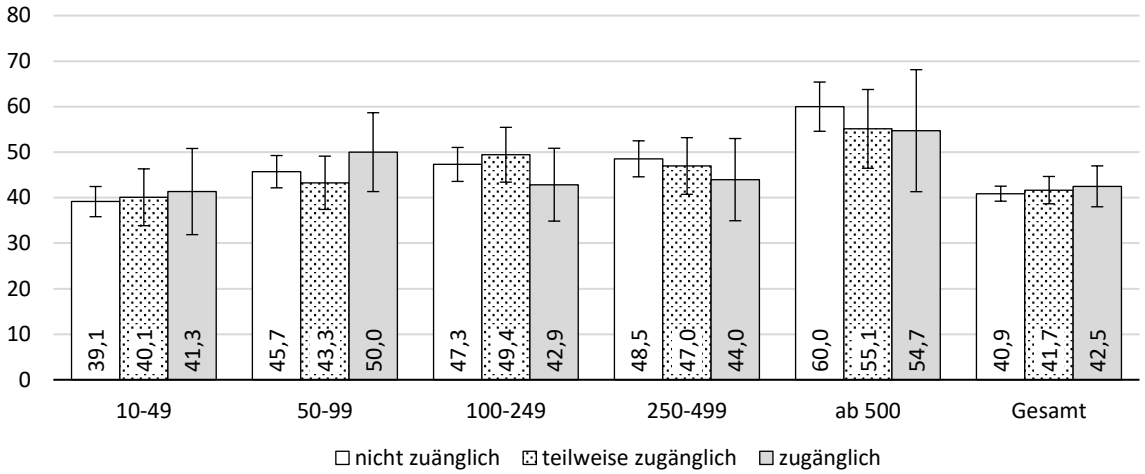


Die Prävalenzraten der exportierenden Unternehmen steigen ähnlich der nicht exportierenden mit zunehmender Unternehmensgröße an, was darauf hinweist, dass die Exporttätigkeiten für die Erklärung der Prävalenzunterschiede zwischen den Beschäftigtengrößenklassen weniger geeignet zu sein scheinen.

8.3 Öffentlich zugängliche Informationen zu Beschäftigten

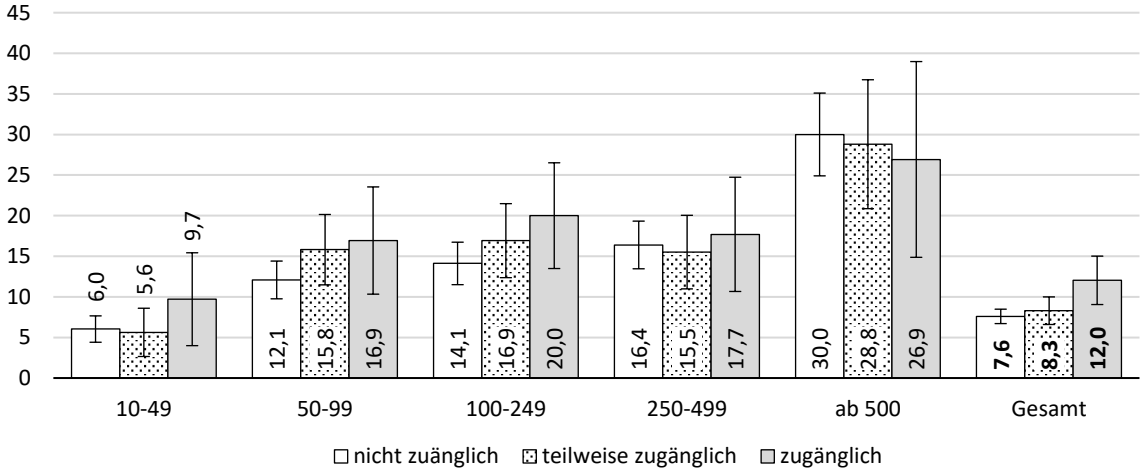
Die Veröffentlichung von detaillierten Zuständigkeiten, Kontakte und Stellenbeschreibungen der Beschäftigten könnte ebenfalls im Zusammenhang mit einer höheren Betroffenheit von Cyberangriffen in den letzten zwölf Monaten stehen, da diese Informationen möglicherweise für Cyberangriffe insbesondere im Bereich Social Engineering (z.B. CEO-Fraud) ausgenutzt werden könnten.

Abbildung 45 **Jahresprävalenz insg. nach öffentl. zugängl. Informationen im Internet und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



In Hinblick auf die Prävalenzrate für Cyberangriffe insgesamt sind zunächst weder einheitliche Tendenzen noch statistisch signifikante Unterschiede zwischen den Unternehmen zu erkennen, die entsprechende Informationen online veröffentlichen, die dies teilweise und die dies gar nicht tun (Abbildung 45). Bezieht man diese Unterscheidung auf die Jahresprävalenz für die Cyberangriffsart CEO-Fraud, dann wird der erwartete Zusammenhang erkennbar (Abbildung 46). Insgesamt betrachtet waren Unternehmen, die Unternehmensinformationen zu den Beschäftigten im Internet veröffentlichten signifikant häufiger von CEO-Fraud betroffen (12,0 %; N=457) als Unternehmen, bei denen solche Informationen nur teilweise (8,3 %; N=1.013) oder nicht zugänglich waren (7,6 %; N=3.410). Unter Kontrolle der Beschäftigtengrößenklasse ist dieser Zusammenhang lediglich tendenziell zu erkennen, was daran liegen mag, dass die Fallzahlen der zusätzlich differenzierten Vergleichsgruppen relativ klein sind.

Abbildung 46 **Jahresprävalenz für CEO-Fraud nach öffentl. zugängl. Info. im Internet und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



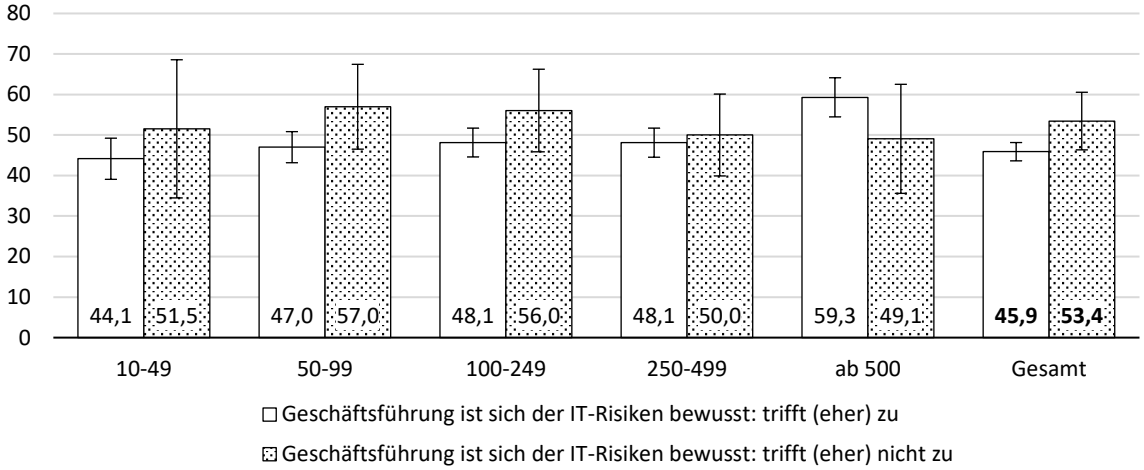
Dass die Prävalenzen in allen drei Gruppen tendenziell mit zunehmender Beschäftigtengröße ansteigen, ist ein Hinweis darauf, dass die Verfügbarkeit von bestimmten Unternehmensinformationen im Internet keine Erklärung für die unterschiedlichen Prävalenzraten der Beschäftigtengrößenklassen bietet.

8.4 Risikobewusstsein innerhalb des Unternehmens

Ob das Bewusstsein für IT-Risiken innerhalb des Unternehmens vorhanden ist, wurde lediglich über die Einschätzung der befragten Unternehmensvertreter*innen erhoben und ist insofern subjektiv geprägt. Wie bereits oben dargestellt, hängt diese Einschätzung mit der Position zusammen, die die Befragten innerhalb der Unternehmen innehatten.[281] Daher werden für den Vergleich der Jahresprävalenz für Cyberangriffe insgesamt nach Einschätzung des Risikobewusstseins, lediglich auf die Aussagen der IT-Beschäftigten zurückgegriffen.[282]

Im Vergleich haben Unternehmen, deren Vertreter*innen aus dem IT-Bereich (eher) zustimmten, dass die Geschäftsführung sich der IT-Risiken bewusst ist und die Vorgaben einhält, eine niedrigere Prävalenzrate für Cyberangriffe insgesamt (45,9 %; N=1.868) als Unternehmen, deren Vertreter*innen dem (eher) nicht zustimmten (53,4 %; N=189; Abbildung 47). Dies trifft tendenziell auf alle Beschäftigtengrößenklassen, bis auf die großen Unternehmen (ab 500 Besch.), zu, bei denen sich ein gegenläufiger aber nicht signifikanter Zusammenhang zeigt. Dieser könnte zufällig zustande gekommen sein oder mit anderen Variablen zusammenhängen, die bei großen Unternehmen entscheidender sind.

Abbildung 47 **Jahresprävalenz insg. nach Risikobewusstsein der Geschf. und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test); nur Antworten von IT-Besch.



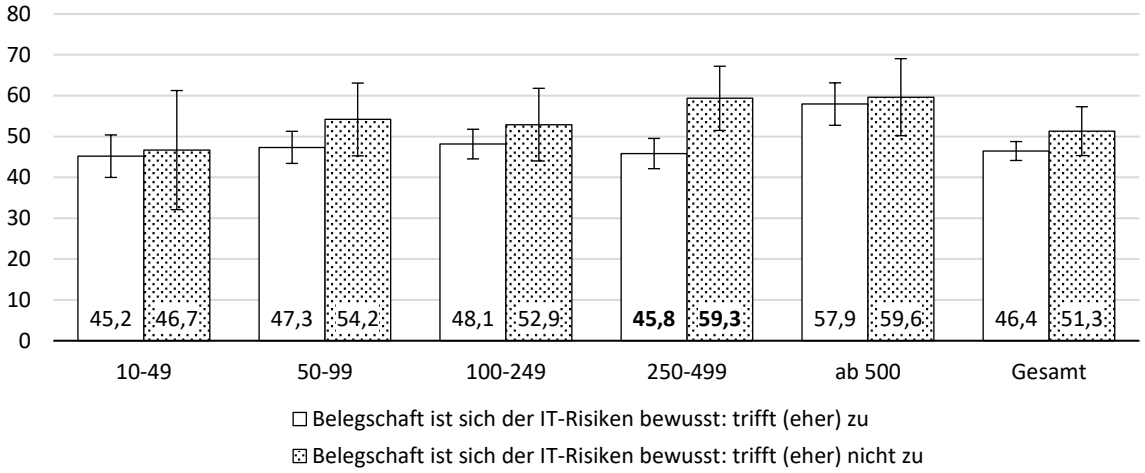
Daneben ist zu erkennen, dass sich die Prävalenzunterschiede zwischen den Beschäftigtengrößenklassen sowohl innerhalb der Unternehmen mit (eher) risikobewusster Geschäftsführung als auch innerhalb der Unternehmen mit (eher) risikounbewusster Geschäftsführung nivellieren. Das ist ein Hinweis darauf, dass auch dieses Merkmal zur Erklärung der Prävalenzunterschiede zwischen den Beschäftigtengrößenklassen dienen kann. D.h., wenn sich die Geschäftsführung der IT-Risiken nicht bewusst ist, scheint die Größe des Unternehmens kaum eine Rolle zu spielen, denn das Risiko ist in allen Beschäftigtengrößenklassen ähnlich hoch. Ist sich die Geschäftsführung der Risiken bewusst, scheint das Risiko von Cyberangriffen zumindest zwischen kleinen und mittleren Unternehmen gleich zu sein. Lediglich große Unternehmen heben

[281] Siehe Abschnitt 6.1.

[282] Dies wird dadurch begründet, dass die IT-Beschäftigten die größte Gruppe der interviewten Personen darstellen.

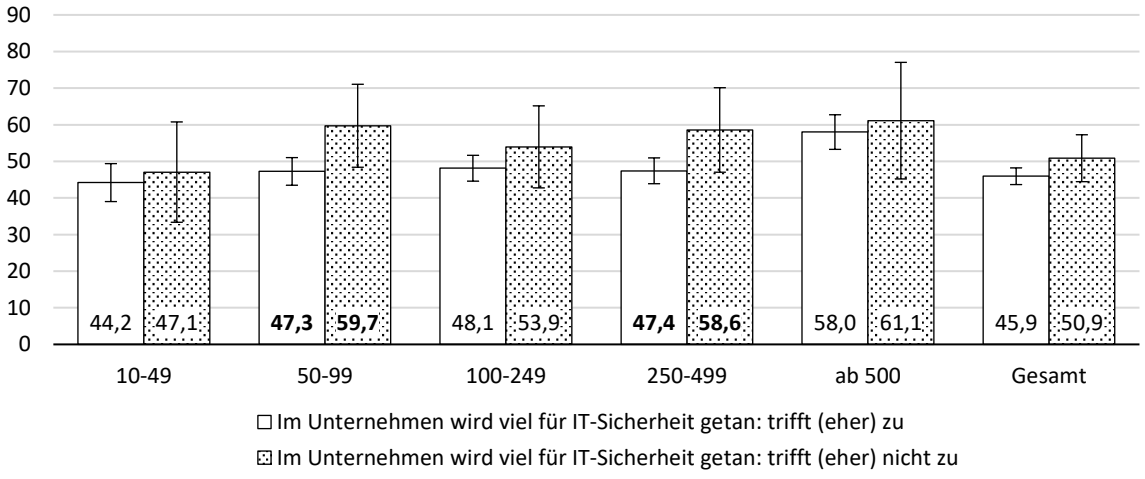
sich in dieser Gruppe deutlich ab. Möglicherweise ist in großen Unternehmen das Risikobewusstsein der Geschäftsführung unabhängiger von weiteren Faktoren, die eine Rolle bezüglich des Risikos spielen.

Abbildung 48 **Jahresprävalenz insg. nach Risikobewusstsein der Belegschaft und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test); nur Antworten von IT-Besch.



Beim Vergleich der Jahresprävalenzraten für Cyberangriffe insgesamt hinsichtlich der Einschätzung der befragten IT-Beschäftigten zum Risikobewusstsein der Belegschaft ist zumindest eine einheitliche Tendenz zu erkennen (Abbildung 48): Unternehmen, in denen der Aussage, dass die Belegschaft sich der IT-Risiken bewusst ist und sie die Vorgaben einhält, (eher) zugestimmt wurde, sind anteilig seltener betroffen als Unternehmen, in denen dem (eher) nicht zugestimmt wurde. Statistisch signifikant ist der Zusammenhang lediglich bei Unternehmen mit 250-499 Beschäftigten. Ein Hinweis darauf, dass das Risikobewusstsein der Belegschaft nicht zur Erklärung der Prävalenzunterschiede zwischen den Beschäftigtengrößenklassen geeignet ist, zeigt sich an den weiterhin tendenziell mit zunehmender Beschäftigtenzahl ansteigenden Prävalenzraten in beiden Vergleichsgruppen.

Abbildung 49 **Jahresprävalenz insg. nach Risikobewusstsein der Belegschaft und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test); nur Antworten von IT-Besch.



Ein ähnliches Bild ergibt sich bezüglich der Einschätzungen zu der Aussage, dass im Unternehmen viel für die IT-Sicherheit getan wird. Unternehmen, deren befragte Vertreter*innen aus

dem IT-Bereich (eher) zustimmten, waren zumindest tendenziell weniger durch Cyberangriffe insg. belastet als Unternehmen, deren Vertreter*innen (eher) nicht zustimmten (Abbildung 49). Statistisch signifikante Unterschiede sind diesbezüglich bei Unternehmen mit 50 bis 99 sowie mit 250-499 Beschäftigten zu sehen (47,3 % vs. 59,7 % bzw. 47,4 % vs. 58,6 %).

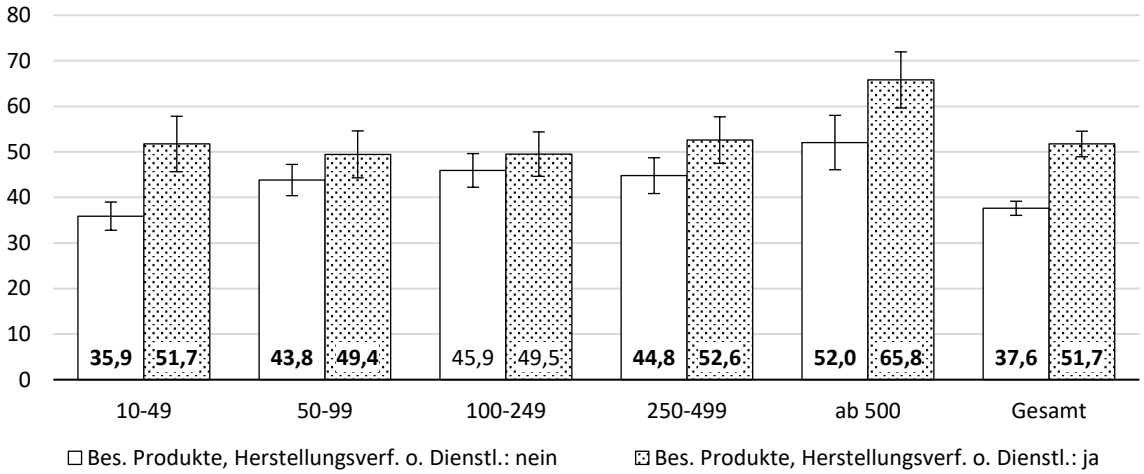
In der Gruppe der Unternehmen, in denen (eher) nicht viel für die IT-Sicherheit getan wird, unterscheiden sich die Prävalenzraten der einzelnen Beschäftigtengrößenklassen nicht mehr signifikant, was allerding mit der geringen Fallzahl in diesen Klassen zusammenhängen könnte, zumal die Prozentsatzdifferenz zwischen den kleinen und großen Unternehmen immerhin noch 13 Prozentpunkte beträgt. Zur Erklärung der Prävalenzunterschiede zwischen den Beschäftigtengrößenklassen scheint dieses Merkmal daher weniger geeignet zu sein.

8.5 Potentielle Angriffsziele

8.5.1 Besondere Produkte, Herstellungsverfahren oder Dienstleistungen

Insofern ein Teil der Cyberangriffe gezielt auf bestimmte Unternehmen oder Branchen erfolgt, ist ein höheres Risiko für Unternehmen mit potentiellen Zielen wie besondere Produkten, Herstellungsverfahren oder Dienstleistungen anzunehmen.[283]

Abbildung 50 **Jahresprävalenz insg. nach potentiellen Zielen (bes. Produkten etc.) und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



Ein Vergleich der Jahresprävalenz für Cyberangriffe insgesamt von Unternehmen ohne und mit solchen Besonderheiten kann diese Annahme bekräftigen (Abbildung 50). Unternehmen, die die Frage nach besonderen Produkten etc. bejahten, waren signifikant häufiger von Cyberangriffen betroffen (51,7 %; N=1.212) als Unternehmen, die diese Frage verneinten (37,6 %; N=3.743). Mit einer Ausnahme (Unternehmen mit 100-249 Besch.) bestätigt sich dieses Ergebnis auch in den jeweiligen Beschäftigtengrößenklassen.

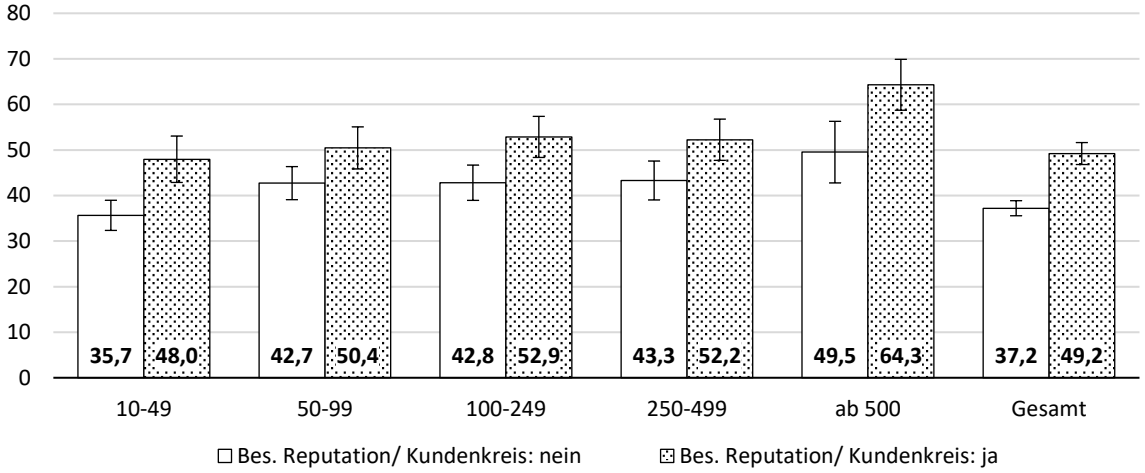
8.5.2 Besondere Reputation oder Kundenkreis

Als weiteres potentielles Ziel für Angreifer*innen wurde nach einer besonderen Reputation oder einem besonderen Kundenkreis gefragt. Hierbei zeigt sich ebenfalls ein eindeutiges Bild

[283] Die Einschätzung der „Besonderheit“ oblag den Befragten selber (siehe Abschnitt 6.3).

(Abbildung 51): Unternehmen, die diese Frage bejahten, d.h., die nach eigener Einschätzung über eine besondere Reputation bzw. Kundenkreis verfügen, waren signifikant häufiger von Cyberangriffen in den letzten zwölf Monaten betroffen (49,2 %; N=49,2 %) als diejenigen, die diese Frage verneinten (37,2 %; N=3.276). Dieses Ergebnis bleibt auch unter Kontrolle der Beschäftigtengrößenklasse in allen Klassen erhalten.

Abbildung 51 **Jahresprävalenz insg. nach potentiellen Zielen (bes. Reputation etc.) und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



In beiden Gruppen, die besondere Produkte etc. bzw. eine besondere Reputation haben nivelliert sich der Prävalenzunterschied zwischen den kleinen und mittleren Unternehmen. D.h., das Vorhandensein dieser potentiellen Angriffsziele kann einen Beitrag zur Erklärung des Prävalenzunterschiedes zwischen den Beschäftigtengrößenklassen leisten.

8.6 Unternehmen der Daseinsvorsorge

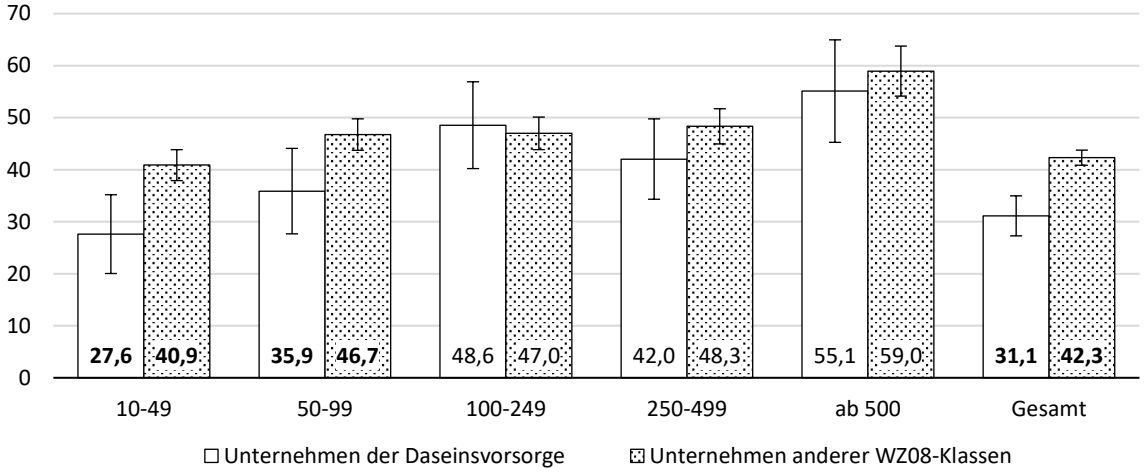
Die Gruppe der Unternehmen der Daseinsvorsorge[284] könnte ebenfalls ein besonderes Ziel für Cyberangriffe darstellen, da deren Schädigung ein weitreichenderes Ausmaß und schnell spürbare Konsequenzen für die Bevölkerung (bspw. für die Patient*innen eines Krankenhauses)[285] haben kann. Dies könnte von potentiellen Täter*innen z.B. im Zusammenhang mit einer Erpressung ausgenutzt werden. Vor diesem Hintergrund sollten entsprechende Unternehmen besonders vor Cyberangriffen geschützt sein. Zwar bestätigte sich dies lediglich in Hinblick auf drei organisatorische IT-Sicherheitsmaßnahmen (Zertifizierung der IT-Sicherheit, Schulungen zur IT-Sicherheit für Beschäftigten, Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme), die bei Unternehmen der Daseinsvorsorge anteilig häufiger vorhanden waren als bei Unternehmen der übrigen WZ08-Klassen (Abbildung 15 und Abbildung 22), dennoch könnte bereits damit ein höherer Schutz verbunden sein, der sich auf die Prävalenzrate auswirkt.

[284] Siehe dazu Fn. 194 sowie Tabelle 4 in Abschnitt 3.4.1. Eine Auflistung aller dazugehörigen WZ-Klassen findet sich in Tabelle 43 im Anhang 1.

[285] So berichtete die Süddeutsche Zeitung (Online) am 17.07.2019 von 13 Krankenhäusern, die von einem Ransomware-Angriff betroffen waren: https://www.sueddeutsche.de/digital/krankenhaeuser-schadsoftware-ransomware-virus-drk-1.4529406 (zuletzt geprüft am 02.09.2019). Siehe dazu auch Bundesamt für Sicherheit in der Informationstechnik (2019c).

Beim Vergleich der vorhandenen IT-Sicherheitsmaßnahmen zwischen Unternehmen der Daseinsvorsorge und Unternehmen anderer WZ08-Klassen zeigt sich dieser vermutete Zusammenhang zumindest teilweise.

Abbildung 52 **Jahresprävalenz insg. nach Zugehörigkeit zur Daseinsvorsorge**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



Unabhängig von der Beschäftigtengrößenklasse liegt der Anteil der im Vorjahr von mindestens einem Cyberangriff betroffenen Unternehmen in der Gruppe der Daseinsvorsorge-Unternehmen signifikant um ca. elf Prozentpunkte unter dem Anteil von Unternehmen der übrigen WZ08-Klassen (31,1 % vs. 42,3 %; N=556 bzw. 4.425; Abbildung 52). Differenziert nach Beschäftigtengrößenklasse trifft dies insbesondere auf kleinere Unternehmen (10-49 und 50-99 Besch.) zu.

8.7 Zwischenresümee

Zusammenfassend lässt sich nach diesen Merkmalsgruppenvergleichen festhalten, dass es neben der Unternehmensgröße und der Branche weitere Merkmale gibt, die mit dem Risiko von Cyberangriffen in Zusammenhang stehen. Ob eines dieser Merkmale entscheidender ist als andere, lässt sich im Rahmen dieser Analyse nicht bestimmen. Dazu bedarf es weiterer multivariater Analysen, deren Ergebnisse an anderer Stelle veröffentlicht werden. Dennoch fallen bereits hier besonders deutliche Prävalenzunterschiede hinsichtlich der Anzahl der Standorte in Deutschland, des Vorhandenseins eines Auslandstandortes, der Exporttätigkeit und des Vorhandensein potentieller Ziele für Angreifer, z.B. besondere Produkte/ Herstellungsverfahren/ Dienstleistungen oder besondere Reputation/ Kundenkreis, auf. Unternehmen mit mehreren Standorten im Inland, mindestens einem Standort im Ausland, die im Exportgeschäft tätig sind oder die besondere Produkte etc. anbieten bzw. über eine besondere Reputation/ Kundenkreis verfügen, waren unabhängig von ihrer Größe signifikant häufiger von Cyberangriffen betroffen als Unternehmen ohne diese Merkmale. Insbesondere kleine Unternehmen der Daseinsvorsorge (10-99 Besch.) waren deutlich seltener von Cyberangriffen betroffen als Unternehmen anderer Branchen, was auf einen höheren Schutz der Daseinsvorsorge-Unternehmen hinweist.

Weniger eindeutig sind die Ergebnisse bezogen auf die Verfügbarkeit von Informationen zu den Beschäftigten (z.B. detaillierte Zuständigkeiten, Kontakte, Stellenbeschreibungen) sowie

bezüglich des Risikobewusstseins innerhalb der Unternehmen. Letzteres wurde über die subjektive Einschätzung eines/r Unternehmensvertreters*in erhoben und könnte dadurch verzerrt sein.

Allerdings scheint insbesondere das Risikobewusstsein der Geschäftsführung eine bedeutende Rolle bei der Erklärung der Prävalenzunterschiede zwischen den Unternehmen unterschiedlicher Beschäftigtengrößenklassen zu spielen, da sich unter Kontrolle des eingeschätzten Risikobewusstseins der Geschäftsführung diese Unterschiede weitgehend ausgleichen. Die Jahresprävalenzraten für Cyberangriffe insgesamt unterscheiden sich bei Unternehmen mit mehreren Standorten in Deutschland oder mit mindestens einem Auslandsstandort ebenfalls nicht mehr signifikant zwischen den Beschäftigtengrößenklassen, womit diese Merkmale ebenfalls einen Beitrag zur Erklärung dieses oben berichteten Unterschiedes zu leisten scheinen.

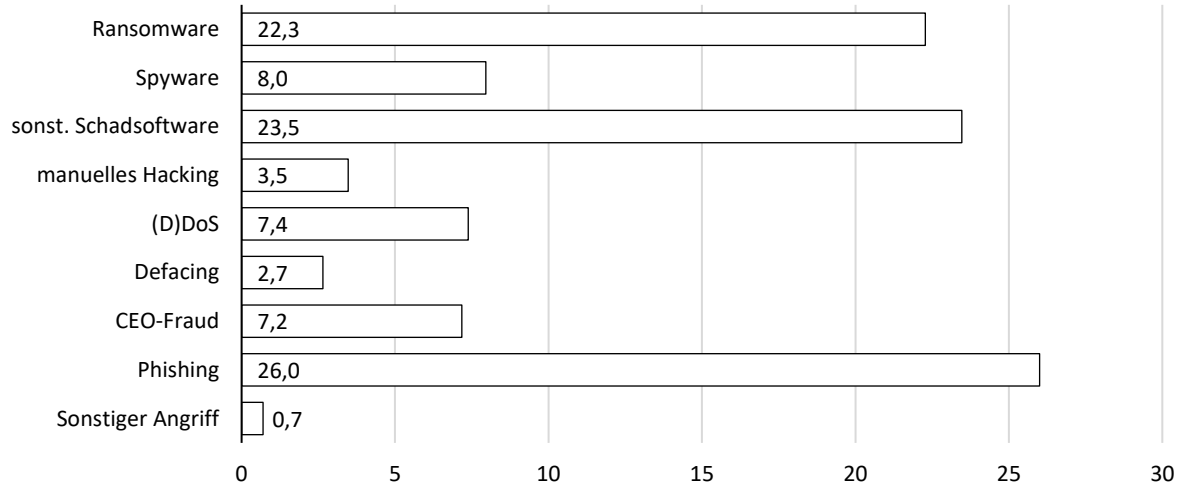
9 SCHWERWIEGENDSTER ANGRIFF

Da aufgrund der beschränkten Interviewdauer nicht jeder von den Unternehmen erlebte Cyberangriff detailliert erhoben werden konnten, sollten sich die in den vorangegangenen zwölf Monaten betroffenen Unternehmen bei der Beantwortung der Detailfragen nur auf den schwerwiegendsten Cyberangriff konzentrieren. Wie schwerwiegend diese Angriffe waren, bleibt dabei erst einmal offen, kann jedoch durch die Beurteilung der berichteten Schäden geschätzt werden. Wurde nur ein Angriff erlebt, gilt dieser als schwerwiegendster.

9.1 Angriffsart

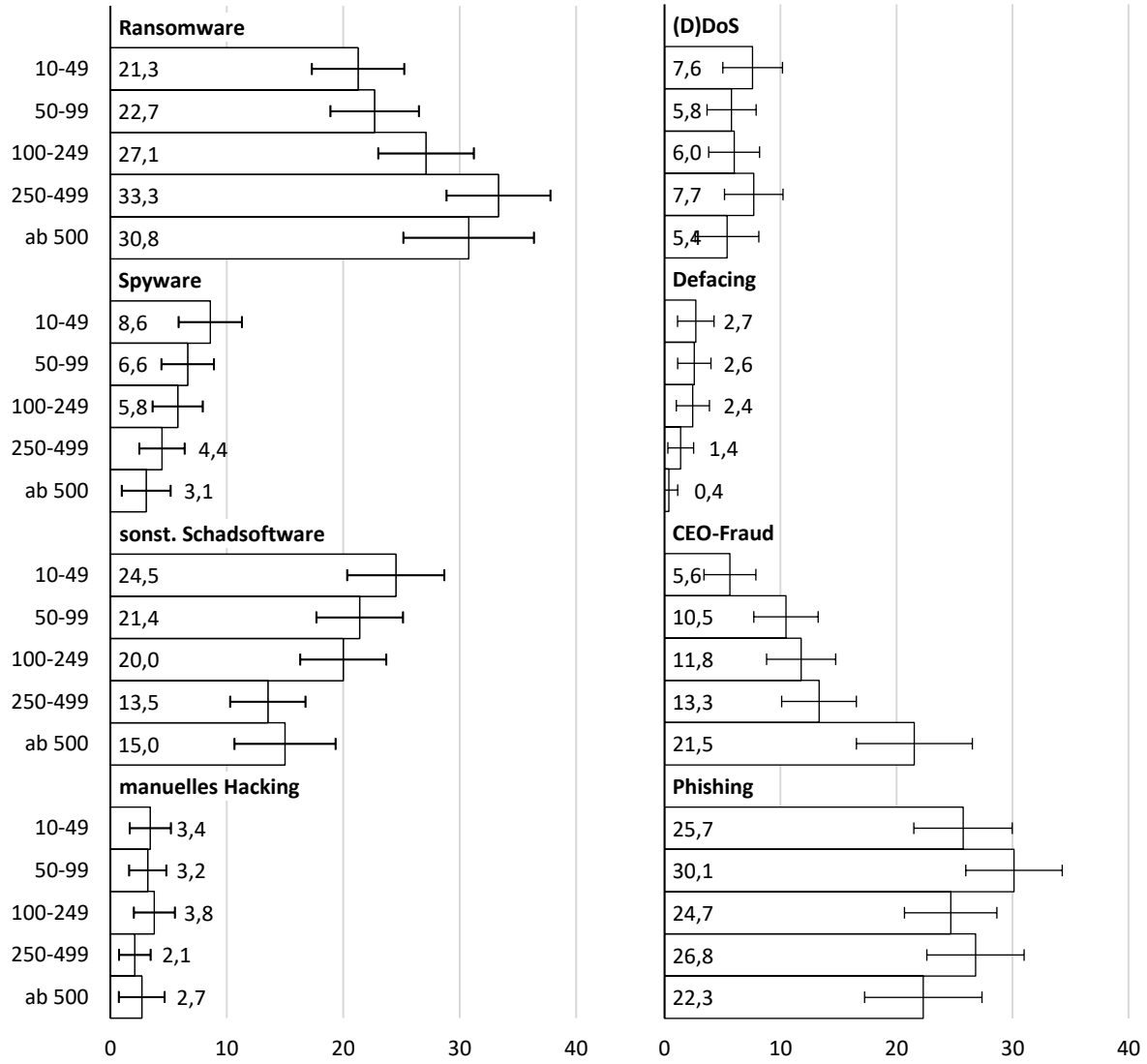
Zu den Angriffsarten, die bezogen auf den schwerwiegendsten Cyberangriff der vorangegangen zwölf Monate am häufigsten genannt wurden (Abbildung 53), zählen Phishing (26,0 %), Ransomware (22,3 %) und sonstige Schadsoftware (23,4 %). Deutlich seltener wurden Spyware (8,0 %), (D)DoS (7,4 %) und CEO-Fraud (7,2 %) genannt, gefolgt von manuellem Hacking (3,5 %), Defacing (2,7 %) und sonstigen Cyberangriffen (0,7 %).[286] Die Frage, ob dieser Angriff im Vorhinein angedroht wurde, bejahte lediglich ein sehr kleiner Anteil von 0,4 % (N=1.787).

Abbildung 53 **Schwerwiegendster Cyberangriff nach Angriffsart**
in Prozent; gewichtete Daten; Mehrfachantwort möglich; N=1.787



[286] Genannt wurde hier insbesondere illegales Krypto-Mining, wobei unklar bleibt, ob andere Unternehmen den Einsatz von Krypto-Malware unter sonstige Schadsoftware subsumiert haben.

Abbildung 54 **Schwerwiegendster Angriff der letzten zwölf Monate nach Angriffsart und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI; Mehrfachantworten möglich



Beim Vergleich der von den Unternehmen am schwerwiegendsten bewerteten Angriffe nach Angriffsart und Beschäftigtengrößenklassen gibt es zum Teil deutliche Unterschiede (Abbildung 54): Ransomware-Angriffe werden signifikant häufiger von größeren Unternehmen im Zusammenhang mit dem schwerwiegendsten Angriff genannt (250-499 Besch.: 33,3 %; ab 500 Besch.: 30,8 %) als von kleinen (10-49 Besch.: 21,3 %). Kleine Unternehmen nennen hingegen sonstige Schadsoftware signifikant häufiger (10-49 Besch.: 24,5 %) als größere Unternehmen (250-499 Besch.: 13,5 %; ab 500 Besch.: 15,0 %). Weitere statistisch relevante Unterschiede finden sich bei Spyware und CEO-Fraud: Während Spyware bei kleinen Unternehmen signifikant häufiger zum schwerwiegendsten Ereignis führte (10-49 Besch.: 8,6 %) als bei großen Unternehmen (ab 500 Besch.: 3,1 %), wurde CEO-Fraud deutlich häufiger von großen Unternehmen (ab 500 Besch.: 21,5 %) angegeben als von kleineren, wobei sich die mittleren Beschäftigtengrößenklassen (50-99 Besch.: 10,5 %; 100-249 Besch.: 11,8 %; 250-499 Besch.: 13,3 %) ebenfalls signifikant von den kleinen Unternehmen (10-49 Besch.: 5,6 %) unterscheiden. Bei den übrigen Angriffsarten finden sich keine statistisch relevanten Unterschiede zwischen den Beschäftigtengrößenklassen und mit Ausnahme von Phishing wurden diese vergleichsweise selten im Zusammenhang mit dem schwerwiegendsten

Cyberangriff genannt. Phishing ist dagegen nicht nur eine der am häufigsten verbreiteten Angriffsarten (siehe Abbildung 36 und Abbildung 37), sondern wird in vielen Fällen auch als am schwerwiegendsten erlebte Angriffsart der letzten zwölf Monate angegeben.

