UNIVERSITÄT BERN

Rechtswissenschaftliche Fakultät

Institut für Strafrecht und Kriminologie

Bern, 31.8.2022

Befragung zur Sicherheit in Unternehmen bezüglich digitaler und physischer Angriffe

Auswertungsbericht zuhanden des Verbands Swissmem

Anna Isenhardt[1], Louise Frey[2], Ueli Hostettler[3]

[1] Dr. phil., Kriminologin, Ko-Projektleitung

[2] BA, Sozialanthropologin, Projektmitarbeiterin

[3] Prof. Dr. habil., Sozialanthropologe, Ko-Projektleitung (ueli.hostettler@krim.unibe.ch)

Zitiervorschlag:
Isenhardt, Anna, Frey, Louise & Hostettler, Ueli (2022). Befragung zur Sicherheit in Unternehmen bezüglich digitaler und physischer Angriffe. Auswertungsbericht zuhanden des Verbands Swissmem. Bern: Universität Bern – Institut für Strafrecht und Kriminologie.

Inhaltsverzeichnis

1 Hintergrund

Die Universität Bern wurde vom Verband Swissmem beauftragt, eine Online-Befragung zum Thema Sicherheit in der MEM-Industrie unter ihren Mitgliedern durchzuführen. Partner des Projekts ist die Initiative Industrie 2025. Die Studie wurde in Vorbereitung auf den Swissmem-Industrietag im Jahr 2022 erarbeitet. Inhalt der Studie waren, neben der Abfrage der Betroffenheit durch verschiedene Arten von digitalen und physischen Angriffen, insbesondere auch die von den befragten Firmen eingesetzten Schutz- und Interventionsmassnahmen, um entsprechende Angriffe zu vermeiden oder auf diese zu reagieren. Berücksichtigt wurden sowohl die Betroffenheit durch Angriffe seit Bestehen des Unternehmens sowie im Verlauf der letzten zwei Jahren vor der Befragung. Die Studie schliesst damit an vorhandene Studien an, in denen ähnliche Erfassungszeiträume abgefragt wurden (siehe z.B. Barth et al., 2020). Gefragt wurde ausserdem nach dem schwerwiegendsten Angriff in den letzten zwei Jahren vor der Befragung gewesen. In Bezug auf diesen schwersten Angriff wurden dann verschiedene Anschlussfragen gestellt, wie bspw. nach den Täterinnen und Tätern, den Folgen, den betroffenen Daten oder der Schadenshöhe. Welche Themen abgedeckt und welche Fragen im Einzelnen gestellt wurden, kann dem Fragenkatalog im Anhang entnommen werden. Der Fragebogen wurde von den Firmen im Online-Format ausgefüllt.

Die einzelnen Fragen wurden jeweils von unterschiedlich vielen Unternehmen beantwortet. Entweder, weil ihnen einzelne Fragen nicht angezeigt wurden, wenn sie z.B. keinen schwerwiegendsten Angriff angegeben haben und ihnen deshalb keine weiteren Fragen zu diesem gestellt wurden, oder, weil einzelne Fragen nicht beantwortet wurden. Wie viele Unternehmen die Fragen im Einzelnen beantwortet haben, wird im Bericht jeweils angegeben (N=Anzahl). In den Darstellungen können die Prozentangaben rundungsbedingt in der Summe mehr als 100% (z.B. 100.1%) oder weniger als 100% (z.B. 99.9%) betragen.

2 Ergebnisse anderer Studien

Ein Blick auf den aktuellen Forschungsstand zeigt, dass Unternehmen von einer Vielzahl von verschiedenen Arten von Angriffen betroffen sind, bei denen die Unternehmen durch Aktivitäten Dritter mittels illegaler Mittel und in krimineller Absicht geschädigt werden. Dementsprechend gibt es auch vielfältige Untersuchungsmöglichkeiten und entsprechend vielfältig sind auch die Ergebnisse von Studien, die in der näheren Vergangenheit im besagten Themenfeld durchgeführt wurden. Die meisten stimmen jedoch in der Folgerung überein, dass in Zeiten der zunehmenden (digitalen und analogen) Vernetzung die Resilienz der Wirtschaft gegen Gefahren aus dem Cyberraum eine tragende Rolle für Unternehmen spielt. Im Folgenden werden einige ausgewählte Studien und Befunde beleuchtet, um den

vorliegenden Bericht zu kontextualisieren und dessen Anknüpfungspunkte an die aktuellen Forschungsbefunde bezogen auf den deutschsprachigen Raum aufzuzeigen.

2.1 Deutschland

2020 untersuchten Barth et al. im Auftrag des Digitalverbands Bitkom e.V. (wie auch bereits 2015 und 2017) Unternehmen in Deutschland hinsichtlich ihres Wirtschaftsschutzes. Dafür wurden im Jahr 2020 insgesamt 1070 nach Branchen und Grössenklassen repräsentativ ausgewählte Unternehmen mittels eines standardisierten Fragebogens befragt. Die Untersuchung zeigte, dass 75% der befragten Unternehmen in den zwei Jahren vor dem Befragungszeitpunkt von Datendiebstahl, Industriespionage oder Sabotage betroffen waren. Da sich Angriffe nicht immer zweifelsfrei feststellen lassen, gaben weitere 13% an, vermutlich betroffen gewesen zu sein. Für Barth et al. steht darum fest: «Fast die gesamte Industrie Deutschlands ist von Wirtschaftsspionage, Sabotage oder Datendiebstahl (vermutet oder bestätigt) betroffen» (Barth et al. 2020: 7). Zudem haben Umfang und Qualität der Angriffe auf Unternehmen deutlich zugenommen, wie ein Vergleich mit 2015 und 2017 zeigt: Damals gab nur gut jedes zweite Unternehmen an, von Besagtem betroffen zu sein. Diese Zunahme gilt laut Barth et al. (2020) für alle Unternehmensgrössen, am stärksten jedoch für Kleinunternehmen, wobei jeweils in den Bereichen Marketing und Betrieb am häufigsten Angriffe festgestellt oder vermutet wurden. Neben der allgemeinen Betroffenheit von Unternehmen, befassten sich Barth et al. auch mit der Frage danach, von welchen unterschiedlichen Arten von digitalen und analogen Angriffen die Unternehmen betroffen waren. Gemäss der Studie berichtet jedes fünfte Unternehmen (21%) vom Diebstahl sensibler digitaler Daten bzw. Informationen und ähnlich viele Unternehmen (17%) waren von der Sabotage der Informations- und Produktionssysteme oder Betriebsabläufe betroffen. Ungefähr jedes achte Unternehmen (13%) berichtete davon, dass ihre digitale Kommunikation ausgespäht worden sei. Daneben wurden Unternehmen aber auch analog angegriffen, wie die Studie dokumentiert. Bei rund einem Drittel der Unternehmen (32%) wurden IT oder Telekommunikationsgeräte gestohlen. Sensible physische Dokumente, Maschinen oder Bauteile wurden bei jedem Sechsten entwendet. Weiter nimmt, so berichten Barth et al. (2020), das sogenannte Social Engineering zu; 22% der Unternehmen waren davon analog betroffen und 15% digital.

Einen spezifischen Blick auf Cyberangriffe – sprich auf Angriffe im digitalen Raum – gegen Unternehmen sowie auf die dagegen getroffenen betrieblichen Massnahmen werfen Dreissigacker et al. (2020). Im Rahmen eines am Kriminologischen Forschungsinstitut Niedersachsen (KFN) angesiedelten Forschungsprojekts wurde hierfür neben Experteninterviews und verschiedenen Feldstudien mit IT-Beschäftigten in KMU eine CATI-Befragung von 5000 Unternehmen mit mindestens zehn Beschäftigten sowie Sitz in Deutschland auf der Grundlage einer disproportional geschichteten Zufallsstichprobe durchgeführt. Dreissigacker et al. (2020) dokumentieren, dass 41.1% der befragten Unternehmen im

Jahr vor der Befragung mindestens einen Cyberangriff erlebt haben, auf den reagiert werden musste. Weiter halten sie fest, dass insbesondere grosse Unternehmen (ab 500 Beschäftigten) mit einer Jahresprävalenzrate von 58.2% signifikant häufiger betroffen sind als mittlere (45.6-47.3%) und kleine Unternehmen (39.4%). Ein Blick auf die Angriffsarten zeigt weiter: Angriffe mittels Schadsoftware sind besonders häufig. So war etwa jedes achte Unternehmen (12.5%) in den zwölf Monaten vor der Befragung von einem Ransomware-Angriff betroffen, jedes neunte (11.3%) von einem Spyware-Angriff und etwa jedes fünfte (21.3%) von sonstigen Schadsoftware-Angriffen. Weiter lag der Anteil der von Phishing betroffenen Unternehmen bei 22.0%. Seltener berichteten die Unternehmen hingegen von CEO-Fraud (8.1%) und (D)DoS-Angriffen (6.4%) und nur ein kleiner Anteil war von manuellem Hacking (2.8%) oder Defacing-Angriffen (3.1%) betroffen. Hinsichtlich der Frage, welche IT-Sicherheitsmassnahmen die Unternehmen gegen Cyberangriffe eingerichtet haben, wurden in der Studie organisatorische (z.B. schriftlich fixierte Richtlinien zur Informations- bzw. IT-Sicherheit) und technische (z.B. Mindestanforderungen für Passwörter oder regelmässige Backups) IT-Sicherheitsmassnahmen voneinander unterschieden. Dabei stellen Dreissigacker et al. (2020) fest, dass technische Massnahmen in den Unternehmen sehr weit verbreitet zu sein scheinen und es nur marginale quantitative Unterschiede zwischen den Beschäftigtengrössenklassen und verschiedenen Wirtschaftszweigen, unterschieden nach WZ08-Klassen gibt. Im Gegensatz dazu werden organisatorische Massnahmen allgemein seltener getroffen, und wenn, dann eher in grösseren Unternehmen. Folgt man wiederum den allgemeinen Einschätzungen der befragten Unternehmensvertretenden, so ist das Bewusstsein gegenüber IT-Risiken dennoch grösstenteils vorhanden. 84.9% der Befragten, gaben an, dass in ihrem Unternehmen sehr viel für die IT-Sicherheit getan werde. Demgegenüber gaben nur 8.0% bzw. 11.3% an, dass sich die Geschäftsführung und Belegschaft ihres Unternehmens besagten IT-Risiken nicht bewusst sei.

2.2 Schweiz

Im Vergleich mit der Deutschen Forschungslandschaft ist die Datenlage in der Schweizer Forschungslandschaft verhältnismässig dünn. Dennoch lassen sich einige Zahlen darlegen, insbesondere in Bezug auf Cybersicherheit – d.h. auf die Sicherheit im digitalen Raum. So dokumentiert etwa das Nationale Zentrum für Cybersicherheit (NCSC) sämtliche Meldungen zu Cybervorfällen, welche in der Schweiz gemeldet werden. Dabei hält die zum Eidgenössischen Finanzdepartement gehörende Fachstelle in ihren 2021 erschienenen Halbjahresberichten bspw. fest, dass sich insbesondere Betrugsversuche im Internet häufen. Allein in der ersten Jahreshälfte 2021 wurden 10‘234 Fälle gemeldet – was ungefähr doppelt so viele wie im ersten Halbjahr 2020 sind (NCSC 2021). Dabei ist jedoch anzumerken, dass in besagter Statistik auch Angriffe, die durch Privatpersonen gemeldet wurden, aufgeführt werden. Wei-

ter handelt es sich dabei nicht nur um Schadensmeldungen, sondern ebenfalls um Meldungen zu Vorfällen, welche frühzeitig erkannt wurden und in vielen Fällen keinen Schaden anzurichten vormochten. Ausserdem sind in den Zahlen nur diejenigen Angriffe bzw. Versuche enthalten, die auch gemeldet wurden. Solche, die nicht gemeldet werden, bleiben dadurch im Verborgenen. Die tatsächliche Anzahl der Angriffe dürfte deutlich höher liegen, da insbesondere für den Deliktsbereich Cybercrime davon ausgegangen wird, dass das so genannte Dunkelfeld und damit der Anteil Straftaten, der nicht zur Kenntnis der Behörden gelangt, besonders gross ist. Allgemein unterstreicht das NCSC jedoch ausdrücklich, dass Unternehmen in Zeiten der Digitalisierung grosse Angriffsflächen für Cyberkriminelle bieten und dementsprechende technische und organisatorische Massnahmen notwendig seien. Etwa Betrugsstrategien wie Social Engineering oder Phishing, aber auch Angriffe durch Ransomware oder das Eindringen via Schwachstellen in Software-Komponenten, gelte es dabei zu berücksichtigen.

Zu einem ähnlichen Schluss kommt das Schweizer Markt- und Sozialforschungsinstitut gfs-zürich, welches im Jahr 2017 301 Interviews mit Geschäftsführenden von Schweizer KMU durchführte. Ziel der Studie war es, Kenntnisse, Einstellungen und getroffene Massnahmen zum Thema Cyberrisiken in KMU zu untersuchen (Mändli Lerch & Repic 2017). Dabei stellten sie fest, dass die Risikoeinschätzung der Betriebe im Kontrast zu deren tatsächlicher Betroffenheit steht: Während lediglich 14% der Befragten es als grosse bis sehr grosse Gefahr einschätzen, Opfer eines Cyberangriffs zu werden, sind die tatsächlichen Betroffenheitszahlen hingegen höher. So kommt die Studie etwa zum Schluss, dass die Anzahl an von Erpressung betroffenen Firmen auf 23'000 (4%) geschätzt werden kann und dass weiter ca. 209'000 Unternehmen (36%) von Malware betroffen sind. Vor solchen Angriffsformen seien die Unternehmen nur teilweise geschützt, wie die Studie zeigt: Rund 60% der Befragten geben an, Grundschutzmassnahmen wie Malware-Schutz, Firewall, Patch-Management und Backup voll und ganz umgesetzt zu haben. Erkennungssysteme und Prozesse zur Behandlung von Cyber-Vorfällen wurden nur von rund 20% der Unternehmen vollständig eingeführt, und Trainings der Mitarbeitenden über den sicheren Gebrauch von IT sogar nur von rund jedem siebten Unternehmen (15%). Die Datenerhebung zeigt jedoch auch eine grosse Bereitschaft der Befragten, die Sicherheit ihres Unternehmens in Zukunft ernster zu nehmen: 45% der Befragten gaben an, in den nächsten zwei bis drei Jahren ihren Schutz gegen Cyberangriffe ausbauen und verbessern zu wollen. Die Autorinnen und Autoren der Studie kommen aufgrund der hohen Betroffenheitszahlen von Cyberangriffen und dem daneben eher geringen Fachwissen resp. den noch wenig umgesetzten Sicherheitsmassnahmen zum Schluss, dass die Sensibilität der Unternehmen in diesem Themenbereich gestärkt werden sollte.

Sicherheit in Schweizer Unternehmen untersuchten derweil auch Zwahlen et al. (2020), wobei diese in ihrer Studie auf den konkreten Bereich der Wirtschaftsspionage fokussierten. Auf der Basis von qualitativen Befragungen (Einzelinterviews) sowie einer quantitativen Befragung im Rahmen einer reprä-

sentativen Stichprobe von relevanten Firmen verschiedener Grössen und aus verschiedenen Tätigkeitsbereichen, dokumentierte die Studie finanzielle und andere Schäden und eruierte die Qualität der Zusammenarbeit zwischen den Unternehmen und den Behörden. Von den befragten Unternehmen (3065 angefragte Unternehmen, Rücklauf: 12% resp. 362 Unternehmen) gaben in der quantitativen Studie 15% an, von einem Wirtschaftsspionagevorfall betroffen zu sein. Die Einzelinterviews (40 Interviews) zeigten wiederum, dass 1/3 der Unternehmen schon mindestens einmal Opfer von Wirtschaftsspionage geworden sind. Die Unternehmensgrösse spiele dabei keine wesentliche Rolle, argumentieren Zwahlen et al. (2020): Von Wirtschaftsspionage betroffen seien sowohl KMU als auch Grossunternehmen. Die Ergebnisse der Studie zeigen zudem, dass insbesondere die Branchen Maschinenbau und Industrie (Ergebnis quantitative Studie) und Pharma und Life Science (Ergebnis qualitative Studie) am stärksten von konkreten Spionagevorfällen betroffen sind. Zwahlen et al. (2020) zeigen weiter, dass die befragten Firmen interne Prävention für deutlich wichtiger halten als die Unterstützung durch externe Spezialistinnen und Spezialisten oder durch staatliche Stellen. Hierfür werden in den Unternehmen verschiedene Präventionsmassnahmen getroffen, etwa strukturelle Anpassungen und organisatorische Regelungen, Schulungen und Sensibilisierung von Mitarbeitenden, Massnahmen im Bereich Informatik und Telekommunikation sowie physische und technische Sicherung. Der Grad der Präventionsbemühungen ist jedoch sehr unterschiedlich und hängt stark mit der Unternehmensgrösse und damit auch mit den vorhandenen Ressourcen für Spionageprävention zusammen. Zwahlen et al. (2020) berichten zudem, dass vor allem in KMU das Bewusstsein für die Risiken in Bezug auf Datenaustausch und digitale Kommunikation (etwa E-Mails) oft sehr wenig ausgeprägt sei.

In Bezug auf die Covid-19 Pandemie und allfällige Konsequenzen für die Sicherheit in KMU untersuchten Peter et al. (2020) Digitalisierung, Home-Office und Cyber-Sicherheit in Schweizer Unternehmen mit 4-49 Mitarbeitenden. Hierfür wurde zwischen August und Oktober 2020 eine Online-Befragung durchgeführt. Die Stichprobe umfasste 503 Geschäftsführende aus Schweizer KMU (bei einer Grundgesamtheit von ca. 153‘000 KMU gemäss BfS Schweiz). Die Ergebnisse zeigen, dass insbesondere mit den wachsenden Zahlen von Mitarbeitenden im Homeoffice, die Gefahr von Cyberangriffen stieg und sich viele KMU dementsprechend in der Pflicht sahen, passende Sicherheitsmassnahmen zu entwickeln. So berichten Peter et al. (2020) etwa, dass rund 25% der Schweizer KMU bereits Opfer von Cyberangriffen wurden, deren Schadensbehebung mit erheblichem Aufwand verbunden waren. Rund ein Drittel der Befragten bezog sich dabei auf einen finanziellen Schaden und 10% sahen einen Reputationsschaden und /oder den Verlust von Kundendaten. Auch Peter et al. (2020) stellen dieser Datenlage gegenüber, dass noch immer ein mangelndes Gefahrenbewusstsein seitens der KMU besteht, dass man Opfer eines Cyberangriffes werden könnte. Lediglich 11% der Befragten schätzen das Risiko, durch einen Cyberangriff einen Tag ausser Gefecht gesetzt zu werden, als gross ein. Gleichzeitig fühlen

sich 20% der Geschäftsleitenden von Schweizer KMU zu den wichtigen Themen zur Cyber-Sicherheit überhaupt nicht oder nur wenig informiert.

Ergebnisse anderer Studien sind jedoch nicht eins zu eins mit den Ergebnissen der vorliegenden Studie vergleichbar, auch wenn zum Teil dieselben Messinstrumente verwendet wurden. Zum einen wurden in der vorliegenden Studie eine besonders grosse Anzahl verschiedener Angriffsarten einbezogen, was die Betroffenheit im Allgemeinen erhöhen dürfte. Zudem wurden mit den letzten zwei Jahren vor der Befragung Angaben zu ganz speziellen Jahren abgefragt, waren diese doch weitestgehend von der Covid-19-Pandemie geprägt. Die Angaben vieler der hier zitierten Studien beziehen sich auf die Zeit vor Corona.

3 Methodisches Vorgehen und Beteiligung

Die vorliegende Studie bezieht sich auf Unternehmen verschiedener Grösse aus der MEM-Industrie, genauer gesagt auf diejenigen Unternehmen aus der MEM-Industrie, die Mitglied im Verband Swissmem sind. Der Link zum Online-Fragebogen wurde am 09.03.2022 an insgesamt 1200 E-Mailadressen respektive Firmen versandt. Nach zwei Wochen wurden die Unternehmen das erste Mal an die Befragung erinnert, nach weiteren zwei Wochen ein zweites Mal. Am 21.04.2022 wurde die Befragung abgeschlossen. Die Befragung wurde mit Hilfe des Online-Befragungstools Unipark von Tivian als reine Online-Befragung durchgeführt. Die Teilnahme an der Befragung war für die angeschriebenen Unternehmen freiwillig und die Befragung wurde vollständig anonym durchgeführt. Anhand der gemachten Angaben können keine Rückschlüsse auf einzelne Unternehmen vorgenommen werden. Die Befragten konnten auswählen, ob sie den Fragebogen auf Deutsch oder Französisch ausfüllen.

Insgesamt haben von den 1200 angeschriebenen Unternehmen 271 den Fragebogen so weit ausgefüllt, dass ihre Antworten in die Analyse einbezogen werden konnten. Das entspricht einem Rücklauf von 22.6%. Insgesamt 15 Firmen haben nur die ersten beiden Seiten des Online-Fragebogens ausgefüllt (5.54% von 271). Obwohl sie damit nur knapp die Hälfte des Fragebogens ausgefüllt haben (vorausgesetzt sie waren in den letzten 24 Monaten von keinem Angriff betroffen) wurden die Antworten dieser Firmen in die Analyse einbezogen, da sie mit den Fragen zu den Angriffsarten zentrale Fragen beantwortet haben. Gefragt nach der Unternehmensgrösse gaben 42.1% (N=242) an, ihr Unternehmen habe 1-49 Mitarbeitende. 28.5% der befragten Unternehmen haben 50-249 Mitarbeitende, 12.4% 250-999 und 16.9% über 1000 Mitarbeitende.

