KRIMINOLOGISCHES FORSCHUNGSINSTITUT NIEDERSACHSEN E.V.

Forschungsbericht Nr. 162

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

IT-Sicherheit IN DER WIRTSCHAFT

aufgrund eines Beschlusses des Deutschen Bundestages

Cyberangriffe gegen Unternehmen in Deutschland

Ergebnisse einer Folgebefragung 2020

Zusatzförderung durch: pwc VHV STIFTUNG

Arne Dreißigacker, Bennet von Skarczinski, Gina Rosa Wollinger

2021

FORSCHUNGSBERICHT Nr. 162

Cyberangriffe gegen Unternehmen in Deutschland

Ergebnisse einer Folgebefragung 2020

Arne Dreißigacker, Bennet von Skarczinski, Gina Rosa Wollinger

2021

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 (verlängert bis Mrz. 2021)

Initiative „IT-Sicherheit in der Wirtschaft“

Das Projekt „Cyberangriffe gegen Unternehmen“ ist Teil der Initiative „IT-Sicherheit in der Wirtschaft“ im Förderschwerpunkt Mittelstand-Digital.

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand 4.0-Kompetenzzentren, der Initiative „IT-Sicherheit in der Wirtschaft“ und Digital Jetzt umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.mittelstand-digital.de und www.it-sicherheit-in-der-wirtschaft.de.

ISBN: 978-3-948647-11-7

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

ABKÜRZUNGEN

2FA	Zwei-Faktor-Authentifizierung
ADM	Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.
AG	Aktiengesellschaft
BCM	Business Continuity Management
Besch.	Beschäftigte
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BMWi	Bundesministerium für Wirtschaft und Energie
BYOD	Bring your own device
BSI	Bundesamt für Sicherheit in der Informationstechnik
CATI	Computer Assisted Telephone Interview
DDos	Distributed Denial of Service
DoS	Denial of Service
Geschf.	Geschäftsführung
GmbH	Gesellschaft mit beschränkter Haftung
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
OHG	Offene Handelsgesellschaft
Pentest	Penetrationtest (Informatik)
PKS	Polizeiliche Kriminalstatistik
PwC	PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft
SIEM	Security Information and Event Management
SOC	Security Operation Center
URS	Unternehmensregistersystem
WZ	Wirtschaftszweig
ZAC	Zentrale Ansprechstelle Cybercrime für die Wirtschaft

INHALT

1 EINLEITUNG

Die Digitalisierung in der deutschen Wirtschaft nimmt weiter zu und hat zuletzt bedingt durch die Corona-Krise zusätzlich an Bedeutung gewonnen – so lautet das Ergebnis einer Bitkom-Studie[1] Ende des Jahres 2020. Fast alle der befragten Unternehmen (97 %) sehen die Digitalisierung mittlerweile eher als Chance denn als Risiko.[2] Dass es dennoch Risiken gibt, dürfte in Anbetracht der kürzlich erfolgten schwerwiegenden Ransomware-Angriffen auf das US-amerikanische Unternehmen Colonial Pipeline,[3] den französischen Versicherungskonzern Axa[4] und den irischen Gesundheitsdienst HSE[5] ebenfalls unbestritten sein. Unklarheit herrschte hingegen lange bei der Frage, wie groß die Risiken für Unternehmen unterschiedlicher Größen und Branchen in Deutschland sind. Die Hellfelddaten der Polizeilichen Kriminalstatistik (PKS) weisen zwar seit einigen Jahren auf einen Anstieg der Fallzahlen im Bereich Cyberkriminalität hin, aber die Fragen zum Ausmaß in Deutschland lassen sich mit ihnen aufgrund eines sehr großen Dunkelfeldes (bspw. aufgrund nicht angezeigter Fälle) nicht beantworten.[6]

Um differenziertes Wissen zu Art, Häufigkeit und Folgen von Cyberangriffen gegen Unternehmen sowie zu Risiko- und Schutzmaßnahmen zu erlangen, wurde vom Kriminologische Forschungsinstitut Niedersachsen e.V. (KFN) in Kooperation mit dem Forschungszentrum L3S der Leibniz Universität Hannover eine breit angelegte Untersuchung durchgeführt.[7]

Das Forschungsprojekt „Cyberangriffe gegen Unternehmen“ wurde im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie gefördert und erhält eine zusätzliche Förderung durch Wirtschaftsprüfungsgesellschaft und Unternehmensberatung PricewaterhouseCoopers sowie durch die VHV-Stiftung. Die Forschung wird durch einen beratenden Projektbeirat[8] unterstützt (Abbildung 1).[9] Das Projekt ist Modular aufgebaut und nutzt für die Beantwortung der jeweiligen Forschungsfragen unterschiedliche Erhebungsmethoden (Abbildung 2). Die Laufzeit des Projektes war auf drei Jahre von Dezember 2017 bis November 2020 angelegt, wurde aber im Zusammenhang Corona-Krise um 4 Monate bis März 2021 verlängert.

---

1 Bitkom e.V. (2020).

2 Ebd.

3 Quelle: https://www.heise.de/-6041854 (zuletzt geprüft am 17.05.2021).

4 Quelle: https://www.heise.de/-6046853 (zuletzt geprüft am 17.05.2021).

5 Quelle: https://www.faz.net/-ikh-abq1h (zuletzt geprüft am 17.05.2021).

6 Bayerl & Rüdiger (2018) Zur Problematik von Hellfelddaten im Bereich Cyberkriminalität allgemein siehe z.B. Huber & Pospisil (2020).

7 Siehe dazu detaillierter Dreißigacker et al. (2020a: 13ff.).

8 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.

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

Abbildung 1 **Projektbeteiligte**

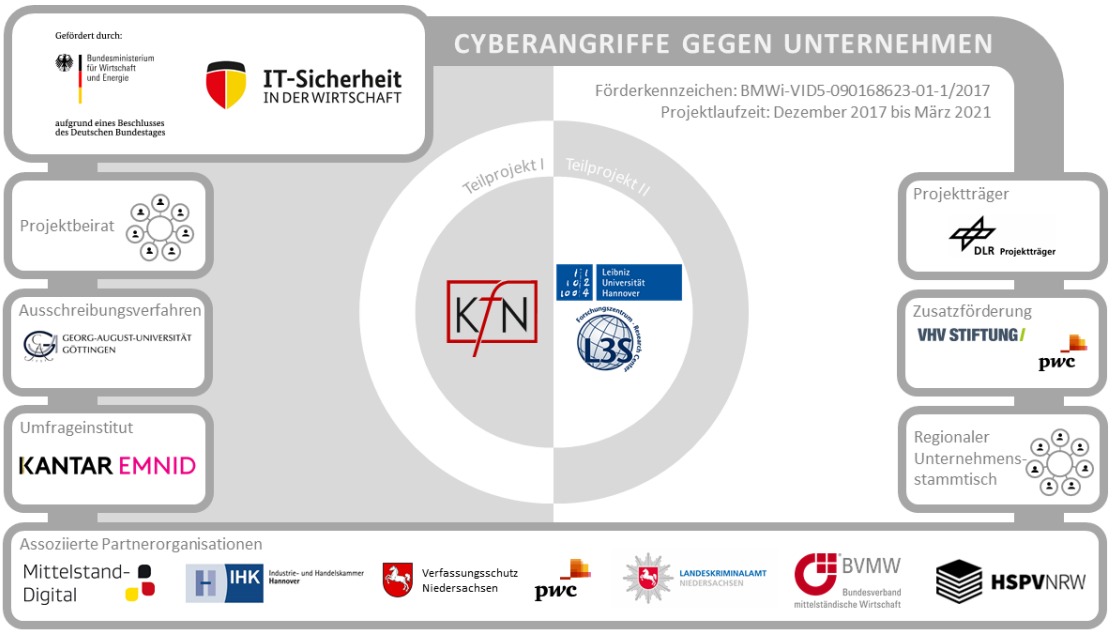
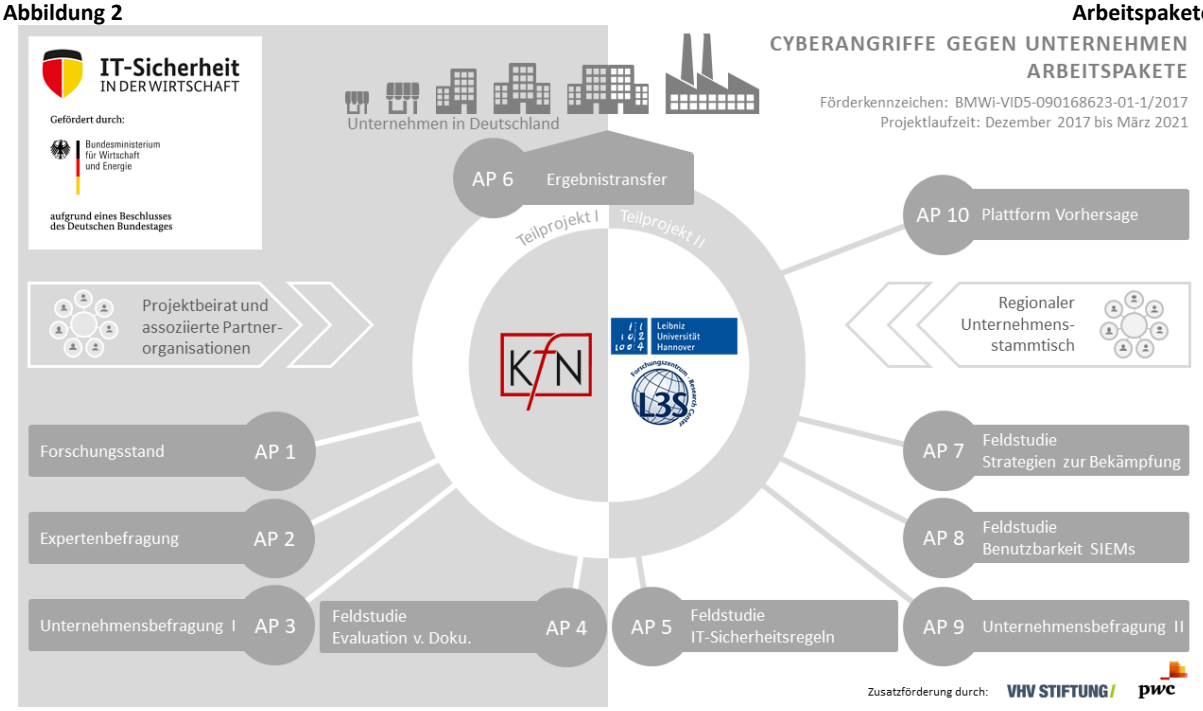


Abbildung 2 **Arbeitspakete**



Bisher liegen Ergebnisse zu den Interviews mit Experten der Strafverfolgungsbehörden, des Verfassungsschutzes, des Bundesamtes für Sicherheit in der Informationstechnik und der Versicherungswirtschaft,[10] sowie zu einer umfangreichen CATI-Befragung von 5.000 Unternehmen in Deutschland[11] (Befragung I) vor.

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

[11] Ergebnisse dieser repräsentativen Unternehmensbefragung finden sich bei Dreißigacker et al. (2020a).

Im Rahmen der Befragung I gaben über zwei Fünftel der Unternehmen (41,1 %) an, dass sie in den zwölf Monaten vor der Befragung auf mindestens einen Cyberangriff reagieren mussten, wobei ein Schwerpunkt bei Phishing und Angriffen mit Schadsoftware (Ransomware, Spyware und sonstiger Malware) zu erkennen war. Die Fragen, wie sich die Betroffenheit innerhalb eines Jahres verändert und welche Entwicklungen es hinsichtlich der IT-Sicherheit von Unternehmen gibt, steht im Fokus der zweiten Unternehmensbefragung (Befragung II). Diese fand in der zweiten Hälfte des Jahres 2020 statt und bildet die Grundlage für diesen Bericht.

Nach einer kurzen Beschreibung des Forschungsgegenstandes, der zentralen Forschungsfragen und der aktuellen Datenlage wird in Abschnitt 2 die Erhebungsmethode und die zugrundeliegende Stichprobe erläutert. Abschnitt 3 widmet sich der Verbreitung von IT-Sicherheitsmaßnahmen insbesondere im Kontext der Corona-Krise und Abschnitt 4 der Entwicklung der Risikoeinschätzung bevor in Abschnitt 5 die Betroffenheit von Cyberangriffen innerhalb eines Jahres vergleichend zu den Ergebnissen von Befragung I dargestellt wird. Anschließend werden in Abschnitt 6 die Ergebnisse der Detailfragen zum schwerwiegendsten Cyberangriff in den letzten zwölf Monaten berichtet. Ein Schwerpunkt dabei liegt auf den Folgen von Cyberangriffen und dem Anzeigeverhalten der Unternehmen. Nach der Darstellung von möglichen Zusammenhängen zwischen der Betroffenheit von Cyberangriffen und vorhandenen IT-Sicherheitsmaßnahmen in Abschnitt 7 werden die zentralen Ergebnisse der Befragung II in Abschnitt 8 zusammengefasst.

1.1 Forschungsgegenstand

1.1.1 Cyberangriffe

Unabhängig von ihrer strafrechtlichen Bewertung wird in dieser Studie 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 entsprechende 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.[12]

1.1.2 Unternehmen

Als zumindest potenziell Betroffene von diesen Cyberangriffen stehen Unternehmen ab 10 Beschäftigten mit Sitz in Deutschland im Mittelpunkt dieser Studie. Nach dem Statistischen Bundesamt werden Unternehmen „als kleinste rechtlich selbstständige Einheit definiert, die aus

[12] Eine Erläuterung der Cyberangriffsarten und deren Operationalisierung findet sich in Abschnitt 5. Nicht als Angriffsart, sondern als Folge bzw. Zweck eines Cyberangriffes wurden z.B. Identitätsdiebstahl oder Kreditkartenbetrug gewertet.

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."[13]

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 innerhalb des Projektes zweiten Unternehmensbefragung ist es erneut, differenzierte Informationen über die Verbreitung von Cyberangriffen, auf die Unternehmen reagieren mussten, zu erlangen und die Folgen (Systemausfälle, Kosten etc.) und Reaktionen (Anzeigeverhalten, Hinzuziehen von IT-Sicherheitsdienstlern etc.) zu erheben. Ferner soll analysiert werden, welche Merkmale das Risiko eines erfolgreichen Angriffs erhöhen und welche IT-Sicherheitsmaßnahmen bestehen. Bezüglich der Reaktion auf Angriffe ist von Interesse, wie viele Cyberangriffe im Vergleich zur Befragung I zur Anzeige gebracht wurden und welche Gründe dafür vorliegen, den Vorfall nicht anzuzeigen. Darüber hinaus soll die Erhebung von spezifischen Unternehmensmerkmalen helfen, sinnvolle Differenzierungen zwischen Unternehmen treffen zu können, die von bestimmten Angriffsarten (nicht) betroffen waren.

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

- Welche IT-Sicherheitsmaßnahmen werden getroffen?
    - Wie weit sind diese im Unternehmen verbreitet?
    - Welchen Reifegrad haben die Maßnahmen?
    - Wurden sie im Zusammenhang mit der veränderten Situation in der Corona-Krise angepasst?
- Auf welche Cyberangriffsarten musste in den letzten zwölf Monaten reagiert werden?
    - Welche Unterschiede zu Art und Häufigkeit von Cyberangriffen zeigen sich, wenn man nach Beschäftigtengrößenklasse und Branchenzugehörigkeit der Unternehmen differenziert?
    - Wie wurden die Angriffe entdeckt?
    - Wie hoch waren eventuelle Lösegelderpressungen?
    - Wie hoch ist der Schaden, der aus wahrgenommenen Cyberangriffen entstanden ist?
    - Welche Entwicklungen zeigen sich im Vergleich zur Befragung I
- Wie ist das Anzeigeverhalten von betroffenen Unternehmen?
    - Gibt es Unterschiede hinsichtlich der Cyberangriffsart?
    - Was sind die Gründe einer Nichtanzeige?
    - Welche Entwicklungen zeigen sich im Vergleich zur Befragung I

[13] Statistisches Bundesamt (2018: 5); siehe dazu auch Hartmann (2017: 188f.).

- Gibt es einen Zusammenhang zwischen der Betroffenheit von Cyberangriffen und 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?

1.3 Datenlage

Die Datenlage bezogen auf Unternehmen als Betroffene von Cyberangriffen ist nach wie vor als unzureichend und fragmentiert zu beschreiben. Neben den diversen kommerziellen Studien aus der IT-, Beratungs- und Versicherungswirtschaft, die aufgrund inhaltlicher Interessenskonflikte und z.T. methodischer Einschränkungen nicht immer als unproblematisch anzusehen sind, herrscht weiterhin ein Mangel an unabhängigen wissenschaftlichen Studien.[14] Diese Lücke sollte für Unternehmen in Deutschland mit den Befragungen I und II innerhalb des Forschungsprojektes „Cyberangriffe gegen Unternehmen“ zumindest ansatzweise geschlossen werden. So liegen nun erste Befunde zur Verbreitung verschiedener Cyberangriffsarten und deren Folgen[15] sowie zu den Einflussfaktoren für die Betroffenheit[16] vor. Ebenfalls mit Bezug zum Forschungsprojekt, wurden organisatorische und technologische Einflussfaktoren zum Abschluss von Cyberversicherungen untersucht.[17]

Für aktuelle empirische Forschungsergebnisse außerhalb des Forschungsprojektes „Cyberangriffe gegen Unternehmen“ sei auf die Studie „Cyber Security Breaches Survey“ des Britischen Ministeriums für Digitales, Kultur, Medien und Sport verwiesen,[18] die sich mittels Repräsentativbefragung den Einschätzungen und Maßnahmen von Unternehmen gegen Cyber-Bedrohungen sowie den Kosten und Auswirkungen von Vorfällen widmet. Die Studie von Buil-Gil et al. (2021) analysiert den Einfluss von Online-Verhalten und dem Vorhandensein von Sicherheitsmaßen auf die Viktimisierung von Unternehmen.[19]

[14] Vgl. Lamprecht & Vladova (2020: 348). Eine ausführliche Darstellung des Forschungsstandes zum Thema Cyberangriffe gegen Unternehmen findet sich bei Dreißigacker et al. (2020a: 21ff.) sowie bezogen auf Cybercrime im engeren Sinne allgemein bei Maimon & Louderback (2019).

[15] Dreißigacker et al. (2020c, 2020a, 2020b).

[16] Huaman et al. (2021).

[17] Skarczinski et al. (2021).

[18] Department for Digital, Culture, Media & Sport (2021).

[19] Eine detailliertere tabellarische Literaturübersicht (Stand März 2020) findet sich bei Dreißigacker et al. (2020a: 183ff.).

2 ERHEBUNG

2.1 Methode

Anders als bei der Befragung I, die zwischen August 2019 und Januar 2020 mittels *Computer Assisted Telephone Interviews* (CATI)[20] durchgeführt wurde, erfolgte die Befragung II webbasiert mit der Umfrageplattform *Qualtrics*[21] zwischen Juli und September 2020 (Abbildung 3). Die Teilnahmebereitschaft für die Befragung II wurde mit einer dafür benötigten E-Mail-Kontaktadresse bei der telefonischen Befragung I erhoben. Der Kontakt erfolgte anschließend über diese E-Mail-Adresse. Nach dem Anschreiben und der Einladung zur Teilnahme an der webbasierten Befragung (Web Survey),[22] wurden vier Erinnerung-E-Mails (zeitlicher Rhythmus siehe Abbildung 4) versendet. Alle E-Mails enthielten einen individuellen Link, der zum Onlinefragebogen führte (Survey-Link). Diese Individualisierung war für die Verbindung der Datensätze aus beiden Befragungen notwendig und ermöglichte es den Teilnehmer*innen, die Befragung zeitlich zu unterbrechen und zu einem späteren Zeitpunkt fortzusetzen.

Abbildung 3 **Zeitliche Einordnung der Befragungen**

Bei dem zum Einsatz kommenden webbasierten Fragebogen handelt es sich um eine modifizierte Form des Fragebogens der Befragung I (CATI),[23] die in die Umfrageplattform Qualtrics übertragen wurde. Die Struktur sowie der Wortlaut der Fragen und Antwortkategorien blieben dabei weitgehend unverändert, um die Vergleichbarkeit der Ergebnisse zur Befragung I zu ermöglichen. Zu den wesentlichen Veränderungen zählt die Überarbeitung der Items zu technischen IT-Sicherheitsmaßnahmen, da es bei diesen in der Befragung I kaum Variation bei den Antworten gab. So gaben in der ersten Befragung z.B. über 95 % der Unternehmensvertreter*innen an, dass technische IT-Sicherheitsmaßnahmen wie regelmäßige Backups, aktuelle Antivirensoftware und Firewall-Schutz im Unternehmen vorhanden sind.[24] Aus diesem Grund wurden zum einen weitere technische IT-Sicherheitsmaßnahmen als Antwortkategorien aufgenommen. Dazu gehören z.B. Zwei-Faktor Authentifizierung, Datenwiederherstellungstests, Security Information and Event Management (SIEM) und Security Operation Center (SOC). Zum anderen wurden neben dem Vorhandensein der jeweiligen Maßnahmen zusätzlich auch Angaben zum Reifegrad und zur Verbreitung innerhalb des Unternehmens erfragt. Darüber hinaus wurden verschiedene Unternehmensmerkmale wie Rechtsform, Exporttätigkeit oder

---

20 Steeh & Charlotte (2008: 237).

21 https://www.qualtrics.com/de/ (02.11.2020).

22 Zur Abgrenzung von Internet- und Online Surveys siehe Callegaro et al. (2015: 12f.).

23 Eine Kurzdarstellung des Fragebogens der CATI-Befragung findet sich bei Dreißigacker et al. (2020a: 191ff.).

24 Dreißigacker et al. (2020a: 156).

Anzahl der Standorte, die sich seit der ersten Befragung nicht wesentlich verändert haben dürften, nicht noch einmal erhoben. Dadurch konnten zusätzliche Fragen mit aufgenommen werden, die sich hauptsächlich auf die veränderte Situation in der Corona-Krise beziehen.[25]

Alle Veränderungen des Fragebogens wurde mit Expert*innen im Projektbeirat sowie im Regionalen Unternehmensstammtisch diskutiert. Ein Pretest des modifizierten Fragebogens wurde zwischen 10.06.2020 und 19.06.2020 mit sieben Vertreter*innen unterschiedlicher Unternehmensgrößen und unter Realbedingung, d.h. über einen per E-Mail versendeten Link zur Testversion des Web Surveys, durchgeführt. Das Feedback erfolgte telefonisch (think-aloud) bzw. schriftlich über zusätzliche dafür eingerichtete Freitextfelder. In der anschließenden Überarbeitung des Fragebogens wurden insbesondere verschiedene Antwortskalen im Wortlaut vereinheitlicht sowie eine weitere zusätzlichen IT-Sicherheitsmaßnahme (Netzwerksegmentierung) als Antwortkategorie mit aufgenommen.[26]

Der finale Fragebogen enthält 54 Fragen insbesondere zu den erlebten Cyberangriffen der letzten 12 Monate auf die reagiert werden musste, Detailfragen zum schwerwiegendsten dieser Angriffe und dessen Folgen sowie Fragen zu den vorhandenen IT-Sicherheitsmaßnahmen und der veränderten Situation in der Corona-Krise. Eine Kurzdarstellung des Fragebogens findet sich im Anhang.

2.2 Stichprobenziehung und -realisierung

Die Grundgesamtheit, aus der eine Stichprobe gezogen werden sollte, bildeten 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 haben.[27]

Da die Unternehmen innerhalb der Grundgesamtheit in Hinblick auf die Beschäftigtengrößenklassen und die Wirtschaftszweigzugehörigkeit sehr schief verteilt sind,[28] fiel die Wahl auf eine disproportional geschichtete Stichprobe. D.h., die in der Grundgesamtheit vergleichsweise selten vorhandenen Teilgesamtheiten (z.B. große Unternehmen ab 500 Beschäftigten mit einem Anteil von rund 2 %) sind im Vergleich zu einer reinen Zufallsauswahl in einer geschichteten Stichprobe anteilig deutlich stärker vertreten (oversampling). Damit ist eine differenzierte Auswertung auch für diese Gruppen möglich. Für repräsentative Gesamtaussagen kann die disproportional geschichtete Stichprobe mit Hilfe eines entsprechenden Gewichtungsfaktors re-proportionalisiert werden.

---

[25] An dieser Stelle werden nur die wesentlichen Modifikationen des Fragebogens angeführt. Detaillierte Informationen zu den Änderungen werden ggf. zusammen mit den Ergebnissen der betroffenen Fragen berichtet.

[26] Der Prozess der Fragebogenerstellung orientierte sich an Callegaro et al. (2015: 112ff.).

[27] Kleinstunternehmen bis neun Beschäftigte wurden 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 Gewerbeabmeldungen 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.

[28] Siehe dazu Dreißigacker et al. (2020a: 49ff.).

2.2.1 Befragung I

Da für die CATI-Befragung telefonische Kontaktadressen benötigt wurden, war eine direkte Ziehung aus der Grundgesamtheit bzw. dem offiziellen Unternehmensregistersystem (URS) nicht möglich. Stattdessen wurde auf die Unternehmensdatenbanken von Bisnode und Heins & Partner zurückgegriffen, die telefonische Kontaktadressen sowie weitere benötigte Unternehmensmerkmale (z.B. Beschäftigtengröße und Wirtschaftszweig) und so gut wie alle Unternehmen ab 10 Beschäftigten mit Sitz in Deutschland enthalten sollen (Auswahlgesamtheit).[29] Für die Realisierung einer Nettostichprobe von 5.000 Unternehmen[30] für die erste Befragung wurden 42.219 Unternehmen aus den Unternehmensdatenbanken zwischen August 2018 und Januar 2019 vom Umfrageinstitut Kantar (ehemals Kantar EMNID) kontaktiert und gebeten, an der CATI-Befragung teilzunehmen. Dies entspricht einer Teilnahmequote von 11,6 %.

2.2.2 Befragung II

Die Nettostichprobe von 5.000 Unternehmen der Befragung I (CATI) bildet gleichzeitig die Bruttostichprobe für Befragung II (Web Survey). Der Wechsel der Erhebungsmethode von CATI zu Web Survey in der zweiten Welle hatte vor allem zeitliche und finanzielle Gründe. Ein Web Survey lässt sich in kürzerer Zeit und deutlich günstiger durchführen als eine erneute CATI-Befragung[31] und scheint insbesondere für eine Folgebefragung im Unternehmenskontext ein geeigneter Weg zu sein. Anders als bei Bevölkerungsbefragungen kann davon ausgegangen werden, dass alle Vertreter*innen der teilnehmenden Unternehmen über betriebliche E-Mail-Adressen erreichbar sind und Zugang zum Internet haben.

Der Verlust von teilnehmenden Unternehmen zwischen Befragung I und II (Panelmortalität) ist jedoch stärker ausgefallen als erwartet und ist größtenteils zu den möglicherweise systematischen Ausfällen zu zählen. Deshalb besteht zumindest theoretisch die Möglichkeit, dass die Ergebnisse verzerrt werden, weil der Ausfall nicht zufällig über alle Unternehmen hinweg erfolgte, sondern Unternehmen mit bestimmten Merkmalen seltener oder gar nicht an der zweiten Befragung teilnahmen. Nach Abzug der für die Auswertung als unproblematisch angesehenen neutralen Ausfälle[32] verblieb für die zweite Befragungswelle zunächst eine bereinigte Bruttostichprobe von 4.677 Unternehmen (Tabelle 1). Zu den größten möglicherweise systematischen Ausfällen zählt die Teilnahmeverweigerung im Vorfeld der zweiten Welle, d.h., von den 5.000 telefonisch befragten Unternehmensvertreter*innen waren 1.569 aus ungenannten Gründen nicht zu einer webbasierten Folgebefragung bereit und gaben dementsprechend erst gar keine E-Mail-Adresse an.[33] Daneben fiel von den zunächst teilnahmebereiten Unternehmen ein unerwartet großer Anteil aus: 1.756 Unternehmen konnte die Einladungs-E-Mail technisch gesehen

---

[29] „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“ (Dreißigacker et al. 2020: 58).

[30] Diese schlüsseln sich gemäß des Stratifizierungsplanes folgendermaßen auf: 1.000 Unternehmen mit 10-49 Beschäftigten, 1.000 Unternehmen mit 50-99 Beschäftigten, 1.000 Unternehmen mit 100-249 Beschäftigten, 500 Unternehmen ab 500 Beschäftigten und 500 Unternehmen der Daseinsvorsorge unabhängig von der Beschäftigtengrößenklasse (siehe Dreißigacker et al. 2020: 52).

[31] Zu den Vor- und Nachteilen eines Web Surveys siehe z.B. Callegaro et al. (2015: 18ff.)

[32] Dazu zählen insbesondere die Unzustellbarkeit aufgrund: ungültiger E-Mail-Adresse, Nichtexistenz oder Deaktivierung des Empfängerkontos, Speicherplatzbegrenzung des Empfängerkontos oder Zustell-Timeout.

[33] Die Teilnahmebereitschaft lag demnach zu diesem Zeitpunkt bei 68,6 %.

zwar zugestellt werden, eine Teilnahme an der Befragung blieb jedoch aus unbekannten Gründen aus, d.h., der Survey-Link wurde nicht angeklickt.[34] Bei 492 Unternehmen gilt die Einladungs-E-Mail als geöffnet, ohne dass dem Survey-Link gefolgt wurde und bei weitere 101 Unternehmen wurde dem Survey-Link gefolgt, eine Teilnahme blieb aber aus und weitere 158 Unternehmensvertreter*innen füllten den webbasierten Fragebogen nicht vollständig aus.

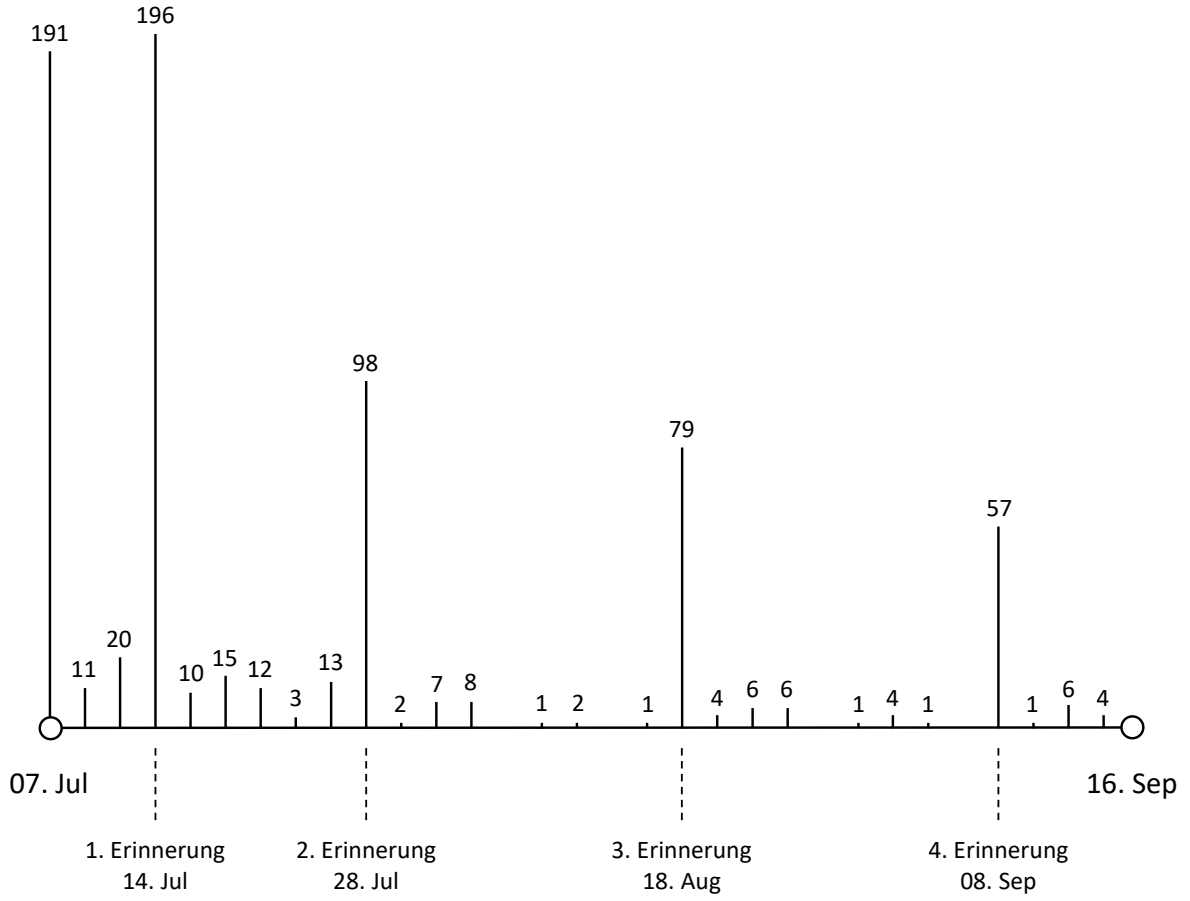
Tabelle 1 **Ausschöpfung**

			Befragung I	Befragung II	
		N	Prozentuierung auf Bruttostichprobe Befragung I	Prozentuierung auf Bruttostichprobe Befragung II	Prozentuierung auf bereinigter Bruttostichprobe Befragung II
Bruttostichprobe Befragung I		43.219	100,0		
Systematische Ausfälle insg.		38.219	88,4		
systematischer 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		
systematischer 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		
Auswertbare Interviews (Nettostichprobe Befragung I = Bruttostichprobe Befragung II)		5.000	11,6	100,0	
neutraler Ausfall vor Kontakt mit Zielperson	E-Mail-Adresse ungültig	19	0,0	0,4	
	E-Mail dauerhaft nicht zustellbar (hard bounce)	277	0,6	5,5	
	E-Mail vorübergehend nicht zustellbar (soft bounce)	27	0,1	0,5	
Bereinigte Bruttostichprobe Befragung II		4.677	10,8	93,5	100,0
systematischer Ausfall vor und nach Kontakt mit Zielperson	Befragung 2 vorher verweigert (keine E-Mail-Adresse angegeben)	1.569	3,6	31,4	33,5
	E-Mail zugestellt aber Survey-Link nicht geöffnet	1.756	4,1	35,1	37,5
	E-Mail geöffnet aber Survey-Link nicht geöffnet	492	1,1	9,8	10,5
	Survey gestartet aber keine Teilnahme	101	0,2	2,0	2,2
	Survey gestartet aber nicht vollständig abgeschlossen	158	0,4	3,2	3,4
	Survey vollständig abgeschlossen	601	1,4	12,0	12,9
Auswertbare Fragebogen* (Nettostichprobe Befragung II)		687	1,6	13,7	14,7

*) mind. zu 60 % ausgefüllt

[34] Neben der Möglichkeit, dass sich die Empfänger*innen mehr oder weniger bewusst gegen die Teilnahme entschieden haben, könnte zumindest ein Teil dieser E-Mails z.B. durch allgemeine Filterregeln beim E-Mail-Client in Spam- oder Junk-Ordner verschoben worden sein.

Abbildung 4 **Stichprobenrealisierung im zeitlichen Verlauf**
Anzahl gestarteter Web Surveys im Befragungszeitraum; N=759



Die Zahl von letztendlich 687 auswertbaren Fragebogen, die in die Analyse einfließen, setzt sich aus 601 vollständig und 86 mindestens zu 60 % ausgefüllten Fragebogen zusammen. Damit ergibt sich eine Teilnahmequote von 14,7 % der bereinigten Bruttostichprobe von Befragung II (Tabelle 1).

Neben einem Anschreiben,[35] das von zwei Absenderadressen per E-Mail versschickt wurde, und der Zusendung des Ergebnisberichts als Incentive wurde der Teilnahmezeitraum zur Erhöhung der Rücklaufquote verlängert und vier Erinnerungen[36] nach einer, drei, sechs und neun Wochen per E-Mail versendet.

Die Gründe für den dennoch recht schwachen Rücklauf werden vor allem an der Kontaktierung per E-Mail liegen, insofern technische Hürden wie Spamfilter und Firewalls die erfolgreiche Zustellung erschweren, die Zahl der E-Mails im beruflichen Kontext hoch und das Vertrauen hinsichtlich E-Mails mit Links auf unbekannte Webseiten gering sein dürfte. Hinzu kommt, dass die Befragung in die Haupturlaubszeit und die Zeit der Corona-Krise fiel.

[35] Siehe Anhang 1.

[36] Siehe beispielhaft 2. Erinnerung im Anhang 2.

2.3 Ausfallanalyse

Um zu überprüfen, ob und ggf. mit welchen Faktoren die Teilnahme (Web Survey mindestens zu 60 % abgeschlossen) bzw. Nichtteilnahme an der zweiten Befragung im Zusammenhang steht, wurde eine binär-logistische Regressionsanalyse durchgeführt, deren Ergebnisse in Tabelle 2 dargestellt sind. Die angegebenen Effektkoeffizienten (Exp(β) = Odds Ratio) lassen sich als Erhöhung (Exp(β)>1) bzw. Verringerung (Exp(β)<1) der Chance auf die Teilnahme an Befragung II interpretieren.[37]

Zu erkennen ist, dass das Modell bei einem Nagelkerke R-Quadrat von 0,034 die Schätzung der Teilnahmewahrscheinlichkeit nur minimal verbessert. Dennoch gibt es drei Variablen, die einen signifikanten Einfluss auf die Teilnahmewahrscheinlichkeit haben. D. h., das Unternehmen der Gruppe „Sonstige Rechtsform“[38] signifikant häufiger an der zweiten Befragung teilnahmen als die Referenzgruppe der Kapitalgesellschaften (GmbH, AG). Unternehmen, die ihre IT-Security an externe Dienstleister ausgelagert haben, nahmen signifikant seltener teil und bei Unternehmen, die in den 12 Monaten vor der ersten Befragung mindestens einen Cyberangriff erlebt haben, war die Teilnahmebereitschaft wiederum höher als bei nichtbetroffenen Unternehmen. Dies weist auf eine leichte Stichprobenverzerrung (Nonresponse-Bias) hin, die insbesondere bei der Interpretation der Ergebnisse für alle Unternehmen insgesamt zu berücksichtigen ist.

Da neben dem sehr kleinen R-Quadrat die beiden Gewichtungsvariablen Beschäftigtengrößenklasse und Wirtschaftszweig, keinen statisch relevanten Einfluss auf die Teilnahmewahrscheinlichkeit haben, wird das Designgewicht zur Re-Proportionalisierung der Stichprobe aus der ersten Befragung unverändert beibehalten und auf ein zusätzliches Korrekturgewicht verzichtet.[39]

[37] Vgl. Urban & Mayerl (2011: 341ff.).

[38] Dazu zählen folgende Rechtsformen: Genossenschaft, Körperschaft/ Anstalt des öffentlichen Rechts, Stiftung, Eigenbetrieb, eingetragener Verein und Versicherungsverein auf Gegenseitigkeit.

[39] Vgl. Schnell & Noack (2015: 64).

Tabelle 2 **Binär-logistische Regression zur Teilnahme an Befragung II**

	Exp(β)
Position im Unternehmen (Referenz: Geschäftsführung)	
IT- & Informationssicherheit	1,277
Sonstige Position	0,866
Unternehmensrisiko in den nächsten 12 Monaten bzgl. eines Angriffs, der gleichzeitig auch viele andere Unternehmen trifft (Antwortskala von 1: „sehr gering“ bis 4: „sehr hoch“)	1,109
Unternehmensrisiko in den nächsten 12 Monaten bzgl. eines Angriffs, der ausschließlich Ihr Unternehmen trifft (Antwortskala von 1: „sehr gering“ bis 4: „sehr hoch“	0,945
Beschäftigtengrößenklasse (Referenz: 10-49 Besch.)	
50-99 Besch.	0,821
100-249 Besch.	0,863
250-499 Besch.	0,889
ab 500 Besch.	0,806
Rechtsform (Referenz: Kapitalgesellschaft (GmbH, AG))	
Einzelunternehmer*in	0,798
Personengesellschaft (z.B. OHG, KG)	0,903
Sonstige Rechtsform	1,758***
Wirtschaftszweig (Referenz: Verarbeitendes Gewerbe (WZ08-C))	
Land- u. Forstwirtschaft, Fischerei (WZ08-A)	1,218
Bergbau u. Gewinnung v. Steinen u. Erden (WZ08-B)	1,542
Energieversorgung (WZ08-D)	0,992
Wasserversor.; Abwasser- u. Abfallentsor. u. Beseitigung v. Umweltverschm. (WZ08-E)	1,306
Baugewerbe (WZ08-F)	0,888
Handel; Instandhaltung u. Reparatur v. Kfz (WZ08-G)	0,797
Verkehr u. Lagerei (WZ08-H)	0,650
Gastgewerbe (WZ08-I)	0,522
Information u. Kommunikation (WZ08-J)	0,801
Finanz- u. Versicherungsdienstl. (WZ08-K)	0,653
Grundstücks- u. Wohnungswesen (WZ08-L)	0,746
Freiberufl., wissenschaftl. u. techn. Dienstl. (WZ08-M)	1,153
Sonstigen wirtschaftl. Dienstl. (WZ08-N)	0,837
Öffentl. Verwaltung, Verteidigung; Sozialversicherung (WZ08-O)	1,259
Erziehung u. Unterricht (WZ08-P)	0,858
Gesundheits- u. Sozialwesen (WZ08-Q)	0,829
Kunst, Unterhaltung u. Erholung (WZ08-R)	1,363
Sonstige Dienstl. (WZ08-S)	1,198
Anzahl der (ggf. vor dem schwersten Angriff) vorhandenen IT-Sicherheitsmaßnahmen	1,020
Exporttätigkeit	1,101
IT-Security ausgelagert	0,815*
Standorte mit eigener IT-Struktur in Deutschland	0,999
Standorte mit eigener IT-Struktur im Ausland	0,979
Mindestens eine Angriffsart in den letzten 12 Monaten erlebt	1,260*
N	4.458
Nagelkerkes R^2	0,034

Signifikanzniveau: * p<.05, ** p<.01, *** p<.001

2.4 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 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)[40] in den Diagrammen mit Hilfe sogenannter Fehlerbalken ausgehend vom Ende der Säulen bzw. von den Punkten dargestellt.[41] 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.[42]

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.