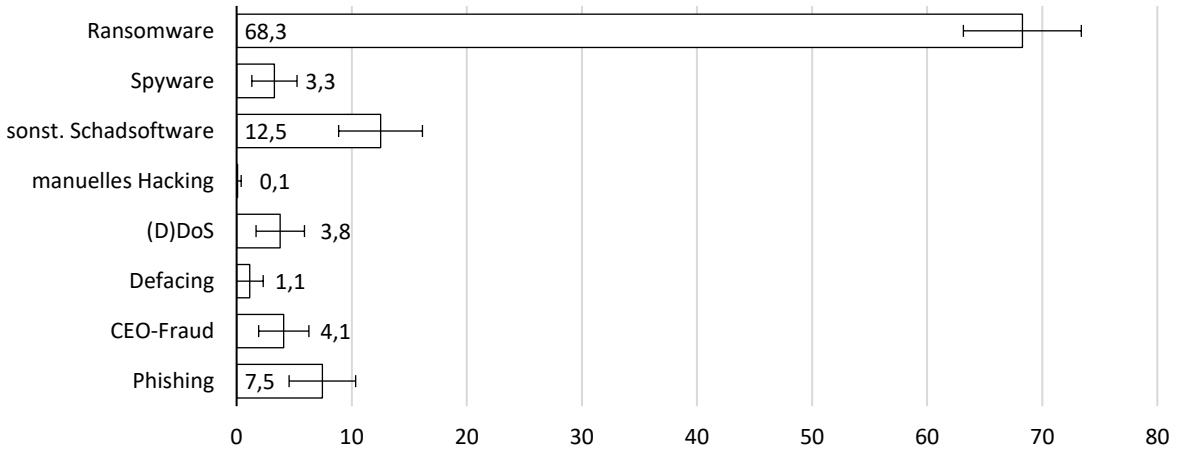
9.2 Vermutungen zu den Täter*innen

Die Angaben zu den vermuteten Täter*innen, die hinter der schwerwiegendsten Tat stecken, sind nicht besonders belastbar. Dies zeigt sich vor allem darin, dass nur jedes dritte betroffene Unternehmen (30,7 %, N=1.787) überhaupt eine entsprechende Vermutung äußerte. Davon gaben 4,4 % (N=532) an, dass der*die Täter*innen mutmaßlich aus dem Kreis der ehemaligen oder aktiven Beschäftigten stammt. Ein Anteil von 1,8 % vermutet Geschäftspartner (z.B. Dienstleister, Lieferanten) hinter der Tat, 6,1 % Mitbewerber*innen und 92,4 % andere Außenstehende.[287] Zusammengefasst geben nur 6,1 % der Unternehmen mit Vermutungen zum Täter*innenkreis an, dass es sich bezogen auf den schwerwiegendsten Cyberangriff mutmaßlich um Innentäter*innen (ehemalige/ aktive Beschäftigte oder Geschäftspartner) handelt. Statistisch bedeutsame Unterschiede zwischen den Beschäftigtengrößenklassen, den Branchen oder zwischen den Angriffsarten lassen sich hierbei auch aufgrund der geringen Fallzahl nicht erkennen. Tendenziell gehen große Unternehmen (ab 500 Besch.: 11,5 %, N=78) häufiger von Innentäter*innen aus als kleine (10-49 Besch.: 4,8 %, N=124).

9.3 Lösegeldforderung

In 18,2 % (N=1.744) der berichteten schwerwiegendsten Cyberangriffe wurde von den Täter*innen Lösegeld gefordert. Diesen Forderungen sind 2,3 % (N=317) der so betroffenen Unternehmen nachgekommen, woraufhin in sechs von sieben Fällen die Täter*innen ihre damit verbundenen Versprechungen (z.B. Datenentschlüsselung bzw. Beenden des Angriffs) eingehalten haben.

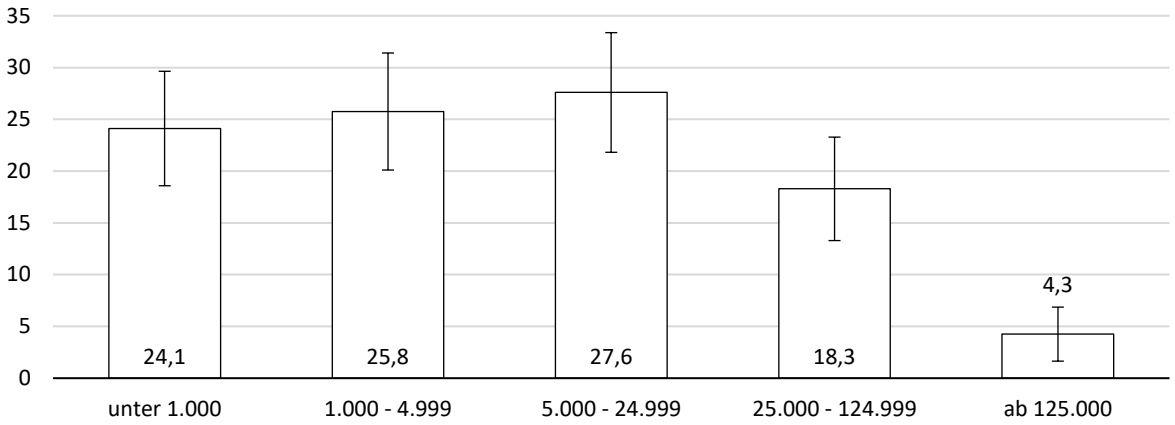
Abbildung 55 **Cyberangriffe mit Lösegeldforderung nach Angriffsarten**
in Prozent; gewichtete Daten; 95%-KI; Mehrfachantworten mögl.; N=317



[287] Mehrfachantworten waren möglich. Befunde zu Täter*innen von Cyberangriffen allgemein finden sich z.B. bei Huber et al. (2018); Huber & Pospisil (2018).

Erwartungsgemäß sind Ransomware-Angriffe unter den mit Lösegeldforderungen verbundenen Cyberangriffen mit 68,7 % am häufigsten zu finden (Abbildung 55). Angriffe mit sonstiger Schadsoftware sind mit 12,5 % und Phishing mit 7,5 % vertreten. Die Anteile der übrigen Angriffsarten befinden sich im unteren einstelligen Bereich (z.B. CEO-Fraud: 4,1 %, (D)DoS: 3,8 % und Spyware: 3,3 %).

Abbildung 56 **Höhe der Lösegeldforderung in EUR (klassiert)**
in Prozent; gewichtete Daten; 95%-KI; N=230



Die Höhe der Lösegeldforderungen bewegt sich in einer sehr großen Spannweite von 100 EUR bis 100 Mio. EUR, wobei die Hälfte der berichteten Forderungen (Median) unter 4.800 EUR und die andere Hälfte darüber lag (N=230).[288] In Abbildung 56 ist eine klassierte Verteilung der Lösegeldforderungen dargestellt: Bei etwa einem Viertel lag die Höhe des Lösegeldes unter 1.000 EUR (24,1 %), bei einem weiteren Viertel zwischen 1.000 und 4.999 EUR (25,8 %). Bei etwas über einem Viertel lag die Forderung zwischen 5.000 und 24.999 EUR (27,6 %), bei knapp einem Fünftel zwischen 25.000 und 124.999 EUR (18,3 %) und bei einem kleinen Anteil von 4,3 % bei 125.000 EUR und mehr.[289]

9.4 Infektionsweg

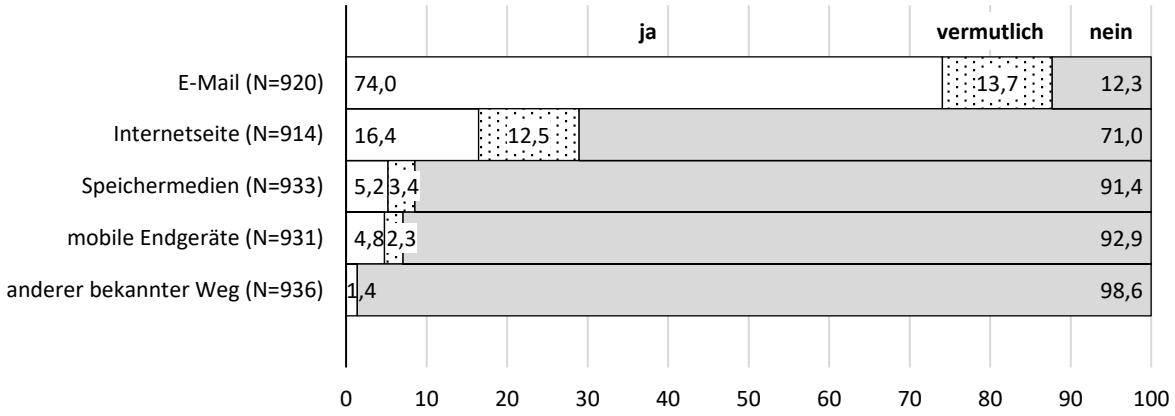
Die Unternehmen, die einen Angriff durch Ransomware, Spyware oder sonstige Schadsoftware (im Folgenden zusammengefasst mit Malware-Angriff) als schwerwiegendsten Cyberangriff der letzten zwölf Monate angegeben haben (N=954), wurden nach dem Weg der Infektion gefragt. Dabei konnten sie für verschiedene vorgegebene Wege angeben, ob dies (vermutlich) der Fall war oder nicht. Ein Anteil von 74,0 % gibt an, dass die Infektion über eine E-Mail erfolgte (N=920) und weitere 13,7 % vermuten dies. Etwa jedes achte Unternehmen (12,3 %) schließt diesen Infektionsweg aus (Abbildung 57). Schon deutlich seltener werden Malware-Infektionen über eine Internetseite (z.B. über aktive Inhalte oder Downloads) angegeben (ja: 16,4 %, vermutlich: 12,5 %). Am kleinesten sind die Anteile, die Speichermedien (z.B. USB-Sticks, SD-

[288] Über ein Viertel (27,4 %, N=317) der von Geldforderungen betroffenen Unternehmen konnte zur Höhe des Lösegeldes keine Angaben machen.

[289] Betrachtet man ausschließlich die Lösegeldforderungen bei Ransomware-Angriffen, sind die Klassen ähnlich besetzt (unter 1.000: 26,2 %, 1.000 – 4.999: 26,4 %, 5.000 – 24.999: 25,0 %, 25.000 – 124.999: 16,6 %, ab 125.000: 5,8 %). Der Median liegt allerdings etwas tiefer bei rund 2.100 EUR (N=146).

Cards, CDs) und mobile Endgeräte (z.B. Net-/Notebooks, Tablets, Smartphones) als Infektionsweg benennen bzw. vermuten (ja: 5,2 % bzw. 4,8 %, vermutlich: 3,4 % bzw. 2,3 %). Neun von zehn Unternehmen (91,4 % bzw. 92,9 %) schließen diese aus.

Abbildung 57 **Infektionsweg bei Malware-Angriffen**
in Prozent; gewichtete Daten

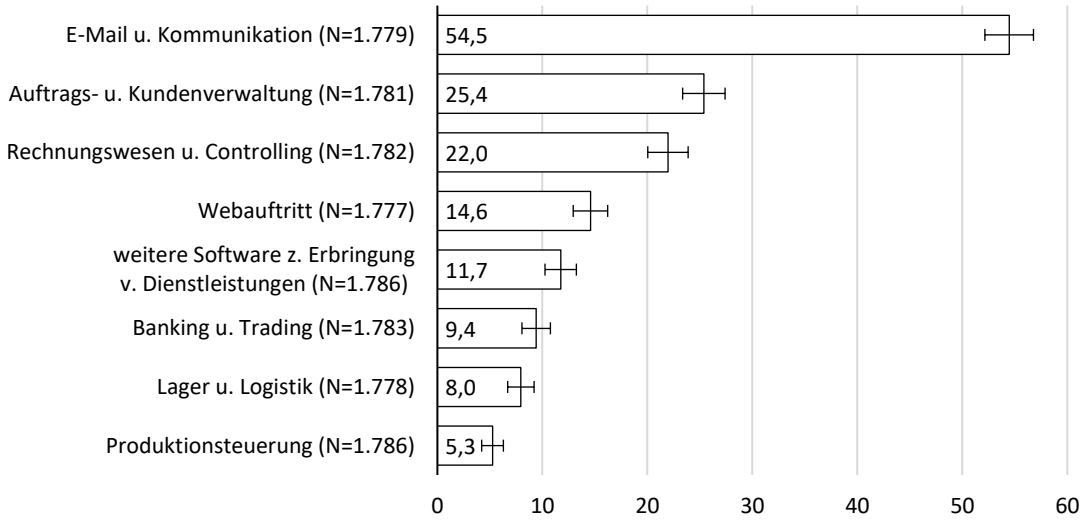


9.5 Folgen

9.5.1 Betroffene Systeme

Zu den drei am häufigsten genannten IT-Systemen, die vom schwerwiegendsten Angriff betroffen waren, d.h., die infolge nicht oder nur stark eingeschränkt genutzt werden konnten, zählen E-Mail und Kommunikation (54,5 %), Auftrags- und Kundenverwaltung (25,4 %) sowie Rechnungswesen und Controlling (22,0 %). Weniger häufig wurden der Webauftritt (14,6 %) und weitere Software zur Erbringung von Dienstleistungen (11,7 %) genannt und noch seltener waren die IT-Systeme im Bereich Banking und Trading (9,4 %), Lager und Logistik (8,0 %) sowie die Produktionssteuerung (5,3 %) betroffen (Abbildung 58).

Abbildung 58 **Vom schwerwiegendsten Cyberangriff betroffene IT-Systeme**
in Prozent; gewichtete Daten; 95%-KI; Mehrfachantworten möglich



Beim Vergleich zwischen den Beschäftigtengrößenklassen ist zu erkennen, dass zumindest tendenziell häufiger kleine Unternehmen vom Ausfall oder stark eingeschränkter Nutzbarkeit der verschiedenen IT-Systeme betroffen sind (Tabelle 26). Statistisch signifikant sind diese Unterschiede in Hinblick auf die IT-Systeme E-Mail und Kommunikation, Auftrags- und Kundenverwaltung sowie Webauftritt: Während z.B. bei über der Hälfte der kleinen Unternehmen (10-49 Besch.: 56,9 %) der E-Mail-Verkehr und die Kommunikation infolge des schwerwiegendsten Cyberangriffs gar nicht oder nur noch stark eingeschränkt funktioniert, trifft dies lediglich auf 37,7 % der großen Unternehmen (ab 500 Besch.) zu.

Tabelle 26 **Vom schwerwiegendsten Cyberangriff betroffene IT-Systeme nach Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; fett: signifikant bei p<.05 (Chi²-Test)

	Beschäftigtengrößenklasse				
IT-System	10-49	50-99	100-249	250-499	ab 500
E-Mail u. Kommunikation	**56,9**	**49,7**	**44,9**	**47,7**	**37,7**
Auftrags- u. Kundenverwaltung	**27,0**	**24,1**	**17,3**	**18,2**	**16,2**
Rechnungswesen u. Controlling	23,1	19,2	18,0	18,2	15,5
Webauftritt	**15,8**	**11,3**	**9,8**	**7,5**	**8,8**
weitere Software z. Erbringung v. Dienstleistungen	11,8	11,8	12,4	9,6	10,9
Banking u. Trading	9,8	9,0	7,6	8,9	6,9
Lager u. Logistik	8,1	8,8	7,3	5,6	5,4
Produktionssteuerung	5,4	4,9	6,2	4,2	2,7
N	407	465	449	427	260

Auch hinsichtlich der WZ08-Klassen sind z.T. deutliche Unterschiede zu erkennen (Tabelle 27). So gibt ein Anteil von 70,3 % des Gastgewerbes (WZ08-I) an, dass das IT-System E-Mail und Kommunikation vom schwerwiegendsten Angriff betroffen wurde und infolge ganz oder teilweise ausfiel. Ebenfalls höher als bei Unternehmen anderer WZ08-Klassen liegen beim Gastgewerbe die Anteile betroffener Auftrags- und Kundenverwaltungssysteme (39,7 %) und Webauftritte (34,9 %). IT-Systeme des Rechnungswesens und Controllings waren am häufigsten in Unternehmen des Gesundheits- und Sozialwesens (WZ08-Q: 35,4 %) sowie des Baugewerbes (WZ08-F: 32,5 %) betroffen. Weitere Software zur Erbringung von Dienstleistungen fiel vergleichsweise häufig im Unternehmensbereich Erziehung und Unterricht (WZ08-P: 20,5 %) und in freiberuflichen, wissenschaftlichen und technischen Dienstleistungen (WZ08-M: 18,7 %) aus. Banking- und Trading-Systeme fallen häufiger im Wirtschaftszweig WZ08-G (Handel; Instandhaltung und Reparatur von Kfz: 15,1 %), Lager und Logistik-Systeme im Wirtschaftszweig WZ08-H (Verkehr und Lagerei: 18,2 %) und Produktionssteuerungssysteme im Wirtschaftszweig WZ08-N (sonstige wirtschaftliche Dienstleistungen: 8,8 %) aus.[290]

[290] Eine weitere Differenzierung nach WZ-Klassen der zweiten Ebene ist aufgrund der geringen Fallzahl nicht sinnvoll.

Tabelle 27 **Vom schwerwiegendsten Cyberangriff betroffene IT-Systeme nach WZ08-Klassen**
in Prozent; gewichtete Daten

	Betroffenes IT-System								
WZ08-Klasse (Ebene 1)[291]	1	2	3	4	5	6	7	8	N
Verarbeitendes Gewerbe (WZ08-C)	52,6	22,3	18,5	6,7	6,7	6,2	8,7	7,2	389
Baugewerbe (WZ08-F)	55,9	30,1	32,5	12,1	15,0	10,6	7,2	7,2	206
Handel; Instandhaltung u. Reparatur v. Kraftfahrzeugen (WZ08-G)	56,0	29,3	28,7	17,2	10,4	**15,1**	17,1	5,3	376
Verkehr u. Lagerei (WZ08-H)	52,7	27,3	18,2	10,9	7,4	5,5	**18,2**	7,3	55
Gastgewerbe (WZ08-I)	**70,3**	**39,7**	15,6	34,9	4,8	9,4	1,6	4,8	64
Information u. Kommunikation (WZ08-J)	41,5	12,3	7,7	**33,8**	3,1	6,2	1,5	1,5	65
Freiberufl., wissenschaftl. u. techn. Dienstl. (WZ08-M)	55,6	22,5	17,1	15,8	18,7	3,2	2,7	3,2	187
Sonst. Wirtschaftl. Dienstl. (WZ08-N)	56,0	35,9	17,0	13,2	9,9	12,1	1,1	**8,8**	90
Erziehung u. Unterricht (WZ08-P)	57,0	25,6	21,3	12,4	**20,5**	7,6	3,3	4,2	121
Gesundheits- u. Sozialwesen (WZ08-Q)	55,4	16,9	**35,4**	20,7	13,3	13,4	1,2	2,4	83
Erbringung v. sonst. Dienstl. (WZ08-S)	50,0	5,0	9,8	15,0	17,5	5,0	13,9	0,0	40

IT-System: 1: E-Mail u. Kommunikation, 2: Auftrags- u. Kundenverwaltung, 3: Rechnungswesen u. Controlling, 4: Webauftritt, 5: weitere Software z. Erbringung v. Dienstleistungen, 6: Banking u. Trading, 7: Lager u. Logistik, 8: Produktionssteuerung
Hervorhebung: fett: größter Anteil je IT-System; grau hinterlegt: die drei größten Anteile je IT-System; unterstrichen: größter Anteil je WZ08-Klasse

Tabelle 28 **Vom schwerwiegendsten Cyberangriff betroffene IT-Systeme nach Angriffsart**
in Prozent; gewichtete Daten

	Cyberangriffsart							
IT-System	1	2	3	4	5	6	7	8
E-Mail u. Kommunikation	**49,2**	**66,7**	**60,2**	**45,2**	**71,2**	40,4	**43,8**	**52,6**
Auftrags- u. Kundenverwaltung	48,2	26,6	24,1	25,8	7,6	2,1	9,4	19,8
Rechnungswesen u. Controlling	37,4	19,7	16,7	40,3	3,8	0,0	18,8	20,9
Webauftritt	8,0	16,2	11,7	21,1	58,0	**87,5**	3,9	5,9
weitere Software zur Erbringung von Dienstleistungen	23,9	14,8	12,4	17,7	4,5	0,0	3,9	4,5
Banking u. Trading	11,1	12,7	7,2	8,1	1,5	0,0	7,0	12,9
Lager u. Logistik	15,6	5,6	9,4	16,1	3,1	0,0	0,0	3,9
Produktionssteuerung	7,8	7,0	5,7	12,9	3,8	0,0	0,0	3,4
N	397	142	418	61	131	47	128	462

Cyberangriffsart: 1: Ransomware, 2: Spyware, 3: sonst. Schadsoftware, 4: manuelles Hacking, 5: (D)DoS, 6: Defacing, 7: CEO-Fraud, 8: Phishing
Hervorhebung: fett: größter Anteil je Angriffsart; grau hinterlegt: die drei größten Anteile je Angriffsart; unterstrichen: größter Anteil je IT-System

Danach aufgeschlüsselt, welche IT-Systeme am häufigsten von den jeweiligen Angriffsarten betroffen sind, ist ein recht homogenes Bild zu erkennen (Tabelle 28). Mit Ausnahme von (D)DoS- und Defacing-Angriffen gehören E-Mail und Kommunikationssysteme, Auftrags- und Kundenverwaltungssysteme sowie Rechnungswesen und Controllingsysteme zu den drei am häufigsten betroffenen, d.h. infolge der schwerwiegendsten Angriffe nicht oder nur stark eingeschränkt nutzbaren, IT-Systemen. (D)DoS- und Defacing-Angriffe wirkten sich neben E-

[291] Klassen mit einer Fallzahl kleiner 30 werden nicht aufgeführt.

Mail- und Kommunikationssystemen gemäß ihrer Zielrichtung insbesondere auf den Webauftritt der Unternehmen aus. Weitere Software zur Erbringung von Dienstleistungen sowie Lager- und Logistiksysteme sind vergleichsweise häufig durch Ransomware-Angriffe und manuelles Hacking betroffen. Letztere Angriffsart spielt auch bei Lager und Logistik- sowie Produktionssteuerungssystemen die größte Rolle. Abweichend von den anderen Angriffsarten kommt CEO-Fraud in Tabelle 28 insofern eine besondere Rolle zu, als dass Formen des Social Engineerings in der Regel keinen direkten schädigenden Einfluss auf IT-Systeme haben. Die Betroffenheit der genannten Systeme durch CEO-Fraud ist an dieser Stelle eher als Angriffsweg zu verstehen.

Unter Betrachtung der größten Anteile je IT-System fällt auf, dass Rechnungswesen- und Controlling-Systeme verhältnismäßig oft durch manuelles Hacking betroffen sind. Dies gilt tendenziell auch für die Systeme Lager und Logistik sowie Produktionssteuerung.

Tabelle 29 **Ausfallzeiten betroffener für die Unternehmen (eher) wichtig eingestufter IT-Systeme**
gewichtete Daten; nur Angaben zum schwerwiegendsten Cyberangriff

			Ausfallzeit (eher) wichtig eingestufter IT-Systemen					
IT-System	Betroffen (%)	davon (eher) wichtig (%)	Median (h)	Ø (h)	SD (h)	Min. (h)	Max. (h)	Max. (d)
E-Mail u. Kommunikation	54,5 (N=1.779)	92,7	24 (N=705)	64,8	201,0	1	2.160	90
Auftrags- u. Kundenverwaltung	25,4 (N=1.781)	95,3	24 (N=393)	76,0	172,1	1	1.440	60
Rechnungswesen u. Controlling	22,0 (N=1.782)	93,4	24 (N=310)	73,3	169,4	1	1.440	60
Webauftritt	14,6 (N=1.777)	68,0	12 (N=161)	337,2	1.463,2	1	8.760	365
weitere Software z. Erbringung v. Dienstleistungen	11,7 (N=1.786)	87,7	24 (N=172)	88,7	166,6	1	720	30
Banking u. Trading	9,4 (N=1.783)	92,6	24 (N=117)	43,9	110,2	1	2.160	90
Lager u. Logistik	8,0 (N=1.778)	85,3	24 (N=103)	72,9	151,7	1	720	30
Produktionsteuerung	5,3 (N=1.786)	94,1	48 (N=82)	65,3	63,4	1	480	20

(h): Stunden
(d): Tage

Wenn die genannten IT-Systeme vom schwerwiegendsten Cyberangriff betroffen waren, konnten die Unternehmen zusätzlich angeben, ob es sich um ein (eher) wichtiges oder ein (eher) unwichtiges IT-System für das Unternehmen handelt,[292] und wie lange dieses System nicht oder nur eingeschränkt genutzt werden konnte.

Ein großer Teil der von den schwerwiegendsten Cyberangriffen der letzten zwölf Monate betroffenen IT-Systeme ist für die Unternehmen (eher) wichtig. Der Webauftritt ist dabei mit dem kleinsten Anteil von 68,0 % seltener (eher) wichtig als die Auftrags- und Kundenverwaltung, am oberen Ende mit einem Anteil von 95,3 % (Tabelle 29). In Hinblick auf die Ausfallzeiten der IT-Systeme („nicht oder nur stark eingeschränkt nutzbar“) sind z.T. sehr große Spannbreiten erkennbar, die von einer Stunde bis zu einem Jahr (Webauftritt: 8.760 Stunden oder 365 Tage[293]) reichen. Aus diesem Grund erscheint der gegenüber Extremwerten robustere Median

[292] Den Hintergrund dieser Frage bildet die Überlegung, dass der Ausfall bestimmter IT-Systeme für die Unternehmen unterschiedlich schwer wiegt. So dürfte z.B. der Ausfall des Webauftritts eines Einzelhandels, das sein Hauptgeschäft Vorort macht, weniger folgenschwer sein als für einen Online-Versandhandel, dessen Existenz am Funktionieren des Webauftritts hängt.

[293] Der Wert von 365 Tagen Ausfallzeit für einen als (eher) wichtig eingestuften Webauftritt scheint sehr hoch. Weitere Hintergründe konnten aus Zeitgründen leider nicht erfragt werden. Denkbar wäre hier z.B., dass die Zeit des Ausfalls durch einen parallel geschalteten Webauftritt überbrückt wurde.

im Vergleich zum arithmetischen Mittel als der geeignetere Lageparameter zur Beschreibung der Verteilung. Dieser liegt im Vergleich der betroffenen (eher) wichtigen IT-Systeme zwischen 12 Stunden beim Webauftritt und 48 Stunden bei der Produktionssteuerung. D.h., bei 50,0 % der betroffenen Unternehmen fielen die (eher) wichtig eingestuften Webauftritte höchstens einen halben Tag und die (eher) wichtig eingestuften Produktionssteuerungssysteme höchstens zwei Tage aus. Die anderen 50,0 % mussten entsprechend höhere Ausfallzeiten verkraften. Bezogen auf die übrigen IT-Systeme liegt der Median der Ausfallzeit bei 24 Stunden. Auffallend ist zudem, dass Produktionssteuerungssysteme mit 5,3 % am seltensten betroffen sind, wenn dies der Fall ist jedoch die höchste Ausfallzeit (Median: 48 Stunden) aufweisen. Zugleich weisen sie mit 480 Stunden die geringste maximale Ausfallzeit auf, was darauf hindeuten kann, dass Unternehmen im Falle eines Angriffes diese Systeme mit einer hohen Priorität wieder in einen betriebsbereiten Zustand versetzen.

Tabelle 30 **Ausfallzeit (eher) wichtig eingestufter IT-Systeme nach Cyberangriffsart**
Median in Stunden; gewichtete Daten; nur Angaben zum schwerwiegendsten Cyberangriff

	Cyberangriffsart								
IT-System	1	2	3	4	5	6	7	8	9
E-Mail/Kommunikation	24 (N=163)	48 (N=77)	24 (N=182)	3 (N=20)	6 (N=80)	6 (N=19)	1 (N=30)	12 (N=145)	24 (N=705)
Auftrags- und Kundenverwaltung	48 (N=163)	34 (N=36)	48 (N=94)	2 (N=15)	11 (N=9)		1 (N=6)	6 (N=76)	24 (N=393)
Rechnungswesen und Controlling	48 (N=138)	25 (N=20)	48 (N=59)	10 (N=20)			1 (N=17)	24 (N=58)	24 (N=310)
Webauftritt	48 (N=22)	24 (N=20)	24 (N=34)		5 (N=54)	45 (N=21)		12 (N=11)	12 (N=161)
weitere Software zur Erbringung von Dienstleistungen	48 (N=92)	48 (N=17)	24 (N=34)	168 (N=6)				1 (N=17)	24 (N=172)
Banking und Trading	36 (N=38)	43 (N=17)	24 (N=28)					24 (N=29)	24 (N=117)
Lager und Logistik	36 (N=42)		48 (N=29)	49 (N=10)				24 (N=15)	24 (N=103)
Produktionsteuerung	72 (N=26)	48 (N=9)	48 (N=24)	168 (N=7)				24 (N=15)	48 (N=82)

Cyberangriffsart: 1: Ransomware, 2: Spyware, 3: sonst. Schadsoftware, 4: manuelles Hacking, 5: (D)DoS, 6: Defacing, 7: CEO-Fraud, 8: Phishing, 9: Cyberangriffe insg.

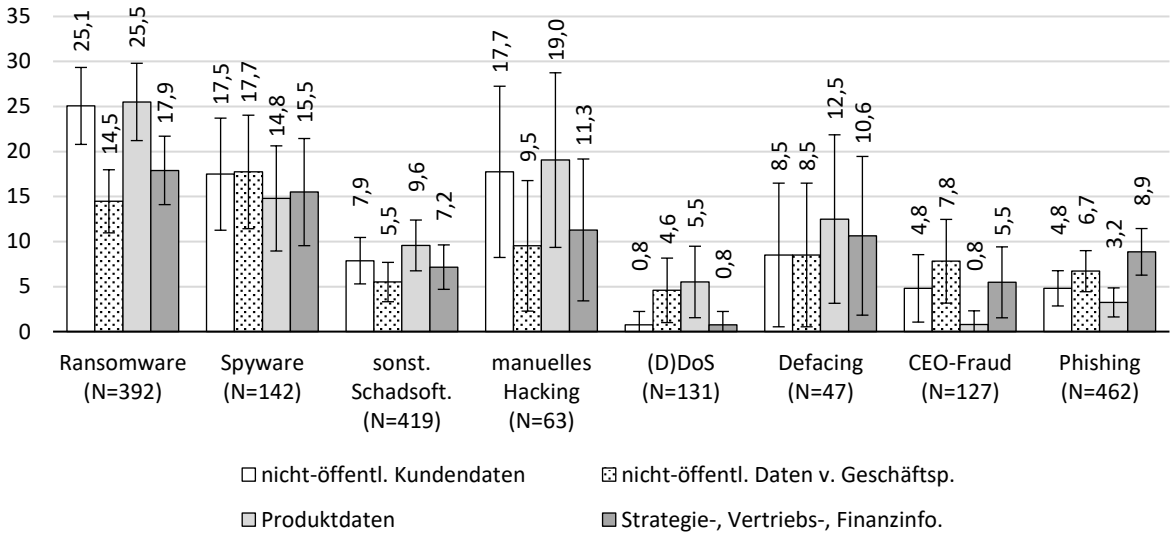
Die nach Cyberangriffsart differenzierten mittleren Ausfallzeiten (Median in Stunden) der einzelnen als (eher) wichtig eingestuften IT Systeme (Tabelle 30) sind aufgrund von teilweise sehr geringen Fallzahlen nur eingeschränkt interpretierbar: Längere Ausfallzeiten bei Systemen der Produktionssteuerung und bei weiterer Software zur Erbringung von Dienstleistungen scheinen insbesondere infolge von manuellen Hacking aufzutreten (Median: jeweils 168 Stunden). Sind IT-Systeme der Produktionssteuerung von Ransomware-Angriffen betroffen, scheinen auch hier die Ausfallzeiten vergleichsweise lang zu sein (Median: 72 Stunden). Da die Angriffsart CEO-Fraud in der Regel weniger darauf ausgelegt ist, IT-Systeme zu schädigen, wäre eine mögliche Erklärung, dass es sich hier um Varianten des CEO-Frauds, wie z.B. die Veranlassung von unautorisierten Änderungen von Stammdaten, Anlage von Kontaktinformationen oder Kreditoren/Debitoren durch Anwendung von Social-Engineering handelte. Möglich ist aber auch, dass z.B. die Dauer forensischer Maßnahmen oder der Systemwartung infolge des Angriffs hierunter subsumiert wurde.

9.5.2 Betroffene Daten

Die durch die jeweiligen Angriffsarten betroffen Daten wurden nach nicht-öffentliche Daten von Kund*innen (z.B. Zugangsdaten, Bankdaten, Adressen, Patient*innendaten) [294], nicht-öffentliche Daten von Geschäftspartner*innen (z.B. Zugangsdaten, Bankdaten, Adressen), Produktdaten (z.B. Konstruktionspläne, Rezepturen, Quellcodes) sowie Strategie-, Vertriebs und Finanzinformationen (z.B. Preislisten, Sanierungspläne, Akquisitionen, Finanz- und Rechnungswesen-Daten) differenziert erhoben. Bei rund einem Viertel der Unternehmen waren durch den schwerwiegendsten Cyberangriff im Vorjahr derartige Daten betroffen (25,2 %; N=1.783), d.h., sie wurden unbefugt gelöscht, manipuliert, gestohlen/ kopiert oder verschlüsselt.

Hinsichtlich ihrer Betroffenheit sind weder zwischen den differenzierten Datenarten noch zwischen den Unternehmen unterschiedlicher Beschäftigtengrößenklassen statistisch relevante Unterschiede festzustellen.

Abbildung 59 **Anteil der Unternehmen mit betroffenen Daten nach Daten- und Angriffsart**
in Prozent; gewichtete Daten; 95%-KI; nur Angaben zum schwerwiegendsten Cyberangriff



Demgegenüber sind z.T. signifikante Unterschiede innerhalb und zwischen den Angriffsarten erkennbar (Abbildung 59): So sind z.B. bei Unternehmen, die von einem Ransomware-Angriff als schwerwiegendsten Cyberangriff berichten, besonders nicht-öffentliche Kundendaten (25,1 %) und Produktdaten (25,5 %) betroffen und weniger nicht öffentliche Daten von Geschäftspartnern (14,5 %) und Strategie-, Vertriebs- und Finanzinformationen (17,9 %). Gleichzeitig sind bei dieser Angriffsart erwartungsgemäß Daten generell stärker betroffen als bei einem (D)DoS- oder Phishing-Angriff. Auch nicht erkennbar ist, dass es Spyware-Angriffe insbesondere auf bestimmte Daten, z.B. Produkt- oder Strategieinformationen absehen, um etwa gezielt Spionage zu betreiben.

[294] Bei der ersten Kategorie, Daten von Kunden, handelt es sich somit um personenbezogene Daten im Sinne der europäischen Datenschutzgrundverordnung. Im Falle der zweiten Kategorie, Daten von Geschäftspartnern, kann es sich ebenfalls um personenbezogene Daten handeln. Dies konnte aber aufgrund von Zeit- und Komplexitätsgründen nicht einzeln erhoben werden.

Entsprechend der unterschiedlichen Betroffenheit der Unternehmen verschiedener WZ08-Klassen in Hinblick auf die Cyberangriffsarten, variieren auch die Anteile der vom schwerwiegendsten Cyberangriff betroffenen Daten zwischen den WZ08-Klassen.

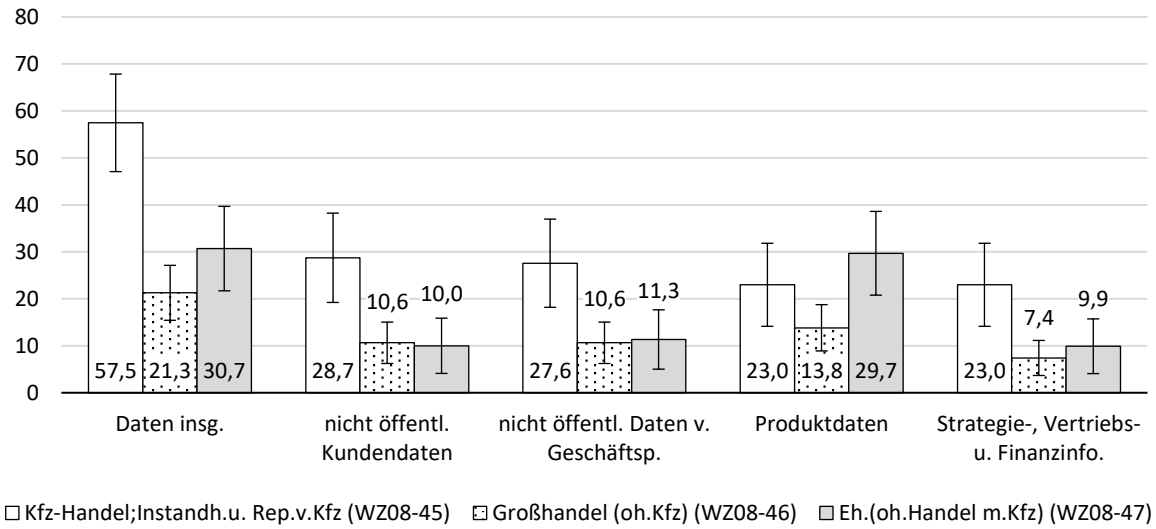
Tabelle 31 **Anteil der Unternehmen mit betroffenen Daten nach Datenart und WZ08-Klassen**
in Prozent; gewichtete Daten

	Datenart					
WZ08-Klassen (Ebene 1; Kurzbezeichnung; nur wenn N≥30)	1	2	3	4	5.	N
Verarbeitendes Gewerbe (WZ08-C)	25,2	10,5	7,2	10,5	11,5	388
Baugewerbe (WZ08-F)	20,3	5,3	9,7	7,7	5,3	207
Handel; Instandhaltung u. Reparatur v. Kfz (WZ08-G)	32,2	14,9	**15,1**	**20,2**	11,7	375
Verkehr u. Lagerei (WZ08-H)	18,5	12,7	1,9	9,1	7,4	54
Gastgewerbe (WZ08-I)	17,2	14,3	11,1	1,6	1,6	63
Information u. Kommunikation (WZ08-J)	3,1	1,5	1,5	1,5	1,5	65
Freiberufl., wissenschaftl. u. techn. Dienstl. (WZ08-M)	25,7	9,8	9,3	16,0	13,4	185
Sonstigen wirtschaftl. Dienstl. (WZ08-N)	33,0	**16,1**	11,0	4,4	14,3	90
Erziehung u. Unterricht (WZ08-P)	22,3	10,7	3,3	11,6	9,1	121
Gesundheits- u. Sozialwesen (WZ08-Q)	**36,1**	13,4	8,5	4,8	**22,0**	82
Sonstige Dienstl. (WZ08-S)	10,0	2,6	2,5	2,8	5,0	39

Datenart: 1: Daten insg., 2: nicht öffentl. Kundendaten, 3: nicht öffentl. Daten von Geschäftspartnern*innen, 4: Produktdaten, 5: Strategie-, Vertriebs- u. Finanzinfo.
Hervorhebung: fett: größter Anteil je Datenart; grau hinterlegt: die drei größten Anteile je Datenart

Die WZ08-Klasse G (Handel; Instandhaltung u. Reparatur v. Kfz) war z.B. relativ häufig von Angriffen mit Schadsoftware (Ransomware, Spyware und sonst. Schadsoftware) betroffen[295] und zählt erwartungsgemäß WZ08-Klassen bei deren Unternehmen häufiger Daten betroffen sind (Daten insg.: 32,2 %). Dabei handelt es sich insbesondere um Produktdaten und nicht öffentliche Daten von Geschäftspartnern.

Abbildung 60 **Betroffene Daten nach WZ08-Klassen**
in Prozent; gewichtete Daten; 95%-KI; Mehrfachantworten mögl.



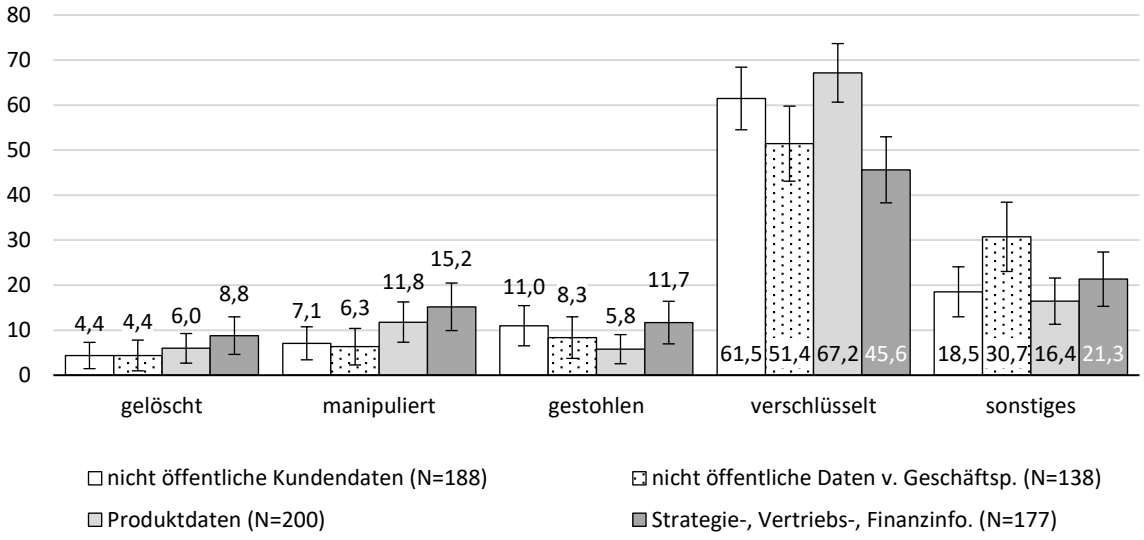
[295] Siehe Abschnitt 7.1.2 Tabelle 24.