Im Folgenden findet sich eine umfassende Auswertung aller Fragen des Fragebogens. Nachdem zunächst die deskriptiven Ergebnisse (absolute Häufigkeiten und/oder Prozentwerte) zu den einzelnen Fragen dargestellt sind, werden im Anschluss die Ergebnisse nach Unternehmensgrösse und z.T. auch nach Angriffsart getrennt dargestellt. Dabei wird jeweils auch angegeben, ob sich die berichteten Unterschiede nach Unternehmensgrösse und Angriffsart statistisch signifikant unterscheiden und damit,

ob diese Unterschiede mit einer gewissen Wahrscheinlichkeit nicht nur zufällig zustande gekommen sind. Zu beachten gilt dabei jedoch, dass die erhaltene Stichprobe nicht als repräsentativ für die Mitglieder des Verbands Swissmem angesehen werden kann bzw. dass nicht abschliessend geprüft werden kann, ob die Stichprobe repräsentativ ist oder nicht.

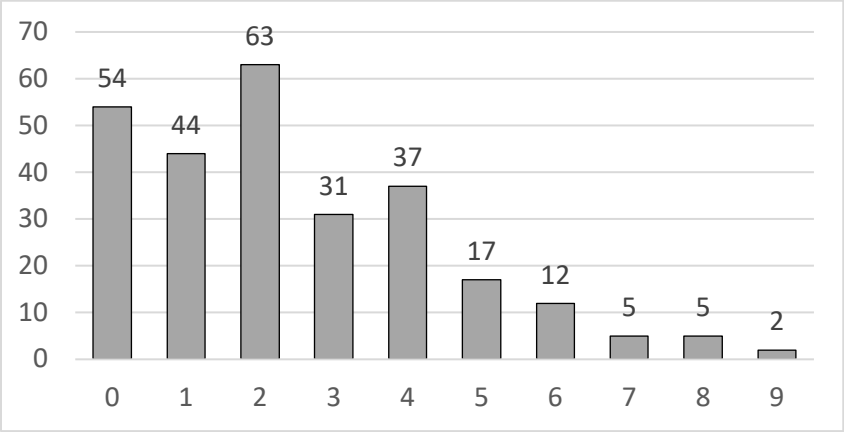
4 Angriffsarten

Im ersten Abschnitt des Fragebogens wurde die Betroffenheit durch eine umfassende Anzahl von physischen und digitalen Angriffsarten erfragt. Dabei wurde jeweils zunächst erfasst, ob die befragten Unternehmen jemals seit ihrem Bestehen Opfer von den beschriebenen Angriffsarten geworden sind. Antwortoptionen waren «ja» und «nein bzw. nicht bekannt». Daran anschliessend wurde erhoben, wie häufig in den letzten 24 Monaten vor der Befragung eine Opferwerdung durch die genannten Angriffsarten erfolgt ist. Hier wurden die Befragten gebeten, die Anzahl Fälle anzugeben von «0», «1», «2» usw. bis «über 20» (siehe die Frage 1 und 2 des Fragenkatalogs im Anhang). Die Formulierungen der Beschreibungen der einzelnen Angriffsarten wurden weitestgehend von anderen Studien übernommen und gegebenenfalls, in Zusammenarbeit mit der Swissmem-Projektgruppe, angepasst (siehe Barth et al., 2020; Dreissigacker et al., 2020; Corporate Trust, 2014; Zwahlen et al., 2020). Im Folgenden sind zunächst die Ergebnisse für die Zeit seit dem Bestehen des Unternehmens und anschliessend für die letzten 24 Monate dargestellt. Anschliessend erfolgt eine Analyse der Unterschiede nach Unternehmensgrösse.

4.1 Angriffe seit Bestehen des Unternehmens

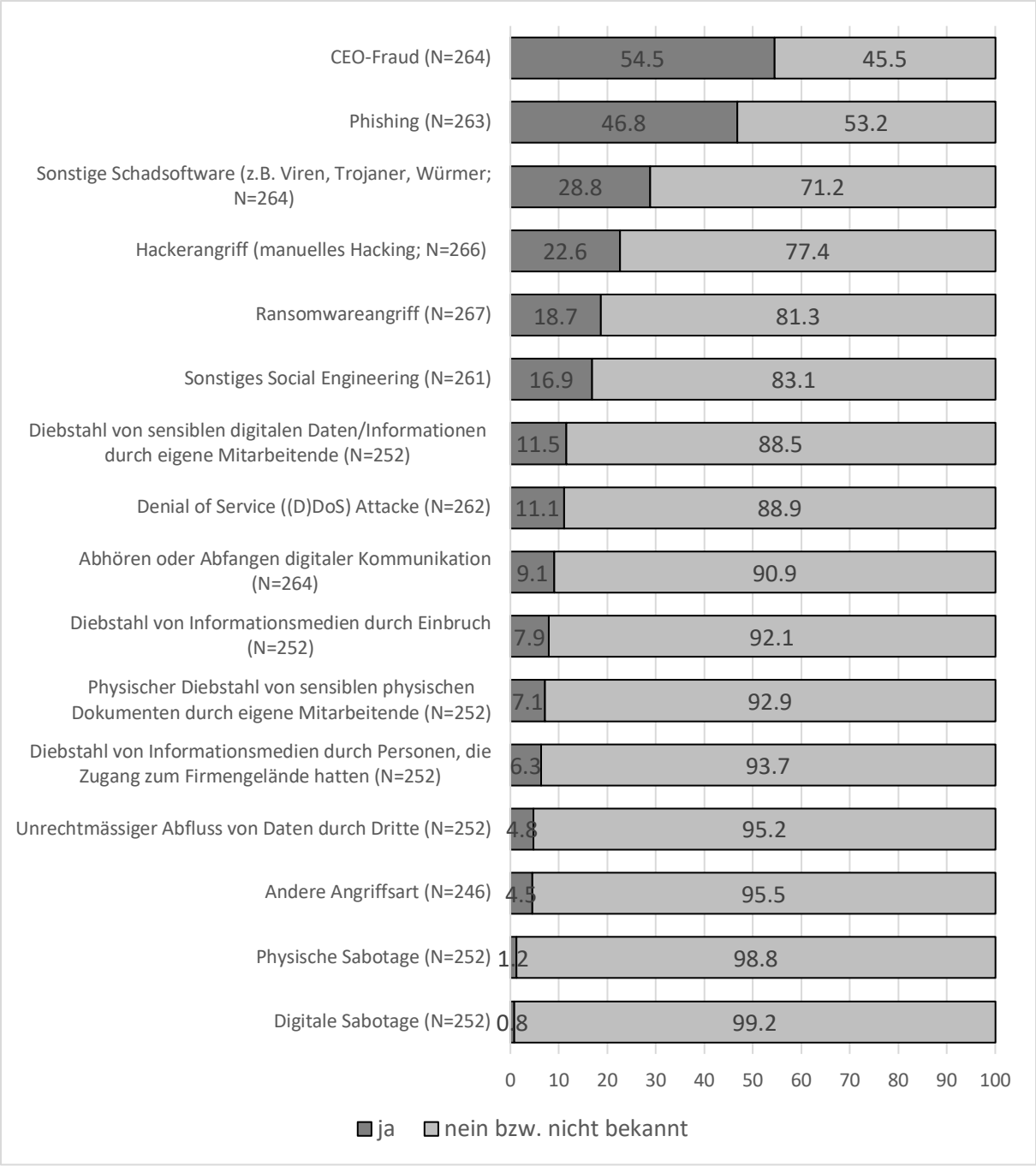
Insgesamt sind 216 (80.0%, N=270) der Unternehmen, welche die Fragen dazu, ob sie jemals seit dem Bestehen Opfer von irgendeiner Form der abgefragten Angriffe geworden sind beantwortet haben, von mindestens einer Angriffsart betroffen gewesen. Im Durchschnitt waren die Unternehmen von 2.4 (SD 2.1) verschiedenen Arten von Angriffen betroffen. Eine Verteilung findet sich in Grafik 1, in der auf der X-Achse die Anzahl verschiedener Angriffsarten und auf der Y-Achse die Anzahl der betroffenen Unternehmen abgebildet sind.

Wie aus Grafik 1 ersichtlich, waren insgesamt 54 (20.0%) der 270 Unternehmen, welche die Frage nach der Betroffenheit durch die verschiedenen Arten von Angriffen seit Bestehen des Unternehmens beantwortet haben, noch nie von einer der abgefragten Angriffsarten betroffen. Weitere 44 (16.3%) Unternehmen berichten, seit dem Bestehen von einer Angriffsart betroffen gewesen zu sein, 63 (23.3%) von zwei verschiedenen, 31 (11.5%) von drei verschiedenen 37 (13.7%) von vier verschiedenen usw. Zwei Unternehmen waren von neun verschiedenen Angriffsarten betroffen. Es zeigt sich also eine gewisse Mehrfachbetroffenheit durch unterschiedliche Angriffsarten bei vielen der befragten Unternehmen.



Grafik 1: Betroffenheit nach Anzahl verschiedener Angriffsarten seit dem Bestehen des Unternehmens (absolute Häufigkeiten; N=270)

Für welche Angriffsarten im Einzelnen eine Betroffenheit seit Bestehen des Unternehmens berichtet wurde, kann Grafik 2 entnommen werden. Mehr als die Hälfte der befragten Unternehmen berichtet, zu irgendeinem Zeitpunkt seit Bestehen des Unternehmens Opfer von CEO-Fraud geworden zu sein. Ebenso ist fast die Hälfte von einem erfolgreichen Phishing Angriff betroffen gewesen. Etwas mehr als ein Viertel wurde Opfer durch sonstige Schadsoftware wie z.B. Viren, Würmer und Trojaner. Rund jedes vierte befragte Unternehmen wurde Opfer eines Hackerangriffs, etwa jedes fünfte von einem Ransomwareangriff und jedes sechste von sonstigem Social Engineering, bei dem Mitarbeitende gezielt ausgefragt bzw. ausspioniert wurden, etwa am Telefon, in sozialen Netzwerken/Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen. Jeweils jedes neunte befragte Unternehmen berichtete vom Diebstahl digitaler Daten und/oder von (D)DoS-Attacken. Wiederum berichteten weniger als zehn Prozent von Fällen des Abhörens und Abfangens von digitaler Kommunikation, Diebstahl von Informationsmedien durch Einbruch, Diebstahl von sensiblen physischen Dokumenten durch eigene Mitarbeitende sowie Diebstahl von Informationsmedien, die Zugang zum Firmengelände hatten, wie z.B. Mitarbeitende, Besucher o.ä. als Angriffsarten, von denen sie bereits mindestens einmal seit dem Bestehen des Unternehmens betroffen waren. Weniger als fünf Prozent waren von unrechtmässigem Abfluss von Daten durch Dritte, z.B. durch Zulieferer, Dienstleistern oder Kundenanlagen und physischer oder digitaler Sabotage betroffen.



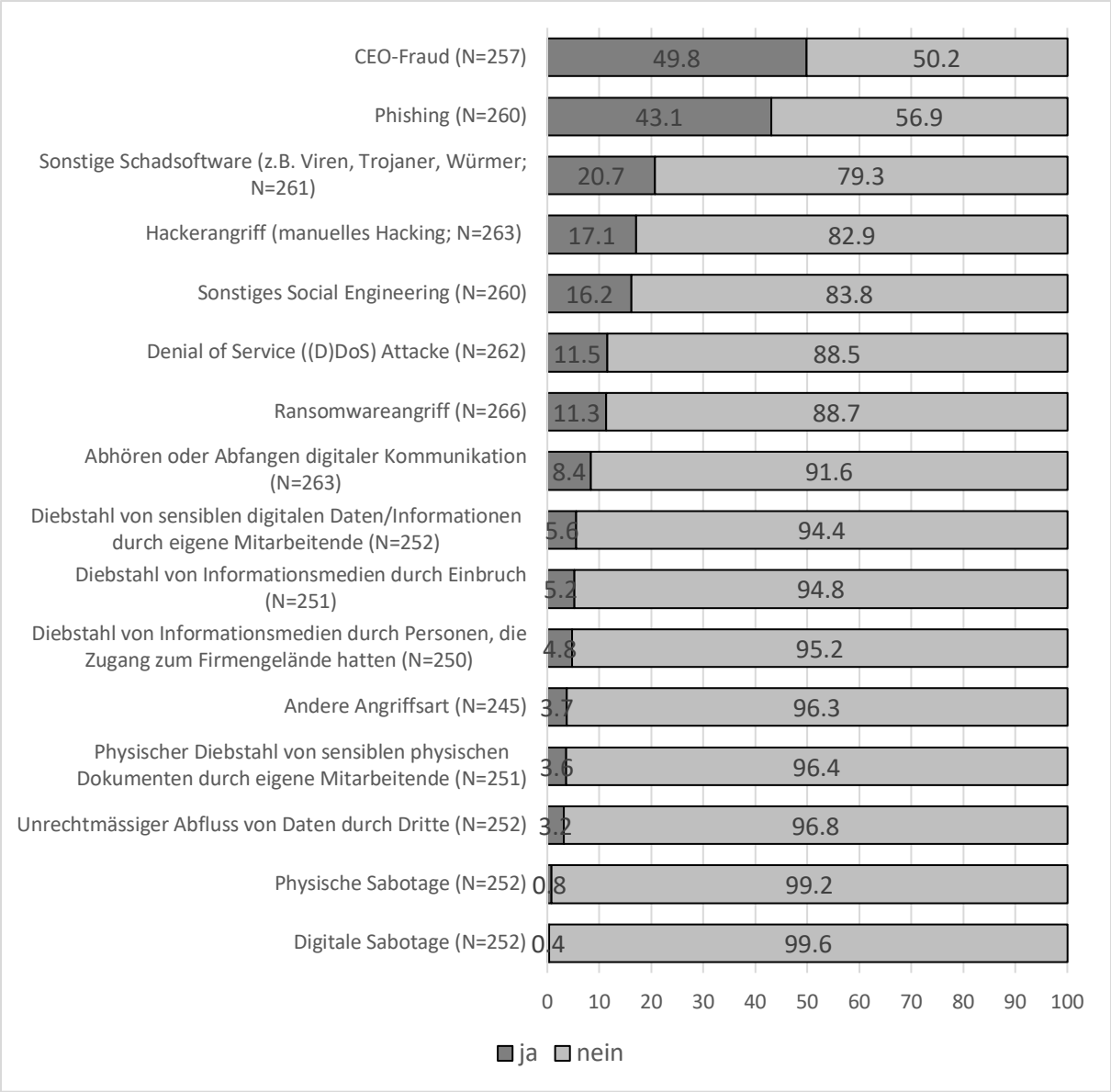
Grafik 2: Betroffenheit durch einzelne Angriffsarten seit dem Bestehen des Unternehmens (sortiert nach Häufigkeit; in Prozent)

Von 4.5% der befragten Unternehmen wurde angegeben, dass sie von einer anderen als den abgefragten Angriffsarten betroffen waren. Die Befragten, die eine andere Angriffsart angegeben haben, wurden zusätzlich gebeten nähere Angaben zu diesen anderen Angriffsarten vorzunehmen. Genannt wurden zum einen Versuche, z.B. durch Ransomware über Clients/Mail oder CEO-Fraud ebenso wie Erpressung durch die Änderung einer Lieferantenrechnung nach einem Zugriff auf ein E-Mail Postfach, Brute Force Attack, Diebstähle von Laptops ausserhalb des Firmenareals, aus geparkten Fahrzeugen,

das Hacking von Computern durch Offizielle, der Missbrauch von offline Zahlungssoftware, um Zahlungen im Onlinebanking durchzuführen sowie die Übernahme von Lieferantenmail, mit dem Ziel, den Zahlungsweg umzuleiten. Ein Unternehmen hat zudem angemerkt, dass ständig Angriffe durchgeführt würden, insbesondere durch Phishing, diese aber zum Glück meist nicht erfolgreich seien.

4.2 Angriffe in den letzten 24 Monaten vor der Befragung

Insgesamt 190 (70.4%, N=270) der befragten Unternehmen waren in den letzten zwei Jahren vor der Befragung Opfer von mindestens einer der abgefragten Angriffsarten. Einige bis zu über zwanzigmal. Einen Überblick über die Betroffenheit durch die einzelnen Angriffsarten findet sich in Grafik 3. Im Vergleich zur Betroffenheit durch verschiedene Angriffsarten seit Bestehen des Unternehmens sind die Häufigkeiten für die letzten 24 Monate etwas geringer. Bei einigen Angriffsarten, insbesondere bei den drei häufigsten, CEO-Fraud, Phishing und sonstige Schadsoftware äusserten die Befragten jedoch auch für die letzten zwei Jahre vor der Befragung eine fast vergleichbar hohe Betroffenheit wie seit Bestehen des Unternehmens. Es kann also davon ausgegangen werden, dass viele der seit Bestehen des Unternehmens berichteten Angriffe in den letzten zwei Jahren vor der Befragung stattfanden. Wie auch bezüglich der Häufigkeit der erlebten Angriffe seit Bestehen des Unternehmens, war die häufigste Angriffsart CEO-Fraud. Etwa die Hälfte der befragten Unternehmen war in den zwei Jahren vor der Befragung betroffen. Auch von Phishing-Angriffen berichteten mehr als 40% der Befragten. Jedes fünfte Unternehmen wurde Opfer von Schadsoftware wie Viren, Würmern und Trojanern, jedes sechste von Hackerangriffen. Von sonstigem Social Engineering, in Abgrenzung zum CEO-Fraud, bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, berichtete ebenfalls rund jedes sechste Unternehmen. Jedes neunte Unternehmen war Opfer von (D)DoS Attacken und Ransomwareangriffen, rund jedes zwölfte vom Abhören und Abfangen digitaler Kommunikation. Die übrigen Angriffsarten kamen vergleichsweise seltener vor. Einen Diebstahl von sensiblen digitalen Informationen durch eigene Mitarbeitende berichtete rund jedes 18. Unternehmen. Einbrüche oder Diebstähle von Kommunikationsmedien oder sensiblen digitalen Daten durch Personen, die Zugang zum Firmengelände hatten (darunter auch eigene Mitarbeitende) erlebte immerhin noch jedes 19. bis 20. Unternehmen. Besonders selten waren Diebstähle von physischen Dokumenten durch Mitarbeitende, der unrechtmässige Abfluss von Daten durch Dritte sowie gezielte Sabotageakte (digital oder physisch). 3.7% der befragten Unternehmen berichteten von einer Opferwerdung durch eine andere Angriffsart (siehe oben im Abschnitt Angriffe seit Bestehen des Unternehmens für Beispiele anderer Angriffsarten).



Grafik 3: Betroffenheit durch einzelne Angriffsarten in den letzten 24 Monaten vor der Befragung (sortiert nach Häufigkeit; in Prozent)

Während in Grafik 3 dargestellt ist, wie viele der befragten Unternehmen in den letzten 24 Monaten vor der Befragung von den einzelnen Angriffsarten betroffen waren, ist in Tabelle 1 zusätzlich angegeben, wie häufig die Unternehmen jeweils Opfer geworden sind.

Bei allen Angriffsarten waren die Anteile Betroffener in der Kategorie ein- bis zweimal am grössten. Von einigen Angriffsarten waren viele Unternehmen jedoch deutlich häufiger betroffen, bis zu mehr als zwanzigmal. Im Vergleich zu den anderen Angriffsarten äusserten insbesondere bei Phishing Angriffen besonders viele Unternehmen eine hohe Betroffenheit von mehr als zwanzigmal (13.5%). Vergleichsweise häufiger mehrfachbetroffen waren die Unternehmen auch von CEO-Fraud. Rund jedes zehnte Unternehmen war in den 24 Monaten vor der Befragung drei- bis fünfmal von CEO-Fraud be-

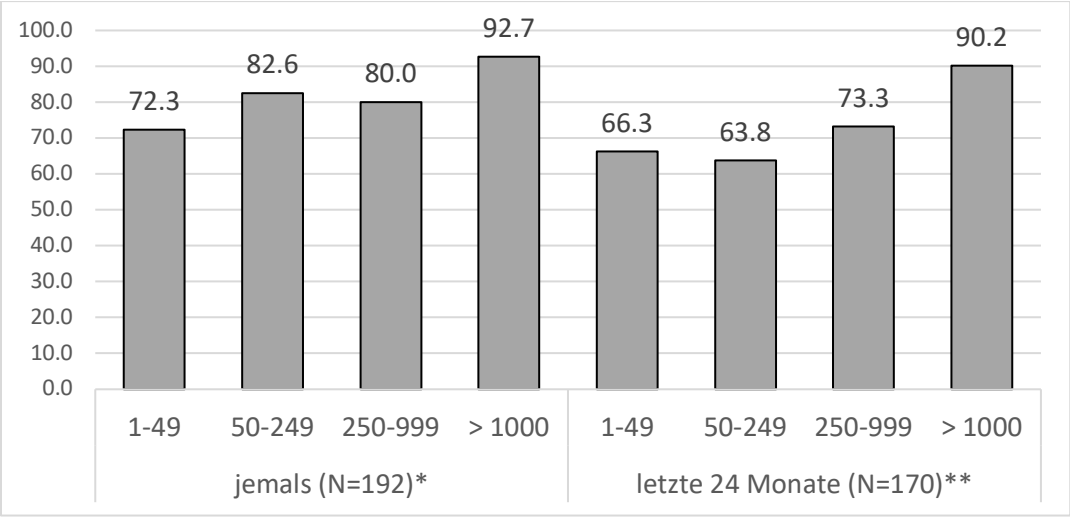
troffen, rund jedes 20. Unternehmen sechs- bis zehnmal und jedes 17. Unternehmen mehr als zwanzigmal. Bei sonstigem Social Engineering, sonstiger Schadsoftware, wie Viren, Trojaner oder Würmer, Hackerangriffen, (D)DoS-Attacken, dem Abhören und Abfangen digitaler Kommunikation sowie dem Diebstahl von Informationsmedien durch Einbruch gaben ebenfalls jeweils einige wenige Unternehmen an, mehr als zwanzigmal betroffen gewesen zu sein.