2.4.1 Beschäftigtengrößenklassen

In Tabelle 3 sind die Stichprobenverteilungen der Befragungen I und II hinsichtlich der Beschäftigtengrößenklassen zu erkennen. Die Anteile der Unternehmen der einzelnen Beschäftigtengrößenklassen stimmen beim Vergleich der beiden ungewichteten Stichproben weitgehend überein, was ebenfalls dafürspricht, dass der Stichprobenausfall hinsichtlich der Beschäftigtengrößenklasse keine großen Verzerrungen verursacht hat.

Die gewichteten Anteile von Befragung II entsprechen ebenfalls weitgehend denen der Befragung I und damit auch denen in der Auswahlgesamtheit. Die leichten Abweichungen weisen

---

[40] 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.

[41] 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.

[42] 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.

darauf hin, dass insbesondere kleine Unternehmen (10-49 Besch.) in der gewichteten Stichprobe von Befragung II mit einem Anteil von 77,6 % im Vergleich zur Auswahlgesamtheit leicht unterrepräsentiert sind.

Tabelle 3 **Stichprobe nach Beschäftigtengrößenklassen und dem Merkmal Daseinsvorsorge**

	Befragung I			Befragung II		
	ungewichtet		gewichtet	ungewichtet		gewichtet
Beschäftigtengrößenklassen	Anzahl	Prozent	Prozent	Anzahl	Prozent	Prozent
10-49 Besch.	1.190	23,8	79,1	147	21,4	77,6
50-99 Besch.	1.181	23,6	10,5	161	23,4	10,7
100-249 Besch.	1.120	22,4	6,5	162	23,6	7,5
250-499 Besch.	1.005	20,1	2,2	149	21,7	2,4
ab 500 Besch.	504	10,1	1,8	68	9,9	1,7
Gesamt	5.000	100,0	100,0	687	100,0	100,0
Unternehmen der Daseinsvorsorge						
ja	847	16,9	11,2	114	16,6	11,8
nein	4.153	83,1	88,8	573	83,4	88,2
Gesamt	5.000	100,0	100,0	687	100,0	100,0

Unternehmen der Daseinsvorsorge sind gemessen an ihrem Anteil in der Auswahlgesamtheit auch in der ungewichteten Stichprobe von Befragung II mit 16,6 % etwas überrepräsentiert und werden daher bei Gesamtaussagen auf 11,8 % heruntergewichtet.

2.4.2 Branchen

Die Branchenzugehörigkeit der Unternehmen ist bereits in Form der Klassifikation der Wirtschaftszweige des Statistischen Bundesamts von 2008 (WZ 2008)[43] in der Firmendatenbank, die zur Stichprobenziehung für die Befragung I 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 4 sind die Verteilungen der 19 WZ-Klassen (Ebene 1) über alle Unternehmen hinweg in den ungewichteten und gewichteten Stichproben von Befragung I und II zu erkennen. Auch hier zeigen sich im Vergleich zwischen beiden Befragungen nur kleinere Unterschiede: So ist z.B. der Anteil von Unternehmen des Baugewerbes in der gewichteten Stichprobe der zweiten Befragung rund vier Prozentpunkte kleiner als in Befragung I, während Unternehmen der WZ-Klasse Erziehung und Unterreicht um vier Prozentpunkte stärker vertreten sind.[44] Insgesamt

[43] Vgl. Statistisches Bundesamt (2008).

[44] Diese Unterschiede ließen sich zwar durch ein zusätzliches Korrekturgewicht verkleinern, dadurch wäre eine Verzerrung der gewichteten Stichprobe allerding nicht ausgeschlossen. In dem Fall, dass z.B. nur bestimmte Unternehmen des Baugewerbes mit einem weiteren interessierenden Merkmal ausgefallen sind, würde die Höhergewichtung der teilgenommenen Unternehmen des Baugewerbes zur Unterschätzung dieses Merkmals in der Gesamtstichprobe führen, vgl. Schnell & Noack (2015: 64).

zeigt sich allerdings, dass der Stichprobenausfall keinen speziellen Wirtschaftszweig betraf und diesbezüglich keine größeren Verzerrungen verursacht hat.

Tabelle 4 **Stichprobe nach Branchen (WZ 2008)**

	Befragung I			Befragung II		
	ungewichtet		gewichtet	ungewichtet		gewichtet
Branche (WZ08)	Anzahl	Prozent	Prozent	Anzahl	Prozent	Prozent
Land- und Forstwirtschaft, Fischerei (A)	39	0,8	1,4	9	1,3	1,7
Bergbau und Gewinnung von Steinen und Erden (B)	17	0,3	0,3	3	0,4	0,1
Verarbeitendes Gewerbe (C)	1.328	26,6	20,7	189	27,5	21,9
Energieversorgung (D)	68	1,4	0,5	10	1,5	0,5
Wasserversorgung; Abwasser- u. Abfallentsorgung u. Beseitigung v. Umweltverschmutzungen (E)	89	1,8	0,9	15	2,2	1,0
Baugewerbe (F)	310	6,2	12,9	37	5,4	8,8
Handel; Instandhaltung und Reparatur von Kraftfahrzeugen (G)	607	12,1	18,0	68	9,9	15,3
Verkehr und Lagerei (H)	329	6,6	4,7	33	4,8	3,0
Gastgewerbe (I)	130	2,6	4,2	9	1,3	2,4
Information und Kommunikation (J)	152	3,0	3,1	21	3,1	4,1
Erbringung von Finanz- und Versicherungsdienstleistungen (K)	209	4,2	2,1	31	4,5	2,1
Grundstücks- und Wohnungswesen (L)	105	2,1	1,6	11	1,6	1,1
Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen (M)	434	8,7	9,1	74	10,8	13,3
Erbringung von sonstigen wirtschaftl. Dienstleistungen (N)	235	4,7	4,3	24	3,5	1,6
Öffentliche Verwaltung, Verteidigung; Sozialversicherung (O)	19	0,4	0,4	3	0,4	0,6
Erziehung und Unterricht (P)	274	5,5	6,4	47	6,8	10,5
Gesundheits- und Sozialwesen (Q)	436	8,7	5,8	60	8,7	7,1
Kunst, Unterhaltung und Erholung (R)	64	1,3	1,2	12	1,7	0,7
Erbringung von sonstigen Dienstleistungen (S)	155	3,1	2,5	31	4,5	4,1
Gesamt	5.000	100,0	100,0	687	100,0	100,0

2.4.3 Rechtsform

Die Rechtsform der teilnehmenden Unternehmen wurde ebenfalls den zur Stichprobenziehung verwendeten Firmendatenbanken entnommen. Wie bereits in der Ausfallanalyse zu erkennen, steht die Rechtsform in einem statistischen Zusammenhang mit der (Nicht-)Teilnahme an der zweiten Befragung. In Tabelle 5 ist zu erkennen, dass vor allem eingetragene Vereine, Genossenschaften und Körperschaften bzw. Anstalten des öffentlichen Rechts[45] in der Stichprobe von Befragung II stärker vertreten sind als in Befragung I.

[45] In der Ausfallanalyse wurden diese zu den sonstigen Rechtsformen gezählt.

Tabelle 5 **Stichprobe nach Rechtsform**
(zusammengefasste Kategorien)

	Befragung I			Befragung II		
	ungewichtet		gewichtet	ungewichtet		gewichtet
Rechtsform	Anzahl	Prozent	Prozent	Anzahl	Prozent	Prozent
Gesellschaft mit beschränkter Haftung	2925	60,9	64,5	387	58,7	64,5
Gesellschaft mit beschränkter Haftung & Co. Kommanditgesellschaft	827	17,2	13,6	103	15,6	11,0
Eingetragene/r Kaufmann/Kauffrau	124	2,6	5,2	11	1,7	4,3
Aktiengesellschaft	139	2,9	1,9	17	2,6	2,1
Genossenschaft	177	3,7	4,7	24	3,6	5,7
Körperschaft/Anstalt des öffentlichen Rechts	224	4,7	1,9	48	7,3	3,6
Kommanditgesellschaft	48	1,0	0,7	7	1,1	0,3
Offene Handelsgesellschaft	31	0,6	1,4	1	0,2	0,1
Eingetragener Verein	224	4,7	5,0	47	7,1	7,2
Partnerschaftsgesellschaft	28	0,6	0,7	3	0,5	0,1
Stiftung	27	0,6	0,3	5	0,8	0,9
Sonstige	31	0,6	0,1	6	0,9	0,2
Gesamt	4.805	100,0	100,0	659	100,0	100,0

2.4.4 Unternehmensstandort

In Tabelle 6 ist die Stichprobenverteilung nach Bundesland der Unternehmensstandorte zu sehen. Im Vergleich zur Befragung I sind lediglich kleinere Unterschiede zu erkennen. So sind z.B. Unternehmen mit Standort in Bayern in der zweiten Befragung etwas seltener und Unternehmen mit Standort in Nordrhein-Westfalen etwas häufiger vertreten.

Tabelle 6 **Stichprobe nach Bundesland**

	Befragung I			Befragung II		
	ungewichtet		gewichtet	ungewichtet		gewichtet
Standort	Anzahl	Prozent	Prozent	Anzahl	Prozent	Prozent
Schleswig-Holstein	169	3,4	4,0	24	3,5	3,3
Hamburg	140	2,8	2,7	17	2,5	3,2
Niedersachsen	565	11,3	11,0	80	11,6	9,4
Bremen	46	0,9	0,4	3	0,4	0,1
Nordrhein-Westfalen	950	19,0	19,0	137	19,9	21,8
Hessen	304	6,1	5,8	43	6,3	6,6
Rheinland-Pfalz	196	3,9	4,4	23	3,3	5,4
Baden-Württemberg	712	14,2	12,6	89	13,0	12,9
Bayern	930	18,6	19,3	110	16,0	17,0
Saarland	59	1,2	1,1	9	1,3	0,7
Berlin	138	2,8	3,5	17	2,5	2,1
Brandenburg	144	2,9	2,6	29	4,2	3,9
Mecklenburg-Vorpommern	103	2,1	2,1	18	2,6	1,8
Sachsen	270	5,4	6,5	46	6,7	7,6
Sachsen-Anhalt	124	2,5	2,7	18	2,6	3,1
Thüringen	150	3,0	2,4	24	3,5	1,1
Gesamt	5.000	100,0	100,0	687	100,0	100,0

2.4.5 Position der Interviewten innerhalb des Unternehmens

Wie oben angesprochen, liegt eine Schwierigkeit bei Unternehmensbefragungen in der Auswahl eines/r Unternehmensvertreters*in, der*die Auskunft zum Unternehmen gibt. Die bevorzugte Zielperson bei der Befragung I 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 übernommen wird, wurde ein/e Vertreter*in zur Teilnahme gebeten, in dessen/deren Zuständigkeitsbereich das Thema IT & Informationssicherheit fällt.

Bei den an Befragung II teilnehmenden Unternehmensvertreter*innen handelt es sich zu einem Großteil (73,2 %) um die gleiche Person, die bereits an der Befragung I für ihr Unternehmen die Antworten gab, und zu 8,2 % um eine andere Person aus dem jeweiligen Unternehmen. Ein Anteil von 18,5 % wusste nicht mehr, ob sie schon einmal teilgenommen hatte oder nicht (N=680).

Da sich der Tätigkeitsbereich der Befragten möglicherweise auf das Antwortverhalten auswirkt und sich die Zusammensetzung durch neue Unternehmensvertreter*innen verändert haben könnte, wurde die Position innerhalb des Unternehmens erneut erfragt.

Tabelle 7 **Stichprobe nach Position der Interviewten**
(zusammengefasste Kategorien)

	Befragung I ungewichtet		Befragung II ungewichtet		Befragung II gewichtet Prozentanteile nach Beschäftigtengrößenklassen				
Position	Anzahl	Prozent	Anzahl	Prozent	10-49	50-99	100-249	250-499	ab 500
IT- o. Informationssicherheit	3.345	67,0	472	69,5	36,7	64,2	76,7	87,9	88,9
Geschäftsführung	1.171	23,5	148	21,8	52,0	23,9	16,4	6,4	7,9
Sonstige Position	477	9,6	59	8,7	11,3	11,9	6,9	5,7	3,2
Gesamt	4.993	100,0	679	100,0	100,0	100,0	100,0	100,0	100,0

In Tabelle 7 ist zu erkennen, dass die Mehrzahl der befragten Vertreter*innen auch in der Befragung II im Bereich der IT- oder Informationssicherheit arbeitet (69,5 %), und dass es weiterhin 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 (88,9 %), trifft dies in Unternehmen zwischen zehn und 49 Beschäftigten lediglich auf 36,7 % der Befragten zu. Befragte aus dem Bereich Geschäftsführung und sonstigen Positionen sind in kleinen Unternehmen entsprechend stärker vertreten.[46]

2.5 Limitation und Stärken

Auch für die Befragung II gilt, dass lediglich eine Person als Unternehmensvertreter*in zum jeweiligen Unternehmen befragt werden konnte. Die Auswahl geeigneter Repräsentanten*innen erfolgte bei der Kontaktaufnahme mit den Unternehmen in Befragung I, dennoch bleibt das Problem bestehen, dass deren Antworten immer den jeweiligen Wissensstand sowie persönliche Motivationen und Einstellungen widerspiegeln (sogenanntes Self-Reporting-Bias). Bestehen bleibt außerdem, 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 Formen eines sozial erwünschten bzw. dem Unternehmen gegenüber loyalen Antwortverhaltens zumindest ansatzweise zu kontrollieren, wird auch hier das Antwortverhalten verschiedener Befragtengruppen miteinander 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

[46] Mehrfachantworten wurden aufgelöst und die Positionen folgendermaßen zusammengefasst: Befragte, die „Geschäftsführung, Vorstand“ und eine weitere Position angegeben haben, wurden lediglich der Geschäftsführung zugeordnet. Befragte, die „IT- oder Informationssicherheit“ und eine weitere Position mit Ausnahme von „Geschäftsführung, Vorstand“ angegeben haben, wurden ausschließlich der „IT- oder Informationssicherheit“ zugeordnet. Alle anderen Positionen (z.B. Governance und Datenschutz) wurden in der Kategorie „sonstige Position“ zusammengefasst

zudem möglich, dass bestimmte Ereignisse Einfluss auf das Antwortverhalten hatten.[47] So könnten z.B. der Anteil der Unternehmen, die das Risiko von Cyberangriffen (eher) hoch bewerteten, überschätzt sein.

Aus forschungspragmatischen Gründen konnte das Vorhandensein bestimmter Merkmale und Maßnahmen nur recht oberflächlich erfragt werden. Im Unterschied zur Befragung I, die als CATI-Befragung durchgeführt wurde, war es allerdings in Befragung II mittels Web Survey möglich, komplexere Fragekonstruktionen (Matrix-Fragen) einzusetzen und vergleichsweise detaillierte Angaben z.B. zu den eingesetzten IT-Sicherheitsmaßnahmen zu erheben (Reifegrad und Verbreitung im Unternehmen).

Ein weiterer Vorteil liegt darin, dass mit beiden Befragungen Paneldaten erhoben wurden, d.h. es liegen, soweit wir sehen, erstmals Daten zum Thema „Cyberangriffe gegen Unternehmen" einer disproportional geschichteten Zufallsstichprobe mit zwei Messzeitpunkten vor. Im Gegensatz zu einzelnen Querschnittsbefragungen ist es mit diesem Längsschnitt möglich, Entwicklungen aufzeigen zu können.

Trotz des relativ geringen Rücklaufs bei Befragung II, nehmen wir im Lichte der beschriebenen Ausfallanalyse an, dass verallgemeinerbare Aussagen möglich sind, wenn auch mit größerer Unsicherheit aufgrund der kleineren Stichprobengröße.

[47] Das Thema IT-Sicherheit war im Zusammenhang mit der Corona-Krise und der Zunahme digitaler Anwendungen medial sehr präsent und könnte die Antworten beeinflusst haben. Daher wurden zusätzliche Kontrollfragen zu den Veränderungen in der Corona-Krise in den Fragebogen aufgenommen. Zu den Ergebnissen siehe insbesondere Abschnitt 3.5.

3 IT-SICHERHEITSSTRUKTUR

Zu den Befunden der ersten Unternehmensbefragung zählte, dass „organisatorische Sicherheitsmaßnahmen [neben Branchenunterschieden] in kleineren Unternehmen weniger verbreitet sind, als in größeren“[48] und dass „die erfragten technischen IT-Sicherheitsmaßnahmen quantitativ betrachtet bereits sehr stark verbreitet zu sein scheinen“[49]. Daher, so die Schlussfolgerung, „wird es in der weiteren Forschung darauf ankommen, nach den qualitativen Unterschieden zu suchen.“[50]

Um insbesondere zu den technischen IT-Sicherheitsmaßnahmen ein differenzierteres Bild zu erhalten, wurden in der zweiten Befragung entsprechende Fragen teilweise spezifiziert und weitere IT-Sicherheitsmaßnahmen erfragt. Zu den zusätzlich IT-Sicherheitsmaßnahmen zählen:

- Zwei-Faktor Authentifizierung,
- Test der Datenwiederherstellung (Restoring),
- Netzwerksegmentierung,
- Security Information and Event Management (SIEM),
- Security Operation Center (SOC),
- Austausch von Bedrohungsdaten (z.B. Threat Intelligence),
- künstliche Intelligenz basierte Maßnahmen,
- Verschlüsselung von Kommunikation,
- Verschlüsselung von sensiblen Daten sowie
- verstärkte physische Sicherheit.

Ein Vergleich mit den Ergebnissen zur ersten Befragung ist aufgrund der deutlich veränderten Abfrage nur sehr beschränkt möglich. Daher werden im Folgenden lediglich die Ergebnisse für die IT-Sicherheitsmaßnahmen gegenübergestellt, bei denen der Wortlaut unverändert geblieben ist. Entsprechende Unterschiede sind dennoch mit Vorsicht zu interpretieren, da sich nicht nur viele der übrigen Antwortmöglichkeiten, sondern auch die Erhebungsmethode verändert hat. Bei einem Web Survey können die Befragten länger über die Fragen und Antwortmöglichkeiten nachdenken und geben bei komplexen Fragestellungen möglicherweise zutreffendere Antworten als bei einer telefonischen Befragung.

Neben zusätzlichen IT-Sicherheitsmaßnahmen wurde deren Reifegrad und Verbreitung innerhalb des Unternehmens erfragt. Der Reifegrad wurde für jede Maßnahme anhand einer vierstufigen Skala von 1: „Grundfunktionalität“ bis 4: „Erweiterte Funktionalität und regelmäßige Überprüfung bzw. Optimierung“ erhoben und die Verbreitung der Maßnahmen innerhalb des Unternehmens mit einer dreistufigen Skala von 1: „stark begrenzt“, 2: „teilweise“ bis 3: „weitgehend“ (Abbildung 5).

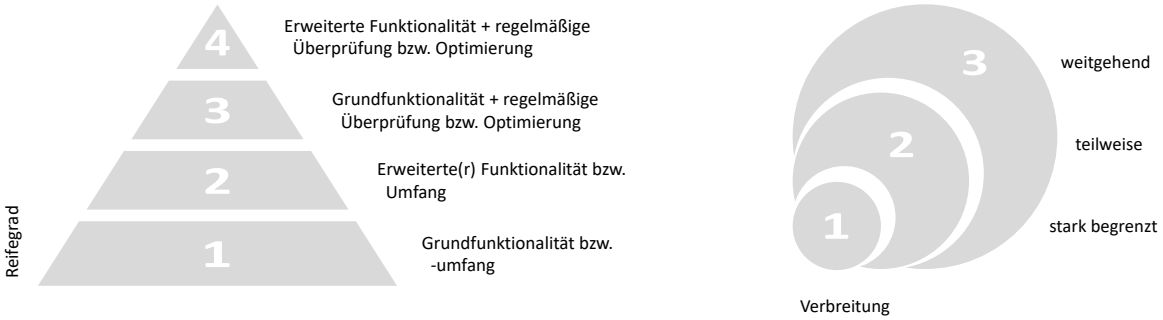
---

[48] Dreißigacker et al. (2020a: 88).

[49] Dreißigacker et al. (2020a: 164).

[50] Ebd.

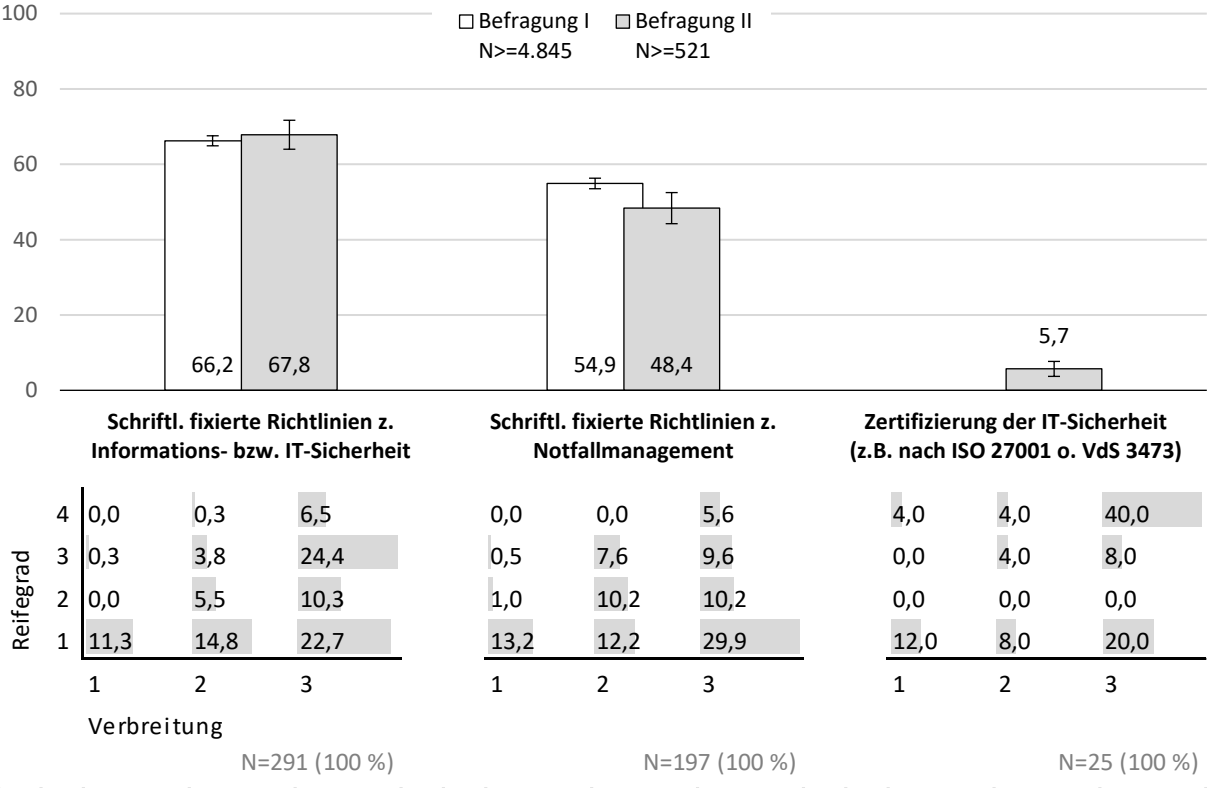
Abbildung 5 **Skalen zum Reifegrad und zur Verbreitung im Unternehmen**



Die Darstellungen der Verteilungen nach Reife- und Verbreitungsgrad (in Prozent) beziehen sich im Folgenden immer auf Befragung II und erfolgen jeweils über eine Zwölf-Felder-Matrix unterhalb der Diagramme zu den Unternehmensanteilen mit den entsprechenden IT-Sicherheitsmaßnahmen. In den unteren linken Ecken der Matrizen sind z.B. die Anteile der Unternehmen mit den jeweiligen IT-Sicherheitsmaßnahmen mit geringem Reifegrad (Grundfunktionalität/ -umfang) und stark begrenzter Verbreitung im Unternehmen abzulesen. In den entgegengesetzten oberen rechten Ecken werden die Anteile der Unternehmen abgetragen, die über die erfragten IT-Sicherheitsmaßnahmen mit hohem Reifegrad (erweiterte Funktionalität und regelmäßiger Überprüfung bzw. Optimierung) und weitgehender Verbreitung im Unternehmen verfügen (siehe z.B. Abbildung 6 zu Richtlinien und Zertifizierung der IT-Sicherheit).

3.1 Organisatorische IT-Sicherheitsmaßnahmen

Abbildung 6 **Richtlinien und Zertifizierung der IT-Sicherheit**
in Prozent; gewichtete Daten



Der Anteil der Unternehmen, die über schriftlich fixierte Richtlinien zur Informations- bzw. IT-Sicherheit verfügen (Abbildung 6) hat sich zwischen den Befragung I (2018/19) und Befragung II (2020) nicht statistisch relevant verändert (66,2 % vs. 67,8 %). Bezieht man die Angaben zu Reifegrad und Verbreitung innerhalb des Unternehmens ein, ist zu erkennen, dass in den meisten Unternehmen diesbezüglich noch Optimierungspotential besteht: So wird der Reifegrad dieser Richtlinien in knapp der Hälfte als gering eingeschätzt (48,8 %) und in jedem neunten Unternehmen beziehen sich IT-Sicherheitsrichtlinien lediglich auf einen stark begrenzten Unternehmensbereich.

Ein ähnliches Bild ergibt sich in Hinblick auf schriftlich fixierte Richtlinen zum Notfallmanagement, die mit 48,4 % etwas seltener bei den befragten Unternehmen vorhanden sind. Der zu erkennende Unterschied zur Befragung I (54,9%) könnte auf die Veränderung der Erhebungsmethode zurückzuführen sein, da der Anteilswert auch unter den erneut teilnehmenden Unternehmen in der Befragung I größer ausfiel als in Befragung II. Möglicherweise haben die Unternehmensvertreter*innen in der telefonischen Befragung eher sozial erwünscht geantwortet als in Web Survey.

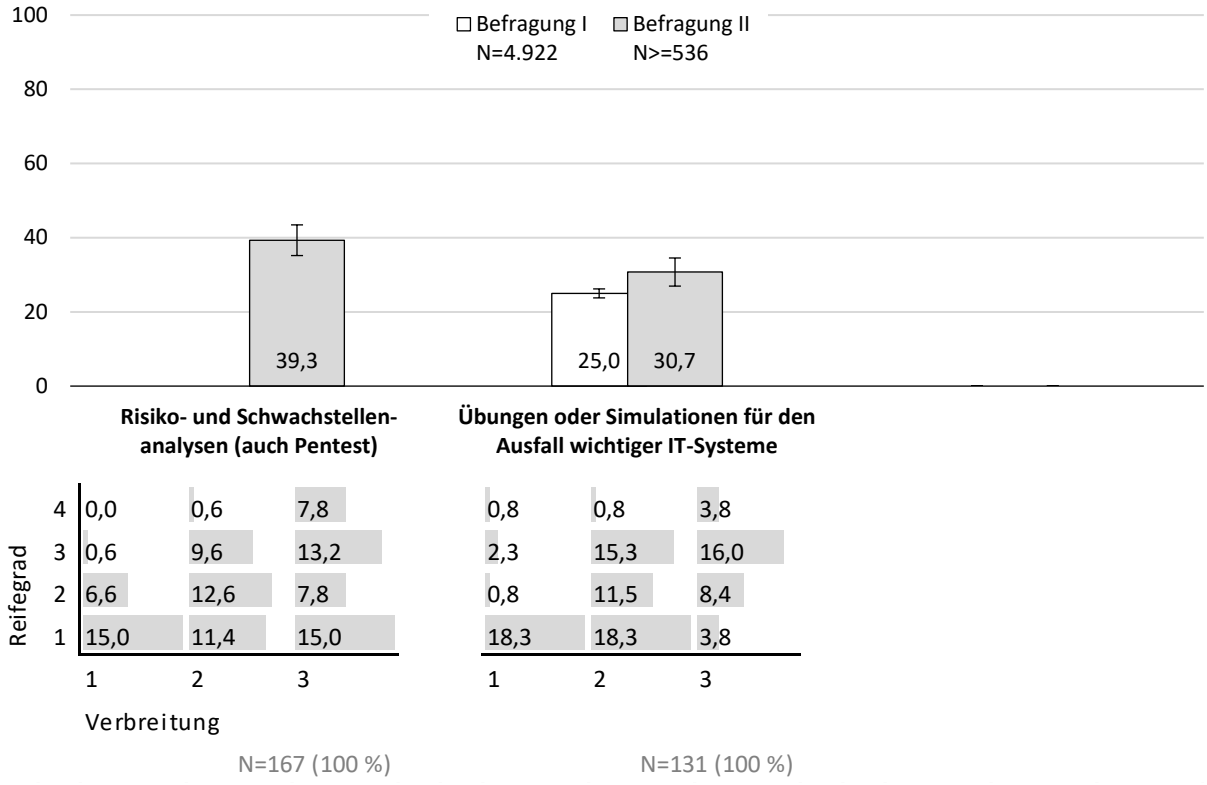
Lediglich 5,7 % der Unternehmen haben ihre IT-Sicherheit z.B. nach ISO 27001 oder VdS 3437 zertifizieren lassen.[51] Wenn eine Zertifizierung vorhanden ist, dann bezieht sie sich größtenteils auf das gesamte Unternehmen und nicht nur auf einen Teilbereich und hat relativ häufig einen hohen Reifegrad (Abbildung 6).

Etwa zwei Fünftel der Unternehmen führen Risiko- und Schwachstellenanalysen (auch Penetrationtesting) durch (39,3 %; Abbildung 7),[52] die sich allerdings relativ häufig nur auf einen Teilbereich des Unternehmens beziehen und hinsichtlich des Reifegrades lediglich Grundfunktionen abdecken, ohne dass diese regelmäßig überprüft bzw. optimiert werden.

[51] Ein Vergleich mit dem Ergebnis der Befragung I ist nicht sinnvoll, da sich neben der Erhebungsmethode auch der Wortlaut der Abfrage verändert hat. Die Frage, ob es im Unternehmen eine „Zertifizierung der IT-Sicherheit (z.B. nach ISO 27001 oder BSI Grundschutz)“ gibt, bejahte in Befragung I ein Anteil von 24,8 %. Dieser relativ große Anteil ist vermutlich auf die beispielhafte Nennung des BSI Grundschutzes zurückzuführen. Da es sich dabei allerdings um eine vom BSI entwickelte Vorgehensweise zur Identifikation von Schwachstellen und zur Umsetzung von Sicherheitsmaßnahmen handelt und nicht mit einer Zertifizierung verbunden sein muss, dürfte das aktuelle Ergebnis zur Zertifizierung der IT-Sicherheit in Befragung II realistischer sein.

[52] Da auch hierzu der Wortlaut der Abfrage verändert wurde (von „regelmäßige Risiko- und Schwachstellenanalysen“ in Befragung I zu „Risiko- und Schwachstellenanalysen (auch Pentest)“ in Befragung II), ist ein Vergleich der Ergebnisse ebenfalls nicht sinnvoll.

Abbildung 7 **Risiko- u. Schwachstellenanalysen und Übungen o. Simulationen für den Ausfall wichtiger Systeme**
in Prozent; gewichtete Daten



3.1.1 Schulungen zur IT-Sicherheit für Beschäftigte

Statt der Frage, ob Schulungen zur IT-Sicherheit für Beschäftigte durchgeführt werden, was in der Befragung I ein Gesamtanteil von 49,8 % bejaht hat,[53] wurde in der zweiten Befragung die Zustimmung[54] zu den folgenden Aussagen erhoben:

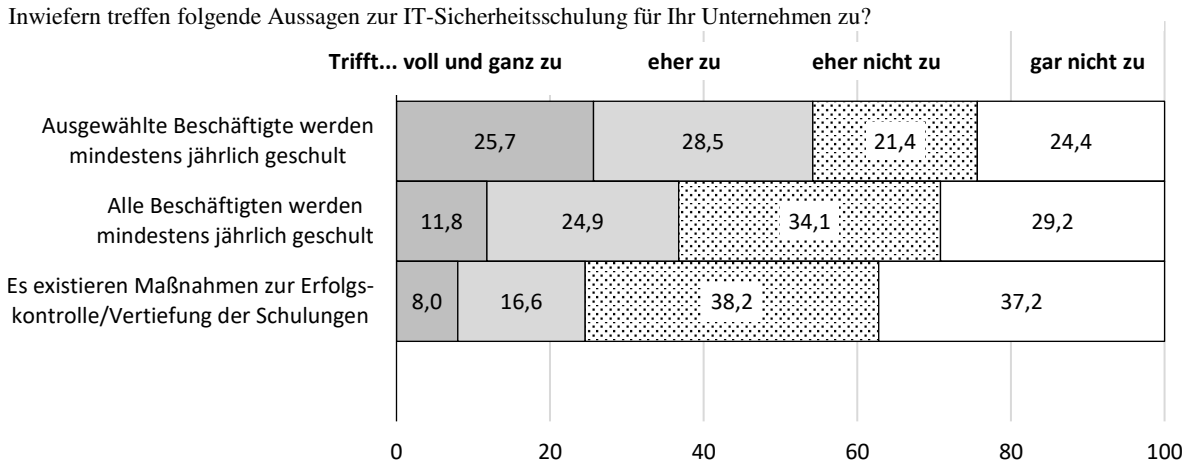
- Ausgewählte Beschäftigte werden mindestens jährlich geschult
- Alle Beschäftigten werden mindestens jährlich geschult
- Es existieren Maßnahmen zur Erfolgskontrolle/ Vertiefung der Schulungen

Dass es zumindest für ausgewählte Beschäftigte mindestens jährlich Schulungen gibt, trifft demnach für 54,2 % eher bzw. voll und ganz zu und entspricht damit dem oben genannten Anteil zu IT-Sicherheitsschulungen aus der ersten Befragung. Bezogen auf jährliche Schulungen für alle Beschäftigten liegt der Anteil der (eher) zustimmenden Befragten nur noch bei 36,7 % und hinsichtlich vorhandener Maßnahmen zur Erfolgskontrolle/ Vertiefung der Schulungen mit einem Anteil von 24,6 % noch einmal deutlich darunter (Abbildung 8).

[53] Dreißigacker et al. (2020a: 75).

[54] Vierstufige Antwortskala (1: „Trifft gar nicht zu“, 2: „Trifft eher nicht zu“, 3: „Trifft eher zu“, 4: „Trifft voll und ganz zu“)

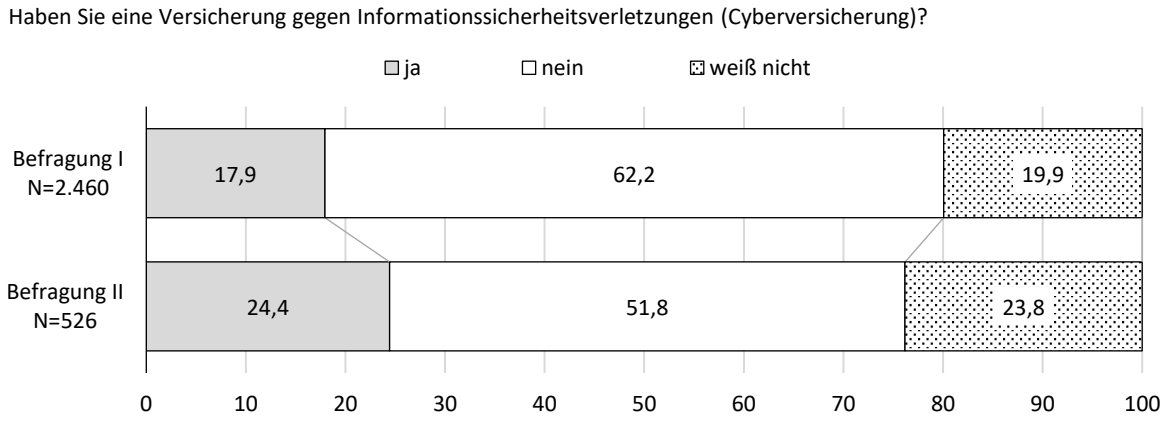
Abbildung 8 **Einschätzungen zu IT-Sicherheitsschulung für Beschäftigte**
in Prozent; gewichtete Daten



3.1.2 Versicherung gegen Informationssicherheitsverletzungen (Cyberversicherung)

Der Anteil der Unternehmen mit einer Versicherung gegen Informationssicherheitsverletzungen hat sich unter Einbezug der Antwortkategorie „weiß nicht“ zur ersten Befragung von 17,9 % (N=2.460) auf 24,4 % (N=526) erhöht (Abbildung 9). Der Anteil derjenigen, die dazu keine Angabe machen konnten, stiegt dabei ebenfalls leicht von 19,9 % auf 23,8 %. Um der plausiblen Annahme zu folgen, dass Unternehmen für den Abschluss einer Cyberversicherung einen gewissen IT-Sicherheitsstandard haben müssen und daher vergleichsweise besser geschützt sind als Unternehmen ohne Cyberversicherung, wurde eine entsprechende Nachfrage gestellt. Überraschenderweise verneinten fast zwei Drittel der Unternehmen mit einer solchen Versicherung (62,2 %; N=107) die Frage, ob ggf. zum Abschluss der Cyberversicherung bestimmte IT-Sicherheitsstandards nachgewiesen werden mussten.

Abbildung 9 **Versicherung gegen Informationssicherheitsverletzungen**
in Prozent; gewichtete Daten



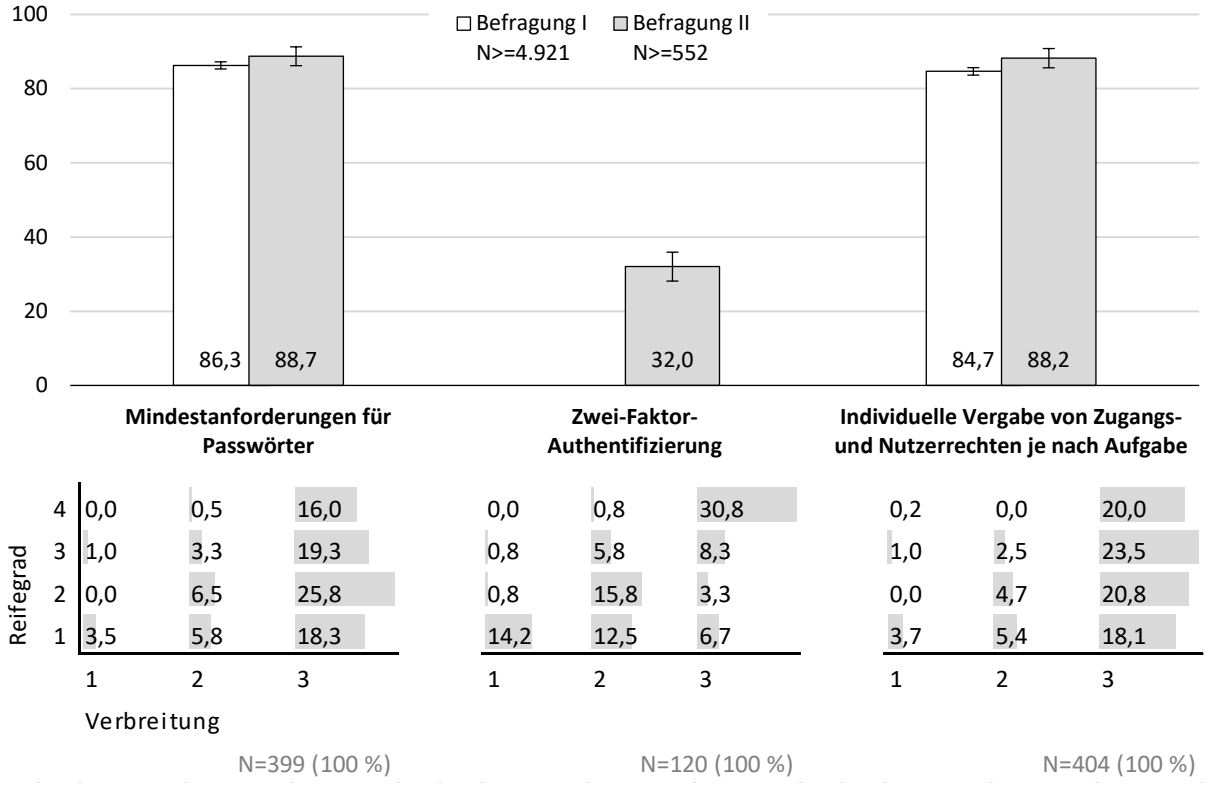
3.2 Technische IT-Sicherheitsmaßnahmen

Die Anteile der Unternehmen mit Mindestanforderungen für Passwörter und individueller Vergabe von Zugangs- und Nutzerrechten je nach Aufgabe der Beschäftigten haben sich im Vergleich zur Befragung I zumindest tendenziell auf 88,7 bzw. 88,2 % erhöht (Abbildung 10).