Mit Blick auf die zweite Ebene der WZ08-Klassen ist davon vor allem der Kfz-Handel inkl. Instandhaltung und Reparatur von Kraftfahrzeugen (WZ08-45) betroffen (Abbildung 60). Lediglich in Hinblick auf Produktdaten ist der Einzelhandel ohne Handel mit Kfz (WZ08-47) zumindest tendenziell stärker betroffen. Bezüglich betroffener Strategie, Vertriebs- und Finanzinformationen haben Maschinenbauunternehmen (WZ08-28) den höchsten Anteil (30,4 %).[296]

Neben der Betroffenheit der Daten wurde danach gefragt, was mit diesen Daten passiert ist. Als Antwortmöglichkeiten wurden: „gelöscht", „manipuliert", „gestohlen" und „verschlüsselt" vorgegeben.[297]

In den meisten Fällen wurden die betroffenen Daten verschlüsselt, wobei dies im Vergleich zu nicht öffentlichen Daten von Geschäftspartner*innen (51,4 %) und Strategie-, Vertriebs- und Finanzinformationen (45,6 %) vor allem auf Produktdaten (67,2 %) zutraf (Abbildung 61). Letztere wurden hingegen signifikant häufiger manipuliert (15,2 %) als nicht öffentliche Daten von Kunden (7,1 %) und Geschäftspartner*innen (6,3 %).

Abbildung 61 **Folgen für die betroffenen Daten nach Datenart**
in Prozent; gewichtete Daten; 95%-KI; Mehrfachantworten mögl.



9.5.3 Kostenpositionen

Ob durch den schwerwiegendsten Cyberangriff der letzten zwölf Monate Kosten entstanden sind, wurde für folgende Positionen erfragt: Externe Beratung (z.B. Rechtsberatung, Notfallmanagement), Sofortmaßnahmen zur Abwehr und Aufklärung, Schadensersatz/Strafen, abgeflossene Gelder, Betriebsunterbrechung sowie Wiederherstellung/Wiederbeschaffung. Bei knapp einem Drittel der Unternehmen (30,0 %; N=1.772) sind beim schwerwiegendsten Cy-

[296] Wie an diesen Beispielen zu erkennen, spiegeln sich solche Unterschiede und Auffälligkeiten auf der zweiten Ebene der WZ08-Klassen nicht immer auf der ersten Ebene wieder. Daher lohnt ein differenzierterer Vergleich (siehe Tabelle 52 im Anhang 1).

[297] Bei der Erhebung hat das Umfrageinstitut noch die Kategorie „sonstiges" hinzugefügt, da die Befragten die Antwortmöglichkeiten als nicht erschöpfend wahrgenommen haben. Dies könnte z.B. daran liegen, dass die Kategorie „gestohlen" missverstanden wurde, insofern mit dem Diebstahl der gleichzeitige Verlust der Daten assoziiert wurde. In zukünftigen Erhebungen könnte stattdessen von „unbefugt kopiert/ genutzt/ eingesehen" o.ä. gesprochen werden.

berangriff keine derartigen Kosten entstanden. Ein Anteil von 28,6 % berichten von entstandenen Kosten bei einer dieser sechs Positionen, 24,7 % bei zwei und die übrigen 16,7 % bei drei und mehr Positionen. Die Höhe der Kosten bleibt dabei zunächst unberücksichtigt.

Tabelle 32 **Anteil der Unternehmen mit Kosten infolge des schwerwiegendsten Cyberangriffs**
in Prozent; gewichtete Daten; Mehrfachantworten möglich; fett: signifikant bei p<.05 (Chi²-Test)

		Beschäftigtengrößenklasse				
Kostenposition	Gesamt	10-49	50-99	100-249	250-499	ab 500
externe Beratung	30,3	**31,9**	**28,2**	**23,3**	**21,2**	**14,3**
Sofortmaßnahmen zur Abwehr und Aufklärung	39,9	**41,4**	**36,6**	**33,6**	**33,8**	**41,7**
Schadensersatz/Strafen	1,4	1,5	1,1	2,0	0,5	1,2
abgeflossene Gelder	2,2	2,0	3,4	2,5	1,2	3,5
Betriebsunterbrechung	25,7	26,6	24,1	23,5	23,8	17,1
Wiederherstellung/Wiederbeschaffung	33,0	**34,9**	**29,7**	**24,0**	**23,5**	**26,5**
Kosten bei mindestens einer Position entstanden	70,0	**72,3**	**65,7**	**60,4**	**62,6**	**64,5**
N	1.772	404	467	447	425	259

Bei den am häufigsten genannten Positionen, bei denen Kosten infolge des schwerwiegendsten Cyberangriffs entstanden sind (Sofortmaßnahmen zur Abwehr und Aufklärung: 39,9 %; Wiederherstellung und Wiederbeschaffung: 33,0 % sowie externe Beratung: 30,3 %), weisen statistisch signifikante Unterschiede zwischen den Beschäftigtengrößenklassen auf (Tabelle 32): Bei kleinen Unternehmen entstanden demnach deutlich häufiger Kosten durch externe Beratung und Wiederherstellung/Wiederbeschaffung (10-49 Besch.: 31,9 % bzw. 34,9 %) als bei großen (ab 50 Besch.: 14,3 % bzw. 26,5 %). Kosten für Sofortmaßnahmen zur Abwehr und Aufklärung entstanden am häufigsten in kleinen und großen Unternehmen (10-49 Besch.: 41,4 %; ab 500 Besch.: 41,7 %) und am seltensten in Unternehmen mit 100-249 Beschäftigten (33,6 %) und 250-499 Beschäftigten (33,8 %). Kosten durch Betriebsunterbrechung entstanden tendenziell ebenfalls häufiger in kleinen als in großen Unternehmen (10-49 Besch.: 26,6 %; ab 500 Besch.: 17,1 %), während Kosten durch Schadensersatz/Strafen und abgeflossene Gelder in allen Unternehmensgrößen eine ähnlich geringe Rolle spielten und lediglich im unteren einstelligen Prozentbereich auftraten.

Differenziert nach Angriffsart (Tabelle 33) wird erkennbar, dass bei den Unternehmen, die Ransomware, Spyware und manuelles Hacking als schwerwiegendsten Angriff benannt haben, deutlich häufiger Kosten entstanden sind (85,9 %, 86,6 % bzw. 80,6 %) als bei den anderen Angriffsarten (z.B. CEO-Fraud: 46,0 %). Mit Blick auf die größten Anteile je Kostenposition zeigt sich beispielsweise, dass entgegen der naheliegenden Vermutung, abgeflossene Gelder durch manuelles Hacking (20,6 %) anteilig öfter eine Rolle spielen als etwa beim CEO-Fraud (6,3 %).

Sieht man sich darüber hinaus an, welche Kostenpositionen bei den jeweiligen Angriffsarten am häufigsten genannt wurden, fallen weitere Unterschiede auf: Bei Ransomware und manuellem Hacking ist Wiederherstellung und Wiederbeschaffung die am häufigsten genannte Kostenposition (52,4 % bzw. 50,0 %), während dies bei allen anderen Angriffsarten, wenn auch unterschiedlich häufig, die Position Sofortmaßnahmen zur Abwehr und Aufklärung ist.

Tabelle 33 **Anteil der Unternehmen mit Kosten infolge des schwerwiegendsten Cyberangriffs nach Angriffsart**
in Prozent; gewichtete Daten; Mehrfachantworten möglich

	Cyberangriffsart							
Kostenposition	1	2	3	4	5	6	7	8
externe Beratung	37,6	45,8	36,9	35,5	21,2	37,5	20,3	17,6
Sofortmaßnahmen zur Abwehr und Aufklärung	45,7	**49,0**	**44,0**	43,5	**35,6**	**42,6**	**26,8**	**33,2**
Schadensersatz und Strafen	1,5	0,0	2,6	8,1	0,8	0,0	0,0	0,6
abgeflossene Gelder	1,5	0,0	0,2	20,6	0,0	0,0	6,3	2,6
Betriebsunterbrechung	42,0	34,8	28,6	29,5	19,7	17,0	9,3	13,7
Wiederherstellung und Wiederbeschaffung	**52,4**	34,3	34,6	**50,0**	25,0	38,3	5,6	20,9
Kosten bei mindestens einer Position entstanden	85,9	86,6	78,1	80,6	61,8	72,3	46,0	50,8
N	398	142	415	62	131	47	124	459

Cyberangriffsart: 1: Ransomware, 2: Spyware, 3: sonst. Schadsoftware, 4: manuelles Hacking, 5: (D)DoS, 6: Defacing, 7: CEO-Fraud, 8: Phishing
Hervorhebung: fett: größter Anteil je Angriffsart; unterstrichen: größter Anteil je Kostenposition

Kosten für externe Beratung sowie für Sofortmaßnahmen zur Abwehr und Aufklärung fielen im Vergleich zwischen den Angriffsarten am häufigsten nach Spyware-Angriffen an (45,8 % bzw. 49,0 %). Schadensersatz und Strafen sowie abgeflossene Gelder wurden am häufigsten bei manuellem Hacking genannt (8,1 % bzw. 20,6 %). Kosten infolge von Betriebsunterbrechungen sowie für Wiederherstellung/Wiederbeschaffung entstanden am häufigsten nach Ransomware-Angriffen (42,0 % bzw. 52,4 %).

9.5.4 Kostenhöhe

Generell sind verlässliche Studien zu entstandenen Schäden durch Cyberangriffe selten. Diese Seltenheit ist u.a. auch in der schwierigen Operationalisierung bzw. Erfassung der Kosten, der mäßigen Auskunftsbereitschaft der Unternehmen sowie dem Umstand geschuldet, dass nur wenige Unternehmen die entstanden direkten Kostenpositionen tatsächlich ermitteln und nachhalten.[298] Indirekte Kosten wie Reputationsschäden, Auftragsausfälle oder Wettbewerbsnachteile, die zeitlich stark versetzt vom Cyberangriff auftreten können, sind zudem kaum realistisch zu beziffern.

Bei den Ergebnissen zur Höhe der durch den schwerwiegendsten Cyberangriff der letzten zwölf Monate verursachten direkten Kosten ist daher zu berücksichtigen, dass es sich häufig um Circa-Angaben handelt, die von einem relativ großen Anteil der Befragten gegeben werden konnte. Die Gesamtkosten über alle oben erfragten Kostenpositionen hinweg wurden daher nur berechnet, wenn zu allen Positionen gültige Werte zur Kostenhöhe vorhanden waren, die summiert werden konnten. Nicht gültige Werte sind in diesem Fall die Antworten „keine Angabe“ oder „weiß ich nicht“. Von den 70,0 % der Unternehmen, die angegeben haben, dass bei mindestens einer der Positionen Kosten entstanden sind (N=1.772), konnten bei 30,9 % (N=1.240) aufgrund fehlender Angaben zur ungefähren Kostenhöhe einzelner Positionen keine Gesamtkosten berechnet werden. Dies bedeutet, dass nur „gesicherte“ und vollständige Angaben zu direkten Gesamtkosten einbezogen wurden und Fälle mit unklaren Kostenbestandteilen bzw.

[298] Auch Klahr et al. (2017) berichten, dass es unüblich für Unternehmen ist, finanzielle Kosten von Cybersecurity Vorfällen zu ermitteln und nachzuhalten.

Kostenhöhen unberücksichtigt blieben, um einen möglichst realistischen Anhaltspunkt für entstehende direkte Gesamtkosten zu ermitteln.

Bei den Unternehmen, bei denen Kosten entstanden sind und alle entsprechenden Angaben vorlagen, bewegten sich die Gesamtkosten zwischen 10 EUR und 2 Mio. EUR und im Durchschnitt bei rund 16.900 EUR (N=857). Tendenziell fielen die Durchschnittskosten in größeren Unternehmen höher aus als in kleineren und beim Vergleich der Kostenpositionen fallen abgeflossene Gelder mit den höchsten Durchschnittskosten von rund 27.900 EUR auf (Tabelle 34).

Tabelle 34 **Durchschnittskosten nach Kostenposition und Beschäftigtengrößenklasse**
in EUR; gerundet; gewichtete Daten; Mehrfachantworten möglich; nur Unternehmen mit Kosten

		Beschäftigtengrößenklasse				
Kostenposition	Gesamt	10-49	50-99	100-249	250-499	ab 500
externe Beratung	1.900 (N=412)	1.600 (N=99)	2.000 (N=104)	5.300 (N=78)	4.800 (N=69)	3.900* (N=25)
Sofortmaßnahmen zur Abwehr und Aufklärung	8.800 (N=559)	7.200 (N=136)	15.200 (N=122)	8.500 (N=103)	13.500 (N=102)	33.200 (N=73)
Schadensersatz und Strafen	4.200* (N=23)	2.700* (N=6)	1.000* (N=3)	12.200* (N=6)	50.000* (N=1)	31.600* (N=3)
abgeflossene Gelder	27.900 (N=30)	24.700* (N=7)	48.700* (N=9)	6.700* (N=5)	16.900* (N=3)	47.700* (N=7)
Betriebsunterbrechung	12.000 (N=283)	10.700 (N=70)	10.000 (N=55)	22.600 (N=49)	48.100 (N=53)	12.200* (N=20)
Wiederherstellung und Wiederbeschaffung	13.100 (N=487)	13.100 (N=121)	11.900 (N=107)	20.100 (N=77)	2.500 (N=76)	7.800 (N=53)
Gesamtkosten	16.900 (N=857)	15.900 (N=208)	18.500 (N=194)	19.500 (N=158)	22.900 (N=167)	31.200 (N=98)

*) sehr geringe Fallzahl (N < 30)

Da Durchschnittswerte stark von Extremwerten beeinflusst sein können, wird zusätzlich der demgegenüber robustere Median angegeben, der die Verteilung in zwei gleich große Hälften teilt. Der Median der Gesamtkosten über alle Kostenpositionen hinweg liegt bei 1.000 EUR, d.h., wenn Kosten durch den schwerwiegendsten Cyberangriff verursachte wurden, lagen diese bei einer Hälfte der Unternehmen bei bis zu 1.000 EUR und bei der anderen Hälfte über 1.000 EUR, wobei keine signifikanten Unterschiede zwischen den Beschäftigtengrößenklassen erkennbar sind. Allerdings scheinen bei kleinen Unternehmen tendenziell häufiger geringere Kosten entstanden zu sein als bei den großen (Tabelle 35). Dabei ist jedoch zu berücksichtigen, dass es hinsichtlich der Verbreitung der verschiedenen Cyberangriffsarten z.T. deutliche Unterschiede zwischen den Beschäftigtengrößenklassen gibt.

Differenziert nach einzelnen Kostenpositionen fällt auf, dass die Mediane der Kosten externer Beratung und für Sofortmaßnahmen zur Abwehr und Aufklärung deutlich geringer sind (870 bzw. 800 EUR) als die Mediane der Kosten, die durch abgeflossene Gelder und Betriebsunterbrechungen entstanden sind (jeweils 2.000 EUR).

Tabelle 35 **Median der Kosten nach Kostenposition und Beschäftigtengrößenklasse**
in EUR; gerundet; gewichtete Daten; Mehrfachantworten möglich; nur Unternehmen mit Kosten

		Beschäftigtengrößenklasse				
Kostenposition	Gesamt	10-49	50-99	100-249	250-499	ab 500
externe Beratung	870 (N=412)	790 (N=99)	1.000 (N=104)	1.000 (N=78)	1.000 (N=69)	2.000* (N=25)
Sofortmaßnahmen zur Abwehr und Aufklärung	800 (N=559)	600 (N=136)	1.000 (N=122)	1.000 (N=103)	1.000 (N=102)	1.500 (N=73)
Schadensersatz und Strafen	910* (N=23)	670* (N=6)	850* (N=3)	8.550* (N=6)	50.000* (N=1)	11.110* (N=3)
abgeflossene Gelder	2.000 (N=30)	2.760* (N=7)	2.000* (N=9)	3.620* (N=5)	15.700* (N=3)	31.250* (N=7)
Betriebsunterbrechung	2.000 (N=283)	2.000 (N=70)	3.000 (N=55)	5.000 (N=49)	2.810 (N=53)	5.000* (N=20)
Wiederherstellung und Wiederbeschaffung	1.000 (N=487)	1.000 (N=121)	800 (N=107)	1.000 (N=77)	800 (N=76)	1.100 (N=53)
Gesamtkosten	1.000 (N=857)	1.000 (N=208)	1.200 (N=194)	1.500 (N=158)	1.500 (N=167)	1.470 (N=98)

*) sehr geringe Fallzahl (N < 30)

Tabelle 36 **Durchschnittskosten nach Kostenposition und Cyberangriffsart**
in EUR; gerundet; gewichtete Daten; Mehrfachantworten möglich; nur Unternehmen mit Kosten

	Cyberangriffsart							
Kostenposition	1	2	3	4	5	6	7	8
externe Beratung	1.900 (N=93)	1.200 (N=56)	1.600 (N=126)	6.800* (N=18)	2.100* (N=24)	1.700 (N=11)	1.900* (N=24)	1.700 (N=61)
Sofortmaßnahmen zur Abwehr und Aufklärung	20.100 (N=133)	5.500 (N=52)	3.000 (N=146)	4.000* (N=23)	14.400 (N=41)	1.600* (N=18)	2.600 (N=30)	6.500 (N=111)
Schadensersatz und Strafen	2.900* (N=5)		1.300* (N=10)	10.300* (N=5)	100* (N=1)			10.700* (N=2)
abgeflossene Gelder	800* (N=5)			39.900* (N=12)			22.900* (N=2)	28.000* (N=10)
Betriebsunterbrechung	11.900 (N=85)	1.600 (N=30)	9.600 (N=81)	65.100 (N=13)	19.300 (N=16)		32.100 (N=6)	3.600 (N=49)
Wiederherstellung und Wiederbeschaffung	20.400 (N=172)	1.200 (N=37)	6.600 (N=119)	10.900* (N=26)	27.000 (N=31)	1.200* (N=13)	2.900* (N=6)	7.100 (N=76)
Gesamtkosten	32.200 (N=201)	4.700 (N=92)	8.200 (N=230)	43.700 (N=35)	25.600 (N=66)	2.600* (N=21)	8.600 (N=40)	9.300 (N=166)

Cyberangriffsart: 1: Ransomware, 2: Spyware, 3: sonst. Schadsoftware, 4: manuelles Hacking, 5: (D)DoS, 6: Defacing, 7: CEO-Fraud, 8: Phishing
*) sehr geringe Fallzahl (N < 30)

Weitere Unterschiede finden sich beim Vergleich der direkten Gesamtkosten nach Angriffsart (Tabelle 36 und Tabelle 37): So liegen die Kosten über alle Positionen hinweg bei Ransomware-Angriffen und manuellem Hacking im Durchschnitt mit 32.200 EUR bzw. 43.700 EUR (Median:1.300 bzw. 2.800 EUR) deutlich über den Kosten der anderen Angriffsarten, insbesondere über den direkten Kosten von Spyware-Angriffen, sonstigen Schadsoftware-Angriffen und Defacing (Durchschnitt: 4.700 EUR, 8.200 EUR bzw. 2.600 EUR; Median: 750 EUR, 790 EUR bzw. 990 EUR).

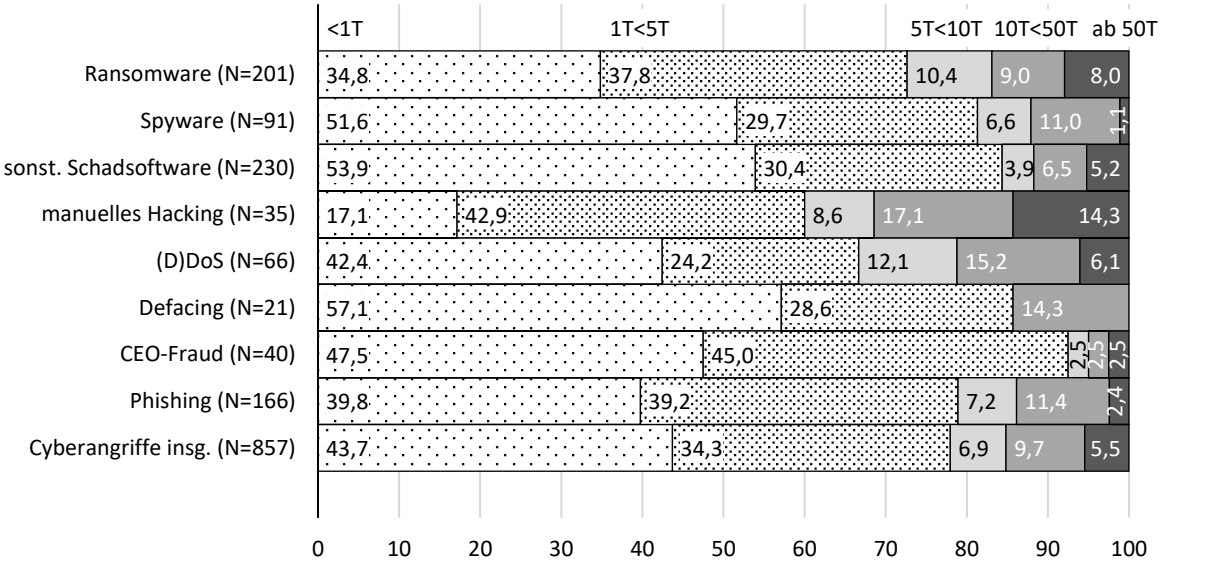
Tabelle 37 **Median der Kosten nach Kostenposition und Cyberangriffsart**
in EUR; gerundet; gewichtete Daten; Mehrfachantworten möglich; nur Unternehmen mit Kosten

	Cyberangriffsart							
Kostenposition	1	2	3	4	5	6	7	8
externe Beratung	1.500 (N=93)	550 (N=56)	500 (N=126)	2.000* (N=18)	1.000* (N=24)	100 (N=11)	1.460* (N=24)	500 (N=61)
Sofortmaßnahmen zur Abwehr und Aufklärung	1.000 (N=133)	750 (N=52)	500 (N=146)	2.000* (N=23)	1.000 (N=41)	990* (N=18)	500 (N=30)	1.000 (N=111)
Schadensersatz und Strafen	100* (N=5)		990* (N=10)	10.000* (N=5)				
abgeflossene Gelder	500* (N=5)			5.000* (N=12)			19.700* (N=2)	2.000* (N=10)
Betriebsunterbrechung	2.000 (N=85)	1.500 (N=30)	2.000 (N=81)	100.000* (N=13)	10.000* (N=16)		500* (N=6)	740 (N=49)
Wiederherstellung und Wiederbeschaffung	1.000 (N=172)	400 (N=37)	1.000 (N=119)	4210* (N=26)	1.000 (N=31)	950* (N=13)	1.000* (N=6)	500 (N=76)
Gesamtkosten	1.300 (N=201)	750 (N=92)	790 (N=230)	2.800 (N=35)	1.090 (N=66)	990* (N=21)	1.000 (N=40)	1.000 (N=166)

Cyberangriffsart: 1: Ransomware, 2: Spyware, 3: sonst. Schadsoftware, 4: manuelles Hacking, 5: (D)DoS, 6: Defacing, 7: CEO-Fraud, 8: Phishing
*) sehr geringe Fallzahl (N < 30)

Mit der Einschränkung, dass die zugrundeliegenden Fallzahlen zum Teil sehr klein sind, kann mit aller Vorsicht gezeigt werden, dass das relativ selten vorkommende manuelle Hacking in allen Positionen, vor allem aber in Hinblick auf Betriebsunterbrechung sowie Schadensersatz und Strafen, beim Medianvergleich sowie im Durchschnitt relativ hohe Kosten verursachte. Die höheren mittleren Kosten durch Betriebsunterbrechung infolge von manuellem Hacking stehen zudem im Einklang mit den oben (Tabelle 30) erkennbaren längeren mittleren Ausfallzeiten von Produktionssteuerungssystemen und weiterer Software zur Erbringung von Dienstleistungen bei dieser Angriffsart.

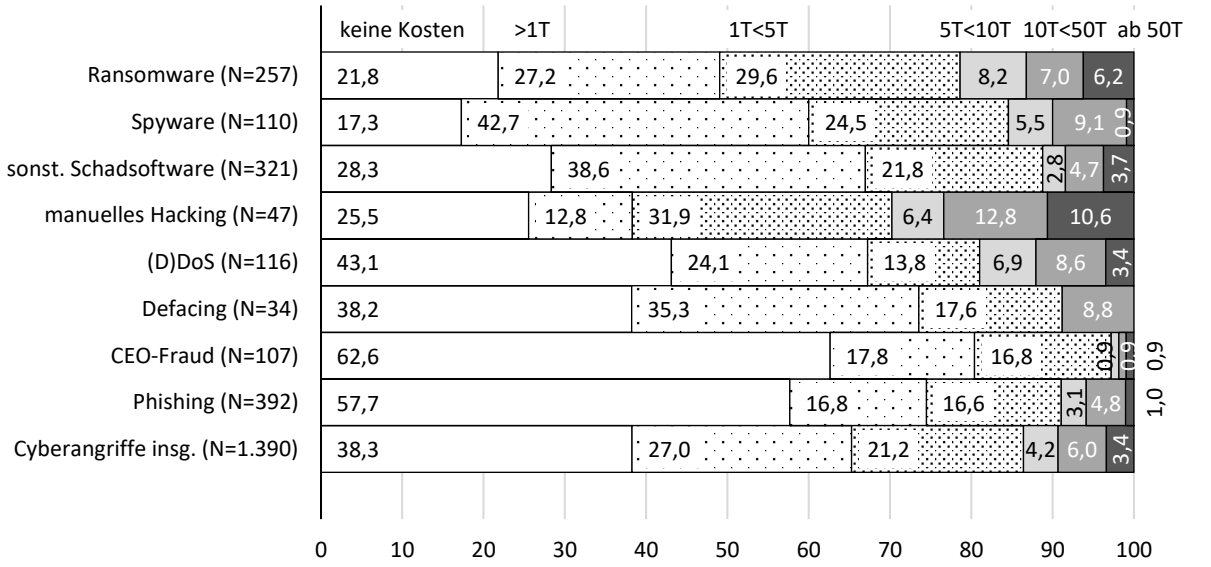
Abbildung 62 **Klassifizierte Gesamtkosten nach Cyberangriffsart**
in Prozent; Klassen in Tausend EUR; gewichtete Daten; nur Unternehmen mit Kosten



Ganz allgemein kann ebenso festgestellt werden, dass die infolge der verschiedenen Angriffsarten entstandenen Kosten in den meisten Fällen relativ gering ausfielen (Abbildung 62): Bei

78,0 % der berichteten schwerwiegendsten Cyberangriffe lagen die über die erfragten Kostenpositionen errechneten Gesamtkosten unter 5.000 EUR. Bei 6,9 % entstanden Kosten zwischen 5.000 und 10.000 EUR, bei 9,7 % zwischen 10.000 und 50.000 EUR und bei einem kleinen Anteil von 5,5 % lagen die Gesamtkosten bei 50.000 EUR und darüber.

Abbildung 63 **Klassifizierte Gesamtkosten nach Cyberangriffsart**
in Prozent; Klassen in Tausend EUR; gewichtete Daten



Bezieht man die Unternehmen, bei denen durch den schwerwiegendsten Cyberangriff der letzten zwölf Monate keine Kosten entstanden sind, als weitere Klasse mit ein (Abbildung 63), wird noch deutlicher, dass nur ein relativ kleiner Anteil größere direkte Kosten zu bewältigen hatte: Bezogen auf alle Cyberangriffe insgesamt liegt der Anteil der Unternehmen, bei denen entweder keine Kosten oder Kosten unter 5.000 EUR entstanden sind, bei 86,4 %. Daneben fällt auf, dass sich die Anteile der Unternehmen ohne Kosten zwischen den Cyberangriffsarten unterscheiden. Über die Hälfte der Unternehmen, die im Zusammenhang mit dem schwerwiegendsten Cyberangriff von CEO-Fraud oder Phishing berichteten, hatten keine der erfragten Kosten zu begleichen (62,6 % bzw. 57,7). Demgegenüber liegt dieser Anteil vor allem bei Angriffen mit Schadsoftware (Spyware:17,3 %, Ransomware: 21,8 %, sonstige Schadsoftware: 28,3 %) sowie bei manuellem Hacking (25,5 %) deutlich darunter.

Mit Blick auf vergleichbare Literatur fällt auf, dass neben den am Anfang des Abschnitts erwähnten Limitationen vor allem der Betrachtungsgegenstand des schwerwiegendsten Angriffes dazu führt, kaum direkte Vergleiche ziehen zu können. Ein überwiegender Teil der bisherigen Studien schätzt die Kosten von Cyberangriffen auf einen bestimmten Zeitraum[299] (z.B. letzte 12 Monate) und nicht für einen konkreten Vorfall.[300]

Der britische Versicherungskonzern Hiscox hingegen nennt geschätzte Durchschnittskosten für den größten Cybersecurity-Vorfall in den letzten 12 Monaten (Erhebungszeitraum: Herbst 2017). Demnach sind deutsche Unternehmen sogar stärker als niederländische, spanische, britische und US-amerikanische Unternehmen betroffen und weisen Kosten von durchschnittlich

[299] Siehe z.B. Klahr et al. (2017); Rantala (2008); Vanson Bourne (2014).

[300] Ein Bezug zum schwerwiegendsten Angriff erfolgt z.B. bei Paoli et al. (2018), jedoch nur als Kostenkategorie, ohne die mittleren Gesamtkosten in EUR (z.B. Median) anzugeben.

11.918 USD (bis 249 Mitarbeiter), 86.834 USD (250 bis 999 Mitarbeiter) und 150.891 USD (mehr als 1.000 Mitarbeiter) auf. Die genauen Kostenbestandteile und weitere strukturelle Merkmale werden zwar nicht angegeben, insgesamt scheinen die Kostenschätzungen jedoch über den Ergebnissen dieser Studie zu liegen.[301] Klahr et al. beziehen sich u.a. ebenfalls auf den schwerwiegendsten Vorfall der letzten 12 Monate: Wenn in diesen direkte Kosten entstanden sind, wurden sie durchschnittlich mit 1.320 GBP (Median: 150 GBP) beziffert.[302] Diese Kostenangaben bewegen sich damit unter denen in dieser Studie.[303] Dies gilt auch, wenn berücksichtigt wird, dass in der Stichprobe von Klahr et al. Kleinstunternehmen unter zehn Beschäftigten enthalten sind.[304]

Völlig unbestritten bleibt, dass generell durch Cyberangriffe hohe Kosten in Unternehmen entstehen können und extreme Ereignisse auch tatsächlich vorkommen. Nach den vorliegenden Ergebnissen der auf Selbstauskunft beruhenden Schätzungen der befragten Personen, scheinen allerdings nur wenige Unternehmen von extrem hohen Kosten durch Cyberangriffe betroffen zu sein.

9.6 Informations- und Anzeigeverhalten

9.6.1 Information nicht-staatlicher Stellen

Bezüglich des schwerwiegendsten Vorfalls wurden die Unternehmensvertreter*innen befragt, welche nicht-staatliche Stelle von dem Vorfall erfahren hat. Zur Auswahl standen die Antwortmöglichkeiten: Kunden, Geschäftspartner, Versicherer, Eigentümer des Unternehmens und die Öffentlichkeit. Auf welchem Weg die Information erlangt wurde (über das Unternehmen selbst oder auf anderem Weg), blieb dabei außen vor.

Tabelle 38 **Nicht-staatliche Stelle, die von dem Vorfall erfahren hat, nach Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; Mehrfachantworten möglich; fett: signifikant bei p<.05 (Chi²-Test)

		Beschäftigtengrößenklassen				
Nicht-staatliche Stelle	Gesamt	10-49	50-99	100-249	250-499	ab 500
Kunden	15,5	**16,8**	**11,1**	**11,9**	**10,4**	**11,9**
Geschäftspartner	21,4	**23,1**	**16,2**	**16,0**	**13,6**	**13,8**
Versicherer	9,1	9,2	9,1	8,4	9,7	9,2
Eigentümer*innen des Unternehmens	91,5	**93,4**	**88,5**	**85,8**	**85,9**	**76,0**
Öffentlichkeit	4,0	4,4	3,1	2,5	2,1	1,9
N	1.769	406	455	442	424	258

In den meisten Fällen haben die Eigentümer*innen von den schwerwiegendsten Cyberangriffen erfahren (91,5 %), wobei dies in kleinen Unternehmen signifikant häufiger so stattfand (10-49 Besch.: 93,4 %) als in großen (ab 500 Besch.: 76,0 %; Tabelle 38). In der Regel wird dies

[301] Vgl. Hiscox (2018) Bei dem derzeitigen Wechselkurs von 1,11 USD pro EUR liegen die durchschnittlichen Gesamtkosten für Unternehmen ab zehn Beschäftigten, bei denen Kosten entstanden sind, in dieser Studie bei rund 18.700 USD.

[302] Vgl. Klahr et al. (2017).

[303] Bei dem derzeitigen Wechselkurs von 0,86 GBP pro EUR liegen die durchschnittlichen Gesamtkosten für Unternehmen ab zehn Beschäftigten, bei denen Kosten entstanden sind, in dieser Studie bei rund 14.500 GBP. Der Median liegt danach bei 860 GBP.

[304] Für große Unternehmen ab 250 Beschäftigten werden z.B. direkte Durchschnittskosten von 4.270 GBP (Median: 870 GBP) ausgewiesen. Im Vergleich liegen diese für Unternehmen mit 250-499 Beschäftigten in dieser Studie umgerechnet bei 19.700 GBP (Median: 1.290 GBP).

dadurch begründet sein, dass bei kleinen Unternehmen die Eigentümer*innen auch häufiger eine aktive Rolle in der Geschäftsführung spielen, als etwa bei großen Unternehmen. Von rund einem Fünftel (21,4 %) der berichteten schwerwiegendsten Vorfälle erfuhren die Geschäftspartner der Unternehmen, von 15,5 % wurden Kunden informiert. Auch dabei gibt es statistisch relevante Unterschiede zwischen den Beschäftigtengrößenklassen, insofern Geschäftspartner und Kunden in kleinen Unternehmen eher informiert wurden als in großen (10-49 Besch.: 23,1 % bzw. 16,8 %; ab 500 Besch.: 13,8 % bzw. 11,9 %). In 9,1 % der Fälle erlangten Versicherer und lediglich in 4,0 % die Öffentlichkeit Informationen über den schwerwiegendsten Vorfall. Auch wenn die Unterschiede zwischen den Beschäftigtengrößenklassen hierbei statistisch unbedeutend sind, ist bezüglich der Öffentlichkeit zumindest tendenziell zu erkennen, dass diese bei den Vorfällen kleiner Unternehmen eher informiert wird als bei den größeren.

Differenziert nach Cyberangriffsarten fallen vor allem manuelles Hacking und Defacing-Angriffe auf, von denen nicht-staatlichen Stellen vergleichsweise häufig Kenntnis erlangten (Tabelle 39). Zu den Cyberangriffsarten, von denen anteilig relativ selten Informationen an diese Stellen gelangten, zählen CEO-Fraud, Phishing und Angriffe mit sonstiger Schadsoftware: Bezogen auf die schwerwiegendsten Cyberangriffe erhielten bspw. Geschäftspartner*innen lediglich von 10,9 % bzw. 14,9 % der von CEO-Fraud und Phishing betroffenen Unternehmen Kenntnis, während sie von über einem Drittel der von (D)DoS betroffenen Unternehmen Informationen erhielten (37,1 %).

Tabelle 39 **Nicht-staatliche Stelle, die von dem Vorfall erfahren hat, nach Cyberangriffsart**
in Prozent; gewichtete Daten; Mehrfachantworten möglich

	Cyberangriffsart							
Nicht-staatliche Stelle	1	2	3	4	5	6	7	8
Kunden	16,7	23,2	10,1	29,0	35,2	**52,4**	6,3	9,9
Geschäftspartner	27,0	23,2	18,1	30,6	**37,1**	31,9	10,9	14,9
Versicherer	14,1	9,2	7,7	**25,8**	12,2	6,4	3,3	5,5
Eigentümer*innen der Unternehmen	96,0	95,8	89,9	96,8	84,0	**100,0**	84,4	90,3
Öffentlichkeit	3,5	4,9	3,6	22,6	5,3	**26,2**	0,8	1,1
N	395	142	413	62	131	45	127	462

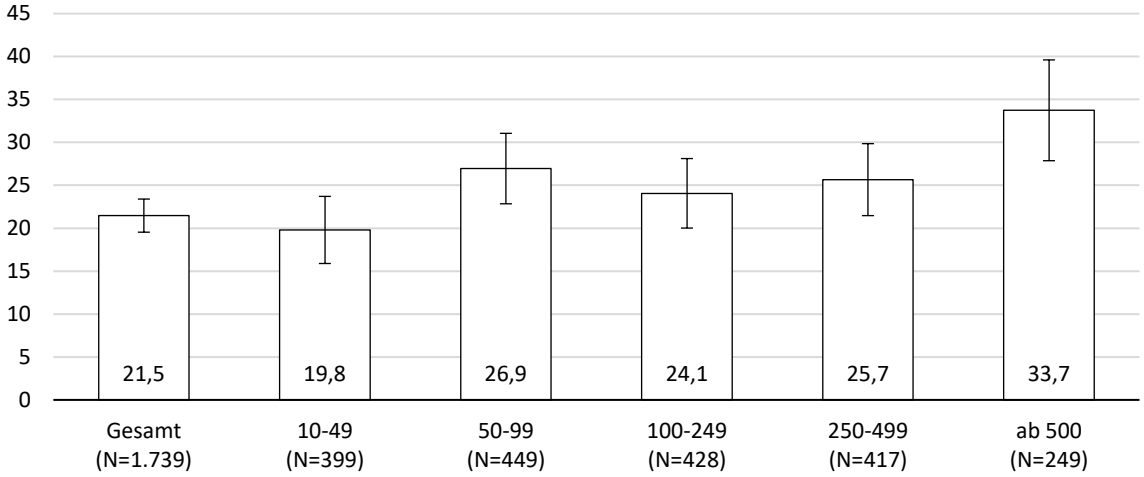
Cyberangriffsart: 1: Ransomware, 2: Spyware, 3: sonst. Schadsoftware, 4: manuelles Hacking, 5: (D)DoS, 6: Defacing, 7: CEO-Fraud, 8: Phishing
Hervorhebung: fett: größter Anteil je nicht-staatliche Stelle; grau hinterlegt: die drei größten Anteile je nicht staatliche Stelle

9.6.2 Kontakt mit staatlichen Stellen

Weiterhin bezogen auf den schwerwiegendsten Cyberangriff der letzten zwölf Monate wurden die Unternehmensvertreter*innen gefragt, an welche Stelle bzw. Behörde sich das Unternehmen wegen dieses Vorfalls gewendet hat. Folgende Antwortmöglichkeiten waren dazu vorgegeben: nächste Polizeidienststelle, auf Cybercrime spezialisierte Polizeidienststelle, Verfas-

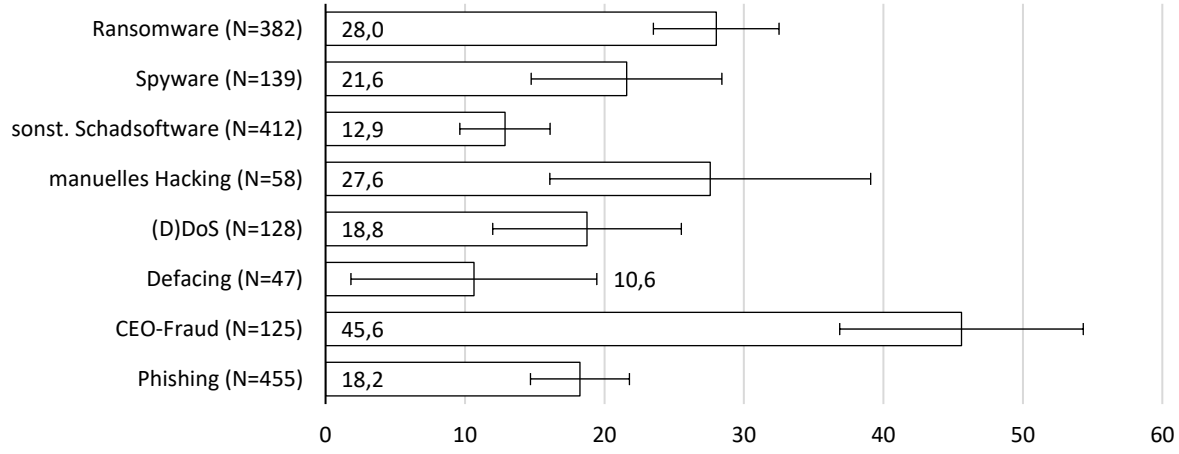
sungsschutz, Bundesamt für Sicherheit in der Informationstechnik (BSI), Landesdatenschutzbeauftragte*r und sonstige.[305] Dabei bleibt zunächst unberücksichtigt, ob die Unternehmen Strafanzeige erstattet haben oder nicht.[306]

Abbildung 64 **Betroffene Unternehmen mit Behördenkontakt nach Beschäftigtengrößenklassen**
in Prozent; gewichtete Daten; 95%-KI; nur Angaben zum schwerwiegendsten Cyberangriff



An mindestens eine dieser staatlichen Stellen hat sich gut einem Fünftel der von Cyberangriffen betroffenen Unternehmen gewendet (21,5 %), wobei der Anteil bei großen Unternehmen (ab 500 Besch.) signifikant höher liegt (33,7 %) als bei kleinen Unternehmen (10-49 Besch.: 19,8 %; Abbildung 64).