Tabelle 1: Häufigkeit der Betroffenheit durch einzelne Angriffsarten in den letzten 24 Monaten vor der Befragung (in Prozent)

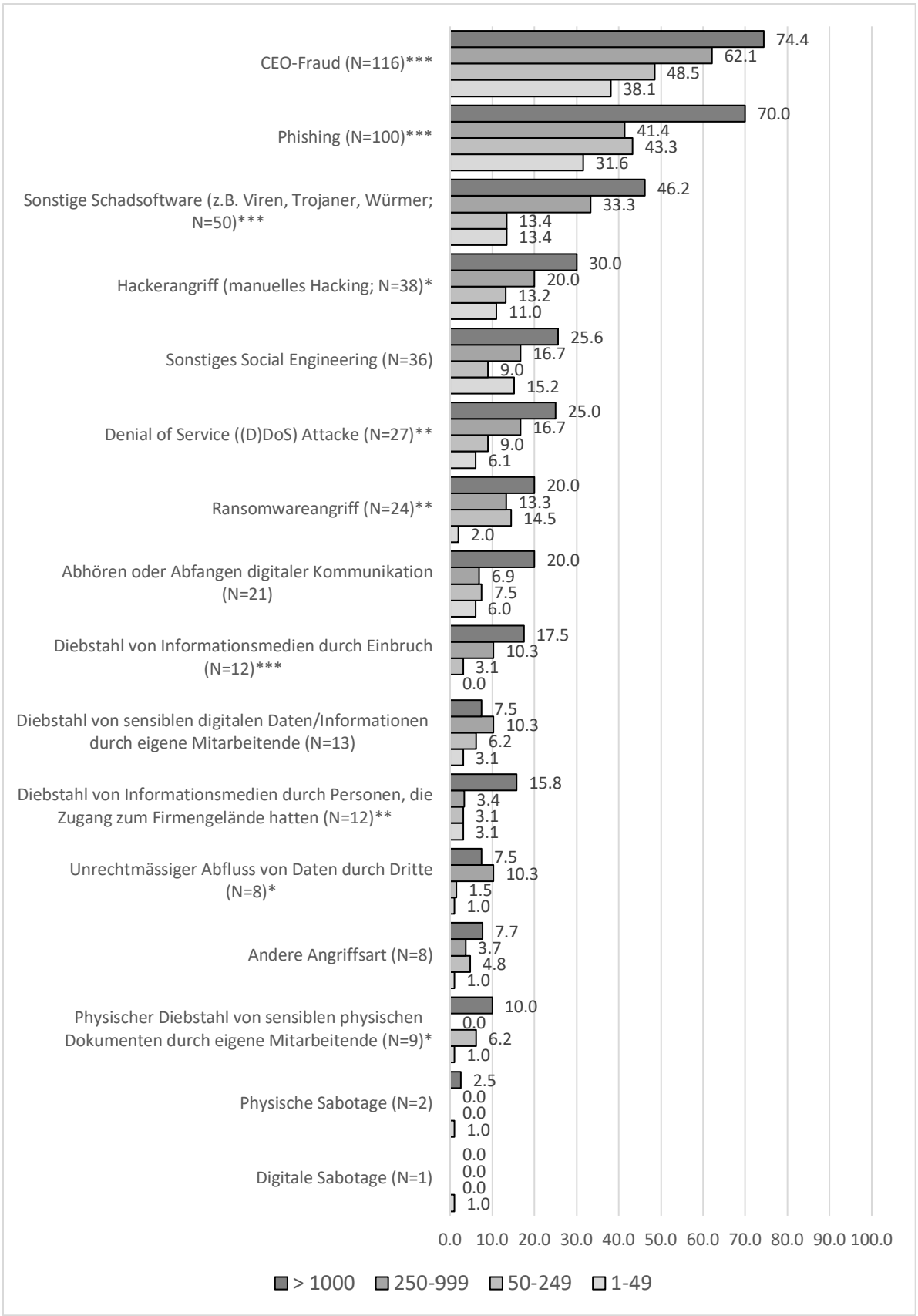
	0mal	1-2mal	3-5mal	6-10mal	11-20mal	mehr als 20mal
Hackerangriff (manuelles Hacking; N=263)	82.9	11.0	3.0	1.5	0.0	1.5
Ransomwareangriff (N=266)	88.7	10.5	0.8	0.0	0.0	0.0
Sonstige Schadsoftware (z.B. Viren, Trojaner, Würmer; N=261)	79.3	12.3	5.4	1.1	0.4	1.5
Denial of Service ((D)DoS) Attack (N=262)	88.5	7.6	1.1	1.5	0.0	1.1
Phishing (N=260)	56.9	17.7	6.5	4.2	1.2	13.5
Abhören oder Abfangen digitaler Kommunikation (N=263)	91.6	6.5	0.8	0.0	0.4	0.8
CEO-Fraud (N=257)	50.2	26.5	10.5	5.1	1.9	5.8
Sonstiges Social Engineering (N=260)	83.8	6.9	4.2	1.9	0.0	3.1
Diebstahl von Informationsmedien durch Einbruch (N=251)	94.8	4.4	0.4	0.0	0.0	0.4
Diebstahl von Informationsmedien durch Personen, die Zugang zum Firmengelände hatten (N=250)	95.2	3.6	1.2	0.0	0.0	0.0
Diebstahl von sensiblen digitalen Daten/Informationen durch eigene Mitarbeitende (N=252)	94.4	4.8	0.8	0.0	0.0	0.0
Physischer Diebstahl von sensiblen physischen Dokumenten durch eigene Mitarbeitende (N=251)	96.4	3.2	0.4	0.0	0.0	0.0
Unrechtmässiger Abfluss von Daten durch Dritte (N=252)	96.8	2.4	0.4	0.4	0.0	0.0
Digitale Sabotage (N=252)	99.6	0.4	0.0	0.0	0.0	0.0
Physische Sabotage (N=252)	99.2	0.8	0.0	0.0	0.0	0.0

4.3 Angriffe nach Unternehmensgrösse

Im folgenden Abschnitt wird der Frage nachgegangen, ob und inwieweit sich die Unternehmen in ihrer Betroffenheit durch die verschiedenen Angriffsarten je nach ihrer Grösse unterscheiden. Wie aus Grafik 4 ersichtlich, zeigten sich sowohl für die Betroffenheit seit Bestehen des Unternehmens als auch in den letzten 24 Monaten vor der Befragung statistisch signifikante Unterschiede. Die in Grafik 4 dargestellten Unterschiede sind also mit einer gewissen Wahrscheinlichkeit nicht zufällig zustande gekommen. Bei Betrachtung der Grafik 4 wird ausserdem deutlich, dass insbesondere grössere Unternehmen mit mehr als 1000 Mitarbeitenden durch mindestens eine der abgefragten Angriffsart betroffen waren. Dieser Befund zeigt sich für die Betroffenheit seit Bestehen des Unternehmens ebenso wie für die Betroffenheit in den zwei Jahren vor der Befragung. Jeweils mehr als 90% der Unternehmen in dieser Grössenklasse wurden Opfer. Jemals betroffen waren am seltensten Unternehmen mit einer Grösse von 1-49 Mitarbeitenden. 72.3% der Unternehmen mit dieser Grösse sind betroffen gewesen. Bezüglich der letzten 24 Monate vor der Befragung waren Unternehmen mit einer Grösse von 50-249 Mitarbeitenden am seltensten Opfer (63.8%). Bei den Häufigkeiten seit Bestehen des Unternehmens zeigte sich mit 82.6% hingegen die zweithöchste Betroffenheit innerhalb dieser Grössenklasse. Die Unterschiede zu Unternehmen mit einer Grösse von 250-999 Mitarbeitenden sind jedoch gering (80.0%).



Grafik 4: Betroffenheit seit Bestehen des Unternehmens und in den letzten 24 Monaten vor der Befragung nach Unternehmensgrösse (dargestellt sind die Anteile Betroffener; in Prozent; Chi-Quadrat Test: *p<.05, **p<.03, ***p<.001)



Grafik 5: Betroffenheit durch einzelne Angriffsarten in den letzten 24 Monaten vor der Befragung nach Unternehmensgrösse (sortiert nach Häufigkeit; in Prozent; dargestellt: Anteile Betroffener; Chi-Quadrat Test: *p<.05, **p<.03, ***p<.001)

Wie sich die Unternehmen nach ihrer Grösse hinsichtlich der einzelnen Angriffsarten unterscheiden, kann Grafik 5 entnommen werden. Bei dieser Analyse wurden im Sinne der Übersichtlichkeit nur die Angriffe der letzten 24 Monate berücksichtigt. In der Grafik ist zudem angegeben, ob die dargestellten Unterschiede statistisch signifikant sind.

Mit Ausnahme des Diebstahls von sensiblen digitalen Daten durch eigene Mitarbeitende, dem unrechtmässigen Abfluss von Daten durch Dritte sowie digitaler Sabotage sind von allen anderen Angriffsarten häufiger Unternehmen mit mehr als 1000 Mitarbeitenden betroffen. Bezüglich des Diebstahls von sensiblen digitalen Daten durch eigene Mitarbeitende und des unrechtmässigen Abflusses von Daten durch Dritte waren am häufigsten Unternehmen mit 250-999 Mitarbeitenden Opfer. Von digitaler Sabotage wurde in den zwei Jahren vor der Befragung nur ein Unternehmen Opfer. Dieses hatte eine Grösse von 1-49 Mitarbeitenden.

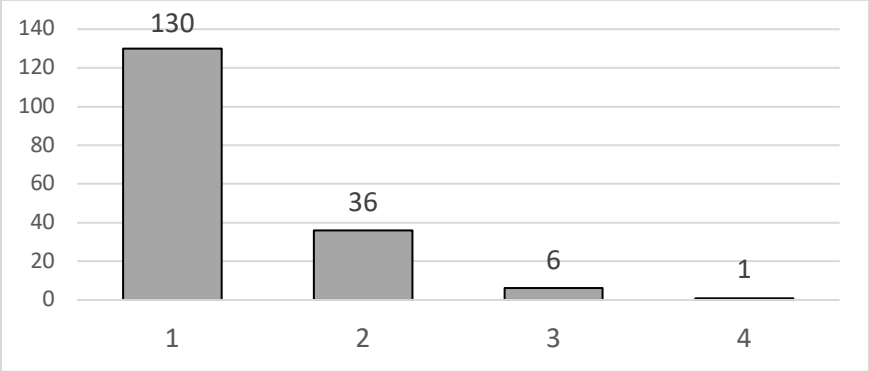
Bei vielen Angriffsarten nimmt die Betroffenheit mit zunehmender Grösse des Unternehmens mehr oder weniger kontinuierlich zu. Dies gilt insbesondere für CEO-Fraud, sonstige Schadsoftware, Hackerangriffe, (D)DoS-Attacken sowie für den Diebstahl von Informationsmedien durch Einbruch. Grössere Unternehmen mit mehr als 1000 Mitarbeitenden sind im Vergleich zu Unternehmen anderer Grösse auch deutlich häufiger betroffen von Phishing-Angriffen. Insgesamt sind jedoch Unternehmen jeglicher Grösse insbesondere von CEO-Fraud, Phishing, sonstiger Schadsoftware, wie Viren, Trojaner und Würmer sowie von Hackerangriffen betroffen.

5 Schwerwiegendster Angriff

Diejenigen Firmen, die angegeben haben, in den letzten 24 Monaten vor der Befragung von einer oder mehreren Angriffsarten betroffen gewesen zu sein, wurden in einem nächsten Schritt gebeten, zu benennen, welcher der Angriffe, die sie angegeben haben, der schwerwiegendste gewesen ist. Die Unternehmen hatten die Möglichkeit, mehrere der beschriebenen Angriffsarten auszuwählen, wenn diese Teil ein und desselben Angriffs gewesen sind. Es waren also Mehrfachantworten möglich. Angezeigt wurden nur die Angriffsarten, für welche vorher angegeben wurde, dass das Unternehmen in den letzten zwei Jahren vor der Befragung von diesen betroffen war. Alle anderen wurden jeweils ausgeblendet (siehe Frage 3 des Fragenkatalogs im Anhang). Mit Bezug zu dem schwerwiegendsten Angriff wurden dann diverse Anschlussfragen gestellt, deren Auswertungen in den folgenden Abschnitten dargestellt sind.

Insgesamt 173 Unternehmen und damit 63.8% der 271 befragten Unternehmen haben einen schwerwiegendsten Angriff angegeben. Von den 173 Unternehmen, die einen schwerwiegendsten Angriff angegeben haben, wählten 130 Unternehmen (75.1%) eine einzelne Angriffsart aus (siehe Grafik 6). Weitere 36 (20.8%) Unternehmen gaben einen schwerwiegendsten Angriff an, der aus einer Kombination aus zwei Angriffsarten bestand, sechs Unternehmen (3.5%) einen Angriff, der aus einer Kombination

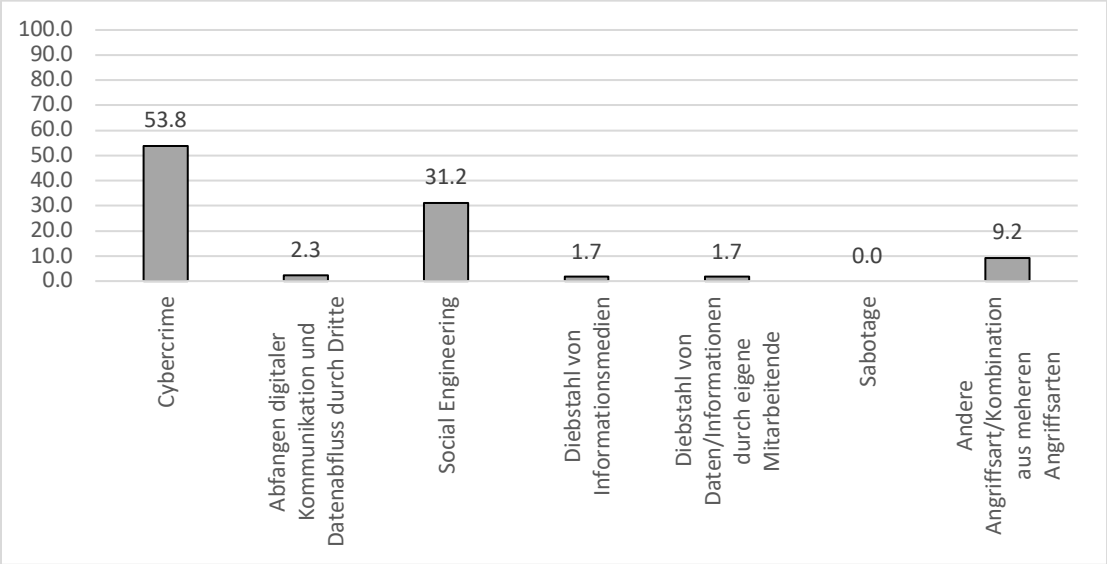
aus drei Angriffsarten bestand und ein Unternehmen (0.6%) einen Angriff, der aus einer Kombination aus vier Angriffsarten bestand. Häufig genannte Kombinationen aus Angriffsarten sind die Kombination aus sonstiger Schadsoftware und CEO-Fraud sowie insbesondere die Kombination aus Phishing und CEO-Fraud.



Grafik 6: Anzahl genannter schwerwiegendster Angriffsarten (absolute Häufigkeiten; N=173)

Für die weiteren Auswertungen werden die einzelnen Angriffsarten zu den folgenden Kategorien zusammengefasst (eine Auflistung, welche Angriffsarten jeweils in den Kategorien enthalten sind, findet sich im Anhang):

1. Angriffe durch Cybercrime
2. Abfangen digitaler Kommunikation und Datenabfluss durch Dritte
3. Social Engineering
4. Diebstahl von Informationsmedien
5. Diebstahl von sensiblen Daten/Informationen durch eigene Mitarbeitenden
6. Sabotage
7. Andere Angriffsart oder Kombination aus mehreren Angriffsarten



Grafik 7: Art des schwerwiegendsten Angriffs (in Prozent; N=173)

Wie aus Grafik 7 ersichtlich, fällt mit mehr als der Hälfte der Grossteil der berichteten schwerwiegendsten Angriffe in den Bereich Cybercrime. Den zweitgrössten Anteil stellen Angriffe aus dem Bereich Social Engineering dar. Rund jeder dritte schwerste Angriff wurde dieser Kategorie zugeordnet. Etwa jeder elfte Angriff ist eine Kombination aus mehreren Angriffsarten oder eine andere, in den Antwortkategorien nicht vorgegebene, Angriffsart. Alle anderen Angriffsarten wurden deutlich seltener genannt; von drei bzw. vier der befragten Unternehmen. Sabotage findet sich gar nicht unter den berichteten schwerwiegendsten Vorfällen und wird aus diesem Grund bei den folgenden Auswertungen nicht weiter berücksichtigt.

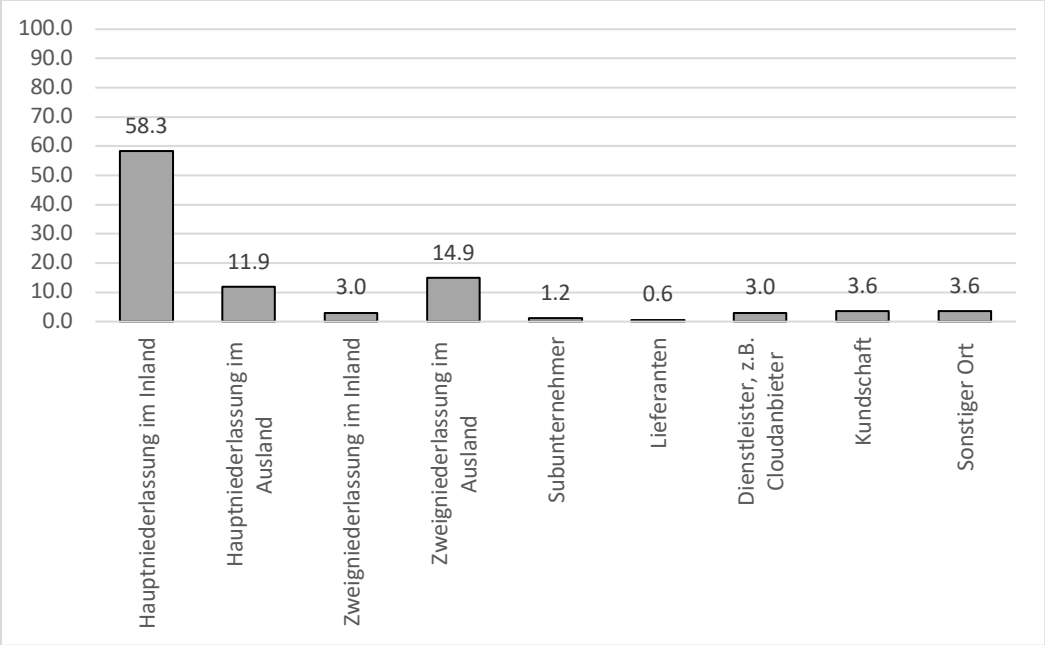
5.1 Initialer Angriffspunkt

Als erste Frage in Bezug auf den schwerwiegendsten Angriff wurde gefragt, wo der initiale Angriffspunkt des Angriffs gewesen ist (siehe Frage 4 des Fragenkatalogs im Anhang). Zur Beantwortung dieser Frage standen die in Grafik 8 aufgeführten Antwortkategorien zur Verfügung. Zusätzlich bestand die Möglichkeit, einen anderen Angriffspunkt anzugeben sowie das Land einzutragen, wenn der Angriffspunkt eine Haupt- oder Zweigniederlassung im Ausland gewesen ist.

Insgesamt 168 Unternehmen haben die Frage danach, wo der initiale Angriffspunkt des schwerwiegendsten Angriffs war beantwortet. Wie aus Grafik 8 deutlich wird, war dieser überwiegend in der Hauptniederlassung im Inland. Eine Hauptniederlassung im Ausland wurde von rund jedem achten Unternehmen genannt. Gefragt nach dem Land, in dem sich die Hauptniederlassung befindet, wurde insbesondere Deutschland angegeben, aber auch die USA, Indien, Australien, Brasilien, Dänemark, Luxemburg, Schweden und Taiwan (die Reihenfolge entspricht der Häufigkeit der Nennungen, ab Australien gab es jeweils nur eine Nennung des Landes). Noch etwas häufiger als eine Hauptniederlassung im Ausland wurde eine Zweigniederlassung im Ausland als initialer Angriffspunkt genannt. Hier wurden insbesondere die USA, Deutschland, China, England und Italien genannt, aber auch Australien, Brasilien, Mexiko, Polen, Singapur, Spanien, die Türkei und Indien (die Reihenfolge entspricht der Häufigkeit der Nennungen, ab Australien gab es jeweils nur eine Nennung des Landes). Die übrigen Möglichkeiten wurden deutlich seltener als Angriffspunkt angegeben. 3.6% und damit sechs Unternehmen haben einen anderen Ort als Angriffspunkt als Antwortoption ausgewählt. Gefragt nach näheren Angaben wurden der Dienstleister eines Kunden, alle Niederlassungen, Website und Swissmem genannt.