Positiv zu bewerten ist auch die zumeist weitgehende Verbreitung innerhalb der Unternehmen, auch wenn sich der Reifegrad dieser Maßnahmen bei gut einem Viertel der Unternehmen als basal bezeichnen lässt (Grundfunktionalität/ -umfang). Etwa ein Drittel der Unternehmen setzt zusätzlich auf Zwei-Faktor-Authentifizierung.

Abbildung 10 **Passwortanforderung, 2FA u. Zugangs-/ Nutzerrechte**

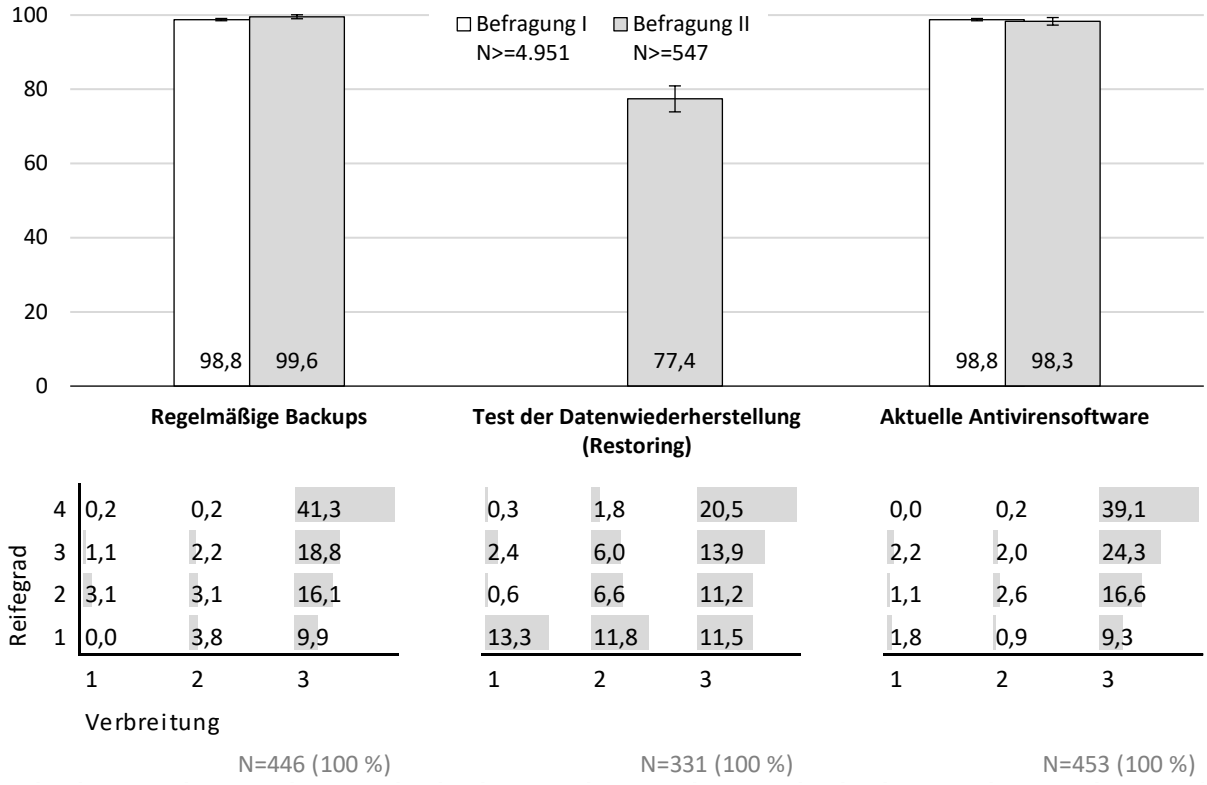
in Prozent; gewichtete Daten



Wie bereits bei der Befragung I gaben fast alle Unternehmensvertreter*innen an, dass in ihren Unternehmen regelmäßig Backups durchgeführt werden (99,6 %) und aktuelle Antivirensoftware zum Einsatz kommt (98,3 %; Abbildung 11). Diese Maßnahmen sind ebenfalls weitgehend in den Unternehmen verbreitet, bei jedem siebten bis achten Unternehmen allerdings mit basalem Reifegrad. Ob die Datenwiederherstellung mit Hilfe der Backups funktioniert (Restoring), testen über drei Viertel der Unternehmen (77,4 %). In rund jedem sechsten Unternehmen erfolgen diese Tests aber lediglich für einen stark begrenzten Bereich und bei über einem Drittel wird der Reifegrad dieser Maßnahme als gering eingestuft.

Abbildung 11 **Backup, Restoring, Antivirensoftware**

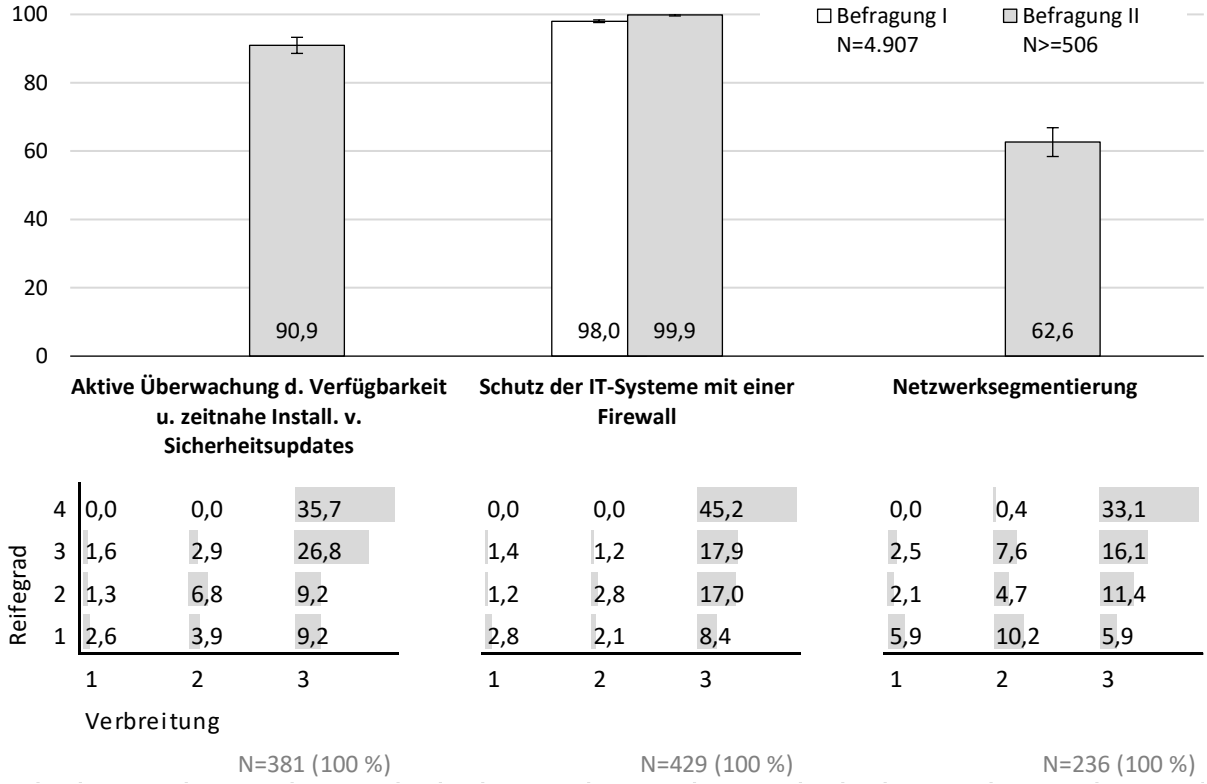
in Prozent; gewichtete Daten



N=446 (100 %) N=331 (100 %) N=453 (100 %)

Abbildung 12 **Sicherheitsupdates, Firewall u. Netzwerksegmentierung**

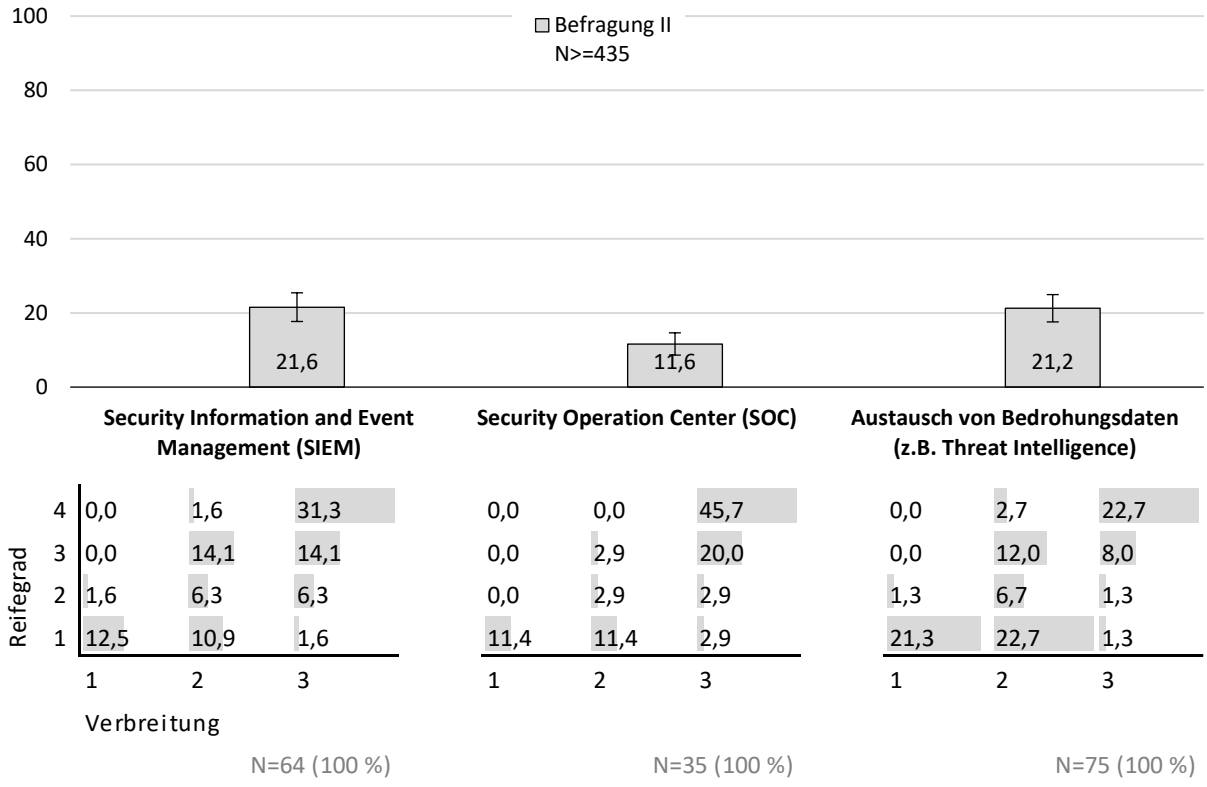
in Prozent; gewichtete Daten



N=381 (100 %) N=429 (100 %) N=236 (100 %)

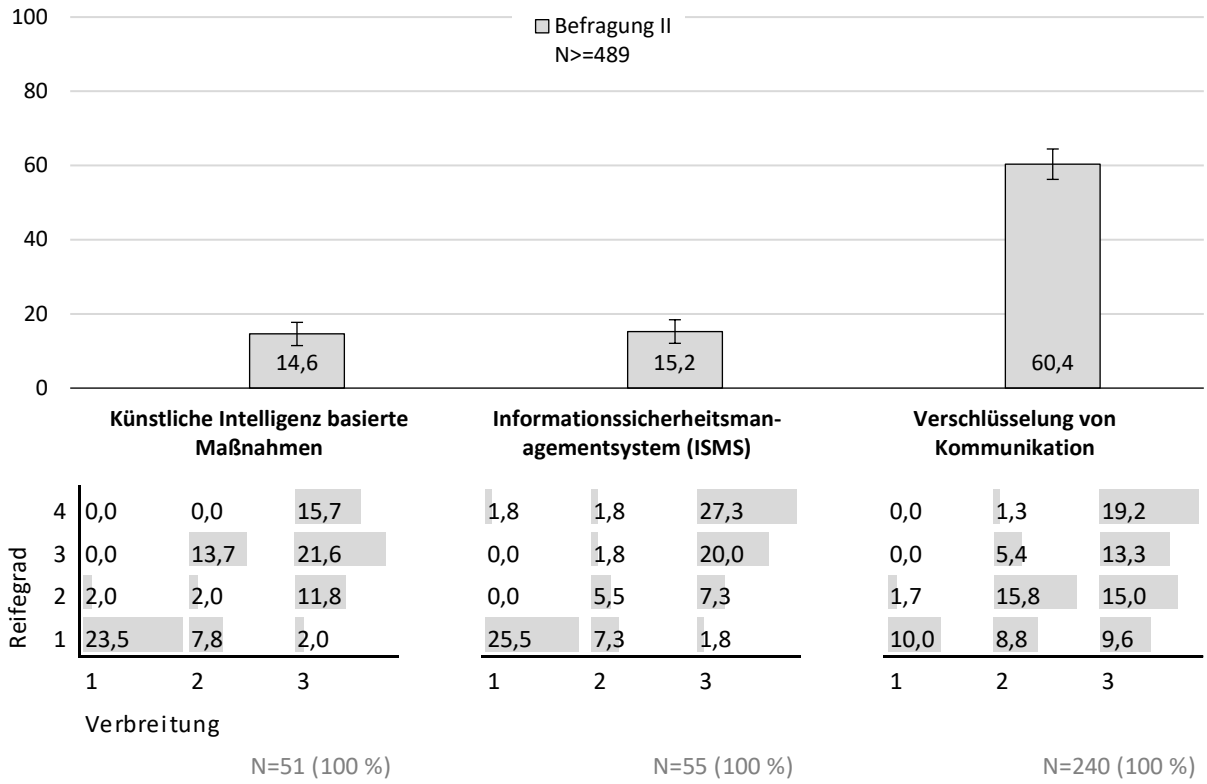
Hinsichtlich der Installation verfügbarer Sicherheitsupdates wurde im Vergleich zur Befragung I die Formulierung verändert. Während 95,7 % der Unternehmen in Befragung I angaben, regelmäßige und zeitnahe Installationen verfügbarer Sicherheitsupdates und Patches vorzunehmen, liegt der Anteil der Unternehmen in Befragung II, der die Verfügbarkeit von Sicherheitsupdates aktiv überwacht und diese ggf. zeitnah installiert, mit 90,9 % etwas niedriger (Abbildung 12). Der Schutz der IT-Systeme mit einer Firewall ist nach wie vor fast überall und weitgehend verbreitet vorhanden, aber auch hier zeigen sich Unterschiede im Reifegrad: Bei jedem siebten bis achten Unternehmen werden lediglich Firewalls mit Grundfunktionalität eingesetzt. Die Netzwerksegmentierung, d.h. die Unterteilung des Unternehmensnetzwerkes in einzelne Bereiche z.B. mit dem Ziel, die Ausbreitung von Schadsoftware ggf. zu begrenzen, erfolgt in knapp zwei Dritteln der Unternehmen (62,6 %). Der Reifegrad dieser Maßnahme wird von über einem Fünftel dieser Unternehmen als gering eingeschätzt (Grundfunktionalität/ -umfang).

Abbildung 13 **SIEM, SOC und Threat Intelligence**
in Prozent; gewichtete Daten



Neben der Netzwerksegmentierung wurden weitere Maßnahmen in Befragung II zusätzlich erhoben, mit denen die IT-Sicherheit verbessert werden kann. Über ein Security Information and Event Management (SIEM) verfügt etwa ein Fünftel der Unternehmen (21,6 %). Ein Security Operation Center (SOC) haben 11,6 % eingerichtet und mit dem Austausch von Bedrohungsdaten (z.B. Nutzung von Threat Intelligence Diensten) arbeitet ebenfalls gut ein Fünftel (21,2 %), wobei der Reifegrad dieser Maßnahme relativ häufig als gering eingeschätzt wird und sich oft nicht auf das ganze Unternehmen erstreckt.

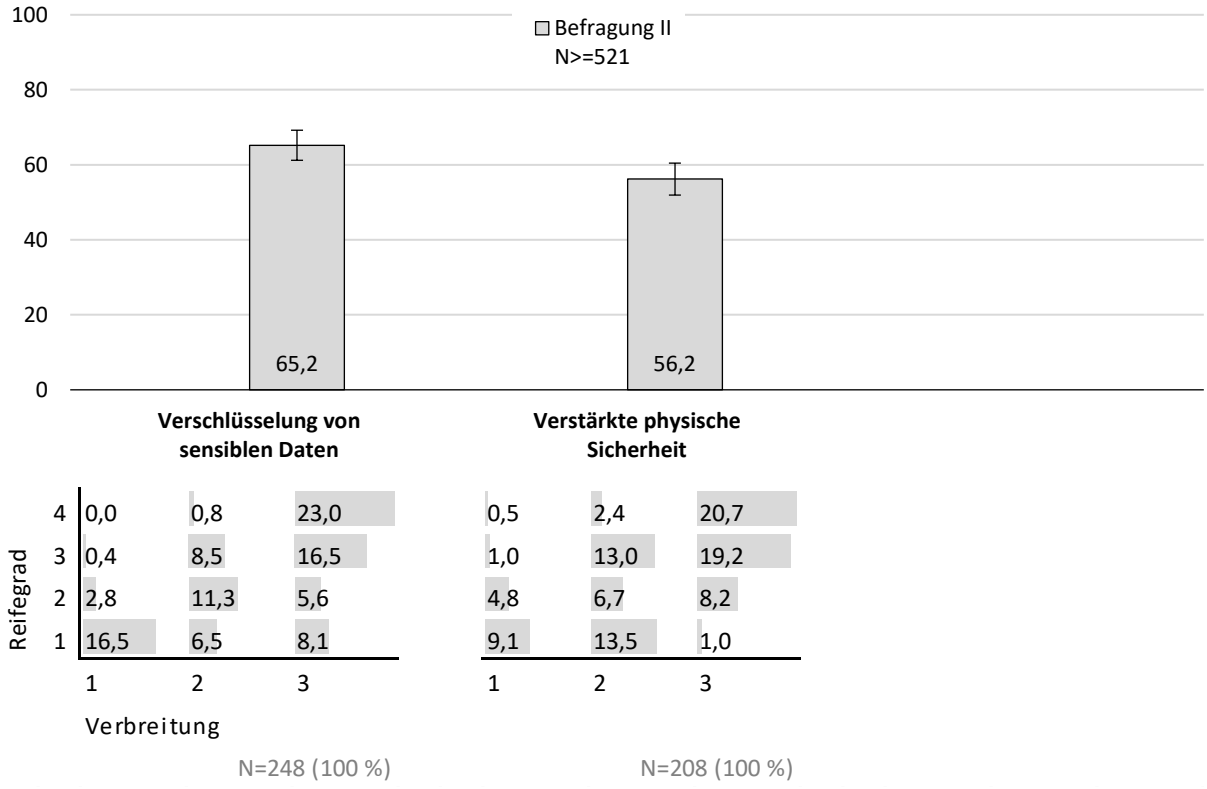
Abbildung 14 **KI, ISMS, u. Verschlüsselung v. Kommunikation**
in Prozent; gewichtete Daten



IT-Sicherheitsmaßnahmen, die auf künstlicher Intelligenz basieren und Informationssicherheitsmanagementsysteme (ISMS) werden mit 14,6 bzw. 15,2 % vergleichsweise selten eingesetzt (Abbildung 14). Hinzu kommt, dass sowohl deren Reifegrad als auch deren Verbreitung innerhalb des Unternehmens relativ häufig als gering (Grundfunktionalität/ -umfang bzw. stark begrenzt) eingeschätzt wird. Ein Anteil von 60,4 % setzt auf verschlüsselte Kommunikation und auch hiervon gibt etwa jedes neunte Unternehmen an, dass sich die Verschlüsselung nur auf einen stark begrenzten Bereich bezieht.

Bei einem Anteil von 65,2 % der Unternehmen werden sensible Daten verschlüsselt (Abbildung 15) und damit vor unberechtigtem Zugriff geschützt. Etwas über die Hälfte (56,2 %) verfügt über eine verstärkte physische Sicherheit. Auch bei diesen beiden Maßnahmen ist eine relativ große Varianz hinsichtlich des Reifegrads und der Verbreitung innerhalb des Unternehmen zu erkennen.

Abbildung 15 **Verschlüsselung v. sensiblen Daten u. physische Sicherheit**
in Prozent; gewichtete Daten



3.3 Ausgelagerte IT-Funktionen

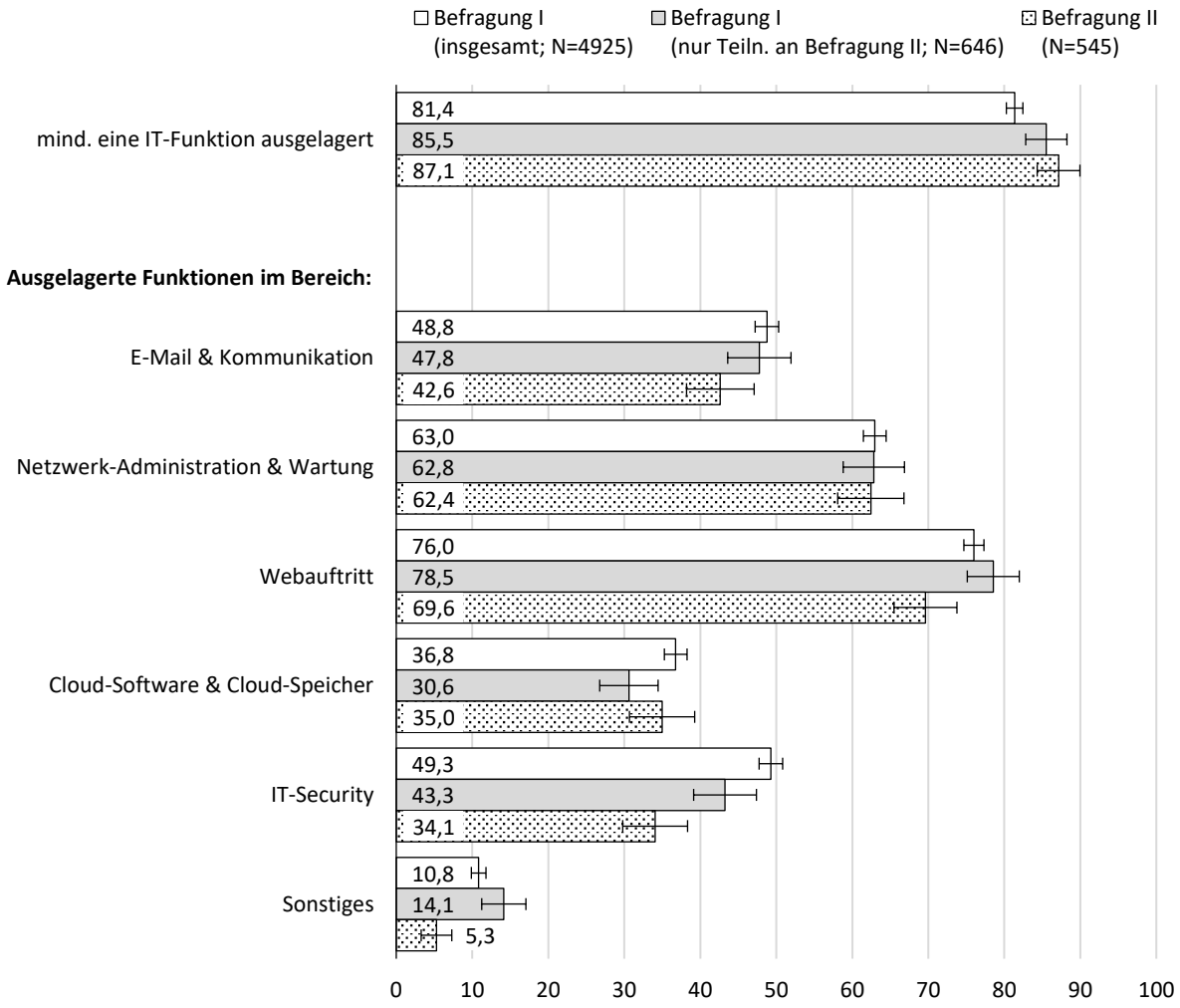
Der Anteil der Unternehmen, die mindestens in einem Bereich IT-Funktionen auslagern und von externen Dienstleister erbringen lassen, hat sich im Vergleich zur Befragung I unter Kontrolle der Beteiligung an Befragung II[55] statistisch nicht relevant verändert und bleibt auf einem relativ hohem Niveau von über 80 % (Abbildung 16).

Deutliche Unterschiede sind hingegen in Hinblick auf ausgelagerte IT-Funktionen in den Bereichen Webauftritt und IT-Security zu erkennen. Der Anteil der Unternehmen, bei denen der Webauftritt (z.B. Online-Marktplätze, Shops, Kundenportale) von einem Dienstleister erbracht wird, sank von 78,5 % auf 69,6 % und in Hinblick auf die IT-Security (z.B. Incident Detection, SIEM, Threat Intelligence) von 43,3 % auf 34,1 %.[56] Daneben sank auch der Anteil mit sonstigen ausgelagerten IT-Funktionen von 14,1 % auf 5,3 %.

[55] Unternehmen mit ausgelagerter IT-Security in Befragung I haben signifikant seltener an der Befragung II teilgenommen (siehe Abschnitt 2.3). Aus diesem Grund werden hier lediglich die Ergebnisse der Unternehmen verglichen, die an beiden Befragungen teilgenommen haben.

[56] Am deutlichsten sank dieser Anteil bei den kleinen Unternehmen (10-49 Besch.: von 44,7 % auf 35,1 %). Bei großen Unternehmen (ab 500 Besch.) blieb der Anteilswert hingegen fast unverändert (23,1 % vs. 24,5 %).

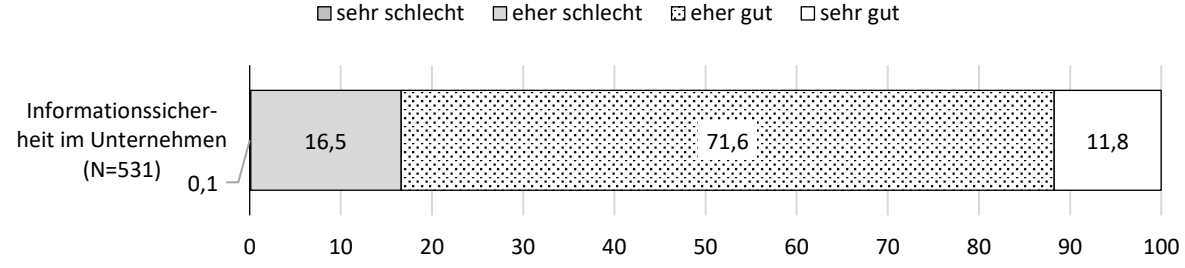
Abbildung 16 **Anteil der Unternehmen mit ausgelagerten IT-Funktionen**
in Prozent; gewichtete Daten; 95%-KI; Mehrfachantworten hinsichtl. der IT-Funktionsbereiche mögl.



3.4 Einschätzung der Informationssicherheit

Die Frage „Wie gut schätzen Sie die Informationssicherheit in Ihrem Unternehmen insgesamt ein?“ konnte auf einer Skala von 1 „Sehr schlecht“ bis 4 „sehr gut“ beantwortet werden. Die Vertreter*innen etwa jedes sechsten Unternehmens (16,6 %) bewerteten diese als sehr/eher schlecht ein, wobei „sehr schlecht“ nur ein einziges Mal (0,1 %) angegeben wurde (Abbildung 17).

Abbildung 17 **Einschätzung der Informationssicherheit im Unternehmen**
in Prozent; gewichtete Daten



Diese Einschätzung steht in Zusammenhang mit der Position der befragten Unternehmensvertreter*innen. So schätzten etwa jede/r neunte Unternehmensvertreter*in aus der Geschäftsführung bzw. des Vorstands die Informationssicherheit im Unternehmen als sehr/eher schlecht ein (11,5 %), wohingegen dies jede/r fünfte aus der IT-/Informationssicherheit sowie aus sonstigen Bereichen so sah (19,9 % bzw. 19,7 %). In Hinblick auf die Beschäftigtengrößenklassen sind diesbezüglich keine statistisch relevanten Unterschiede zu erkennen.

Tabelle 8 **Einschätzung der Informationssicherheit im Unternehmen nach Position und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)

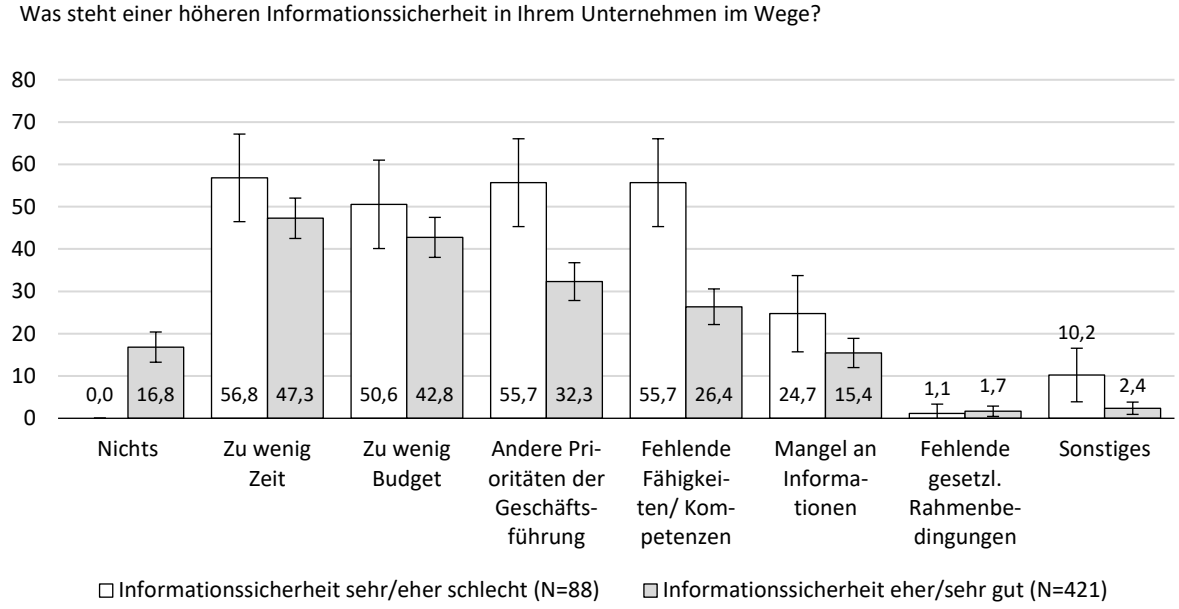
		Position innerhalb des Unternehmens			Beschäftigtengrößenklasse				
	Gesamt	Gschf.	IT	Sonst.	10-49	50-99	100-249	250-499	ab 500
	Anteile der Antworten "sehr/eher schlecht"								
Informationssicherheit im Unternehmen (N=531)	16,6	**11,5**	**19,9**	**19,7**	17,2	14,3	12,8	10,9	18,6
Was steht einer höheren Informationssicherheit in Ihrem Unternehmen im Wege? (Mehrfachantwort möglich; N=527)									
Nichts	13,4	**22,3**	**5,1**	**16,4**	**14,8**	9,8	6,6	8,0	**1,8**
Zu wenig Zeit	48,5	**40,3**	**58,9**	**34,3**	**45,1**	**62,9**	**61,3**	**64,0**	**78,9**
Zu wenig Budget	43,0	**33,0**	**50,8**	**44,8**	**38,5**	**57,6**	**57,7**	**60,0**	**54,4**
Andere Prioritäten der Geschäftsführung	36,0	**24,3**	**49,6**	**20,9**	34,1	41,7	47,1	48,8	35,7
Fehlende Fähigkeiten/ Kompetenzen	32,1	**38,8**	**30,4**	**17,6**	31,7	37,9	35,0	31,2	32,1
Mangel an Informationen	18,2	**28,6**	**14,2**	**1,5**	**21,1**	17,3	**7,3**	16,0	12,3
Fehlende gesetzliche Rahmenbedingungen	1,5	2,9	0,8	0,0	0,8	2,3	2,9	4,0	7,1
Sonstiges	4,3	2,9	5,5	4,5	4,1	3,0	4,4	3,2	7,0

Danach gefragt, was einer höheren Informationssicherheit im Unternehmen im Wege steht, wurde insgesamt am häufigsten ein Mangel an Zeit (48,5 %) und finanziellen Ressourcen (43,0 %) genannt (Tabelle 8). Eine andere Priorisierung der Geschäftsführung sowie fehlende Fähigkeiten/ Kompetenzen wurden von 36,0 % bzw. 32,1 % angegeben und ein Mangel an Informationen von 18,2 %. Fehlende gesetzliche Rahmenbedingungen scheinen bei der Verbesserung der Informationssicherheit in Unternehmen kein bedeutender Hinderungsgrund zu sein, da dies lediglich 1,5 % nannten. Zu den sonstigen Gründen, die von 4,3 % angegeben wurden, zählte vor allem fehlendes Personal, veraltete Software, fehlende Einsicht und Motivation bei Beschäftigten sowie fehlende Angebote und Förderprogramme.

Beim Vergleich der genannten Hürden bei der Verbesserung der Informationssicherheit im Unternehmen nach den Positionen der Unternehmensvertreterinnen fallen deutliche Unterschiede auf (Tabelle 8). Insbesondere der Zeitmangel, der Budgetmangel und die Priorisierung der Geschäftsführung wird von Befragten aus dem Bereich der IT-/Informationssicherheit deutlich häufiger genannt als von Befragten der Geschäftsführung bzw. des Vorstands. Fehlende Fähig-

keiten/ Kompetenzen und mangelnde Informationen sind hingegen signifikant häufiger genannte Hürden aus Sicht der Geschäftsführung bzw. des Vorstands im Vergleich mit den anderen Positionen. Die Nennung von Zeit- und Budgetmangel steht ebenfalls in Zusammenhang mit der Beschäftigtengrößenklasse, insofern diese in größeren Unternehmen deutlich häufiger angegeben wurden als in kleineren.[57]

Abbildung 18 **Hürden bei der Verbesserung der Informationssicherheit nach deren Bewertung**
in Prozent; gewichtete Daten; 95%-KI



In Abbildung 18 ist abzulesen, wie sich die Häufigkeit der jeweiligen Verbesserungshürden zwischen den Unternehmen unterscheiden, deren Informationssicherheit entweder als sehr/eher schlecht oder als eher/sehr gut eingeschätzt wurde. Die Unternehmensvertreter*innen, die die Informationssicherheit in ihrem Unternehmen als sehr/eher schlecht einstuften, gaben signifikant häufiger an, dass eine andere Priorisierung der Geschäftsführung (55,7 %) und fehlende Fähigkeiten/ Kompetenzen (55,7 %) einer Verbesserung der Informationssicherheit im Wege stehen als Vertreter*innen, die die Informationssicherheit besser bewerteten.

3.5 IT-Sicherheit in der Corona-Krise

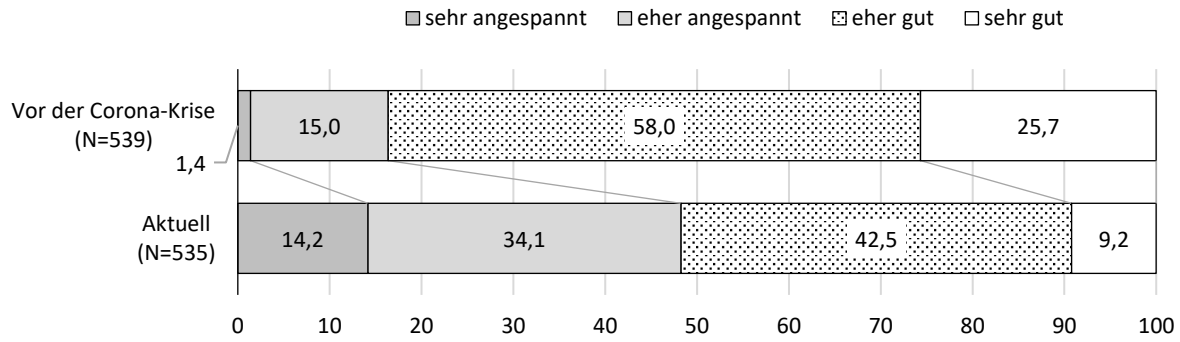
3.5.1 Einschätzung der wirtschaftlichen Situation des Unternehmens

Die wirtschaftliche Situation der Unternehmen war vor Beginn der Corona-Krise im ersten Quartal des Jahres 2020 noch überwiegend sehr/eher gut. Lediglich 1,4 % berichteten von einer sehr angespannten und weitere 15,0 % von einer eher angespannten Situation. Bezogen auf die Zeit der krisenbedingten Maßnahmen zur Pandemiebekämpfung änderte sich diese Einschätzung sehr deutlich (Abbildung 19). Zur Befragungszeit im Sommer 2020 befanden sich viele Unternehmen in einer wirtschaftlich sehr oder eher angespannten Situation (14,2 % bzw.

[57] Da die Position der Befragten ebenfalls mit der Beschäftigtengrößenklasse in Zusammenhang steht, sich also z.B. der Anteil der Befragten der Geschäftsführung mit zunehmender Unternehmensgröße verkleinert, und die Fallzahl für eine entsprechende Kontrolle zu klein ist, bleibt unklar, welches Merkmal für die Erklärung der Unterschiede bezüglich der Verbesserungshürden entscheidender ist.

34,1 %), wobei keine statistisch relevanten Unterschiede hinsichtlich der Beschäftigtengrößenklasse erkennbar sind.[58]

Abbildung 19 **Einschätzung der wirtschaftlichen Situation des Unternehmens**
in Prozent; gewichtete Daten



3.5.2 Veränderungen der IT-Struktur seit der Corona-Krise

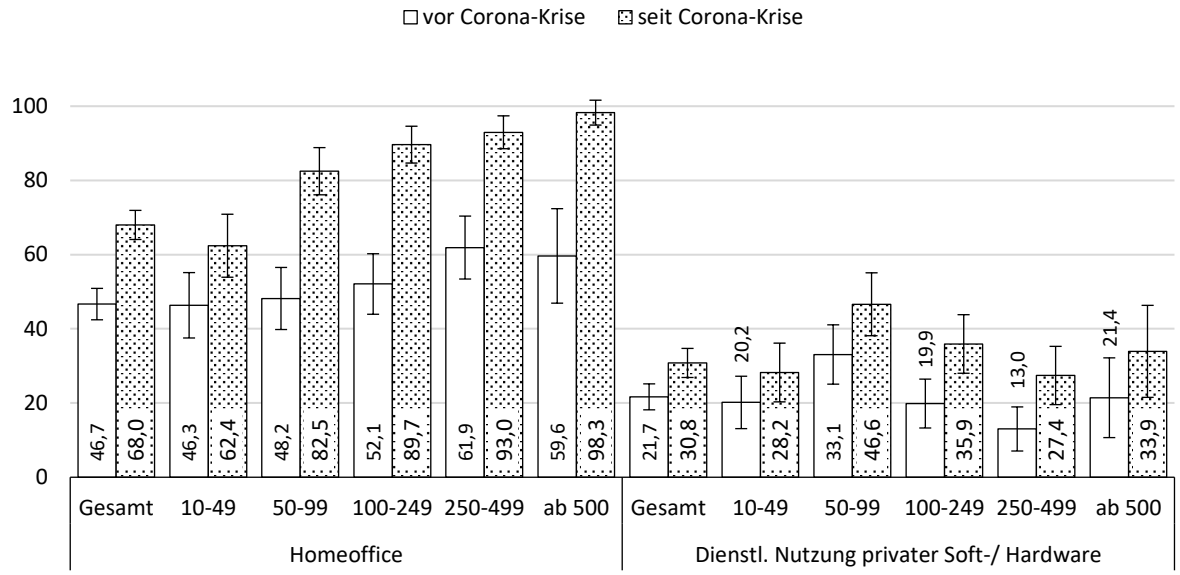
Vor der Corona-Krise gab es in knapp der Hälfte der Unternehmen (46,7 %; N=534) die Möglichkeit zu Homeoffice und in etwa jedem fünften Unternehmen (21,7 %; N=533) wurde private Soft-/Hardware zu dienstlichen Zwecken genutzt (Abbildung 20). Diese Anteile stiegen seit der Corona-Krise signifikant auf 68,0 % bzw. 30,8 %.