Abbildung 65 **Betroffene Unternehmen mit Behördenkontakt nach Cyberangriffsart**
in Prozent; gewichtete Daten; 95%-KI; nur Angaben zum schwerwiegendsten Cyberangriff



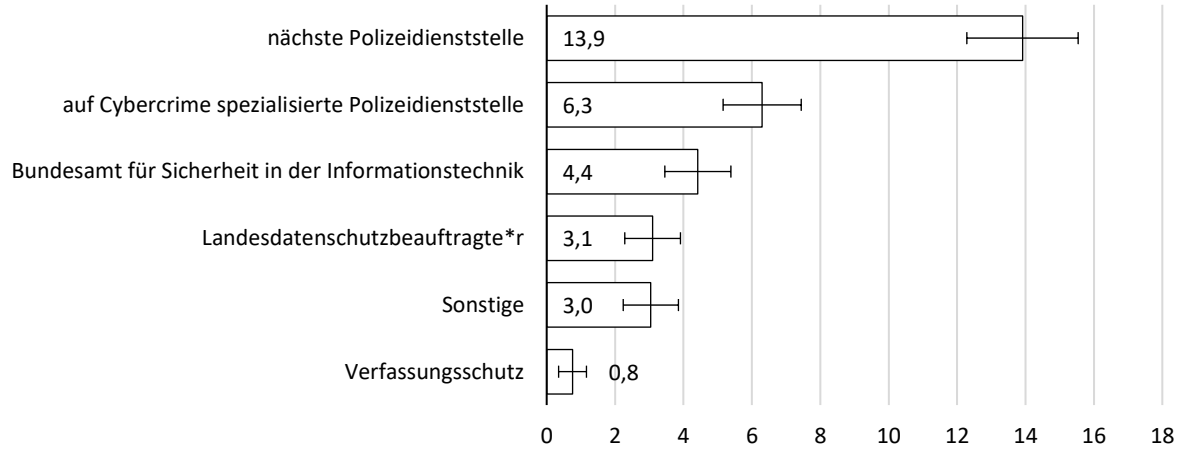
Unternehmen, die von CEO-Fraud als schwerwiegendstem Cyberangriff betroffen waren, wandten sich fast zur Hälfte (45,6 %) an mindestens eine staatliche Stelle (Abbildung 65). Am

[305] Die Kategorie „sonstige“ wurde bei der Befragung aus zeitökonomischen Gründen nicht freitextlich erhoben.

[306] Cybercrimedelikte fallen häufig in den Bereich der Offizialdelikte, d.h., dass diese von den Strafverfolgungsbehörden von Amts wegen verfolgt werden müssen, sobald sie davon Kenntnis erlangen. Bei Vergehen wie Datenveränderung nach § 303a StGB oder Datenausspähung nach § 202a StGB ist hingegen ein Strafantrag des anzeigenden Unternehmens erforderlich, damit die Strafverfolgungsbehörden die Ermittlung aufnehmen bzw. das Strafverfahren beginnen und vorantreiben kann. Das BSI, der Verfassungsschutz und der/die Landesdatenschutzbeauftragte zählen nicht zu den Strafverfolgungsbehörden.

seltensten wandten sich Unternehmen infolge eines Defacing-Angriffs (10,6 %) oder eines Angriffs mit sonstiger Schadsoftware (12,9 %) an die Behörden.

Abbildung 66 **Betroffene Unternehmen mit Behördenkontakt nach staatlichen Stellen**
in Prozent; gewichtete Daten; 95%-KI; Mehrfachangaben möglich; N=1.739



Aufgegliedert nach den verschiedenen Stellen zeigt sich, dass sich die betroffenen Unternehmen insgesamt mit einem Anteil von 13,9 % am häufigsten an die nächste Polizeidienststelle gewendet haben (Abbildung 66). Danach folgen auf Cybercrime spezialisierte Polizeidienststellen (6,3 %), das BSI (4,4 %), der*die Landesdatenschutzbeauftragte (3,1 %), Sonstige (3,0 %) und der Verfassungsschutz (0,8 %). Im Vergleich zwischen den Beschäftigtengrößenklassen gibt es keine statistisch relevanten Unterschiede, was auch mit der relativ geringen Fallzahl zusammenhängen dürfte. Große Unternehmen wenden sich allerdings zumindest tendenziell häufiger an (auf Cybercrime spezialisierte) Polizeidienststellen, das BSI und an den Verfassungsschutz als kleine Unternehmen.

Tabelle 40 **Betroffene Unternehmen mit Behördenkontakt nach staatlichen Stellen und Cyberangriffsart**
in Prozent; gewichtete Daten; Mehrfachantworten möglich

	Cyberangriffsart							
Staatliche Stelle	1	2	3	4	5	6	7	8
nächste Polizeidienststelle	21,5	11,5	8,5	19,3	4,7	6,3	**34,4**	9,2
auf Cybercrime spezialisierte Polizeidienststelle	7,9	10,8	2,2	1,7	8,6	0,0	**16,0**	4,4
Verfassungsschutz	1,8	**3,6**	0,0	0,0	0,0	0,0	0,0	0,2
Bundesamt für Sicherheit in der Informationstechnik	6,5	5,0	2,9	**17,5**	2,3	0,0	4,8	2,9
Landesdatenschutzbeauftragter	4,2	2,9	1,7	**17,2**	0,8	4,3	2,4	2,6
Sonstige	2,9	3,6	2,4	5,2	**7,0**	0,0	3,2	3,3
N	382	139	412	58	128	48	125	455

Cyberangriffsart: 1: Ransomware, 2: Spyware, 3: sonst. Schadsoftware, 4: manuelles Hacking, 5: (D)DoS, 6: Defacing, 7: CEO-Fraud, 8: Phishing
Hervorhebung: fett: größter Anteil je staatliche Stelle; grau hinterlegt: die drei größten Anteile je staatliche Stelle

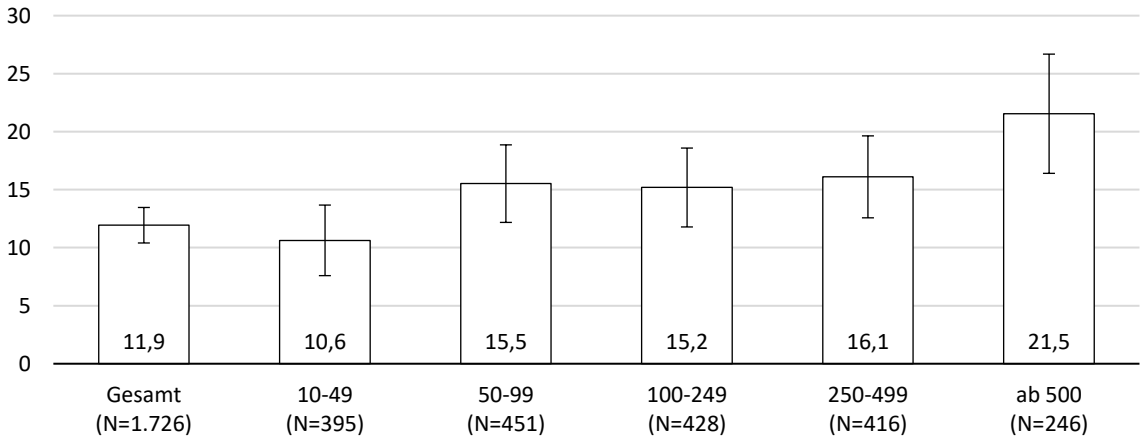
In Tabelle 40 sind die Anteile der Unternehmen differenziert nach Art des schwerwiegendsten Cyberangriffs dargestellt, die sich aufgrund dieser Angriffe an die verschiedenen staatlichen Stellen gewendet haben. Die nächsten Polizeidienststellen wurden z.B. gehäuft von Betroffenen

eines CEO-Fraud-Angriffs (34,4 %), eines Ransomware-Angriffs (21,5 %) oder von manuellem Hacking (19,3 %) angelaufen, aber vergleichsweise selten bei (D)DoS-Angriffen (4,7 %). Auf Cybercrime spezialisierte Polizeidienststellen wurden ebenfalls am ehesten von CEO-Fraud-Betroffenen kontaktiert (16,0 %), der Verfassungsschutz von Spyware-Betroffenen (3,6 %) und das BSI sowie der*die Landesdatenschutzbeauftragte von Betroffenen manuellen Hackings (17,5 % bzw. 17,2 %). In Hinblick auf die noch nicht genannten Cyberangriffsarten der sonstigen Schadsoftware, Defacing und Phishing wandten sich betroffene Unternehmen am ehesten an die nächste Polizeidienststelle (8,5 %, 6,3 % bzw. 9,2 %).

9.6.3 Anzeigeerstattung

Die Frage, ob für den schwerwiegendsten Cyberangriff der letzten zwölf Monate Strafanzeige erstattet wurde, bejahte insgesamt ein Anteil von 11,9 % (Abbildung 67). Damit kann die Annahme, dass es im Bereich der Cyberkriminalität gegen Unternehmen ein sehr großes Dunkelfeld gibt, bestätigt werden.[307] Die Anzeigequote der großen Unternehmen (ab 500 Besch.) ist mit 21,5 % etwa doppelt so hoch wie die von kleinen Unternehmen (10-49 Besch.: 10,6 %). Dies könnte u.a. damit zusammenhängen, dass es neben Unterschieden hinsichtlich der Betroffenheit durch verschiedene Cyberangriffsarten zwischen den Beschäftigtengrößenklassen auch Unterschiede bei den Anzeigequoten zwischen den Cyberangriffsarten gibt (Abbildung 68): So wurde z.B. die Cyberangriffsart CEO-Fraud, wovon große Unternehmen signifikant häufiger betroffen sind (Abbildung 37, S. 108), mit einem Anteil von 24,6 % am häufigsten angezeigt.[308] Neben CEO-Fraud werden auch Spyware- und Ransomware-Angriffe (19,7 % bzw. 15,7 %) sowie manuelles Hacking (19,4 %) vergleichsweise häufig angezeigt. Am größten scheint das Dunkelfeld bezogen auf Angriffe mit sonstiger Schadsoftware und bezogen auf Defacing mit Anzeigequote von 4,4 % bzw. 6,4 % zu sein.

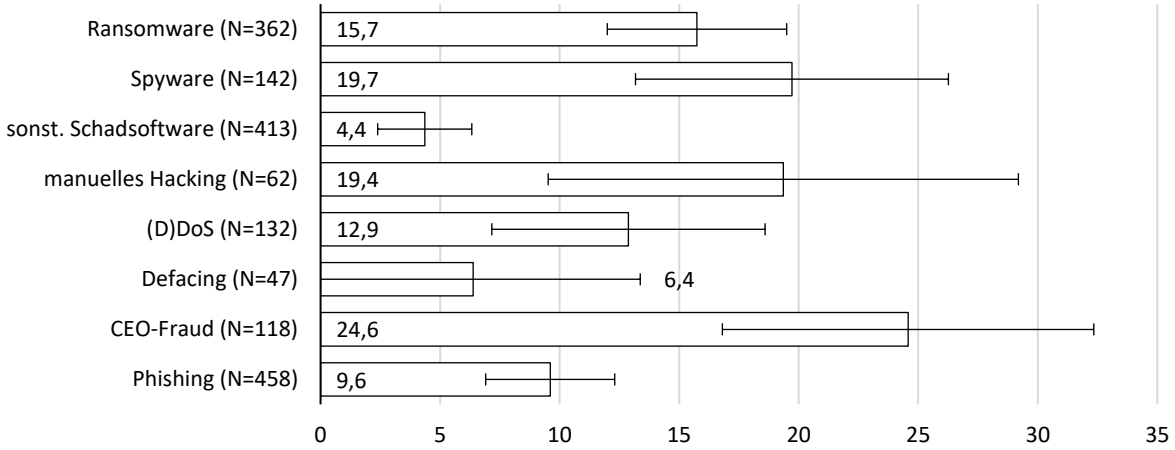
Abbildung 67 **Anzeigequote nach Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI; nur Angaben zum schwerwiegendsten Cyberangriff



[307] Es besteht zudem die Möglichkeit, dass die Anzeigequote von 11,9 % noch überschätzt ist, da sie sich nur auf die schwerwiegendsten Vorfälle bezieht und weniger schwere Vorfälle mutmaßlich noch seltener zur Anzeige gelangen.

[308] Warum dies so ist, bleibt dabei allerdings offen und kann an dieser Stelle nur vermutete werden. Mögliche erklärende Faktoren könnten z.B. die Art der betroffenen Daten, die Höhe der entstandenen Kosten, das Vorhandensein einer Cyberversicherung oder etwaige Vermutungen zu den Täter*innen sein. Zu Faktoren die das Anzeigeverhalten von Privatpersonen im Kontext von Cyberkriminalität beeinflussen siehe van de Weijer et al. (2019).

Abbildung 68 **Anzeigequote nach Cyberangriffsart**
in Prozent; gewichtete Daten; 95%-KI; nur Angaben zum schwerwiegendsten Cyberangriff



Die Unterschiede der nach Angriffsart differenzierten Anzeigequoten zwischen den Beschäftigtengrößenklassen sind bei den häufiger vorkommenden Angriffsarten Ransomware und Phishing statistisch nicht signifikant. Aufgrund der geringen Fallzahl insbesondere bei den Teilgruppen der seltener vorkommenden Angriffsarten bleibt ein weiterer Vergleich aus.

9.6.4 Nichtanzeigegründe

Wenn der schwerwiegendste Cyberangriff nicht angezeigt wurde, konnten die Unternehmensvertreter*innen die ausschlaggebenden Gründe dafür angeben. Zu den vorgegebenen Antwortmöglichkeiten zählten: „…weil ein Imageschaden zu befürchten war“, „…weil Arbeitsbehinderungen zu befürchten waren“, „…weil Behörden Einsicht in vertrauliche Daten fordern könnten“, „…fehlende Aussicht auf Ermittlungserfolg“, „…wusste nicht, an wen man sich dafür wenden muss“ und „Sonstiges“.[309]

Tabelle 41 **Nichtanzeigegründe nach Beschäftigtengrößenklassen**
in Prozent; gewichtete Daten; Mehrfachnennung möglich; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)

Warum haben Sie keine Strafanzeige erstattet?	Gesamt	Position innerhalb des Unternehmens			Beschäftigtengrößenklasse				
		Gschf.	IT	Sonst.	10-49	50-99	100-249	250-499	ab 500
…weil ein Imageschaden zu befürchten war	3,0	**4,9**	**1,6**	**1,1**	2,5	3,8	3,6	8,5	2,5
…weil Arbeitsbehinderungen zu befürchten waren	11,3	**18,4**	**7,5**	**2,1**	11,9	12,6	10,8	6,7	3,7
…weil Behörden Einsicht in vertrauliche Daten fordern könnten	5,0	**8,5**	**2,9**	**1,1**	5,1	4,9	2,4	6,1	2,5
…fehlende Aussicht auf Ermittlungserfolg	72,0	**77,7**	**74,3**	**47,9**	72,3	75,3	70,1	71,2	67,9
…wusste nicht, an wen man sich dafür wenden muss	20,7	**29,9**	**10,7**	**25,5**	**22,6**	**22,5**	**15,6**	**12,3**	**6,1**
Sonstiges	30,1	**23,9**	**30,6**	**46,8**	28,9	31,7	32,5	36,8	35,8
N	686	284	308	94	159	183	167	164	82

[309] Aus zeitökonomischen Gründen wurde die Kategorie „sonstiges“ bei dieser Frage nicht freitextlich erhoben. Zudem wurde aus eben diesen Gründen ein Split-Half-Verfahren angewendet, demzufolge nur die Hälfte der teilnehmenden Unternehmen diese Frage gestellt bekam (siehe dazu Abschnitt 5.4).

Dass die Befürchtungen eines Imageschadens, ein Grund für die Nichtanzeige waren, gaben lediglich 3,0 % der Unternehmensvertreter*innen an (Tabelle 41). Ebenso selten wurde die Befürchtung, dass Behörden Einsicht in vertrauliche Daten fordern könnten, genannt (5,0 %). In jedem neunten Unternehmen, die den schwerwiegendsten Cyberangriff nicht zur Anzeige gebracht haben, gab es Befürchtungen, dass durch die Ermittlungen die Arbeit im Unternehmen behindert werden würde (11,3 %). Etwa ein Fünftel gab als Nichtanzeigegrund an, nicht zu wissen, an wen man sich für eine Anzeige von Cyberangriffen wenden muss (20,7 %) und fast drei Viertel begründen dies mit fehlenden Aussichten auf einen Ermittlungserfolg (72,0 %). Die Kategorie „Sonstiges“ wurde mit 30,1 % ebenfalls vergleichsweise häufig genannt. Hier kann vermutet werden, dass ein erhöhter Arbeitsaufwand für die Anzeige, welcher einem geringen erwarteten Nutzen gegenübersteht, eingeflossen ist. Dieser wurde im Telefon-Interview nicht als einzelne Antwortmöglichkeit gegeben.

Zwischen den Beschäftigtengrößenklassen sind ledig bezüglich des Nichtwissens, an wen man sich für eine Anzeige wenden muss, statistisch relevante Unterschiede erkennbar: So wurde diese Antwort signifikant häufiger von den kleinen als von den großen Unternehmen gegeben (10-49 Besch.: 22,6 % bzw. 50-99 Besch.: 22,5 % vs. ab 500 Besch.: 6,1 %). Dies könnte mit den Positionen der Unternehmensvertreter*innen zusammenhängen, insofern das Nichtwissen in der Geschäftsführung diesbezüglich ausgeprägter zu sein scheint als bei den IT-Beschäftigten (29,9 % vs. 10,7 %) und die Geschäftsführung vor allem bei kleinen Unternehmen befragt wurde. Mit Ausnahme der fehlenden Aussicht auf Ermittlungserfolg, als Grund für die Nichtanzeige, den Geschäftsführung und IT-Beschäftigte etwa gleich häufig angeben, äußern die Geschäftsführungen alle übrigen Gründe häufiger als IT-Beschäftigte. Insbesondere die Befürchtung von Arbeitsbehinderungen scheint einen relativ hohen Einfluss auf die Entscheidung für oder gegen eine Anzeige in dieser Gruppe zu haben.

Tabelle 42 **Betroffene Unternehmen mit Behördenkontakt nach staatlichen Stellen und Cyberangriffsart**
in Prozent; gewichtete Daten; Mehrfachantworten möglich

	Cyberangriffsart							
Nichtanzeigegrund	1	2	3	4	5	6*	7	8
…weil ein Imageschaden zu befürchten war	4,4	12,2	0,6	6,5	0,0	0/18	2,6	3,2
…weil Arbeitsbehinderungen zu befürchten waren	13,1	12,5	5,2	19,4	13,7	1/18	16,2	11,8
…weil Behörden Einsicht in vertrauliche Daten fordern könnten	4,4	10,4	0,6	32,3	0,0	0/18	0,0	5,9
…fehlende Aussicht auf Ermittlungserfolg	**82,5**	**75,0**	**64,4**	**96,8**	**72,0**	**13/18**	**60,5**	**68,3**
…wusste nicht, an wen man sich dafür wenden muss	21,2	27,1	21,3	16,1	29,4	2/18	18,4	18,3
Sonstiges	35,8	8,3	40,2	19,4	18,0	6/18	31,6	27,4
N	137	48	174	31	51	18	38	186

Cyberangriffsart: 1: Ransomware, 2: Spyware, 3: sonst. Schadsoftware, 4: manuelles Hacking, 5: (D)DoS, 6: Defacing, 7: CEO-Fraud, 8: Phishing
*) Aufgrund der geringen Fallzahl Angabe in absoluten Zahlen
Hervorhebung: fett: größter Anteil je Cyberangriffsart; grau hinterlegt: die drei größten Anteile je Cyberangriffsart

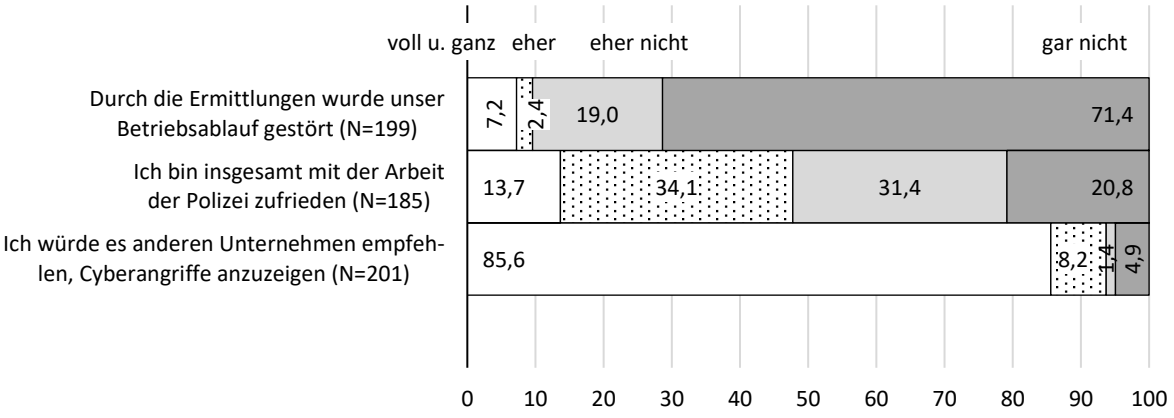
Im Vergleich der Nichtanzeigegründe nach Cyberangriffsart ist zunächst auffällig, dass die fehlende Aussicht auf einen Ermittlungserfolg viele Unternehmen abhielt, den schwerwiegendsten Vorfall der letzten zwölf Monate anzuzeigen (Tabelle 42). Dennoch scheint dies bei den Angriffsarten manuelles Hacking und Ransomware stärker der Fall zu sein (96,8 % bzw. 82,5 %)

als bei Angriffen mit sonstiger Schadsoftware oder CEO-Fraud (64,4 % bzw. 60,5 %). Bezogen auf manuelles Hacking gab ein signifikant größerer Anteil die Befürchtung an, dass die Behörden Einsicht in vertrauliche Daten fordern könnten (32,3 %), als bei Unternehmen, die von anderen Angriffsarten betroffen waren. Demgegenüber scheint das Nichtwissen, an wen man sich für die Anzeige wenden muss, bei manuellem Hacking eine tendenziell kleinere Rolle zu spielen (16,1 %) als bei den anderen Angriffsarten, insbesondere bei (D)DoS-Angriffen (29,4 %). Die z.T. sehr häufig genannte Kategorie „Sonstiges“ (z.B. bei Ransomware-Angriffen oder Angriffen mit sonstiger Schadsoftware: 35,8 % bzw. 40,2 %) verweist auf weitere Gründe, die bei der Entscheidung zum Nichtanzeigen von Cyberangriffen eine Rolle spielen und die in zukünftiger Forschung in den Blick genommen werden sollten.

9.7 Bewertung der Strafverfolgungsbehörden

Für die Bewertung der Arbeit der Polizei bzw. der Strafverfolgungsbehörden in den Fällen, in denen der schwerwiegendste Cyberangriff der letzten zwölf Monate angezeigt wurde, konnten die Befragten auf einer vierstufigen Skala von 1 „stimme voll und ganz zu“ bis 4 „stimme gar nicht zu“ ihre Einschätzung zu folgenden Aussagen treffen: „Durch die Ermittlungen wurde unser Betriebsablauf gestört“, „Ich bin insgesamt mit der Arbeit der Polizei zufrieden“ sowie „Ich würde es anderen Unternehmen empfehlen, Cyberangriffe anzuzeigen“.

Abbildung 69 **Bewertung der Arbeit der Strafverfolgungsbehörden**
in Prozent; gewichtete Daten; nur Unternehmen, die den schwerwiegendsten Vorfall anzeigten



Lediglich ein Zehntel der anzeigenden Unternehmen (9,6 %) stimmte der Aussage eher/voll und ganz zu, dass die Ermittlungen den Betriebsablauf gestört haben (Abbildung 69). Über zwei Drittel konnten dem gar nicht (71,4 %) und ein weiteres Fünftel eher nicht zustimmen (19,0 %). Voll und ganz oder eher zufrieden mit der Arbeit der Polizei zeigte sich knapp die Hälfte (47,7 %). Dennoch würden 93,7 % der Anzeigenden anderen Unternehmen die Anzeige von Cyberangriffen empfehlen. Nur ein kleiner Anteil von 4,9 % würde dies gar nicht tun.

Statistisch bedeutsame Unterschiede gibt es zu diesen Fragen mit einer Ausnahme weder zwischen den Beschäftigtengrößenklassen noch zwischen den Positionen der befragten Unternehmensvertreter*innen. Dies hängt z.T. auch mit der geringen Fallzahl zusammen, womit auch eine Differenzierung der Antworten nach Cyberangriffsart nicht sinnvoll möglich ist. Die Ausnahme betrifft die Zustimmung zur Empfehlung der Anzeige von Cyberangriffen: Während fast

alle Beschäftigten im Bereich IT & Informationssicherheit (98,0 %; N=101) anderen Unternehmen die Anzeige von Cyberangriffen (eher) empfehlen würden, sind es innerhalb der Geschäftsführungen mit 87,3 % (N=79) etwas weniger.[310]

Danach gefragt, ob in diesem angezeigten schwerwiegendsten Cyberangriff die Täter*innen ermittelt werden konnten, antwortete ein kleiner Anteil von 7,7 % (N=201) mit „ja“. In den meisten Fällen (92,3 %) blieb ein Ermittlungserfolg aus.

9.8 Zwischenresümee

Die Detailangaben zum schwerwiegendsten Cyberangriff der letzten zwölf Monate lassen sich folgendermaßen zusammenfassen: Angriffe mit Ransomware, sonstiger Schadsoftware und Phishing-Angriffe wurden am häufigsten als schwerwiegendste Cyberangriffe berichtet. Bei einem Viertel der Unternehmen waren durch den schwerwiegendsten Cyberangriff unterschiedliche digitale Daten betroffen, insofern diese gelöscht, manipuliert, gestohlen/kopiert oder verschlüsselt wurden. Direkte Kosten infolge dieses Angriffs entstanden bei 70,0 % der Unternehmen insbesondere im Zusammenhang mit Sofortmaßnahmen zur Abwehr und Aufklärung, mit der Wiederherstellung/ Wiederbeschaffung sowie mit externer Beratung. Von Schadensersatz/ Strafen und abgeflossenen Geldern wurden hingegen relativ selten berichtet.

Die Spannbreite der berichteten unmittelbaren Gesamtkosten infolge der schwerwiegendsten Cyberangriffe ist sehr breit, reicht von 10 EUR bis 2 Mio. EUR und liegt im Durschnitt bei rund 16.900 EUR. Allerdings lagen die berechneten Gesamtkosten bei über drei Viertel der Unternehmen (78,0 %) unter 5.000 EUR und nur sehr selten bei 50.000 EUR und mehr (3,4 %). Die Verteilung kann bei einem Gesamtkostenwert von 1.000 EUR in zwei gleich große Hälften geteilt werden (Median). Zu den Kostenpositionen mit einem vergleichsweise hohen Median von 2.000 EUR zählen abgeflossene Gelder und Betriebsunterbrechung. Zu den Angriffsarten, die im Median die höchsten Kosten verursacht haben, zählen Ransomware-Angriffe (1.300 EUR) und manuelles Hacking (2.800 EUR).[311]

Lediglich 11,9 % der Unternehmen zeigten den berichteten schwerwiegendsten Cyberangriff polizeilich an, wobei größere Unternehmen häufiger Anzeige erstatteten als kleinere (ab 500 Besch: 21,5 % vs. 10-49 Besch.: 10,6 %). Zu den am häufigsten angezeigten Angriffsarten zählen CEO-Fraud (24,6 %), Spyware (19,7 %) und manuelles Hacking (19,4 %). Demgegenüber wurden Angriffe mit sonstige Schadsoftware und Defacing vergleichsweise selten angezeigt (4,4 % bzw. 6,4 %).

Die fehlende Aussicht auf einen Ermittlungserfolg (72,0 %) und die Unsicherheit darüber, an wen genau man sich für eine Anzeige wenden muss (20,7 %) sind die häufigsten Nichtanzeigegründe. Daneben wurden von 30,1 % der Befragten sonstige Gründe angegeben, zu denen vermutlich auch die häufig nur geringen Schäden und damit verbundenen direkten Kosten zählen. Kaum eine Rolle scheinen hingegen Befürchtungen von Imageschäden, Einsichtnahmen in vertrauliche Daten oder Arbeitsbehinderungen zu spielen.

---

[310] Die Unternehmensvertreter*innen in sonstigen Positionen stimmten alle der Aussage zu (21 von 21).

[311] Schäden und Kosten durch Reputationsverluste oder mittelbar bzw. stark zeitversetzt wirkende Effekte, wie z.B. Marktanteilsverluste infolge gestohlener Konstruktionspläne und nachgeahmter Produkte, wurden in dieser Studie nicht untersucht.

Von den Unternehmen, die Anzeige erstattet haben, ist lediglich knapp die Hälfte (47,8 %) insgesamt (eher) zufrieden mit der polizeilichen Arbeit. Dies dürfte damit zusammenhängen, dass nur bei 7,7 % der Anzeigen Täter*innen ermittelt werden konnten. Dennoch würde es die Mehrzahl von 93,8 % anderen Unternehmen empfehlen Cyberangriffe anzuzeigen. Lediglich bei zehn von 100 Unternehmen kam es im Zuge der Ermittlung zu Störungen im Betriebsablauf (9,6 %).

Neben diesen Detailfragen zum schwerwiegendsten Cyberangriff der letzten zwölf Monate wurden die Befragten gebeten, das Vorhandensein der in Abschnitt 5.3 dargestellten IT-Sicherheitsmaßnahmen zeitlich einzuordnen, d.h. anzugeben, ob eine genutzte IT-Sicherheitsmaßnahme schon vor oder erst nach dem schwerwiegendsten Vorfall vorhanden war. Auf dieser Grundlage soll im folgenden Kapitel überprüft werden, ob von diesen vorher vorhandenen Maßnahmen eine schützende Wirkung ausging.

10 MÖGLICHE SCHUTZFAKTOREN

Während in Kapitel 8 Unternehmensmerkmale analysiert wurden, die in Zusammenhang mit einer häufigeren Betroffenheit von Cyberangriffen in den letzten zwölf Monaten stehen und somit als potentielle Risikofaktoren angesehen werden können,[312] wird in diesem Kapitel nach IT-Sicherheitsmaßnahmen gesucht, die im Zusammenhang mit einer geringeren Betroffenheit von Cyberangriffen in den letzten zwölf Monaten stehen und damit als potentielle Schutzfaktoren in Frage kommen.

Beim Vergleich der Anteile betroffener Unternehmen nach vorhandenen IT-Sicherheitsmaßnahmen ist zu berücksichtigen, dass diese möglicherweise erst nach einem schädigenden Ereignis umgesetzt wurden. Deshalb wurde bei der Befragung zusätzlich erhoben, ob die angegebenen IT-Sicherheitsmaßnahmen gegebenenfalls schon vor oder eben erst nach dem Cyberangriff vorhanden waren.

Da diese zeitliche Einordnung der IT-Sicherheitsmaßnahmen nicht für alle erlebten Cyberangriffe der letzten zwölf Monate erfasst werden konnte, sondern lediglich für den als schwerwiegendsten Cyberangriff berichteten Vorfall, bezieht sich die folgende Auswertung anders als bei den potentiellen Risikofaktoren nicht auf die Jahresprävalenz. Stattdessen können nur die Anteile betroffener Unternehmen hinsichtlich vorhandener IT-Sicherheitsmaßnahmen verglichen werden, die die Detailfragen zum schwerwiegendsten Cyberangriff beantwortet haben (37,8 %; N=4.723).[313]

Unternehmen, die bestimmte IT-Sicherheitsmaßnahmen erst nach dem schwerwiegendsten Vorfall eingeführt haben, wurden zu den betroffenen Unternehmen ohne diese Maßnahme gezählt, was insbesondere bei organisatorischen IT-Sicherheitsmaßnahmen häufiger der Fall war als bei den technischen: So führten z.B. 12,8 % der betroffenen Unternehmen schriftlich fixierte Richtlinien zur Informations- bzw. IT Sicherheit erst nach dem berichteten schwerwiegendsten Cyberangriff ein (Abbildung 70).

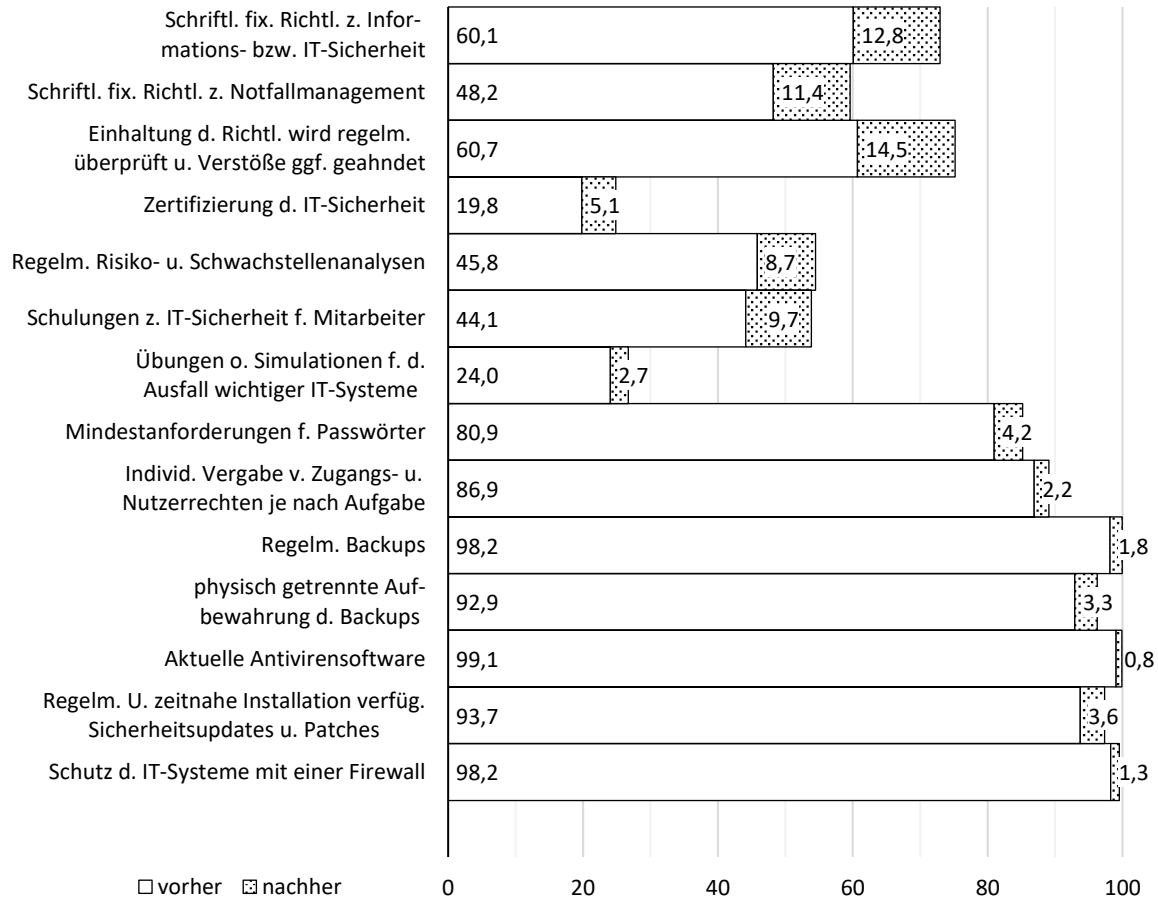
Ähnlich wie bei der Suche nach potentiellen Risikofaktoren wird das Vorhandensein von IT-Sicherheitsmaßnahmen zum Anteil der betroffenen Unternehmen in Beziehung gesetzt und dabei die Beschäftigtengrößenklasse kontrolliert. So lässt sich überprüfen, ob ein Zusammenhang ggf. in allen oder lediglich in einzelnen Größenklassen besteht. Wenn der Anteil der betroffenen Unternehmen mit einer bestimmten IT-Sicherheitsmaßnahme deutlich kleiner ausfällt als der Anteil der betroffenen Unternehmen ohne sie, dann deutet dies auf deren präventive Wirkung hin.

---

[312] Dazu zählen neben der Beschäftigtengrößenklasse und der Branche vor allem die Anzahl der Standorte in Deutschland, das Vorhandensein mindestens eines Auslandsstandortes, die Exporttätigkeit sowie das Vorhandensein besonderer Produkte/ Herstellungsverfahren/ Dienstleistungen bzw. besonderer Reputationen/ Kundenkreise.

[313] Unternehmen, die mindestens einen Cyberangriff in den letzten zwölf Monaten erlebt haben, die Detailfragen zum schwerwiegendsten Vorfall aber nicht beantworteten, wurden bei diesem Vergleich ausgeschlossen. Dadurch reduzierten sich die zugrundeliegende Fallzahl und der Anteil der Betroffenen im Vergleich zur Jahresprävalenzrate für die erhobenen Cyberangriffe insgesamt.

Abbildung 70 **Vorhandene IT-Sicherheitsmaßnahmen vor bzw. erst nach dem schwerwiegendsten Cyberangriff**
in Prozent; gewichtete Daten; nur betroffene Unternehmen

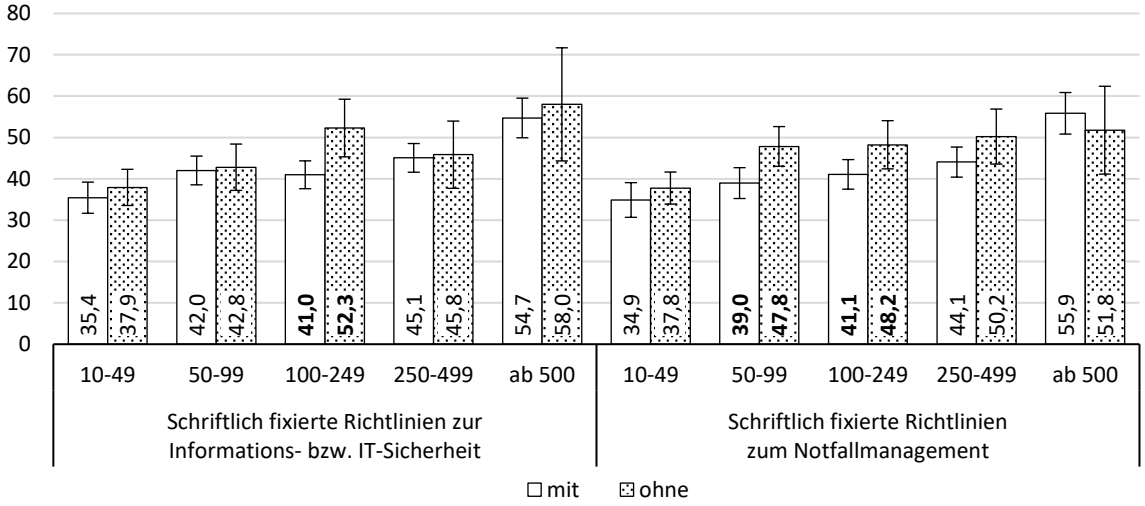


10.1 Organisatorische Maßnahmen

Auch wenn schriftlich fixierte Richtlinien zur Informations-/IT-Sicherheit oder zum Notfallmanagement durch ihr bloßes Vorhandensein keine präventive Wirkung entfalten können, stehen sie für eine Auseinandersetzung mit dem Thema innerhalb der Unternehmen und zumindest teilweise für eine gelebte Praxis, die einen Unterschied machen könnte.