Es zeigen sich statistisch signifikante Unterschiede bezüglich des initialen Angriffspunkts je nach Unternehmensgrösse (siehe Tabelle 2). Bei Unternehmen bis zu einer Grösse von 999 Mitarbeitenden war der initiale Angriffspunkt am häufigsten die Hauptniederlassung im Inland. Bei den befragten Unternehmen mit einer Grösse von mehr als 1000 Mitarbeitenden war dieser jedoch am häufigsten in einer Zweigniederlassung im Ausland. Bei den befragten Unternehmen aus den übrigen Grössenklas-

sen war dies seltener der Fall. Bei Firmen mit mehr als 1000 Mitarbeitenden war auch eine Zweigniederlassung im Ausland im Vergleich zu Unternehmen anderer Grösse häufiger der Ort, wo der Angriff startete.



Grafik 8: Initialer Angriffspunkt des schwerwiegendsten Angriffs (in Prozent; N=168)

Bei Unternehmen mit einer Grösse von 1-49 Mitarbeitenden war der initiale Angriffspunkt ebenfalls bei jedem zehnten befragten Unternehmen eine Hauptniederlassung im Ausland. Bei den Unternehmen der übrigen Grössenklassen war dies weniger häufig der Fall. Dass der initiale Angriffspunkt bei einem Dienstleister, z.B. einem Cloudanbieter, war, berichteten zwei befragte Unternehmen mit einer Grösse von 250-999 Mitarbeitenden. Bei den übrigen traf dies nur auf jeweils ein Unternehmen zu. Auch die anderen potenziellen Angriffspunkte wurden jeweils nur von rund ein bis zwei Unternehmen als initialer Angriffspunkt genannt.

Bezüglich der Angriffsart zeigen sich keine statistisch signifikanten Unterschiede nach dem initialen Angriffspunkt. Bei allen Angriffsarten fand der Angriff insbesondere in der Hauptniederlassung im Inland statt (siehe Tabelle 2). Bei einigen Angriffsarten, insbesondere beim Diebstahl von Daten/Informationen durch eigene Mitarbeitende und dem Diebstahl von Informationsmedien, sind die Fallzahlen sehr gering. Es gaben nur sehr wenige Unternehmen einen entsprechenden Angriff an, weshalb hohe Prozentzahlen hier nur sehr wenige Fälle repräsentieren.

Tabelle 2: Initialer Angriffspunkt des schwerwiegendsten Angriffs nach Unternehmensgrösse und Angriffsart (in Prozent)

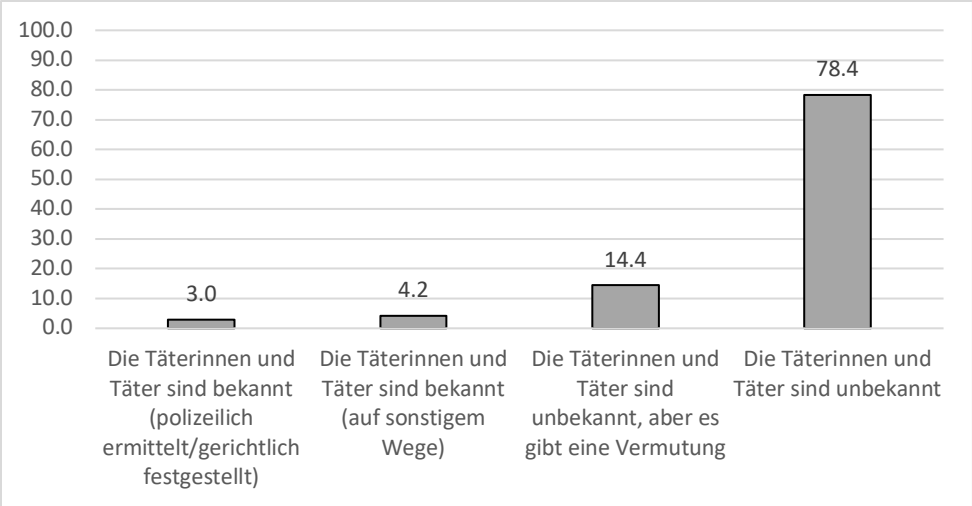
	Hauptniederlassung im Inland	Hauptniederlassung im Ausland	Zweigniederlassung im Inland	Zweigniederlassung im Ausland	Subunternehmer	Lieferanten	Dienstleister, z.B. Cloudanbieter	Kundschaft	Sonstiger Ort
Unternehmensgrösse									
1-49 (N=60)	68.3	10.0	3.3	6.7	0.0	0.0	1.7	5.0	5.0
50-249 (N=43)	74.4	7.0	0.0	11.6	0.0	0.0	2.3	4.7	0.0
250-999 (N=19)	63.2	5.3	0.0	10.5	0.0	5.3	10.5	0.0	5.3
> 1000 (N=35)	20.0	25.7	5.7	37.1	2.9	0.0	2.9	0.0	5.7
Angriffsart									
Cybercrime (N=90)	56.7	14.4	3.3	14.4	1.1	0.0	5.6	1.1	3.3
Abfangen digitaler Kommunikation und Datenabfluss durch Dritte (N=4)	50.0	0.0	0.0	50.0	0.0	0.0	0.0	0.0	0.0
Social Engineering (N=53)	60.4	7.5	1.9	17.0	0.0	1.9	0.0	9.4	1.9
Diebstahl von Informationsmedien (N=3)	66.7	0.0	33.3	0.0	0.0	0.0	0.0	0.0	0.0
Diebstahl von Daten/Informationen durch eigene Mitarbeitende (N=2)	50.0	50.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Andere Angriffsart/Kombination aus mehreren Angriffsarten (N=16)	62.5	12.5	0.0	6.3	6.3	0.0	0.0	0.0	12.5

Chi-Quadrat Test Unternehmensgrösse p<.001/Chi-Quadrat-Test Angriffsart n.s.

5.2 Täterinnen bzw. Täter

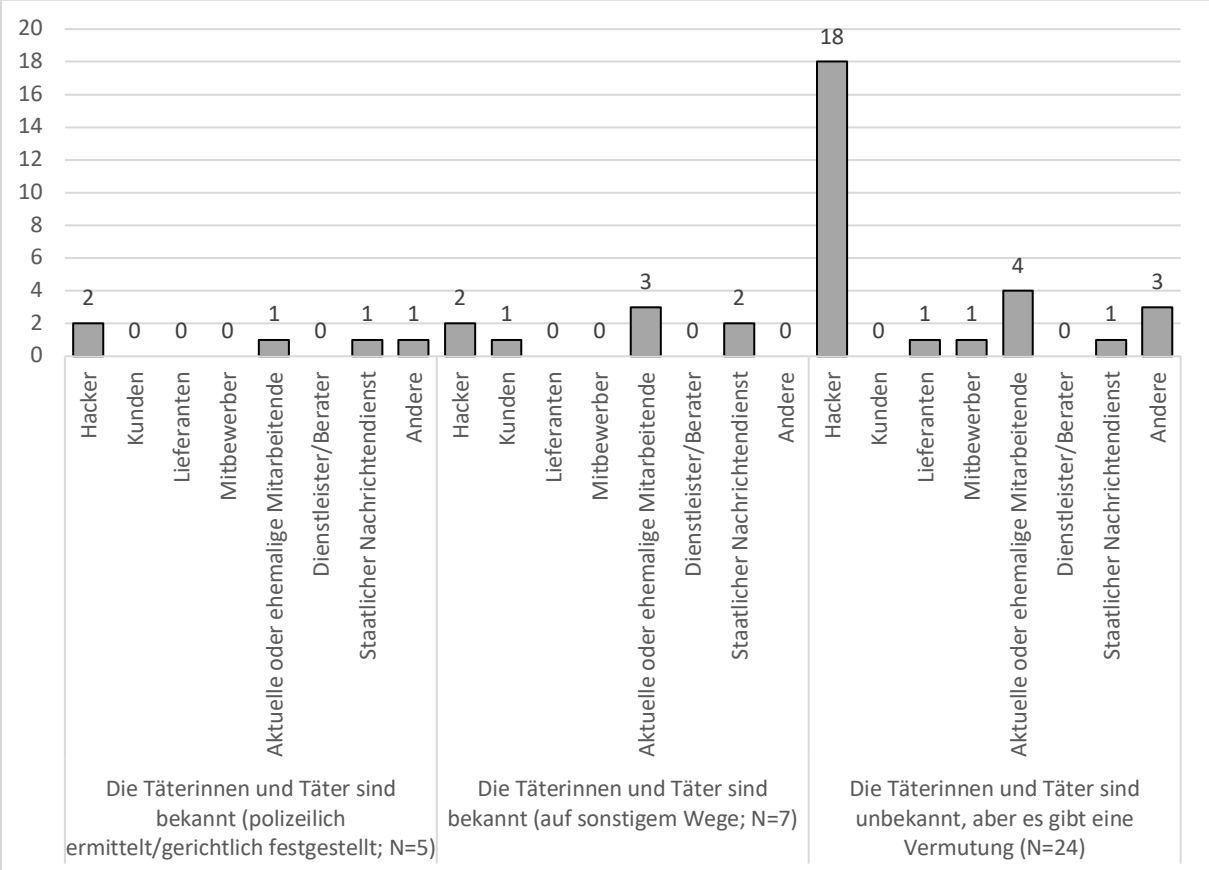
Die befragten Unternehmen wurden, in Anlehnung an die Studie von Zwahlen et al. (2020), zudem gebeten, anzugeben, ob sie wissen, wer die Täter bzw. Täterinnen des von ihnen angegebenen schwerwiegendsten Angriffs waren (siehe Frage 5 des Fragenkatalogs im Anhang).

Im Ergebnis zeigte sich, dass in der überwiegenden Mehrheit der Fälle die Täterinnen und Täter des schwersten Angriffs unbekannt sind (siehe Grafik 9). Jedes siebte Unternehmen gab an, es gäbe aber eine Vermutung. Dass der Täter bzw. die Täterin polizeilich ermittelt wurde, gaben fünf Unternehmen an. Dass der Täter bzw. die Täterin auf anderem Wege bekannt geworden ist, gaben sieben Unternehmen an.



Grafik 9: Kenntnis der Täter bzw. Täterinnen (in Prozent; N=167)

Diejenigen Unternehmen, welche angaben, der Täter bzw. die Täterinnen seien bekannt oder sie hätten eine Vermutung, wurden ergänzend gefragt, um welche Personen es sich handelt (insgesamt 36 Unternehmen; siehe Frage 6 des Fragenkatalogs im Anhang).



Grafik 10: Person des Täters/der Täterin (Mehrfachantworten möglich; Anteile ja, absolute Häufigkeiten)

Vergleichsweise häufig werden Hacker (einzeln, im Kollektiv oder organisierte Kriminalität) als Täter bzw. Täterinnen genannt, insbesondere dann, wenn die Täter bzw. Täterinnen nicht ermittelt oder auf sonstigem Wege bekannt wurden, es aber eine Vermutung gab (siehe Grafik 10). Wenn die Täter bzw. Täterinnen polizeilich ermittelt wurden, wurden von zwei Unternehmen Hacker sowie von jeweils einem Unternehmen aktuelle oder ehemalige Mitarbeitende, staatliche Nachrichtendienste und andere genannt. Sind die Täter bzw. Täterinnen auf anderem Wege bekannt geworden, wurden von drei Unternehmen aktuelle oder ehemalige Mitarbeitende angegeben, von zwei jeweils Hacker und staatliche Nachrichtendienste sowie von einem Kunden. Waren die Täter bzw. Täterinnen unbekannt, aber es gibt eine Vermutung, wurden, wie bereits geschrieben, besonders häufig Hacker genannt. Vier Unternehmen vermuten aktuelle oder ehemalige Mitarbeitende hinter dem von ihnen angegebenen schwerwiegendsten Angriff, drei benennen andere als die aufgelisteten potenziellen Täter bzw. Täterinnen. Jeweils ein Unternehmen vermutet Lieferanten, Mitbewerber und staatliche Nachrichtendienste. Diejenigen Unternehmen, die andere Täter bzw. Täterinnen als Antwortkategorie gewählt haben, wurden gebeten, nähere Angaben zu machen. Genannt wurden Einbrecher oder aber, dass sie es nicht wissen würden, die meisten IP's aber in China verortet werden könnten.

Bezüglich der Unternehmensgrösse finden sich keine statistisch signifikanten Unterschiede hinsichtlich der Kenntnis der Täter bzw. Täterinnen (siehe Tabelle 3). Von Unternehmen mit mehr als 1000 Mitarbeitenden wurde im Vergleich zu den befragten Unternehmen anderer Grösse häufiger angegeben, dass die Täter bzw. Täterinnen unbekannt seien, es aber eine Vermutung gebe. Dass die Täter bzw. Täterinnen unbekannt seien wurde am häufigsten von Unternehmen mit einer Grösse von 50-249 und 250-999 Mitarbeitenden angegeben. Etwas weniger häufig von kleineren Unternehmen mit 1-49 Mitarbeitenden und am seltensten von Unternehmen mit mehr als 1000 Mitarbeitenden.

Bezüglich der Angriffsart des schwerwiegendsten Angriffs sind die Unterschiede hingegen signifikant (siehe Tabelle 3). Erwartungsgemäss haben die befragten Unternehmen besonders häufig in Bezug auf Cybercrime und Social Engineering angegeben, dass die Täter bzw. Täterinnen nicht bekannt seien. Beim Diebstahl von Informationsmedien, dem Diebstahl von digitalen Informationen oder sensiblen physischen Dokumenten durch Mitarbeitende und bei anderen als den vorgegeben Angriffsarten bzw. einer Kombination aus mehreren Angriffen, war dies weniger häufig der Fall und die Täter bzw. Täterinnen waren häufiger bekannt. In den letztgenannten Kategorien von Angriffsarten sind die Fallzahlen jedoch z.T. sehr klein, sodass sich hinter grossen Prozentzahlen nur ein oder zwei Unternehmen verbergen.

Tabelle 3: Kenntnis der Täter bzw. Täterinnen nach Unternehmensgrösse und Angriffsart (in Prozent)

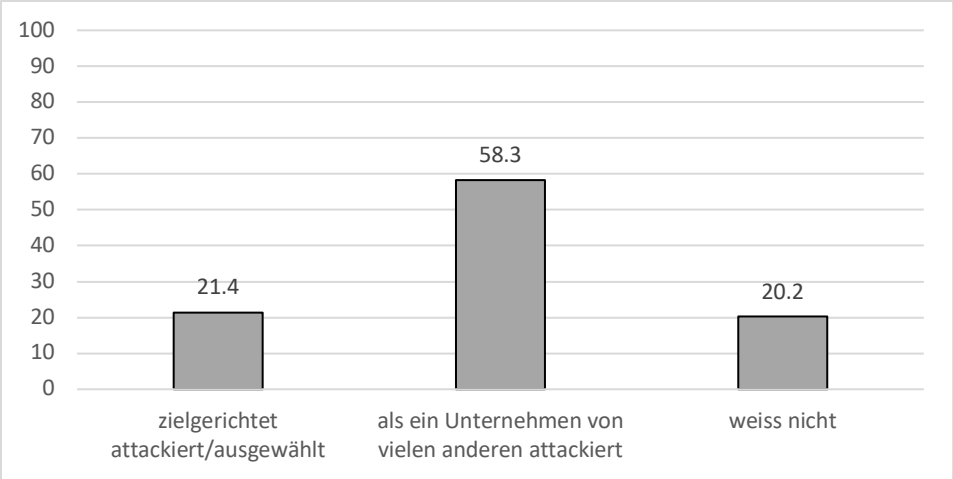
	Die Täterinnen und Täter sind bekannt (polizeilich ermittelt/gerichtlich festgestellt)	Die Täterinnen und Täter sind bekannt (auf sonstigem Wege)	Die Täterinnen und Täter sind unbekannt, aber es gibt eine Vermutung	Die Täterinnen und Täter sind unbekannt
Unternehmensgrösse				
1-49 (N=60)	3.3	6.7	11.7	78.3
50-249 (N=43)	2.3	2.3	9.3	86.0
250-999 (N=19)	0.0	0.0	10.5	89.5
> 1000 (N=34)	2.9	5.9	26.5	64.7
Angriffsart				
Cybercrime (N=90)	1.1	3.3	18.9	76.7
Abfangen digitaler Kommunikation und Datenabfluss durch Dritte (N=4)	0.0	0.0	50.0	50.0
Social Engineering (N=53)	0.0	1.9	3.8	94.3
Diebstahl von Informationsmedien (N=3)	66.7	0.0	0.0	33.3
Diebstahl von Daten/Informationen durch eigene Mitarbeitende (N=2)	0.0	50.0	50.0	0.0
Andere Angriffsart/Kombination aus mehreren Angriffsarten (N=15)	13.3	13.3	13.3	60.0

Chi-Quadrat Test Unternehmensgrösse n.s./Chi-Quadrat-Test Angriffsart p<.001.

5.3 Zielgerichtetheit des Angriffs

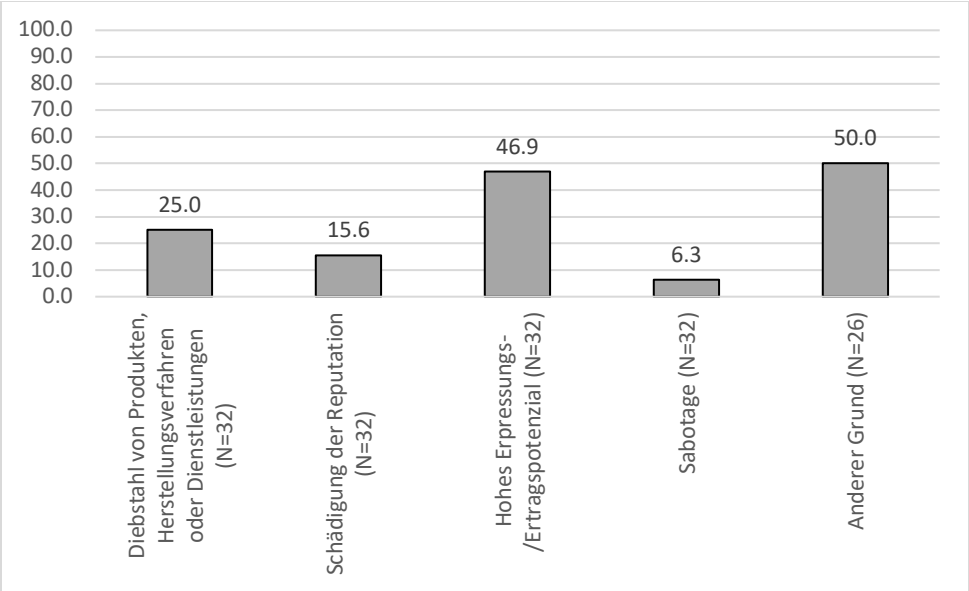
In Anlehnung an Dreissigacker et al. (2020) wurde erfasst, ob der schwerwiegendste Angriff nach Einschätzung der befragten Unternehmen zielgerichtet erfolgt ist, z.B. im Rahmen eines gezielten Spionageangriffs, oder ob das eigene Unternehmen als ein Unternehmen von vielen anderen attackiert wurde, z.B. bei massenhaft versendeter Schadsoftware, Ransomwareangriffen oder dem Ausnützen von technischen Schwachstellen (siehe Frage 7 des Fragenkatalogs im Anhang). Zudem bestand die Möglichkeit, anzugeben, dass man nicht wisse, ob der Angriff zielgerichtet erfolgt ist oder nicht.

Wie aus Grafik 11 ersichtlich ist, gab die Mehrheit an, dass sie gemäss ihrer Einschätzung als ein Unternehmen von vielen anderen attackiert wurde. Jeweils rund jedes fünfte befragte Unternehmen berichtete demgegenüber, der auf sie erfolgte schwerwiegendste Angriff war zielgerichtet oder dass sie nicht genau wissen, ob der Angriff zielgerichtet erfolgte oder nicht.



Grafik 11: Zielgerichtetheit des Angriffs (in Prozent; N=168)

An die Frage nach der Zielgerichtetheit des Angriffs anschliessend wurden diejenigen Unternehmen, die angaben, der Angriff erfolgte zielgerichtet, in Anlehnung an Dreissigacker et al. (2020) gefragt, was ihrer Einschätzung nach der Grund dafür war (siehe Frage 8 des Fragenkatalogs im Anhang). Die von Dreissigacker et al. (2020) eingesetzten Antwortmöglichkeiten wurden angepasst und um weitere Antwortmöglichkeiten ergänzt. Es waren Mehrfachantworten möglich. Es konnten also mehrere Gründe angegeben werden. Als Antwortoptionen standen jeweils die Antwortkategorien «ja», «nein» sowie «weiss nicht» zur Verfügung.



Grafik 12: Gründe für Zielgerichtetheit des Angriffs (in Prozent; Mehrfachantworten möglich; Anteile: ja)

Zu den vorgegebenen potenziellen Gründen für die Zielgerichtetheit des Angriffs wurden von 32 Unternehmen Angaben gemacht. Vergleichsweise häufig als Grund ausgewählt wurde ein hohes Erpressungs- und Ertragspotenzial (siehe Grafik 12). Ein Viertel nannte den Diebstahl von Produkten, Herstellungsverfahren oder Dienstleistungen bzw. Know how (z.B. aufgrund spezieller Technik, Design, Materialien oder Innovation). Vergleichsweise weniger relevant war die Schädigung der Reputation des Unternehmens, etwa wegen besonders gutem Image der Firma, wegen hohen Sicherheitsstandards oder besonderer Vertrauenswürdigkeit. Sabotage wurde von zwei Unternehmen als Grund angeführt. 13 Unternehmen haben zudem einen anderen Grund als Anlass für den Angriff genannt: Angesprochen wurden Aspekte wie finanzielle Bereicherung und finanzielle Schädigung, starke Exportorientierung und Spezialwerkzeuge.