In Hinblick auf die Möglichkeit von Homeoffice vor der Corona-Krise sind lediglich tendenzielle Unterschiede zwischen den Beschäftigtengrößenklassen zu erkennen, die allerdings mit der Corona-Krise deutlicher geworden sind. Zwar erhöhten sich die Anteile in allen Beschäftigtengrößenklassen signifikant, aber während z.B. in knapp zwei Drittel der kleinen Unternehmen (10-49 Besch.: 62,4 %) Homeoffice praktiziert wird, ist dies in fast allen großen Unternehmen der Fall (ab 500 Besch.: 98,3 %).[59]

[58] Der Anteil der Unternehmen, deren wirtschaftliche Situation bereits vor der Corona-Krise sehr/eher angespannt war, liegt zwischen 13,5 % (250-499 Besch.) und 21,4 % (ab 500 Besch.) und bezogen auf die Zeit seit der Corona-Krise zwischen 40,9 % (250-499 Besch.) und 50,0 % (ab 500 Besch.). Siehe dazu auch Bitkom e.V. (2021).

[59] Gemäß Pawlowska & Scherer (2021: 5) stiegt der Anteil der Beschäftigten im Homeoffice in den Unternehmen infolge der Corona-Krise von 25 % auf 64 %.

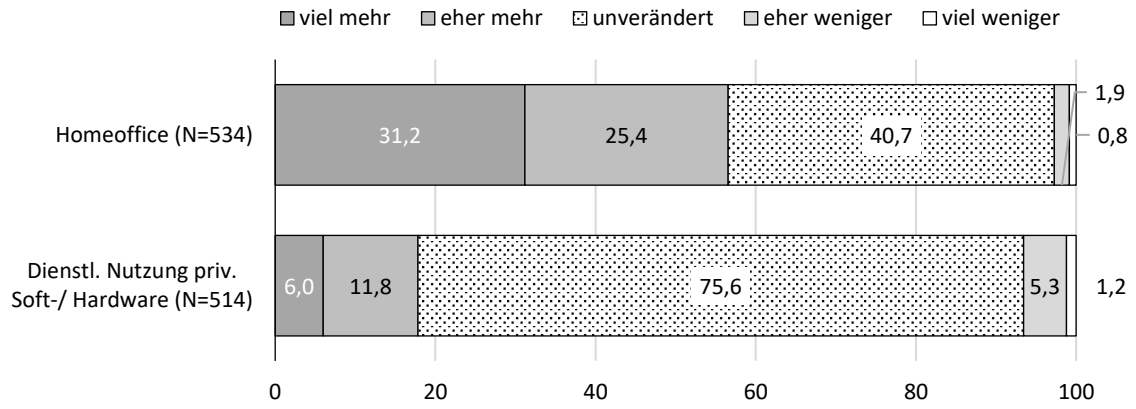
Abbildung 20 **Möglichkeit zu Homeoffice bzw. dienstl. Nutzung priv. Soft-/ Hardware vor und seit der Corona-Krise**
in Prozent; gewichtete Daten; 95%-KI



Bezogen auf die dienstliche Nutzung privater Soft- und Hardware vor und seit der Corona-Krise ist ebenfalls in allen Beschäftigtengrößenklassen ein Anstieg zu erkennen, der aber nur bei Unternehmen mit 100 bis 249 und 250 bis 499 Beschäftigten statistisch signifikant ist (19,9 % vs. 35,9 % bzw. 13,0 % vs. 27,4 %).

Daneben konnten die Befragten auf einer fünfstufigen Skala angeben, wie stark sich die Arbeit im Homeoffice und die dienstl. Nutzung privater Soft-/Hardware seit der Corona-Krise verändert haben (Abbildung 21). Knapp ein Drittel (31,2 %) gibt an, dass viel mehr, und ein weiteres Viertel (25,4 %), dass eher mehr im Homeoffice gearbeitet wird. Demgegenüber nahm die dienstliche Nutzung von privater Soft-/Hardware in lediglich 6,0 % viel mehr zu, in 11,8 % (eher) zu und blieb bei einem Großteil unverändert (75,6 %).

Abbildung 21 **Veränderung von Homeoffice bzw. dienstl. Nutzung priv. Soft-/ Hardware seit der Corona-Krise**
in Prozent; gewichtete Daten

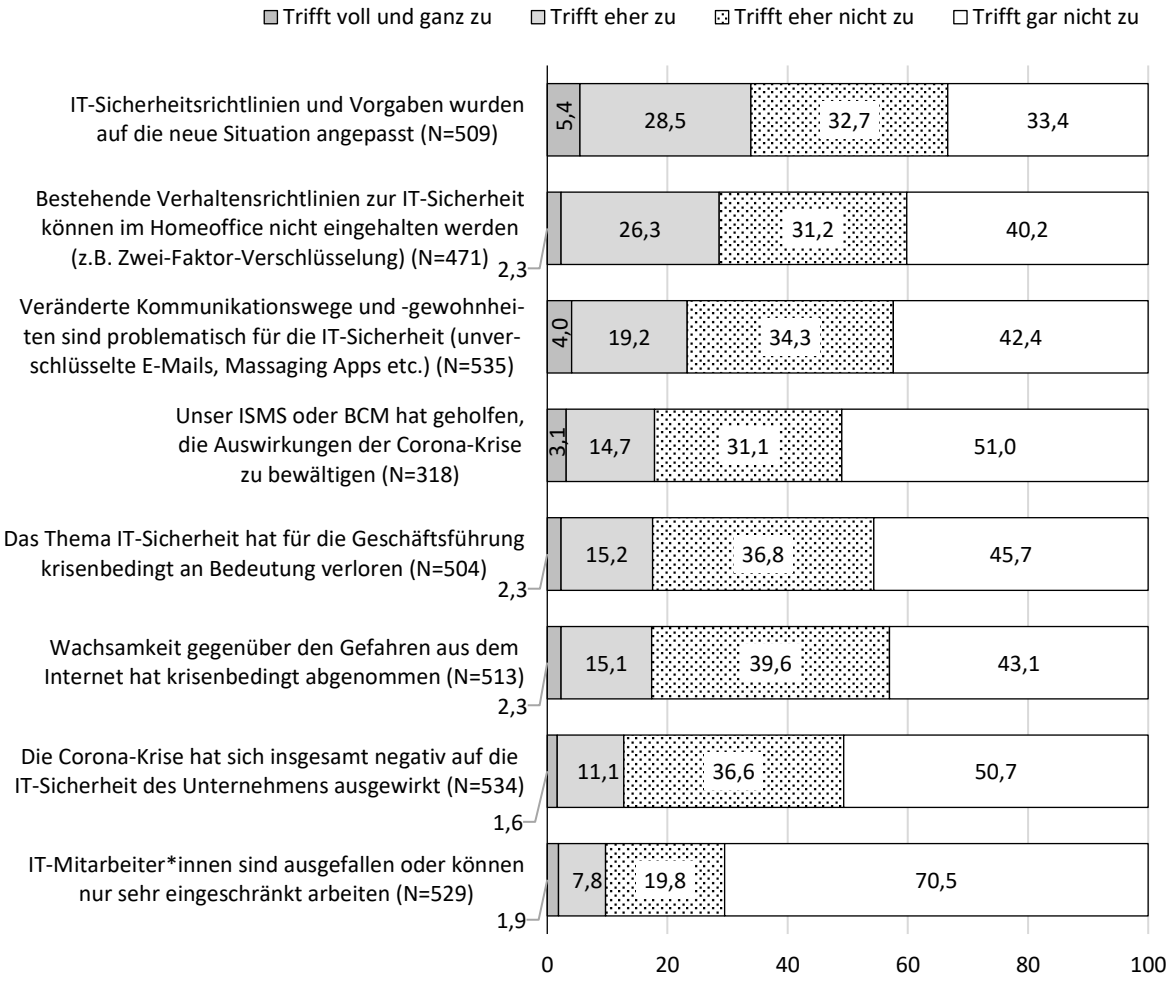


3.5.3 Einschätzungen zu den Auswirkungen auf die IT-Sicherheit

Um die Auswirkungen der Corona-Krise auf die IT-Sicherheit zu untersuchen, wurden die Befragten gebeten, eine Einschätzung zu acht Aussagen auf einer Skala von 1 „Trifft gar nicht zu“ bis 4 „Trifft voll und ganz zu“ zu treffen.

Der Aussage, dass IT-Sicherheitsrichtlinien und Vorgaben auf die neue Situation in der Corona-Krise angepasst wurden, stimmte etwa ein Drittel (33,9 %) eher/ voll und ganz zu, während bei zwei Drittel (eher) keine entsprechende Anpassung erfolgte (Abbildung 22). Über ein Viertel (28,6 %) gaben zudem an, dass bestehende Verhaltensrichtlinien im Homeoffice (eher) nicht eingehalten werden können und 23,3 %, dass krisenbedingt veränderte Kommunikationswege und Gewohnheiten (eher) problematisch für die IT-Sicherheit sind. Bei etwa jedem sechsten Unternehmen hat nach Einschätzung der befragten Unternehmensvertreter*innen das Thema IT-Sicherheit für die Geschäftsführung krisenbedingt (eher) an Bedeutung verloren (17,5 %) und die Wachsamkeit gegenüber den Gefahren aus dem Internet (eher) abgenommen. In etwa jedem achten Unternehmen hat sich die Corona-Krise insgesamt (eher) negativ auf die IT-Sicherheit ausgewirkt (12,7 %). Ein Anteil von 17,8 % stimmte der Aussage (eher) zu, dass ein Information Security Management System (ISMS) oder ein Business Continuity Management bei der Bewältigung der Corona-Krise hilfreich sei.[60]

Abbildung 22 **Einschätzungen zu den Auswirkungen der Corona-Krise auf die IT-Sicherheit**
in Prozent; gewichtete Daten

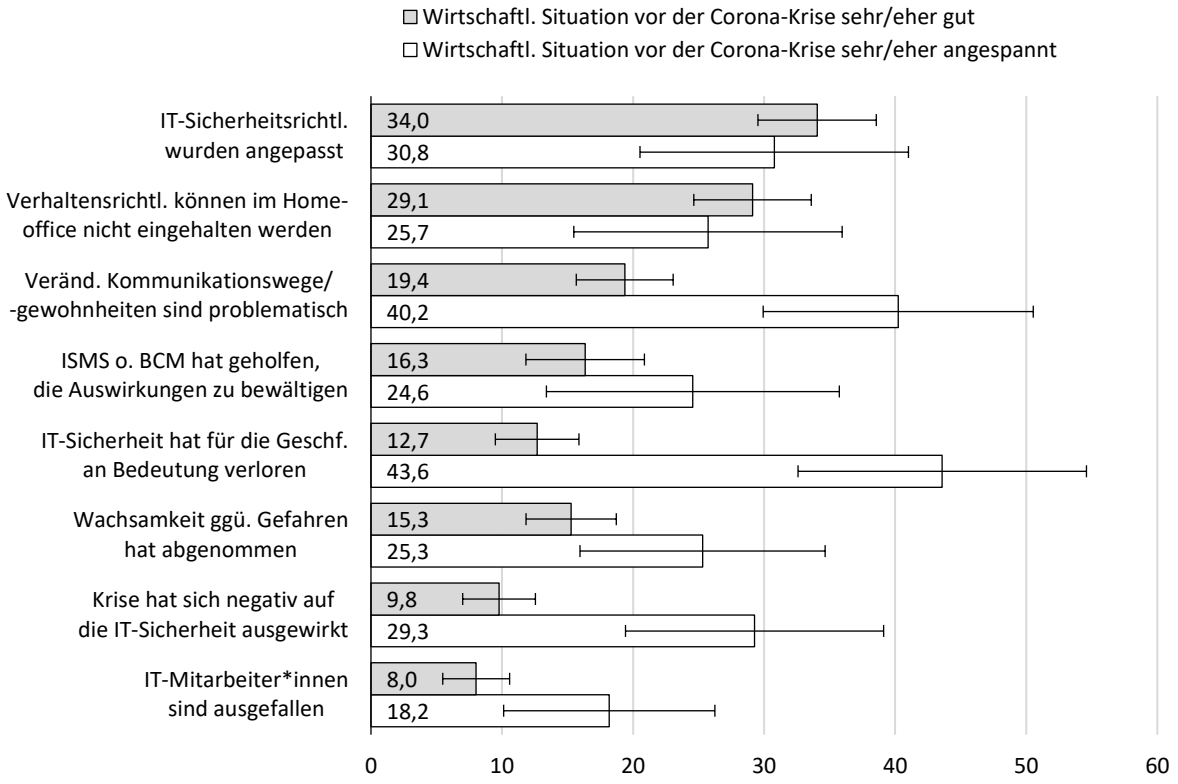


In Hinblick auf die Beschäftigtengrößenklasse sind bei diesen Einschätzungen mit einer Ausnahme keine signifikanten Unterschiede zu erkennen. Lediglich der (eher) zustimmende Anteil,

[60] Wenn nur die Angaben der Unternehmen einbezogen werden, die ein ISMS haben (N=52), liegt der (eher) zustimmende Anteil bei 51,1 %.

dass sich das ISMS oder BCM hilfreich bei der Krisenbewältigung zeigt, ist in größeren Unternehmen höher als in kleinen und variiert zwischen 13,7 % (10-49 Besch.; N=73) und 42,9 % (ab 500 Besch.; N=42).

Abbildung 23 **Einschätzungen zu den Folgen der Corona-Krise nach wirtschaftlicher Situation vor der Krise**
Angaben „Trifft eher/ voll u. ganz zu“ in Prozent; gewichtete Daten; 95%-KI

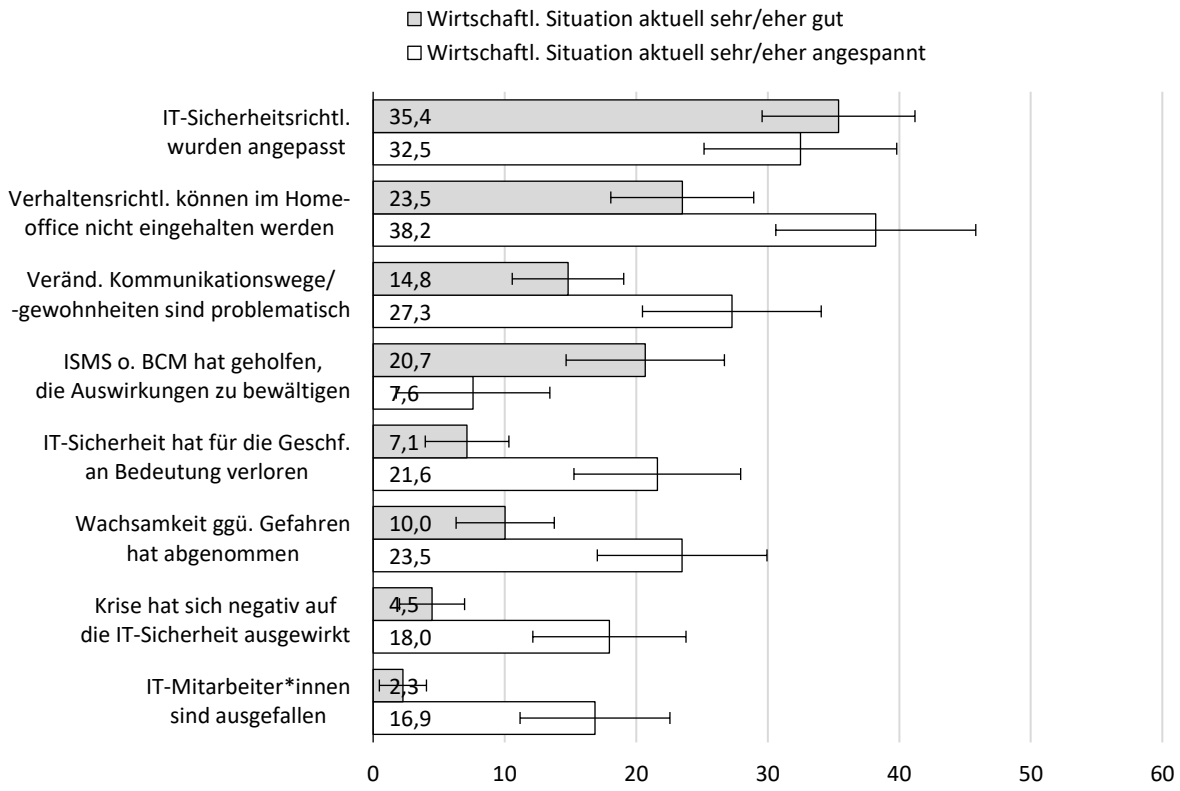


Um zu überprüfen, ob die wirtschaftlichen Situation der Unternehmen im Zusammenhang mit den Auswirkungen der Corona-Krise auf die IT-Sicherheit steht, werden im Folgenden zwei Gruppenvergleiche vorgenommen. Zuerst werden die Anteile der Angaben „Trifft eher/ voll und ganz zu“ zwischen Unternehmen mit sehr/ eher guter und Unternehmen mit sehr/ eher angespannter wirtschaftlicher Situation vor der Corona Krise verglichen.

Unternehmen, deren wirtschaftliche Situation bereits vor der Corona-Krise sehr/ eher angespannt war, gaben z.B. deutlich häufiger als wirtschaftlich (eher) gut situierte Unternehmen an, dass die krisenbedingt veränderten Kommunikationswege und -gewohnheiten problematisch für die IT-Sicherheit sind (40,2 % vs. 19,4 %), dass die IT-Sicherheit für die Geschäftsführung zusätzlich an Bedeutung verloren hat (43,6 % vs. 12,7 %) und dass sich die Corona-Krise insgesamt negativ auf die IT-Sicherheit im Unternehmen ausgewirkt hat (29,3 % vs. 9,8 %).

Beim zweiten Vergleich werden lediglich die Unternehmen einbezogen, deren wirtschaftliche Situation vor der Corona-Krise als sehr/ eher gut eingeschätzt wurde. Verglichen werden wiederum die Anteile der Angaben „Trifft eher/ voll und ganz zu“, nun allerdings zwischen den Unternehmen, deren wirtschaftliche Situation sich nach Einschätzung der Unternehmensvertreter*innen erst in der Corona-Krise verschlechtert hat und den Unternehmen, denen es wirtschaftlich nach wie vor gut geht.

Abbildung 24 **Einschätzungen zu den Folgen der Corona-Krise nach aktueller wirtschaftlicher Situation**
Angaben „Trifft eher/ voll u. ganz zu“ in Prozent; gewichtete Daten; 95%-KI;
nur Unternehmen mit sehr/ eher guter wirtschaftl. Situation vor der Corona-Krise;



Vertreter*innen aus Unternehmen mit krisenbedingt verschlechterter wirtschaftlicher Situation gaben signifikant häufiger an, dass Verhaltensrichtlinien und Vorgaben zur IT-Sicherheit im Homeoffice nicht eingehalten werden können (38,2 % vs. 23,5 %), veränderten Kommunikationswege und -gewohnheiten problematisch für die IT-Sicherheit sind (27,3 % vs. 14,8 %), die IT-Sicherheit für die Geschäftsführung an Bedeutung verloren hat (21,6 % vs. 7,1 %) und dass sich die Corona-Krise insgesamt negativ auf die IT-Sicherheit im Unternehmen ausgewirkt hat (18,0 % vs. 4,5 %). Daneben wurde auch deutlich häufiger eingeschätzt, dass die Wachsamkeit gegenüber den Gefahren aus dem Internet krisenbedingt abgenommen hat (23,5 % vs. 10,0 %) und dass IT-Mitarbeiter*innen ausgefallen sind bzw. seither nur sehr eingeschränkt arbeiten können (16,9 % vs. 2,3 %).

3.5.4 Zusätzliche IT-Sicherheitsmaßnahmen

Die Frage, ob zusätzliche IT-Sicherheitsmaßnahmen aufgrund der veränderten Situation in der Corona-Krise getroffen wurden, bejahte ein Anteil von 20,1 % (N=467) der Unternehmen, wobei keine statistisch relevanten Unterschiede hinsichtlich der Beschäftigtengrößenklasse erkennbar sind.[61] Allerdings gaben Unternehmen, deren wirtschaftliche Lage seit der Corona-Krise (eher) angespannt ist, mit 14,2 % (N=141) deutlich seltener an, zusätzliche IT-Sicherheitsmaßnahmen getroffen zu haben, als Unternehmen, deren wirtschaftliche Situation nach wie vor (eher) gut eingeschätzt wurde (22,6 %; N=243).

[61] Die Anteile variieren zwischen 19,8 % (50-99 Besch.) und 25,6 % (100-249 Besch.).

Für den Fall, dass zusätzliche Maßnahmen getroffen wurden, konnten die Befragten die drei wichtigsten über Freitextfelder angeben. Zu den häufigsten Nennungen gehörten:

- Einrichtung und Absicherung von (zusätzlichen) VPN-Zugangsmöglichkeiten
- Anschaffung und Absicherung von zusätzlicher Soft- und Hardware für die Arbeit im Homeoffice, insbesondere um die Risiken der Nutzung privater Soft- und Hardware zu minimieren
- Einrichtung von Zwei- oder Mehr-Faktor-Authentifizierung
- Awareness-Maßnahmen
- Schulungen zur IT-Sicherheit
- Vorgaben zur Nutzung von Videokonferenz-Tools
- Stärkung der Firewall und der Serversicherheit
- Anpassung der IT-Richtlinien
- verstärktes Monitoring

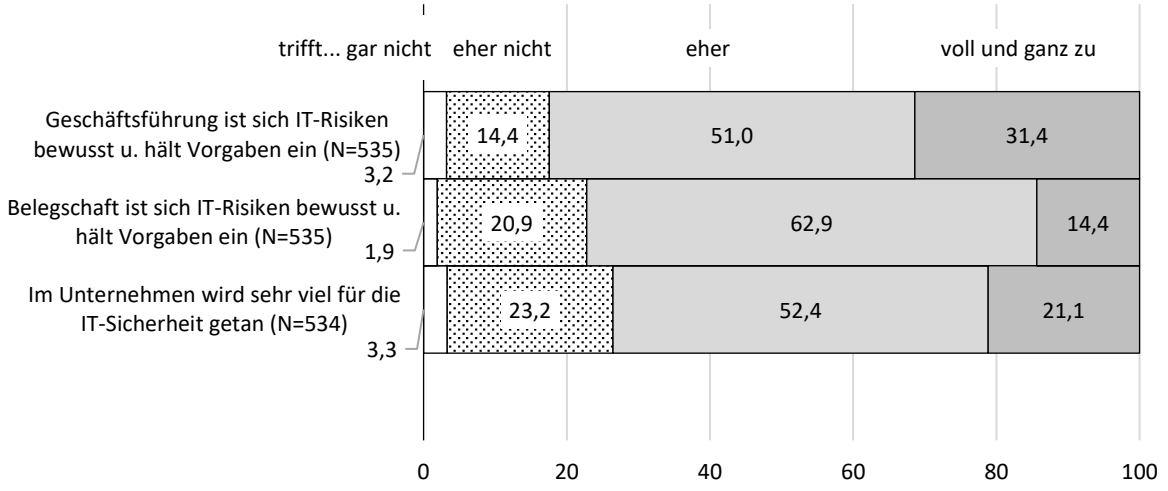
4 ENTWICKLUNG DER RISIKOEINSCHÄTZUNG

Eine basale Grundvoraussetzung für die Etablierung von Schutzmaßnahmen zur Prävention ist, dass Unternehmen um das Risiko von Cyberangriffen und die Möglichkeit der eigenen Betroffenheit wissen. Hierbei ist auch von Interesse, inwiefern ein Risikobewusstsein nicht ausschließlich bei den Beauftragten der IT-Sicherheit, sondern auch in weiteren Unternehmensbereichen verankert ist. Aus diesem Grund wurden die Befragten zum einen danach gefragt, wie sie das Bewusstsein bezüglich des Risikos innerhalb des Unternehmens einschätzen. Zum anderen wurden sie nach ihrer Einschätzung über das Risiko für das Unternehmen, einen Cyberangriff zu erfahren, gefragt.

4.1 Risikobewusstsein innerhalb des Unternehmens

Unverändert zu Befragung I konnten die erneut Teilnehmenden auf einer vierstufigen Skala von 1 „Trifft gar nicht zu“ bis 4 „Trifft voll und ganz zu“ ihre Einschätzung zu drei Aussagen zum Thema Risikobewusstsein im Unternehmen geben. Auch in Befragung II zeigt sich, dass ein Großteil der befragten Unternehmensvertreter*innen von einem eher hohen Risikobewusstsein in ihren Unternehmen ausgehen. Dennoch konnte ein Anteil von 17,6 % der Aussage, dass die Geschäftsführung sich der IT-Risiken bewusst ist und entsprechende Vorgaben einhält, gar nicht oder eher nicht zustimmen. Bezogen auf die Belegschaft ist dieser Anteil mit 22,8 % noch etwas größer und bezüglich der Aussage, dass im Unternehmen sehr viel für die IT-Sicherheit getan wir, stimmten über ein Viertel (26,5 %) gar nicht oder eher nicht zu (Abbildung 25).

Abbildung 25 **Einschätzung zum Risikobewusstsein im Unternehmen**
in Prozent; gewichtete Daten



Für die weitere Auswertung sowie für den Vergleich zu den Ergebnissen der Befragung I wurde aus diesen drei Einzelaspekten der Mittelwertindex „Risikobewusstsein im Unternehmen“ gebildet.[62]

In Tabelle 9 ist zu erkennen, dass sich die Anteile der Unternehmen mit (eher) geringem Risikobewusstsein nicht signifikant zwischen den Positionen der befragten Unternehmensvertreter*innen und den Beschäftigtengrößenklassen unterscheiden. Lediglich bei den Einzelaspekten lassen sich statistisch relevante Unterschiede erkennen. So hält über ein Drittel der Befragten aus dem Bereich der IT- und Informationssicherheit es für (eher) unzutreffend, dass im Unternehmen viel für die IT-Sicherheit getan wird, während dies nur 17,2 % der Befragten aus der Geschäftsführung bzw. dem Vorstand so sehen. Dies ist insofern erstaunlich, als dass die IT-Beschäftigten in der Befragung I diesbezüglich noch weniger kritisch waren als die Befragten der Geschäftsführung.

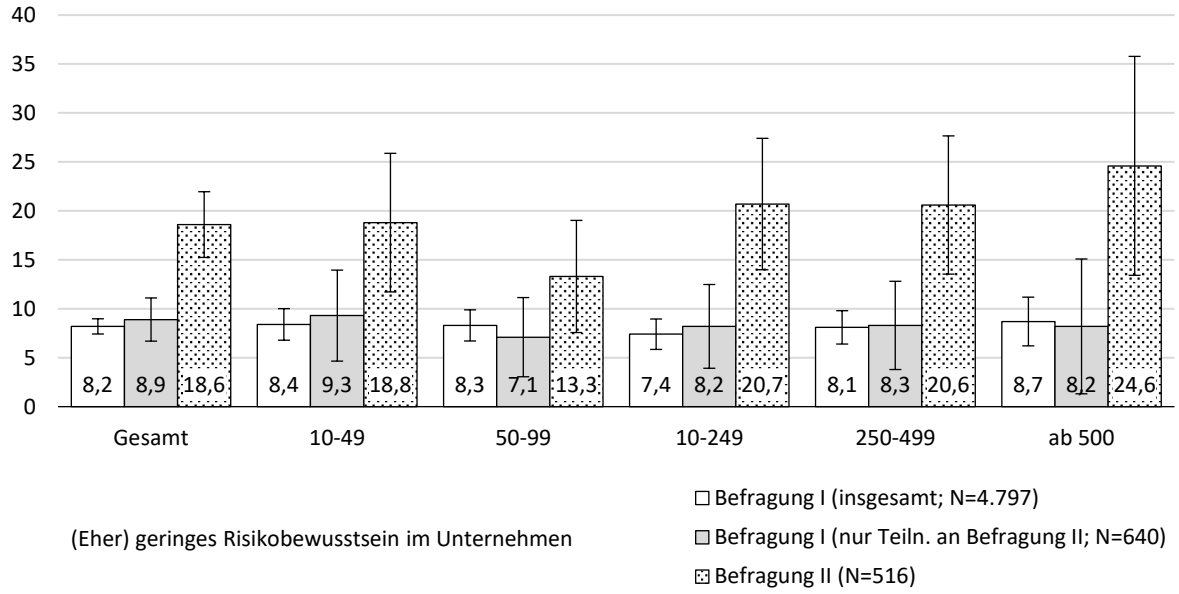
Tabelle 9 **Einschätzung zum Risikobewusstsein im Unternehmen**
in Prozent; gewichtete Daten; fett: Unterschiede signifikant bei p<.05 (Chi²-Test)

		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=516)	18,6	15,2	20,8	19,7	18,8	13,3	20,7	20,6	24,6
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=535)	17,6	**9,7**	**25,0**	16,1	17,9	15,4	18,1	22,2	22,4
Belegschaft ist sich der IT-Risiken bewusst und hält Vorgaben ein (N=535)	22,8	22,4	21,7	29,0	22,8	**16,9**	25,0	24,2	**40,7**
Im Unternehmen wird viel für IT-Sicherheit getan (N=534)	26,5	**17,2**	**34,6**	23,4	26,8	23,9	27,3	23,4	20,3

Im Vergleich zu den Ergebnissen der Befragung I ist insgesamt ein deutlich angewachsener Anteil an (eher) kritischen Einschätzungen zum Risikobewusstsein im Unternehmen von 8,2 % auf 18,6 % zu erkennen (Abbildung 26), der auch unter Kontrolle der Teilnahme an Befragung II bestehen bleibt (8,9 % vs. 18,6 %). Es scheint also nicht so zu sein, dass vor allem kritische Unternehmensvertreter*innen erneut an der Befragung teilgenommen haben. Diese Zunahme zeigt sich zudem in allen Beschäftigtengrößenklassen, auch wenn der Unterschied nicht überall signifikant ist, was vor allem auf die geringe Fallzahl zurückzuführen sein dürfte.

[62] 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). Cronbachs Alpha liegt in diesem Fall bei 0,73 und deutet auf eine relativ gute Konsistenz hin. Die Maßzahl Cronbachs Alpha beziffert das Ausmaß der Beziehung der enthaltenen Einzelaspekte (Items), kann Werte zwischen minus unendlich und 1 annehmen und dient der Einschätzung der internen Konsistenz des Indexes.

Abbildung 26 **(Eher) geringes Risikobewusstsein im Unternehmen nach Befragung**
Mittelwertindex; in Prozent; gewichtete Daten; 95%-KI

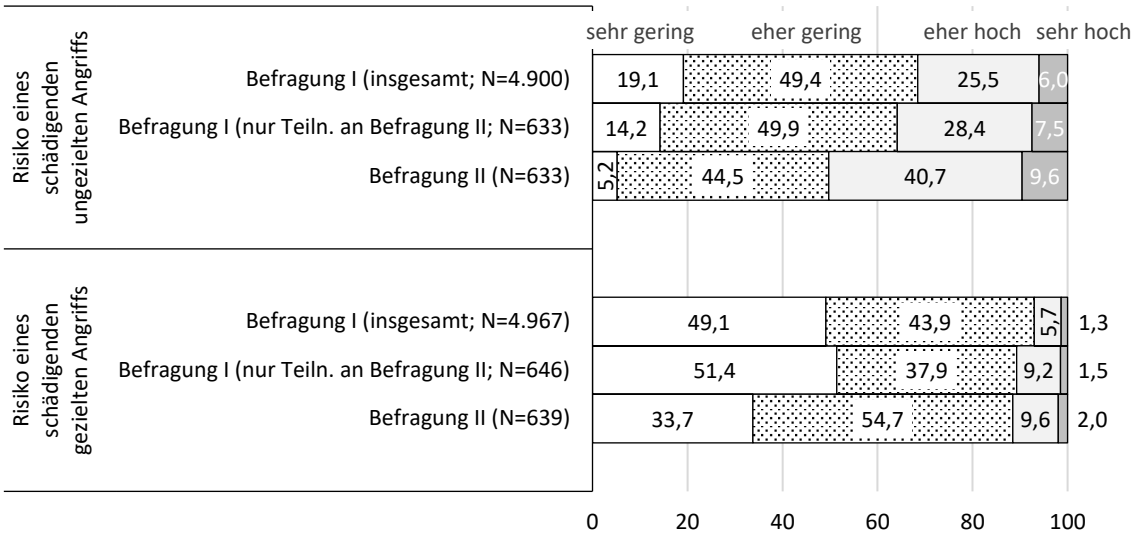


Eine mögliche Erklärung für diese kritischere Einschätzung des Risikobewusstseins im Unternehmen könnte die veränderte Situation in der Corona-Krise sein, auf die an vorheriger Stelle schon eingegangen wurde (Abschnitt 3.5).

4.2 Einschätzung des Unternehmensrisikos

Neben dem Risikobewusstsein im Unternehmen konnte auf einer vierstufigen Skala von 1 „sehr gering“ bis 4 „sehr hoch“ das Unternehmensrisiko bezüglich ungezielter und gezielter Cyberangriffe in den nächsten zwölf Monaten eingeschätzt werden. Auch hier lassen sich deutliche Veränderungen zu den Ergebnissen der Befragung I erkennen. So stieg der Anteil derjenigen, die das Risiko eines schädigenden ungezielten Angriffs für sehr/ eher hoch halten, von 31,5 % bzw. 35,9 % unter Kontrolle der erneuten Befragungsteilnahme auf 50,3 % (Abbildung 27). Hinsichtlich des Risikos schädigender gezielter Angriffe erhöhte sich dieser Anteil zwar kaum, dennoch fällt ein deutlich abnehmender Anteil derjenigen auf, die dieses Risiko für sehr gering halten. Dieser verkleinerte sich zugunsten der Kategorie „eher gering“ von 49,1 % bzw. 51,4 % auf 33,7 %.

Abbildung 27 **Risikoeinschätzung für eine Schädigung in den nächsten 12 Monaten durch (un)gezielte Cyberangriffe**
in Prozent; gewichtete Daten



In Tabelle 10 ist zudem zu erkennen, dass sowohl Befragte aus der Geschäftsführung als auch aus der IT und sonstigen Bereichen das Risiko schädigender ungezielter Cyberangriffe deutlich höher einschätzen als noch in Befragung I, wobei diese Veränderung bei IT-Beschäftigten vergleichsweise verhalten ausfiel: Bezogen auf ungezielte Angriffe schätzen IT-Beschäftigte in Befragung II das Risiko signifikant seltener sehr/ eher hoch ein als Befragte der Geschäftsführung und aus sonstigen Bereichen. Etwas anders verhält es sich bezüglich gezielter Cyberangriffe. Hier steigt der Anteil der Besorgten bei den IT-Beschäftigten von 8,5 % auf 13,3 %, während die Anteile bei den anderen Positionen etwas kleiner geworden sind, und liegt zudem deutlich über dem Anteil der Befragten aus der Geschäftsführung (7,6 %).

Tabelle 10 **Risikoeinschätzung für eine Schädigung des Unternehmens durch (un)gezielte Cyberangriffe**
in Prozent; gewichtete Daten; fett: Gruppenunterschiede 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 …	Befragung	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	I*	35,9	34,8	37,6	30,9	34,9	38,4	37,1	38,3	44,4
	II	50,3	**56,7**	**42,9**	**57,7**	50,0	51,0	50,6	53,5	70,5
… ausschließlich das eigene Unternehmen trifft	I*	10,7	10,6	8,5	23,2	11,8	7,8	11,3	8,5	11,1
	II	11,5	**7,6**	**13,3**	**22,4**	**12,0**	**5,7**	**15,7**	**14,8**	**27,4**

*) nur Teiln. an Befragung II

Im Vergleich der Beschäftigtengrößenklassen ist hinsichtlich gezielter Cyberangriffe zu erkennen, dass in großen Unternehmen (ab 500 Besch.) das Risiko häufiger sehr/ eher hoch eingeschätzt wird als in mittleren und kleinen Unternehmen. In Hinblick auf ungezielte Angriffe ist ein entsprechender Unterschied zumindest tendenziell zu erkennen.

5 ENTWICKLUNG DER CYBERANGRIFFE

Unabhängig von der Methode bestehen bei der Erhebung von Cyberangriffen in Unternehmen verschiedene Schwierigkeiten, die vor allem mit der Komplexität der IT-Struktur in Unternehmen, der Kombinierbarkeit und Vielfältigkeit von Cyberangriffsarten aber auch mit der Erhebung über eine*n Unternehmensvertreter*in zusammenhängen.[63]

Vor diesem Hintergrund wurden, ohne Anspruch auf eine vollständige Erfassung, die folgenden Angriffsarten unterschieden und sowohl in der Befragung I (CATI) als auch in der Befragung II (Web Survey) im Wortlaut unverändert erhoben:[64]

„Bezogen auf die letzten 12 Monate: Von welchen Angriffsarten war Ihr Unternehmen 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;
- Sonstiger Cyberangriff

Diese weniger technische und relativ breite Klassifikation unterscheidet sich von gängigen strafrechtlichen Einordnungen[65] und wurde aus zwei Gründen gewählt. Zum einen, um unabhängig von bestimmten Angriffsvektoren, Techniken und Tools sowie betroffenen Domänen bzw. Systemen oder Daten[66] zu sein, die sich im Zeitverlauf ändern können.[67] Zum anderen, um die Verständlichkeit und Akzeptanz bei den Befragten zu fördern und den eingeschränkten

---

63 Vgl. Dreißigacker et al. (2020a: 99).

64 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 regionalen Unternehmensstammtisch erstellt. Für eine ausführlichere Beschreibung siehe Dreißigacker et al. (2020a: 99ff.).

65 Dabei wird zwischen Cybercrime im engeren und im weiteren Sinne unterschieden und hinsichtlich verschiedener Tatbestandsmerkmale auf die Handlungen der Täter*innen fokussiert (vgl. z.B. Bundeskriminalamt 2015: 5-7), die für die Betroffenen nicht immer ersichtlich sind (z.B. die Verwendung wiederrechtlich erlangter Daten).

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

67 Ein ähnliches Vorgehen wählten auch Paoli et al. (2018).

Erklärungsmöglichkeiten bei einem Telefoninterview bzw. einem Web Survey gerecht zu werden.

5.1 Entwicklung der Prävalenzraten

5.1.1 Cyberangriffe insgesamt

Bezogen auf die letzten 12 Monate (2019/2020) gaben 59,6 % der befragten Unternehmen an, mindestens eine der erfragten Cyberangriffsarten erlebt bzw. auf diese reagiert zu haben (N=635). Im Vergleich mit dem Anteil von 41,1 % in Befragung I (2017/2018) ist dies eine statistisch relevante Steigerung von rund 19 Prozentpunkten (Abbildung 28). Und auch unter Kontrolle der Teilnahmebereitschaft, die bei betroffenen Unternehmen in Befragung I größer war als bei den nichtbetroffenen, ist zu Befragung I eine signifikante Steigerung von rund 9 Prozentpunkten zu erkennen (50,2 % vs. 59,6 %). Etwa ein Drittel (36,5 %; N=378) der betroffenen Unternehmen in Befragung II musste dabei auf eine der Angriffsarten reagieren und zwei Drittel auf mehrere (63,5 %).