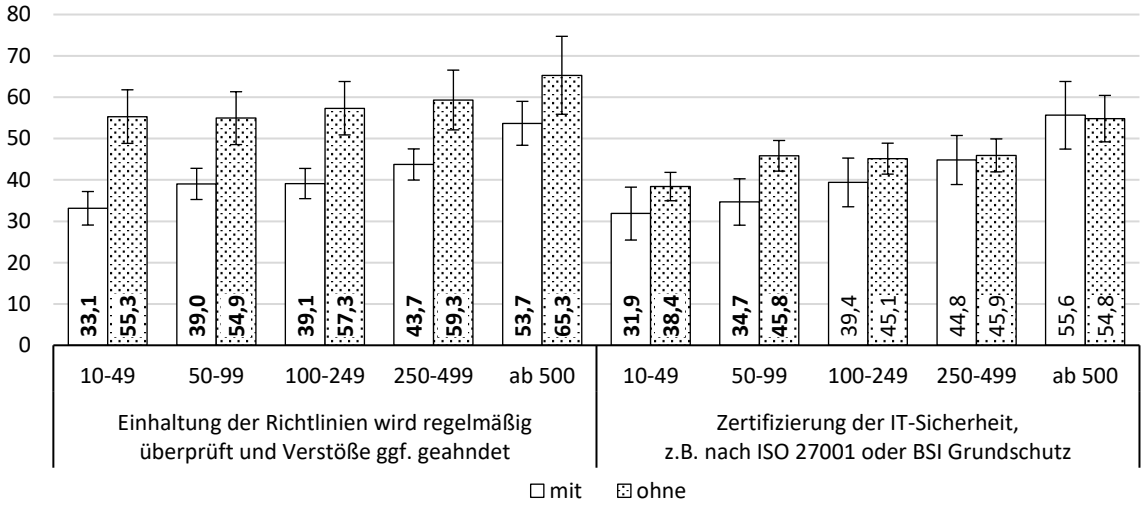
Tendenziell liegen die Anteile betroffener Unternehmen mit solchen Richtlinien erwartungsgemäß unter den Anteilen der Unternehmen, die keine hatten oder erst nach dem schwerwiegendsten Cyberangriff (Abbildung 71). Statistisch bedeutsam ist der Zusammenhang in Hinblick auf Richtlinien zur Informations- bzw. IT-Sicherheit bei Unternehmen mit 100 bis 249 Beschäftigten und hinsichtlich der Richtlinien zum Notfallmanagement bei Unternehmen mit 50 bis 99 und 100 bis 249 Beschäftigten: Während rund die Hälfte ohne derartige Richtlinien von mindestens einem Vorfall betroffen war, liegen die Anteile bei Unternehmen mit Richtlinien bei etwa zwei Fünftel.

Abbildung 71 **Anteil der Betroffenen mit und ohne Richtlinien zu IT-Sicherheit bzw. Notfallmanagement**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



Dass es darauf ankommt solche Richtlinien umzusetzen und im Unternehmen „zu leben", zeigen die in allen Beschäftigtengrößenklassen signifikant niedrigeren Anteile betroffener Unternehmen, die diese Richtlinien regelmäßig überprüfen und Verstöße ggf. ahnden (Abbildung 72). Am deutlichsten ist der Unterschied zu Unternehmen, die dies nicht taten in der Gruppe der kleinen Unternehmen (10-49 Besch.: 33,1 % vs. 55,3 % Betroffene). Die Zertifizierung der IT-Sicherheit steht ebenfalls in einem negativen Zusammenhang mit der Betroffenheit und erweist sich bei den kleineren Unternehmen als statistisch bedeutsam (10-49 Besch.: 31,9 % vs. 38,4 % und 50-99 Besch.: 34,7 % vs. 45,8 % Betroffene).

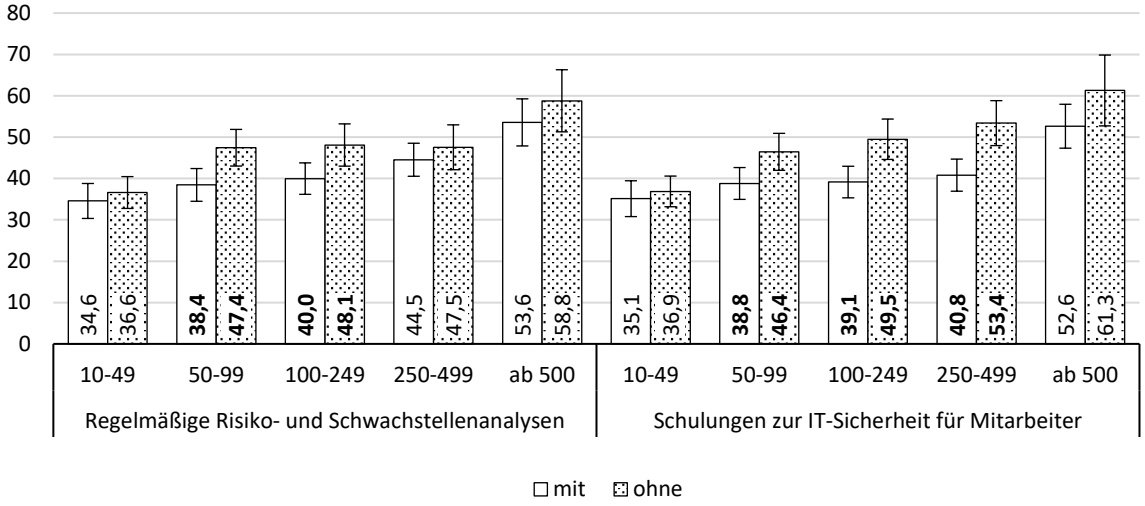
Abbildung 72 **Anteil der Betroffenen mit und ohne Richtlinienüberprüfung bzw. Zertifizierung**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



Regelmäßige Risiko- und Schwachstellenanalysen stehen ebenfalls in Zusammenhang mit geringeren Betroffenheitsanteilen und können demnach über die mit ihnen verbundenen Maßnahmen einen präventiven Beitrag leisten (Abbildung 73). Das zeigt sich tendenziell in allen Beschäftigtengrößenklassen und statistisch signifikant in den Gruppen mit 50 bis 99 und 100 bis 249 Beschäftigten (38,4 % vs. 47,4 % bzw. 40,0 % vs. 48,1 % Betroffene). Noch etwas größer scheint der Einfluss von Schulungen zur IT-Sicherheit für Beschäftigten zu sein, der sich in den mittelgroßen Unternehmen (50-99, 100-249 und 250-499 Besch.) als signifikant erweist: In der

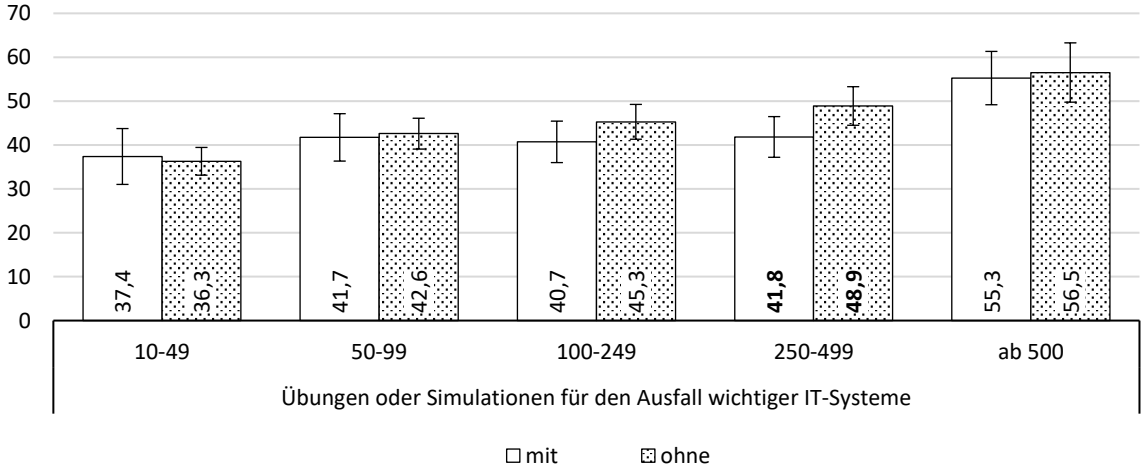
Klasse 250 bis 499 Beschäftigte war z.B. ein Anteil von 40,8 % mit und 53,4 % ohne Schulungsmaßnahmen von mindestens einem Cyberangriff im Vorjahr betroffen.

Abbildung 73 **Anteil der Betroffenen mit und ohne Risiko-/Schwachstellenanalysen bzw. Schulungen**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme stehen bei Unternehmen mit 250 bis 499 Beschäftigten in einem negativen Zusammenhang zur Betroffenheit, insofern der Anteil betroffener Unternehmen, die Übungen und Simulationen durchführen etwa 8 Prozentpunkt unter dem Anteil der Unternehmen liegt, die diese nicht vorsehen (41,8 % vs. 48,9 %; Abbildung 74).

Abbildung 74 **Anteil der Betroffenen mit und ohne Übungen/Simulationen für den Ausfall wichtiger IT-Systeme**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



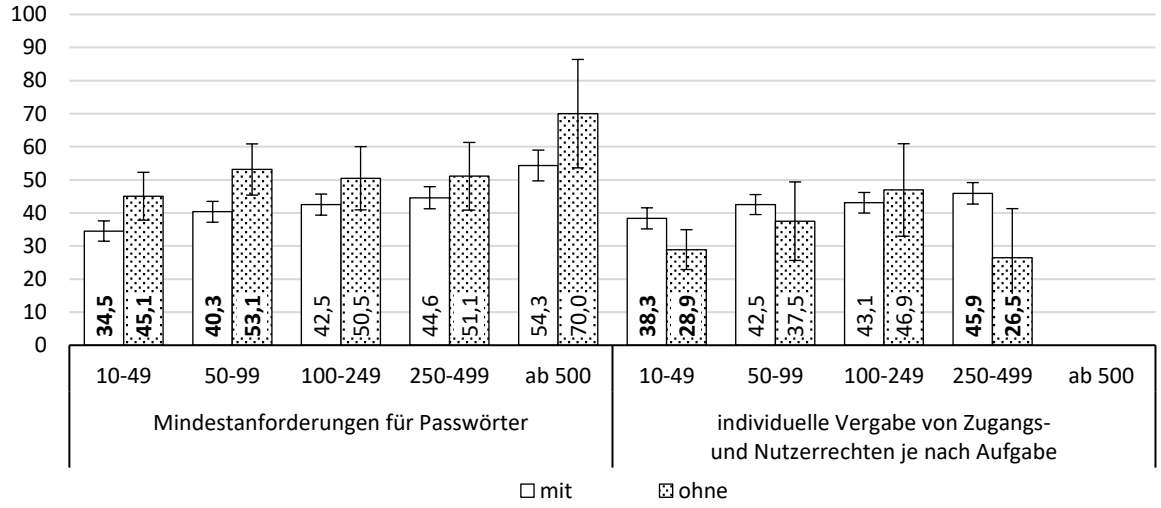
10.2 Technische Maßnahmen

Der Einfluss technischer IT-Sicherheitsmaßnahmen lässt sich im Vergleich zu den organisatorischen kaum aufzeigen, da die Varianz der Antworten der Unternehmen häufig zu gering ausfiel. Wie bereits dargestellt, gaben fast alle Unternehmen an, regelmäßig und zeitnah verfügbare Sicherheitsupdates und Patches zu installieren, Backups durchzuführen einen Firewall- oder Antivirenschutz zu haben. Die Gruppe der Unternehmen, die diese Maßnahmen bisher nicht

umsetzte, ist für einen sinnvollen Vergleich oftmals zu klein, insbesondere dann, wenn weitere Variablen wie die Beschäftigtengrößenklasse kontrolliert werden.

In Hinblick auf das Vorhandensein von Mindestanforderungen für Passwörter[314] lässt sich der Vergleich noch in allen Beschäftigtengrößenklassen durchführen und erkennen, dass Unternehmen mit Mindestanforderungen für Passwörter seltener von Cyberangriffen im Vorjahr betroffen waren (Abbildung 75). Signifikant erscheint der Unterschied in der Gruppe der Unternehmen mit 10 bis 49 Beschäftigten (34,5 % vs. 45,1 %) sowie mit 50-99 Beschäftigten (40,3 % vs. 53,1 %). Ein deutlich sichtbarer Unterschied ist auch bei den großen Unternehmen (ab 500 Besch.: 54,3 % vs. 70,0 %) zu sehen, da aber die Gruppe ohne Mindestanforderungen in dieser Größenklasse sehr klein ist (N=30) kann bei einer statistischen Irrtumswahrscheinlichkeit von 5 % nicht ausgeschlossen werden, dass dieser Unterschied über die Stichprobenziehung zufällig zustande gekommen ist.

Abbildung 75 Anteil der Betroffenen mit und ohne Mindestanforderungen f. PW bzw. indiv. Zugangs-/Nutzerrechten
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



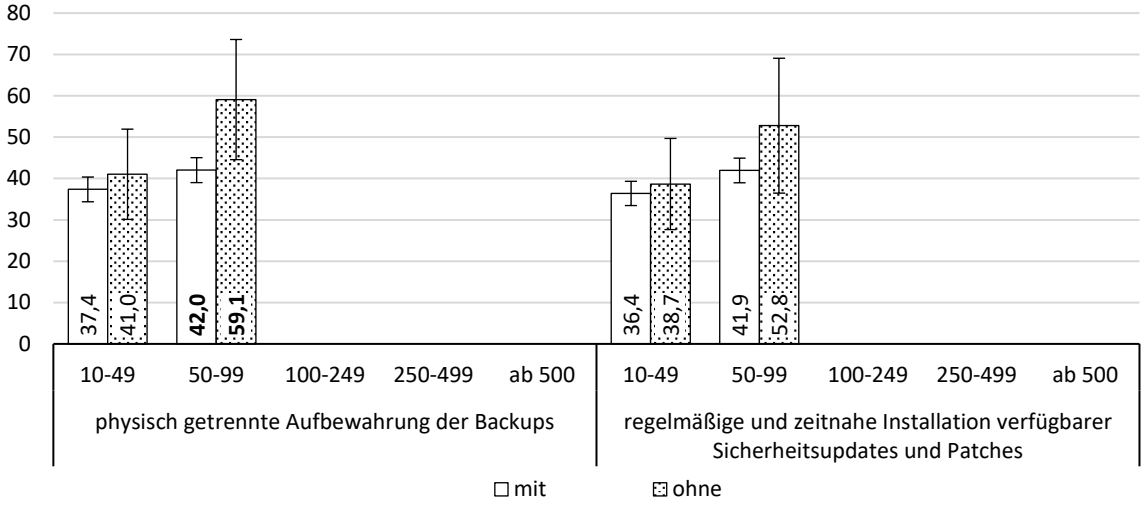
Ein kontraintuitives Ergebnis zeigt sich bezüglich der individuellen Vergabe von Zugangs- und Nutzerrechten je nach Aufgabe der Beschäftigten (Abbildung 75). Diese Maßnahme, die den ungehinderten Zugang aller Beschäftigten in sämtliche Bereiche des IT-Systems des Unternehmens beschränken und es damit internen wie externen Angreifern z.B. schwerer machen soll, sich innerhalb des Netzwerkes zu bewegen und an relevante Daten zu gelangen, steht in einem signifikant positiven Zusammenhang mit der Betroffenheit von Unternehmen mit 10 bis 49 sowie mit 250 bis 499 Beschäftigten. Vor dem Hintergrund kleiner Fallzahlen bei den Unternehmen ohne individuelle Rechtevergabe könnte dieser Unterschied mit einem geringeren Grad der Digitalisierung erklärt werden, der das Risiko von Cyberangriffen bei diesen Unternehmen unabhängig von IT-Sicherheitsmaßnahmen verringert. Zum anderen sind insbesondere bei den betroffenen Unternehmen mit 250 bis 499 Beschäftigten Unterschiede hinsichtlich der Cyberangriffsarten zu erkennen: Diejenigen, die in dieser Größenklasse individuelle Zugangs- und Nutzerrechte vor dem schwerwiegendsten Cyberangriff vergeben hatten, waren häufiger von Angriffen im Bereich Social Engineering (CEO-Fraud und Phishing) betroffen, gegen die beschränkte Zugangs- und Nutzerrechte kaum präventiv wirken können. Insofern spricht vieles

[314] Siehe dazu Fn. 235 (S. 77).

für einen Scheinzusammenhang zwischen individueller Rechtevergabe und höherer Betroffenheitsrate, der durch andere, nicht betrachtete Variablen verursacht wird.

Da die Gruppe der Unternehmen ohne physisch getrennte Aufbewahrung von Backups ebenfalls sehr klein ist, lassen sich lediglich die Betroffenheitsraten der unteren beiden Beschäftigtengrößenklassen sinnvoll miteinander vergleichen, wobei ein signifikanter Unterschied in der Größenklasse 50 bis 99 Beschäftigte erkennbar ist (Abbildung 76): Unternehmen mit physisch getrennt aufbewahrten Backups sind demnach seltener von Cyberangriffen betroffen als Unternehmen, die diese Maßnahme nicht umsetzen (42,0 % vs. 59,1 %). Da Backups und deren Aufbewahrung vorwiegend Maßnahmen zu Schadensbegrenzung sind[315] und nicht der Prävention von Angriffen dienen, dürften andere damit verbundene präventive Maßnahmen für den beschriebene Zusammenhang verantwortlich sein.

Abbildung 76 **Anteil der Betroffenen mit und ohne phys. getrennte Backups bzw. regelm. Updates/Patches**
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



Bezüglich der unteren beiden Beschäftigtengrößenklassen können die Betroffenheitsraten der Unternehmen mit und ohne regelmäßige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches verglichen werden, wobei allenfalls tendenzielle Unterschiede in erwarteter Richtung sichtbar sind (Abbildung 76).

Die verbliebenen technischen IT-Sicherheitsmaßnahmen (aktuelle Antivirensoftware, regelmäßige Backups und Schutz der IT-Systeme mit einer Firewall) lassen sich wie bereits angedeutet aufgrund der fehlenden Varianz nicht sinnvoll mit der Betroffenheitsrate in Beziehung setzen.

Bezogen auf den Firewall-Schutz wurde differenzierter erhoben, ob es sich um eine einfache Firewall, d.h. Paketfilterung nach Quell- und Zieladresse durch Software-Firewall oder Router auf Netzwerkebene, oder um eine erweiterte Firewall, d.h. zusätzliche Überwachung und Filterung nach Paketinhalt auf Anwendungsebene, handelt. Auch wenn der Anteil der Befragten, die mit dieser Unterscheidung nichts anzufangen wusste, relativ groß ist,[316] können diese beiden Unternehmensgruppen hinsichtlich der Betroffenheitsrate miteinander verglichen werden. Dabei kann erwartet werden, dass Unternehmen mit erweiterter Firewall aufgrund des höheren

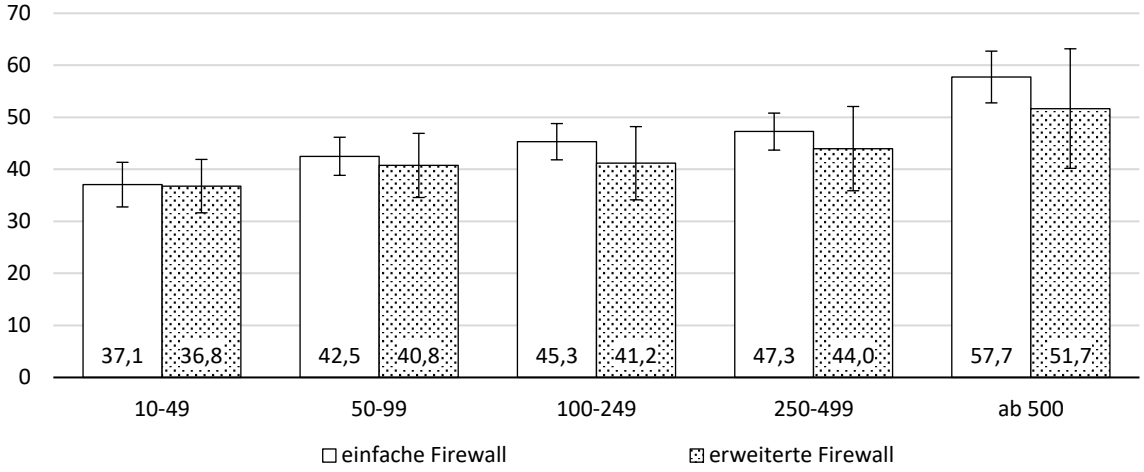
[315] Neben der regelmäßigen Backupsicherung und deren physisch getrennter Aufbewahrung ist im Schadensfall entscheidend, dass die Wiederherstellung der Daten (Restore) zeitnah funktioniert.

[316] Siehe Abbildung 21 in Abschnitt 5.3.2.

technischen Schutzes seltener von Cyberangriffe betroffen sind, auf die aktiv reagiert werden muss.

Abbildung 77 **Anteil der Betroffenen nach Art der Firewall**

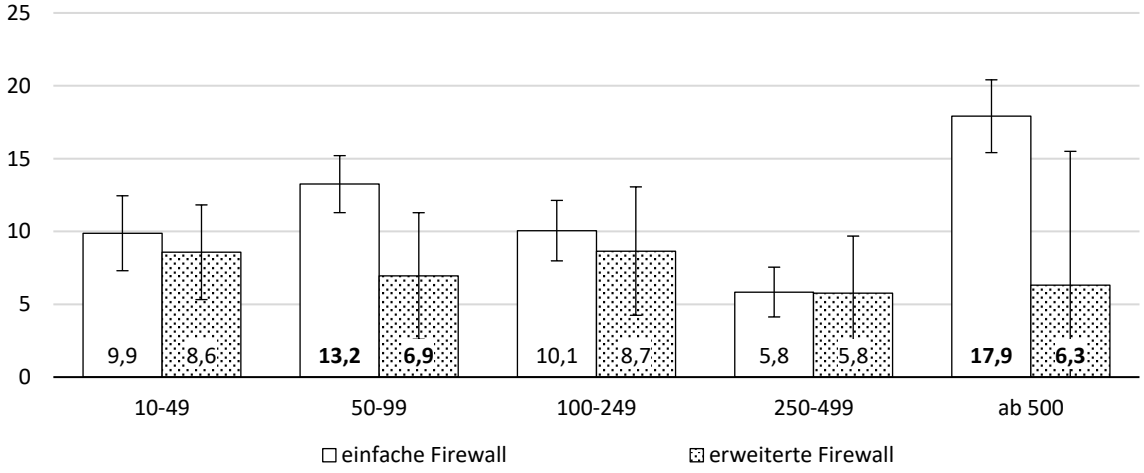
in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



Bezogen auf alle Cyberangriffe insgesamt zeigen sich zwar kleine Unterschiede in erwarteter Richtung, die aber statistisch nicht bedeutsam sind (Abbildung 77). Da eine solche technische Maßnahme bei Angriffen im Bereich Social Engineering kaum Wirkung entfalten kann, wird der Gruppenvergleich noch einmal bezogen auf Schadsoftware-Angriffe durchgeführt.

Abbildung 78 **Anteil der Betroffenen von sonstiger Schadsoftware nach Art der Firewall**

in Prozent; gewichtete Daten; 95%-KI; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)



Bei diesem Vergleich sind z.T. deutliche Unterschiede zu erkennen (Abbildung 78): So waren Unternehmen mit 50 bis 99 Beschäftigten sowie ab 500 Beschäftigten, die bereits vor dem schwerwiegendsten Cyberangriff eine erweiterte Firewall eingesetzt haben, seltener von Angriffen mit sonstiger Schadsoftware betroffen, als entsprechende Unternehmen mit einfacher Firewall (6,9 % vs. 13,2 % bzw. 6,3 % vs. 17,9 %). Dies weist darauf hin, dass die Qualität und der Reifegrad technischer Schutzmaßnahmen eine bedeutsame Rolle spielten. Warum sich dieser Zusammenhang in den anderen Beschäftigtengrößenklassen nicht so deutlich zeigt, könnte damit zusammenhängen, dass sich weitere Faktoren wie die fachgerechte Implementierung und Anwendung sowie die regelmäßige Wartung auswirken, die hier nicht kontrolliert werden können.

10.3 Zwischenresümee

Zusammenfassend lässt sich nach diesen Vergleichen der Anteile betroffener Unternehmen mit und ohne die jeweiligen IT-Sicherheitsmaßnahmen festhalten, dass vor allem von einzelnen organisatorische Maßnahmen eine präventive Wirkung auszugehen scheint und der Faktor Mensch eine bedeutende Rolle bei der Prävention von Cyberangriffen spielt. Vor allem wirkten sich die Überprüfung von Richtlinien und deren Einhaltung sowie die Schulung von Beschäftigten zur IT-Sicherheit in Richtung eines niedrigeren Betroffenheitsanteils aus.

Diese organisatorischen Maßnahmen setzen allerdings andere organisatorische und technische IT-Sicherheitsmaßnahmen voraus, die ihren Teil zur präventiven Wirkung beitragen.[317] Auch wenn nur wenige bivariate Zusammenhänge zwischen technischen Maßnahmen und dem Anteil der betroffenen Unternehmen gefunden wurden, sollte daher nicht auf deren Wirkungslosigkeit geschlossen werden. Dies gilt umso mehr, als dass lediglich deren Vorhandensein erfragt wurde und qualitative Unterschiede weitgehend außen vor bleiben. Hinzu kommt, dass so gut wie alle Unternehmen diese Fragen nach dem Vorhandensein technischer Maßnahmen bejahten, was durchaus positiv bewertet werden kann, aber ebenfalls Fragen nach qualitativen Unterschiede bei deren Ausgestaltung und Umsetzung aufwirft (z.B. der Reifegrad bzw. die sachgerechte Konfiguration einer vorhandenen Firewall). In zukünftigen Studien sollten technische IT-Sicherheitsmaßnahmen deshalb detaillierter hinsichtlich ihres Reifegrades und ihrer fachgerechten Umsetzung, Wartung und Zyklizität untersucht werden.[318] Daneben ist auch die Frage des Designs und der Nutzbarkeit technischer Maßnahmen im Arbeitsalltag[319] sowie das Zusammenspiel aller IT-Sicherheitsmaßnahmen in den Blick zu nehmen.[320]

Um genauere Aussagen über das Zusammenwirken einzelner technischer und organisatorischer Maßnahmen und deren partielle Einflüsse auf die Wahrscheinlichkeit eines Cyberangriffs vor dem Hintergrund verschiedener Angriffsarten und Unternehmensmerkmalen treffen zu können, sind weiter multivariate Analysen geplant, die auf diesen Ergebnissen aufbauen.

---

317 Bspw. lassen sich Richtlinien zum Umgang mit Passwörtern nur überprüfen, wenn es eine entsprechende Richtlinie gibt und der Passwortschutz technisch vorgesehen ist.

318 Bspw. ließe sich bezüglich der Backups erfragen, ob die Systemwiederherstellung von einem Backup (Backup-Restoring) getestet wird. Hinsichtlich des Passwortschutzes könnte der Einsatz einer Zwei-Faktor-Authentifizierung erfragt werden und bezogen auf Sicherheitsupdates, ob Software ohne Herstellersupport genutzt wird, die keine Updates und Patches mehr erhält etc.

319 Lassen sich z.B. die mit technischen Maßnahmen verbundenen Verhaltensregeln einhalten bzw. in die jeweilige Arbeitspraxis sinnvoll integrieren, ohne nicht intendierte Nebenfolgen wie Reaktanz und problematisches Ausweichverhalten bei den Nutzer*innen zu verursachen? Zum Thema „Usable Security“ siehe z.B. Adams & Sasse (1999); Nurse et al. (2011); Sasse et al. (2001).

320 Connolly & Wall (2019) weisen darauf hin, dass es vor dem Hintergrund komplexer Bedrohungen wie z.B. Ransomware-Angriffen auf das Zusammenspiel von sozio-technischen Maßnahmen, engagierter Führungskräfte und aktiver Unterstützung durch das Unternehmensmanagement ankommt (S. 14).

11 ZUSAMMENFASSUNG ZENTRALER ERGEBNISSE

Entscheidungen zur Absicherung von IT-Systemen erhalten im Zusammenhang mit einer rasanten Digitalisierung und den damit verbundenen Risiken verschiedenster Cyberangriffsarten eine größer werdende Bedeutung für Unternehmen. Um derartige Entscheidungen begründet und evidenzbasiert treffen zu können, sind unabhängige wissenschaftliche Forschungsergebnisse notwendig, die im Bereich Cyberangriffe gegen Unternehmen in Deutschland aber auch darüber hinaus bisher weitgehend fehlen.

Vor diesem Hintergrund führt das Kriminologische Forschungsinstitut Niedersachsen e.V. zusammen mit dem Forschungszentrum L3S der Leibniz-Universität Hannover das Forschungsprojekt „Cyberangriffe gegen Unternehmen“ durch, in dem differenziertes Wissen zu den Angriffsarten, zur Häufigkeit der Cyberangriffe, zur Verbreitung von Präventionsmaßnahmen und IT-Sicherheitsstandards als auch zu Risiko- und Schutzfaktoren erarbeitet werden soll. Ein weiteres Ziel dieses Projektes ist es, das erarbeitete Wissen handlungspraktisch aufzubereiten und in die Unternehmen zu transferieren, um insbesondere kleinen und mittleren Unternehmen mit begrenzten personellen und materiellen Ressourcen zu unterstützen, ihre IT-Sicherheit gezielt zu verbessern. Dazu wird z.B. auf Basis des vorliegenden Forschungsberichtes eine zusätzliche praxisrelevante Kurzfassung erstellt, die auf bedeutsame Unterschiede zwischen KMU und großen Unternehmen insbesondere hinsichtlich möglicher Risiko- und Schutzfaktoren adressatengerecht eingeht.

Das Projekt mit einer dreijährigen Laufzeit von Dezember 2017 bis November 2020 wird im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie (BMWi) gefördert und erhält eine zusätzliche Förderung durch die VHV-Stiftung sowie von PricewaterhouseCoopers Deutschland. Neben Experteninterviews und verschiedenen Feldstudien mit IT-Beschäftigten in kleinen und mittleren Unternehmen wurde eine CATI-Befragung von 5.000 Unternehmen ab zehn Beschäftigten und mit Sitz in Deutschland auf Basis einer disproportional geschichteten Zufallsstichprobe durchgeführt.

Die Ergebnisse der Befragung sind Inhalt des vorliegenden Forschungsberichtes und werden im Folgenden, gegliedert nach den Hauptforschungsfragen aus Abschnitt 1.2, noch einmal zusammengefasst. Anschließend wird auf methodische Restriktionen hingewiesen und einen Ausblick hinsichtlich weiterer Forschungsschritte gegeben.

1) Welche IT-Sicherheitsmaßnahmen gegen Cyberangriffe haben die Unternehmen eingerichtet?

Bei der IT-Sicherheitsstruktur wurden organisatorische und technische IT-Sicherheitsmaßnahmen voneinander unterschieden. Dabei kann allgemein festgestellt werden, dass technische Maßnahmen sehr weit verbreitet zu sein scheinen und es allenfalls geringe quantitative Unterschiede zwischen den Beschäftigtengrößenklassen und WZ08-Klassen gibt, wohingegen organisatorische Maßnahmen seltener sind und eher in größeren Unternehmen und bestimmten WZ08-Klassen eingesetzt werden.

Organisatorische Maßnahmen

Bei allen erfragten organisatorischen Maßnahmen fanden sich deutliche Unterschiede bei ihrer Verbreitung: Zum Beispiel sind in den kleinen Unternehmen (10-49 Besch.) schriftlich fixierte Richtlinien zur Informations- bzw. IT-Sicherheit (62,6 %) sowie zum Notfallmanagement (50.6 %), die von der Präsenz und einer intensiveren Auseinandersetzung mit dem Thema innerhalb der Unternehmen zeugen, deutlich seltener vorhanden als in den großen (ab 500 Besch.: 92,0 % bzw. 84,4 %) und z.B. innerhalb des Baugewerbes (WZ08-F: 48,9 % bzw. 33,8 %) seltener als bei Finanz- & Versicherungsdienstleistern (WZ08-K: 94,3 % bzw. 89,3 %). Unternehmen, die solche Richtlinien eingeführt haben, überprüfen mehrheitlich regelmäßig deren Einhaltung und ahnden ggf. Verstöße (76,7 %). Unterschiede zwischen den Beschäftigtengrößenklassen und WZ08-Klassen fallen diesbezüglich vergleichsweise gering aus, was dafür spricht, dass solche Richtlinien häufig nicht nur auf dem Papier vorhanden, sondern auch handlungsleitend sind. Schulungen zur IT-Sicherheit für Beschäftigten werden als ein weiteres Beispiel für organisatorische Maßnahmen von über drei Viertel der großen Unternehmen (ab 500 Besch.: 76,2 %) aber von weniger als der Hälfte der kleinen Unternehmen (10-49 Besch.: 46,5 %) durchgeführt. Die Unterschiede zwischen Unternehmen des Baugewerbes und der Finanz- & Versicherungsdienstleister fielen noch deutlicher aus (14,3 % vs. 77,1 %).

Technische Maßnahmen

Im Gegensatz zu den organisatorischen Maßnahmen liegen die Anteile der Unternehmen, die Mindestanforderungen für Passwörter haben, Zugangs- und Nutzerrechte individuell und nach Aufgabe vergeben, regelmäßig Backups durchführen, diese physisch getrennt aufbewahren, Antivirensoftware und Firewall einsetzen und die Sicherheitsupdates und Patches regelmäßig installieren in allen Beschäftigtengrößenklassen über 80 % und zum großen Teil sogar über 90 %. Größere Unterschiede zwischen den Beschäftigtengrößenklassen zeigte sich lediglich bezüglich der Mindestanforderungen für Passwörter sowie der individuellen Vergabe von Zugangs- und Nutzerrechten je nach Aufgabe: Die Anteile der Unternehmen mit solchen Mindestanforderungen bzw. mit einer entsprechenden Rechtevergabe liegt bei den kleinen (10-49 Besch.: 85,4 % bzw. 82,0 %) immerhin zehn bzw. vierzehn Prozentpunkte unter denen der großen Unternehmen (ab 500 Besch.: 95,4 % bzw. 96,4 %).

Da die erfragten technischen IT-Sicherheitsmaßnahmen quantitativ betrachtet bereits sehr stark verbreitet zu sein scheinen, wird es in der weiteren Forschung darauf ankommen, nach den qualitativen Unterschieden zu suchen, die möglicherweise im Zusammenhang mit dem Risiko von Cyberangriffen stehen, um Unternehmen diesbezüglich sinnvoll beraten und bei deren Umsetzung unterstützen zu können. Bezüglich der organisatorischen Maßnahmen kann daneben ein Förderbedarf bei deren Verbreitung aus den Ergebnissen dieser Befragung abgeleitet werden, der insbesondere kleinere und mittlere Unternehmen betrifft.

Einschätzungen zu IT-Risiken

Folgt man den Einschätzungen der befragten Unternehmensvertreter*innen, dann ist das Bewusstsein über IT-Risiken in den Geschäftsführungen der Unternehmen und in den Belegschaften mehrheitlich vorhanden. Lediglich 8,0 % bzw. 11,3 % gaben an, dass sich die Geschäftsführung bzw. die Belegschaft ihres Unternehmens der IT-Risiken nicht bewusst

sei. Ein hoher Anteil von 84,9 % stimmte (eher) der Aussage zu, dass in ihrem Unternehmen sehr viel für die IT-Sicherheit getan wird.

Nach diesem Ergebnis überrascht es nicht, dass das Risiko des eigenen Unternehmens in den nächsten zwölf Monaten von einem gezielten Cyberangriff betroffen zu werden, überwiegend sehr/ eher gering eingeschätzt wird (93,0 %). Der Anteil, der dies bezüglich ungezielter Cyberangriffe so sieht, fällt mit 68,5 % zwar etwas niedriger, aber immer noch relativ hoch aus. Nur etwa ein Drittel der Unternehmensvertreter schätzt dies gegenteilig ein. Interessant dabei ist der Zusammenhang zwischen Risikoeinschätzung und dem Vorhandensein potentieller Angriffsziele im Unternehmen (z.B. besondere Produkte oder ein besonderer Kundenkreis), der auch in Hinblick auf ungezielte Cyberangriffe besteht: In Unternehmen, in denen es nach Einschätzung der befragten Vertreter*innen keine potentiellen Angriffsziele gibt, wird nicht nur das Risiko für gezielte, sondern auch für ungezielte Cyberangriffe signifikant niedriger eingeschätzt als in Unternehmen mit potentiellen Angriffszielen. Damit laufen insbesondere erstere Gefahr, das Risiko ungezielter Cyberangriffen zu unterschätzen.

2) Auf welche Cyberangriffsarten mussten Unternehmen in den letzten zwölf Monaten reagieren?

Über zwei Fünftel (41,1 %) der befragten Unternehmen haben in den vorhergehenden zwölf Monaten mindestens einen Cyberangriff erlebt, auf den reagiert werden musste, d.h., Angriffe, die automatisiert (z.B. über den Spam-Filter der Firewall oder Antivirensoftware) vereitelt oder gar nicht erkannt wurden (z.B. Spyware-Angriffe), sind dabei nicht inkludiert. Große Unternehmen (ab 500 Besch.) sind mit einer Jahresprävalenzrate von 58,2 % signifikant häufiger betroffen als mittlere (zwischen 45,6 und 47,3 %) und kleine Unternehmen (10-49 Besch.: 39,4 %). Dies entspricht tendenziell den unterschiedlichen Risikoeinschätzungen der Beschäftigtengrößenklassen, wonach kleine Unternehmen das Risiko eines zukünftigen Cyberangriffs geringer einschätzen als größere. Allerdings liegen die Anteile der im Vorjahr von mindestens einem Cyberangriff betroffenen Unternehmen in allen Beschäftigungsgrößenklassen über den Anteilen der Unternehmen, die das Risiko solcher Angriffe in den nächsten zwölf Monaten als eher/sehr hoch bewerten. Dies weist auf eine allgemeine Unterschätzung des entsprechenden Unternehmensrisikos hin.

Angriffsarten[321]

Angriffe mittels Schadsoftware bilden hinsichtlich der Verbreitung der unterschiedenen Cyberangriffsarten neben Phishing-Angriffen einen Schwerpunkt: Jedes achte Unternehmen (12,5 %) war in den letzten zwölf Monaten von einem Ransomware-Angriff betroffen, jedes

[321] Folgende Angriffsarten wurden dabei unterschieden:
Ransomware-Angriff: Verschlüsselung von Unternehmensdaten (i.d.R. verbunden mit einer Erpressung);
Spyware-Angriff: Ausspähung von Nutzeraktivitäten oder sonstiger Daten innerhalb von IT-Systemen;
Sonstiger Schadsoftware-Angriff: Infizierung von IT-Systemen mit Viren, Würmern oder Trojanern etc.;
Manuelles Hacking: Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware;
Denial of Service Angriff ((D)DoS): Überlastung von Web- oder E-Mail-Servern, die auf deren Ausfall zielt;
Defacing-Angriff: unbefugte Veränderung von Webinhalte des Unternehmens;
CEO-Fraud: Vortäuschung einer Führungspersönlichkeit des Unternehmens zur Manipulation von Beschäftigten;
Phishing-Angriff: Täuschung mit fingierten E-Mails oder Webseiten zur Erlangung sensibler Unternehmensdaten etc.

neunte (11,3 %) von einem Spyware-Angriff und etwa jedes fünfte (21,3 %) von sonstigen Schadsoftware-Angriffen.

Der Anteil von Phishing betroffener Unternehmen lag ebenfalls bei über einem Fünftel (22,0 %). Hingegen berichteten die Unternehmen seltener von CEO-Fraud (8,1 %) und (D)DoS-Angriffen (6,4 %) und nur ein kleiner Anteil war von manuellem Hacking (2,8 %) oder Defacing-Angriffen (3,1 %) betroffen.

Betrachtet man die Cyberangriffsarten nach der Anzahl der erlebten Vorfälle, auf die reagiert werden musste, dann bilden Phishing-Angriffe mit 52,0 % aller berichteten Vorfälle den Schwerpunkt, gefolgt von sonstigen Schadsoftware-Angriffen (24,0 %) und Spyware-Angriffen (11,9 %). Ransomware-Angriffe machten lediglich 3,3 % aller berichteten Vorfälle aus, d.h., diese Angriffsart ist zwar vergleichsweise weit verbreitet (11,3 % der Unternehmen waren betroffen), aber die Anzahl derartiger Vorfälle, die von betroffenen Unternehmen berichtet wurde, ist relativ klein. Die Anzahl der Vorfälle von manuellem Hacking, CEO-Fraud, (D)DoS und Defacing liegt anteilig ebenfalls im unteren einstelligen Bereich (2,9 %, 2,4 %, 2,2 % bzw. 1,2 %).