Tabelle 4: Zielgerichtetheit des schwerwiegendsten Angriffs nach Unternehmensgrösse und Angriffsart (in Prozent)

	zielgerichtet attackiert/ ausgewählt	als ein Unternehmen von vielen anderen attackiert	Weiss nicht
Unternehmensgrösse			
1-49 (N=60)	18.3	60.0	21.7
50-249 (N=43)	18.6	60.5	20.9
250-999 (N=19)	21.1	52.6	26.3
> 1000 (N=35)	31.4	54.3	14.3
Angriffsart			
Cybercrime (N=90)	7.8	74.4	17.8
Abfangen digitaler Kommunikation und Datenabfluss durch Dritte (N=4)	75.0	25.0	0.0
Social Engineering (N=53)	30.2	45.3	24.5
Diebstahl von Informationsmedien (N=3)	66.7	0.0	33.3
Diebstahl von Daten/Informationen durch eigene Mitarbeitende (N=2)	50.0	0.0	50.0
Andere Angriffsart/Kombination aus mehreren Angriffsarten (N=16)	43.8	37.5	18.8

Chi-Quadrat Test Unternehmensgrösse n.s./Chi-Quadrat-Test Angriffsart p<.001.

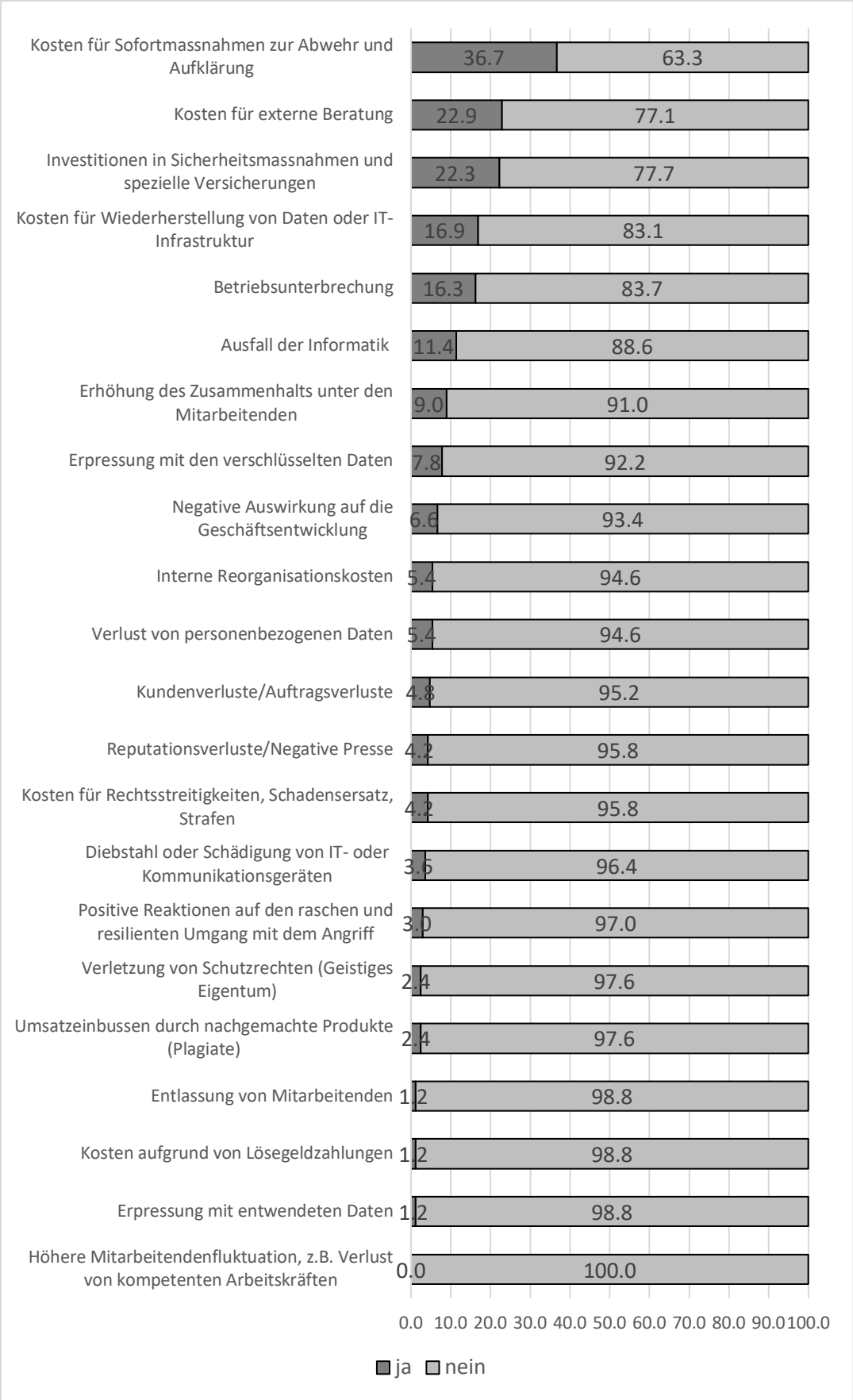
Grössere Unternehmen gaben im Vergleich zu Unternehmen anderer Grösse häufiger an, dass sie zielgerichtet attackiert wurden und seltener, dass sie als ein Unternehmen von vielen anderen attackiert wurden (siehe Tabelle 4). Diese Unterschiede sind jedoch nicht statistisch signifikant. Insgesamt ist auch bei Unternehmen aller Grössen der Anteil derjenigen, die angaben, sie seien nicht zielgerichtet attackiert worden, am grössten.

Bezüglich der Angriffsart zeigten sich hingegen signifikante Unterschiede. Insbesondere Unternehmen, die von einem Angriff aus dem Bereich Cybercrime betroffen waren, gaben häufiger an, dass sie nicht zielgerichtet, sondern als ein Unternehmen von vielen anderen attackiert wurden. Auch im Bereich des Social Engineerings äusserten mehr betroffene Unternehmen, dass sie nicht zielgerichtet attackiert wurden. Rund jedes dritte Unternehmen, das von einem Angriff aus diesem Bereich betroffen war, gab jedoch an, dass der ihnen geltende Angriff zielgerichtet war. Das Abfangen digitaler Kommunikation und der Datenabfluss durch Dritte, der Diebstahl von Informationsmedien sowie der Diebstahl von sensiblen Daten und Dokumenten durch Mitarbeitende wurden hingegen häufiger durch die Betroffenen als zielgerichtet wahrgenommen. Zu bedenken bleibt bei diesen Angriffsarten jedoch erneut, dass die Fallzahlen sehr gering sind und sich hinter hohen Prozentzahlen nur sehr wenige Unternehmen verbergen.

5.4 Folgen

Bezogen auf den schwerwiegendsten Angriff wurde zudem für insgesamt 22 potenzielle, überwiegend negative, zum Teil aber auch positive Folgen abgefragt, ob diese eingetreten sind (siehe Frage 9 des Fragenkatalogs im Anhang). Angelehnt wurde sich bei der Erfassung der Folgen an die Studien von Barth et al. (2020), Dreissigacker et al. (2020) sowie Zwahlen et al. (2020). Die dort verwendeten Formulierungen wurden zum Teil angepasst und um weitere Folgen ergänzt. Pro abgefragte Folge konnte angegeben werden, ob diese zutraf oder nicht. Es waren also Mehrfachantworten möglich.

Insgesamt 52 (31.3%) von 166 Unternehmen, denen die Frage zu den Folgen angezeigt wurde, gaben an, dass der Angriff nicht mit Folgen verbunden gewesen ist. Von den übrigen wurde mindestens eine Folge genannt. Welche Folgen wie häufig angegeben wurden, kann Grafik 13 entnommen werden.



Grafik 13: Folgen des schwerwiegendsten Angriffs (in Prozent; jeweils N=166)

Wie aus Grafik 13 ersichtlich, entstanden bei den befragten Unternehmen insbesondere Kosten durch Sofortmassnahmen zur Abwehr und Aufklärung des genannten schwersten Falls. Rund jedes dritte Unternehmen gab an, von dieser Folge betroffen gewesen zu sein. Etwa jedes Vierte berichtete von Kosten für externe Beratung und Investitionen in Sicherheitsmassnahmen und spezielle Versicherungen. Von Kosten für die Wiederherstellung von Daten oder IT-Infrastruktur (Hardware und Software) und von einer Betriebsunterbrechung (d.h. vollständiger oder teilweiser Ausfall der Produktion und Administration) war rund jedes sechste Unternehmen von allen, die Angaben zu diesen Folgen machten, betroffen. Einen Ausfall der Informatik berichtete etwa jedes neunte Unternehmen, eine Erhöhung des Zusammenhalts unter den Mitarbeitenden als eine positive Folge des Angriffs rund jedes elfte. Eine Erpressung mit den verschlüsselten Daten gaben 13 Unternehmen an, negative Auswirkungen auf die Geschäftsentwicklung wurden von elf und interne Reorganisationskosten und der Verlust von personenbezogenen Daten, z.B. Kundendaten oder Daten von Mitarbeitenden wurde jeweils von neun Unternehmen berichtet. Kunden- oder Auftragsverluste nannten acht Unternehmen als Folge, Reputationsverluste/negative Presse und Kosten für Rechtsstreitigkeiten, Schadensersatz und Strafen jeweils sieben, Diebstahl oder Schädigung von IT- oder Kommunikationsgeräten sechs und positive Reaktionen (z.B. von Kundinnen und Kunden) auf den raschen und resilienten Umgang mit dem Angriff fünf Unternehmen. Die übrigen Folgen waren weniger häufig und wurden jeweils von null bis vier Unternehmen genannt.

Zusätzlich hatten die Befragten die Möglichkeit, über eine offene Antwortmöglichkeit weitere positive und negative Folgen anzugeben. Als weitere positive Folgen wurde häufig genannt, dass der Angriff als Anlass für Sensibilisierungs- und Awarenessschulungen genutzt wurde oder aber, dass der Angriff auch ohne spezifische Schulungen zu einer weiteren Sensibilisierung der Mitarbeitenden, aber auch der Geschäftsleitung und von Führungspersonen geführt habe. So schrieb z.B. eine Firma, dass «die Awareness in der GL/VR stark angestiegen [sei] und Cyber-Security zu einem stetigen (Top) Thema wurde». Auch einige andere Firmen berichteten, dass Sicherheitsmassnahmen ausgebaut und neu etabliert wurden, z.B. in den Bereichen der Datensicherung, des Schutzes von internen Systemen (genannt wurde Zero Trust als Schlagwort) sowie bei der Aktualisierung von Betriebssystemen sowie von einer Erhöhung des Budgets für Cybersicherheit. Ein weiteres Unternehmen berichtete bezüglich der Frage nach weiteren positiven Folgen folgendes: «Obwohl das Bewusstsein für die verschiedenen Arten von Computerangriffen schon früher geschärft wurde, sind sich die Menschen erst jetzt wirklich bewusst geworden, welche Auswirkungen ein Angriff tatsächlich auf den reibungslosen Betrieb eines Unternehmens hat. Die Mentalität hat sich geändert und die Menschen sind vorsichtiger geworden. Manchmal muss man erst einen Schaden erleiden, um sich seiner Auswirkungen bewusst zu werden. Man sollte immer das Positive in schweren Schicksalsschlägen finden. Die Mitarbeiter sind gestärkt aus dieser Krise hervorgegangen und haben einen echten Teamgeist bewiesen, um das Unternehmen schnell

wieder in Gang zu bringen und die Auswirkungen auf unsere Kunden oder Partner so gering wie möglich zu halten».

Als weitere negative Folgen, neben den bereits abgefragten, wurden insbesondere finanzielle Verluste angesprochen, z.B. durch den Abfluss von Geldern, Fehlüberweisungen, Umleitungen von Zahlungen, Gelddiebstahl oder überhöhte Telefonrechnungen. Es wurden aber auch Ausfallstunden wegen Unterbrechung kompletter oder bestimmter IT-Systeme, ein erhöhter Aufwand durch interne Abstimmung und die Information und Warnung der Mitarbeitenden sowie Lecks bei technischen Daten oder ganz allgemein Zeitverlust, Zeitverschwendung und Misstrauen genannt.

In Tabelle 5 findet sich eine Darstellung der zwölf am häufigsten genannten Folgen nach Unternehmensgrösse und Angriffsart. Bezüglich der Unternehmensgrösse sind die dargestellten Unterschiede nicht statistisch signifikant. Kosten für Sofortmassnahmen zur Abwehr und Aufklärung werden etwas weniger häufig von kleinen Unternehmen mit 1-49 Mitarbeitenden berichtet. Kosten für externe Beratung entstanden am häufigsten in Unternehmen mit einer Grösse von 50-249 Mitarbeitenden. Die Unternehmen anderer Grösse unterscheiden sich diesbezüglich hingegen kaum. Investitionen in Sicherheitsmassnahmen und spezielle Versicherungen wurden mit zunehmender Unternehmensgrösse häufiger als Folge genannt. Kosten für die Wiederherstellung von Daten oder IT-Infrastruktur entstanden am seltensten in Unternehmen mit einer Grösse von 250-999 Mitarbeitenden und am häufigsten in Unternehmen mit mehr als 1000 Mitarbeitenden. Hinsichtlich der Häufigkeit von Betriebsunterbrechungen unterscheiden sich die befragten Unternehmen hingegen kaum nach Grösse. Von einem Ausfall der Informatik berichteten insbesondere Unternehmen mit 50-249 Mitarbeitenden und solche mit mehr als 1000 Angestellten. Von Unternehmen mit 250-999 Mitarbeitenden wurde diese Folge gar nicht genannt. Eine Erhöhung des Zusammenhalts unter Mitarbeitenden berichteten insbesondere Unternehmen mit einer Grösse von 50-249 Mitarbeitenden. Ebenso von einer Erpressung mit den verschlüsselten Daten. Negative Auswirkungen auf die Geschäftsentwicklung nannten hingegen häufiger kleine Unternehmen mit 1-49 Mitarbeitenden und in dieser Grössenklasse jedes zehnte Unternehmen. Interne Reorganisationskosten und den Verlust von personenbezogenen Daten (z.B. Kundendaten oder Daten von Mitarbeitenden) nannten hingegen jeweils ähnlich wenige Unternehmen. In Unternehmen mit 250-999 Mitarbeitenden wurde beides gar nicht als Folge angesprochen. Von Kundenverlusten bzw. Auftragsverlusten waren Unternehmen mit 250-999 und solche mit mehr als 1000 Mitarbeitenden im Vergleich zu Unternehmen mit 1-49 und 50-249 Mitarbeitenden häufiger betroffen, jedoch auch immer noch eher selten.

Tabelle 5: Zwölf häufigste Folgen nach Unternehmensgrösse und Angriffsart (in Prozent; Mehrfachnennungen möglich; Anteile: Folge ausgewählt)

	Kosten für Sofortmassnahmen zur Abwehr und Aufklärung	Kosten für externe Beratung	Investitionen in Sicherheitsmassnahmen/Versicherungen	Kosten für Wiederherstellung von Daten oder IT-Infrastruktur	Betriebsunterbrechung	Ausfall der Informatik	Erhöhung des Zusammenhalts unter den Mitarbeitenden	Erpressung mit den verschlüsselten Daten	Negative Auswirkung auf die Geschäftsentwicklung	Interne Reorganisationskosten	Verlust von personenbezogenen Daten	Kundenverluste/ Auftrags-verluste
Unternehmensgrösse												
1-49 (N=60)	31.7	20.0	11.7	15.0	16.7	6.7	6.7	6.7	10.0	6.7	6.7	3.3
50-249 (N=43)	37.2	30.2	23.3	16.3	16.3	18.6	16.3	14.0	2.3	7.0	7.0	2.3
250-999 (N=19)	42.1	21.1	26.3	10.5	15.8	0.0	5.3	0.0	5.3	0.0	0.0	5.3
> 1000 (N=35)	40.0	20.0	34.3	22.9	17.1	17.1	5.7	8.6	5.7	5.7	5.7	8.6
Angriffsart												
Cybercrime (N=88)	**51.1**	**34.1**	27.3	**29.5**	**25.0**	18.2	8.0	**13.6**	6.8	**2.3**	5.7	**3.4**
Abfangen digitaler Kommunikation / Datenabfluss durch Dritte (N=4)	**50.0**	**0.0**	25.0	**0.0**	**25.0**	0.0	0.0	**25.0**	25.0	**50.0**	0.0	**0.0**
Social Engineering (N=53)	**17.0**	**7.5**	9.4	**0.0**	**1.9**	1.9	13.2	**0.0**	3.8	3.8	1.9	**1.9**
Diebstahl von Informationsmedien (N=3)	**0.0**	**0.0**	33.3	**0.0**	**33.3**	0.0	0.0	**0.0**	0.0	**33.3**	0.0	**0.0**
Diebstahl von Daten/Informationen durch eigene Mitarbeitende (N=2)	**0.0**	**0.0**	0.0	**0.0**	**0.0**	0.0	0.0	**0.0**	0.0	**0.0**	0.0	**0.0**
Andere Angriffsart/ Kombination aus mehreren Angriffsarten (N=16)	**31.3**	**25.0**	37.5	**12.5**	**12.5**	12.5	6.3	**0.0**	12.5	**12.5**	18.8	**25.0**

Fett gedruckt: Unterschiede signifikant auf einem Niveau von 5%.

Bezüglich der Angriffsart zeigten sich für einige Folgen statistisch signifikante Unterschiede (siehe Tabelle 5). Kosten für Sofortmassnahmen zur Abwehr und Aufklärung wurden insbesondere von Unternehmen berichtet, die von Cybercrime, dem Abfangen digitaler Kommunikation und Datenabfluss durch Dritte, Social Engineering sowie von einer anderen Angriffsart oder einer Kombination von Angriffsarten betroffen waren. Kosten für externe Beratung entstanden nur für Betroffene von Cybercrime, Social Engineering und einer anderen Angriffsart oder einer Kombination von Angriffsarten. Investitionen in Sicherheitsmassnahmen oder spezielle Versicherungen nannten hingegen mit Ausnahme von Opfern von Diebstahl von Daten/ Informationen durch eigene Mitarbeitende Opfer aller anderen Angriffsarten. Kosten für Wiederherstellung von Daten oder IT-Infrastruktur und auch Ausfälle der Informatik entstanden insbesondere bei Unternehmen, die von Cybercrime betroffen waren. Betriebsunterbrechungen als Folge beichteten, mit Ausnahme von Betroffenen von Diebstahl von Daten/ Informationen durch eigene Mitarbeitende, betroffene Unternehmen aller anderen Angriffsarten. Eine Erhöhung des Zusammenhalts unter Mitarbeitenden wurde von Unternehmen berichtet, die von Social Engineering betroffen waren, z.T. aber auch von Betroffenen von Cybercrime und anderer Angriffsarten bzw. einer Kombination mehrerer Angriffsarten. Erpressung mit verschlüsselten Daten wurde vorwiegend von Unternehmen als Folge angegeben, die Opfer vom Abfangen digitaler Kommunikation und Datenabfluss durch Dritte wurden (hier ist die Fallzahl jedoch sehr klein) und von Opfern von Cybercrime. Interne Reorganisationskosten entstanden insbesondere für Betroffene vom Abfangen digitaler Kommunikation und Datenabfluss durch Dritte und vom Diebstahl von Informationsmedien. Bei beiden Angriffsarten ist die Fallzahl überhaupt Betroffener jedoch sehr klein. Einen Verlust von personenbezogenen Daten oder Kundenverluste bzw. Auftragsverluste berichteten insbesondere Unternehmen, die von einer anderen Angriffsart bzw. einer Kombination aus mehreren Angriffsarten betroffen waren.

5.4.1 Rangfolge der Folgen

In einem zweiten Schritt wurden diejenigen Unternehmen, die Angaben zu den Folgen gemacht haben, gebeten, diese mit Hilfe einer drag-and-drop Liste entsprechend der Einschätzung der Schwere der einzelnen Folgen für ihr Unternehmen in eine Rangfolge zu bringen. Angezeigt wurden den Unternehmen dabei nur diejenigen Folgen, bei denen sie vorher angegeben hatten, dass diese Folge bei dem von ihnen berichteten schwerstem Vorfall entstanden ist. Bei der Bildung der Rangfolge sollte die schwerste Folge eine Eins erhalten, die zweitschwerste eine Zwei usw. (siehe Frage 10 des Fragenkatalogs im Anhang).

Insgesamt haben 71 Unternehmen Angabe zur Rangfolge gemacht und eine oder mehrere der zuvor von ihnen angegebenen Folgen in eine Rangfolge gebracht. Dabei haben 16.9% bei der vorherigen Frage nur eine Folge als Antwort angegeben. Es konnte also keine Rangfolge verschiedener Folgen gebildet werden und diese eine Folge ist die schwerwiegendste. 23.9% brachten zwei verschiedene

Folgen in eine Rangfolge, weitere 23.9% drei, 8.5% vier und 26.8% mehr als fünf. Auf welchen Rang die Unternehmen, die eine Folge jeweils angegebenen haben, diese gesetzt haben, kann Tabelle 6 entnommen werden.