Abbildung 28 **Jahresprävalenz Cyberangriffe insgesamt nach Befragung**
in Prozent; gewichtete Daten; 95%-KI

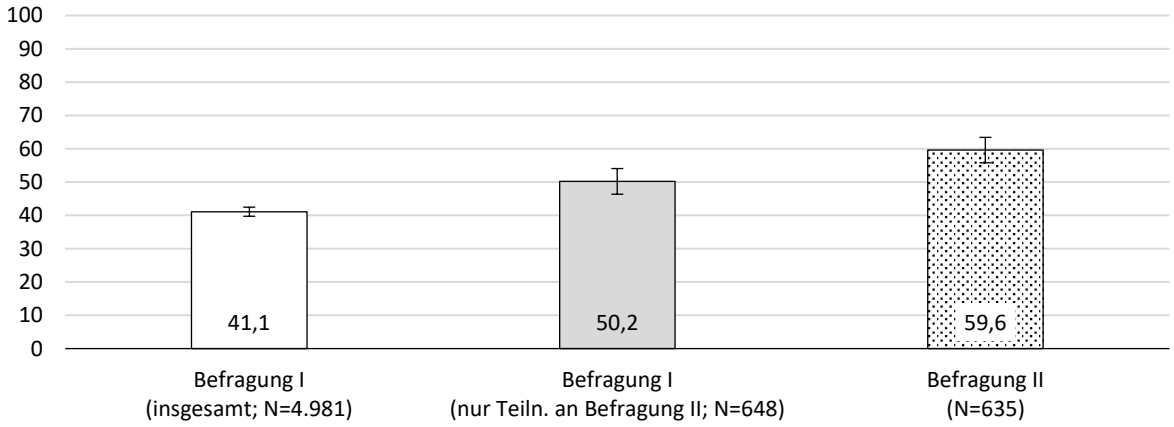
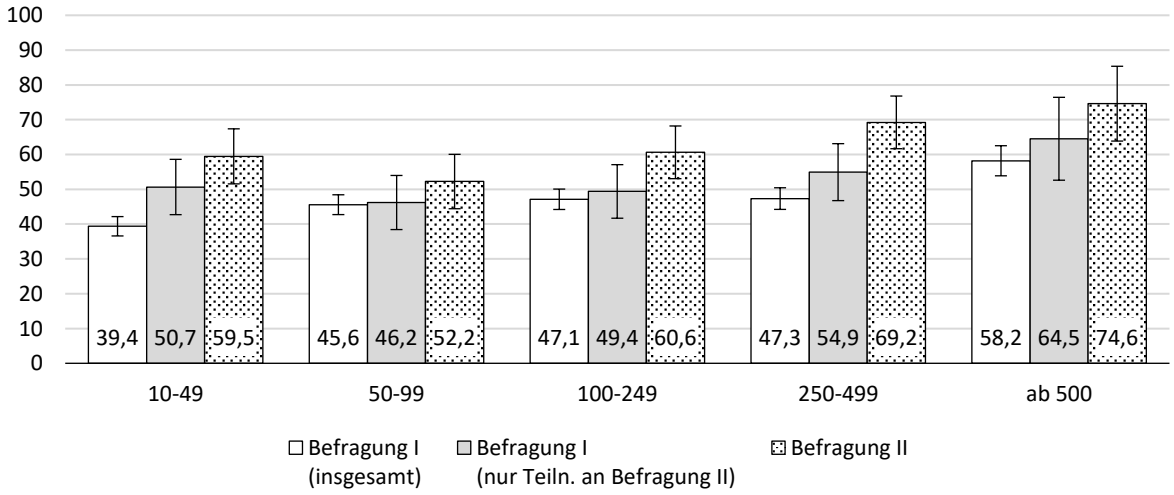
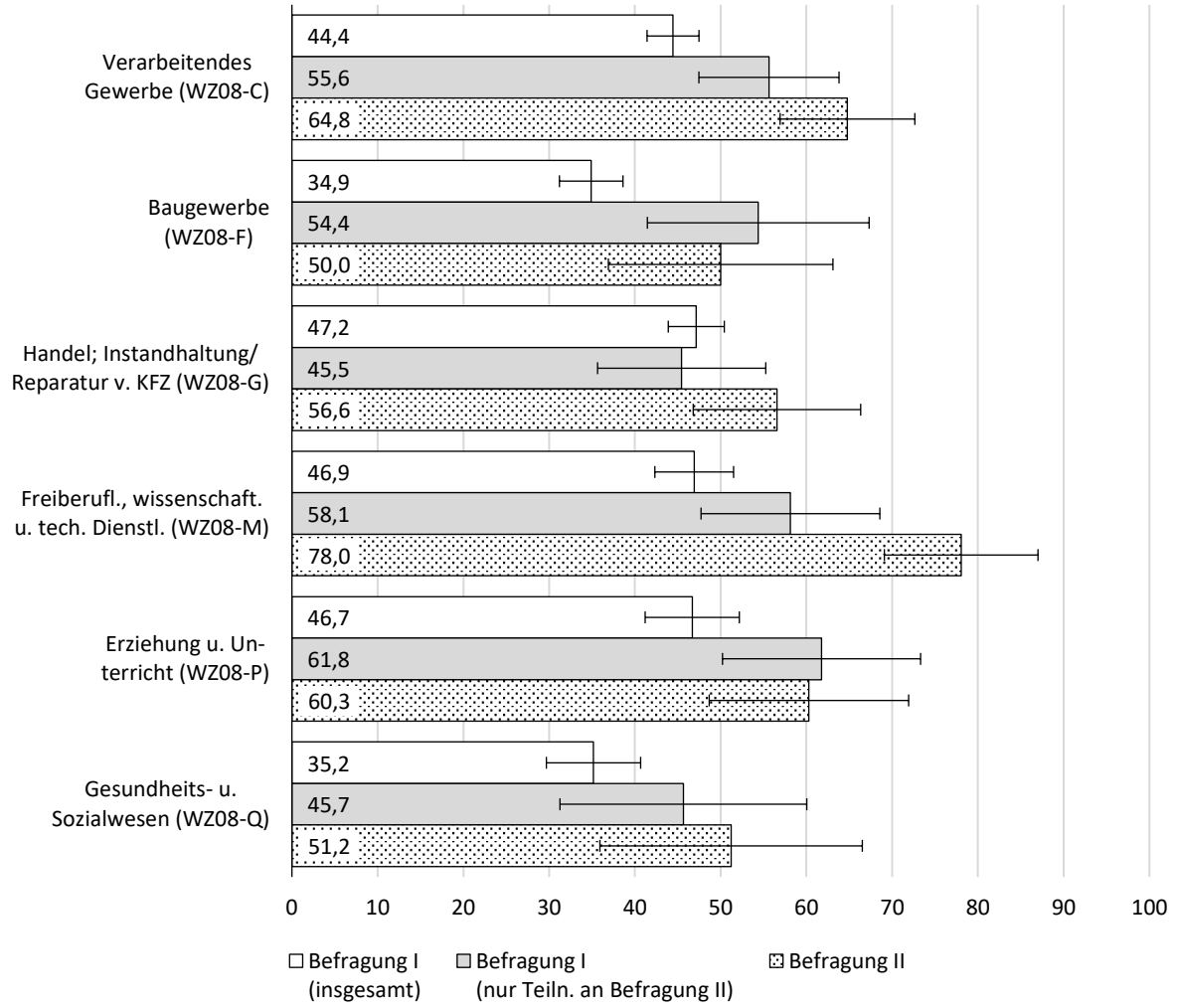


Abbildung 29 **Jahresprävalenz Cyberangriffe insgesamt nach Befragung und Beschäftigtengrößenklasse**
in Prozent; gewichtete Daten; 95%-KI



Dieser Anstieg der Jahresprävalenzraten zwischen beiden Befragungen zeigt sich zumindest tendenziell in allen Beschäftigtengrößenklassen (Abbildung 29). Am deutlichsten fällt der Unterschied bei den Unternehmen mit 250 bis 499 Beschäftigten aus (47,3 bzw. 54,9 % vs. 69,2 %). Gleichzeitig ist zu erkennen, dass tendenziell nach wie vor größere Unternehmen häufiger von Cyberangriffen betroffen sind als kleinere.

Abbildung 30 **Prävalenzraten für Cyberangriffe insgesamt nach Befragung und WZ08-Klassen (erste Ebene)**
in Prozent; gewichtete Daten; 95%-KI; nur, wenn N≥30

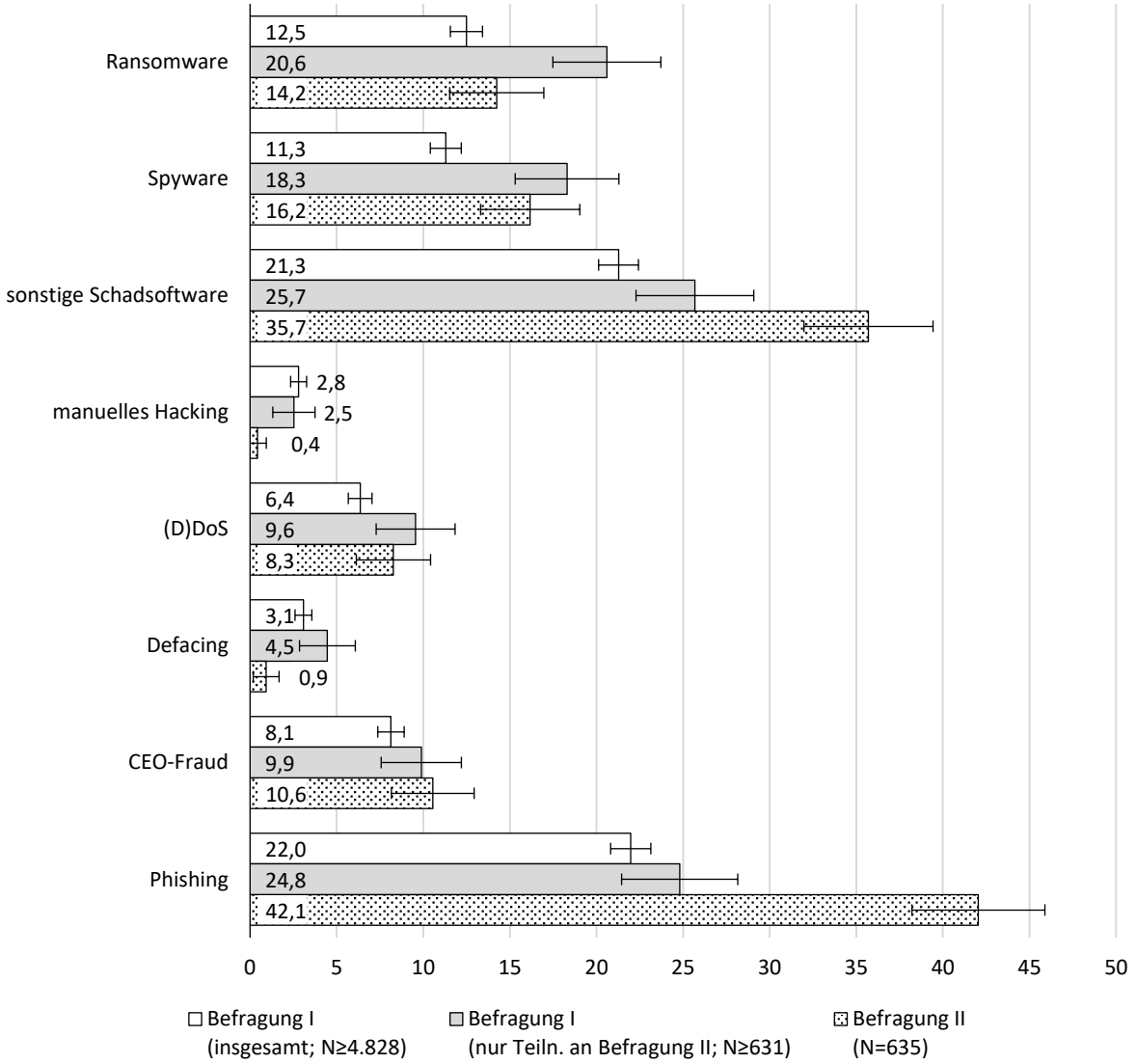


Da die in Befragung II zugrundeliegende Fallzahl wesentlich kleiner ist als in Befragung I, sind den Differenzierungsmöglichkeiten entsprechend begrenzter. So kann z.B. die Prävalenzrate nur für 6 von 19 Wirtschaftszweigklassen (WZ08 Ebene 1) sinnvoll berechnet und mit den Ergebnissen der Befragung I verglichen werden (Abbildung 30). Tendenziell sind auch hier gestiegene Prävalenzraten festzustellen, die sich unter Kontrolle der Teilnahme an Befragung II teilweise auflösen bzw. relativieren. Lediglich bei den Unternehmen der freiberuflichen, wissenschaftlichen und technischen Dienstleister (WZ08-M) ist eine statistisch signifikante Steigerung von 46,9 % bzw. 58,1 % auf 78,0 % Betroffenen zu erkennen.

5.1.2 Cyberangriffsarten

Differenziert nach Angriffsart[68] zeigen sich unterschiedliche Entwicklungen beim Vergleich der Ergebnisse aus den Befragungen I und II. Mit Blick auf Ransomware-Angriffe ist unter Kontrolle der Teilnahmebereitschaft von einer Abnahme der Betroffenheit auszugehen, d. h. bei Unternehmen die an beiden Befragungen teilnahmen sank der Anteil, der von Ransomware-Angriffen Betroffenen, von 20,6 % auf 14,2 % (Abbildung 31). Dies könnte mit der Corona-Krise in Zusammenhang stehen, insofern sich Täter*innen diesbezüglich mit Rücksicht auf Krankenhäuser für eine „Corona-Pause“[69] bezüglich aussprachen.[70] Auch die Anteile von Unternehmen, die auf manuelles Hacking oder Defacing reagieren mussten, sind von 2,5 % auf 0,4 % bzw. 4,5 % auf 0,9 % gesunken.

Abbildung 31 **Jahresprävalenz nach Angriffsart und Befragung**
in Prozent; gewichtete Daten; 95%-KI



[68] Wenn ein erlebter Cyberangriff aus einer Kombination verschiedener Angriffsarten bestand, sollten diese gesondert angegeben werden.

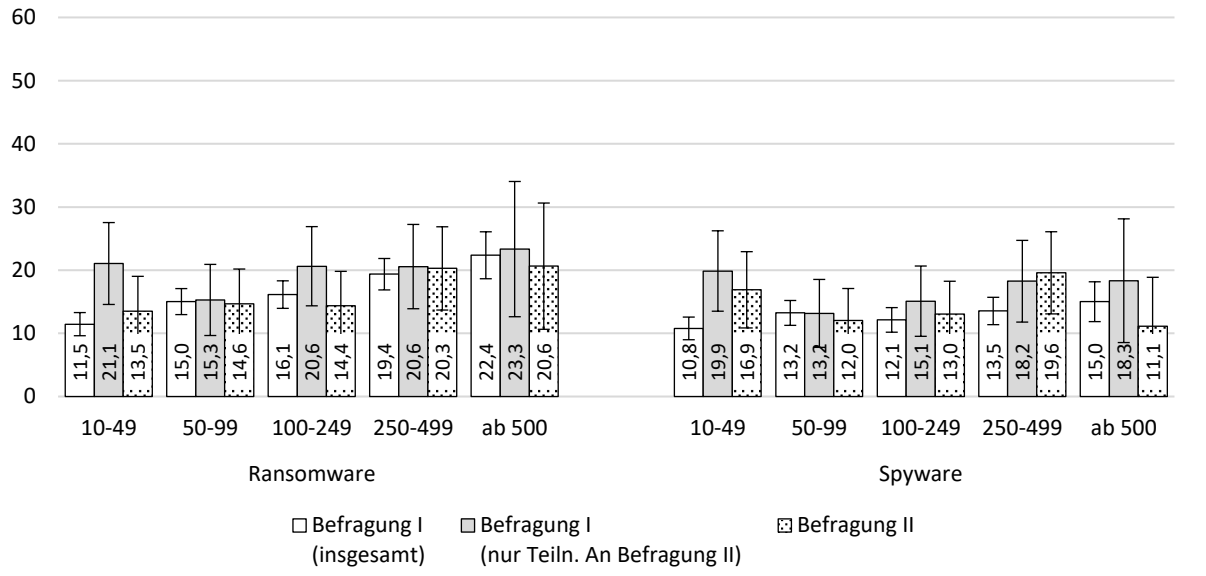
[69] Schmidt (2020).

[70] Vgl. Neubert et al. (2020: 355).

Keine signifikanten Veränderungen zur Befragung I sind in Hinblick auf Spyware-Angriffe, (D)DoS-Angriffe und CEO-Fraud festzustellen. Demgegenüber haben Angriffe mit sonstiger Schadsoftware und Phishing sehr deutlich zugenommen. Die Anteile der Unternehmen, die mit diesen Angriffsarten umzugehen hatten, stiegen von 25,7 % bzw. 24,8 % in Befragung I auf 35,7 % bzw. 42,1 % in Befragung II. Auch diese Entwicklung könnte mit den Veränderungen infolge der Corona-Krise, z.B. mit der Zunahme von Homeoffice Arbeit, im Zusammenhang stehen.[71]

Zusätzlich differenziert nach Beschäftigtengrößenklassen sind bei Ransomware-Angriffen lediglich bei den kleinen Unternehmen (10-49 Besch.) und mittleren Unternehmen (100-249) leichte Rückgänge festzustellen (Abbildung 32). Im Gesamtbild spricht dies dafür, dass die Belastung durch Ransomware insgesamt eher gleichgeblieben ist und allenfalls leicht abgenommen hat. Die in Befragung I festgestellte größere Belastung bei größeren Unternehmen ist tendenziell auch in Befragung II zu erkennen. Das Gesamtbild einer eher gleichgebliebenen Belastung durch Spyware bestätigt sich auch im Vergleich der Beschäftigtengrößenklassen. Der größte, aber statistisch nicht relevante, Unterschied zwischen den Befragungen I und II ist bei den großen Unternehmen (ab 500 Besch.) zu erkennen (18,3 % vs. 11,1 %).

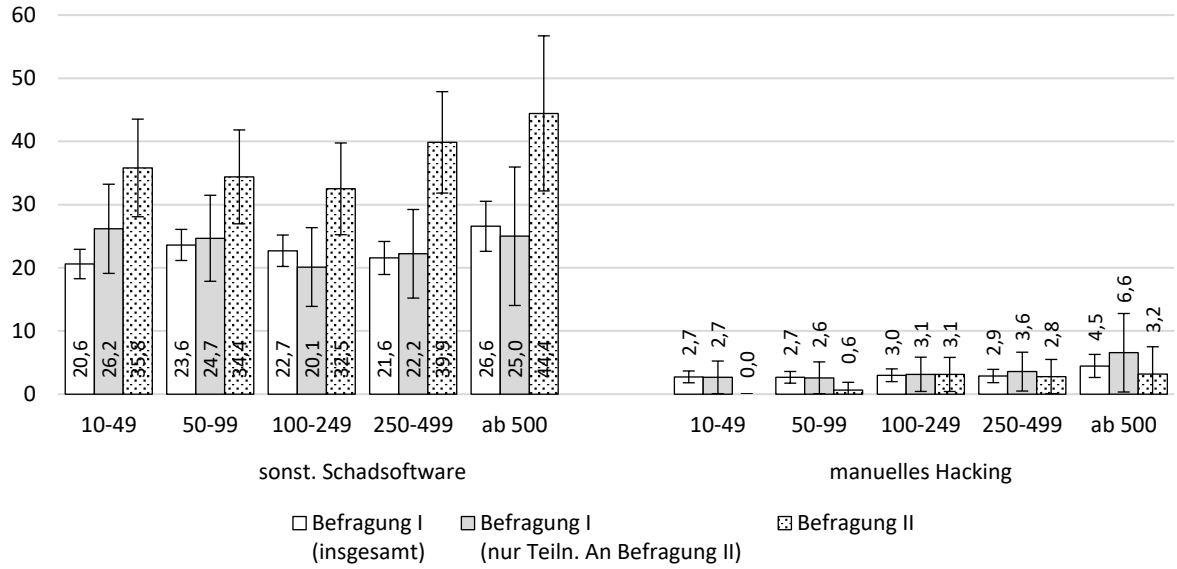
Abbildung 32 **Jahresprävalenz (Ransomware, Spyware) nach Beschäftigtengrößenklasse und Befragung**
in Prozent; gewichtete Daten; 95%-KI



Die zugenommene Belastung durch sonstige Schadsoftware (z.B. Viren, Würmer, Trojaner) ist auch in den einzelnen Beschäftigtengrößenklassen deutlich sichtbar (Abbildung 33) und stützt den Gesamteindruck. Demgegenüber ist hinsichtlich des manuellen Hackings eine eher gleichbleibend geringe Belastung in Unternehmen aller Größenklassen festzustellen. Der Rückgang in der Gesamtbetrachtung ist insbesondere auf kleine Unternehmen bis 99 Beschäftigte zurückzuführen, die in Befragung II nur noch sehr vereinzelt von solchen Angriffen berichteten.

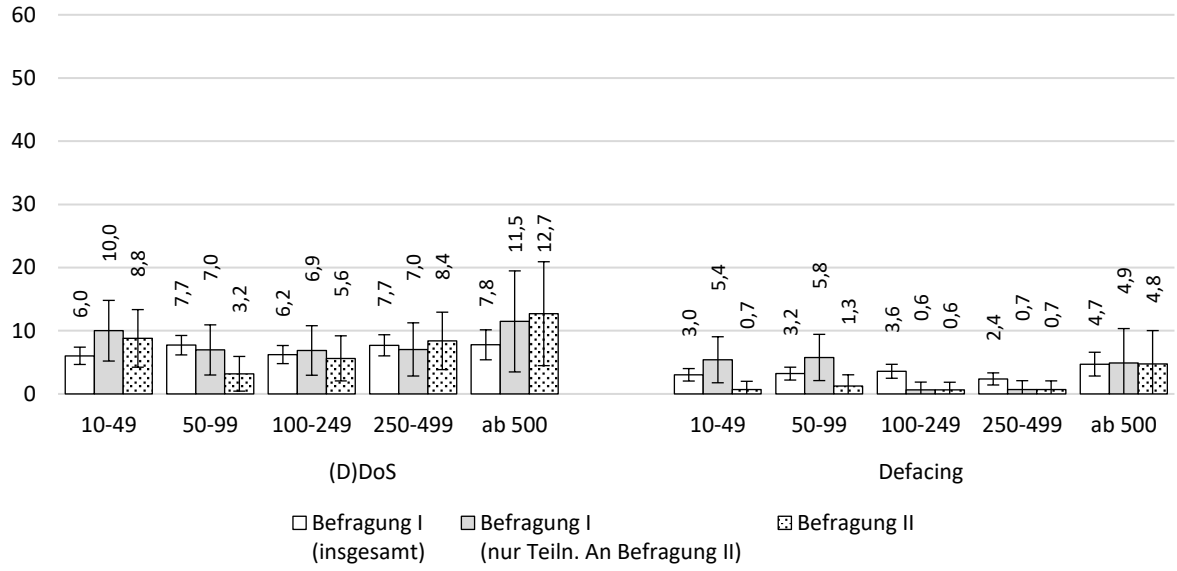
[71] Vgl. Neubert et al. (2020: 353f.) Zur Entwicklung der Cyberkriminalität in der Corona-Krise siehe z.B. Buil-Gil et al. (2020); Hawdon et al. (2020); Naidoo (2020); Minnaar (2020).

Abbildung 33 Jahresprävalenz (sonst. Schadsoftware, manuell. Hacking) nach Beschäftigtengrößenklasse und Befragung
in Prozent; gewichtete Daten; 95%-KI



Von einer gleichgebliebenen Belastung durch (D)Dos-Angriffen ist auch nach dem Vergleich der Beschäftigtengrößenklassen auszugehen (Abbildung 34), bei dem sich keine statistisch relevanten Veränderungen zeigen. Etwas anders stellt sich die Entwicklung bei Defacing-Angriffen dar. Während kleine und mittlere Unternehmen in Befragung II nur noch sehr vereinzelt von solchen Angriffen berichteten, blieb die Prävalenzrate bei großen Unternehmen (ab 500 Besch.) stabil bei rund 5 %. Auch wenn sich dies aufgrund der geringen Gruppengröße nicht mit statistischer Sicherheit sagen lässt, scheinen große Unternehmen vom Rückgang der Belastung durch Defacing ausgenommen zu sein.

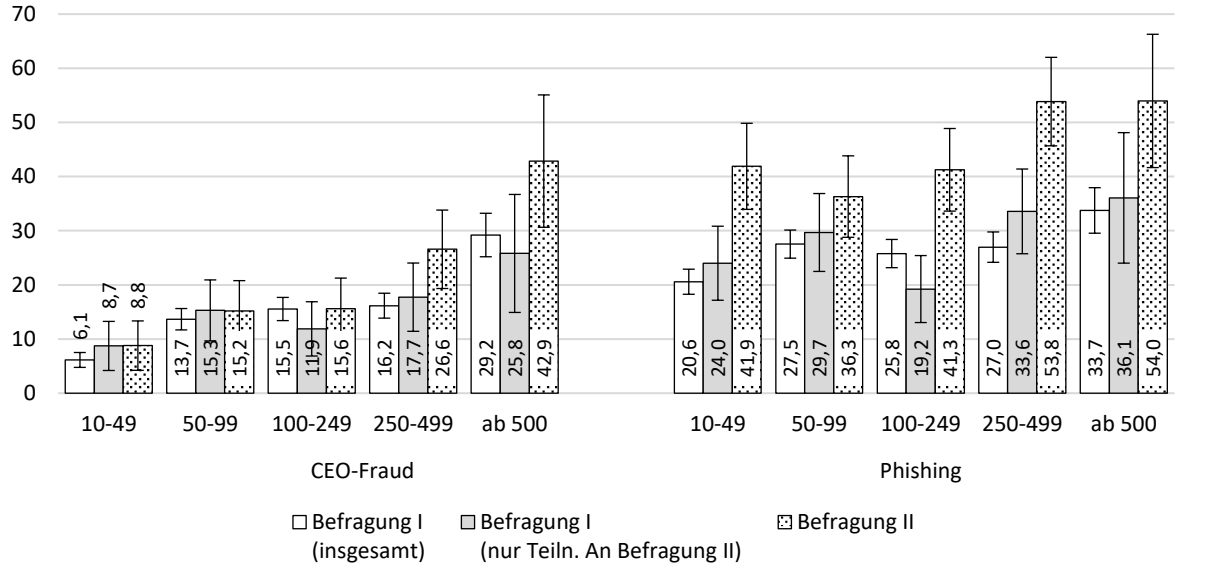
Abbildung 34 Jahresprävalenz ((D)DoS, Defacing) nach Beschäftigtengrößenklasse und Befragung
in Prozent; gewichtete Daten; 95%-KI



Ähnlich verhält es sich mit den Prävalenzraten von CEO-Fraud. Von einer insgesamt gleichbleibenden Belastung kann nur bei Unternehmen bis 249 Beschäftigten ausgegangen werden. Bei Unternehmen ab 250 Beschäftigten sind größere Anstiege zu erkennen, die darauf hindeu-

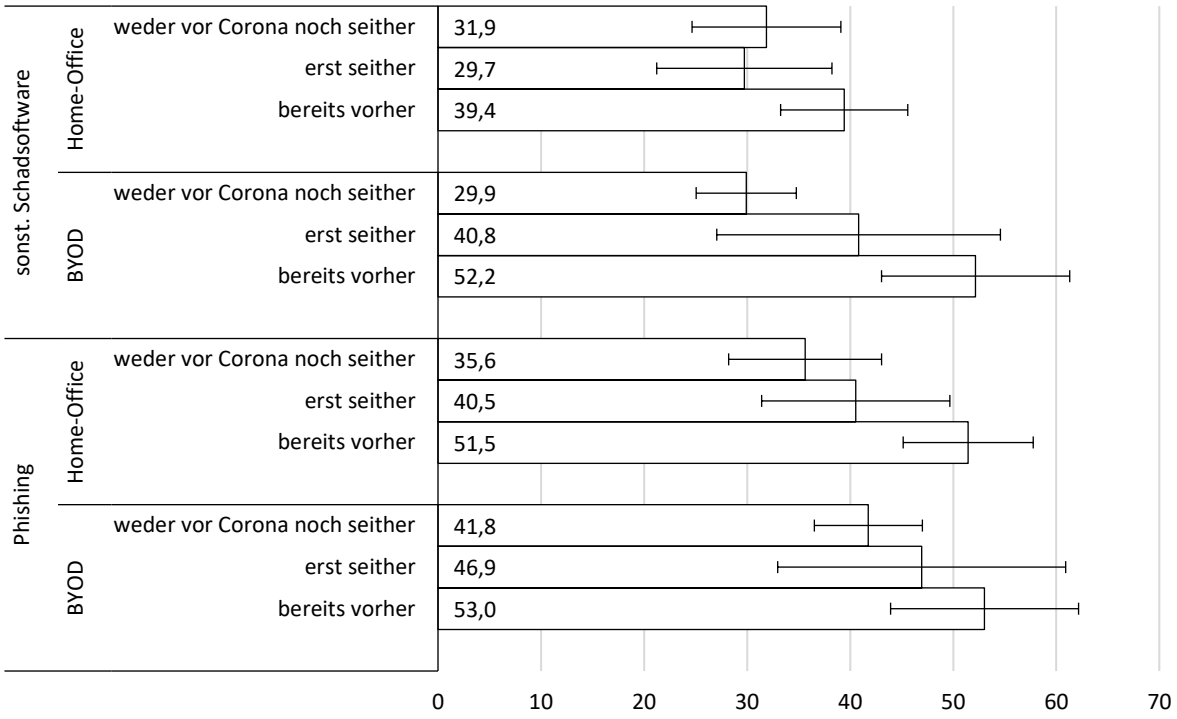
ten, dass in größeren Unternehmen die Belastung eher zugenommen hat, auch wenn diese Unterschiede aufgrund der geringen Gruppengröße statistisch nicht signifikant ausfallen (Abbildung 35). Während in Befragung I etwa ein Viertel der an beiden Befragungen teilnehmenden großen Unternehmen (ab 500 Besch.) von mindestens einem CEO-Fraud berichtete (25,8 %), sind es in Befragung II über zwei Fünftel (42,9 %). Damit verdeutlicht sich auch noch einmal der Befund der ersten Befragung, dass größere Unternehmen deutlich häufiger von dieser Angriffsart betroffen sind. Die Zunahme von Phishing-Angriffen ist wiederum in allen Größenklassen deutlich sichtbar und auch hier sind größere Unternehmen nach wie vor zumindest tendenziell stärker betroffen.

Abbildung 35 **Jahresprävalenz (CEO-Fraud, Phishing) nach Beschäftigtengrößenklasse und Befragung**
in Prozent; gewichtete Daten; 95%-KI



In Abbildung 36 wird der oben geäußerten Vermutung nachgegangen, dass die Anstiege von sonstigen Schadsoftware-Angriffen und Phishing im Zusammenhang mit der veränderten Situation seit der Corona-Krise stehen könnten. Dazu werden die Prävalenzraten derjenigen Unternehmen miteinander verglichen, bei denen weder vor noch seit der Corona-Krise Homeoffice bzw. die dienstliche Nutzung von privater Hard-/ Software (Bring Your Own Device – BYOD) möglich ist, bei denen dies erst seit der Corona-Krise möglich ist und bei denen dies bereits vorher gängige Praxis war. Zu erkennen ist, dass bei beiden Angriffsarten zumindest tendenziell die Unternehmen am stärksten betroffen sind, die bereits vor der Corona-Krise Homeoffice und BYOD ermöglichten. Gleichzeitig deutet sich aber auch wie vermutet an, dass Unternehmen, die dies erst seither ermöglichen, mit einer Ausnahme (Homeoffice bzgl. sonst. Schadsoftware), tendenziell stärker betroffen sind als Unternehmen, die dies weder vorher noch seither ermöglichen. Einschränkend ist allerdings zu erwähnen, dass hierbei die Beschäftigtengrößenklasse aufgrund der geringen Fallzahl nicht kontrolliert werden konnte und unklar bleibt, ob die berichteten Cyberangriffe vor oder nach Beginn der Corona-Krise stattgefunden haben.

Abbildung 36 **Jahresprävalenz (sonst. Schadsoftware, Phishing) nach Möglichkeiten zu Homeoffice und BYOD**
in Prozent; gewichtete Daten; 95%-KI



5.2 Entwicklung der Inzidenzraten

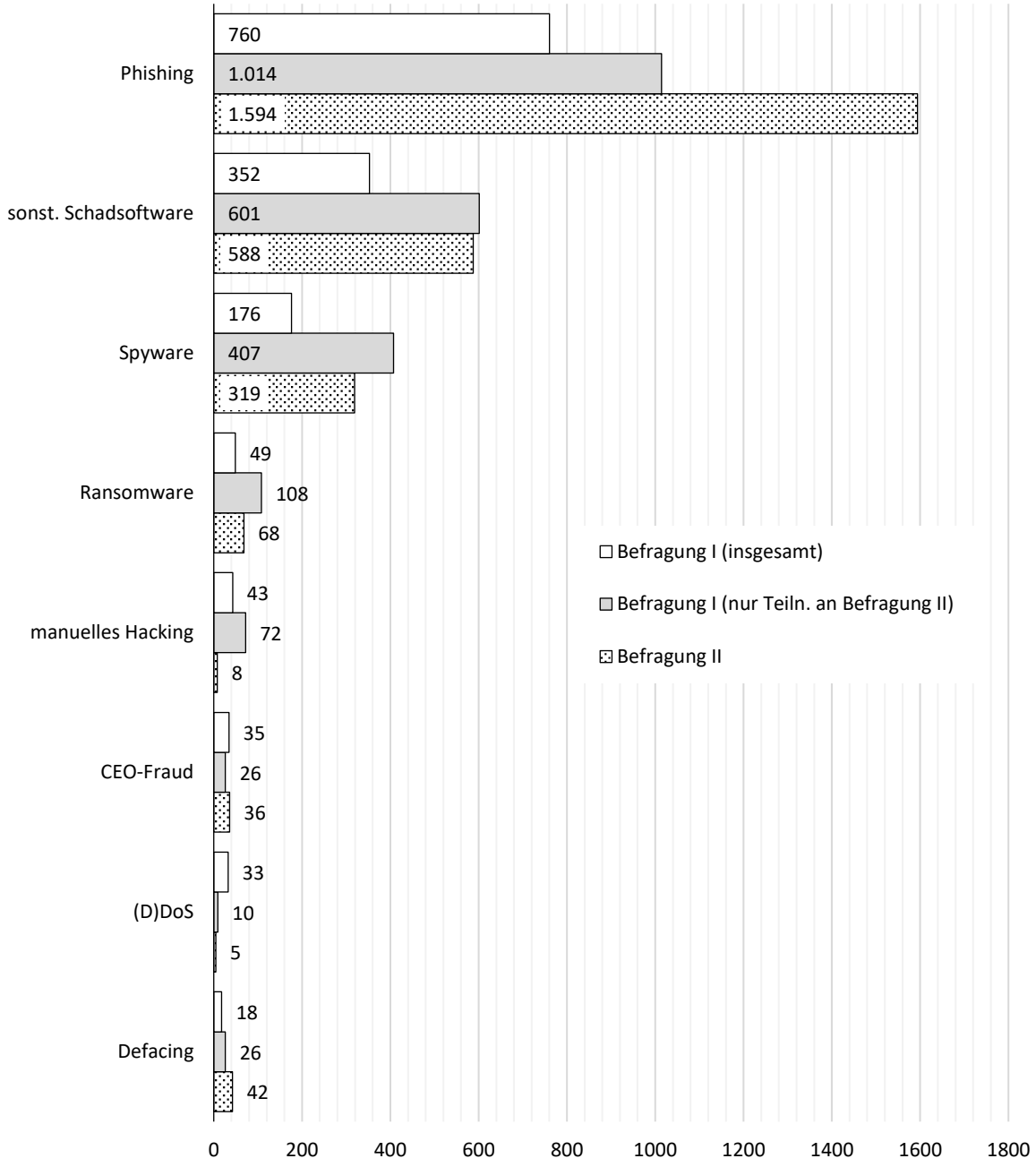
Neben der Anzahl der befragten Unternehmen, die in den vorangegangenen zwölf Monaten mindestens einmal von der jeweiligen Angriffsart betroffen waren (Prävalenz), wurde erneut die Anzahl der Cyberangriffe, auf die in diesem Zeitraum reagiert werden musste, erhoben (Inzidenz).[72] Die durchschnittliche Anzahl der Angriffe, von denen die Unternehmen für diesen Zeitraum berichteten (Inzidenzrate), wird in Abbildung 37 pro 100 Unternehmen und differenziert nach Cyberangriffsart angegeben. Phishing-Angriffe sind nach wie vor an oberster Stelle, gefolgt von sonstigen Schadsoftware-Angriffen. 100 Unternehmen mussten in den letzten zwölf Monaten demnach durchschnittlich auf rund 1.600 Phishing- und rund 590 sonstige Schadsoftware-Angriffe reagieren. Während die Inzidenzrate von Phishing bei den Unternehmen, die an beiden Befragungen teilgenommen haben, sehr deutlich angestiegen ist, blieb diese bei sonstiger Schadsoftware unverändert. In Zusammenschau mit den Prävalenzraten bedeutet dies, dass im Vergleich zur Befragung I deutlich mehr Unternehmen von diesen Angriffsarten betroffen sind und die von Phishing-Angriffen betroffene Unternehmen zudem auf deutlich mehr Phishing-Angriffe innerhalb von zwölf Monaten reagieren mussten als dies in Befragung I der Fall war. Bei von sonstiger Schadsoftware betroffenen Unternehmen blieb die Mehrfachbelastung durch diese Angriffsart hingegen auf einem ähnlichen Niveau. Bezüglich der anderen Angriffsarten zeigt sich eine Verschiebung, insofern die Inzidenzrate von manuellem Hacking und

[72] 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 berechnet wurde (bei Unternehmen ab 500 Besch.: Mittelwert addiert mit vier Standardabweichungen). 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.

(D)DoS-Angriffen kleiner geworden ist, d.h., derart betroffene Unternehmen mussten vergleichsweise weniger häufig auf solche Angriffe reagieren.

Abbildung 37 **Inzidenzraten nach Angriffsart und Befragung**

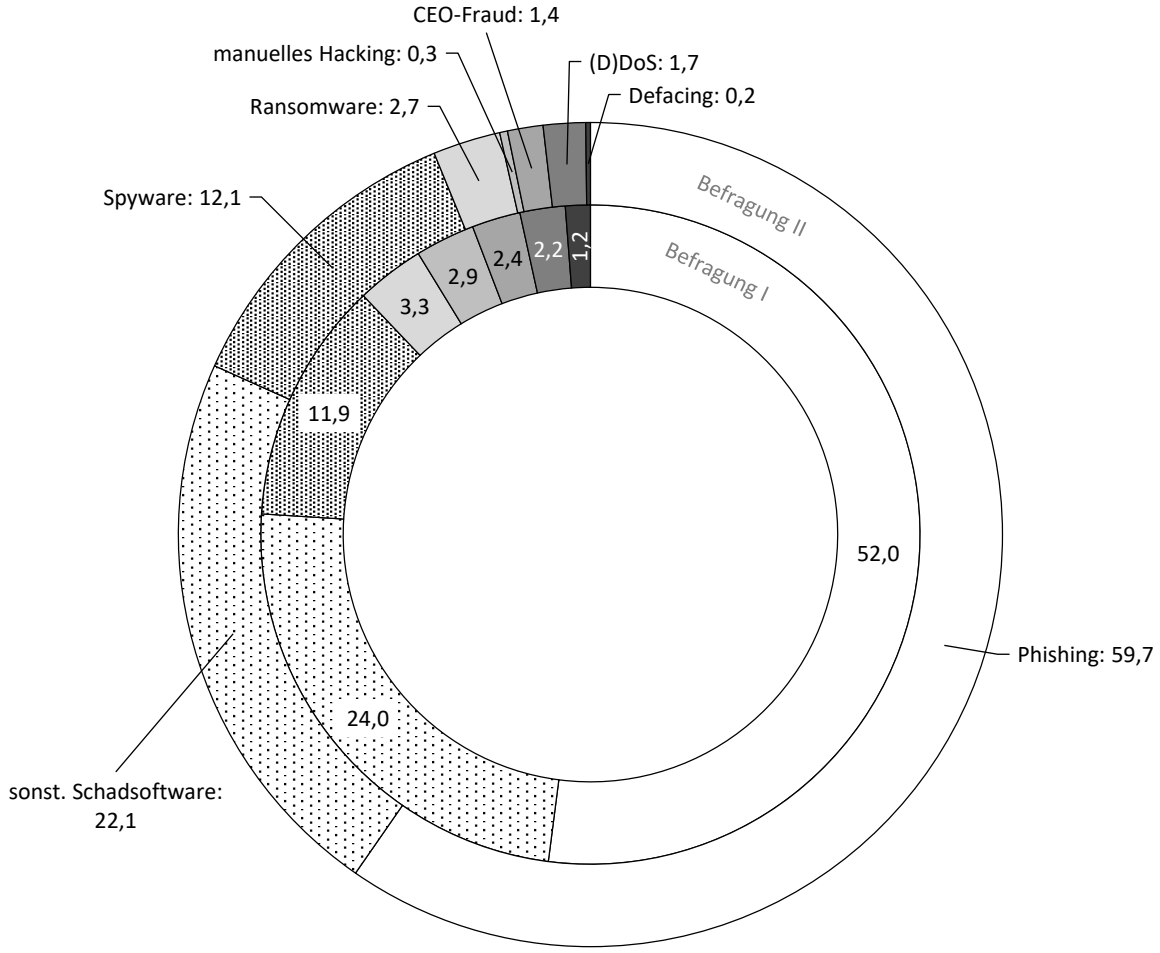
durchschnittliche Anzahl der Cyberangriffe in 12 Monaten je 100 Unternehmen; gewichtete Daten



Für die Darstellung in Abbildung 38 wurden die für jede Angriffsart berichteten Vorfälle summiert und ins Verhältnis zur Gesamtzahl aller berichteten Cyberangriffe gesetzt. Beim Vergleich der Anteile zwischen den Befragungen I und II wird noch einmal deutlich, dass nach wie vor über die Hälfte aller berichteten Cyberangriffe innerhalb eines Jahres zur Kategorie Phishing gehören, wobei der Anteil noch einmal von 52,0 % auf 59,7 % zugenommen hat.