Mögliche Risikofaktoren

Allgemein kann gesagt werden, dass größere Unternehmen stärker von Cyberangriffen betroffen sind als kleinere. Dies gilt insbesondere für Ransomware-Angriffe, CEO-Fraud und Phishing-Angriffen. Demgegenüber scheint die Beschäftigtengrößenklasse bei den übrigen Angriffsarten allenfalls eine kleine Rolle zu spielen.

Im Vergleich der Betroffenheitsraten nach Branchen bzw. Wirtschaftszweigen, fallen weitere signifikante Unterschiede auf: Z.B. sind der Handel; Instandhaltung/Reparatur von KFZ oder freiberufliche, wissenschaftliche und technische Dienstleistungen häufiger von Cyberangriffen betroffen als die Wasserversorgung; Abwasser- und Abfallentsorgung und Beseitigung von Umweltverschmutzungen oder die Land- und Forstwirtschaft und Fischerei.

Daneben stehen die Anzahl der Unternehmensstandorte, der Export von Dienstleistungen und Waren und das Vorhandensein potentieller Angriffsziele wie besondere Produkte, Herstellungsverfahren oder Dienstleistungen und besondere Reputation oder Kundenkreis im Zusammenhang mit einer höheren Betroffenheit. Die öffentliche Zugänglichkeit detaillierter Informationen zu den Beschäftigten scheint insbesondere bei der Angriffsart CEO-Fraud eine risikosteigernde Rolle zu spielen.

Unternehmen der Daseinsvorsorge waren hingegen seltener betroffen (31,1 %) als Unternehmen der übrigen Branchen (42,3 %). Vor allem kleinere Unternehmen dieser Gruppe scheinen damit besser geschützt zu sein als in den anderen Wirtschaftszweigen.

Ausmaß und Folgen von Cyberangriffen

Zu den am häufigsten von den berichteten schwerwiegendsten Cyberangriffen betroffenen IT-Systemen gehören: E-Mail und Kommunikation, Auftrags- und Kundenverwaltung sowie Rechnungswesen und Controlling, die von über 90 % der Unternehmen als (eher) wichtig für das Unternehmen eingestuft wurden. Die Dauer, in denen diese Systeme infolge des

Cyberangriffs gar nicht oder nur stark eingeschränkt genutzt werden konnten, reichte von einer Stunde bis 90 Tage, wobei der Median jeweils bei 24 Stunden lag. Am seltensten war die Produktionssteuerung betroffen, fiel aber mit einem Median von 48 Stunden länger aus als andere Systeme.

Bei einem Viertel der Unternehmen (25,2 %) waren durch den schwerwiegendsten Cyberangriff unterschiedliche digitale Daten betroffen, d.h., sie wurden gelöscht, manipuliert, gestohlen/kopiert oder verschlüsselt. Bei 70,0 % entstanden infolge des Angriffs direkte Kosten für das Unternehmen. Dazu zählten insbesondere Kosten im Zusammenhang mit Sofortmaßnahmen zur Abwehr und Aufklärung, Wiederherstellungs-/ Wiederbeschaffungskosten sowie Kosten für externe Beratung. Sehr selten wurde von Schadensersatz/ Strafen und abgeflossenen Geldern berichtet.

Die Spannbreite der berichteten direkten Gesamtkosten infolge der schwerwiegendsten Cyberangriffe liegt zwischen 10 EUR und 2 Mio. EUR und reicht damit insbesondere für viele kleinere Unternehmen in einen existenzbedrohlichen Bereich. Wenn Kosten verursacht wurden, lässt sich aber ebenso feststellen, dass diese in der überwiegende Mehrzahl (78,0 %) unter 5.000 EUR lagen und nur sehr selten bei 50.000 EUR und mehr (3,4 %). Der Durchschnitt der berichteten Gesamtkosten liegt bei rund 16.900 EUR, der Median bei 1.000 EUR. Zu den Kostenpositionen mit einem vergleichsweise hohen Median von 2.000 EUR zählen abgeflossene Gelder und Betriebsunterbrechung. Zu den Angriffsarten, die im Median die höchsten Kosten verursacht haben, zählen Ransomware-Angriffe (1.300 EUR) und manuelles Hacking (2.800 EUR)

3) Wie ist das Anzeigeverhalten von betroffenen Unternehmen?

Ein Anteil von 11,9 % der Unternehmen, die Angaben zum schwerwiegendsten Cyberangriff machten, zeigten diese polizeilich an. Somit ist allgemein von einem großen Dunkelfeld bei Cyberangriffen gegen Unternehmen auszugehen. Daneben konnte festgestellt werden, dass größere Unternehmen häufiger Anzeige erstatteten als kleinere (ab 500 Besch: 21,5 % vs. 10-49 Besch.: 10,6 %) und sich deutliche Unterschiede zwischen den Angriffsarten zeigen. CEO-Fraud, Spyware und manuelles Hacking wurden vergleichsweise häufig zur Anzeige gebracht (24,6 %, 19,7 % bzw. 19,4 %), während sonstige Schadsoftware- und Defacing-Angriffe der Polizei nur sehr selten zur Kenntnis gelangten (4,4 % bzw. 6,4 %).

Die am häufigsten genannten Nichtanzeigegründe waren die fehlende Aussicht auf einen Ermittlungserfolg (72,0 %) und sonstige Gründe (30,1 %) zu denen vermutlich die geringen entstandenen Kosten zählen. An dritter Stelle äußerten nichtanzeigende Unternehmen, dass sie nicht wussten, an wen man sich dafür wenden muss (20,7 %). Befürchtungen von Imageschäden, Einsichtnahmen in vertrauliche Daten oder Arbeitsbehinderungen scheinen hingegen bei der Entscheidung zur (Nicht-)Anzeige eine eher untergeordnete Rolle zu spielen.

Bewertung der Strafverfolgungsbehörden

Über die Hälfte der Unternehmen, die den schwerwiegendsten Vorfall zur Anzeige gebracht haben, äußerten sich insgesamt (eher) unzufrieden mit der Arbeit der Polizei (52,2 %) und ein Zehntel stimmte (eher) zu, dass durch die Ermittlungen der Betriebsablauf gestört wurde (9,6 %). Und auch wenn nur in 7,7 % der angezeigten schwerwiegendsten Cyberangriffe

Täter*innen ermittelt werden konnten, würden es 93,8 % der Unternehmen anderen empfehlen, Cyberangriffe anzuzeigen. Deren Motivation dürfte demnach vermutlich weniger in der Aussicht auf einen Ermittlungserfolg der Polizei liegen als in der polizeilichen Registrierung von Straftaten oder in Informations- und Beratungsmöglichkeiten der Polizei zum Schutz vor zukünftigen Cyberangriffen.

4) Gibt es einen Zusammenhang zwischen der Häufigkeit von Cyberangriffen mit dem Vorhandensein bestimmter IT-Sicherheitsmaßnahmen?

Um potentielle Schutzfaktoren gegen Cyberangriffe herauszuarbeiten, wurden Gruppenvergleiche zwischen Unternehmen mit und ohne die verschiedenen IT-Sicherheitsmaßnahmen in Hinblick auf deren Betroffenheit durchgeführt. Diese Vergleiche zusammenfassend lässt sich festhalten, dass vorwiegend von verschiedenen organisatorischen Maßnahmen eine präventive Wirkung auszugehen scheint und der Faktor Mensch eine bedeutende Rolle bei der Prävention von Cyberangriffen spielt. Insbesondere die Überprüfung von Richtlinien und deren Einhaltung sowie die Schulung von Beschäftigten zur IT-Sicherheit wirkten sich in Richtung eines niedrigeren Betroffenheitsanteils aus.

Dadurch, dass die technischen IT-Sicherheitsmaßnahmen, so wie sie erfragt wurden, in fast allen Unternehmen vorhanden waren, gab es häufig keine ausreichend große Vergleichsgruppe. Eine Ausnahme, bei der sich der erwartete Zusammenhang zeigte, bilden Mindestanforderungen an Passwörter. Unternehmen, die diese Maßnahme bisher nicht umsetzten, waren häufiger von Cyberangriffen betroffen als die anderen. Dies zeigte sich in statistisch signifikanter Weise bei den kleineren Unternehmen bis 99 Beschäftigten.

Auch wenn kaum bivariate Zusammenhänge zwischen technischen Maßnahmen und dem Anteil der betroffenen Unternehmen gefunden werden konnten, kann nicht auf deren Wirkungslosigkeit geschlossen werden. Dies gilt umso mehr, als dass lediglich deren Vorhandensein erfragt wurde, qualitative Unterschiede weitgehend außen vor blieben und organisatorischen Maßnahmen viele der technischen IT-Sicherheitsmaßnahmen voraussetzen. In zukünftigen Studien sollten technische IT-Sicherheitsmaßnahmen deshalb viel detaillierter hinsichtlich ihres Reifegrades, ihrer Qualität und Nutzbarkeit sowie im Zusammenspiel mit organisatorischen Maßnahmen und den Nutzer*innen in den Blick genommen werden.

Jede Forschung ist mit verschiedenen Limitationen verbunden, die die Aussagekraft der Ergebnisse einschränken und die bei der Ergebnisinterpretation berücksichtigt werden müssen. Im Zusammenhang mit den oben vorgestellten Ergebnissen betrifft dies insbesondere folgende Punkte: Die Stichprobenziehung erfolgte aus einer Auswahlgesamtheit und nicht direkt aus der Grundgesamtheit. Auch wenn die Stichprobe hinsichtlich der Verteilung aller kontrollierten Merkmale weitgehend der Grundgesamtheit entspricht und keine Hinweise auf eine systematische Verzerrung vorliegen und sie somit als repräsentativ für Unternehmen ab zehn Mitarbeiter*innen in Deutschland gelten kann, bleibt damit eine Unsicherheit hinsichtlich des Coverage-Problems bestehen, insofern nicht erfasste Unternehmen keine Chance hatten, in die Stichprobe zu gelangen. Daneben sind derartige Unternehmensbefragungen darauf beschränkt, dass lediglich eine Person als Unternehmensvertreter*in befragt werden kann. Neben dem Problem der Auswahl geeigneter Repräsentanten*innen, spiegeln deren Antworten immer den jeweiligen

Wissensstand wider und sind z.T. nur subjektive Einschätzungen. Hinzu kommt, dass insbesondere die Fragen nach vorgefallenen Cyberangriffen retrospektiv gestellt wurden, was mit entsprechenden Verzerrungen verbunden sein kann, wenn erfragte Ereignisse z.B. gar nicht erinnert werden oder in Wahrheit länger zurückliegen als in der Erinnerung der Befragten. Eine weitere bereits angesprochene Limitation liegt darin, dass aus forschungspragmatischen Gründen zum einen lediglich das Vorhandensein bestimmter Merkmale und Maßnahmen erfragt werden konnte und daher keine Aussagen zu qualitativen Unterschieden gemacht werden können. Zum anderen konnten Detailfragen u.a. zu Ausmaß und Folgen der Cyberangriffe nur zu einem Angriff gestellt werden. Sobald mehrere Angriffe im Zeitraum der letzten zwölf Monate stattfanden, beziehen sich die Antworten auf den als „schwerwiegendsten Angriff" bestimmten Cyberangriff.

Trotz dieser Einschränkungen erlauben die Ergebnisse dieser Studie einen sehr differenzierten Blick auf das Phänomen Cyberangriffe gegen Unternehmen in Deutschland mit mehr als neun Beschäftigten. So konnte z.B. verdeutlicht werden, dass ein großer Teil dieser Unternehmen in den letzten zwölf Monaten von Cyberangriffen betroffen war, was sich aufgrund einer sehr niedrigen Anzeigequote nicht in den offiziellen Kriminalitätsstatistiken widerspiegelt. Daneben zeigte sich, dass die Spannbreite der durch Cyberangriffe verursachten Schäden sehr groß ist, wenngleich die entstandenen direkten Kosten mehrheitlich überschaubar blieben. Insbesondere organisatorische Maßnahmen, die den Faktor Mensch betreffen, scheinen bei der Prävention von Cyberangriffen einen Unterschied zu machen und sind demnach in Hinblick auf ihre Verbreitung vor allem bei kleinen und mittleren Unternehmen besonders zu fördern. Darüber hinaus wurde aber auch deutlich, dass es keine einfachen Antworten zum Cyberangriffsrisiko und zu entsprechenden Schutzmaßnahmen geben wird. Dies hängt u.a. mit der Komplexität der Cyberangriffe und Angriffsvektoren als auch mit der z.T. sehr komplexen IT-Struktur der Unternehmen zusammen, die in einer quantitativen Befragung zudem nur grob erhoben werden kann.

Auch wenn die Auswertungen zur Unternehmensbefragung mit diesem Bericht noch nicht abgeschlossen sind und weitere multivariate Analysen und Ergebnisse z.B. zur Risiko- und Schutzfaktoren im Zusammenhang mit Cyberangriffen sowie zum Schadensausmaß folgen, können auch mit dieser Studie nicht alle Fragen beantwortet werden. Neben Differenzierungen der IT-Sicherheitsmaßnahmen nach Reifegrad bleibt z.B. das Zusammenspiel von Beschäftigten und verfügbaren IT-Sicherheitsmaßnahmen, die Entdeckung verschiedener Angriffsarten und deren Angriffswege oder die Entwicklungen im Bereich der Angriffsarten unterbelichtet.

Es ist daher wünschenswert, wenn in Zukunft weitere Forschung zum vermutlich mit der Digitalisierung wachsenden Phänomen Cyberkriminalität und speziell Cyberkriminalität gegen Unternehmen betrieben wird. Um die Entwicklung innerhalb eines Jahres in diesem Bereich untersuchen zu können, ist im Rahmen dieses Projektes eine zweite Befragung mit den Unternehmen und deren Vertreter*innen geplant, die uns im Zuge der ersten Befragung ihre Teilnahmebereitschaft signalisiert haben und denen wir an dieser Stelle noch einmal herzlich dafür danken!

ANHANG 1: ZUSATZTABELLEN

Tabelle 43 **WZ08-Klassen der Daseinsvorsorge-Unternehmen**

WZ08-Klassen Ebene 1	Ebene 4	Bezeichnung
WZ08-D Energieversor.	35.11.1	Elektrizitätserzeugung oh. Verteilung
	35.11.2	Elektrizitätserzeugung m. Fremdbezug z. Verteilung
	35.11.3	Elektrizitätserzeugung oh. Fremdbezug z. Verteilung
	35.12.0	Elektrizitätsübertragung
	35.13.0	Elektrizitätsverteilung
	35.14.0	Elektrizitätshandel
	35.21.1	Gaserzeugung oh. Verteilung
	35.21.2	Gaserzeugung m. Fremdbezug z. Verteilung
	35.21.3	Gaserzeugung oh. Fremdbezug z. Verteilung
	35.22.0	Gasverteilung durch Rohrleitungen
	35.23.0	Gashandel durch Rohrleitungen
	35.30.0	Wärme- u. Kälteversorgung
WZ08-E Wasserversor.; Abwasser- u. Abfallentsor. u. Beseitigung v. Umweltverschm.	36.00.1	Wassergewinnung m. Fremdbezug z. Verteilung
	36.00.2	Wassergewinnung oh. Fremdbezug z. Verteilung
	36.00.3	Wasserverteilung oh. Gewinnung
	37.00.1	Betrieb der Sammelkanalisation
	37.00.2	Betrieb v. Kläranlagen
	38.11.0	Sammlung nicht gefährlicher Abfälle
	38.12.0	Sammlung gefährlicher Abfälle
	38.21.0	Behandlung u. Beseitigung nicht gefährlicher Abfälle
	38.22.0	Behandlung u. Beseitigung gefährlicher Abfälle
	38.31.0	Zerlegen v. Schiffs- u. Fahrzeugwracks u. anderen Altwaren
	38.32.0	Rückgewinnung sortierter Werkstoffe
	39.00.0	Beseitigung v. Umweltverschmutzungen u. sonstige Entsorgung
WZ08-H Verkehr u. Lagerei	49.10.0	Personenbeförderung im Eisenbahnfernverkehr
	49.20.0	Güterbeförderung im Eisenbahnverkehr
	49.31.0	Personenbeförderung im Nahverkehr zu Lande (oh. Taxis)
	49.39.1	Personenbeförderung im Omnibus-Linienfernverkehr
	49.39.2	Personenbeförderung im Omnibus-Gelegenheitsverkehr
	49.39.9	Personenbeförderung im Landverkehr a. n. g.
	49.41.0	Güterbeförderung im Straßenverkehr
	49.50.0	Transport in Rohrfernleitungen
	50.10.0	Personenbeförderung i. d. See- u. Küstenschifffahrt
	50.20.0	Güterbeförderung i. d. See- u. Küstenschifffahrt
	50.30.0	Personenbeförderung i. d. Binnenschifffahrt
	50.40.0	Güterbeförderung i. d. Binnenschifffahrt
	51.10.0	Personenbeförderung i. d. Luftfahrt
	51.21.0	Güterbeförderung i. d. Luftfahrt
	52.10.0	Lagerei

	52.21.2	Betrieb v. Verkehrswegen f. Straßenfahrzeuge
	52.21.3	Betrieb v. Verkehrswegen f. Schienenfahrzeuge
	52.21.4	Betrieb v. Bahnhöfen f. den Personenverkehr einschließlich Omnibusbahnhöfe
	52.21.5	Betrieb v. Güterabfertigungseinrichtungen f. Schienen- u. Straßenfahrzeuge (oh. Frachtumschlag)
	52.21.9	Erbringung v. sonstigen Dienstleistungen f. den Landverkehr a. n. g.
	52.22.1	Betrieb v. Wasserstraßen
	52.22.2	Betrieb v. Häfen
	52.22.3	Lotsinnen u. Lotsen i. d. Schifffahrt
	52.22.9	Erbringung v. sonstigen Dienstleistungen f. die Schifffahrt a. n. g.
	52.23.1	Betrieb v. Flughäfen u. Landeplätzen f. Luftfahrzeuge
	52.23.9	Erbringung v. sonstigen Dienstleistungen f. die Luftfahrt a. n. g.
	52.24.0	Frachtumschlag
	53.10.0	Postdienste v. Universaldienstleistungsanbietern
	53.20.0	Sonstige Post-, Kurier- u. Expressdienste
WZ08-J Information u. Kommunikation	61.10.0	Leitungsgebundene Telekommunikation
	61.20.0	Drahtlose Telekommunikation
	61.30.0	Satellitentelekommunikation
	61.90.1	Internetserviceprovider
WZ08-K Finanz- u. Versicherungsdienstl.	64.11.0	Zentralbanken
	64.19.2	Kreditinstitute des Sparkassensektors
	64.19.3	Kreditinstitute des Genossenschaftssektors
WZ08-L Grundstücks- u. Wohnungswesen	68.10.1	Kauf u. Verkauf v. eigenen Wohngrundstücken, Wohngebäuden u. Wohnungen
	68.20.1	Vermietung, Verpachtung v. eigenen oder geleasten Wohngrundstücken, Wohngebäuden u. Wohnungen
	68.31.1	Vermittlung v. Wohngrundstücken, Wohngebäuden u. Wohnungen f. Dritte
	68.32.1	Verwaltung v. Wohngrundstücken, Wohngebäuden u. Wohnungen f. Dritte
WZ08-O Öffentliche Verwaltung, Verteidigung; Sozialversicherung	84.21.0	Auswärtige Angelegenheiten
	84.22.0	Verteidigung
	84.23.0	Rechtspflege
	84.24.0	Öffentliche Sicherheit u. Ordnung
	84.25.0	Feuerwehren
	84.30.0	Sozialversicherung
WZ08-P Erziehung u. Unterricht	85.42.1	Universitäten
	85.42.2	Allgemeine Fachhochschulen
	85.42.3	Verwaltungsfachhochschulen
	85.42.4	Berufsakademien, Fachakademien, Schulen d. Gesundheitswesens
WZ08-Q Gesundheits- u. Sozialwesen	86.10.1	Krankenhäuser (oh. Hochschulkliniken, Vorsorge- u. Rehabilitationskliniken)
	86.10.2	Hochschulkliniken
	86.10.3	Vorsorge- u. Rehabilitationskliniken

Tabelle 44 **Stichprobe nach WZ08-Klassen**

WZ08-Klassen (Kurzbezeichnung)		ungewichtet		gewichtet
Ebene 1	Ebene 2	Anzahl	Prozent	Prozent
WZ08-A Land- u. Forstwirtschaft, Fischerei	Landwirtschaft,Jagd u. verbundene Tätigkeiten (WZ08-01)	38	0,8	1,4
	Forstwirtschaft und Holzeinschlag (WZ08-02)	1	0,0	0,0
WZ08-B Bergbau u. Gewinnung v. Steinen u. Erden	Gew.v.Steinen u.Erden, sonst.Bergbau (WZ08-08)	15	0,3	0,3
	Erbrg.v.Dienstleistg.f. Bergbau u.Gew.v.Steinen (WZ08-09)	2	0,0	0,0
WZ08-C Verarbeitendes Gewerbe	H.v.Nahrungs-u. Futtermitteln (WZ08-10)	95	1,9	1,5
	Getränkeherstellung (WZ08-11)	17	0,3	0,2
	Tabakverarbeitung (WZ08-12)	3	0,1	0,0
	H.v.Textilien (WZ08-13)	36	0,7	0,5
	H.v.Bekleidung (WZ08-14)	11	0,2	0,2
	H.v.Leder,Lederwaren u.Schuhen (WZ08-15)	5	0,1	0,1
	H.v.Holz-,Flecht-,Korb- u.Korkwaren (oh.Möbel) (WZ08-16)	48	1,0	1,2
	H.v.Papier,Pappe u. Waren daraus (WZ08-17)	31	0,6	0,2
	H.v.Druckerzgn.Vervielf. v.Ton-,Bild-,Datenträger (WZ08-18)	37	0,7	1,0
	Kokerei u. Mineralölverarbeitung (WZ08-19)	1	0,0	0,0
	H.v.chem.Erzeugn. (WZ08-20)	50	1,0	0,8
	H.v.pharmazeut.Erzeugn. (WZ08-21)	13	0,3	0,1
	H.v.Gummi-u. Kunststoffwaren (WZ08-22)	93	1,9	1,0
	H.v.Glas,-waren,Keramik, Verarb.v.Steinen u.Erden (WZ08-23)	60	1,2	1,2
	Metallerzeugung u.-bearbeitung (WZ08-24)	51	1,0	0,7
	H.v.Metallerzeugnissen (WZ08-25)	231	4,6	3,9
	H.v.DV-Gerät.,elektron. u.opt.Erzeugn. (WZ08-26)	96	1,9	1,1
	H.v.elektr.Ausrüstg. (WZ08-27)	75	1,5	1,6
	Maschinenbau (WZ08-28)	200	4,0	2,4
	H.v.Kraftwagen u. Kraftwagenteilen (WZ08-29)	34	0,7	0,4
	Sonstiger Fahrzeugbau (WZ08-30)	9	0,2	0,0
	H.v.Möbeln (WZ08-31)	38	0,8	1,0
	H.v.sonst.Waren (WZ08-32)	71	1,4	1,1
	Rep.u.Inst.v.Maschinen u.Ausrüstungen (WZ08-33)	23	0,5	0,6
WZ08-D Energieversorgung	Energieversorgung (WZ08-35)	68	1,4	0,5
WZ08-E Wasserversor.; Abwasser- u. Abfallentsor. u. Beseitigung v. Umweltverschm.	Wasserversorgung (WZ08-36)	16	0,3	0,1
	Abwasserentsorgung (WZ08-37)	7	0,1	0,1
	Sammlung,Abfallbeseitigung,Rückgewinnung (WZ08-38)	62	1,2	0,7
	Beseitigung v.Umweltverschm.u.sonst.Entsorg. (WZ08-39)	4	0,1	0,0
WZ08-F Baugewerbe	Hochbau (WZ08-41)	70	1,4	2,6
	Tiefbau (WZ08-42)	53	1,1	1,3
	Vorb.Baustellenarbeiten, Bauinstall.,sonst.Ausbau (WZ08-43)	187	3,7	9,0
WZ08-G Handel; Instandhaltung u. Reparatur v. Kfz	Kfz-Handel;Instandh.u. Rep.v.Kfz (WZ08-45)	124	2,5	4,1
	Großhandel (oh.Kfz) (WZ08-46)	331	6,6	8,3
	Eh.(oh.Handel m.Kfz) (WZ08-47)	152	3,0	5,5
WZ08-H Verkehr u. Lagerei	Landverkehr;Transport i. Rohrleitungen (WZ08-49)	185	3,7	2,9
	Schifffahrt (WZ08-50)	19	0,4	0,4
	Luftfahrt (WZ08-51)	5	0,1	0,1
	Lagerei;sonst.Dienstleistg.f.d.Verkehr (WZ08-52)	104	2,1	1,2
	Post-,Kurier-u. Expressdienste (WZ08-53)	16	0,3	0,2

WZ08-I Gastgewerbe	Beherbergung (WZ08-55)	91	1,8	2,7
	Gastronomie (WZ08-56)	39	0,8	1,4
WZ08-J Information u. Kommunikation	Verlagswesen (WZ08-58)	36	0,7	0,6
	Film,TV-Programme,Kinos; Tonstudios,Musikverlag (WZ08-59)	5	0,1	0,1
	Rundfunkveranstalter (WZ08-60)	5	0,1	0,0
	Telekommunikation (WZ08-61)	6	0,1	0,3
	Dienstleistg.d. Informat.technologie (WZ08-62)	90	1,8	1,8
	Informat.dienstleistg. (WZ08-63)	10	0,2	0,2
WZ08-K Finanz- u. Versicherungsdienstl.	Finanzdientleistg. (WZ08-64)	170	3,4	1,7
	Versicherungen u. Pensionskassen (WZ08-65)	14	0,3	0,0
	M.Finanz-,Versicherungsdiensten verb.Tätigk. (WZ08-66)	25	0,5	0,4
WZ08-L Grundstücks- u. Wohnungswesen	Grundstücks-u. Wohnungswesen (WZ08-68)	105	2,1	1,6
WZ08-M Freiberufl., wissenschaftl. u. techn. Dienstl.	Rechts-u.Steuerberatung,Wirtschaftsprüfung (WZ08-69)	75	1,5	2,1
	Verwaltung u.Führung v. Untern.,Untern.beratung (WZ08-70)	146	2,9	1,7
	Architektur-,Ing.büros, techn.,physik.U.suchung (WZ08-71)	142	2,8	3,9
	Forschung u.Entwicklung (WZ08-72)	30	0,6	0,2
	Werbung u.Marktforschung (WZ08-73)	30	0,6	0,7
	Freiberuf.,wiss.u.techn. Tätigk. (WZ08-74)	9	0,2	0,4
	Veterinärwesen (WZ08-75)	2	0,0	0,2
WZ08-N Sonstigen wirtschaftl. Dienstl.	Verm.v.bewegl.Sachen (WZ08-77)	11	0,2	0,3
	Vermittl.u.Überlassung v.Arbeitskräften (WZ08-78)	59	1,2	0,5
	Reisebüros,-veranstalter u.sonst.Reservierungen (WZ08-79)	25	0,5	1,0
	Wach-u.Sicherheitsdienste,Detekteien (WZ08-80)	16	0,3	0,2
	Garten-u.Landschaftsbau; Gebäudebetreuung (WZ08-81)	70	1,4	1,3
	Dienstleistg.f.Untern.u. Privatpers.ang (WZ08-82)	54	1,1	0,9
WZ08-O Öffentl. Verwaltung, Verteidigung; Sozialversicherung	Öff.Verw.,Verteidigung; Sozialversicherung (WZ08-84)	19	0,4	0,4
WZ08-P Erziehung u. Unterricht	Erziehung u.Unterricht (WZ08-85)	274	5,5	6,4
WZ08-Q Gesundheits- u. Sozialwesen	Gesundheitswesen (WZ08-86)	169	3,4	1,9
	Heime (oh.Erholungs- u.Ferienheime) (WZ08-87)	116	2,3	1,5
	Sozialwesen(oh.Heime) (WZ08-88)	151	3,0	2,4
WZ08-R Kunst, Unterhaltung u. Erholung	Kreative,künstler.u. unterhaltende Tätigk. (WZ08-90)	17	0,3	0,1
	Bibliotheken,Archive, Museen,zoolog.u.ä.Gärten (WZ08-91)	9	0,2	0,2
	Spiel-,Wett-u. Lotteriewesen (WZ08-92)	7	0,1	0,0
	Diensleistg.d.Sports,d. Unterhaltg.u.Erholung (WZ08-93)	31	0,6	0,8
WZ08-S Sonstige Dienstl.	Interessenvertr.,kirchl. u.sonst.Vereinigungen (WZ08-94)	104	2,1	1,0
	Rep.v.DV-Gerät. u.Geb.güt. (WZ08-95)	5	0,1	0,1
	Sonst.übw.persönl. Dienstleistg. (WZ08-96)	46	0,9	1,4
	Gesamt	5.000	100,0	100,0

Tabelle 45 **Organisatorische IT-Sicherheitsmaßnahmen nach WZ08-Klassen der ersten Ebene**
in Prozent; gewichtete Daten

	IT-Sicherheitsmaßnahme						
WZ08-Klassen (Ebene 1; Kurzbezeichnung; nur wenn N≥30)	1	2	3*	4	5	6	7
Land- u. Forstwirtschaft, Fischerei (WZ08-A)	35,3	31,5	92,0	20,4	56,9	38,4	20,8
Verarbeitendes Gewerbe (WZ08-C)	63,6	54,6	73,2	16,9	46,9	48,1	24,1
Wasserversorgung; Abwasser- u. Abfallentsorgung u. Beseitigung v. Umweltverschmutzungen (WZ08-E)	63,0	58,7	75,8	30,8	59,1	52,2	24,4
Baugewerbe (WZ08-F)	48,9	33,8	73,0	**15,4**	44,4	**30,4**	**14,3**
Handel; Instandhaltung u. Reparatur v. Kfz (WZ08-G)	68,1	58,6	81,4	27,7	50,1	50,5	26,9
Verkehr u. Lagerei (WZ08-H)	47,0	40,2	70,7	23,0	45,8	40,3	21,0
Gastgewerbe (WZ08-I)	62,9	50,5	82,8	33,9	40,6	41,3	22,9
Information u. Kommunikation (WZ08-J)	76,7	67,1	70,0	33,3	62,7	72,5	47,7
Erbringung v. Finanz- u. Versicherungsdienstl. (WZ08-K)	94,3	89,3	99,0	63,8	89,8	89,5	77,1
Grundstücks- u. Wohnungswesen (WZ08-L)	72,5	63,0	78,0	28,0	51,9	53,1	28,0
Freiberufl., wissenschaftl. u. techn. Dienstl. (WZ08-M)	79,4	66,9	70,1	29,5	55,5	55,3	26,2
Sonst. wirtschaftl. Dienstl. (WZ08-N)	68,9	56,5	82,6	29,6	62,8	50,2	25,1
Erziehung u. Unterricht (WZ08-P)	77,6	60,5	78,5	22,3	51,3	60,6	23,9
Gesundheits- u. Sozialwesen (WZ08-Q)	79,2	64,2	80,3	27,9	65,1	60,4	17,3
Kunst, Unterhaltung u. Erholung (WZ08-R)	71,9	50,9	**64,3**	35,8	**36,2**	37,9	20,0
Sonst. Dienstl. (WZ08-S)	62,4	50,4	73,6	20,8	62,0	58,7	31,0

IT-Sicherheitsmaßnahme: 1: schriftl. fix. Richtl. z. Informations-/IT-Sicherheit, 2: schriftl. fix. Richtl. z. Notfallmanagement, 3: Einhaltung d. Richtl. wird regelm. überprüft u. Verstöße ggf. geahndet, 4: Zertifizierung d. IT-Sicherheit, 5: regelm. Risiko- u. Schwachstellenanalysen, 6: Übungen/Simulationen f. d. Ausfall wichtiger IT-Systeme, 7: Schulungen z. IT-Sicherheit f. MA
*) nur Unternehmen mit Richtlinien (1 u./o. 2)
Hervorhebung: fett: kleinster Anteil je IT-Sicherheitsmaßn.; grau hinterlegt: die drei kleinsten Anteile je IT-Sicherheitsmaßn.

Tabelle 46 **Technische IT-Sicherheitsmaßnahmen nach WZ08-Klassen der ersten Ebene**
in Prozent; gewichtete Daten

	IT-Sicherheitsmaßnahme						
WZ08-Klassen (Ebene 1; Kurzbezeichnung; nur wenn N≥30)	8	9	10	11	12	13	14
Land- u. Forstwirtschaft, Fischerei (WZ08-A)	79,5	80,6	100,0	100,0	**93,2**	93,1	100,0
Verarbeitendes Gewerbe (WZ08-C)	79,7	83,1	98,9	95,2	98,5	95,0	99,0
Wasserversorgung; Abwasser- u. Abfallentsorgung u. Beseitigung v. Umweltverschmutzungen (WZ08-E)	80,4	91,3	97,8	95,3	100,0	95,6	100,0
Baugewerbe (WZ08-F)	86,8	70,9	97,0	94,2	100,0	94,4	96,9
Handel; Instandhaltung u. Reparatur v. Kfz (WZ08-G)	87,2	88,4	99,4	93,1	98,9	96,5	98,3
Verkehr u. Lagerei (WZ08-H)	**77,4**	**68,2**	96,6	**91,0**	97,8	**89,3**	94,3
Gastgewerbe (WZ08-I)	83,7	74,0	**96,1**	94,1	96,2	91,6	93,1
Information u. Kommunikation (WZ08-J)	92,2	95,4	100,0	98,0	100,0	98,0	100,0
Erbringung v. Finanz- u. Versicherungsdienstl. (WZ08-K)	97,1	94,2	100,0	96,8	100,0	100,0	100,0
Grundstücks- u. Wohnungswesen (WZ08-L)	89,0	92,7	100,0	97,5	100,0	97,6	100,0
Freiberufl., wissenschaftl. u. techn. Dienstl. (WZ08-M)	89,5	94,8	100,0	98,0	98,9	98,9	98,0
Sonst. wirtschaftl. Dienstl. (WZ08-N)	91,5	86,3	100,0	97,1	100,0	99,1	99,5
Erziehung u. Unterricht (WZ08-P)	90,3	92,1	98,4	94,2	97,4	98,1	100,0
Gesundheits- u. Sozialwesen (WZ08-Q)	87,5	90,6	99,7	95,8	98,3	91,3	97,9
Kunst, Unterhaltung u. Erholung (WZ08-R)	94,7	94,7	100,0	91,2	100,0	94,7	100,0
Sonst. Dienstl. (WZ08-S)	98,3	85,7	100,0	95,2	100,0	99,2	**92,9**

IT-Sicherheitsmaßnahme: 8: Mindestanford. f. PW., 9: Individ. Vergabe v. Zugangs- u. Nutzerrechten je Aufg., 10: regelm. Backups, 11: phys. getrennte Aufbewahrung d. Backups, 12: aktuelle Antivirensoftware, 13: regelm. u. zeitnahe Installation verfügb. Sicherheitsupdates u. Patches, 14: Schutz d. IT-Systeme m. e. Firewall
Hervorhebung: fett: kleinster Anteil je IT-Sicherheitsmaßn.; grau hinterlegt: die dre kleinsten Anteile je IT-Sicherheitsmaßn.

Tabelle 47 **Organisatorische IT-Sicherheitsmaßnahmen nach WZ08-Klassen der zweiten Ebene**
in Prozent; gewichtete Daten

	IT-Sicherheitsmaßnahme						
WZ08-Klassen (Ebene 2; Kurzbezeichnung; nur wenn N≥30)	1	2	3	4	5	6	7
Landwirtschaft,Jagd u. verbundene Tätigkeiten (WZ08-01)	**35,3**	31,5		20,4	56,9	38,4	20,8
H.v.Nahrungs-u. Futtermitteln (WZ08-10)	60,3	50,0	69,0	14,0	37,3	43,8	15,3
H.v.Holz-,Flecht-,Korb- u.Korkwaren (oh.Möbel) (WZ08-16)	41,2	36,4		4,0	32,7	25,0	7,1
H.v.Druckerzgn.Vervielf. v.Ton-,Bild-,Datenträger (WZ08-18)	69,4	67,3	84,6	20,4	65,3	44,9	12,2
H.v.chem.Erzeugn. (WZ08-20)	60,5	71,1		21,2	44,7	84,6	23,7
H.v.Gummi-u. Kunststoffwaren (WZ08-22)	86,3	56,9	72,7	10,6	39,2	49,0	23,1
H.v.Glas,-waren,Keramik, Verarb.v.Steinen u.Erden (WZ08-23)	44,3	27,1	**54,8**	13,0	35,0	26,7	8,2
Metallerzeugung u.-bearbeitung (WZ08-24)	50,0	46,9			32,3	34,4	9,7
H.v.Metallerzeugnissen (WZ08-25)	64,8	54,7	78,5	18,8	55,2	47,7	37,8
H.v.DV-Gerät.,elektron. u.opt.Erzeugn. (WZ08-26)	68,5	63,0	57,1	18,9	57,4	70,4	31,5
H.v.elektr.Ausrüstg. (WZ08-27)	66,7	59,5	87,0	19,1	43,2	53,8	38,0
Maschinenbau (WZ08-28)	74,6	61,5	76,3	17,3	55,7	49,2	27,6
H.v.Möbeln (WZ08-31)	51,0	30,6		**2,0**	**16,3**	38,8	22,4
H.v.sonst.Waren (WZ08-32)	62,5	69,6	75,6	32,6	66,1	59,6	17,5
Sammlung,Abfallbeseitigung,Rückgewinnung (WZ08-38)	55,9	55,9			59,4	51,5	24,2
Hochbau (WZ08-41)	61,8	47,1	72,3	10,6	50,0	42,6	13,3
Tiefbau (WZ08-42)	37,7	**26,7**		21,7	53,3	**21,3**	29,5
Vorb.Baustellenarbeiten, Bauinstall.,sonst.Ausbau (WZ08-43)	46,8	31,1	72,8	16,1	41,3	28,3	12,5
Kfz-Handel;Instandh.u. Rep.v.Kfz (WZ08-45)	68,5	57,9	79,6	25,4	48,2	43,6	22,1
Großhandel (oh.Kfz) (WZ08-46)	71,4	60,0	81,6	25,1	51,0	56,2	24,4
Eh.(oh.Handel m.Kfz) (WZ08-47)	62,7	57,4	82,5	33,3	50,2	47,3	34,3
Landverkehr;Transport i. Rohrleitungen (WZ08-49)	42,4	34,5	71,6	18,7	42,9	31,3	17,1
Lagerei;sonst.Dienstleistg.f.d.Verkehr (WZ08-52)	52,6	56,1	66,7	32,7	42,1	50,9	28,1
Beherbergung (WZ08-55)	60,2	49,6	80,6	36,1	41,5	43,1	28,5
Gastronomie (WZ08-56)	67,6	52,2	85,4	28,6	38,0	38,0	11,8
Verlagswesen (WZ08-58)	54,8	64,5		30,0	61,3	54,8	22,6
Dienstleistg.d. Informat.technologie (WZ08-62)	92,0	79,5	80,5	38,3	73,0	84,3	61,8
Finanzdientleistg. (WZ08-64)	97,6	95,2	98,8	71,2	92,5	92,9	85,7
Grundstücks-u. Wohnungswesen (WZ08-68)	72,5	63,0	78,0	28,0	51,9	53,1	28,0
Rechts-u.Steuerberatung,Wirtschaftsprüfung (WZ08-69)	78,8	61,1	75,6	47,7	46,9	68,3	24,0
Verwaltung u.Führung v. Untern.,Untern.beratung (WZ08-70)	87,1	69,4	85,1	27,8	56,5	55,3	31,0
Architektur-,Ing.büros, techn.,physik.U.suchung (WZ08-71)	79,8	67,4	64,1	21,3	54,1	44,8	25,0
Werbung u.Marktforschung (WZ08-73)	69,7	69,7		18,8	81,8	81,8	33,3
Reisebüros,-veranstalter u.sonst.Reservierungen (WZ08-79)	77,1	77,1	90,0	52,3	66,7	58,3	33,3
Garten-u.Landschaftsbau; Gebäudebetreuung (WZ08-81)	69,2	39,4	71,4	10,6	53,2	24,2	**6,0**
Dienstleistg.f.Untern.u. Privatpers.ang (WZ08-82)	68,9	60,0	81,3	28,2	58,7	69,6	46,7
Erziehung u.Unterricht (WZ08-85)	77,6	60,5	78,5	22,3	51,3	60,6	23,9
Gesundheitswesen (WZ08-86)	75,8	66,7	86,7	40,0	54,8	64,6	13,5
Heime (oh.Erholungs- u.Ferienheime) (WZ08-87)	80,0	62,9	77,2	22,6	76,8	48,6	24,3
Sozialwesen(oh.Heime) (WZ08-88)	80,7	64,0	77,5	21,5	66,7	63,9	16,1
Diensleistg.d.Sports,d. Unterhaltg.u.Erholung (WZ08-93)	66,7	39,0		32,4	31,0	33,3	15,4
Interessenvertr.,kirchl. u.sonst.Vereinigungen (WZ08-94)	66,7	70,8	75,7	25,5	61,5	75,0	36,5
Sonst.übw.persönl. Dienstleistg. (WZ08-96)	55,6	39,7	79,2	18,5	59,4	44,1	29,0

IT-Sicherheitsmaßnahme: 1: schriftl. fix. Richtl. z. Informations-/IT-Sicherheit, 2: schriftl. fix. Richtl. z. Notfallmanagement, 3: Einhaltung d. Richtl. wird regelm. überprüft u. Verstöße ggf. geahndet, 4: Zertifizierung d. IT-Sicherheit, 5: regelm. Risiko- u. Schwachstellenanalysen, 6: Übungen/Simulationen f. d. Ausfall wichtiger IT-Systeme, 7: Schulungen z. IT-Sicherheit f. MA
Hervorhebung: fett: kleinster Anteil je IT-Sicherheitsmaßn.; grau hinterlegt: die fünf kleinsten Anteile je IT-Sicherheitsmaßn.