Tabelle 6: Rangfolge der Folgen (in Prozent)

	Rang									
	1	2	3	4	5	6	7	8	9	10
Ausfall der Informatik (N=15)	40.0	33.3	0.0	6.7	6.7	6.7	0.0	6.7	0.0	0.0
Diebstahl oder Schädigung von IT- oder Kommunikationsgeräten (N=5)	20.0	20.0	20.0	0.0	20.0	0.0	0.0	20.0	0.0	0.0
Betriebsunterbrechung (N=25)	64.0	20.0	4.0	4.0	0.0	0.0	4.0	0.0	4.0	0.0
Erpressung mit den verschlüsselten Daten (N=11)	0.0	18.2	0.0	9.1	36.4	18.2	9.1	9.1	0.0	0.0
Erpressung mit entwendeten Daten (N=2)	0.0	0.0	50.0	0.0	0.0	0.0	50.0	0.0	0.0	0.0
Kosten für Sofortmassnahmen zur Abwehr und Aufklärung (N=52)	26.9	28.8	28.8	11.5	0.0	3.8	0.0	0.0	0.0	0.0
Kosten von Lösegeldzahlungen (N=1)	0.0	100.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Kosten für Wiederherstellung von Daten oder IT-Infrastruktur (N=22)	18.2	36.4	27.3	9.1	9.1	0.0	0.0	0.0	0.0	0.0
Kosten für externe Beratung (N=33)	15.2	27.3	21.2	12.1	12.1	6.1	3.0	0.0	0.0	3.0
Kosten für Rechtsstreitigkeiten, Schadensersatz, Strafen (N=5)	80.0	0.0	0.0	0.0	0.0	20.0	0.0	0.0	0.0	0.0
Investitionen in Sicherheitsmassnahmen und spezielle Versicherungen (N=32)	37.5	15.6	12.5	6.3	9.4	12.5	6.3	0.0	0.0	0.0
Negative Auswirkung auf die Geschäftsentwicklung (N=8)	25.0	12.5	0.0	25.0	12.5	12.5	12.5	0.0	0.0	0.0
Kundenverluste/Auftragsverluste (N=7)	28.6	28.6	14.3	0.0	14.3	14.3	0.0	0.0	0.0	0.0
Umsatzeinbussen durch nachgemachte Produkte (Plagiate, N=4)	25.0	50.0	0.0	0.0	0.0	0.0	25.0	0.0	0.0	0.0
Verletzung von Schutzrechten (Geistiges Eigentum, N=3)	0.0	0.0	66.7	33.3	0.0	0.0	0.0	0.0	0.0	0.0
Verlust personenbezogener Daten (N=7)	0.0	0.0	28.6	28.6	28.6	0.0	14.3	0.0	0.0	0.0
Reputationsverluste/Negative Presse (N=7)	57.1	14.3	0.0	14.3	0.0	0.0	14.3	0.0	0.0	0.0
Interne Reorganisationskosten (N=6)	0.0	33.3	16.7	33.3	0.0	16.7	0.0	0.0	0.0	0.0
Entlassung von Mitarbeitenden (N=2)	0.0	0.0	50.0	0.0	0.0	0.0	0.0	50.0	0.0	0.0
Höhere Mitarbeitendenfluktuation, z.B. Verlust kompetenter Arbeitskräfte (N=0)	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Am häufigsten auf Rang eins gesetzt wurden im Vergleich eine Betriebsunterbrechung, Kosten für Rechtsstreitigkeiten und Reputationsverluste. Kosten für Sofortmassnahmen zur Aufklärung und Abwehr erhielt etwa ähnlich häufig die Plätze eins, zwei sowie drei. Kosten für Wiederherstellung von Daten oder IT-Infrastruktur erhielt im Vergleich zu den anderen Folgen häufiger Platz zwei, ebenso wie Kosten für externe Beratung. Die übrigen Folgen wurden im Vergleich weniger häufig überhaupt als Folge genannt und scheinen im Vergleich etwas weniger folgenschwer zu sein.

In der folgenden Auswertung wurde die Anzahl der insgesamt von den einzelnen Unternehmen in eine Rangfolge gebrachten Folgen mit Hilfe einer Kreuztabelle zur Anzahl der Unternehmen, welche eine Folge auf Rang eins gesetzt hat, in Beziehung gesetzt (siehe Tabelle 7). Dadurch lässt sich weiterführend bestimmen, wie schwer eine Folge im Vergleich zu anderen Folgen bewertet wurde. So dürfte eine Folge, die häufig auf Rang eins gesetzt wurde und bei der viele Unternehmen insgesamt viele verschiedene Folgen in eine Rangfolge gebracht haben, schwerwiegender sein, als eine Folge, die zwar von vielen Unternehmen auf Platz eins gesetzt wurde, die Folge für diese Unternehmen jedoch die einzige Folge gewesen ist und bereits deshalb auf Rang eins gesetzt wurde.

Sechs von 15 Unternehmen, die den Ausfall der Informatik in eine Rangfolge gebracht haben, setzten den Ausfall der Informatik auf Platz eins. Von diesen haben 0.0% insgesamt eine Folge in eine Rangfolge gebracht, 16.7% zwei Folgen, 16.7% drei Folgen (jeweils ein Unternehmen), 0.0% vier Folgen und 66.7% mehr als fünf Folgen. Im Vergleich zu anderen Folgen wird der Ausfall der Informatik also häufig auf Platz eins gesetzt. Diebstahl oder Schädigung von IT- oder Kommunikationsgeräten wurde nur von einer Firma auf Rang eins gesetzt. Diese hatte insgesamt zwei Folgen in Rangfolge gebracht. Diese Folge wurde aber auch insgesamt nur von wenigen Firmen genannt.

Eine Betriebsunterbrechung wurde von 16 von 25 Firmen, welche diese Folge als Folge angegeben und gerankt hatten, auf Platz eins gesetzt und insbesondere auch häufig von Unternehmen, die fünf oder mehr Folgen angegeben haben. Erpressung mit verschlüsselten Daten wurde von zwei Unternehmen auf Rang eins gesetzt. Diese haben beide fünf oder mehr Folgen angegeben. Wenn also Erpressung mit verschlüsselten Daten als Folge angegeben wurde, wurde diese im Vergleich zu anderen Folgen als eher schwer bewertet. Erpressung mit entwendeten Daten wurde nur von einem Unternehmen als schwerste Folge angesehen, wurde aber insgesamt auch nur von zwei Unternehmen überhaupt als Folge genannt. Dieses Unternehmen hatte fünf oder mehr Folgen in eine Rangfolge gebracht. Kosten für Sofortmassnahmen zur Abwehr und Aufklärung wurden von 14 von 52 Unternehmen, von denen diese Folge als Folge gerankt wurde, auf Rang eins gesetzt. Diese hatten insbesondere zwei verschiedene Folgen oder aber nur diese eine Folge genannt. Diese Folge wurde also insbesondere dann als

schwerwiegendste bewertet, wenn insgesamt nicht so viele verschiedene Folgen entstanden sind. Kosten aufgrund von Lösegeldzahlungen wurde von keinem Unternehmen auf Platz eins gesetzt und wurde auch insgesamt nur von einem Unternehmen als Folge genannt.

Tabelle 7: Nennung von Rang 1 pro Folge nach Anzahl der insgesamt von den Unternehmen in Rangfolge gebrachten Folgen (in Prozent)

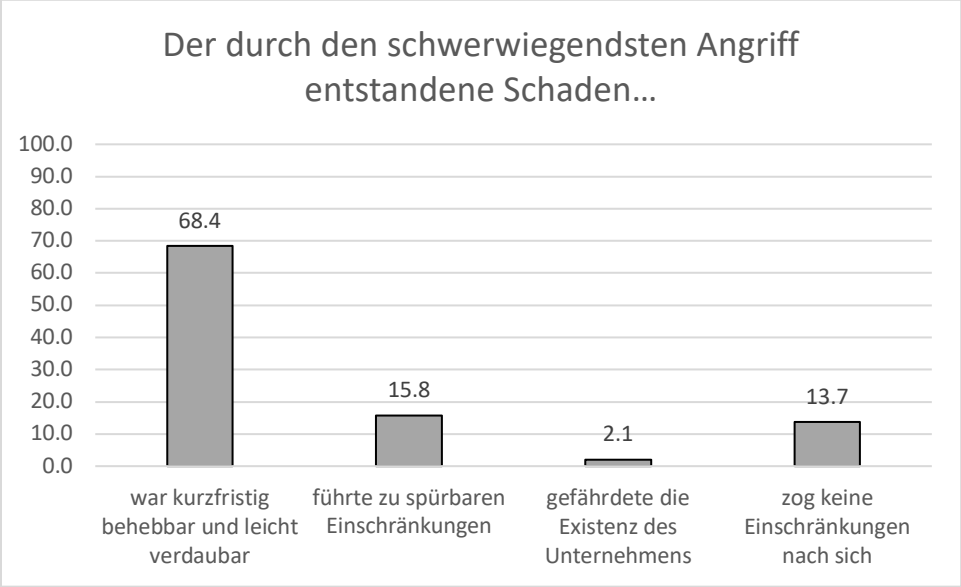
	Anzahl in Rangfolge gebrachter Folgen				
	1	2	3	4	>5
Ausfall der Informatik (N=6)	0.0	16.7	16.7	0.0	66.7
Diebstahl oder Schädigung von IT- oder Kommunikationsgeräten (N=1)	0.0	100.0	0.0	0.0	0.0
Betriebsunterbrechung (N=16)	12.5	12.5	18.8	6.3	50.0
Erpressung mit den verschlüsselten Daten (N=2)	0.0	0.0	0.0	0.0	100.0
Erpressung mit entwendeten Daten (N=1)	0.0	0.0	0.0	0.0	100.0
Kosten für Sofortmassnahmen zur Abwehr und Aufklärung (N=14)	35.7	42.9	14.3	7.1	0.0
Kosten aufgrund von Lösegeldzahlungen (N=1)	0.0	0.0	0.0	0.0	0.0
Kosten für Wiederherstellung von Daten oder IT-Infrastruktur (N=4)	25.0	50.0	0.0	0.0	25.0
Kosten für externe Beratung (N=5)	0.0	40.0	20.0	40.0	0.0
Kosten für Rechtsstreitigkeiten, Schadensersatz, Strafen (N=4)	25.0	25.0	0.0	25.0	25.0
Investitionen in Sicherheitsmassnahmen und spezielle Versicherungen (N=12)	25.0	8.3	50.0	0.0	16.7
Negative Auswirkung auf die Geschäftsentwicklung (N=2)	0.0	0.0	50.0	0.0	50.0
Kundenverluste/Auftragsverluste (N=2)	50.0	0.0	0.0	0.0	50.0
Umsatzeinbussen durch nachgemachte Produkte (Plagiate, N=1)	0.0	0.0	0.0	100.0	0.0
Verletzung von Schutzrechten (Geistiges Eigentum, N=2)	0.0	0.0	0.0	50.0	50.0
Verlust von personenbezogenen Daten (N=2)	0.0	0.0	0.0	50.0	50.0
Reputationsverluste/Negative Presse (N=4)	0.0	0.0	75.0	0.0	25.0
Interne Reorganisationskosten (N=2)	0.0	50.0	0.0	0.0	50.0
Entlassung von Mitarbeitenden (N=1)	0.0	0.0	0.0	0.0	100.0
Höhere Mitarbeitendenfluktuation, z.B. Verlust von kompetenten Arbeitskräften (N=0)	0.0	0.0	0.0	0.0	0.0

Vier von 22 Unternehmen, welche Kosten für die Wiederherstellung von Daten oder IT-Infrastruktur in eine Rangfolge gebracht haben, haben diese Folge auf Platz eins gesetzt. Diese Unternehmen haben vorwiegend ein bis zwei Folgen angegeben. Eines dieser Unternehmen fünf und mehr Folgen. Kosten für externe Beratung wurden von fünf von 33 Unternehmen, die von dieser Folge betroffen waren und diese in eine Rangfolge brachten, haben diese Folge auf Platz eins gesetzt. Von diesen fünf Unternehmen wurden zwei bis vier verschiedene Folgen in eine Rangfolge gebracht. Fünf oder mehr Folgen wurden gar nicht in Rangfolge gebracht. Kosten für Rechtsstreitigkeiten wurden von vier von fünf Unternehmen auf Rang eins gesetzt. Von diesen hat jeweils eins eine Folge, zwei Folgen, vier Folgen und fünf oder mehr Folgen in Rangfolge gebracht. Investitionen in Sicherheitsmassnahmen und spezielle Versicherungen brachten insgesamt 32 Unternehmen in eine Rangfolge. Für zwölf von diesen war dies die schwerwiegendste Folge. Diese haben insbesondere drei verschiedene Folgen in eine Rangfolge gebracht. Negative Auswirkungen auf die Geschäftsentwicklung wurde von zwei von acht Unternehmen auf Rang eins gesetzt. Diese haben einmal drei und einmal fünf oder mehr verschiedene Folgen in eine Rangfolge gebracht. Kunden- bzw. Auftragsverluste wurden von zwei von sieben Unternehmen, welche diese Folge in eine Rangfolge brachten, als schwerste Folge genannt. Für eines der Unternehmen war diese Folge die einzige Folge, für das andere die schwerste von fünf oder mehr Folgen. Umsatzeinbussen durch nachgemachte Produkte wurde von einem von vier Unternehmen auf Platz eins gesetzt. Dieses brachte insgesamt vier verschiedene Folgen in eine Rangfolge. Die Verletzung von Schutzrechten (geistiges Eigentum) war für zwei von drei Unternehmen die schwerste Folge. Diese brachten insgesamt vier respektive fünf oder mehr verschiedene Folgen in eine Rangfolge. Der Verlust von personenbezogenen Daten (z.B. Kundendaten oder Daten von Mitarbeitenden) war für zwei von sieben Unternehmen, die diese Folge in Rangfolge brachten, die schwerste. Diese brachten insgesamt wiederum vier bzw. fünf oder mehr verschiedene Folgen in eine Rangfolge. Reputationsverluste bzw. eine negative Presse wurden von vier von sieben Unternehmen auf Rang eins gesetzt. Von diesen brachten drei jeweils drei verschiedene Folgen in eine Rangfolge und eines fünf oder mehr. Interne Reorganisationskosten wurden von zwei von sechs Unternehmen als schwerste Folge bewertet. Von diesen brachte ein Unternehmen insgesamt zwei Folgen in eine Rangfolge und das andere fünf oder mehr. Die Entlassung von Mitarbeitenden setzte eins von zwei Unternehmen auf Platz eins. Dieses brachte insgesamt fünf oder mehr Folgen in eine Rangfolge. Eine höhere Mitarbeitendenfluktuation wurde, wie bereits dargestellt, von keinem Unternehmen als Folge genannt und dadurch auch von keinem Unternehmen in eine Rangfolge gebracht.

5.4.2 Schaden

Neben den Folgen und einer Rangfolge der Folgen wurden die Unternehmen ausserdem gebeten, nähere Angaben zum durch den schwerwiegendsten Angriff entstandenen Schaden zu machen und den entstandenen Schaden zu beziffern (in CHF; siehe die Fragen 11 und 12 des Fragenkatalogs im Anhang).

Die Erfassung der näheren Angaben zum entstandenen Schaden erfolgte in Anlehnung an Zwahlen et al. (2020). Zur Erfassung der Schadenshöhe wurden die Befragten gebeten, im Rahmen einer offenen Antwortmöglichkeit die Höhe des Schadens einzutragen. Diese beiden Fragen zum Schaden wurden nur denjenigen Unternehmen angezeigt, die nicht angegeben hatten, dass aus dem für sie schwerwiegendsten Angriff keine Folgen entstanden sind. Wie aus Grafik 14 ersichtlich, führte der durch den schwerwiegendsten Angriff verursachte Schaden bei der Mehrheit der befragten Unternehmen nicht zu starken Einschränkungen.



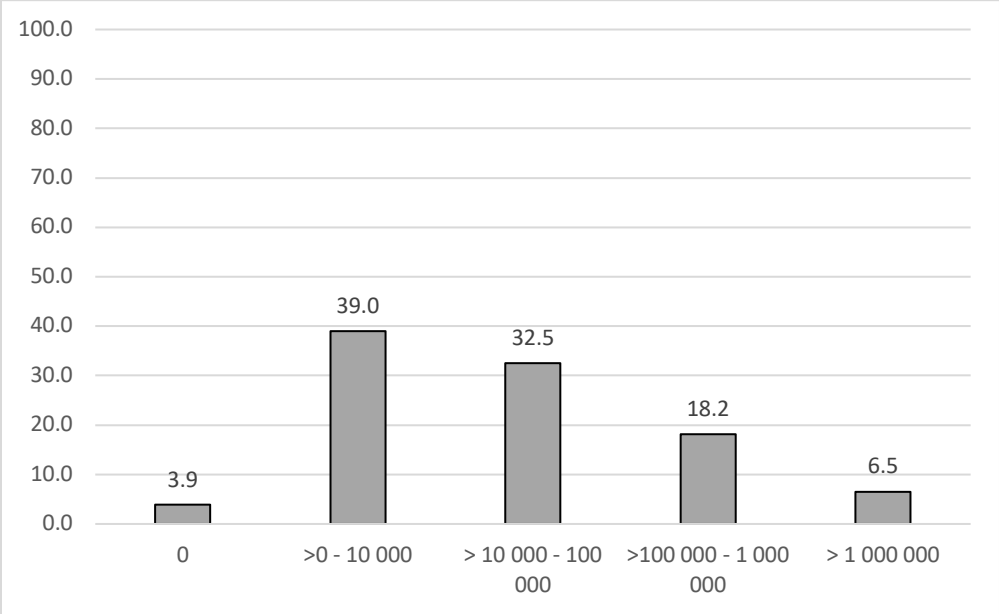
Grafik 14: Nähere Angaben zum entstandenen Schaden (in Prozent; N=95)

Etwas mehr als zwei Drittel der Unternehmen gab an, der Schaden war kurzfristig behebbar und leicht verdaubar. Bei rund jedem sechsten Unternehmen führte der entstandene Schaden hingegen zu spürbaren Einschränkungen, bei zwei Unternehmen gefährdete er sogar die Existenz des Unternehmens. Rund jedes siebte Unternehmen gab an, der durch den schwerwiegendsten Angriff entstandene Schaden zog keine Einschränkungen nach sich.

Insgesamt 77 Unternehmen haben zudem Angaben zur Schadenshöhe gemacht: Das Minimum betrug 0 CHF, das Maximum 2 000 000 CHF. Im Durchschnitt betrug der Schaden 205 142.86 CHF. Der Median und damit der Wert, der genau in der Mitte der von den Unternehmen im einzelnen genannten Summen liegt, beträgt 30 000.00 CHF.

In Anlehnung an die Studie von Zwahlen et al. (2020) wurden die Angaben der Befragten anschliessend in Kategorien eingeteilt (siehe Grafik 15). Die Mehrheit der Unternehmen, die Angaben zum Schaden machten, beziffern diesen mit einer Summe von mehr als null bis zu 10 000 CHF. Dies trifft auf fast 40 Prozent der Unternehmen zu. Etwa bei einem Drittel entstand ein Schaden zwischen 10 000 und 100

000 CHF, bei rund jedem fünften befragten Unternehmen ein Schaden zwischen 100 000 und 1 000 000 CHF und bei fünf Unternehmen ein Schaden von mehr als 1 000 000 CHF.



Grafik 15: Schadenshöhe kategorisiert (in Prozent; N=77)

Bezüglich der Unternehmensgrösse zeigen sich keine statistisch signifikanten Unterschiede in der Bewertung des durch den schwerwiegendsten Angriff entstandenen Schadens (siehe Tabelle 8). Unternehmen aller Grössen berichteten am häufigsten, der entstandene Schaden sei kurzfristig behebbar und leicht verdaubar gewesen. Zu spürbaren Einschränkungen führte er weniger häufig in den kleinsten Unternehmen mit einer Mitarbeiterzahl von 1-49. Zu einer Existenzgefährdung führte er bei einem Unternehmen mit einer Grösse von 1-49 Mitarbeitenden und einem Unternehmen mit einer Grösse von 50-249 Mitarbeitenden. In Unternehmen der anderen beiden Grössenklassen kam dies hingegen gar nicht vor.

Hohe Schadenssummen in Höhe von 1 000 000 CHF und mehr entstanden häufiger in grösseren Unternehmen mit 250-999 und mehr als 1000 Mitarbeitenden. In Unternehmen mit einer Grösse von 1-49 Mitarbeitenden berichtete die Mehrheit der Unternehmen, welche die Frage zur Schadenshöhe beantwortet haben, von einem Schaden zwischen mehr als null und 10 000 CHF (siehe Tabelle 8). Bei Unternehmen mit 50-249 Mitarbeitenden entfiel der höchste Anteil auf eine Schadenshöhe von 10 000 bis 100 000 CHF, bei Unternehmen mit 250 bis 999 Mitarbeitenden ebenfalls. Bei Unternehmen mit mehr als 1000 Mitarbeitenden entfielen die grössten Anteile gleichermassen auf eine Schadenssumme zwischen 10 000 und 100 000 CHF sowie auf eine Schadenssumme zwischen 100 000 und 1 000 000 CHF. Diese Unterschiede erwiesen sich auch als statistisch signifikant.