Demgegenüber sind insbesondere die Anteile von Defacing, manuellem Hacking und CEO-Fraud an allen Cyberangriffen kleiner geworden.

Abbildung 38 **Anteile der Cyberangriffsarten an allen erlebten Angriffen nach Befragung**
in Prozent; gewichtete Daten



Beim Vergleich der Anteile der einzelnen Angriffsarten an der Gesamtanzahl der berichteten Cyberangriffe fällt erneut auf, dass sich im Unterschied zu den Prävalenzraten für keine Angriffsart ein linearer Trend ausmachen lässt (z.B. je größer die Unternehmen, desto größer der Anteil von Phishing-Angriffen). Lediglich der Anteil von Defacing ist bei großen Unternehmen (ab 500 Besch.) größer als bei allen anderen Beschäftigtengrößenklassen, bei denen diese Angriffsart anteilig kaum eine Rolle zu spielen scheint (Tabelle 11).

Tabelle 11 **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	61,9	66,2	58,0	50,2	64,5
sonst. Schadsoftware	19,4	19,5	29,1	35,4	15,9
Spyware	13,4	6,2	3,7	9,2	4,3
Ransomware	2,6	2,1	4,0	2,1	0,9
manuelles Hacking	0,0	0,0	2,8	0,1	0,1
CEO-Fraud	0,7	5,1	2,1	2,3	7,1
(D)DoS	2,0	0,8	0,2	0,7	2,5
Defacing	0,0	0,1	0,0	0,0	4,5
Gesamt	100,0	100,0	100,0	100,0	100,0

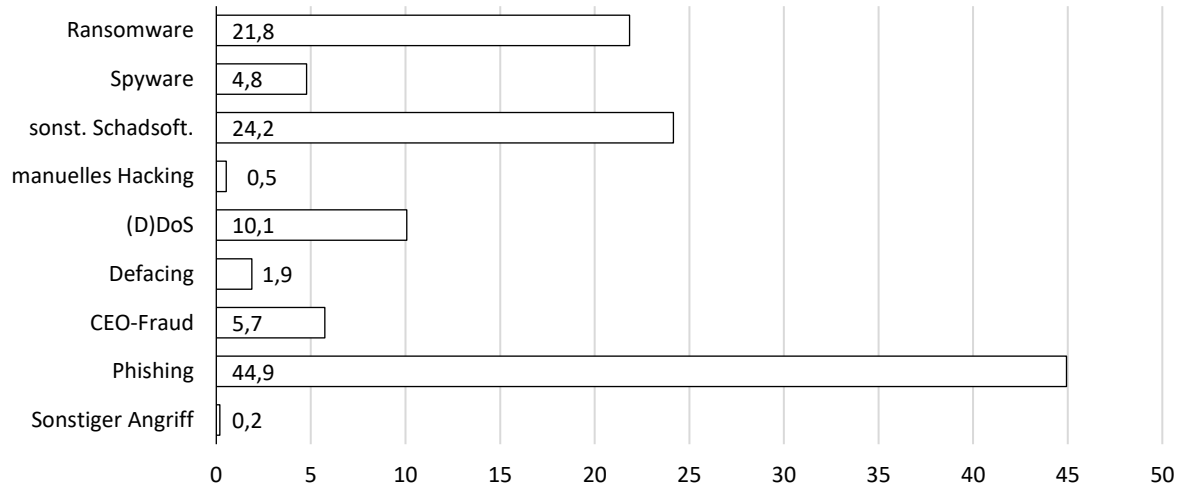
6 SCHWERWIEGENDSTER ANGRIFF

Wie in Befragung I wurden die in den letzten 12 Monaten von Cyberangriffen betroffenen Unternehmen gebeten, weitere Detailfragen zum schwerwiegendsten dieser Angriffe zu beantworten. Wie schwerwiegend diese Angriffe waren, spielt bei dieser Bestimmung durch die Befragten vorerst keine Rolle, kann jedoch zu in einem späteren Auswertungsschritt z.B. anhand der berichteten Schäden eingeschätzt werden. Wurde nur ein Angriff erlebt, gilt dieser als schwerwiegendster.

6.1 Angriffsart

Danach gefragt, zu welcher Angriffsart der in den letzten 12 Monaten erlebte schwerwiegendste Cyberangriff gehört, gaben 44,9 % Phishing, 24,2 % sonstige Schadsoftware, 21,8 % Ransomware und 10,1 % (D)DoS an (Abbildung 39). Seltener wurde CEO-Fraud (5,7 %), Spyware (4,8 %), Defacing (1,9 %) und manuelles Hacking (0,5 %) im Zusammenhang mit dem schwerwiegendsten Angriff genannt.

Abbildung 39 **Schwerwiegendster Cyberangriff nach Angriffsart**
in Prozent; gewichtete Daten; Mehrfachantwort möglich; N=298



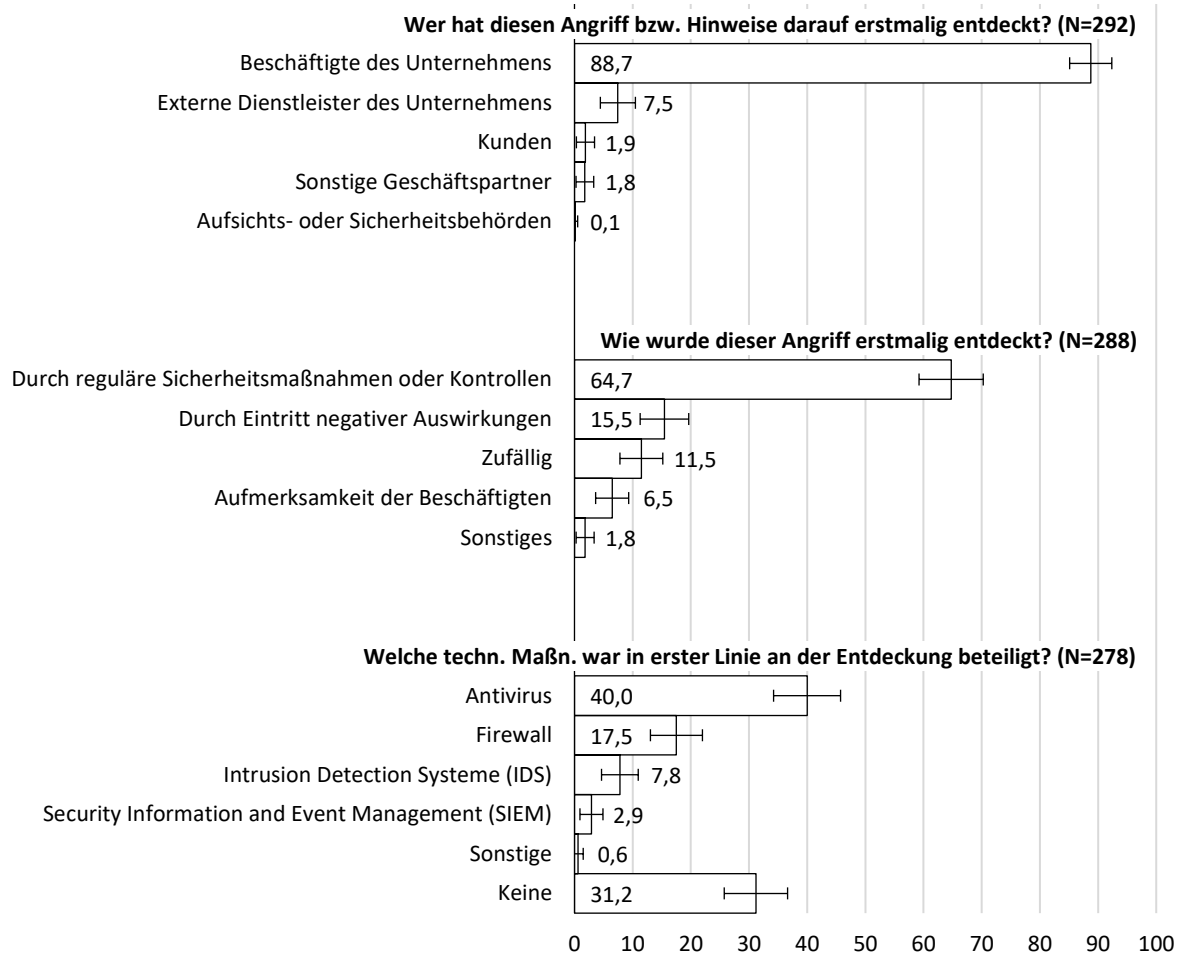
Der größte Unterschied im Vergleich zu den Ergebnissen in Befragung I liegt bei dem rund 19 Prozentpunkte höheren Anteil von Phishing-Angriffen (Befragung I: 26,0 %). Dieser Unterschied dürfte auf die stärkere Verbreitung sowie mit der gestiegenen Anzahl von Phishing-Angriffen zurückzuführen sein. Dass der schwerwiegendste Cyberangriff im Zusammenhang mit der Corona-Pandemie stand, berichtete ein Anteil von 7,0 % (N=297). Ein etwas höherer Anteil von 11,6 % gab an, dass der berichtete schwerwiegendste Cyberangriff der letzten 12 Monate im Verbindung mit der Schadsoftware Emotet[73] erfolgte, wobei dies 46,9 % nicht genau sagen konnten und lediglich von rund zwei Fünftel (41,5 %) ausschlossen wurde.

[73] Emotet galt insbesondere für Unternehmen als eine der gefährlichsten Schadsoftwarekombinationen, deren Infrastruktur vier Monate nach der Befragung II im Januar 2021 zerschlagen werden konnte (Quelle:

6.2 Entdeckung

Bei der Entdeckung des schwerwiegendsten Cyberangriffs spielten vor allem Unternehmensbeschäftigte und reguläre Sicherheitsmaßnahmen oder reguläre Kontrollen eine große Rolle. So gab der überwiegende Anteil von 88,7 % der Unternehmen an, dass der Angriff erstmalig von Beschäftigten entdeckt wurde, gefolgt von externen Dienstleistern (7,5 %). Demgegenüber waren dabei nur selten Kunden, sonstige Geschäftspartner oder Aufsichts- oder Sicherheitsbehörden involviert (Abbildung 40).

Abbildung 40 **Wege der Entdeckung des schwerwiegendsten Cyberangriffs**
in Prozent; gewichtete Daten; 95%-KI



Die Entdeckung erfolgte zudem bei 64,7 % der Unternehmen im Rahmen von regulären Sicherheitsmaßnahmen oder Kontrollen und lediglich bei 15,5 % erst durch den Eintritt negativer Auswirkungen.[74] Immerhin wurde bei etwa jedem neunten Unternehmen (11,5 %) der Angriff rein zufällig entdeckt[75] und bei weiteren 6,5 % durch die Aufmerksamkeit von Beschäftigten.

https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html; zuletzt geprüft am 28.05.2021).

[74] Zu den Angriffsarten, die erst durch ihre negativen Auswirkungen aufgefallen sind zählen vor allem Ransomware und sonstige Schadsoftware (48,8 % bzw. 36,4 % der über negative Auswirkungen entdeckten Cyberangriffe; N=44).

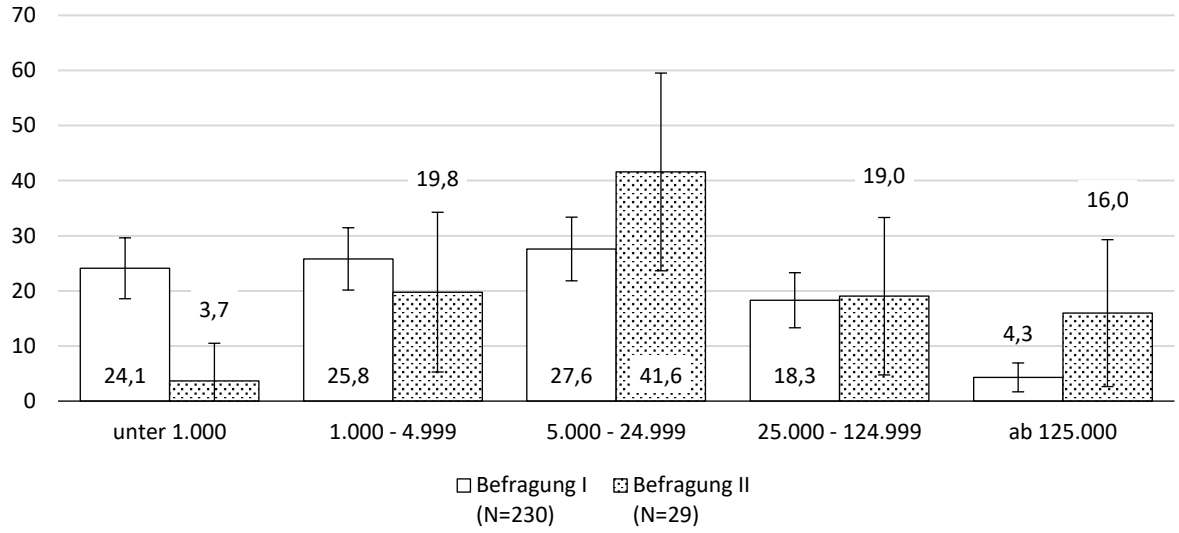
[75] Dazu zählten vor allem Phishing-Angriffe und sonstige Schadsoftware-Angriffe (54,9 % bzw. 31,7 % der zufällig entdeckten Cyberangriffe; N=33).

Bei etwa einem Drittel (31,2 %) war an der Entdeckung in erster Linie keine technische Maßnahme beteiligt.[76] Zwei Fünftel (40,0 %) wurden mit Antivirensoftware und weiteren 17,5 % mit Hilfe einer Firewall entdeckt. Noch seltener wurden Intrusion Detection Systeme (7,8 %) und Security Information and Event Management (2,9 %) genannt.[77]

6.3 Lösegeldforderung

In 11,9 % der berichteten schwerwiegendsten Cyberangriffe (N=280) wurde von den Täter*innen Lösegeld gefordert. Die Spannweite der Lösegeldforderungen ist erneut sehr groß und bewegt sich zwischen 300 EUR und 1 Mio. EUR. Der Median liegt bei rund 14.400 EUR und damit deutlich über dem Median in Befragung I (4.800 EUR), wobei erwähnt werden muss, dass die Fallzahl der Unternehmen, die Angaben dazu machten, in Befragung II sehr klein und somit Vorsicht bei der Interpretation geboten ist. Dennoch lässt sich in Abbildung 41 erkennen, dass im Vergleich zu Befragung I kaum noch Lösegelder unter 1.000 EUR gefordert wurden, wohingegen z.B. der Anteil hoher Lösegelder (ab 125.000 EUR) zumindest tendenziell gestiegen ist.

Abbildung 41 **Höhe der Lösegeldforderung in EUR (klassiert) nach Befragung**
in Prozent; gewichtete Daten; 95%-KI



6.4 Folgen

6.4.1 Betroffene Systeme

Zu den drei am häufigsten genannten IT-Systemen, die von den berichteten schwerwiegendsten Angriffen betroffen waren, d.h., die infolge nicht oder nur stark eingeschränkt genutzt werden konnten, zählen Standard-Arbeitsplätze und Office IT (51,3 %),[78] E-Mail und Kommunikation

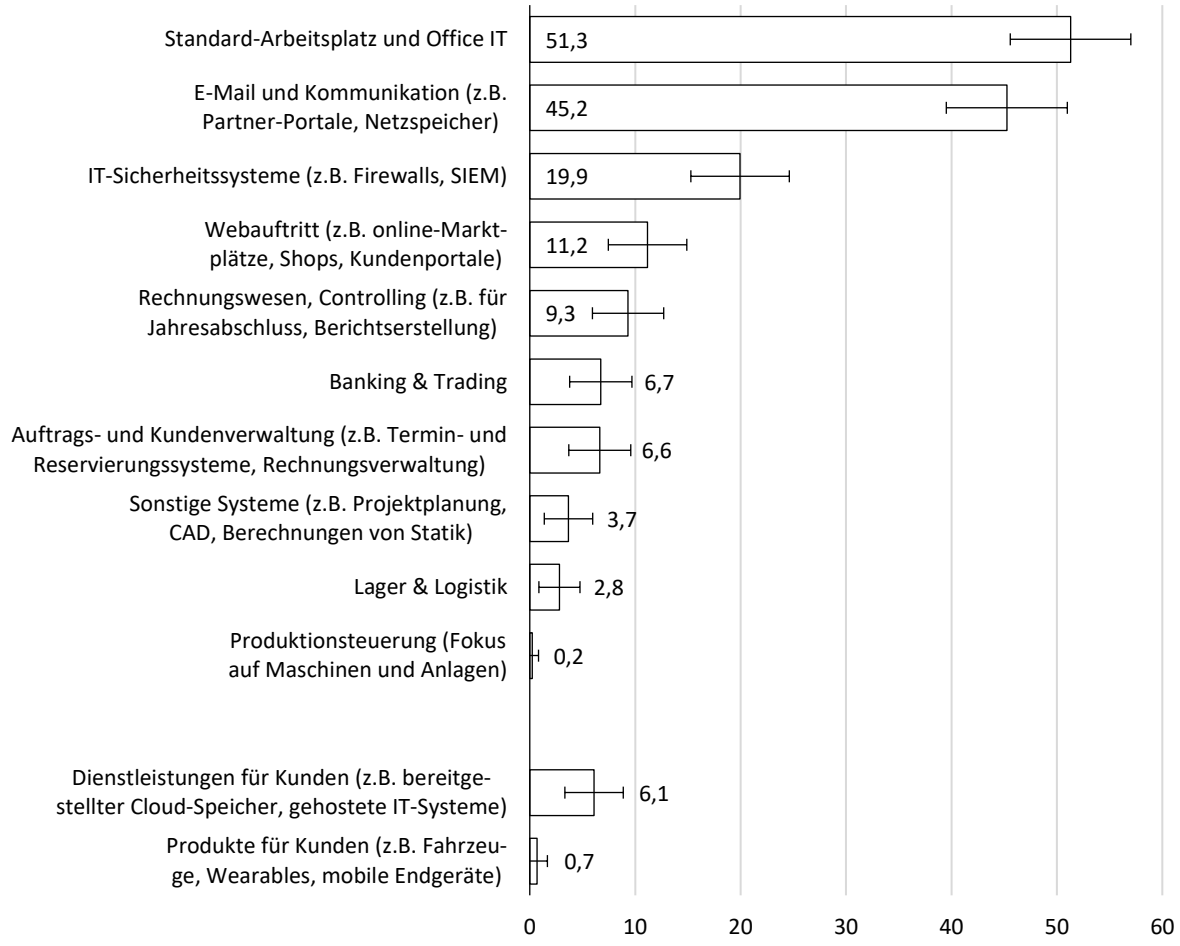
[76] Zu den ohne Technik entdeckten Angriffsarten zählen insbesondere Phishing (41,5 %), Ransomware (26.0 %) und sonstige Schadsoftware (22,0 %; N=87).

[77] Werden nur die Unternehmen einbezogen, die über ein Security Information an Event Management (SIEM) verfügen (N=44), dann waren SIEMs bei 17,4 % maßgeblich an der Entdeckung des schwerwiegendsten Vorfalls beteiligt.

[78] Im Vergleich zu Befragung I wurden bei dieser Frage zusätzlich Antwortkategorien vorgegeben. Dazu zählen Standard-Arbeitsplätze und Office IT, IT-Sicherheitssysteme, Dienstleistungen für Kunden und Produkte für Kunden. Da z.T. auch

(45,2 %) und mit einigem Abstand IT-Sicherheitssysteme (19,9 %). Die Produktionssteuerung mit dem Fokus auf Maschinen und Anlagen, deren Ausfall schnell sehr große Schäden verursache würde, wurden mit 0,2 % am seltensten genannt (Abbildung 42).

Abbildung 42 **Vom schwerwiegendsten Cyberangriff betroffene IT-Systeme**
in Prozent; gewichtete Daten; 95%-KI; Mehrfachantworten möglich

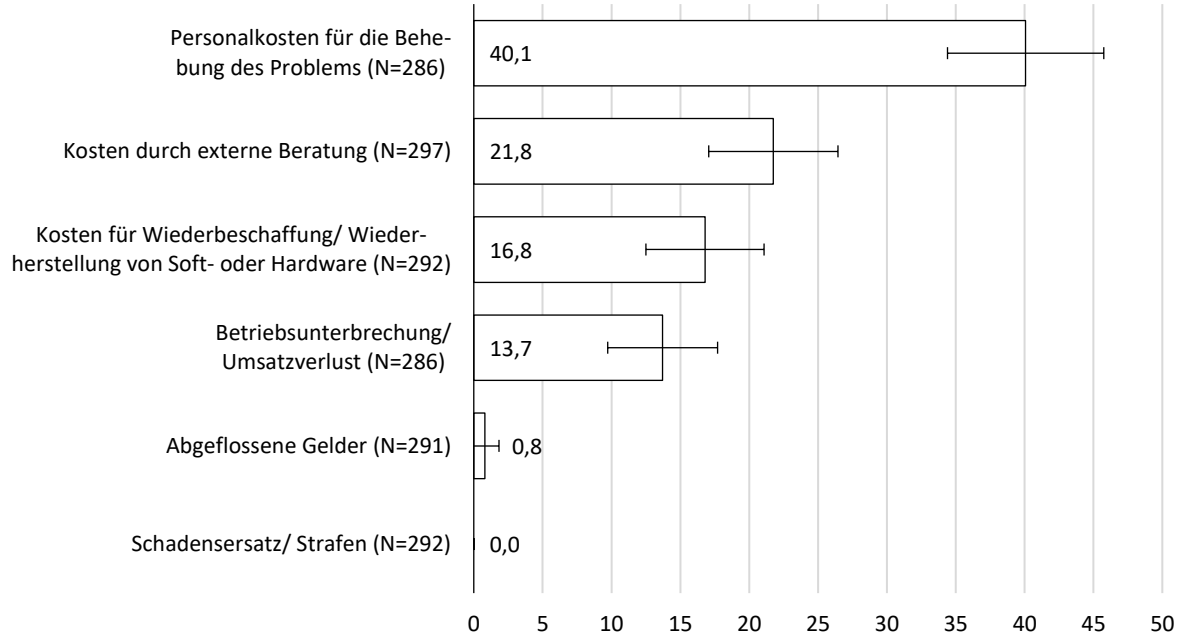


6.4.2 Kostenpositionen

Über die Hälfte der Unternehmen, die detaillierte Angaben zum schwerwiegendsten Cyberangriff der letzten zwölf Monate machten (53,8 %; N=297), gaben an, dass bei mindestens einer der erhobenen Kostenpositionen Kosten entstanden sind. Ohne Berücksichtigung der Höhe der Kosten wurden am häufigsten Personalkosten für die Behebung des Problems angeführt (40,1 %), gefolgt von Kosten durch externe Beratung (21,8 %), Kosten für Wiederbeschaffung/ Wiederherstellung von Soft- oder Hardware (16,8 %) und Betriebsunterbrechungen bzw. Umsatzverlust (13,7 %). Dass Gelder abgeflossen seien, berichtete hingegen nur rund 1 Prozent der Unternehmen und Kosten durch Schadensersatz bzw. Strafen wurden gar nicht genannt (Abbildung 43).

zusätzliche Erläuterungen in Form von Beispielen angefügt wurden, ist ein Vergleich zu den Ergebnissen von Befragung I nicht sinnvoll.

Abbildung 43 **Positionen bei denen Kosten entstanden sind**
in Prozent; gewichtete Daten; 95%-KI; Mehrfachangaben möglich



6.4.3 Kostenhöhe

Neben den erfragten Positionen wurde die Höhe der Kosten erhoben.[79] Die summierten Gesamtkosten[80] liegen im Durchschnitt bei 7.780 EUR und der Median bei 500 Euro[81] (N=131), woran bereits zu erkennen ist, dass die Verteilung erneut sehr schief ist. Während die Durchschnittskosten und der Median damit geringer ausfallen als in Befragung I (16.900 EUR bzw. 1.000 EUR), vergrößerte sich die Spannbreite und liegt zwischen 20 EUR und 3,8 Mio. EUR (Befragung I: 10 EUR - 2 Mio. EUR).[82]

Insgesamt gesehen bestätigt sich damit der in Befragung I gewonnene Eindruck, dass die meisten Cyberangriffe nur relativ geringe Kosten verursachen und lediglich in wenigen Fällen große Schäden für die Unternehmen entstehen. Insbesondere dann, wenn der Betrieb unterbrochen werden musste, fielen die Kosten sowohl im Durchschnitt (3.910 EUR) als auch im Median (1.000 EUR) am höchsten aus.

---

79 Armin et al. (2016) weisen auf die Bedeutung verlässlicher Daten zur Höhe der Kosten, die von Cyberangriffen verursacht werden, für gesetzgeberische und regulatorische Maßnahmen hin.

80 Dabei handelt es sich um „gesicherte“ Gesamtkosten, d.h., diese wurden nur auf Basis der Fälle berechnet, bei denen Kosten entstanden sind und bei denen zu allen Kostenpositionen gültige Werte zur Kostenhöhe vorlagen. Zu den ausgeschlossenen nicht gültigen Werten zählen die Antworten „keine Angabe“ oder „weiß nicht“.

81 D.h., bei der Hälfte der Unternehmen, die angaben, dass ihnen aufgrund eines erlebten Cyberangriffs Kosten entstanden sind, belaufen sich diese in einer Höhe bis zu 500 EUR. Die andere Hälfte verzeichnete Kosten über 500 EUR.

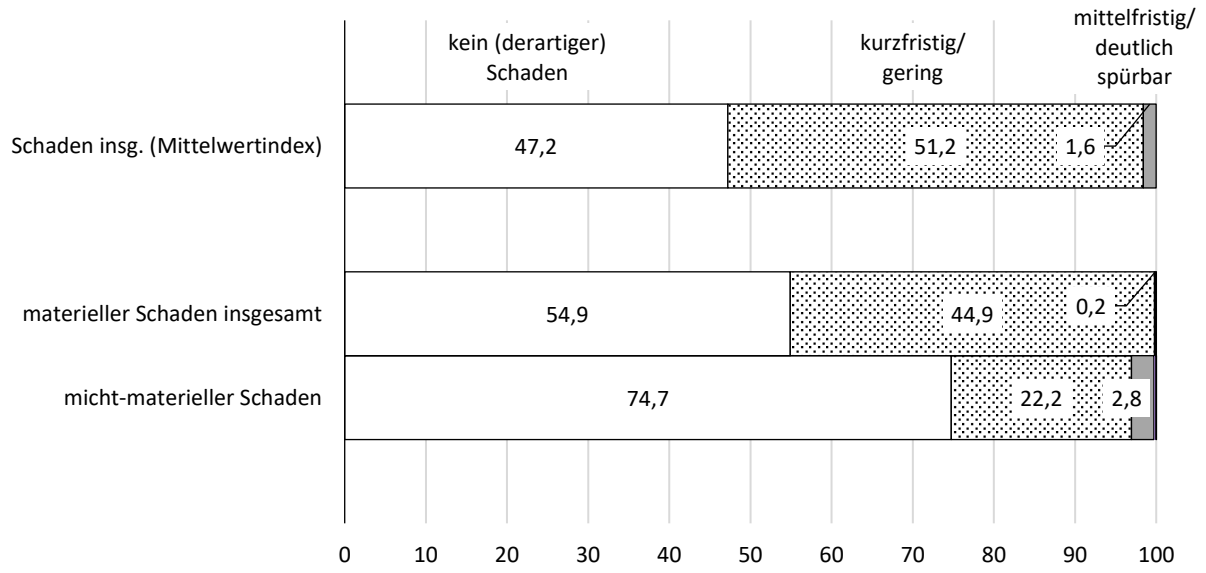
82 In der aktuellen Studien von Hiscox (2021), in der u.a. 1.000 Unternehmen in Deutschland (ab 1 Besch.) befragt wurden, werden die Kosten infolge von Cyberangriffen für Unternehmen in Deutschland im Median mit 24.000 USD beziffert. Aufgrund einer anderen Grundgesamtheit (inkl. Kleinstunternehmen) und fehlender Angaben zur Stichprobenziehung sowie zu deren Zusammensetzung hinsichtlich verschiedener Unternehmensmerkmale, erscheint ein Vergleich mit den Ergebnissen dieser Befragung nicht sinnvoll. Die britische Studie vom Department for Digital, Culture, Media & Sport (2021: 52) berichtet Durchschittskosten von 8.460 GBP (Median 500 GBP), die infolge aller bemerkten Cyberangriffe der letzten zwölf Monate entstanden sind.

Tabelle 12 **Kostenhöhe der schwerwiegendsten Cyberangriffe nach Kostenposition**
In EUR; gerundet; gewichtete Daten; Mehrfachantworten möglich; nur Unternehmen mit Kosten

	N	Mittelwert	Median	Minimum	Maximum
Personalkosten für die Behebung des Problems (Abwehr & Aufklärung)	89	1.320	400	20	20.000
Kosten durch externe Beratung (z.B. IT-Dienstleister, Rechtsberatung)	47	1.800	840	50	50.000
Kosten für Wiederbeschaffung/ Wiederherstellung von Soft- oder Hardware (keine Personalkosten)	37	1.210	500	50	15.000
Betriebsunterbrechung/ Umsatzverlust (z.B. durch Mitarbeiter, die nicht arbeiten konnten oder Systeme, die ausfielen)	35	3.910	1.000	30	50.000
Abgeflossene Gelder	2			1.000	3.800.000
Schadensersatz/ Strafen	0				
Gesamtkosten	131	7.780	500	20	3.800.000

Entsprechend fiel auch die Bewertung der Schäden durch die Befragten aus (Abbildung 44), bei der auch nicht-materielle Schäden (z.B. Reputationsverlust oder Wettbewerbsnachteil) einbezogen wurden. Nur 1,6 % gaben an, dass der durch den schwerwiegendsten Cyberangriff verursachte Schaden insgesamt mittelfristig/ deutlich spürbar ausfiel und über die Hälfte stufte die Schäden als kurzfristig/ gering ein. Bei dem verbleibenden Anteil von 47,2 % entstand weder ein materieller noch ein nicht-materieller Schaden.

Abbildung 44 **Einschätzung der Schäden**
in Prozent; gewichtete Daten



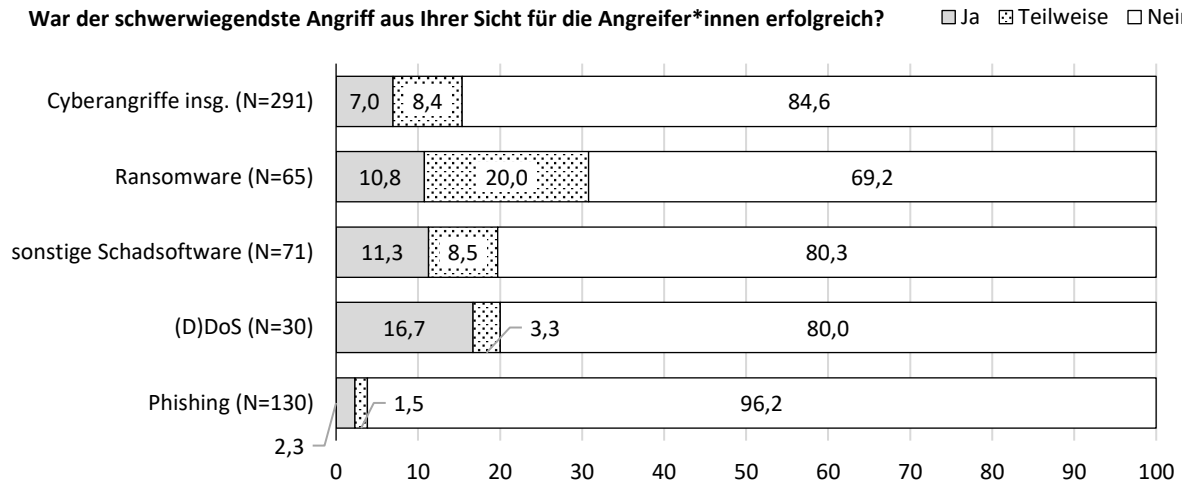
6.4.4 Betroffene Daten

Bei einem Anteil von 15,7 % der Unternehmen (N=283) war durch den schwerwiegendsten Angriff mindestens eine der erhobenen Datenarten betroffen. Dabei wurden am häufigsten personenbezogene Daten (44,2 %; N=44) und Strategie-, Vertriebs- und Finanzinformationen (z.B. Preislisten, Sanierungspläne, Akquisitionen, Finanz- und Rechnungswesensdaten) genannt (41,3 %). Etwas seltener wurden Produktdaten (z.B. Konstruktionspläne, Rezepturen, Quellcodes etc.) und sonstige Daten aufgeführt (23,1 % bzw. 17,0 %).

*6.4.5 Erfolg aus Sicht der Täter*innen*

Da sich von den direkten Folgen der berichteten schwerwiegendsten Cyberangriffen nicht eindeutig ableiten lässt, in welchem Stadium der (versuchte) Cyberangriff abgewehrt bzw. unterbunden werden konnte, wurden die Befragten gebeten, die Perspektive der Täter*innen einzunehmen und einzuschätzen, ob der Angriff „erfolgreich", „teilweise erfolgreich" oder „erfolglos" verlaufen ist. Über alle Angriffsarten hinweg berichteten 7,0 % von einem erfolgreichen und weitere 8,4 % von einem teilweise erfolgreichen Angriff (Abbildung 45). In der überwiegenden Mehrzahl blieben die berichteten Cyberangriffe anscheinend in einem frühen Versuchsstadium stecken.[83]

Abbildung 45 **Einschätzung zum Erfolg der schwerwiegendsten Cyberangriffe nach Angriffsart**
in Prozent, gewichtete Daten, nur Angriffsarten mit N≥30



6.5 Anzeigeverhalten

6.5.1 Kontakt mit staatlichen Stellen

Auch in der zweiten Befragung wurde mit Bezug auf den schwerwiegendsten Cyberangriff der letzten zwölf Monate gefragt, ob sich das Unternehmen wegen dieses Vorfalls an eine staatliche Stelle gewendet hat und ggf. an welche. Dabei standen wiederum folgende Antwortmöglichkeiten zu Auswahl: nächste Polizeidienststelle, auf Cybercrime spezialisierte Polizeidienststelle, Verfassungsschutz, Bundesamt für Sicherheit in der Informationstechnik (BSI), Landesdatenschutzbeauftragte*r und sonstige. Dabei bleibt zunächst erneut unberücksichtigt, ob die Unternehmen Strafanzeige erstattet haben oder nicht.[84]

Bei der ersten Befragung lag der Anteil der Unternehmen mit Kontakt zu mindestens einer staatlichen Stelle bei 21,5 % (N=1.739). Im Vergleich dazu liegt der entsprechende Anteil in

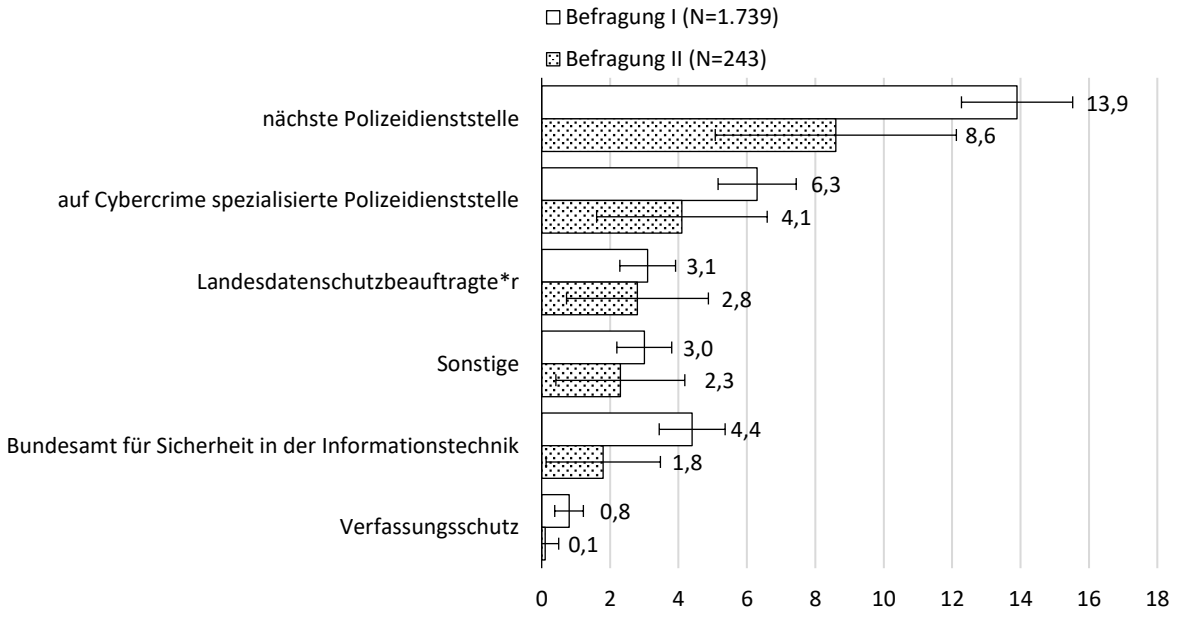
[83] Einschränkend sei angemerkt, dass sich der Taterfolg nicht immer unmittelbar zeigt und möglicherweise erst sehr viel später erkenntlich wird (z.B. bei Spyware-Angriffen).

[84] 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.

der zweiten Befragung mit 15,1 % (N=243) deutlich darunter, was auf eine rückläufige Kontaktsuche von Seiten der Unternehmen hindeutet.[85] Ein Grund dafür liegt in der Schwere der Vorfälle. Wenn bei der Auswertung kontrolliert wird, ob durch den berichteten Vorfall Kosten entstanden sind oder nicht, dann zeigen sich in den Gruppen mit Kosten infolge des schwerwiegendsten Angriffs sehr ähnlich Anteile mit Behördenkontakt (Befragung I: 23,6 %; Befragung II: 24,4 %). In der Gruppe ohne Kosten sank hingegen der Anteil mit Behördenkontakt von 11,5 % (N=515) in Befragung I auf 4,8 % (N=104) in Befragung II.

Im Vergleich der staatlichen Stellen nahm der Anteil mit Kontakt am deutlichsten bezüglich der nächsten Polizeidienststelle (Befragung I: 13,9 %; Befragung II: 8,6 %; Abbildung 13) sowie des Bundesamts für Sicherheit in der Informationstechnik ab (Befragung I: 4,4 %; Befragung II: 1,8 %).

Abbildung 46 **Betroffene Unternehmen mit Behördenkontakt nach staatlichen Stellen**
in Prozent; gewichtete Daten; 95%-KI; Mehrfachangaben möglich

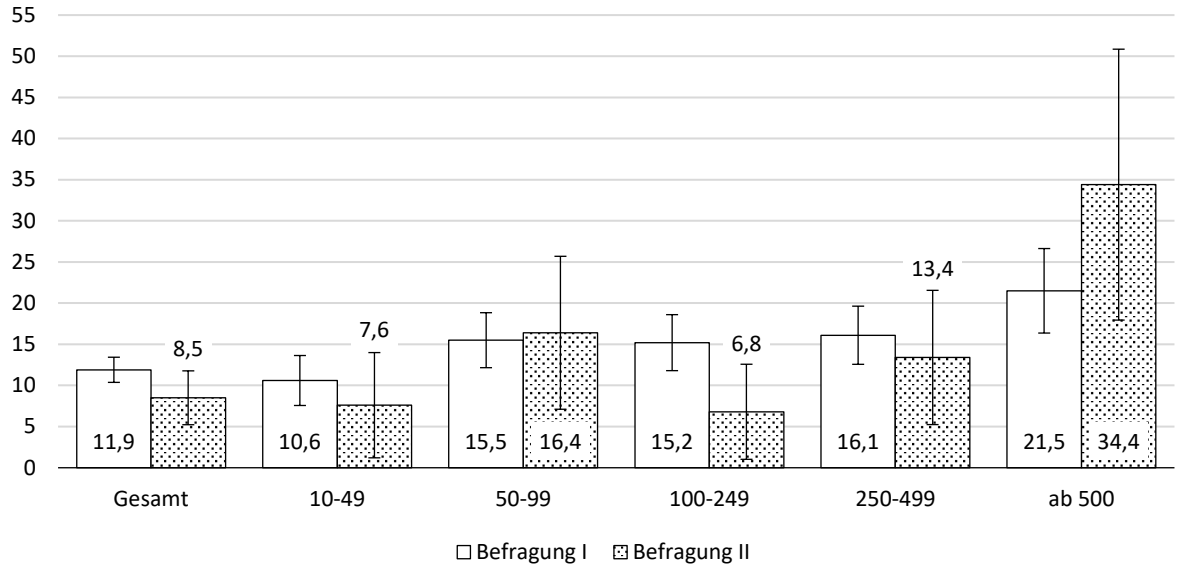


6.5.2 Anzeigeerstattung

Bezogen auf den schwerwiegendsten Vorfall gaben in Befragung II lediglich 8,5 % der betroffenen Unternehmen an, diesen Vorfall angezeigt zu haben (N=279). Auch wenn der Unterschied zu Befragung I (11,9 %; N=1.726) statistisch nicht signifikant ist, verweist der tendenziell kleiner gewordene Anteil erneut auf eine geringe Anzeigebereitschaft und ein sehr großes Dunkelfeld im Bereich der Cyberkriminalität gegen Unternehmen. Zugenommen hat diesbezüglich der Unterschied zwischen kleinen und großen Unternehmen (Abbildung 47): Während lediglich 7,6 % (N=66) der kleinen Unternehmen (10-49 Beschäftigte) Anzeige erstatteten, liegt der Anteil der großen Unternehmen (ab 500 Beschäftigte) in Befragung II bei 34,4 % (N=32).