Tabelle 48 **Technische IT-Sicherheitsmaßnahmen nach WZ08-Klassen der zweiten Ebene**
in Prozent; gewichtete Daten

	IT-Sicherheitsmaßnahme						
WZ08-Klassen (Ebene 2; Kurzbezeichnung; nur wenn N≥30)	8	9	10	11	12	13	14
Landwirtschaft,Jagd u. verbundene Tätigkeiten (WZ08-01)	79,5	80,6	100,0	100,0	93,2	93,1	100,0
H.v.Nahrungs-u. Futtermitteln (WZ08-10)	**52,9**	59,7	92,6	91,4	100,0	91,7	100,0
H.v.Holz-,Flecht-,Korb- u.Korkwaren (oh.Möbel) (WZ08-16)	80,4	82,1	100,0	98,2	100,0	100,0	100,0
H.v.Druckerzgn.Vervielf. v.Ton-,Bild-,Datenträger (WZ08-18)	98,0	100,0	100,0	**81,3**	100,0	100,0	100,0
H.v.chem.Erzeugn. (WZ08-20)	84,2	100,0	100,0	100,0	100,0	100,0	100,0
H.v.Gummi-u. Kunststoffwaren (WZ08-22)	76,5	82,4	100,0	100,0	100,0	90,4	100,0
H.v.Glas,-waren,Keramik, Verarb.v.Steinen u.Erden (WZ08-23)	83,3	**58,2**	100,0	85,0	100,0	85,0	100,0
Metallerzeugung u.-bearbeitung (WZ08-24)	56,3	84,8	100,0	84,4	100,0	**71,9**	100,0
H.v.Metallerzeugnissen (WZ08-25)	80,2	84,5	99,5	96,9	97,5	91,9	97,4
H.v.DV-Gerät.,elektron. u.opt.Erzeugn. (WZ08-26)	94,4	100,0	100,0	98,1	100,0	100,0	100,0
H.v.elektr.Ausrüstg. (WZ08-27)	82,1	82,3	100,0	100,0	100,0	98,7	100,0
Maschinenbau (WZ08-28)	84,6	91,9	100,0	95,1	100,0	100,0	95,9
H.v.Möbeln (WZ08-31)	69,4	63,3	**89,8**	100,0	**89,8**	100,0	100,0
H.v.sonst.Waren (WZ08-32)	87,5	91,1	100,0	98,2	100,0	100,0	100,0
Sammlung,Abfallbeseitigung,Rückgewinnung (WZ08-38)	76,5	87,9	97,0	93,5	100,0	93,8	100,0
Hochbau (WZ08-41)	80,6	76,7	96,1	99,2	100,0	95,2	100,0
Tiefbau (WZ08-42)	83,3	69,2	100,0	90,9	100,0	91,8	91,8
Vorb.Baustellenarbeiten, Bauinstall.,sonst.Ausbau (WZ08-43)	89,0	69,2	96,6	93,0	100,0	94,3	96,8
Kfz-Handel;Instandh.u. Rep.v.Kfz (WZ08-45)	89,9	85,2	97,5	92,2	100,0	95,1	97,5
Großhandel (oh.Kfz) (WZ08-46)	87,5	95,1	100,0	94,6	98,8	98,5	98,8
Eh.(oh.Handel m.Kfz) (WZ08-47)	85,0	80,2	100,0	91,2	98,2	94,5	98,2
Landverkehr;Transport i. Rohrleitungen (WZ08-49)	72,6	59,7	95,2	92,7	99,3	86,3	92,1
Lagerei;sonst.Dienstleistg.f.d.Verkehr (WZ08-52)	86,0	82,5	98,2	85,7	93,0	91,2	94,8
Beherbergung (WZ08-55)	83,9	75,2	97,8	91,4	97,8	94,2	95,5
Gastronomie (WZ08-56)	83,1	71,8	91,5	100,0	91,5	86,4	87,3
Verlagswesen (WZ08-58)	87,1	100,0	100,0	90,3	100,0	100,0	100,0
Dienstleistg.d. Informat.technologie (WZ08-62)	96,6	98,9	100,0	100,0	100,0	96,6	100,0
Finanzdientleistg. (WZ08-64)	98,8	97,6	100,0	96,1	100,0	100,0	100,0
Grundstücks-u. Wohnungswesen (WZ08-68)	89,0	92,7	100,0	97,5	100,0	97,6	100,0
Rechts-u.Steuerberatung,Wirtschaftsprüfung (WZ08-69)	87,6	95,0	100,0	96,0	100,0	100,0	96,2
Verwaltung u.Führung v. Untern.,Untern.beratung (WZ08-70)	98,8	84,7	100,0	95,2	95,3	94,1	100,0
Architektur-,Ing.büros, techn.,physik.U.suchung (WZ08-71)	87,2	97,3	100,0	100,0	100,0	100,0	100,0
Werbung u.Marktforschung (WZ08-73)	100,0	100,0	100,0	100,0	97,0	100,0	87,5
Reisebüros,-veranstalter u.sonst.Reservierungen (WZ08-79)	98,0	91,8	100,0	100,0	100,0	100,0	100,0
Garten-u.Landschaftsbau; Gebäudebetreuung (WZ08-81)	87,9	83,3	100,0	91,9	100,0	100,0	100,0
Dienstleistg.f.Untern.u. Privatpers.ang (WZ08-82)	86,7	82,2	100,0	100,0	100,0	100,0	100,0
Erziehung u.Unterricht (WZ08-85)	90,3	92,1	98,4	94,2	97,4	98,1	100,0
Gesundheitswesen (WZ08-86)	83,3	84,4	99,0	100,0	100,0	93,8	100,0
Heime (oh.Erholungs- u.Ferienheime) (WZ08-87)	95,9	98,6	100,0	92,3	100,0	87,7	93,3
Sozialwesen(oh.Heime) (WZ08-88)	85,7	90,8	100,0	95,4	95,8	91,6	100,0
Diensleistg.d.Sports,d. Unterhaltg.u.Erholung (WZ08-93)	92,9	100,0	100,0	92,9	100,0	92,9	100,0
Interessenvertr.,kirchl. u.sonst.Vereinigungen (WZ08-94)	98,1	100,0	100,0	98,1	100,0	100,0	100,0
Sonst.übw.persönl. Dienstleistg. (WZ08-96)	98,5	73,9	100,0	92,8	100,0	98,5	**87,0**

IT-Sicherheitsmaßnahme: 8: Mindestanford. f. PW., 9: Individ. Vergabe v. Zugangs- u. Nutzerrechten je Aufg., 10: regelm. Backups, 11: phys. getrennte Aufbewahrung d. Backups, 12: aktuelle Antivirensoftware, 13: regelm. u. zeitnahe Installation verfügb. Sicherheitsupdates u. Patches, 14: Schutz d. IT-Systeme m. e. Firewall
Hervorhebung: fett: kleinster Anteil je IT-Sicherheitsmaßn.; grau hinterlegt: die fünf kleinsten Anteile je IT-Sicherheitsmaßn.

Tabelle 49 **Unternehmen mit Cyberversicherung nach WZ08-Klassen der zweiten Ebene**

in Prozent; gewichtete Daten

	Hat Ihr Unternehmen eine Versicherung gegen Informationssicherheitsverletzungen?			
WZ08-Klassen (Ebene 2; Kurzbezeichnung; nur wenn N≥30)	ja	nein	weiß nicht	N
Landwirtschaft,Jagd u. verbundene Tätigkeiten (WZ08-01)	**0,0**	87,5	12,5	40
H.v.Holz-,Flecht-,Korb- u.Korkwaren (oh.Möbel) (WZ08-16)	**0,0**	97,0	3,0	33
H.v.Metallerzeugnissen (WZ08-25)	21,7	57,6	20,7	92
H.v.elektr.Ausrüstg. (WZ08-27)	32,4	38,2	29,4	34
Maschinenbau (WZ08-28)	24,6	54,4	21,1	57
Hochbau (WZ08-41)	14,3	65,3	20,4	49
Tiefbau (WZ08-42)	5,3	92,1	2,6	38
Vorb.Baustellenarbeiten, Bauinstall.,sonst.Ausbau (WZ08-43)	14,5	72,9	12,6	214
Kfz-Handel;Instandh.u. Rep.v.Kfz (WZ08-45)	12,8	65,1	22,1	86
Großhandel (oh.Kfz) (WZ08-46)	16,8	56,7	26,4	208
Eh.(oh.Handel m.Kfz) (WZ08-47)	17,7	56,7	25,5	141
Landverkehr;Transport i. Rohrleitungen (WZ08-49)	17,9	74,4	7,7	78
Lagerei;sonst.Dienstleistg.f.d.Verkehr (WZ08-52)	9,1	75,8	15,2	33
Beherbergung (WZ08-55)	24,6	63,2	12,3	57
Gastronomie (WZ08-56)	19,4	77,4	3,2	31
Dienstleistg.d. Informat.technologie (WZ08-62)	8,1	62,2	29,7	37
Finanzdientleistg. (WZ08-64)	69,0	19,0	11,9	42
Grundstücks-u. Wohnungswesen (WZ08-68)	20,5	61,4	18,2	44
Rechts-u.Steuerberatung,Wirtschaftsprüfung (WZ08-69)	10,7	51,8	37,5	56
Verwaltung u.Führung v. Untern.,Untern.beratung (WZ08-70)	17,1	43,9	39,0	41
Architektur-,Ing.büros, techn.,physik.U.suchung (WZ08-71)	15,0	54,0	31,0	100
Garten-u.Landschaftsbau; Gebäudebetreuung (WZ08-81)	15,4	71,8	12,8	39
Erziehung u.Unterricht (WZ08-85)	15,3	63,8	20,9	177
Gesundheitswesen (WZ08-86)	46,9	28,6	24,5	49
Heime (oh.Erholungs- u.Ferienheime) (WZ08-87)	26,5	61,8	11,8	34
Sozialwesen(oh.Heime) (WZ08-88)	25,0	39,1	35,9	64
Interessenvertr.,kirchl. u.sonst.Vereinigungen (WZ08-94)	29,4	67,6	2,9	34
Sonst.übw.persönl. Dienstleistg. (WZ08-96)	22,7	65,9	11,4	44

Hervorhebung: fett: kleinster Anteil; grau hinterlegt: die fünf kleinsten Anteile

Tabelle 50 **Prävalenzraten für Cyberangriffe insg. nach WZ08-Klassen der zweiten Ebene**

in Prozent; gewichtete Daten

WZ08-Klassen (Ebene 2; Kurzbezeichnung; nur wenn N≥30)	Cyberangriffe insg.[322] Jahresprävalenz	Lebenszeitprävalenz[323]
Landwirtschaft,Jagd u. verbundene Tätigkeiten (WZ08-01)	23,6 (n=72)	48,5 (n=68)
H.v.Nahrungs-u. Futtermitteln (WZ08-10)	35,6 (n=73)	58,8 (n=68)
H.v.Holz-,Flecht-,Korb- u.Korkwaren (oh.Möbel) (WZ08-16)	28,3 (n=60)	36,4 (n=55)
H.v.Druckerzgn.Vervielf. v.Ton-,Bild-,Datenträger (WZ08-18)	46,9 (n=49)	87,8 (n=49)
H.v.chem.Erzeugn. (WZ08-20)	46,2 (n=39)	71,1 (n=38)
H.v.Gummi-u. Kunststoffwaren (WZ08-22)	46,2 (n=52)	68,6 (n=51)
H.v.Glas,-waren,Keramik, Verarb.v.Steinen u.Erden (WZ08-23)	60,0 (n=60)	**94,5** (n=55)
Metallerzeugung u.-bearbeitung (WZ08-24)	43,8 (n=32)	
H.v.Metallerzeugnissen (WZ08-25)	41,4 (n=198)	64,6 (n=192)
H.v.DV-Gerät.,elektron. u.opt.Erzeugn. (WZ08-26)	40,7 (n=54)	74,1 (n=54)
H.v.elektr.Ausrüstg. (WZ08-27)	49,4 (n=79)	71,8 (n=78)
Maschinenbau (WZ08-28)	56,1 (n=123)	80,3 (n=117)
H.v.Möbeln (WZ08-31)	46,9 (n=49)	70,8 (n=48)
H.v.sonst.Waren (WZ08-32)	46,4 (n=56)	85,7 (n=56)
Sammlung,Abfallbeseitigung,Rückgewinnung (WZ08-38)	25,0 (n=32)	61,3 (n=31)
Hochbau (WZ08-41)	26,6 (n=128)	58,8 (n=119)
Tiefbau (WZ08-42)	22,7 (n=66)	37,7 (n=61)
Vorb.Baustellenarbeiten, Bauinstall.,sonst.Ausbau (WZ08-43)	39,1 (n=442)	52,7 (n=431)
Kfz-Handel;Instandh.u. Rep.v.Kfz (WZ08-45)	46,3 (n=203)	72,4 (n=203)
Großhandel (oh.Kfz) (WZ08-46)	53,1 (n=416)	73,7 (n=410)
Eh.(oh.Handel m.Kfz) (WZ08-47)	38,6 (n=277)	63,8 (n=271)
Landverkehr;Transport i. Rohrleitungen (WZ08-49)	26,7 (n=146)	47,6 (n=143)
Lagerei;sonst.Dienstleistg.f.d.Verkehr (WZ08-52)	32,8 (n=58)	52,6 (n=57)
Beherbergung (WZ08-55)	33,6 (n=137)	57,8 (n=135)
Gastronomie (WZ08-56)	33,8 (n=71)	64,2 (n=67)
Verlagswesen (WZ08-58)	**71,0** (n=31)	86,7 (n=30)
Dienstleistg.d. Informat.technologie (WZ08-62)	40,9 (n=88)	62,5 (n=88)
Finanzdientleistg. (WZ08-64)	29,4 (n=85)	54,4 (n=79)
Grundstücks-u. Wohnungswesen (WZ08-68)	35,8 (n=81)	55,0 (n=80)
Rechts-u.Steuerberatung,Wirtschaftsprüfung (WZ08-69)	34,3 (n=105)	58,1 (n=105)
Verwaltung u.Führung v. Untern.,Untern.beratung (WZ08-70)	48,8 (n=86)	79,0 (n=81)
Architektur-,Ing.büros, techn.,physik.U.suchung (WZ08-71)	53,4 (n=193)	73,8 (n=187)
Werbung u.Marktforschung (WZ08-73)	24,2 (n=33)	45,5 (n=33)
Reisebüros,-veranstalter u.sonst.Reservierungen (WZ08-79)	56,3 (n=48)	75,0 (n=48)
Garten-u.Landschaftsbau; Gebäudebetreuung (WZ08-81)	62,1 (n=66)	79,0 (n=62)
Dienstleistg.f.Untern.u. Privatpers.ang (WZ08-82)	34,8 (n=46)	76,1 (n=46)
Erziehung u.Unterricht (WZ08-85)	46,7 (n=317)	77,2 (n=312)
Gesundheitswesen (WZ08-86)	30,2 (n=96)	61,1 (n=90)
Heime (oh.Erholungs- u.Ferienheime) (WZ08-87)	25,3 (n=75)	40,5 (n=74)
Sozialwesen(oh.Heime) (WZ08-88)	45,4 (n=119)	62,2 (n=119)
Diensleistg.d.Sports,d. Unterhaltg.u.Erholung (WZ08-93)	24,4 (n=41)	52,4 (n=42)
Interessenvertr.,kirchl. u.sonst.Vereinigungen (WZ08-94)	62,3 (n=53)	94,2 (n=52)
Sonst.übw.persönl. Dienstleistg. (WZ08-96)	20,3 (n=69)	47,1 (n=68)

Hervorhebung: fett: größter Anteil; grau hinterlegt: die fünf größten Anteile

[322] Zur Beschreibung der einbezogenen Angriffsarten siehe Kapitel 6 auf S. 89.

[323] Siehe Fn. 268 (S. 102).

Tabelle 51 **Jahresprävalenzraten nach Cyberangriffsart und WZ08-Klassen der zweiten Ebene**
in Prozent; gewichtete Daten

	Cyberangriffsart							
WZ08-Klassen (Ebene 2; Kurzbezeichnung; nur wenn N≥30)	1	2	3	4	5	6	7	8
Landwirtschaft,Jagd u. verbundene Tätigkeiten (WZ08-01)	13,7	6,8	8,3	0,0	7,4	0,0	1,4	8,3
H.v.Nahrungs-u. Futtermitteln (WZ08-10)	4,1	3,2	9,9	0,0	6,9	0,0	2,7	19,4
H.v.Holz-,Flecht-,Korb- u.Korkwaren (oh.Möbel) (WZ08-16)	23,3	23,3	18,3	0,0	16,1	0,0	11,7	25,0
H.v.Druckerzgn.Vervielf. v.Ton-,Bild-,Datenträger (WZ08-18)	4,1	0,0	24,5	10,4	10,4	2,0	2,3	33,3
H.v.chem.Erzeugn. (WZ08-20)	15,8	13,2	28,9	0,0	0,0	**13,2**	2,6	28,9
H.v.Gummi-u. Kunststoffwaren (WZ08-22)	15,7	13,7	9,8	0,0	3,9	1,9	5,9	19,6
H.v.Glas,-waren,Keramik, Verarb.v.Steinen u.Erden (WZ08-23)	21,4	**26,8**	37,5	8,9	**30,0**	0,0	10,0	36,7
Metallerzeugung u.-bearbeitung (WZ08-24)	3,1	3,1	9,4	0,0	0,0	3,1	21,9	37,5
H.v.Metallerzeugnissen (WZ08-25)	11,2	3,1	16,9	1,0	1,6	1,1	6,6	25,6
H.v.DV-Gerät.,elektron. u.opt.Erzeugn. (WZ08-26)	13,0	3,7	14,8	0,0	3,7	1,9	5,6	24,5
H.v.elektr.Ausrüstg. (WZ08-27)	20,3	8,1	32,1	6,4	1,3	6,8	9,0	23,1
Maschinenbau (WZ08-28)	22,2	32,2	39,2	1,6	2,7	6,0	16,9	38,3
H.v.Möbeln (WZ08-31)	12,2	12,2	14,3	0,0	18,8	10,4	10,4	32,7
H.v.sonst.Waren (WZ08-32)	**26,8**	23,2	28,6	1,8	8,9	11,5	3,6	38,2
Sammlung,Abfallbeseitigung,Rückgewinnung (WZ08-38)	9,4	6,5	12,5	0,0	6,5	0,0	9,4	9,4
Hochbau (WZ08-41)	16,3	8,5	12,5	3,9	3,9	0,0	9,3	2,3
Tiefbau (WZ08-42)	9,1	9,1	18,2	1,5	0,0	0,0	9,1	11,5
Vorb.Baustellenarbeiten, Bauinstall.,sonst.Ausbau (WZ08-43)	8,1	10,3	23,7	1,1	3,7	1,1	3,0	23,6
Kfz-Handel;Instandh.u. Rep.v.Kfz (WZ08-45)	19,1	20,7	27,2	4,9	5,4	3,0	12,8	23,2
Großhandel (oh.Kfz) (WZ08-46)	10,1	12,0	26,1	5,2	5,4	1,5	11,4	26,7
Eh.(oh.Handel m.Kfz) (WZ08-47)	17,6	9,3	19,0	5,5	4,1	5,4	4,3	17,0
Landverkehr;Transport i. Rohrleitungen (WZ08-49)	6,3	9,1	12,8	2,1	4,8	4,1	7,6	11,8
Lagerei;sonst.Dienstleistg.f.d.Verkehr (WZ08-52)	12,5	3,5	15,8	0,0	1,8	1,8	8,8	17,9
Beherbergung (WZ08-55)	16,1	6,6	21,3	2,2	6,0	2,9	2,2	18,7
Gastronomie (WZ08-56)	1,4	23,9	18,8	4,2	8,8	4,4	8,7	20,6
Verlagswesen (WZ08-58)	6,3	3,2	**58,1**	0,0	15,6	12,9	3,2	**53,3**
Dienstleistg.d. Informat.technologie (WZ08-62)	8,0	4,5	17,2	1,1	21,6	1,1	6,8	17,0
Finanzdientleistg. (WZ08-64)	3,5	10,8	15,7	0,0	2,4	0,0	3,5	22,2
Grundstücks-u. Wohnungswesen (WZ08-68)	12,5	8,8	15,2	1,2	8,8	3,7	12,2	25,0
Rechts-u.Steuerberatung,Wirtschaftsprüfung (WZ08-69)	14,3	6,7	11,4	0,0	1,0	0,0	1,9	24,0
Verwaltung u.Führung v. Untern.,Untern.beratung (WZ08-70)	12,9	10,1	44,7	**10,6**	8,3	5,9	9,4	17,9
Architektur-,Ing.büros, techn.,physik.U.suchung (WZ08-71)	18,1	12,8	24,9	6,8	11,5	7,3	10,9	27,7
Werbung u.Marktforschung (WZ08-73)	3,0	3,1	3,1	0,0	15,2	0,0	3,0	21,2
Reisebüros,-veranstalter u.sonst.Reservierungen (WZ08-79)	2,1	8,9	24,5	0,0	2,1	8,3	**31,3**	39,6
Garten-u.Landschaftsbau; Gebäudebetreuung (WZ08-81)	16,1	12,7	25,8	7,6	11,9	1,6	15,2	28,8
Dienstleistg.f.Untern.u. Privatpers.ang (WZ08-82)	4,4	7,1	8,7	2,3	4,8	0,0	17,4	24,4
Erziehung u.Unterricht (WZ08-85)	16,4	14,8	21,7	2,6	8,3	5,0	7,4	16,8
Gesundheitswesen (WZ08-86)	9,5	15,8	12,4	0,0	10,4	5,6	14,6	14,6
Heime (oh.Erholungs- u.Ferienheime) (WZ08-87)	11,4	10,7	13,5	0,0	1,3	0,0	1,4	20,3
Sozialwesen(oh.Heime) (WZ08-88)	14,0	9,5	32,2	4,2	1,7	9,2	17,6	31,1
Diensleistg.d.Sports,d. Unterhaltg.u.Erholung (WZ08-93)	16,7	2,4	9,5	0,0	2,4	2,4	2,4	4,8
Interessenvertr.,kirchl. u.sonst.Vereinigungen (WZ08-94)	5,8	12,2	27,1	2,1	20,8	0,0	25,0	30,8
Sonst.übw.persönl. Dienstleistg. (WZ08-96)	1,4	1,6	10,3	0,0	0,0	0,0	2,9	10,3

Cyberangriffsart: 1: Ransomware, 2: Spyware, 3: sonst. Schadsoftware, 4: manuelles Hacking, 5: (D)DoS, 6: Defacing, 7: CEO-Fraud, 8: Phishing
Hervorhebung: fett: größter Anteil je Angriffsart; grau hinterlegt: die fünf größten Anteile je Angriffsart

Tabelle 52 **Anteil der Unternehmen mit betroffenen Daten nach Datenart und WZ08-Klassen der zweiten Ebene**
in Prozent; gewichtete Daten

	Datenart					
WZ08-Klasse (Ebene 2; Kurzbezeichnung; nur wenn N≥30)	1	2	3	4	5	N
H.v.Metallerzeugnissen (WZ08-25)	21,3	9,8	16,4	4,9	1,6	61
H.v.elektr.Ausrüstg. (WZ08-27)	15,8	0,0	0,0	13,5	2,9	37
Maschinenbau (WZ08-28)	43,9	19,3	3,6	22,8	**30,4**	57
Hochbau (WZ08-41)	0,0	0,0	0,0	0,0	0,0	33
Vorb.Baustellenarbeiten, Bauinstall.,sonst.Ausbau (WZ08-43)	25,6	6,9	12,5	9,4	6,3	160
Kfz-Handel;Instandh.u. Rep.v.Kfz (WZ08-45)	**57,5**	**28,7**	**27,6**	23,0	23,0	87
Großhandel (oh.Kfz) (WZ08-46)	21,3	10,6	10,6	13,8	7,4	188
Eh.(oh.Handel m.Kfz) (WZ08-47)	30,7	10,0	11,3	**29,7**	9,9	100
Landverkehr;Transport i. Rohrleitungen (WZ08-49)	17,1	16,7	2,9	5,6	5,6	36
Beherbergung (WZ08-55)	23,3	21,4	16,3	0,0	2,3	43
Dienstleistg.d. Informat.technologie (WZ08-62)	2,9	2,8	0,0	2,8	0,0	35
Rechts-u.Steuerberatung,Wirtschaftsprüfung (WZ08-69)	31,4	20,0	5,7	14,3	28,6	34
Verwaltung u.Führung v. Untern.,Untern.beratung (WZ08-70)	30,6	13,9	13,9	27,0	16,2	36
Architektur-,Ing.büros, techn.,physik.U.suchung (WZ08-71)	22,7	6,7	11,9	12,4	10,2	88
Garten-u.Landschaftsbau; Gebäudebetreuung (WZ08-81)	30,0	11,1	9,8	0,0	9,8	40
Erziehung u.Unterricht (WZ08-85)	22,3	10,7	3,3	11,6	9,1	121
Sozialwesen(oh.Heime) (WZ08-88)	38,6	20,5	4,5	6,8	27,3	44

Datenart: 1: Daten insg., 2: nicht öffentl. Kundendaten, 3: nicht öffentl. Daten von Geschäftspartnern*innen, 4: Produktdaten, 6: Strategie-, Vertriebs- u. Finanzinfo.
Hervorhebung: fett: größter Anteil je Datenart; grau hinterlegt: die drei größten Anteile je Datenart

Tabelle 53 **Übersicht zum Forschungsstand in Kapitel 2**

	Merkmale	Studien/Berichte 1	2	3	4	5
formal	**Autor*in/ Institution**	Bitkom e.V.	Bitkom e.V.	Bundeskriminalamt (BKA)	BSI, Allianz für Cybersicherheit	BSI, Allianz für Cybersicherheit
	Erscheinungsjahr	2017	2018	2018	2018	2019
	Titel	Wirtschaftsschutz in der digitalen Welt	Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie	Cybercrime - Bundeslagebild 2017	Cyber-Sicherheits-Umfrage 2017	Cyber-Sicherheits-Umfrage 2018 (Fassung 18.04.2019)
methodisch	**Methode**	CATI	CATI	Sekundäranalyse (PKS)	Onlinebefragung	Onlinebefragung
	Region	DEU	DEU	DEU	DEU	DEU
	Erhebungszeitraum	01.-03.2017	05.2018	2017	10.-11.2017	02.-03.2019
	Grundgesamtheit	alle Unternehmen >10 Besch.	Industrieunternehmen >10 Besch.	n.r.	k.A.	k.A.
	Auswahlgesamtheit (Kontaktdaten)	k.A.	k.A.	n.r.	k.A.	k.A.
	Stichprobenart	geschichtete Zufallsstichprobe	geschichtete Zufallsstichprobe	n.r.	willkürliche Stichprobe	willkürliche Stichprobe
	Nettostichprobe	1.069	503	n.r.	879	1.039
	Branchendifferenzierung	Keine Branchen genannt	5 Branchen Chemie/Pharma, Automobil, Maschinen- u. Anlagenbau, H.v. Kommunikation/Elektronik, Sonst.	n.r.	4 Branchen Anwenderunternehmen (49%), IT-DL/Hersteller/Provider (20%), Sonstige (17%), Öffentlicher Dienst (14%)	4 Branchen Andere (54%), Information & Kommunikation (18%), Energieversorgung (17%), Öffentliche Verwaltung (11%)
	Größendifferenzierung	10-99 100-499 > 500	10-99 100-499 > 500	n.r.	1-499 MA (66%) >500 MA (33%)	1-249 MA (57%) >250 MA (43%)
inhaltlich	**Risikoeinschätzung**				✓	✓
	Prävalenz	✓	✓		✓	✓
	IT-Sicherheitsstrukturen	✓	✓		✓	✓
	Investitionen/ Budget					
	Nicht-finanzielle Schäden/ Folgen	✓	✓	✓	✓	✓
	Entstandene Kosten in EUR	✓	✓	✓		
	Anzeigeverhalten	✓	✓	✓		
	Cyberversicherungen		✓			
	Handlungsempfehlungen		✓			

	Merkmale	Studien 6	7	8	9	10
formal	**Autor*in/ Institution**	BSI, Allianz für Cybersicherheit	Bundesdruckerei GmbH	CISCO Inc.	DsiN e.V.	Eco e.V.
	Erscheinungsjahr	2016	2017	2017	2016	2017
	Titel	Umfrage zur Betroffenheit durch Ransomware	Digitalisierung und IT-Sicherheit in deutschen Unternehmen	2017 Annual Cybersecurity Report/ Security Capabilities Benchmark Study	Sicherheitsmonitor Mittelstand 2016	eco Studie IT-Sicherheit 2017
methodisch	**Methode**	Onlinebefragung	CATI	k.A.	Onlinebefragung	Experteninterviews
	Region	DEU	DEU	International (13 Länder)	DEU	DEU
	Erhebungszeitraum	04.2016	02.-03.2017	k.A.	06.15-03.2016	k.A.
	Grundgesamtheit	k.A.	alle Unternehmen >20 Besch.	k.A.	k.A.	k.A.
	Auswahlgesamtheit (Kontaktdaten)	k.A.	k.A.	k.A.	k.A.	k.A.
	Stichprobenart	k.A.	geschichtete Zufallsstichprobe	k.A.	k.A.	k.A.
	Nettostichprobe	592	500	2.912	1.320	590
	Branchendifferenzierung	keine Branchen genannt	9 Branchen **Top 3:** Maschinen/Anlagenbau (13%), Banken/Versicherungen (13%), IT/Telekommunikation (13%)	11 Branchen **Top 3:** Financial Services (18%), Non-Key Industry (16%), Manufacturing (12%)	Keine Branchen genannt	7 Branchen **Top 3:** IT/TK (49%), Dienstleistungen (21%), Öffentliche Einrichtungen (9%)
	Größendifferenzierung	1-49 (30%) 50-249 (20%) 250-999 (20%) 1.000-10.000 (20%) >10.000 (7%)	20-99 (35%) 100-499 (35%) 500-1.999 (20%) >2.000 (10%)	250-999 (50%) 1.000-9.999 (38%) >10.000 (12%)	1-9 (34%) 10-50 (26%) 51-200 (18%) 201-500 (10%) <500 (12%)	1-10 (24%) 11-50 (24%) 51-250 (18%) 251-1000 (15%) <1000 (18%)
inhaltlich	**Risikoeinschätzung**	✓		✓		✓
	Prävalenz	✓				
	IT-Sicherheitsstrukturen	✓	✓	✓	✓	✓
	Investitionen/ Budget		✓	✓		✓
	Nicht-finanzielle Schäden/ Folgen	✓		✓		
	Entstandene Kosten in EUR	✓				
	Anzeigeverhalten	✓				
	Cyberversicherungen					
	Handlungsempfehlungen				✓	

	Merkmale	Studien 11	12	13	14	15
formal	**Autor*in/ Institution**	GDV e.V.	Gehem et al. (The Hague Centre for Strategic Studies)	Hillebrand et al. (wik GmbH)	Hiscox Ltd	IBM Cooperation
	Erscheinungsjahr	2018	2015	2017	2018	2018
	Titel	Cyberrisiken im Mittelstand	Assessing Cyber Security	Aktuelle Lage der IT-Sicherheit in KMU	Hiscox Cyber Readiness Report	IBM X-Force Threat Intelligence Index 2018
methodisch	**Methode**	Interviews	Qualitative Meta-Analyse verfüg. Berichte	CATI	Onlinebefragung	Sekundäranalyse Kundensystem-daten
	Region	DEU	International (15 Länder)	DEU	International (5 Länder)	International
	Erhebungszeitraum	03.-04.2018	k.A.	03.-05.2017	10.-11.2017	2017
	Grundgesamtheit	k.A.	n.r.	alle Unternehmen relev. Branchen m. 1-499 Besch.	k.A.	k.A.
	Auswahlgesamtheit (Kontaktdaten)	k.A.	n.r.	kommezielle Firmendatenbank	k.A.	k.A.
	Stichprobenart	k.A.	n.r.	geschichtete Zufallsstichprobe	k.A.	k.A.
	Nettostichprobe	300	65 Reports	1.508	4.103	> 1 Mio
	Branchendifferenzierung	k.A.	n.r.	12 Branchen nach WZ-Klassen	16 Branchen **Top 3:** Technology/ Media/ Communication (14%), Retail & Wholesale (8%), Healthcare & Pharmaceutical (8%)	5 Branchen Financial Services, Information & Communication, Manufacturing, Retail, Professional Services
	Größendifferenzierung	k.A.	n.r.	1-49 (33%) 50-99 (33%) 100-499 (33%)	2-249 (70%) >250 (30%)	k.A.
inhaltlich	**Risikoeinschätzung**	✓		✓	✓	
	Prävalenz		✓		✓	✓
	IT-Sicherheitsstrukturen	✓		✓	✓	✓
	Investitionen/ Budget	✓		✓	✓	
	Nicht-finanzielle Schäden/ Folgen	✓	✓	✓	✓	
	Entstandene Kosten in EUR		✓		✓	
	Anzeigeverhalten					
	Cyberversicherungen	✓			✓	
	Handlungsempfehlungen	✓		✓		

	Merkmale	Studien 16	17	18	19	20
formal	**Autor*in/ Institution**	IHK Nord	Institut für Demoskopie Allensbach (i.A. Deutsche Telekom)	Maria Kjaerland	Klahr et al. (i.A. UK Department for Culture, Media & Sport)	Bollhöfer & Jäger (MPI)
	Erscheinungsjahr	2013	2015	2006	2017	2018
	Titel	Unternehmens-befragung zur Betroffenheit der norddeutschen Wirtschaft von Cybercrime	Cyber Security Report 2015	A taxonomy and comparison of computer security incidents from the commercial and government sectors	Cyber Security Breaches Survey 2017	Wirtschaftsspionage und Konkurrenzausspähung
methodisch	**Methode**	Onlinebefragung	CATI	Sekundäranalyse Eventdaten (CERT CC)	CATI + Face-to-Face-Interviews	Paper-Pencil- + Onlinebefragung
	Region	DEU	DEU	USA	UK	DEU
	Erhebungszeitraum	01.-02.2013	08.-10.2015	2001/02	10.2016-01.2017	06.-09.2017
	Grundgesamtheit	Mitgliedsunternehmen div. Verbände in Norddtl.	k.A.	n.r.	k.A.	Industrienahe Unt. <251 Besch.
	Auswahlgesamtheit (Kontaktdaten)	6.000 Unternehmen angeschrieben	k.A.	n.r.	k.A.	23.462 Unternehmen, auf Basis Hoppenstedt Firmendatenbank, 6.284 angeschrieben
	Stichprobenart	k.A.	k.A.	n.r.	Zufallsstichprobe	Zufallsstichprobe
	Nettostichprobe	713	645	1.397	1.523	583
	Branchendifferenzierung	4 Branchen Dienstleistungswirtschaft (47%), Industrie (24%), Handel (17%), Sonstige (12%)	keine Branchen genannt	kommerzieller u. öffentlicher Sektor	Alle Branchen exklusive Einzelunternehmen, Öffentlicher Sektor, Forst- und Landwirtschaft, Fischerei und Bergbau	15 Branchen des produzierenden Gewerbes bzw. industrienahen DL **Top 3:** Maschinenbau (23%), Metallindustrie (15%), Elektrotechnik (11%)
	Größendifferenzierung	1-10 (21%) 11-50 (26%) 51-100 (11%) 101-250 (16%) >250 (26%)	50-99 100-249 250-999 >1.000	k.A.	2-9 (33%) 10-49 (31%) 50-249 (24%) >250 (11%)	1-9 (5%) 10-49 (41%) 50-249 (44%) >250 (10%)
inhaltlich	**Risikoeinschätzung**	✓	✓		✓	✓
	Prävalenz	✓			✓	✓
	IT-Sicherheitsstrukturen	✓			✓	✓
	Investitionen/ Budget	✓	✓		✓	
	Nicht-finanzielle Schäden/ Folgen	✓			✓	✓
	Entstandene Kosten in EUR				✓	
	Anzeigeverhalten	✓			✓	✓
	Cyberversicherungen				✓	
	Handlungsempfehlungen	✓			✓	

	Merkmale	Studien 21	22	23	24	25
formal	**Autor*in/ Institution**	Paoli et al.	Ponemon Institute (i.A. Accenture)	Ponemon Institute (i.A. IBM)	Ponemon Institute (i.A. IBM)	PwC Network
	Erscheinungsjahr	2018	2017	2016	2017	2018
	Titel	The impact of cybercrime on businesses	COST OF CYBER CRIME STUDY	The Cyber Resilient Organization in Germany	2017 Cost of Data Breach Study	1. Strengthening digital society against cyber shocks und 2. Revitalizing privacy and trust in a data-driven world
methodisch	**Methode**	Onlinebefragung	Qualitative Interviews	Fragebogen	Qualitative Interviews	Onlinebefragung
	Region	BEL	International (7 Länder)	DEU, US, UK	International	International (122 Länder)
	Erhebungszeitraum	07.-08.2016	k.A.	05.2015	k.A.	04.-05.2017
	Grundgesamtheit	alle bel. Unternehmen mit bes. Relevanz für Cyberangriffe	k.A.	k.A.	k.A.	k.A.
	Auswahlgesamtheit (Kontaktdaten)	9.249 Unt. mit bes. Relevanz zu Cyberangriffen (Handel, DL, Finanzen) auf Basis FEB-Daten wurden kontaktiert	k.A.	k.A.	k.A.	k.A.
	Stichprobenart	Bewusste Auswahl	k.A.	k.A.	k.A.	k.A.
	Nettostichprobe	310	254	445	419	9.500
	Branchendifferenzierung	4 Branchen Other (57%), Technology (23%), Chemical & Life Science (10%), Commerce & Services (10%)	15 Branchen mit < 2.000 bis >25.000 **Top 3:** Financial (16%), Industrial (12%), Services (11%)	14 Branchen **Top 3:** Financial Services (15%), Public Sector (11%), Health & Pharmaceuticals (10%)	17 Branchen **Top 3:** Financial (15%), Industrial (15%), Services (14%)	k.A.
	Größendifferenzierung	1-49 (52%) 50-249 (22%) >250 (27%)	<2.000 (11%) 2.000-5.000 (17%) 5.001-10.000 (22%) >10.001 (50%)	1-499 (11%) 500-1.000 (19%) 1.001-5.000 (27%) 5.001-10.000 (24%) >10.000 (19%)	1-499 (12%) 500-1.000 (20%) 1.001-5.000 (26%) 5.001-10.000 (21%) >10.000 (21%)	k.A.
inhaltlich	**Risikoeinschätzung**			✓		✓
	Prävalenz	✓				
	IT-Sicherheitsstrukturen		✓	✓		✓
	Investitionen/ Budget		✓	✓		
	Nicht-finanzielle Schäden/ Folgen	✓	✓			
	Entstandene Kosten in EUR	✓	✓		✓	
	Anzeigeverhalten					
	Cyberversicherungen					
	Handlungsempfehlungen					