Tabelle 8: Nähere Angaben zum Schaden und der Schadenshöhe nach Unternehmensgrösse und Angriffsart (in Prozent)

	Nähere Angaben zum Schaden				Schadenshöhe				
	war kurzfristig behebbar und leicht verdaubar	führte zu spürbaren Einschränkungen	gefährdete die Existenz des Unternehmens	zog keine Einschränkungen nach sich	0	>0 - 10 000	> 10 000 - 100 000	>100 000 - 1 000 000	> 1 000 000
Unternehmensgrösse									
1-49 (NSchaden=35; NSchadenshöhe=29)	74.3	8.6	2.9	14.3	6.9	69.0	13.8	6.9	3.4
50-249 (NSchaden=21; NSchadenshöhe=20)	61.9	23.8	4.8	9.5	0.0	30.0	45.0	25.0	0.0
250-999 (NSchaden=12; NSchadenshöhe=7)	58.3	16.7	0.0	25.0	14.3	14.3	42.9	14.3	14.3
> 1000 (NSchaden=23; NSchadenshöhe=18)	69.6	21.7	0.0	8.7	0.0	16.7	33.3	33.3	16.7
Angriffsart									
Cybercrime (NSchaden=61; NSchadenshöhe=45)	70.5	18.0	1.6	9.8	0.0	46.7	31.1	17.8	4.4
Abfangen digitaler Kommunikation und Datenabfluss durch Dritte (NSchaden=2; NSchadenshöhe=2)	100.0	0.0	0.0	0.0	0.0	0.0	50.0	50.0	0.0
Social Engineering (NSchaden=18; NSchadenshöhe=18)	66.7	5.6	0.0	27.8	11.1	44.4	44.4	0.0	0.0
Diebstahl von Informationsmedien (NSchaden=2; NSchadenshöhe=2)	100.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	0.0
Diebstahl von Daten/Informationen durch eigene Mitarbeitende (NSchaden=1; NSchadenshöhe=0)	0.0	0.0	0.0	100.0	0.0	0.0	0.0	0.0	0.0
Andere Angriffsart/Kombination aus mehreren Angriffsarten (NSchaden=11; NSchadenshöhe=10)	54.5	27.3	9.1	9.1	10.0	10.0	20.0	30.0	30.0

Chi-Quadrat Test Unternehmensgrösse nähere Angaben zum Schaden n.s.; Schadenshöhe p<.03/Chi-Quadrat-Test Angriffsart nähere Angaben zum Schaden n.s.; Schadenshöhe p<.03

Bezüglich der Unterschiede bei den näheren Angaben zum entstandenen Schaden nach Angriffsart erwiesen sich die in Tabelle 8 dargestellten Unterschiede nicht als statistisch signifikant. Bei der Angriffsart Cybercrime gab die Mehrheit der Unternehmen, welche die Frage beantwortet haben, an, der Schaden sei kurzfristig behebbar und leicht verdaubar gewesen. Für rund jedes sechste Unternehmen entstanden jedoch spürbare Einschränkungen und ein Unternehmen berichtete von einer Existenzgefährdung. Bei Angriffen aus dem Bereich Social Engineering entstand für die weit überwiegende Mehrheit ein leicht behebbarer oder kein Schaden. Ein Unternehmen berichtete von spürbaren Einschränkungen. Unternehmen, die von einer anderen Angriffsart oder einem Angriff, bei dem mehrere Angriffsarten kombiniert wurden, betroffen waren, berichteten in drei Fällen von spürbaren Einschränkungen. Für ein Unternehmen war dieser Angriff existenzbedrohend. Aber auch hier gab die Mehrheit an, der Schaden sei leicht behebbar gewesen. Der durch Cybercrime entstandene Schaden belief sich bei knapp der Hälfte der von dieser Angriffsart betroffenen Unternehmen auf eine Summe zwischen mehr als null und 10 000 CHF. Jedes dritte Unternehmen berichtete einen Schaden in Höhe von 10 000 bis 100 000 CHF, rund jedes sechste einen Schaden in Höhe von 100 000 bis 1 000 000 CHF sowie zwei Unternehmen einen Schaden in Höhe von mehr als 1 000 000 CHF. Bei von Social Engineering betroffenen Unternehmen waren die Schadenssummen im Vergleich etwas geringer und beliefen sich auf Summen zwischen mehr als null und 100 000 CHF. Von anderen Angriffsarten oder einer Kombination mehrerer Angriffsarten betroffene Unternehmen berichteten überwiegend von eher höheren Schadenssummen zwischen mehr als 100 000 und mehr als 1 000 000 CHF, jedes fünfte Unternehmen berichtete aber auch von einem Schaden zwischen 10 000 und 100 000 CHF und jedes zehnte von einem zwischen mehr als null und 10 000 CHF.

Bei den Angriffsarten Abfangen von digitaler Kommunikation und Abfluss von Daten durch Dritte, Diebstahl von Informationsmedien sowie Diebstahl von Daten oder Informationen durch Mitarbeitende sind die Fallzahlen wiederum sowohl bei den näheren Angaben zum Schaden als auch bei der Schadenshöhe sehr gering. Bei der Schadenshöhe wurden von Betroffenen der Angriffsart Diebstahl von Daten oder Informationen durch Mitarbeitende gar keine Angaben gemacht. Die beiden Unternehmen, die vom Abfangen digitaler Kommunikation oder vom Abfluss von Daten durch Dritte betroffen waren, gaben an, der Schaden habe kurzfristig behoben werden können. Ebenso bei den Betroffenen durch einen Diebstahl von Informationsmedien. Für das durch einen Diebstahl von Daten oder Informationen durch Mitarbeitende betroffenen Unternehmen ist gar kein Schaden entstanden. Der Schaden, der durch das Abfangen digitaler Kommunikation entstand, belief sich bei einem Unternehmen auf eine Summe zwischen 10 000 und 100 000 CHF, bei dem zweiten zwischen 100 000 und 1 000 000

CHF. Der durch den Diebstahl von Kommunikationsmedien entstandene Schaden betrug bei beiden Unternehmen zwischen 100 000 und 1 000 000 CHF.

5.4.3 Lösegeldforderung

Wenn Erpressung mit den verschlüsselten oder entwendeten Daten als Folge angegeben wurde, wurde als Anschlussfrage die Frage danach gestellt, ob es eine Lösegeldforderung gab (siehe Frage 13 des Fragenkatalogs im Anhang). Diese Frage wurde von 13 Firmen beantwortet. Zehn von diesen (76.9%) bejahten diese Frage, eine (7.7%) Firma verneinte. Weitere zwei (15.4%) Firmen haben die Antwortoption «weiss nicht» ausgewählt.

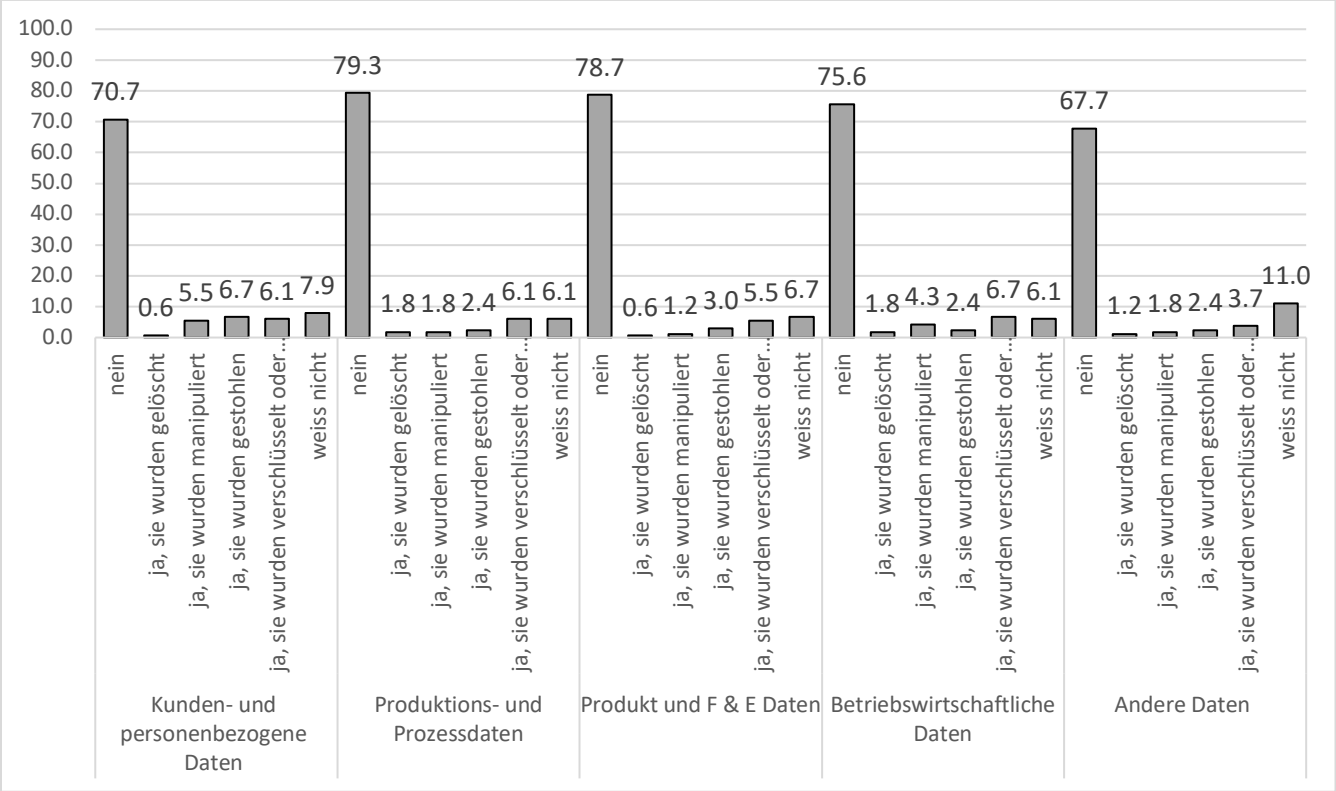
5.5 Betroffene Daten

An die Fragen nach den Folgen anschliessend wurden die Firmen gefragt, welche Daten bei dem von ihnen angegebenen schwerwiegendsten Vorfall betroffen waren. Die Frage wurde allen Firmen gestellt, die einen schwerwiegendsten Vorfall angegeben hatten und die Erfassung erfolgte, mit einigen Anpassungen, in Anlehnung an die Studie von Dreissigacker et al. (2020; siehe Frage 14 des Fragenkatalogs im Anhang). Berücksichtigt wurden alle in Grafik 16 aufgeführten Arten von Daten und es konnten pro Datentyp Angaben gemacht werden. Zudem waren jeweils Mehrfachantworten möglich. Es konnte also sowohl angegeben werden, dass Daten gelöscht als auch, dass Daten manipuliert wurden usw., da davon ausgegangen werden kann, dass Mehreres gleichzeitig vorkommen kann.

In Grafik 16 dargestellt sind jeweils die Anteile der Unternehmen, welche die jeweilige Antwortoption ausgewählt haben. Bei allen Arten von Daten hat die Mehrheit der befragten Unternehmen angegeben, dass diese nicht betroffen waren. Im Vergleich zu Produktions- und Prozessdaten sowie Produkt und F & E Daten waren kunden- und personenbezogene Daten häufiger betroffen. Hier ist der Anteil der Unternehmen, die insgesamt eine Betroffenheit in irgendeiner Form berichteten, grösser und der Anteil jener Unternehmen, die keine Betroffenheit bei diesem Datentyp angegeben haben, geringer. Bei allen Arten von Daten gilt, dass diese insbesondere verschlüsselt und seltener gestohlen, manipuliert oder gelöscht wurden. Eine Ausnahme bilden kunden- und personenbezogene Daten. Diese wurden etwa ähnlich häufig bzw. geringfügig häufiger gestohlen als verschlüsselt. Bei allen abgefragten Datentypen hat zudem jedes 13. bis 16. Unternehmen angegeben, dass es nicht wisse, ob entsprechende Daten betroffen sind oder nicht.

Einige Unternehmen haben zudem eine Betroffenheit von anderen als den bereits vorgegebenen Daten angesprochen, auch wenn auch hier der Anteil derjenigen, die auch bei anderen Daten keine Betroffenheit berichten am grössten ist. Diejenigen, die angegeben hatten, dass andere Daten betroffen waren, wurden zusätzlich gebeten, anzugeben, welche anderen Daten betroffen gewesen sind. Genannt wurden häufig E-Mails und Zugangsdaten sowie darüber hinaus Daten aus dem Active Directory

(Windows-Verzeichnis), Informationen über die Struktur/Architektur der internen Informationssysteme, Konfigurationsdateien eines Servers, das Adressbuch des betroffenen Nutzers, Veränderung von Kontodaten (z.B. von einem Lieferanten) sowie die Website.



Grafik 16: Beim schwerwiegendsten Angriff betroffene Daten (in Prozent; Mehrfachantworten möglich; jeweils N=164)

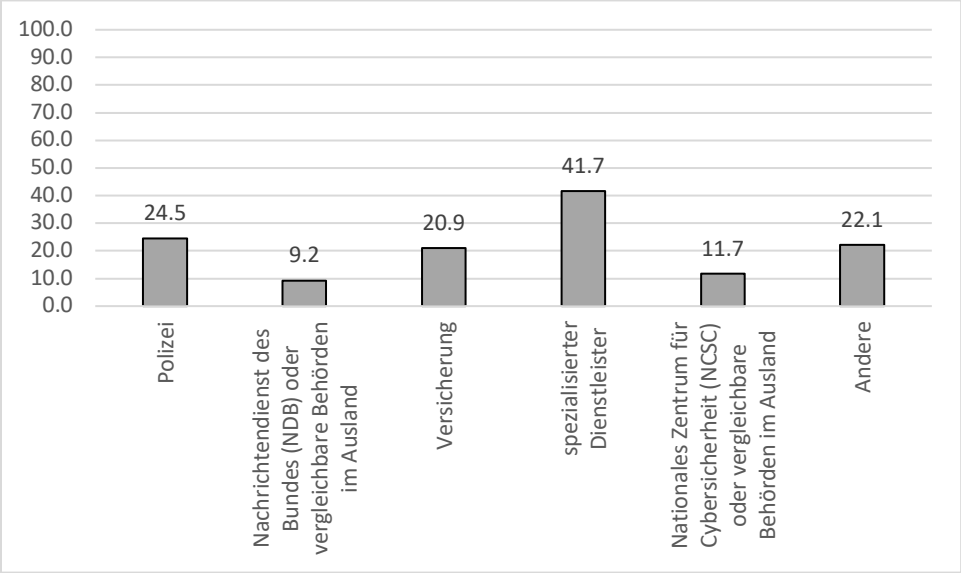
Eine Firma berichtete, dass vor allem die Daten, die auf den persönlichen Bereichen der Mitarbeitenden gespeichert waren (Analysen, Sitzungsberichte usw.), verloren gingen. Es wurde aber auch davon berichtet, dass vom Prinzip her alle der genannten Datentypen betroffen gewesen sein könnten und man es nicht sicher sagen könnte oder dass zum Glück rechtzeitig erkannt wurde, dass ein Angriff stattgefunden hat bzw. stattfindet und die weitere Verschlüsselung von Daten so abgewendet werden konnte. Bei letzterem Fall wurden dadurch nur Teile verschiedener Daten verschlüsselt und diese konnten auch erfolgreich wiederhergestellt werden. Auch andere Firmen gaben an, dass sie Glück gehabt hätten und dass Schlimmeres verhindert werden konnte.

5.6 Kontaktaufnahme zu Akteurinnen und Akteuren

In Anlehnung an die Studie von Zwahlen et al. (2020) wurden die Unternehmen, welche einen schwerwiegendsten Angriff berichtet haben, gefragt, ob nach dem schwerwiegendsten Angriff zu einer Reihe von Akteurinnen und Akteuren (z.B. Polizei, Nachrichtendienst des Bundes oder einer Versicherung)

Kontakt aufgenommen wurde (siehe Frage 15 des Fragenkatalogs im Anhang sowie Grafik 17). Es waren Mehrfachantworten möglich. Es konnten somit mehrere Akteurinnen und Akteure angegeben werden.

Von den verschiedenen vorgegebenen Akteurinnen und Akteuren wurde am häufigsten angegeben, dass spezialisierte Dienstleister kontaktiert wurden (siehe Grafik 17). Rund ein Viertel der Unternehmen, welche diese Frage beantworteten, hatte zudem Kontakt zur Polizei aufgenommen. Kontakt zur Versicherung hatte rund jedes fünfte befragte Unternehmen. Etwa gleich viele kontaktierten zudem andere, nicht im Fragebogen genannte Akteurinnen und Akteure. Im Vergleich deutlich seltener, nämlich von ungefähr jedem neunten befragten Unternehmen, wurde Kontakt zum Nationalen Zentrum für Cybersicherheit (NCSC) oder zu einer vergleichbaren Behörde im Ausland aufgenommen. Kontakt zum Nachrichtendienst des Bundes (NDB) oder zu einer vergleichbaren Behörde im Ausland nahm rund jedes elfte Unternehmen auf.



Grafik 17: Kontaktaufnahme zu Akteurinnen und Akteuren (in Prozent; Mehrfachantworten möglich; N=163 (jeweils))

Diejenigen Unternehmen, die als Antwortoption «Andere» gewählt hatten, wurden zudem gebeten, anzugeben, um welche Akteurinnen bzw. Akteure es sich handelte. Genannt wurden die Bank, Beauftragte für Datenschutz, Behörden vor Ort, wenn der Angriff im Ausland stattgefunden hatte (erwähnt wurden z.B. Deutschland und China), die eigene IT-Abteilung und IT-Sicherheitsberatende, die interne Rechtsabteilung, Betreibende des Rechenzentrums oder Vertriebspartnerinnnen und Vertriebspartner im Ausland. Genannt wurde ausserdem MELANI, die Melde- und Analysestelle Informationssicherung. Einige Unternehmen gaben aber auch an, dass nur das Kader sensibilisiert wurde oder aber dass man ohne weitere Hilfe und Unterstützung den Angriff bewältigen konnte.

Wie aus Tabelle 9 ersichtlich, unterscheiden sich die Antworten aus Unternehmen verschiedener Grösse insbesondere hinsichtlich der Kontaktaufnahme zur Polizei statistisch signifikant voneinander. Insbesondere grosse Unternehmen mit mehr als 1000 Mitarbeitenden haben aufgrund des von ihnen berichteten schwerwiegendsten Angriff Kontakt zur Polizei aufgenommen. Eine Kontaktaufnahme zum NDB oder zu einer vergleichbaren Behörde erfolgte am häufigsten durch Unternehmen mit einer Grösse von 250-999 Mitarbeitenden. Kontakt zur Versicherung wurde im Vergleich wiederum häufiger von Unternehmen mit mehr als 1000 Mitarbeitenden aufgenommen. Eine Kontaktaufnahme zu spezialisierten Dienstleistern erfolgte im Vergleich wiederum häufiger von Unternehmen mit einer Grösse von 250-999 Mitarbeitenden, aber auch von denen mit einer Grösse von mehr als 1000 Mitarbeitenden. Unternehmen mit einer Grösse von mehr als 1000 Mitarbeitenden nahmen auch am häufigsten Kontakt zum NCSC oder einer vergleichbaren Behörde im Ausland auf. Bei allen abgefragten Akteurinnen und Akteuren (mit Ausnahme von anderen Akteurinnen bzw. Akteuren) erfolgte die Kontaktaufnahme zu den abgefragten Akteurinnen und Akteuren im Vergleich seltener durch Unternehmen mit einer Grösse von 1-49 Mitarbeitenden.

Bezüglich allfälliger Unterschiede in der Häufigkeit der Kontaktaufnahme zu den verschiedenen Akteurinnen und Akteuren nach Angriffsart zeigten sich hinsichtlich der Kontaktaufnahme mit spezialisierten Dienstleistern statistisch signifikante Unterschiede (siehe Tabelle 9). Diese wurden besonders häufig kontaktiert, wenn ein schwerwiegendster Angriff aus dem Bereich Cybercrime, Diebstahl von Daten oder Informationen durch eigene Mitarbeitende oder eine andere Angriffsart bzw. Kombination von mehreren Angriffsarten berichtet wurde. Bei den Angriffsarten Abfangen digitaler Kommunikation und Datenabfluss durch Dritte, Diebstahl von Informationsmedien sowie Diebstahl von Daten/Informationen durch eigene Mitarbeitende gilt jedoch wiederum zu beachten, dass die Fallzahlen sehr gering sind und sich hinter hohen Prozentzahlen nur sehr wenige Firmen verbergen.

Betroffene von einem Abfangen digitaler Kommunikation und Datenabfluss durch Dritte, Diebstahl von Informationsmedien und einer anderen Angriffsart bzw. Kombination von mehreren Angriffsarten haben vergleichsweise häufiger die Polizei kontaktiert. Dies trifft auch auf rund ein Viertel der von Cybercrime betroffene Unternehmen zu sowie auf jedes sechste von Social Engineering betroffene Unternehmen. Eine Kontaktaufnahme zum Nachrichtendienst des Bundes (NDB) oder zu einer vergleichbaren Behörde im Ausland erfolgte nur durch von Cybercrime, Social Engineering oder einer anderen Angriffsart bzw. Kombination aus mehreren Angriffsarten betroffene Unternehmen. Insgesamt jedoch auch von diesen eher selten.

Kontakt zur Versicherung wurde von zwei von drei Unternehmen aufgenommen, die von einem Diebstahl von Informationsmedien betroffen waren, sowie auch von zwei der insgesamt vier Unternehmen, die einen schwerwiegendsten Angriff aus dem Bereich Abfangen digitaler Kommunikation und Datenabfluss durch Dritte angegeben haben. Von den von Cybercrime betroffenen Unternehmen gab rund

jedes fünfte an, die Versicherung kontaktiert zu haben. Zum Nationalen Zentrum für Cybersicherheit (NCSC) oder zu einer vergleichbaren Behörde im Ausland wurde insbesondere von Unternehmen Kontakt aufgenommen, die von Cybercrime oder dem Abfangen digitaler Kommunikation und Datenabfluss durch Dritte betroffen waren.