[85] Diese Abnahme ist auch unter Kontrolle der Teilnahme an Befragung II zu erkennen (Ergebnis der ersten Befragung der erneut teilnehmenden Unternehmen: 19,9 %; N=289).

Abbildung 47 **Anzeigequote nach Beschäftigtengrößenklasse und Befragung**
in Prozent; gewichtete Daten; 95%-KI; nur Angaben zum schwerwiegendsten Cyberangriff



Die Anzeige von Cyberangriffen steht in einem statistisch relevanten Zusammenhang mit der Frage, ob der Angriff aus Sicht der Täter*innen zumindest teilweise erfolgreich war. So zeigten immerhin 25,6 % der Unternehmen, den schwerwiegendsten Angriff an, die diese Frage bejahten (N=43), wohingegen nur 5,7 % Anzeige erstatteten, bei denen die Täter*innen keinen Erfolg hatten (N=229). Das bedeutet, dass das Dunkelfeld in Hinblick auf die versuchten Cyberangriffe deutlich größer ist als bei Cyberangriffen, die das Versuchsstadium überschritten haben.

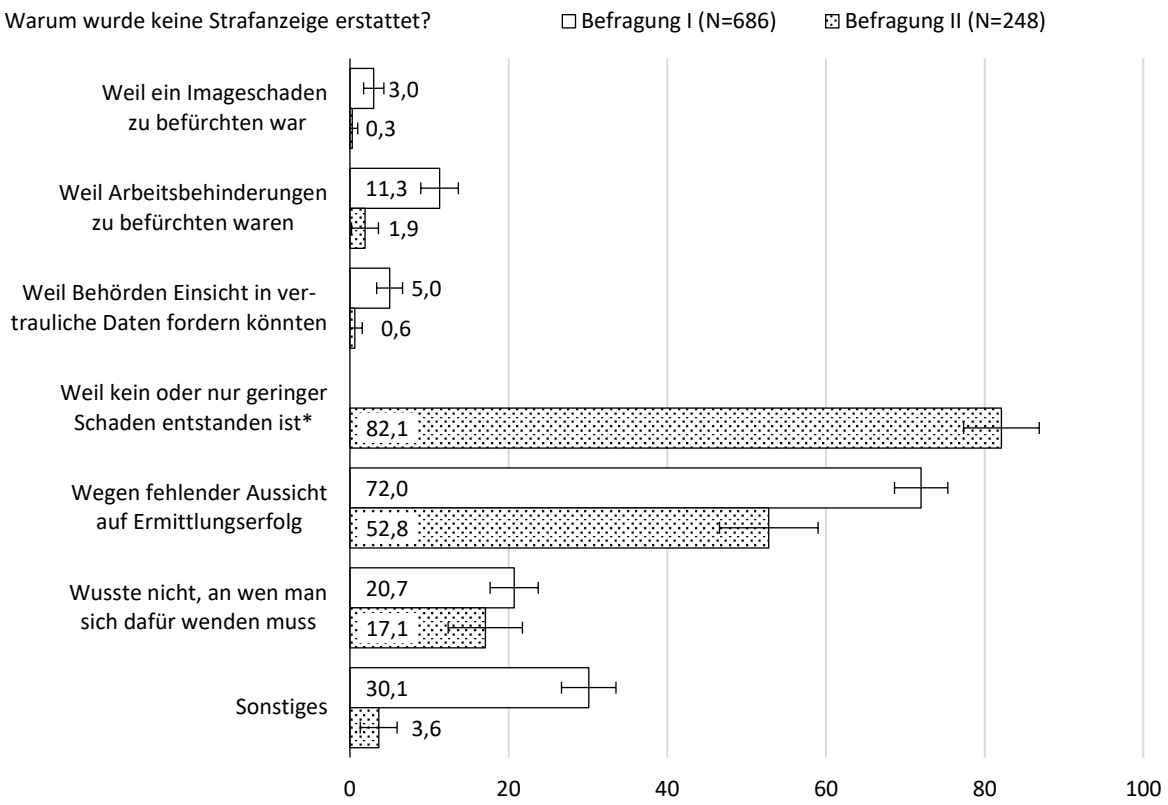
Eine Differenzierung der Anzeigequote nach Angriffsart ist aufgrund der geringen Fallzahl nur sehr eingeschränkt möglich. Dabei lässt sich lediglich erkennen, dass Phishing und (D)DoS-Angriffe tendenziell etwas seltener angezeigt werden (3,1 % bzw. 3,3 %; N=128 bzw. 30), als Angriffe mit Ransomware (8,2 %; N=61) und mit sonstiger Schadsoftware (13,1 %; N=61). Zu den am häufigsten angezeigten Angriffsarten scheinen CEO-Fraud (4 von 16) und Spyware-Angriffe (6 von 11) zu zählen, was dem Ergebnis aus Befragung I entspricht.

6.5.3 Nichtanzeigegründe

Wenn der schwerwiegendste Cyberangriff nicht angezeigt wurde, konnten die Unternehmensvertreter*innen die ausschlaggebenden Gründe dafür angeben. Zur Befragung I gleichgeblieben sind die vorgegebenen Antwortmöglichkeiten: „Weil ein Imageschaden zu befürchten war“, „Weil Arbeitsbehinderungen zu befürchten waren“, „Weil Behörden Einsicht in vertrauliche Daten fordern könnten“, „Wegen fehlender Aussicht auf Ermittlungserfolg“, „Wusste nicht, an wen man sich dafür wenden muss“ und „Sonstiges“. Neu hinzugekommen ist die Antwortmöglichkeit „Weil kein oder nur geringer Schaden entstanden ist“. Diese wurde in Befragung II mit 82,1 % am häufigsten ausgewählt (Abbildung 48). Wie erwartet, konnte mit ihr die in Befragung I noch relativ häufig gewählte Antwortkategorie „Sonstiges“ fast vollständig aufgelöst werden.[86]

[86] Die Kategorie „Sonstiges“ wurde in Befragung II zusätzlich freitextlich erhoben. Dabei wurde vor allem auf den (zeitlichen) Aufwand verwiesen, der nicht im Verhältnis mit dem Vorfall stand.

Abbildung 48 **Nichtanzeigegründe nach Befragung**
in Prozent; gewichtete Daten; 95%-KI; nur Angaben zum schwerwiegendsten Cyberangriff; Mehrfachantwort möglich



*) Antwortkategorie nur in Befragung II

Die bereits in Befragung I relativ selten genannten Gründe: Befürchtung eines Imageschadens, Arbeitsbehinderung und Behördeneinsicht in vertrauliche Daten spielten in Befragung II fast gar keine Rolle mehr. Die fehlende Aussicht auf Ermittlungserfolg wurde mit 52,8 % deutlich seltener angegeben. Nur wenig verändert hat sich hingegen der Anteil derjenigen Unternehmen, die nicht genau wissen, an wen man sich für eine Anzeige des berichteten schwerwiegendsten Vorfalls wenden muss.

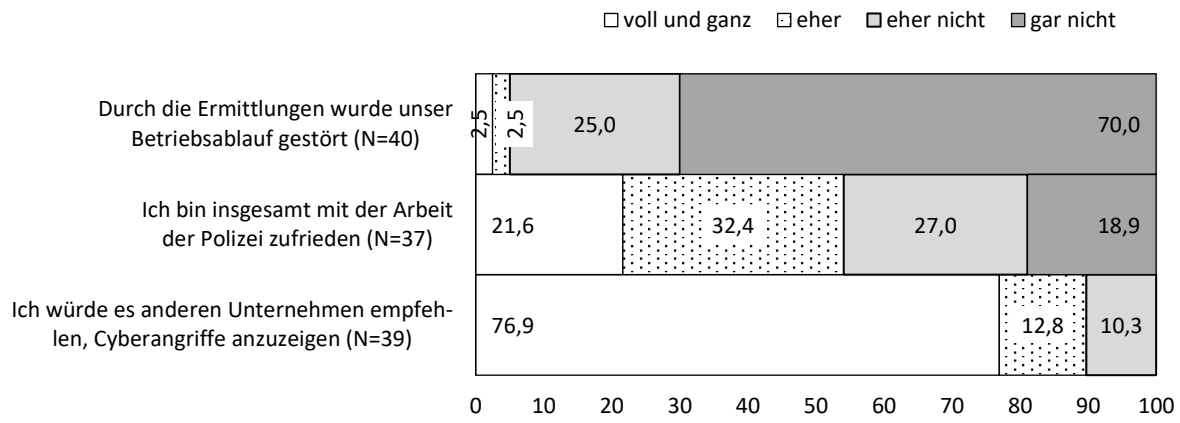
6.6 Bewertung der Strafverfolgungsbehörden

Da die Fallzahl der Unternehmen, die den schwerwiegendsten Vorfall zur Anzeige gebracht haben und Aussagen zu den Ermittlungen der Strafverfolgungsbehörden machen konnten, sehr klein ist und sie sich im Zuge einer Datengewichtung weiter reduzieren würde,[87] werden hier die Ergebnisse der ungewichteten Daten berichtet. D.h., große Unternehmen gehen überproportional in diese Auswertung ein. Dennoch zeigt sich ein recht ähnliches Bild, wie in Befragung I. Nur bei einem geringen Anteil der anzeigenden Unternehmen (5,0 %) wurde der Betriebsablauf durch die daraufhin folgenden Ermittlungen (eher) gestört (Abbildung 49). Bei 70,0 % traf dies gar nicht zu. Insgesamt (eher) zufrieden mit der Arbeit der Polizei zeigte sich etwa die

[87] Dies liegt im Wesentlichen darin begründet, dass große Unternehmen, die in der ungewichteten Stichprobe überrepräsentiert sind, häufiger Anzeige erstatten als kleinere und somit auch bei diesen Angaben stärker vertreten sind.

Hälfte der anzeigenden Unternehmen (54,0 %) und ein Großteil (89,7 %) würde es anderen Unternehmen (eher) empfehlen, Cyberangriffe anzuzeigen.

Abbildung 49 **Bewertung der Arbeit der Strafverfolgungsbehörden**
in Prozent, ungewichtete Daten; nur Unternehmen, die den schwerwiegendsten Vorfall anzeigten



Die Frage, ob zu dem angezeigten Vorfall von den Strafverfolgungsbehörden Täter*innen ermittelt werden konnten, bejahte ein Anteil von 9,1 % (N=33). In den meisten dieser Fälle (90,9 %) blieb ein Ermittlungserfolg hingegen aus. Auch dieses Ergebnis entspricht dem Befund aus Befragung I, bei der dieser Anteil bei 7,7 % lag (gewichtete Daten).

7 RISIKOMERKMALE UND SCHUTZMAßNAHMEN

Bei der Auswertung von Befragung I wurde in Hinblick auf die Frage nach potentiellen Risiko- und Schutzfaktoren das Vorhandensein von unterschiedlichen Unternehmensmerkmalen bzw. das Vorhandensein von verschiedenen IT-Sicherheitsmaßnahmen zum Anteil der in den letzten zwölf Monaten von Cyberangriffen betroffenen Unternehmen in Beziehung gesetzt. Dabei wurde nach Beschäftigtengrößenklasse differenziert und festgestellt, dass es bestimmte Merkmale gibt, die zumindest tendenziell in alle Beschäftigtengrößenklassen mit höheren Betroffenheitsraten verbunden sind. Demgegenüber fanden sich hinsichtlich der IT-Sicherheitsmaßnahmen nicht immer in allen Größenklassen statistisch relevante Zusammenhänge in erwarteter Richtung. So waren z.B. mittlere Unternehmen, die Mitarbeiter*innenschulungen zur IT-Sicherheit durchführen, seltener betroffen, bei kleinen Unternehmen machten Schulungen hingegen keinen relevanten Unterschied.

Aufgrund der geringen Fallzahl ist die nach Größenklassen differenzierte Auswertung von Befragung II nicht sinnvoll. Da sich in Befragungen I zeigte, dass die Unternehmensgröße mit der Betroffenheit von Cyberangriffen und mit dem Vorhandensein der meisten IT-Sicherheitsmaßnahmen positiv korreliert ist, sind die diesbezüglich undifferenzierten gewichteten Gesamtergebnisse insbesondere zum Zusammenhang von IT-Sicherheitsmaßnahmen und Betroffenheit mit Vorsicht zu interpretieren, da die Antworten der kleinen Unternehmen entsprechend ihrem Anteil in der Grundgesamtheit stärker in die Auswertung eingehen als die der anderen Beschäftigtengrößenklassen.

Wie oben dargestellt, haben die Anteile der Unternehmen, die in den letzten zwölf Monaten auf mindestens einen Cyberangriff reagieren mussten, im Vergleich zu Befragung I zugenommen. Weil darunter auch viele versuchte Angriffe fallen, die mit einer rechtzeitigen Reaktion frühzeitig abgewehrt werden konnten und häufig keine oder allenfalls geringe Schäden verursachten, werden die IT-Sicherheitsmaßnahmen ebenfalls mit dem Erleben eines als „(teilweise) erfolgreich“ bewerteten Cyberangriffs in Beziehung gesetzt. Diese haben nach Einschätzung der teilnehmenden Unternehmen die Grenze des Versuchs in gewisser Hinsicht überschritten und konnten nicht mehr rechtzeitig abgewehrt werden.

In den folgenden Tabellen 13 bis 15 sind die die Phi-Koeffizienten (φ) als Maß für die jeweiligen bivariaten Zusammenhänge ausgewiesen. Phi kann Werte von -1 bis +1 annehmen und gibt damit die Richtung und Stärke des Zusammenhangs zwischen zwei binären Variablen an, wobei 0 für „kein Zusammenhang“ und |1| für einen „perfekten Zusammenhang“ steht. Ein Phi-Wert zwischen 0,1 und 0,3 gilt nach der Cohens Konvention für Kontingenzmaße als keiner Effekt, zwischen 0,3 und 0,5 als mittlerer und ab 0,5 als großer Effekt.[88]

[88] Cohen (1992: 157).

Tabelle 13 **Bivariate Zusammenhänge zwischen Betroffenheit und Risikomerkmalen**
Phi, nur Unternehmen mit Angaben zum schwerwiegendsten Cyberangriff

	Kontingenzkoeffizient ϕ	
Risikomerkmal vorhanden (0: nein, 1: ja)	Angriff(sversuch) erlebt (0: nein, 1: ja)	(teilw.) erfolgr. Angriff erlebt (0: nein, 1: ja)
Mehr als ein Standort in Deutschland	,070	,006
Mindestens einen Standort im Ausland	,110*	-,009
Exporttätigkeit	,030	,019
Besondere Produkte, Herstellungsverfahren oder Dienstleistungen	,234***	-,107*
Besondere Reputation oder Kundenkreis	,113**	-,115**

Signifikanzniveau: * p<.05, ** p<.01, *** p<.001

In Tabelle 13 zeigt sich, wie bereits in Befragung I, dass Unternehmen mit mindestens einem Standort im Ausland, mit besonderen Produkten, Herstellungsverfahren oder Dienstleistungen bzw. mit besonderer Reputation oder Kundenkreis häufiger (versuchte) Angriffe erleben bzw. auf diese reagieren. Entsprechenden Zusammenhänge zur Exporttätigkeit und zu mehreren Standorten in Deutschland können in Befragung II hingegen nicht repliziert werden.

Mit Blick auf die rechte Tabellenspalte zum Erleben (teilweise) erfolgreicher Angriffe fallen zwei signifikant negative Zusammenhänge auf: Unternehmen mit besonderen Produkten, Herstellungsverfahren oder Dienstleistungen bzw. mit besonderer Reputation oder Kundenkreis erleben demnach deutlich seltener Angriff, die das Versuchsstadium überschreiten. Das weist wiederum darauf hin, dass sich solche Unternehmen besser schützen, also mehr Angriffsversuche detektieren und dann rechtzeitig und erfolgreicher auf diese reagieren können. Dies scheint bei Unternehmen mit Auslandsstandort(en) nicht der Fall zu sein.

Um dies zu überprüfen, werden die drei Unternehmensmerkmale mit dem Vorhandensein der einzelnen IT-Sicherheitsmaßnahmen gesetzt (Tabelle 14). Wie vermutet setzen Unternehmen mit besonderen Produkten, Herstellungsverfahren oder Dienstleistungen bzw. mit besonderer Reputation oder Kundenkreis viele der erhobenen Maßnahmen deutlich häufiger ein, als die Gruppe der Unternehmen mit Standort(en) im Ausland und andere Unternehmen. Dies betrifft insbesondere organisatorische Maßnahmen wie schriftlich fixierte Richtlinien zur Informations- bzw. IT-Sicherheit und zum Notfallmanagement und Risiko- und Schwachstellenanalysen. Daneben setzen sie häufiger Netzwerksegmentierung und Informationssicherheitsmanagementsysteme ein, verschlüsseln häufiger sensible Daten, verstärken eher die physische Sicherheit und lagern die IT-Security öfter an externe Dienstleister aus. Unternehmen mit besonderer Reputation oder Kundenkreis setzen zudem häufiger auf Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme und verschlüsselte Kommunikation. Diese Unterschiede dürften eine Erklärung für die seltenere Betroffenheit (teilweise) erfolgreicher Angriffe sein. Anzumerken ist dabei, dass auch diese Merkmalsgruppen nicht trennscharf voneinander sind, d.h., sie können sich überschneiden, insofern einige Unternehmen mehrere dieser Merkmale tragen.

Tabelle 14 **Bivariate Zusammenhänge zwischen vorhandenen IT-Sicherheitsmaßnahmen und Betroffenheit**
Phi, nur Unternehmen mit Angaben zum schwerwiegendsten Cyberangriff

	Kontingenzkoeffizient ϕ		
IT-Sicherheitsmaßnahme vorhanden (0: nein, 1: ja)	Standort(e) im Ausland (0: nein, 1: ja)	Bes. Produkte, etc. (0: nein, 1: ja)	Bes. Reputation etc. (0: nein, 1: ja)
Schriftliche Richtlinien zur Informations- bzw. IT-Sicherheit	,078	,241***	171***
Schriftliche Richtlinien zum Notfallmanagement	,017	,223***	166***
Zertifizierung der IT-Sicherheit (z.B. nach ISO 27001 o. VdS 3473)	-,013	,029	,053
Risiko- u. Schwachstellenanalysen (auch Pentest)	,058	,218***	,255***
Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme	-,041	,051	,199***
Mindestanforderungen für Passwörter	-,007	,046	,061
Zwei-Faktor Authentifizierung	,119**	-,012	,049
Individuelle Vergabe von Zugangs- u. Nutzerrechten	,007	,140**	,057
Regelmäßige Backups	,021	,051	-,083
Test der Datenwiederherstellung (Restoring)	-,015	,105*	,092*
Antivirensoftware	,038	,065	,084*
Aktive Überwachung der Verfügbarkeit u. zeitnahe Installation von Sicherheitsupdates	,008	,120**	,069
Schutz der IT-Systeme mit einer Firewall	,000	,029	,034
Netzwerksegmentierung	,060	,224***	,228***
Security Information and Event Management (SIEM)	,130**	,135**	,203***
Security Operation Center (SOC)	,153**	,094	,103*
Austausch von Bedrohungsdaten (z.B. Threat Intelligence)	,105*	,119*	,200***
Künstliche Intelligenz basierte Maßnahmen	,161***	,207***	,197***
Informationssicherheitsmanagementsystem (ISMS)	,032	,191***	,166***
Verschlüsselung von Kommunikation	-,039	,072	,139**
Verschlüsselung von sensiblen Daten	,051	,153***	,097*
Verstärkte physische Sicherheit	-,013	,252***	,185***
IT-Security an externen Dienstleister ausgelagert	-,046	,189***	,113*

Signifikanzniveau: * p<.05, ** p<.01, *** p<.001

In Tabelle 15 sind die bivariaten Zusammenhänge zwischen IT-Sicherheitsmaßnahmen und Betroffenheit aufgelistet. Einige der Maßnahmen sind signifikant positiv mit dem Erleben mindestens eines (versuchten) Cyberangriffs korreliert, d.h., Unternehmen mit schriftlichen Richtlinien zur Informations- bzw. IT-Sicherheit, Risiko- und Schwachstellenanalysen, aktiver Überwachung der Verfügbarkeit und zeitnaher Installation von Sicherheitsupdates oder mit Netzwerksegmentierung haben innerhalb der letzten zwölf Monate häufiger auf (versuchte) Cyberangriffe reagiert.

Die Verschlüsselung von Kommunikation ist in dieser Hinsicht die einzige Maßnahme mit einem kleinen aber signifikant negativem Effekt ($\varphi = -0{,}108$). Dies kann ein Hinweis darauf sein, dass sich mit dieser IT-Sicherheitsmaßnahme das Risiko auf (versuchte) Cyberangriffe reagieren zu müssen, reduzieren lässt. Das ist insbesondere in Hinblick auf Cyberangriffe, die bei der Unternehmenskommunikation bzw. bei der Manipulation/ Täuschung der IT-Nutzer*innen ansetzen (z.B. CEO-Fraud und Phishing), durchaus plausibel.

Tabelle 15 **Bivariate Zusammenhänge zwischen Betroffenheit und vorhandenen IT-Sicherheitsmaßnahmen**
Phi, nur Unternehmen mit Angaben zum schwerwiegendsten Cyberangriff

	Kontingenzkoeffizient ϕ	
IT-Sicherheitsmaßnahme vorhanden (0: nein, 1: ja)	Angriff(sversuch) erlebt (0: nein, 1: ja)	(teilw.) erfolgr. Angriff erlebt (0: nein, 1: ja)
Schriftliche Richtlinien zur Informations- bzw. IT-Sicherheit	,219***	-,098*
Schriftliche Richtlinien zum Notfallmanagement	,129**	-,059
Zertifizierung der IT-Sicherheit (z.B. nach ISO 27001 o. VdS 3473)	,046	-,041
Risiko- u. Schwachstellenanalysen (auch Pentest)	,312***	-,138**
Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme	,132**	-,019
Mindestanforderungen für Passwörter	,129**	,003
Zwei-Faktor Authentifizierung	,087	,081
Individuelle Vergabe von Zugangs- u. Nutzerrechten	,046	-,061
Regelmäßige Backups	-,069	,024
Test der Datenwiederherstellung (Restoring)	,097*	,076
Antivirensoftware	,125**	-,006
Aktive Überwachung der Verfügbarkeit u. zeitnahe Installation von Sicherheitsupdates	,199***	,055
Schutz der IT-Systeme mit einer Firewall	-,040	,000
Netzwerksegmentierung	,189***	,066
Security Information and Event Management (SIEM)	,060	-,088
Security Operation Center (SOC)	,092	-,051
Austausch von Bedrohungsdaten (z.B. Threat Intelligence)	,162**	-,045
Künstliche Intelligenz basierte Maßnahmen	,106*	-,065
Informationssicherheitsmanagementsystem (ISMS)	,079	-,094
Verschlüsselung von Kommunikation	-,108*	-,140**
Verschlüsselung von sensiblen Daten	,052	-,115*
Verstärkte physische Sicherheit	,086	-,036
IT-Security an externen Dienstleister ausgelagert	,109*	-,100*

Signifikanzniveau: * p<.05, ** p<.01, *** p<.001

In der rechten Spalte von Tabelle 15 finden sich die Phi-Koeffizienten für die bivariaten Zusammenhänge zwischen IT-Sicherheitsmaßnahmen und dem Erleben bzw. der Reaktion auf einen Cyberangriff, der als „(teilweise) erfolgreich“ bewertet wurde. Zu erkennen ist, dass fast alle Zusammenhänge negativ ausfallen, d.h., die entsprechenden IT-Sicherheitsmaßnahmen stehen zumindest tendenziell mit einer geringeren Wahrscheinlichkeit des Erlebens von Cyberangriffen in Beziehung, die das Versuchsstadium überschritten haben. Statistische Signifikanz zeigt sich bei schriftlichen Richtlinien zur Informations- bzw. IT-Sicherheit (φ = -0,098), Risiko- u. Schwachstellenanalysen (φ = -0,108), Verschlüsselung von Kommunikation (φ = -0,140) und sensibler Daten (φ = -0,115) sowie bei Outsourcing der IT-Security an externe Dienstleister (φ = -0,100), auch wenn die Stärken der Zusammenhänge durchweg als gering zu bewerten sind.

Die Ergebnisse bezüglich der (teilweise) erfolgreichen Cyberangriffe führt auch zu einer etwas anderen Interpretation der positiven bivariaten Zusammenhänge zum Erleben mindestens eines (versuchten) Cyberangriffs, insofern sich darin die mit den IT-Sicherheitsmaßnahmen gestie-

gene Aufmerksamkeit und Fähigkeit zur Entdeckung (versuchter) Cyberangriffe wiederspiegeln dürfte, die eine rechtzeitig Reaktion erst ermöglichen. Am Beispiel der Risiko- und Schwachstellenanalysen wird dies besonders deutlich. Während diese Maßnahme den größten positiven Effekt auf das Erleben mindestens eines (versuchten) Cyberangriffs aufweist (φ = 0,312), also die Wahrscheinlichkeit, reagieren zu müssen oder eben zu können, signifikant steigert, steht sie gleichzeitig signifikant negativ mit dem Erleben eines (teilweise) erfolgreichen Cyberangriffs in Beziehung (φ =-0,138).

Die Richtung des Zusammenhangs in Hinblick auf die Verschlüsselung von Kommunikation bleibt demgegenüber gleich und vergrößert sich bezüglich der (teilweise) erfolgreichen Cyberangriffe von φ =-0,108 auf φ =-0,140. Dies weist auf eine wirksame Möglichkeit zur Reduktion der Angriffsfläche als auch der Erfolgsaussichten für Angreifer*innen hin.

Zu betonen ist noch einmal, dass die gefundenen bivariaten Zusammenhängen von anderen Variablen beeinflusst sein könnten und es sich lediglich um erste Hinweise auf mögliche Einflussfaktoren handelt. Das bedeutet ebenfalls, dass damit kein Nachweis für die Unwirksamkeit von IT-Sicherheitsmaßnahmen geführt wurde, bei denen sich keine statistisch signifikanten Koeffizienten zeigten. Generell ist eher davon auszugehen, dass es für die Verbesserung der IT-Sicherheit von Unternehmen ein Zusammenspiel aus verschiedenen organisatorischen und technischen IT-Sicherheitsmaßnahmen braucht, zumal viele der Maßnahmen untereinander z.T. relativ hoch korreliert sind. Für die Überprüfung der gefundenen Zusammenhänge unter Einbezug von Angaben zum Reifegrad und zur Verbreitung im Unternehmen sind weitere multivariate Analysen und Publikationen geplant.

8 ZUSAMMENFASSUNG ZENTRALER ERGEBNISSE

Durch die Corona-Krise haben die Nutzungen digitaler Anwendungen sowohl im privaten als auch beruflichen Alltag stark zugenommen. Die Chancen und Möglichkeiten der Digitalisierung traten durch die Krisensituation deutlich hervor. Vor diesem Hintergrund kommt der Absicherung von IT-Systemen insbesondere vor den Risiken verschiedenster Cyberangriffsarten eine noch größere Bedeutung zu als zuvor. Insbesondere Unternehmen, deren Beschäftigte vermehrt aus dem Homeoffice arbeiten, geschäftliche Treffen in den digitalen Raum verlegen oder virtuellen Tagungen und Konferenzen besuchen, stehen vor der Herausforderung, diese notwendigen Veränderungen zu ermöglichen und gleichzeitig die damit verbundenen Risiken gering zu halten. Um diesbezügliche Entscheidungen begründet und evidenzbasiert treffen zu können,[89] sind unabhängige wissenschaftliche Forschungsergebnisse notwendig, die nach wie vor nur selten und fragmentiert verfügbar sind.

Das Kriminologische Forschungsinstitut Niedersachsen e.V. führte zusammen mit dem Forschungszentrum L3S der Leibniz-Universität Hannover das Forschungsprojekt „Cyberangriffe gegen Unternehmen“ durch, in dem differenzierte Befunde zu den Angriffsarten, zur Häufigkeit der Cyberangriffe, zur Verbreitung von Präventionsmaßnahmen und IT-Sicherheitsstandards als auch zu Risiko- und Schutzfaktoren erhoben wurden. Ein weiteres Ziel dieses Projektes war es, das erarbeitete Wissen handlungspraktisch aufzubereiten und in die Unternehmen zu transferieren, um insbesondere kleine und mittlere Unternehmen mit begrenzten personellen und materiellen Ressourcen zu unterstützen, ihre IT-Sicherheit gezielt zu verbessern.

Das Projekt wurde mit einer Laufzeit von Dezember 2017 bis November 2020 (verlängert bis März 2021) im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie (BMWi) gefördert und erhielt eine zusätzliche Förderung von PricewaterhouseCoopers Deutschland und der VHV-Stiftung. Neben Experteninterviews und verschiedenen Feldstudien mit IT-Beschäftigten in kleinen und mittleren Unternehmen wurde eine CATI-Befragung mit 5.000 Unternehmen ab zehn Beschäftigten und mit Sitz in Deutschland sowie eine webbasierte Folgebefragung mit letztendlich 687 dieser Unternehmen durchgeführt. Die Basis beider Befragungen bildet eine disproportional geschichtete Zufallsstichprobe.

Die Ergebnisse zur ersten Befragung wurden bereits im KFN-Forschungsbericht Nr. 152, einem zusätzlichen Kurzbericht[90] und weiteren Beiträgen[91] veröffentlicht. Die ersten deskriptiven Ergebnisse der Folgebefragung 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.

---

[89] Zum Thema evidenzbasierter Polizeiarbeit bezüglich der Cyberkriminalität siehe Koziarski & Lee (2020).

[90] Dreißigacker et al. (2020a); Kriminologisches Forschungsinstitut Niedersachsen e. V. (2020).

[91] Dreißigacker & Wollinger (2020); Dreißigacker et al. (2020d); Huaman et al. (2021); Skarczinski et al. (2021).

1) Welche IT-Sicherheitsmaßnahmen werden getroffen?

Gemäß der Ergebnisse von Befragung I (2018/19) sind basale technische Maßnahmen wie der Schutz der IT-Systeme durch eine Firewall, regelmäßige Backups, aktuelle Antivirensoftware und regelmäßige Sicherheitsupdates und Patches in fast allen Unternehmen ab zehn Beschäftigten im Einsatz, wohingegen organisatorische Maßnahmen wie Richtlinien zur IT- und Informationssicherheit oder zum Notfallmanagement, IT-Sicherheitsschulungen, Zertifizierung der IT-Sicherheit, regelmäßige Risiko- und Schwachstellenanalysen sowie Übungen/ Simulationen zum Ausfall wichtiger IT-Systeme weniger weit verbreitet sind. Dieser Befund lässt sich mit den Ergebnissen von Befragung II (2020) bestätigen und weiter schärfen, insofern zusätzliche IT-Sicherheitsmaßnahmen und Einschätzungen zum Reifegrad und der Verbreitung innerhalb der Unternehmen erhoben wurden.[92] Dabei zeigt sich einerseits eine weite Verbreitung dieser Basismaßnahmen, andererseits weist der Reifegrad der eingesetzten Maßnahmen eine große Varianz auf.

Die Anteile der Unternehmen, die bereits die folgenden in Befragung II zusätzlich erhobene IT-Sicherheitsmaßnahmen einsetzen, sind vergleichsweise klein: Zwei-Faktor-Authentifizierung (32,0 %), Security Information and Event Management (21,6 %), Security Operation Center (11,6 %), der Austausch von Bedrohungsdaten (21,2 %), Informationssicherheitsmanagementsysteme (15,2 %) und auf künstlicher Intelligenz basierte Maßnahmen (14,6 %). Dies dürfte darauf zurückzuführen sein, dass diese z.T. erst ab einer gewissen Unternehmensgröße sinnvoll sind und mehr personelle wie finanzielle Ressourcen voraussetzen.

Immerhin etwa zwei Drittel der Unternehmen setzen Verschlüsselung von sensiblen Daten (65,2 %), Verschlüsselung von Kommunikation (60,4 %) und Netzwerksegmentierung (62,6 %) ein, wobei es insbesondere beim Thema Verschlüsselung ebenfalls große Varianz bezüglich des Reifegrades und der Verbreitung innerhalb der Unternehmen gibt.

Während fast alle Unternehmen angeben, regelmäßige Backups durchzuführen (99,6 %) und den Reifegrad bzw. die Verbreitung im Unternehmen dabei meist eher hoch einschätzen, testen lediglich drei Viertel (77,4 %) die Datenwiederherstellung (Restoring). Hinzukommt, dass diese Tests mit meist relativ geringem Reifegrad häufig nur einen Teil der Unternehmens-IT einbeziehen.

Mit Beginn der Corona-Krise im ersten Quartal 2020 veränderte sich die Situation für die IT-Sicherheit in den Unternehmen schlagartig. Es wurden ad hoc Möglichkeiten für Homeoffice geschaffen, über zwei Drittel der Unternehmen (68,0 %) boten dies zum Zeitpunkt der Befragung ihren Beschäftigten an. Damit verbunden stieg auch der Anteil der Unternehmen, bei denen die Nutzung privater Soft-/ Hardware für dienstliche Zwecke möglich ist, auf knapp ein Drittel (30,8 %). In etwa jedem achten Unternehmen (12,7 %) hat sich nach Einschätzung der Unternehmensvertreter*innen die Corona-Krise insgesamt negativ auf die IT-Sicherheit ausgewirkt. Etwa ein Fünftel (20,1 %) traf zusätzliche IT-Sicherheitsmaßnahmen aufgrund der veränderten Situation. Dazu zählen insbesondere die Einrichtung

[92] Die Vergleichbarkeit mit den Ergebnissen von Befragung I ist daher nur eingeschränkt möglich, zumal auch der Wortlaut der erneut abgefragten Maßnahmen teilweise angepasst wurde.

und Absicherung weiterer VPN-Zugangsmöglichkeiten und die Anschaffung und Absicherung zusätzlicher Soft- und Hardware für die Arbeit im Homeoffice.

Über die Hälfte der Unternehmen schätzte das Risiko eines schädigenden ungezielten Cyberangriffs in den nächsten zwölf Monaten als sehr/ eher hoch ein. Da das Treffen zusätzlicher IT-Sicherheitsmaßnahmen in einem statistisch signifikanten Zusammenhang mit der wirtschaftlichen Situation der Unternehmen steht, dürfte sich dieses Risiko insbesondere für krisenbedingt geschwächte Unternehmen auch objektiv erhöht haben.

2) Auf welche Cyberangriffsarten musste in den letzten zwölf Monaten reagiert werden?

Insgesamt gaben 59,6 % der Unternehmen an, dass sie in den zwölf Monaten vor der Befragung II (2020) auf mindestens einen (versuchten) Cyberangriff der erfragten Angriffsarten reagieren mussten. Im Vergleich mit den Ergebnissen der ersten Befragung ist dies ein deutlicher Anstieg, denn bezogen auf die zwölf Monate vor Befragung I (2018/19) waren nur 41,1 % aller befragten Unternehmen betroffen bzw. 50,2 % der Unternehmen, die dann auch an der zweiten Befragung teilgenommen haben. Dieser Anstieg der Gesamtprävalenzrate ist zumindest tendenziell in allen Beschäftigtengrößenklassen erkennbar. Ein Branchenvergleich war aufgrund der geringen Fallzahl nur sehr eingeschränkt möglich, weist aber darauf hin, dass die Entwicklung nicht in allen Branchen gleichermaßen stattgefunden zu haben scheint.

Differenziert nach Angriffsarten ließ sich zeigen, dass insbesondere die signifikante Zunahme der Prävalenzraten von Phishing und von sonstiger Schadsoftware hinter dem Anstieg der Gesamtprävalenzrate steht. Während auf diese Angriffsarten in allen Beschäftigtengrößenklassen häufiger reagiert werden musste, veränderten sich die Prävalenzraten anderer Angriffsarten kaum oder lediglich in einzelnen Beschäftigtengrößenklassen. So ist z.B. für größere Unternehmen ab 250 Beschäftigten erkennbar, dass die Belastung durch CEO-Fraud in der letzten Zeit zumindest tendenziell zugenommen hat, während sie in den übrigen Unternehmen stagnierte.

Die Inzidenzraten verdeutlichen noch einmal, dass die überwiegende Mehrzahl aller Cyberangriffe Phishing-Angriffe sind, deren Anteil zwischen den beiden Befragungen I und II auch weiter zugenommen hat. Fast drei Fünftel aller berichteten Cyberangriffe fielen in diese Kategorie (59,7 %), d.h., nicht nur der Anteil der betroffenen Unternehmen ist groß, sondern auch die Häufigkeit der Angriffe, auf die diese reagieren mussten. Im Vergleich dazu scheint die zahlenmäßige Belastung durch Schadsoftware (Spyware, Ransomware und sonstige Schadsoftware) zu stagnieren oder sogar abgenommen zu haben. Dies könnte ein Hinweis darauf sein, dass diese häufiger gezielt und weniger massenhaft erfolgen. Ein weiterer Hinweis dafür ist die Steigerung der Lösegeldsummen, die von den Täter*innen zur Beendigung der Angriffe gefordert wurden. Diese erhöhten sich bezogen auf die berichteten schwerwiegendsten Cyberangriffe mit Lösegeldforderung im Median von 4.800 EUR (Befragung I) auf 14.400 EUR (Befragung II). Insbesondere der Anteil der Lösegeldforderungen unter 1.000 EUR nahm dabei deutlich ab.

In Hinblick auf die Frage, wie die schwerwiegendsten Cyberangriffe entdeckt wurden, zeigte sich, dass die Mehrzahl der berichteten Angriffe (88,7 %) durch Beschäftigte in den

Unternehmen entdeckt wurden, meist im Rahmen von regulären Sicherheitsmaßnahmen oder Kontrollen (64,7 %). Ein Anteil von 15,5 % gab hingegen an, dass der berichtete Angriff erst durch den Eintritt negativer Auswirkungen erkannt wurde und bei weiteren 11,5 % spielte der Zufall eine entscheidende Rolle. Dies verweist auf Schwierigkeiten bzw. Verbesserungspotentiale bei der rechtzeitigen Erkennung von Cyberangriffen im Rahmen von geregelten Abläufen. Gefragt nach technischen Maßnahmen, die in erster Linie an der Entdeckung beteiligt waren, gaben zwei Fünftel an, auf den Angriff durch die eingesetzte Antivirensoftware (40,0 %) aufmerksam geworden zu sein, weitere 17,5 % erkannten den Angriff mit Hilfe einer Firewall. Bei immerhin knapp einem Drittel (31,2 %) war keine technische Maßnahme beteiligt.

Erneut zeigte sich, dass die Spannbreite der Kosten, die durch die berichteten schwerwiegendsten Cyberangriffe der vergangenen zwölf Monate verursacht wurden, sehr groß ist (20 EUR bis 3,8 Mio EUR), die Kosten mehrheitlich aber relativ gering ausfielen (Durchschnitt: 7.890 EUR, Median: 500 EUR). Dies wird auch durch die von den Unternehmensvertreter*innen vorgenommene Einschätzung der entstandenen materiellen und nicht-materiellen Schäden gestützt. Insgesamt betrachtet war der Schaden lediglich bei 1,6 % mittelfristig/ deutlich spürbar. Lediglich ein Unternehmen berichtete von einem langfristigen/ hohen nicht-materiellen Schaden. Die Antwortoption „Bestandsgefährdend“ wurde von keinem der teilnehmenden Unternehmen gewählt. Auch wenn die meisten Unternehmen auf Cyberangriffe reagieren müssen, scheinen Vorfälle mit sehr schwerwiegenden kostenintensiven Folgen demnach seltene Ausnahmen zu bleiben.

3) Wie ist das Anzeigeverhalten von betroffenen Unternehmen?