	Merkmale	Studien 26	27	28	29	30
formal	**Autor*in/ Institution**	PwC AG	PwC Strategy& (i.A. BMI)	Sasha Romanosky	Ramona Rantala (U.S. Department of Justice)	Osborne et al. (UK Home Office)
	Erscheinungsjahr	2017	2016	2016	2008	2018
	Titel	Im Visier der Cyber-Gangster	Cybersicherheits-strategie	Examining the costs and causes of cyber incidents	Cybercrime against Businesses, 2005	Crime against businesses: Findings from the 2017 Commercial Victimisation Survey
methodisch	**Methode**	CATI	Onlinebefragung	Sekundäranalyse wirtschaftl. Verlustdaten	Paper-Pencil-Befragung	CATI
	Region	DEU	DEU	USA	USA	England, Wales
	Erhebungszeitraum	09.-10.2016	04.-05.2016	k.A.	k.A.	09.-12.2017
	Grundgesamtheit	k.A.	k.A.	k.A.	k.A.	Alle Unternehmen in England und Wales mit mehr als 79.000 GBP Umsatz
	Auswahlgesamtheit (Kontaktdaten)	k.A.	Verbandsunternehmen von BDI, BITKOM, DIHK, UP KRITIS	Kommerzielle Firmendatenbank	Kommerzielle Firmendatenbank Dunn & Bradstreet	Interdepartmental Business Register (IDBR))
	Stichprobenart	k.A.	k.A.		geschichtete Zufallssichtprobe	geschichtete Zufallssichtprobe
	Nettostichprobe	400	309	>12.000 Beobachtungen	8.079	1.865 (Split Half: 4.027)
	Branchendifferenzierung	9 Branchen **Top 3**: Sonstige (22%), Industrie (20%), Handel/Konsum (20%)	19 Branchen **Top 3:** Produzierendes Gewerbe (17%), IT-Dienstleister (16%), Energieversorgung (13%)	10 Branchen nach NAICS	36 Branchen nach NAICS **Top 3:** Manufacturing, Healthcare, Utilities	4 Branchen nach UK SIC Produzierendes Gewerbe (26%), Unterhaltung & Kunst (25%), Groß- & Einzelhandel (24%), Forst- & Landwirtschaft (24%)
	Größendifferenzierung	200-499 MA (50%) 500-1.000 MA (50%)	1-9 (9%) 10-49 (14%) 50-249 (23%) 250-499 (9%) 500-999 (10%) 1.000-9.999 (20%) >10.000 (15%)	k.A.	2-24 (18%) 25-99 (22%) 100-999 (25%) >1.000 (27%)	1-9 (57%) 10-49 (24%) >50 (19%)
inhaltlich	**Risikoeinschätzung**	✓	✓			
	Prävalenz	✓	✓	✓	✓	✓
	IT-Sicherheitsstrukturen	✓	✓		✓	✓
	Investitionen/ Budget	✓	✓			
	Nicht-finanzielle Schäden/ Folgen	✓		✓	✓	
	Entstandene Kosten in EUR	✓		✓	✓	
	Anzeigeverhalten		✓			
	Cyberversicherungen					
	Handlungsempfehlungen	✓				

	Merkmale	Studien 31	32
formal	**Autor*in/ Institution**	Vanson Bourne (i.A. Dell Inc.)	Verizon LLC
	Erscheinungsjahr	2014	2018
	Titel	Protecting the organization against the unknown	2018 Data Breach Investigations Report
methodisch	**Methode**	Onlinebefragung + CATI	Sekundäranalyse Kundensystemdaten
	Region	International	International
	Erhebungszeitraum	10.-11.2013	k.A.
	Grundgesamtheit	k.A.	k.A.
	Auswahlgesamtheit (Kontaktdaten)	k.A.	k.A.
	Stichprobenart	k.A.	k.A.
	Nettostichprobe	1.440	> 1 Mio. Beobachtungen
	Branchendifferenzierung	keine Branchen genannt	21 Branchen
	Größendifferenzierung	501-1.000 (23%) 1001-3.000 (23%) 3.001-5.000 (23%) 5.001-10.000 (23%) >10.000 (8%)	k.A.
inhaltlich	**Risikoeinschätzung**	✓	
	Prävalenz		✓
	IT-Sicherheitsstrukturen	✓	✓
	Investitionen/ Budget	✓	
	Nicht-finanzielle Schäden/ Folgen		
	Entstandene Kosten in EUR	✓	
	Anzeigeverhalten		
	Cyberversicherungen		
	Handlungsempfehlungen		

ANHANG 2: FRAGEBOGEN

Kurzdarstellung des eingesetzten Fragebogens

A Einstieg

A01 In welchem Bereich sind Sie in Ihrem Unternehmen tätig?
(Geschäftsführung/ Vorstand; IT & Informationssicherheit; Datenschutz; Werkssicherheit; Revision/ Prüfung; Externer Dienstleister; Sonstiges [mit Freitext]; Weiß nicht; Keine Angabe [Mehrfachantworten möglich])

A02 Was denken Sie: Warum könnte Ihr Unternehmen Ziel eines Cyberangriffs werden? Haben Sie …?
(Besondere Produkte, Herstellungsverfahren oder Dienstleistungen [z.B. aufgrund spezieller Technik, Design, Materialien, Innovation]; Besondere Reputation/ Kundenkreis [z.B. hoher Bekanntheitsgrad, hohe Sicherheitsstandards, besondere Verschwiegenheit]), Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; Keine Angabe)

A03 Wie hoch schätzen Sie das Risiko für Ihr Unternehmen ein, in den nächsten 12 Monaten von einem Cyberangriff geschädigt zu werden, …
(… der gleichzeitig auch viele andere Unternehmen trifft? [z.B. massenhaft versendete Schadsoftware]; … der ausschließlich Ihr Unternehmen trifft? [z.B. gezielter Spionageangriff]), Antwortmöglichkeiten: (Sehr gering; Eher gering; Eher hoch; Sehr hoch; Weiß nicht; Keine Angabe)

B Erlebte Angriffe

B01 Immer bezogen auf die letzten 12 Monate: Wie oft war Ihr Unternehmen von folgenden Angriffsarten betroffen und musste reagieren?
(Ransomware, die das Ziel hatte, Unternehmensdaten zu verschlüsseln; Spyware, die das Ziel hatte, Nutzeraktivitäten oder sonstige Daten auszuspähen; Sonstige Schadsoftware – z.B. Viren, Würmer oder Trojaner; Manuelles Hacking, d.h. Manipulation von Hard- und Software ohne Nutzung spezieller Schadsoftware; Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten; Defacing-Attacken, die das Ziel hatten, unbefugt Webinhalte des Unternehmens zu verändern; CEO-Fraud, wobei eine Führungspersönlichkeit des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitern zu bewirken; Phishing, wobei Mitarbeiter mit echt aussehenden E-Mails oder Webseiten getäuscht wurden, um z.B. sensible Unternehmensdaten zu erlangen [Mehrfachantworten möglich]), Antwortmöglichkeiten: (Anzahl [nummerisch]; Weiß nicht; Keine Angabe)

B02 Wurde Ihrem Unternehmen in den letzten 12 Monaten einer der beschriebenen Cyberangriffe angedroht?
(Ja; Nein; Weiß nicht; Keine Angabe)

B03 Für wie wahrscheinlich halten Sie es, dass ein Cyberangriff auf Ihr Unternehmen in den letzten 12 Monaten erfolgt ist, aber nicht bemerkt wurde?
(Sehr unwahrscheinlich; Eher unwahrscheinlich; Eher wahrscheinlich; Sehr wahrscheinlich; Weiß nicht; Keine Angabe)

B04 Von welchem Cyberangriff war Ihr Unternehmen jemals betroffen?
(Ransomware-Angriff; Spyware-Angriff; Sonstiger Angriff mit Schadsoftware; Manuelles Hacking; (D)DoS-Attacke; Defacing-Attacke; CEO-Fraud; Phishing; Sonstiger Angriff [Mehrfachantworten möglich]), Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; Keine Angabe)

B05 Welcher Cyberangriff der letzten 12 Monate war der schwerwiegendste?
(Ransomware-Angriff; Spyware-Angriff; Sonstiger Angriff mit Schadsoftware; Manuelles Hacking; (D)DoS-Attacke; Defacing-Attacke; CEO-Fraud; Phishing; Sonstiger Angriff [Mehrfachnennung möglich; nur wenn B01 mindestens einmal Anzahl>0]), Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; Keine Angabe)

B06 Wurde dieser schwerwiegendste Angriff im Vorhinein angedroht?
(Ja; Nein; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B07 Gibt es Vermutungen aus welchem Kreis der oder die Täter stammen?
(Ehemalige oder aktive Mitarbeiter; Geschäftspartner (z.B. Dienstleister, Lieferanten); Mitbewerber; Andere Außenstehende; Nein (keine Vermutung); Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B07a Aus welcher hierarchischen Ebene stammten der oder die Täter?
(Geschäftsführung oder dem Top Management; Mittleren Management; Belegschaft; Weiß nicht; Keine Angabe [Mehrfachantworten möglich; nur wenn B07 = „Mitarbeiter“ oder „Geschäftspartner“; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B08 Gab es bei diesem Angriff eine Lösegeld-Forderung? Wie hoch war diese?
(Ja [mit nummerischer Angabe in EUR]; Nein; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B08a Ist Ihr Unternehmen der Lösegeldforderung nachgekommen?
(Ja; Nein; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B08b Sind die Angreifer ihren Versprechungen (Daten-Entschlüsselung oder Stoppen des Angriffs) nachgekommen?
(Ja; Nein; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B09 Sie wurden Opfer eines Malware-Angriffes. Über welchen Weg ist der Angriff erfolgt? Über …
(E-Mail; Internetseite (z.B. aktive Inhalte, Downloads); Speichermedien (z.B. USN, SD-Cars, CD); mobile Endgeräte (z.B. Net-/Notebooks, Tablets, Smartphones etc.); Sonstigen Weg [Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]) Antwortmöglichkeiten: (Ja; Vermutlich; Nein; Weiß nicht; Keine Angabe)

B10 Waren folgende IT-Systeme vom schwersten Angriff betroffen?
(Webauftritt (z.B. online-Marktplätze, Shops, Kundenportale); E-Mail und Kommunikation (z.B. Partner-Portale, Netzspeicher); Auftrags- und Kundenverwaltung (z.B. Termin- und Reservierungssysteme, Rechnungsverwaltung); Produktionssteuerung (Maschinen- und Anlagensteuerung); Lagen und Logistik; Banking & Trading; Rechnungswesen und Controlling (z.B. für Jahresabschluss, Berichtserstellung); Erbringung von Dienstleistungen (z.B. Projektplanung, CAD, Berechnungen von Statik)

[Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; keine Angabe)

B10a Wenn ja, wie wichtig ist dieses IT-System für ihr Unternehmen?
(Webauftritt; E-Mail und Kommunikation; Auftrags- und Kundenverwaltung; Produktionssteuerung; Lagen und Logistik; Banking & Trading; Rechnungswesen und Controlling; Erbringung von Dienstleistungen [Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: ((eher) wichtig; (eher) unwichtig)

B10b Wie lange konnte es nicht oder nur stark eingeschränkt genutzt werden?
(Webauftritt; E-Mail und Kommunikation; Auftrags- und Kundenverwaltung; Produktionssteuerung; Lagen und Logistik; Banking & Trading; Rechnungswesen und Controlling; Erbringung von Dienstleistungen [Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: Ausfall in Stunden [nummerisch])

B11 Waren durch den Angriff folgende Daten betroffen?
(Nicht öffentliche Kundendaten (z.B. Zugangsdaten, Bankdaten, Adressen, Patientendaten, etc.); Nicht öffentliche Daten von Geschäftspartnern (z.B. Zugangsdaten, Bankdaten, Adressen, etc.); Produktdaten (z.B. Konstruktionspläne, Rezepturen, Quellcodes etc.); Strategie-, Vertriebs- und Finanzinformationen (z.B. Preislisten, Sanierungspläne, Akquisitionen, Finanz- und Rechnungswesendaten [Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; Keine Angabe)

B11a Wurden diese Daten gelöscht, manipuliert, gestohlen oder verschlüsselt?
(Nicht öffentliche Kundendaten (z.B. Zugangsdaten, Bankdaten, Adressen, Patientendaten, etc.); Nicht öffentliche Daten von Geschäftspartnern (z.B. Zugangsdaten, Bankdaten, Adressen, etc.); Produktdaten (z.B. Konstruktionspläne, Rezepturen, Quellcodes etc.); Strategie-, Vertriebs- und Finanzinformationen (z.B. Preislisten, Sanierungspläne, Akquisitionen, Finanz- und Rechnungswesendaten [Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Gelöscht; Manipuliert; Gestohlen; Verschlüsselt; nichts davon; weiß nicht; Keine Angabe)

B12 Sind dem Unternehmen durch den Angriff direkte Kosten entstanden?
(Externe Beratung (z.B. Rechtsberatung, Notfallmanagement); Sofortmaßnahmen zur Abwehr und Aufklärung; Schadensersatz/ Strafen; Abgeflossene Gelder; Betriebsunterbrechung; Wiederherstellung/ Wiederbeschaffung [Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate], Antwortmöglichkeiten: (Ja [mit nummerischer Angabe in EUR]; Nein; Keine Angabe)

B13 Wer hat von diesem Vorfall erfahren?
*(Kunden; Geschäftspartner; Versicherer; Eigentümer*innen des Unternehmens; Öffentlichkeit [Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate], Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; Keine Angabe)*

B14 An welche staatlichen Stellen/ Behörden haben Sie sich wegen dieses Vorfalls gewandt?
*(Nächste Polizeidienststelle; Auf Cybercrime spezialisierte Polizeidienststelle; Verfassungsschutz; Bundesamt für Sicherheit in der Informationstechnik (BSI); Landesdatenschutzbeauftragte*r; Sonstige; An keine staatliche Stelle [Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate], Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; Keine Angabe)*

B15 Haben Sie Strafanzeige erstattet?
(Ja; Nein; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B16 Wie bewerten Sie die Arbeit der Polizei bzw. der Strafverfolgungsbehörden in Ihrem Fall?
(Durch die Ermittlungen wurde unser Betriebsablauf gestört; Ich bin insgesamt zufrieden mit der Arbeit der Polizei; Ich würde es anderen Unternehmen empfehlen, Cyberangriffe anzuzeigen [Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate und bei Anzeige], Antwortmöglichkeiten: (Stimme voll und ganz zu; Stimme eher zu; Stimme eher nicht zu; Stimme gar nicht zu; Weiß nicht; Keine Angabe)

B17 Konnten die Täter in Ihrem Fall ermittelt werden?
(Ja; Nein; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate und bei Anzeige])

B18 Warum haben Sie keine Strafanzeige erstattet?
(Weil ein Imageschaden zu befürchten war; Weil Arbeitsbehinderungen zu befürchten waren; Weil Behörden Einsicht in vertrauliche Daten fordern könnten; fehlende Aussicht auf Ermittlungserfolg; Wusste nicht, an wen man sich dafür wenden muss; Sonstiges [Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate und bei Nichtanzeige]) Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; Keine Angabe)

C IT-Sicherheitsstrukturen

C01 Welche der folgenden Maßnahmen gibt es derzeit in Ihrem Unternehmen? Geben Sie bitte zusätzlich an, ob diese schon vor oder erst nach dem schwerwiegendsten Cyberangriff vorhanden war.
(Schriftlich fixierte Konzepte zur Informations- bzw. IT-Sicherheit; Schriftlich fixierte Konzepte zum Notfallmanagement; Regelmäßige Risiko- und Schwachstellenanalysen; Die Einhaltung der Richtlinien wird regelmäßig überprüft und Verstöße ggf. geahndet; Zertifizierung der IT-Sicherheit (z.B. nach ISO 27001 oder VdS 3473); Schulungen zur IT-Sicherheit für Mitarbeiter; Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme; Mindestanforderungen für Passwörter; individuelle Vergabe von Zugangs- und Nutzerrechten je nach Aufgabe; regelmäßige Backups [täglich; wöchentlich; seltener]; physisch getrennte Aufbewahrung der Backups; Aktuelle Antivirensoftware; Regelmäßige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches; Schutz der IT-Systeme mit einer Firewall [Mehrfachantworten möglich]), Antwortmöglichkeiten: (Ja; Nein; Erst nach dem Angriff; weiß nicht; Keine Angabe)

C02 Welchen Firewall-Typ setzen Sie ein?
(Einfache Firewall, d.h. Paketfilterung nach Quell- und Zieladresse durch Software-Firewall oder Router auf Netzwerkebene; Erweiterte Firewall, d.h. zusätzliche Überwachung und Filterung nach Paketinhalt (Deep Packet Inspection DPI) auf Anwendungsebene und Protokollierung des Datenverkehrs; Weiß nicht; Keine Angabe [nur wenn Schutz der IT-Systeme mit einer Firewall = Ja])

C03 Haben Sie eine Versicherung gegen Informationssicherheitsverletzungen (Cyberversicherung)
(Ja; Nein; Weiß nicht; keine Angabe [Split-Half-Verfahren: nur Gruppe B])

C04 Würden Sie die Cyberversicherung weiterempfehlen?
(Ja; Nein; Weiß nicht; keine Angabe [Split-Half-Verfahren: nur Gruppe B; nur wenn Cyberversicherung vorhanden])

C04a Haben Sie jemals versucht, Leistungen der Cyberversicherung in Anspruch zu nehmen?
(Ja; Nein; Weiß nicht; keine Angabe [Split-Half-Verfahren: nur Gruppe B; nur wenn Cyberversicherung vorhanden])

C04b Haben Sie diese Leistungen auch erhalten?
(Ja; Nein; Weiß nicht; keine Angabe [Split-Half-Verfahren: nur Gruppe B; nur wenn Cyberversicherung vorhanden und Leistungen in Anspruch genommen])

C04c Wurde damit der gesamte Schaden abgedeckt?
(Ja; Nein; Weiß nicht; keine Angabe [Split-Half-Verfahren: nur Gruppe B; nur wenn Cyberversicherung vorhanden und Leistungen in Anspruch genommen und erhalten])

C05 Warum hat Ihr Unternehmen keine Cyberversicherung?
(Wir haben uns damit noch nicht beschäftigt; Das Preis-Leistungs-Verhältnis stimmt nicht; Sonstiger Grund; weiß nicht; Keine Angabe [Split-Half-Verfahren: nur Gruppe B; Mehrfachantworten möglich; nur wenn keine Cyberversicherung vorhanden])

C06 Was ist Ihr Eindruck zum Risikobewusstsein?
(Die Geschäftsführung ist sich der IT-Risiken bewusst und hält die Vorgaben ein; Die Belegschaft ist sich der IT-Risiken bewusst und hält die Vorgaben ein; Im Unternehmen wird sehr viel für die IT-Sicherheit getan (mehr als klassische Schutzmaßnahmen [Mehrfachantworten möglich]), Antwortmöglichkeiten: (Trifft gar nicht zu; Trifft eher nicht zu; Trifft eher zu; Trifft voll und ganz zu; Weiß nicht; Keine Angabe)

C07 Wie groß war das Budget in den letzten 12 Monaten für…
(… die IT insgesamt (inkl. Personal, Beratung, Hard- und Software); … die IT-Sicherheit und Informationssicherheit, inkl. Personal, Beratung, Hard- und Software), Antwortmöglichkeiten: (nummerische Angabe in EUR oder klassiert: ≤ 50.000; < 100.00; < 500.000; < 1 Mio.; < 5 Mio.; < 10 Mio.; 10 Mio. und mehr; Trifft nicht zu, Weiß nicht; Keine Angabe])

C08 An wen wenden Sie sich, um Informationen zur IT-und Informationssicherheit einzuholen?
(Staatliche Institutionen (z.B. Verfassungsschutz, Polizei, BSI); IT-Sicherheitssoftwarehersteller; Beratungsdienstleister; Berufsverbände, Kammern (z.B. IHK, BVMW); Internetrecherche; Fachliteratur/Fachzeitschriften; Sonstige; Wenden uns an Niemanden [Mehrfachantworten möglich]), Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; Keine Angabe)

D Unternehmensmerkmale

D01 Wann wurde Ihr Unternehmen gegründet?
(Jahresangabe oder klassiert: ≤ 2 Jahre; < 10 Jahre; < 25 Jahre; < 100 Jahre; ab 100 Jahre; Weiß nicht; Keine Angabe)

D02 Schätzen Sie Ihr Unternehmen als eine kritische Infrastruktur im Sinne des IT-Sicherheitsgesetzes ein?
(Ja; Nein; Kenne das Gesetz nicht; Weiß nicht; Keine Angabe)

D03 Wie hoch war der Gesamtumsatz Ihres Unternehmens im letzten Geschäftsjahr?
(nummerische Angabe in EUR oder klassiert: ≤ 500.000 EUR; < 1 Mio. EUR; < 2 Mio. EUR; < 10 Mio. EUR; < 50 Mio. EUR; < 500 Mio. EUR; ab 500 Mio. EUR)

D04 Exportiert Ihr Unternehmen Produkte oder Dienstleistungen?
(Ja; Nein; Weiß nicht; Keine Angabe [nur das Unternehmen, nicht der Konzern])

D05 Wie viele Standorte mit eigener IT-Infrastruktur hat Ihr Unternehmen …
(…in Deutschland; im Ausland [nur das Unternehmen, nicht der Konzern]), Antwortmöglichkeiten: (nummerische Angabe; Weiß nicht; Keine Angabe)

D06 Wie viele Beschäftigten Ihres Unternehmens investieren den überwiegenden Teil ihrer Arbeitszeit in …
(… den Betrieb der IT insg.?; davon speziell in den Betrieb von IT- und Informationssicherheit?), Antwortmöglichkeiten: (nummerische Angabe; Weiß nicht; Keine Angabe)

D07 Hat Ihr Unternehmen IT-Funktionen ausgelagert?
(Email & Kommunikation; Netzwerk-Administration & Wartung; Webauftritt (z.B. online-Marktplätze, Shops, Kundenportale); Cloud-Software & Cloud-Speicher; IT-Security (z.B. Incident Detection, SIEM, Threat Intelligence); Sonstiges; Keine IT-Funktionen ausgelagert [Mehrfachantworten möglich]), Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; Keine Angabe)

D08 Sind detaillierte Zuständigkeiten, Kontakte und Stellenbeschreibungen der Mitarbeiter öffentlich im Internet zugänglich?
(Ja; Teilweise; Nein; Weiß nicht; Keine Angabe)

ABBILDUNGEN

TABELLEN

LITERATUR

Adams, A. & M.A. Sasse, 1999: Users are not the enemy. Why users compromise security mechanisms and how to take remedial measures. Communications of the ACM 42: 40–46.

Agrafiotis, I., J.R.C. Nurse, M. Goldsmith, S. Creese & D. Upton, 2018: A taxonomy of cyber-harms. Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity 4.

Bayerl, P.S. & T.-G. Rüdiger, 2018: Braucht eine digitale Gesellschaft eine digitale Polizei? Deutsche Polizei: 4–14.

Berg, A. & M. Niemeier, 2019: Wirtschaftsschutz in der digitalen Welt. Berlin.

Bitkom e.V., 2017: Wirtschaftsschutz in der digitalen Welt.

Bitkom e.V., 2018: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie. Studienbericht 2018.

Blanke, K., B. Gauckler & S. Sattelberger, 2011: Fragebogen auf dem Prüfstand. Testmethoden und deren Einsatz in der amtlichen Statistik. Wirtschaft und Statistik: 641–649.

Böhme, R. (Hrsg.), 2013: The Economics of Information Security and Privacy. Berlin, Heidelberg, s.l.: Springer Berlin Heidelberg.

Bollhöfer, E. & A. Jäger, 2018: Wirtschaftsspionage und Konkurrenzausspähung. Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. Reihe A: Arbeitsberichte 09/2018. Freiburg i. Br.

Brandl, S., M. Zimmermann, N. Grau, S. Wilms & N. Engler, 2016: SicherheitsMonitor 2016 Mittelstand. IT-Sicherheitslage in Deutschland.

Büchner, S., 2018a: Digitale Infrastrukturen. Spezifik, Relationalität und die Paradoxien von Wandel und Kontrolle. Arbeits- und Industriesoziologische Studien (AIS) 11: 279–293.

Büchner, S., 2018b: Zum Verhältnis von Digitalisierung und Organisation. Zeitschrift für Soziologie 47: 332–348.

Bundesamt für Sicherheit in der Informationstechnik: Cyber-Sicherheits-Umfrage 2017. Bonn.

Bundesamt für Sicherheit in der Informationstechnik, 2015: Die Lage der IT-Sicherheit in Deutschland. Bonn.

Bundesamt für Sicherheit in der Informationstechnik, 2016: Umfrage zur Betroffenheit durch Ransomware – 04/2016. Bonn.

Bundesamt für Sicherheit in der Informationstechnik, 2017: Die Lage der IT-Sicherheit in Deutschland 2017. Bonn.

Bundesamt für Sicherheit in der Informationstechnik, 2019a: Cyber-Sicherheits-Umfrage. Cyber-Risiken & Schutzmaßnahmen in Unternehmen. Betrachtungszeitraum 2018. Version 1.1 vom 18.04.2019. Bonn.

Bundesamt für Sicherheit in der Informationstechnik, 2019b: Cyber-Sicherheits-Umfrage. Cyber-Risiken & Schutzmaßnahmen in Unternehmen. Betrachtungszeitraum 2018. Version 1.0 vom 10.04.2019. Bonn.

Bundesamt für Sicherheit in der Informationstechnik, 2019c: Ransomware. Bedrohungslage, Prävention & Reaktion. Bonn.

Bundesdruckerei GmbH, 2017: Digitalisierung und IT-Sicherheit in deutschen Unternehmen. Eine repräsentative Untersuchung, erstellt von der Bundesdruckerei GmbH in Zusammenarbeit mit KANTAR EMNID. Berlin.

Bundeskriminalamt, 2018: Cybercrime. Bundeslagebild 2017. Wiesbaden.

Bundesministerium für Wirtschaft und Energie, 2012: IT-Sicherheitsniveau in kleinen und mittleren Unternehmen. Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie. Berlin.

Burr, W.E., D.F. Dodson, E.M. Newton, R.A. Perlner, W.T. Polk, S. Gupta & E.A. Nabbus, 2003: Electronic Authentication Guideline. NIST Special Publication 800-63-2.

Chen, L., S.S. Ho & M.O. Lwin, 2016: A meta-analysis of factors predicting cyberbullying perpetration and victimization. From the social cognitive and media effects approach. New Media & Society: 1–20.

Cisco, 2017: 2017 Annual Cybersecurity Report.

Cobb, S., 2015: Sizing Cybercrime. Incidents and Accidents, Hints and Allegations. Virus Bulletin Conference September 2015.

Computer Security Institute (CSI), 2011: 2010/2011 Computer Crime and Security Survey. New York, NY.

Connolly, L.Y. & D.S. Wall, 2019: The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers & Security 87.

Dreißigacker, A. & L. Riesner, 2018: Private Internetnutzung und Erfahrung mit computerbezogener Kriminalität. Ergebnisse der Dunkelfeldstudien des Landeskriminalamtes Schleswig-Holstein 2015 und 2017. KFN-Forschungsbericht 139. Hannover.

eco - Verband der Internetwirtschaft e.V., 2017: eco Studie IT-Sicherheit 2017.

Fansher, A.K. & R. Randa, 2018: Risky Social Media Behaviors and the Potential for Victimization. A Descriptive Look at College Students Victimized by Someone Met Online. Violence and Gender.

Florencio, D. & C. Herley, 2012: Sex, Lies and Cyber-crime Surveys. Redmond, WA, USA.

Gehem, M., A. Usanov, E. Frinking & M. Rademaker, 2015: Assessing Cyber Security. A Meta-Analyses of threats, trends and responses to cyber attacks. The Hague.

Georgia Institute of Technology, 2016: Emerging Cyber Threats Report 2016. Atlanta, GA, USA.

Gesamtverband der Deutschen Versicherungswirtschaft e.V., 2018: Cyberrisiken im Mittelstand. Ergebnisse einer Forsa-Befragung Frühjahr 2018. Berlin.

Grassi, P.A., J.L. Fenton, E.M. Newton, R.A. Perlner, A.R. Regenscheid, W.E. Burr, J.P. Richer, N.B. Lefkovitz, J.M. Danker, Y.-Y. Choong, K.K. Greene & M.F. Theofanos, 2017: Digital Identity Guidelines. Authentication and Lifecycle Management. NIST Special Publication 800-63B.

Hartmann, J., 2017: Stichprobenziehung und Feldzugang in Organisationsstudien. S. 185–211 in: S. Liebig, W. Matiaske & S. Rosenbohm (Hrsg.), Handbuch Empirische Organisationsforschung. Wiesbaden: Springer Gabler.

Henson, B., B.W. Reyns & B.S. Fisher, 2016: Cybercrime Victimization. S. 553–570 in: C.A. Cuevas & C.M. Rennison (Hrsg.), The Wiley Handbook on the Psychology of Violence. Chichester, UK: John Wiley & Sons, Ltd.

Hillebrand, A., A. Niederprüm, S. Schäfer, S. Thiele & I. Henseler-Ungar, 2017: Aktuelle Lage der IT-Sicherheit in KMU. Bad Honnef.

Hiscox, 2017: The Hiscox Cyber Readiness Report 2017. London, UK.

Hiscox, 2018: Hiscox Cyber Readiness Report 2018. Hamilton, Bermuda.

Huber, E. & B. Pospisil, 2018: Täter und Opfer von Cybercrime. S. 23–45 in: E. Huber & B. Pospisil (Hrsg.), Die Cyber-Kriminellen in Wien. Eine Analyse von 2006-2016. Krems: Edition Donau-Universität Krems.

Huber, E., B. Pospisil & W. Seböck, 2018: Cybercrime-Delikt in Österreich - Ein Rückblick 2006 bis 2016. S. 265–275 in: K. Boers & M. Schaerff (Hrsg.), Kriminologische Welt in Bewegung. Mönchengladbach: Forum Verlag.

IBM Cooperation, 2018: IBM X-Force Threat Intelligence Index 2018. Armonk, NY, USA.

Industrie- und Handelskammer Nord e.V., 2013: Unternehmensbefragung zur Betroffenheit der norddeutschen Wirtschaft von Cybercrime. Hamburg.

Kantar Emnid, 2019: Cyberangriffe gegen Unternehmen. Methodenreport. Nicht veröffentlicht. Bielefeld.

Kersten, H., G. Klett, J. Reuter & K.-W. Schröder, 2016: IT-Sicherheitsmanagement nach der neuen ISO 27001. ISMS, Risiken, Kennziffern, Controls. Wiesbaden: Springer Vieweg.

Kigerl, A., 2012: Routine Activity Theory and the Determinants of High Cybercrime Countries. Social Science Computer Review 30: 470–486.

Klahr, R., N.J. Shah, P. Sheriffs, T. Rossington, G. Pestell, M. Button & V. Wang, 2017: Cyber Security Breaches Survey 2017. Main Report. London, UK.

McGuire, M. & S. Dowling, 2013: Cyber crime: A review of the evidence:. Chapter 2: Cyber-enabled crimes - fraud and theft. Research Report 75.

Meier, B.-D., 2012: Sicherheit im Internet. Neue Herausforderungen für Kriminologie und Kriminalpolitik. MschrKrim 95: 184.

Meško, G., 2018: On Some Aspects of Cybercrime and Cybervictimization. European Journal of Crime, Criminal Law and Criminal Justice 26: 189–199.

Min, B., V. Varadharajan, U. Tupakula & M. Hitchens, 2014: Antivirus security: naked during updates. Software: Practice and Experience 44: 1201–1222.

Näsi, M., P. Räsänen, M. Kaakinen, T. Keipi & A. Oksanen, 2017: Do routine activities help predict young adults' online harassment: A multi-nation study. Criminology & Criminal Justice 17: 418–432.

Ngo, F. & K. Jaishankar, 2017: Commemorating A Decade In Existence Of The International Journal Of Cyber Criminology. A Research Agenda To Advance The Scholarship On Cyber Crime. International Journal of Cyber Criminology 11.

Nurse, J.R.C., S. Creese, M. Goldsmith & K. Lamberts, 2011: Guidelines for usable cybersecurity: Past and present. Mailand.

Organisation for Economic Co-operation and Development (OECD), 2015: Digital Security Risk Management for Economic and Social Prosperity. Paris: OECD Publishing.

Osborne, S., R. Currenti, M. Calem & H. Husband, 2018: Crime against businesses: findings from the 2017 Commercial Victimisation Survey. Statistical Bulletin 07/18.

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

Pascual, A. & K. Marchini, 2015: 2016 Data Breach Fraud Impact Report. https://www.javelinstrategy.com/press-release/16-billion-stolen-127-million-identity-fraud-victims-2014-according-javelin-strategy (9.9.2016).

Pfeiffer, S., 2015: Warum reden wir eigentlich über Industrie 4.0? Auf dem Weg zum digitalen Despotismus. Mittelweg 36: 14–36.

Ponemon Institute, 2016: The Cyber Resilient Organization in Germany: Learning to Thrive against Threats. Michigan, USA.

Ponemon Institute, 2017a: 2017 Cost of Data Breach Study. Global Overview. Michigan, USA.

Ponemon Institute, 2017b: Cost of Cyber Crime Study. Insights on the Security Investments that make a Difference. Michigan, USA.

Prätor, S., 2014: Ziele und Methoden der Dunkelfeldforschung. Ein Überblick mit Schwerpunkt auf Dunkelfeldbefragungen im Bereich der Jugenddelinquenz. S. 31–65 in: S. Eifler & D. Pollich (Hrsg.), Empirische Forschung über Kriminalität. Methodologische und methodische Grundlagen. Wiesbaden: VS Verl. für Sozialwiss.

PricewaterhouseCoopers AG WPG, 2017: Im Visier der Cyber-Gangster - So gefährdet ist die Informationssicherheit im deutschen Mittelstand.

PricewaterhouseCoopers Network, 2018: Revitalizing privacy and trust in a data-driven world. Key findings from The Global State of Information Security Survey 2018.

Prüfer, P. & M. Rexroth: Kognitive Interviews. ZUMA How-to 15. Mannheim.

PwC Strategy& GmbH, 2016: Cybersicherheitsstrategie. Ergebnisse der Online-Erhebung.

Rantala, R., 2008: Cybercrime against Businesses, 2005. Bureau of Justice Statistics, Special Report. Washington DC, USA.

Romanosky, S., 2016: Examining the costs and causes of cyber incidents. Journal of Cybersecurity 2: 121-135.

Ryan, J.J. & T.I. Jefferson, 2003: The Use, Misuse, and Abuse of Statistics in Information Security Research. Proceedings of the 23rd ASEM National Conference.

Sasse, M.A., S. Brostoff & D. Weirich, 2001: Transforming the ‘weakest link’ — a human/computer interaction approach to usable and effective security. BT Technology Journal 19: 122–131.

Schäfer, M., 2018: Daseinsvorsorge in: Gabler Wirtschaftslexikon. Wiesbaden: Springer Gabler.

Schnell, R. & M. Noack, 2015: Stichproben, Nonresponse und Gewichtung für Viktimisierungsstudien. S. 8–75 in: N. Guzy, C. Birkel & R. Mischkowitz (Hrsg.), Viktimisierungsbefragungen in Deutschland. Methodik und Methodologie. Wiesbaden: Bundeskriminalamt.

Smith, P., 2013: Sampling and Estimation for Business Surveys. S. 165–218 in: G. Snijkers, D. Willimack, G. Haraldsen & J. Jones (Hrsg.), Designing and Conducting Business Surveys. s.l.: Wiley.

Snijkers, G. & A. Meyermann, 2017: Betriebs- und Unternehmenssurveys. Der Surveyprozess und Surveyqualität. S. 241–272 in: S. Liebig, W. Matiaske & S. Rosenbohm (Hrsg.), Handbuch Empirische Organisationsforschung. Wiesbaden: Springer Fachmedien Wiesbaden.

Statistisches Bundesamt (Destatis), 2008: Klassifikation der Wirtschaftszweige (WZ 2008). Mit Erläuderungen. https://www.klassifikationsserver.de/klassService/jsp/variant/downloadpdf?variant=wz2008&language=DE (24.4.2019).

Statistisches Bundesamt (Destatis), 2018: Unternehmensregister-System. Qualitätsbericht 2017. Wiesbaden.

Statistisches Bundesamt (Destatis), 2019a: Unternehmen und Arbeitsstätten. Gewerbeanzeigen. Mai 2019. Fachserie 2 Reihe 5. Wiesbaden.

Statistisches Bundesamt (Destatis), 2019b: Unternehmen und Arbeitsstätten. Insolvenzverfahren. Mai 2019. Fachserie 2 Reihe 4.1. Wiesbaden.

Stiller, A., L. Boll, S. Kretschmer, G.R. Wollinger & A. Dreißigacker, 2020: Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer qualitativen Interviewstudie mit Experten. KFN-Forschungsbericht; in Vorbereitung. Hannover.

Sukwong, O., H. Kim & J. Hoe, 2011: Commercial Antivirus Software Effectiveness: An Empirical Study. Computer 44: 63–70.

techconsult, 2017: IT- und Informationssicherheit: Technische Maßnahmen und Lösungen in Mittelstand und öffentlichen Verwaltungen. Studienbericht zur Security Bilanz Deutschland 2017. Kassel, Haar.

Tsitsika, A., M. Janikian, S. Wójcik, K. Makaruk, E. Tzavela, C. Tzavara, D. Greydanus, J. Merrick & C. Richardson, 2015: Cyberbullying victimization prevalence and associations with internalizing and externalizing problems among adolescents in six European countries. Computers in Human Behavior 51: 1–7.

van de Weijer, S.G.A., R. Leukfeldt & W. Bernasco, 2019: Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. European Journal of Criminology 16: 486–508.

Vanson Bourne, 2014: Protecting the organization against the unknown. A new generation of threats.

Verband der TÜV e.V., 2019: Cybersecurity Studie. Berlin.

Verizon, 2018: 2018 Data Breach Investigations Report 11.

Wegge, D., H. Vandebosch, S. Eggermont, R. van Rossem & M. Walrave, 2016: Divergent Perspectives. Exploring a Multiple Informant Approach to Cyberbullying Victimization and Perpetration. European Journal on Criminal Policy and Research 22: 235–251.

Willis, G.B., 2005: Cognitive interviewing. A tool for improving questionnaire design. Thousand Oaks: SAGE.

AUTOR*INNEN

Arne Dreißigacker studierte an der Fachhochschule für Verwaltung- und Rechtspflege Berlin und war zwischen 2001 und 2004 im gehobenen Dienst der Berliner Polizei tätig. Anschließend studierte er Soziologie an der Martin-Luther-Universität Halle (Saale), erhielt 2013 ein Promotionsstipendium am Kriminologischen Forschungsinstitut Niedersachsen e.V. (KFN) und ist dort seit 2015 wissenschaftlicher Mitarbeiter. Zu seinen Forschungsschwerpunkten gehören das Kriminalitätsdunkelfeld, Wohnungseinbruchdiebstahl, Vorurteilskriminalität und Cyberkriminalität. Seit Oktober 2018 leitet er das Forschungsprojekt Cyberangriffe gegen Unternehmen am KFN.

Bennet von Skarczinski studierte Betriebswirtschaftslehre an der Hochschule Hannover und arbeitet seit 2015 bei PricewaterhouseCoopers (PwC) im Bereich Cyber Security & Privacy. Seit Dezember 2017 ist er zudem assoziierter Mitarbeiter am Kriminologischen Forschungsinstitut Niedersachsen e.V. (KFN) im Projekt Cyberangriffe gegen Unternehmen und promoviert als externer Doktorand am Lehrstuhl für Unternehmensrechnung und Wirtschaftsinformatik der Universität Osnabrück. Zu seinen Schwerpunkten gehören das Management von Informationssicherheit in Unternehmen und Cyber-Economics.

Prof. Dr. Gina Rosa Wollinger studierte Soziologie in Leipzig und promovierte 2018 an der dortigen Fakultät für Sozialwissenschaften und Philosophie. Zwischen 2012 und 2018 arbeitete sie am Kriminologischen Forschungsinstitut Niedersachsen e.V. (KFN) und leitete seit Dezember 2017 das von ihr initiierte Forschungsprojekt Cyberagriffe gegen Unternehmen bevor sie im Oktober 2018 eine Professur für Soziologie und Kriminologie an der Hochschule für Polizei und öffentliche Verwaltung NRW antrat. Zu Ihren Forschungsschwerpunkten zählen Wohnungseinbruchdiebstahl, Cyberkriminalität und die Viktimologie.

ISBN: 978-3-948647-00-1