Das Anzeigeverhalten ist weiterhin als gering zu beschreiben. Lediglich 8,5 % der Unternehmen, die Angaben zum schwerwiegendsten Cyberangriff der letzten zwölf Monate machten, zeigten diesen auch an. Diese Quote liegt tendenziell sogar unter der aus Befragung I (11,9 %). Erneut ist zu erkennen, dass große Unternehmen (ab 500 Besch.) häufiger anzeigen als kleinere sowie dass es Unterschiede zwischen den Angriffsarten gibt, wobei Phishing selten und CEO-Fraud oder Spyware-Angriffe vergleichsweise häufig angezeigt werden. Dabei spielt allerdings auch das Tatstadium eine Rolle. Cyberangriffe, die aus Sicht der Unternehmen zumindest teilweise erfolgreich waren, wurden häufiger angezeigt (25,6 %) als Angriffe, die als „nicht erfolgreich“ eingestuft wurden (5,7 %).

Zu dem mit 82,1 % am häufigsten angegebenen Nichtanzeigegrund zählt dementsprechend die Antwortkategorie „Weil kein oder nur geringer Schaden entstanden ist“. Ein weiterhin sehr häufiger Grund dafür ist die fehlende Aussicht auf einen Ermittlungserfolg (52,8 %) und die Unsicherheit, an wen man sich für eine Anzeige genau wenden muss (17,1 %). Letzteres wurde insbesondere von kleinen Unternehmen (10-49 Besch.) angegeben, bei denen weiterhin ein Informationsdefizit zu bestehen scheint.

4) Gibt es einen Zusammenhang zwischen der Betroffenheit von Cyberangriffen und dem Vorhandensein bestimmter IT-Sicherheitsmaßnahmen?

Etliche der erfragten IT-Sicherheitsmaßnahmen stehen (ohne Kontrolle der Beschäftigtengrößenklasse) positiv im Zusammenhang mit der Betroffenheit von Cyberangriffen, d.h. mit dem Erleben mindestens eines Cyberangriffs in den letzten zwölf Monaten, auf den reagiert werden musste. Dazu zählen insbesondere schriftliche Richtlinien zur Informations- bzw. IT-Sicherheit, Risiko- und Schwachstellenanalysen (auch Pentest), Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme, aktive Überwachung der Verfügbarkeit und zeitnahe Installation von Sicherheitsupdates, Netzwerksegmentierung, Austausch von Bedrohungsdaten (z.B. Threat Intelligence Dienste) sowie die Auslagerung der IT-Security an externe Dienstleister. Dies wurde nach weiteren Gruppenvergleichen so interpretiert, dass mit diesen Maßnahmen die Aufmerksamkeit bzw. die Fähigkeiten zur Detektion von Cyberangriffen steigen. Denn wenn diese Maßnahmen in Zusammenhang mit dem Erleben eines als (teilweise) erfolgreich bewerteten Cyberangriffs gesetzt werden, ändern sich fast durchgehend die Vorzeichen. Insbesondere schriftliche Richtlinien zur Informations- bzw. IT-Sicherheit, Risiko- und Schwachstellenanalysen (auch Penetrationtesting), Verschlüsselung von sensiblen Daten und die Auslagerung der IT-Security an externe Dienstleister stehen mit einer geringeren Wahrscheinlichkeit in Zusammenhang, einen Cyberangriff zu erleben, der das Versuchsstadium überschreitet. Demgemäß zeigte sich, dass Unternehmen mit besonderen Produkten, Herstellungsverfahren oder Dienstleistungen bzw. mit besonderer Reputation oder Kundenkreis, die im Gegensatz zu anderen Unternehmen häufiger auf diese IT-Sicherheitsmaßnahmen setzen, auch häufiger (versuchte) Angriffe detektierten aber deutlich seltener einen (teilweise) erfolgreichen Cyberangriff erlebten.

Dass der Mensch eine zentrale Rolle innerhalb der IT-Sicherheit der Unternehmen spielt,[93] wird an drei Punkten besonders deutlich: Erstens handelt es sich beim Großteil der berichteten Cyberangriffe um Phishing-Angriffe, die auf eine Täuschung von IT-Anwender*innen z.B. zur Erlangung sensibler Informationen abzielen. Auf der anderen Seite wird, zweitens, die Mehrzahl der Angriffe von den Beschäftigten der Unternehmen entdeckt und das häufig auch ohne Beteiligung technischer Maßnahmen. Und drittens können viele technische und organisatorische IT-Sicherheitsmaßnahmen erst eine Wirkung entfalten, wenn diese (richtig) „genutzt“ werden: Insbesondere Richtlinien zur IT-Sicherheit müssen innerhalb der Unternehmen gelebt werden, mit Übungen und Simulationen lassen sich die Aufmerksamkeit und Reaktionsfähigkeit von Beschäftigten gegenüber Cyberangriffen steigern und sinnvolle technische Maßnahmen wie Verschlüsselungen müssen – ihre gute Nutzbarkeit vorausgesetzt[94] – angewendet werden. Die Verschlüsselung von Kommunikation ist im Übrigen die einzige der erhobenen Maßnahmen, die sowohl negativ mit dem Erleben mindestens eines (versuchten) Angriffs als auch mit dem Erleben eines (teilweise) erfolgreichen Angriffs in Zusammenhang steht. Dies spricht mit aller Vorsicht dafür, dass eine

[93] Zum Faktor Mensch in der TI-Sicherheit siehe z.B. Akdemir & Lawless (2020).

[94] Zum Thema „Usable Security“ siehe z.B. Adams & Sasse (1999); Nurse et al. (2011); Sasse et al. (2001).

derartige Verschlüsselung bereits Angriffsversuche unterbinden bzw. die Erfolgsaussichten für die Täter*innen verringern kann.

Wie bereits Befragung I unterliegt auch Befragung II verschiedenen Einschränkungen, die bei der Interpretation der Ergebnisse beachtet werden müssen. Die Stichprobenziehung erfolgte aus Gründen der telefonischen Erreichbarkeit beim Erstkontakt nicht direkt aus der Grundgesamtheit. Ob sowohl die Auswahlgesamtheit, d.h. die Unternehmen in den genutzten Firmendatenbanken, als auch die Stichprobe der Grundgesamtheit entsprechen, konnte nur an einigen wichtigen Unternehmensmerkmalen wie z.B. Beschäftigtengrößenklasse, Branche und Bundesland des Unternehmensstandortes überprüft und trotz des großen Ausfalls an Teilnehmer*innen in Befragung II bestätigt werden. Auch in dieser Folgebefragung hat jeweils nur eine Person als Repräsentant*in für das Unternehmen teilgenommen. Die Antworten spiegeln somit deren individuellen Wissensstand wider und sind zumindest teilweise subjektive Einschätzungen, die bezüglich erlebter Cyberangriffe retrospektiv erhoben wurden und verzerrt sein können. Aufgrund der großen Anzahl an Cyberangriffen, von denen ein Unternehmen im Laufe eines Jahres betroffen sein kann, konnten nur zu einem, d.h. dem als „schwerwiegendsten“ bewerteten, Cyberangriff Detailfragen gestellt werden.

Trotz dieser, mit der Erhebungsmethode verbundenen, Einschränkungen, liegen – soweit wir sehen – erstmals längsschnittliche Daten zum Thema Cyberangriffe gegen Unternehmen in Deutschland vor, die unabhängig und nach wissenschaftlichen Standards erhoben und ausgewertet wurden. Damit sind Schlussfolgerungen zur Entwicklung z.B. hinsichtlich der Belastung von Cyberangriffen oder des Anzeigeverhaltens möglich, die über Erkenntnisse anhand von Hellfelddaten wie der Polizeilichen Kriminalstatistik (PKS) weit hinausgehen. So konnte u.a. gezeigt werden, dass die Belastung durch Cyberangriffe (insbesondere Phishing und sonstige Schadsoftware-Angriffe) zwischen den Jahren 2018 und 2020 gestiegen ist, wobei Vorfälle mit sehr hohen oder sogar bestandsgefährdenden Schäden nach wie vor die Ausnahme sind. Da die Anzeigequote weiterhin sehr gering ausfiel, ist von einem größer gewordenen Dunkelfeld auszugehen. Die Befragung mittels Web Survey in Befragung II machte es zudem möglich, die Komplexität der IT-Sicherheitsstruktur in den Unternehmen detaillierter zu erfassen und zu untersuchen. Dabei zeigten sich trotz fast überall zum Einsatz kommender basaler technischer IT-Sicherheitsmaßnahmen z.T. große qualitative Unterschiede. Wie sich der Reifegrad der jeweiligen IT-Sicherheitsmaßnahmen und deren Verbreitung innerhalb der jeweiligen Unternehmen auf die IT-Sicherheit der Unternehmen auswirken, werden weitere multivariate Auswertungen zeigen. Dabei soll ebenfalls untersucht werden, ob sich die ersten bivariaten Ergebnisse zum Zusammenhang von IT-Sicherheitsmaßnahmen und der Betroffenheit von (versuchten) Cyberangriffen erhärten lassen.

Da auch mit dieser Studie nur einige Fragen zur IT-Sicherheit von Unternehmen sowie zu den Risiko- und Schutzfaktoren im Zusammenhang mit verschiedenen Cyberangriffsarten ansatzweise beantwortet werden können, ist weitere Forschung zu diesen Themen notwendig und

wünschenswert.[95] Dies gilt nicht zuletzt vor dem Hintergrund einer schnellen technischen Entwicklung, die neben neuen Chancen und Möglichkeiten immer auch neue Risiken für Unternehmen in einer digitalisierten Welt mit sich bringen werden.[96]

Abschließend bedanken wir uns noch einmal herzlich bei allen Projektbeteiligten und besonders bei allen Unternehmen und ihren Vertreter*innen, die an den Befragungen teilgenommen haben, für ihre Unterstützung!

[95] Vgl. dazu auch Maimon & Louderback (2019: 202).

[96] Siehe z.B. Trend Micro Research (2020) zur Entwicklung von künstlicher Intelligenz im Zusammenhang mit Cyberangriffen.

ANHANG 1: ANSCHREIBEN

Sehr geehrte Damen und Herren,

vor etwa zwei Jahren hat Ihr Unternehmen an einer telefonischen Befragung im Rahmen des vom Bundeswirtschaftsministerium (BMWi) geförderten Forschungsprojektes Cyberangriffe gegen Unternehmen teilgenommen und sich bereit erklärt, auch an der Wiederholungsbefragung innerhalb des Forschungsprojektes teilzunehmen.

Zu der Wiederholungsbefragung, die uns Aufschluss über Entwicklungen hinsichtlich der Risiken von Cyberangriffen auch in Zeiten der Corona-Krise geben soll, möchten wir Sie nun herzlich einladen.

Die Befragung erfolgt online mit wissenschaftlichen Standards, dauert durchschnittlich rund 20 Minuten (zeitliche Unterbrechung und spätere Fortsetzung sind möglich) und ist über folgenden individuellen Link zu erreichen: Individueller_Link

Wie schon bei der ersten Befragung werden Ihre Antworten nur anonym und in aggregierter Form ausgewertet. Es sind keine Rückschlüsse auf Ihr Unternehmen möglich.

Auf Wunsch bekommen Sie gern die Ergebnisse dieser Wiederholungsbefragung zugesendet.

Wir danken Ihnen sehr für Ihre Unterstützung und die erneute Teilnahme.

Als Ansprechpartner steht Ihnen Arne Dreißigacker vom Kriminologischen Forschungsinstitut Niedersachsen (KFN) zur Verfügung (arne.dreissigacker@kfn.de, Tel: 0511/3483628)

Mit freundlichen Grüßen

Prof. Dr. Sascha Fahl (Teilprojektleiter Leibniz-Universität Hannover) und Dipl.-Soz. Arne Dreißigacker (Teilprojektleiter KFN)

Den Forschungsbericht zur ersten Befragung (Lang- und Kurzfassung) sowie weitere Ergebnisse und Informationen zum Forschungsprojekt finden Sie hier: https://kfn.de/forschungsprojekte/cyberangriffe-gegen-unternehmen/

Klicken Sie auf folgenden Link, wenn sie von uns keine E-Mails mehr erhalten wollen: Aus der Liste austragen

ANHANG 2: ERINNERUNGSSCHREIBEN

Sehr geehrte Damen und Herren,

sofern Sie bereits an der zweiten Unternehmensbefragung im Rahmen des vom Bundeswirtschaftsministerium (BMWi) geförderten Forschungsprojektes **Cyberangriffe gegen Unternehmen** teilgenommen haben, bedanken wir uns herzlich bei Ihnen. Dann betrachten Sie bitte dieses zweite Erinnerungsschreiben als gegenstandslos.

Falls Sie es bisher nicht geschafft haben sollten, an der Befragung teilzunehmen, bitten wir Sie, dies noch zu tun. Gerne senden wir Ihnen noch einmal Ihren individuellen Link: Individueller Link

Bitte geben Sie mir Bescheid (arne.dreissigacker@kfn.de, Tel: 0511/3483628), wenn Sie Probleme mit dem Link haben sollten, z.B. wenn Sie diese E-Mail innerhalb Ihres Unternehmens weitergeleitet bekommen haben und der Link nicht mehr funktioniert. Dann wird für Sie ein neuer individueller Link generiert. Dieses Verfahren ist notwendig, um die Möglichkeit von Mehrfachteilnahmen auszuschließen.

Ihre Unterstützung ist für dieses Forschungsprojekt außerordentlich wichtig und wir sind Ihnen dafür sehr dankbar. Denn nur wenn uns Unternehmen über erlebte Cyberangriffe Auskunft geben, ist es uns möglich, etwas über dieses Thema zu erfahren und zur Verbesserung der IT-Sicherheit von Unternehmen in Deutschland mit wissenschaftlichen Ergebnissen beizutragen.

Die Online-Befragung erfolgt mit wissenschaftlichen Standards und der Umfragesoftware Qualtrics, dauert durchschnittlich rund 20 Minuten. Eine zeitliche Unterbrechung und spätere Fortsetzung sind möglich. Ihre Antworten werden nur anonym und in aggregierter Form ausgewertet. Es sind keine Rückschlüsse auf Ihr Unternehmen möglich.

Mit freundlichen Grüßen

Arne Dreißigacker (Teilprojektleiter KFN)

Klicken Sie auf folgenden Link, wenn sie von uns keine E-Mails mehr erhalten wollen: Aus der Liste austragen

ANHANG 3: FRAGEBOGEN

Kurzdarstellung des eingesetzten Fragebogens

A Einstieg

A00 Haben Sie persönlich bereits in der ersten Befragung für ihr Unternehmen teilgenommen?
(Ja;Nein; Weiß nicht; Keine Angabe)

A01 In welchem Bereich sind Sie in Ihrem Unternehmen tätig?
(Geschäftsführung/ Vorstand; IT, IT-Sicherheit oder Informationssicherheit; Governance & Datenschutz; Sonstiges; Weiß nicht; Keine Angabe [Mehrfachantworten möglich])

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 Bezogen auf die letzten 12 Monate: Von welchen Angriffsarten war Ihr Unternehmen 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; Sonstiger Cyberangriff; kein Angriff erlebt, auf den reagiert werden musste; Weiß nicht; Keine Angabe [Mehrfachantworten möglich])

B01a Wie häufig war Ihr Unternehmen von diesen Angriffsarten in den letzten 12 Monaten betroffen und musste aktiv reagieren?
(Ransomware-Angriff (um Daten zu verschlüsseln); Spyware-Angriff (um Daten auszuspähen); Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner); Manuelles Hacking (um Soft- und Hardware zu manipulieren); (D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten); Defacing-Attacke (um Inhalte von Websites zu verändern); CEO-Fraud (Vortäuschung einer Führungspersönlichkeit); Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten); Sonstiger Cyberangriff), Antwortmöglichkeiten: (Anzahl [nummerisch])

B05 Welcher Cyberangriff der letzten 12 Monate war der schwerwiegendste? (Mehrfachantwort bei einer Kombination von mehreren Angriffsarten möglich)
(Ransomware-Angriff (um Daten zu verschlüsseln); Spyware-Angriff (um Daten auszuspähen); Sonstiger Angriff mit Schadsoftware (Viren, Würmer, Trojaner); Manuelles Hacking (um Soft- und Hardware zu manipulieren); (D)DoS-Attacke (um Web- oder E-Mail-Server zu überlasten); Defacing-Attacke (um Inhalte von Websites zu verändern); CEO-Fraud (Vortäuschung einer Führungspersönlichkeit); Phishing (Täuschung mit echt aussehenden E-Mails oder Webseiten); Sonstiger Cyberangriff; Weiß nicht; Keine Angabe [Mehrfachnennung möglich])

B19 War „Emotet“ an diesem Angriff beteiligt?
(Ja; Nein; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B32 Stand dieser Angriff im Zusammenhang mit der Corona-Krise?
(Ja; Nein; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B23 Wer hat diesen Angriff bzw. Hinweise darauf erstmalig entdeckt?
(Beschäftigte des Unternehmens; Externe Dienstleister des Unternehmens; Sonstige Geschäftspartner; Kunden; Aufsichts- oder Sicherheitsbehörden; Sonstige Dritte [mit Freitext]; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B22 Wie wurde dieser Angriff erstmalig entdeckt?
(Durch reguläre Sicherheitsmaßnahmen oder Kontrollen; Durch Eintritt negativer Auswirkungen; Zufällig, Sonstiges [mit Freitext]; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B24 Welche technische IT-Sicherheitsmaßnahme war in erster Linie an der Entdeckung des Angriffs beteiligt?
(Keine; Firewall; Antivirus; Intrusion Detection System (IDS); Security Information and Event Management (SIEM); Sonstiges [mit Freitext]; Weiß nicht; Keine Angabe[nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B21 Wie viel Zeit ist von der ursprünglichen Infektion/Anbahnung bis zur Entdeckung des Angriffes vergangen?
(Stunden und zwar (Dauer in Stunden): [nummerische Angabe]; Tage und zwar (Dauer in Tagen): [nummerische Angabe]; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B29 Wie lange hat der Angriff, von der erstmaligen Entdeckung bis zur Abwehr bzw. Wiederherstellung der wesentlichen Prozesse insgesamt gedauert?
(Stunden und zwar (Dauer in Stunden): [nummerische Angabe]; Tage und zwar (Dauer in Tagen): [nummerische Angabe]; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B25 War der Angriff aus Ihrer Sicht für die Angreifer erfolgreich?
(Ja; Teilweise; Nein; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B08 Gab es bei diesem Angriff eine Lösegeld-Forderung? Wie hoch war diese? (Falls es mehrere Forderungen bei diesem Angriff gab, bitte summieren)
(Ja [mit nummerischer Angabe in EUR]; Nein; Weiß nicht; Keine Angabe [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B10 Waren folgende IT-Systeme vom schwersten Angriff betroffen?
(Standard-Arbeitsplatz und Office IT; E-Mail und Kommunikation (z.B. Partner-Portale, Netzspeicher); Webauftritt (z.B. online-Marktplätze, Shops, Kundenportale); Auftrags- und Kundenverwaltung (z.B. Termin- und Reservierungssysteme, Rechnungsverwaltung); Produktionssteuerung (Fokus auf Maschinen- und Anlagensteuerung); Lager & Logistik; Banking & Trading; Rechnungswesen, Controlling (z.B. für Jahresabschluss, Berichtserstellung); IT-Sicherheitssysteme (z.B. Firewalls, SIEM); Sonstige Systeme (z.B. Projektplanung, CAD, Berechnungen von Statik) [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; keine Angabe)

B10a Wie wichtig ist dieses betroffene IT-Systeme für Ihr Unternehmen?
(Standard-Arbeitsplatz und Office IT; E-Mail und Kommunikation; Webauftritt; Auftrags- und Kundenverwaltung; Produktionssteuerung; Lager & Logistik; Banking & Trading; Rechnungswesen, Controlling; IT-Sicherheitssysteme; Sonstige Systeme [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: ((eher) unwichtig; (eher) wichtig; Weiß nicht; keine Angabe)

B10b Wie lange konnte das betroffene System (schätzungsweise) nicht oder nur stark eingeschränkt genutzt werden? (Ausfallzeit in Tagen; 0,5=12 Stunden)
(Standard-Arbeitsplatz und Office IT; E-Mail und Kommunikation; Webauftritt; Auftrags- und Kundenverwaltung; Produktionssteuerung; Lager & Logistik; Banking & Trading; Rechnungswesen, Controlling; IT-Sicherheitssysteme; Sonstige Systeme [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Ausfallzeit in Tagen [nummerische Angabe])

B30 Waren Produkte oder Dienstleistungen für Ihre Kunden betroffen?
(Technische und vernetzte Produkte (z.B. Fahrzeuge, Wearables, mobile Endgeräte); Dienstleistungen (z.B. bereitgestellter Cloud-Speicher, gehostete IT-Systeme) [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; keine Angabe)

B30a Wie lange konnten diese (schätzungsweise) nicht oder nur stark eingeschränkt durch Ihre Kunden genutzt werden?
(Technische und vernetzte Produkte (z.B. Fahrzeuge, Wearables, mobile Endgeräte); Dienstleistungen (z.B. bereitgestellter Cloud-Speicher, gehostete IT-Systeme) [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Ausfallzeit in Tagen (0,5=12 Stunden) [nummerische Angabe])

B12 Sind durch diesen Cyberangriff materielle Schäden für folgende Positionen entstanden?
(Kosten durch externe Beratung (z.B. IT-Dienstleister, Rechtsberatung); Schadensersatz/ Strafen; Abgeflossene Gelder; Kosten für Wiederbeschaffung/ Wiederherstellung von Soft- oder Hardware (keine Personalkosten); Personalkosten für die Behebung des Problems (Abwehr & Aufklärung); Betriebsunterbrechung/ Umsatzverlust (z.B. durch Mitarbeiter, die nicht arbeiten konnten oder Systeme, die ausfielen) [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; keine Angabe)

B12a Wie hoch waren die materiellen Schäden (schätzungsweise) für diese Position in Euro?
(Kosten durch externe Beratung (z.B. IT-Dienstleister, Rechtsberatung); Schadensersatz/ Strafen; Abgeflossene Gelder; Kosten für Wiederbeschaffung/ Wiederherstel-

lung von Soft- oder Hardware (keine Personalkosten); Personalkosten für die Behebung des Problems (Abwehr & Aufklärung); Betriebsunterbrechung/ Umsatzverlust (z.B. durch Mitarbeiter, die nicht arbeiten konnten oder Systeme, die ausfielen) [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Kosten in Euro [nummerische Angabe])

B26 Wie schwerwiegend schätzen Sie die verursachten Schäden dieses Angriffes insgesamt ein?
(Materieller Schaden insgesamt; Nicht-materieller Schaden (z.B. Reputationsverlust oder Wettbewerbsnachteil) [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Kein derartiger Schaden; Kurzfristig/gering; Mittelfristig/deutlich spürbar; Langfristig/hoch; Bestandsgefährdend; Weiß nicht; Keine Angabe)

B27 Für die Zeit bis zur Beseitigung des Vorfalls:
(Mussten Mitarbeiter aufgrund des Vorfalls ihre Arbeit unterbrechen?; Haben Mitarbeiter aktiv an der Beseitigung des Vorfalls gearbeitet? [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; keine Angabe)

B27a Wie viele Mitarbeiter haben aufgrund des Vorfalls ...
(... ihre Arbeit unterbrochen?; ... aktiv an der Beseitigung des Vorfalls gearbeitet? [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Anzahl [nummerische Angabe])

B27b Wie lange haben Mitarbeiter im Durchschnitt...
(... ihre Arbeit unterbrochen?; ... aktiv an der Beseitigung des Vorfalls gearbeitet? [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Tage pro Mitarbeiter (0,5=12 Stunden) [nummerische Angabe])

B11 Waren durch den Angriff folgende Daten betroffen?
(Personenbezogene Daten; Strategie-, Vertriebs- und Finanzinformationen (z.B. Preislisten, Sanierungspläne, Akquisitionen, Finanz- und Rechnungswesendaten); Produktdaten (z.B. Konstruktionspläne, Rezepturen, Quellcodes etc.); Sonstige wichtige Daten [nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate]), Antwortmöglichkeiten: (Ja; Nein; Weiß nicht; keine Angabe)

B31 Von welchen Gruppen waren sensible Daten betroffen?
(Kunden; Mitarbeiter; Geschäftspartner; Sonstige [mit Freitext]; Weiß nicht; Keine Angabe [Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

B14 An welche staatlichen Stellen bzw. Behörden haben Sie sich wegen dieses Vorfalls gewandt?
(An keine staatliche Stelle; Nächste Polizeidienststelle; Auf Cybercrime spezialisierte Polizeidienststelle (ZAC); Verfassungsschutz; Bundesamt für Sicherheit in der Informationstechnik (BSI); Landesdatenschutzbeauftragte/r; Sonstige staatliche Stelle/ Behörde; Weiß nicht; Keine Angabe [Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate])

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), 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; Weil der Schaden gering war; Fehlende Aussicht auf Ermittlungserfolg; Wusste nicht, an wen man sich dafür wenden muss; Sonstiges [mit Freitext]; Weiß nicht; Keine Angabe [Mehrfachantworten möglich; nur zum schwerwiegendsten Cyberangriff der letzten 12 Monate und bei Nichtanzeige])

C IT-Sicherheitsstrukturen

C01 Welche der folgenden IT-Sicherheitsmaßnahmen gibt es in Ihrem Unternehmen? Geben Sie bitte gegebenenfalls an, ob die Maßnahme erst nach dem schwerwiegendsten Angriff der letzten 12 Monate eingeführt wurde.
(Schriftliche Richtlinien zur Informations- bzw. IT-Sicherheit; Schriftliche Richtlinien zum Notfallmanagement; Zertifizierung der IT-Sicherheit (z.B. nach ISO 27001 o. VdS 3473); Risiko- und Schwachstellenanalysen (auch Pentest); Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme; Mindestanforderungen für Passwörter; Zwei-Faktor Authentifizierung; Individuelle Vergabe von Zugangs- und Nutzerrechten; Regelmäßige Backups; Test der Datenwiederherstellung (Restoring); Antivirensoftware; Aktive Überwachung der Verfügbarkeit und zeitnahe Installation von Sicherheitsupdates; Schutz der IT-Systeme mit einer Firewall; Netzwerksegmentierung; Security Information and Event Management (SIEM); Security Operation Center (SOC); Austausch von Bedrohungsdaten (z.B. Threat Intelligence); Künstliche Intelligenz basierte Maßnahmen; Informationssicherheitsmanagementsystem (ISMS); Verschlüsselung von Kommunikation; Verschlüsselung von sensiblen Daten; Verstärkte physische Sicherheit), Antwortmöglichkeiten: (Ja; Ja, aber erst nachher; Nein; Weiß nicht; keine Angabe)

C18 Bitte schätzen Sie den Reifegrad und die Verbreitung bzw. den Geltungsbereich der vorhandenen IT-Sicherheitsmaßnahmen im Unternehmen ein. Geben Sie bitte an, was am ehesten für Ihr Unternehmen zutrifft.
(Schriftliche Richtlinien zur Informations- bzw. IT-Sicherheit; Schriftliche Richtlinien zum Notfallmanagement; Zertifizierung der IT-Sicherheit (z.B. nach ISO 27001 o. VdS 3473); Risiko- und Schwachstellenanalysen (auch Pentest); Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme; Mindestanforderungen für Passwörter; Zwei-Faktor Authentifizierung; Individuelle Vergabe von Zugangs- und Nutzerrechten; Regelmäßige Backups; Test der Datenwiederherstellung (Restoring); Antivirensoftware; Aktive Überwachung der Verfügbarkeit und zeitnahe Installation von Sicherheitsupdates; Schutz der IT-Systeme mit einer Firewall; Netzwerksegmentierung; Security Information and Event Management (SIEM); Security Operation

Center (SOC); Austausch von Bedrohungsdaten (z.B. Threat Intelligence); Künstliche Intelligenz basierte Maßnahmen; Informationssicherheitsmanagementsystem (ISMS); Verschlüsselung von Kommunikation; Verschlüsselung von sensiblen Daten; Verstärkte physische Sicherheit), Antwortmöglichkeiten Reifegradskala: (1: Grundfunktionalität/-umfang; 2: Erweiterte Funktionalität/ Umfang; 3: Grundfunktionalität +regelmäßige Überprüfung/ Optimierung; 4: Erweiterte Funktionalität +regelmäßige Überprüfung/ Optimierung), Antwortmöglichkeiten Verbreitung/Geltungsbereich im Unternehmen: (stark begrenzt; teilweise; weitgehend)

C13 Inwiefern treffen folgende Aussagen zur IT-Sicherheitsschulung für Ihr Unternehmen zu?
(Alle Beschäftigten werden mindestens jährlich geschult; Ausgewählte Beschäftigte werden mindestens jährlich geschult; Es existieren Maßnahmen zur Erfolgskontrolle/Vertiefung der Schulungen), Antwortmöglichkeiten: (Trifft gar nicht zu; Trifft eher nicht zu; Trifft eher zu; Trifft voll und ganz zu; Weiß nicht; Keine Angabe)

C03 Haben Sie eine Versicherung gegen Informationssicherheitsverletzungen (Cyberversicherung)
(Ja; Nein; Weiß nicht; Keine Angabe)

C14 Musste zum Abschluss der Cyberversicherungen bestimmte IT-Sicherheitsstandards nachgewiesen werden?
(Ja; Nein; Weiß nicht; Keine Angabe)

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), Antwortmöglichkeiten: (Trifft gar nicht zu; Trifft eher nicht zu; Trifft eher zu; Trifft voll und ganz zu; Weiß nicht; Keine Angabe)

C15 Wie würden Sie den Umgang mit Fehlern und Problemen in Ihrer Organisation beschreiben?
(Mitarbeitern wird es ermöglicht Fehler und Probleme effizient zu melden; Mitarbeiter werden ermutigt Fehler und Probleme zu melden; Meldungen werden ernst genommen und behandelt), Antwortmöglichkeiten: (Trifft gar nicht zu; Trifft eher nicht zu; Trifft eher zu; Trifft voll und ganz zu; Weiß nicht; Keine Angabe)

C16 Wie gut schätzen Sie die Informationssicherheit in Ihrem Unternehmen insgesamt ein?
(Sehr schlecht; Eher schlecht; Eher gut; Sehr gut; Weiß nicht; Keine Angabe)

C17 Was steht einer höheren Informationssicherheit in Ihrem Unternehmen im Wege?
(Nichts; Zu wenig Zeit; Zu wenig Budget; Andere Prioritäten der Geschäftsführung; Fehlende Fähigkeit/ Kompetenzen; Fehlende gesetzliche Rahmenbedingungen; Mangel an Informationen; Sonstiges [mit Freitext]; Weiß nicht; Keine Angabe [Mehrfachantworten möglich])

D Unternehmensmerkmale

D09 Wie viele Mitarbeiter hat Ihr Unternehmen? Wenn Sie es nicht genau wissen, geben Sie bitte einen Schätzwert an.
(Anzahl [nummerische Angabe])

D07 Welche IT-Funktionen werden von einem externen Dienstleister erbracht (Outsourcing)?
(Keine 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 [mit Freitext]; Weiß nicht; Keine Angabe [Mehrfachantworten möglich])

D10 Wie schätzen Sie die wirtschaftliche Gesamtsituation Ihres Unternehmens ein?
(Vor der Corona-Krise; Aktuell), Antwortmöglichkeiten: (Sehr gut; Eher gut; Eher angespannt; Sehr angespannt; Weiß nicht; Keine Angabe)

E Corona-Fragen

E01 Gab es folgende Möglichkeiten bereits vor der Corona-Krise und wie haben sie sich seither verändert?
(Homeoffice; Mitarbeiter nutzen private Soft-/Hardware), Antwortmöglichkeiten Vorhandensein: (Ja; Nein; Weiß nicht; Keine Angabe), Antwortmöglichkeiten Veränderung: (Viel weniger; Eher weniger; Unverändert; Eher mehr; Viel mehr; Weiß nicht; Keine Angabe)

E02 Inwiefern treffen folgende Aussagen auf Ihr Unternehmen seit der Corona-Krise zu?
(IT-Mitarbeiter sind ausgefallen oder können nur sehr eingeschränkt arbeiten; Veränderte Kommunikationswege und -gewohnheiten sind problematisch für die IT-Sicherheit (unverschlüsselte E-Mails, Messaging Apps etc.), Wachsamkeit gegenüber den Gefahren aus dem Internet hat krisenbedingt abgenommen; Bestehende Verhaltensrichtlinien zur IT-Sicherheit können im Homeoffice nicht eingehalten werden (z.B. Zwei-Faktor-Verschlüsselung); IT-Sicherheitsrichtlinien und Vorgaben wurden auf die neue Situation angepasst; Das Thema IT-Sicherheit hat für die Geschäftsführung krisenbedingt an Bedeutung verloren; Die Corona-Krise hat sich insgesamt negativ auf die IT-Sicherheit des Unternehmens ausgewirkt; Unser Information Security Management System (ISMS) oder Business Continuity Management (BCM) hat geholfen die Auswirkungen der Corona-Krise zu bewältigen), Antwortmöglichkeiten: (Trifft gar nicht zu; Trifft eher nicht zu; Trifft eher zu; Trifft voll und ganz zu; Weiß nicht; Keine Angabe)

E03 Welche zusätzlichen IT-Sicherheitsmaßnahmen wurden wegen der Corona-Krise getroffen? Wenn mehrere Maßnahmen getroffen wurden, nennen Sie bitte die drei wichtigsten.
(Maßnahme 1 [mit Freitext]; Maßnahme 2 [mit Freitext]; Maßnahme 3 [mit Freitext]; keine zusätzliche Maßnahme; Weiß nicht; Keine Angabe)

E04 Musste Ihr Unternehmen seit der Corona-Krise auf Cyberangriffe reagieren, die im Zusammenhang mit der Corona-Krise standen?
(Ja; Nein; Weiß nicht; Keine Angabe)

E05 Wie viele der mit der Corona-Krise im Zusammenhang stehenden Cyberangriffe waren in erster Linie ...
(... gezielt auf Mitarbeiter im Homeoffice gerichtet (z.B. Täuschung/ Manipulation)? [nummerische Angabe]; gezielt auf Hard-/Software im Homeoffice gerichtet (z.B. Schadsoftware)? [nummerische Angabe]; sonstige Cyberangriffe? [nummerische 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.

Akdemir, N. & C.J. Lawless, 2020: Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach. Internet Research 30: 1665–1687.

Armin, J., B. Thompson & P. Kijewski, 2016: Cybercrime Economic Costs: No Measure No Solution. S. 135–155 in: B. Akhgar & B. Brewster (Hrsg.), Combatting Cybercrime and Cyberterrorism. Cham: Springer International Publishing.

Bayerl, P.S. & T.-G. Rüdiger, 2018: Braucht eine digitale Gesellschaft eine digitale Polizei? Deutsche Polizei: 4–14.

Bitkom e.V., 2020: Digitalisierung der Wirtschaft. Auswirkung der Corona-Pandemie. Berlin.

Bitkom e.V., 2021: Ein Jahr Corona. Wie digital arbeiten deutsche Unternehmen. Berlin.

Buil-Gil, D., N. Lord & E. Barrett, 2021: The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention. Victims & Offenders 16: 286–315.

Buil-Gil, D., F. Miró-Llinares, A. Moneva, S. Kemp & N. Díaz-Castaño, 2020: Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies: 1–13.

Bundeskriminalamt, 2015: Cybercrime. Bundeslagebild 2015. Wiesbaden.

Callegaro, M., K. Lozar Manfreda & V. Vehovar, 2015: Web Survey Methodology. Los Angeles: Sage Publ.

Cohen, J., 1992: A power primer. Psychological Bulletin 112: 155–159.

Department for Digital, Culture, Media & Sport (DCMS), 2021: Cyber Security Breaches Survey. London, UK.

Dreißigacker, A., B. von Skarczinski & G.R. Wollinger, 2020a: Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019. Hannover.

Dreißigacker, A., B. von Skarczinski & G.R. Wollinger, 2020b: Cyberangriffe gegen Unternehmen: Erste Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland. S. 933–952 in: C. Grafl, M. Stempkowski, K. Beclin & I. Haider (Hrsg.), "Sag, wie hast du's mit der Kriminologie?". Die Kriminologie im Gespräch mit ihren Nachbardisziplinen. Mönchengladbach: Forum Verlag Godesberg.

Dreißigacker, A., B. von Skarczinski & G.R. Wollinger, 2020c: Cyber-attacks against companies in Germany. Results of a representative company survey 2018/2019. Hanover.

Dreißigacker, A., B. von Skarczinski & G.R. Wollinger, 2020d: Im Visier: Repräsentative Studie zur Cyberkriminalität in deutschen Unternehmen. iX - Magazin für professionelle Informationstechnik: 78–81.

Dreißigacker, A. & G.R. Wollinger, 2020: Verbreitung von Cyberkriminalität gegen Unternehmen in Deutschland. S. 89–109 in: G.R. Wollinger & A. Schulze (Hrsg.), Handbuch Cybersecurity für die öffentliche Verwaltung. Wiesbaden: Kommunal- und Schul-Verlag.

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.

Hawdon, J., K. Parti & T.E. Dearden, 2020: Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. American journal of criminal justice : AJCJ 45: 1–17.

Hiscox, 2021: Hiscox Cyber Readiness Report 2021. Don't let cyber be a game of chance. Pembroke, Bermuda.

Huaman, N., B. von Skarczinski, D. Wermke, C. Stransky, Y. Acar, A. Dreißigacker & S. Fahl, 2021: A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. Proceedings of the 30th USENIX Security Symposium.

Huber, E. & B. Pospisil, 2020: Problematik der Hell- und Dunkelfeldanalyse im Bereich Cybercrime. S. 109–133 in: T.-G. Rüdiger & P.S. Bayerl (Hrsg.), Cyberkriminologie. Wiesbaden: Springer Fachmedien Wiesbaden.

Koziarski, J. & J.R. Lee, 2020: Connecting evidence-based policing and cybercrime. Policing: An International Journal 43: 198–211.

Kriminologisches Forschungsinstitut Niedersachsen e. V., 2020: Cyberangriffe gegen Unternehmen. Ergebnisse einer repäsentativen Unternehmensbefragung 2018/2019. Kurzbericht. Hannover.

Lamprecht, S. & G. Vladova, 2020: Cyber-Viktimisierung von Unternehmen. S. 345–371 in: T.-G. Rüdiger & P.S. Bayerl (Hrsg.), Cyberkriminologie. Wiesbaden: Springer Fachmedien Wiesbaden.

Maimon, D. & E.R. Louderback, 2019: Cyber-Dependent Crimes: An Interdisciplinary Review. Annual Review of Criminology 2: 191–216.

Minnaar, A., 2020: 'Gone phishing' : the cynical and opportunistic exploitation of the Coronavirus pandemic by cybercriminals. Acta Criminologica : African Journal of Criminology & Victimology 33: 28–53.

Naidoo, R., 2020: A multi-level influence model of COVID-19 themed cybercrime. European Journal of Information Systems 29: 306–321.

Neubert, C., A. Stiller, T. Bartsch, A. Dreißigacker, A. Isenhardt, Y. Krieg, P. Müller & B. Zietlow, 2020: Kriminalität in der Corona-Krise: Haben die aktuellen Maßnahmen zur Eindämmung des Coronavirus möglicherweise einen Einfluss auf die Kriminalitätsentwicklung in Deutschland? Kriminologie - Das Online-Journal (KrimOJ) 2: 338–371.

Nurse, J.R.C., S. Creese, M. Goldsmith & K. Lamberts, 2011: Guidelines for usable cybersecurity: Past and present. Mailand.

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.

Pawlowska, A. & B. Scherer, 2021: IT-Sicherheit im Home-Office unter besonderer Berücksichtigung der COVID-19 Situation. Ergebniskurzbericht einer repräsentativen Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Bonn.

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.

Schmidt, J., 2020: Cyber-Erpresser versprechen Corona-Pause für Krankenhäuser. heise-online, 19.03.2020. https://www.heise.de/newsticker/meldung/Cyber-Erpresser-versprechen-Corona-Pause-fuer-Krankenhaeuser-4686021.html (16.4.2021).

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. Band 2 - Methodik und Methodologie. Wiesbaden: BKA.

Skarczinski, B. von, L. Boll & F. Teuteberg, 2021: Understanding the adoption of cyber insurance for residual risks. An empirical large-scale survey on organizational factors of the demand side. ECIS 2021 Research Papers.

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.

Steeh & Charlotte, 2008: Telephone surveys. S. 221–238 in: E.D. de Leeuw, J.J. Hox & D.A. Dillman (Hrsg.), International Handbook of Survey Methodology. New York, NY: Psychology Press.

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 155. Hannover.

Trend Micro Research, 2020: Malicious Uses and Abuses of Artificial Intelligence.

Urban, D. & J. Mayerl, 2011: Regressionsanalyse. Theorie, Technik und Anwendung. Wiesbaden: VS Verl. für Sozialwiss.

ISBN: 978-3-948647-11-7