Tabelle 9: Kontaktaufnahme zu Akteurinnen und Akteuren nach Unternehmensgrösse und Angriffsart (in Prozent; Mehrfachantworten möglich)

	Polizei	NDB oder vergleichbare Behörden im Ausland	Versicherung	spezialisierter Dienstleister	NCSC oder vergleichbare Behörden im Ausland	Andere
Unternehmensgrösse						
1-49 (N=60)	**13.3**	8.3	13.3	36.7	6.7	21.7
50-249 (N=43)	**27.9**	9.3	18.6	37.2	14.0	20.9
250-999 (N=19)	**21.1**	15.8	21.1	57.9	10.5	21.1
> 1000 (N=35)	**42.9**	8.6	37.1	45.7	20.0	22.9
Angriffsart						
Cybercrime (N=87)	24.1	11.5	21.8	**55.2**	17.2	13.8
Abfangen digitaler Kommunikation und Datenabfluss durch Dritte (N=4)	50.0	0.0	50.0	**25.0**	25.0	0.0
Social Engineering (N=52)	17.3	7.7	13.5	**21.2**	3.8	34.6
Diebstahl von Informationsmedien (N=3)	66.7	0.0	66.7	**0.0**	0.0	0.0
Diebstahl von Daten/Informationen durch eigene Mitarbeitende (N=2)	0.0	0.0	0.0	**50.0**	0.0	0.0
Andere Angriffsart/Kombination aus mehreren Angriffsarten (N=15)	40.0	6.7	26.7	**46.7**	6.7	40.0

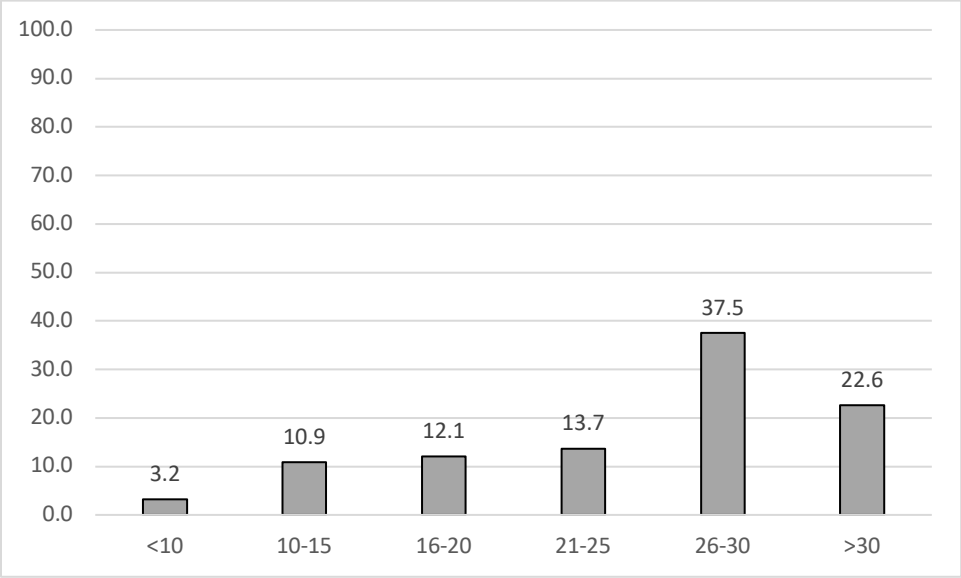
Fett gedruckt: Unterschiede signifikant auf einem Niveau von 5%.

6 Schutz- und Interventionsmassnahmen

Um zu erfassen, welche Massnahmen die befragten Unternehmen ergriffen haben, um sich gegen Angriffe zu schützen, wurde für insgesamt 34 verschiedene Schutz- und Interventionsmassnahmen abgefragt, ob diese im Unternehmen eingesetzt werden oder nicht (siehe die Frage 16 des Fragenkatalog im Anhang sowie Tabelle 11). Zusätzlich bestand die Möglichkeit, weitere Massnahmen anzugeben.

Gestützt wurde sich dabei wiederum auf die Studien von Barth et al. (2020), Dreissigacker et al. (2020) sowie Zwahlen et al. (2020). Die abgefragten Massnahmen dienen je nachdem der Identifikation von Schwachstellen und Risiken und der Sensibilisierung für diese, dem Schutz vor Angriffen, dem Erkennen von Angriffen, der Reaktion auf Angriffe sowie dem Reparieren potenzieller Schäden. Die Fragen zu den Schutzmassnahmen wurden allen teilnehmenden Unternehmen gestellt und nicht nur denjenigen, die einen schwerwiegendsten Vorfall angegeben hatten.

Insgesamt haben 248 Unternehmen zu einer oder mehreren Schutz- und Interventionsmassnahmen Angaben gemacht. Im Durchschnitt wurden für 24.8 von 35 (SD 7.1; einschliesslich der Antwortoption «weitere Massnahmen») Massnahmen angegeben, dass diese vorhanden seien bzw. eingesetzt würden. Das Minimum liegt bei vier, das Maximum bei 35. Keines der befragten Unternehmen hat also keine der abgefragten Massnahmen etabliert und insgesamt fünf Firmen haben angegeben, dass bei ihnen alle abgefragten Massnahmen (einschliesslich weiteren Massnahmen) zum Einsatz kommen würden. Der Median liegt bei 27 vorhandenen Massnahmen. 50% der antwortenden Firmen haben also weniger als bzw. 27 Massnahmen angegeben und 50% gaben mehr als bzw. 27 Massnahmen an. Eine Verteilung der Anzahl der angegebenen Massnahmen in Kategorien ist in Grafik 18 dargestellt.



Grafik 18: Anzahl vorhandener Massnahmen (in Prozent; N=248)

Wie aus Grafik 18 ersichtlich, haben die befragten Unternehmen eher mehr als weniger der abgefragten Massnahmen etabliert. Die Mehrheit der Unternehmen hat angegeben, dass sie über 26-30 der abgefragten Massnahmen verfügen. Mehr als 30 Massnahmen hat rund jedes vierte befragte Unternehmen etabliert. In der Kategorie 21-25 Massnahmen ist es rund jedes siebte, in der Kategorie 16-20 Massnahmen rund jedes achte und in der Kategorie 10-15 rund jedes neunte Unternehmen. Acht Unternehmen haben weniger als 10 Massnahmen etabliert.

Die in Tabelle 10 dargestellten Unterschiede nach Unternehmensgrösse erwiesen sich nicht als statistisch signifikant. Ein Blick auf die Zahlen zeigt jedoch, dass mit zunehmender Unternehmensgrösse häufiger mehr Massnahmen angegeben wurden. Am grössten sind im Vergleich die Anteile in den Kategorien 26-30 und über 30 Massnahmen bei Unternehmen mit mehr als 1000 Mitarbeitenden, am zweitgrössten bei Unternehmen mit einer Grösse von 250-999 Mitarbeitenden. In den übrigen Kategorien sind demgegenüber die Anteile bei Unternehmen mit einer Grösse von 50-249 Mitarbeitenden und mit 1-49 Mitarbeitenden grösser.

Tabelle 10: Anzahl vorhandener Massnahmen nach Unternehmensgrösse (in Prozent)

	<10	10-15	16-20	21-25	26-30	>30
1-49 (N=101)	5.0	11.9	12.9	16.8	35.6	17.8
50-249 (N=68)	2.9	7.4	17.6	16.2	38.2	17.6
250-999 (N=29)	0.0	3.4	10.3	10.3	41.4	34.5
> 1000 (N=41)	2.4	2.4	2.4	7.3	46.3	39.0

Im Folgenden wird die Verbreitung der einzelnen abgefragten Massnahmen dargestellt (siehe Tabelle 11). Regelmässige Backups/Datensicherungen, aktuelle Anitivirensoftware, Schutz der ICT-Systeme mit einer Firewall, eine regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches sowie eine physisch getrennte Aufbewahrung von Backups werden mit 95% und mehr von fast allen Firmen eingesetzt. Auch über Geheimhaltungsverpflichtungen für Mitarbeitende, eine individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe, Mindestanforderungen für Passwörter, Geheimhaltungsverpflichtungen für Geschäftspartner, eine Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen, ein Besucher- und Besucherinnenmanagement bzw. Zutrittskontrollen, physische Sicherheitsmassnahmen wie z.B. Kameras, Alarme oder Badge-Schliesssysteme sowie klare Regelungen für den Umgang mit vertraulichen Informationen verfügen zwischen rund 86 und 93% der befragten Firmen und damit die überwiegende Mehrheit. Bezüglich einer Absicherung von Fernzugriffen (für Wartung und Administration) auf die Leitstelle und Steuerungsanlagen mit starker Authentisierung, schriftlich fixierte Richtlinien zur Informations- bzw. ICT-Sicherheit, Schulungen zur ICT-Sicherheit sowie der eindeutigen Klassifizierung und Kennzeichnung von Betriebsgeheimnissen sind es fast 80 Prozent, die ein Vorhandensein angeben. Das Bestehen schriftlich fixierter Richtlinien zum Notfallmanagement gaben rund drei Viertel an. Etwa gleich viele nehmen eine Kontrolle der über das Unternehmen veröffentlichten Informationen, z.B. auf der Homepage oder durch Mitarbeitende in sozialen Medien vor. Regelmässe Kontrollen von Arbeitsplätzen, Mitarbeitenden etc. auf Einhaltung

der Vorschriften, Weisungen für das Verhalten bei Messen und Ausstellungen, Weisungen für die Mitnahme von vertraulichen Informationen bei Auslandsreisen und Background-Checks von Geschäftspartnern gaben rund 70 bis 72% der Befragten an. Regelmässige Risiko- und Schwachstellenanalysen, eine Clean-Desk-Policy, besondere Sicherheitsmassnahmen bei der Einstellung von ausländischen Bewerbern und Übungen oder Simulationen für den Ausfall wichtiger ICT-Systeme haben etwas mehr als zwei Drittel der befragten Unternehmen, etwas weniger als zwei Drittel haben ein Informationssicherheits-Managementsystem eingeführt. Ein kontinuierliches Monitoring sämtlicher Log-Daten in der Unternehmens-ICT gaben rund 60% an. Über eine Trennung der ICT-Netzwerke der Firma, wie bspw. eine vom Internet getrenntes Netzwerk, eine Verschlüsselung von Festplatten und ein Intrusion Detection System (IDS) verfügt rund jedes zweite befragte Unternehmen. Ein Verbot des Anschlusses privater Peripheriegeräte, wie z.B. USB-Sticks oder Smartphones an das Firmennetzwerk oder die Verschlüsselung von E-Mails wurde im Vergleich seltener genannt, aber immerhin noch von rund jedem dritten befragten Unternehmen.

Dass sie noch über weitere als die genannten Sicherheitsmassnahmen verfügen würden, gaben rund 56% der befragten Firmen an. Diejenigen, die diese Antwortoption gewählt haben, wurden wiederum gebeten nähere Angaben zu machen. Als weitere Massnahmen wurde von mehreren Firmen angegeben, dass die Mitarbeitenden geschult und regelmässig auf Cyber- und sonstige Gefahren aufmerksam gemacht würden, z.B. in Teamsitzungen oder auch durch E-Learning. Eine weitere Firma nannte die Ankündigung von Besucherinnen und Besuchern als weitere Massnahme.

Tabelle 11: Einzelne Schutz- und Interventionsmassnahmen (in Prozent; sortiert nach Häufigkeit der Nennung)

	ja	nein	weiss nicht
Regelmässige Backups/Datensicherungen (N=245)	99.2	0.4	0.4
Aktuelle Anitivirensoftware (N=246)	98.8	0.4	0.8
Schutz der ICT-Systeme mit einer Firewall (N=245)	98.4	0.8	0.8
Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches (N=243)	96.3	2.1	1.6
Physisch getrennte Aufbewahrung von Backups (N=244)	95.1	2.0	2.9
Individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe (N=244)	93.9	4.9	1.2
Geheimhaltungsverpflichtungen für Mitarbeitende (N=230)	93.9	5.7	0.4
Mindestanforderungen für Passwörter/Multifaktor-Authentifikation (N=246)	91.9	7.3	0.8
Geheimhaltungsverpflichtungen für Geschäftspartner (N=231)	90.9	7.8	1.3

Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen (N=230)	89.1	10.9	0.0
Besuchermanagement/Zutrittskontrollen (N=231)	88.3	10.8	0.9
Physische Sicherheitsmassnahmen, z.B. Kameras, Alarme, Badge-Schliesssysteme (N=227)	86.8	12.3	0.9
Klare Regelungen für den Umgang mit vertraulichen Informationen (Informationssicherheitskonzept; N=224)	86.6	12.1	1.3
Alle Fernzugriffe (für Wartung und Administration) auf Leitstelle und Steuerungsanlagen sind mit starker Authentisierung abgesichert (N=243)	79.8	13.2	7.0
Schriftlich fixierte Richtlinien zur Informations- bzw. ICT-Sicherheit (N=246)	79.7	18.3	2.0
Schulungen zur ICT-Sicherheit für Mitarbeitende (N=244)	79.1	19.7	1.2
Eindeutige Klassifizierung/Kennzeichnung von Betriebsgeheimnissen (N=228)	78.9	19.7	1.3
Schriftlich fixierte Richtlinien zum Notfallmanagement (N=213)	74.6	22.5	2.8
Kontrolle der veröffentlichten Informationen, z.B. auf Homepage /durch Mitarbeitende in den sozialen Medien (N=226)	74.3	21.2	4.4
Regelmässige Kontrollen (der Arbeitsplätze, der Mitarbeitenden etc.) in Bezug auf die Einhaltung von Vorschriften (N=226)	72.1	25.2	2.7
Weisungen für das Verhalten bei Messen und Ausstellungen (N=231)	71.4	26.0	2.6
Weisungen für die Mitnahme von vertraulichen Informationen bei Auslandsreisen (N=230)	71.3	26.1	2.6
Background-Checks von Geschäftspartnern (Lieferanten, Dienstleister, Berater etc.; N=229)	70.3	27.1	2.6
Regelmässige Risiko- und Schwachstellenanalysen (N=243)	69.5	23.9	6.6
Clean-Desk-Policy (N=229)	67.7	27.9	4.4
Übungen oder Simulationen für den Ausfall wichtiger ICT-Systeme (N=228)	67.1	28.1	4.8
Anpassung der Rekrutierungsprozesse, z.B. persönliche Sicherheitsüberprüfungen, Straf- und Betreibungsregisterauszüge, zusätzliche Unterlagen bei ausländischen Bewerbern (N=228)	67.1	28.1	4.8
Einführung eines Informationssicherheits-Managementsystems (ISMS; N=218)	64.2	30.7	5.0
Kontinuierliches Monitoring sämtlicher Log-Daten in der Unternehmens ICT (N=242)	59.9	28.1	12.0
Weitere Massnahmen (N=124)	55.6	39.5	4.8
Trennung der ICT-Netzwerke der Firma, wie z. B. ein vom Internet getrenntes Netzwerk (N=241)	54.8	36.9	8.3
Verschlüsselung von Festplatten (N=243)	53.9	35.4	10.7
Intrusion Detection System (IDS; N=243))	48.1	23.5	28.4

Kein Anschluss privater Peripheriegeräte (USB-Sticks, Smartphones etc.) an das Firmennetzwerk (N=240)	35.4	62.1	2.5
Verschlüsselung von E-Mails (N=239)	35.1	56.5	8.4

Diejenigen Firmen, die einen schwerwiegendsten Angriff angegeben haben, wurden ausserdem gebeten, anzugeben, ob sie die jeweiligen Massnahmen, die sie haben, bereits vor dem von ihnen angegebenen schwerwiegendsten Angriff hatten oder erst danach (siehe Tabelle 12).

Tabelle 12: Schutz- und Interventionsmassnahmen bei Unternehmen, die einen schwerwiegendsten Angriff angegeben haben (in Prozent; sortiert nach Häufigkeit der ja Angaben: vor dem Angriff plus nach dem Angriff)

	ja, und bereits vor dem schwersten Angriff	ja, aber erst seit dem schwersten Angriff	nein	weiss nicht
Regelmässige Backups/Datensicherungen (N=155)	98.7	0.6	0.6	0.0
Aktuelle Anitivirensoftware (N=156)	98.7	0.0	0.6	0.6
Schutz der ICT-Systeme mit einer Firewall (N=155)	98.1	0.6	0.6	0.6
Physisch getrennte Aufbewahrung von Backups (N=154)	90.9	4.5	1.3	3.2
Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches (N=153)	91.5	3.9	2.6	2.0
Mindestanforderungen für Passwörter/Multifaktor-Authentifikation (N=156)	80.8	12.8	5.8	0.6
Individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe (N=154)	89.0	2.6	6.5	1.9
Geheimhaltungsverpflichtungen für Mitarbeitende (N=148)	84.5	1.4	11.5	2.7
Schulungen zur ICT-Sicherheit für Mitarbeitende (N=154)	66.9	16.2	15.6	1.3
Geheimhaltungsverpflichtungen für Geschäftspartner (N=147)	80.3	0.7	15.0	4.1
Schriftlich fixierte Richtlinien zur Informations- bzw. ICT-Sicherheit (N=156)	75.0	5.1	17.9	1.9
Alle Fernzugriffe (für Wartung und Administration) auf Leitstelle und Steuerungsanlagen sind mit starker Authentisierung abgesichert (N=154)	72.7	7.1	11.0	9.1
Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen (N=148)	73.6	2.0	21.6	2.7
Besuchermanagement/Zutrittskontrollen (N=149)	73.2	2.0	22.1	2.7
Regelmässige Risiko- und Schwachstellenanalysen (N=154)	55.2	16.2	22.7	5.8

Physische Sicherheitsmassnahmen, z.B. Kameras, Alarme, Badge-Schliesssysteme (N=146)	63.7	2.7	30.8	2.7
Klare Regelungen für den Umgang mit vertraulichen Informationen (Informationssicherheitskonzept; N=150)	58.7	7.3	31.3	2.7
Kontinuierliches Monitoring sämtlicher Log-Daten in der Unternehmens ICT (N=153)	49.0	15.0	24.8	11.1
Verschlüsselung von Festplatten (N=154)	53.2	5.2	27.9	13.6
Trennung der ICT-Netzwerke der Firma, wie z. B. ein vom Internet getrenntes Netzwerk (N=152)	49.3	7.2	34.2	9.2
Schriftlich fixierte Richtlinien zum Notfallmanagement (N=151)	40.4	14.6	40.4	4.6
Intrusion Detection System (IDS; N=154)	41.6	10.4	21.4	26.6
Eindeutige Klassifizierung/Kennzeichnung von Betriebsgeheimnissen (N=148)	42.6	3.4	50.0	4.1
Kontrolle der veröffentlichten Informationen, z.B. auf Homepage /durch Mitarbeitende in den sozialen Medien (N=148)	39.9	3.4	53.4	3.4
Kein Anschluss privater Peripheriegeräte (USB-Sticks, Smartphones etc.) an das Firmennetzwerk (N=150)	29.3	6.7	61.3	2.7
Übungen oder Simulationen für den Ausfall wichtiger ICT-Systeme (N=150)	32.0	4.0	57.3	6.7
Einführung eines Informationssicherheits-Managementsystems (ISMS; N=149)	24.8	10.7	58.4	6.0
Weisungen für das Verhalten bei Messen und Ausstellungen (N=148)	34.5	0.7	54.7	10.1
Background-Checks von Geschäftspartnern (Lieferanten, Dienstleister, Berater etc.; N=148)	32.4	2.7	54.7	10.1
Verschlüsselung von E-Mails (N=150)	29.3	3.3	57.3	10.0
Weisungen für die Mitnahme von vertraulichen Informationen bei Auslandsreisen (N=149)	26.2	2.7	63.8	7.4
Anpassung der Rekrutierungsprozesse, z.B. persönliche Sicherheitsüberprüfungen, Straf- und Betreibungsregisterauszüge, zusätzliche Unterlagen bei ausländischen Bewerbern (N=147)	24.5	2.0	62.6	10.9
Clean-Desk-Policy (N=148)	22.3	2.7	67.6	7.4
Regelmässige Kontrollen (der Arbeitsplätze, der Mitarbeitenden etc.) in Bezug auf die Einhaltung von Vorschriften (N=146)	15.8	2.1	77.4	4.8
Weitere Massnahmen (N=82)	9.8	0.0	70.7	19.5

Regelmässige Backups/Datensicherungen, aktuelle Anitivirensoftware sowie den Schutz der ICT-Systeme mit einer Firewall nutzen so gut wie alle der befragten Unternehmen, die einen schwerwiegendsten Angriff angegeben haben – diese hatten sie auch schon vor dem von ihnen berichteten An-

griff genutzt. Etwas mehr als 90% der Unternehmen verfügen über eine physisch getrennte Aufbewahrung von Backups und nahmen eine regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches vor. Sieben respektive sechs Unternehmen haben diese Massnahmen erst nach dem von ihnen berichteten schwerwiegendsten Angriff etabliert, wobei nicht erfasst wurde, ob der berichtete Angriff der Anlass gewesen ist oder die Massnahmen unabhängig von diesem eingeführt wurden. Mindestanforderungen für Passwörter wurden von rund jedem achten Unternehmen erst nach dem Angriff definiert, während rund 80% diese bereits vorher hatten. Über individuelle Vergaben von Zugangs- und Nutzungsrechten je nach Aufgabe sowie Geheimhaltungsverpflichtungen für Mitarbeitende verfügten ebenfalls die Mehrheit der Unternehmen, und dies auch bereits vor dem berichteten Angriff. Rund jedes 15. befragte Unternehmen verfügt nicht über eine individuelle Vergabe von Passwörtern, rund jedes neunte nicht über Geheimhaltungsverpflichtungen für Mitarbeitende. Schulungen zur ICT-Sicherheit für Mitarbeitende wurden von vergleichsweise vielen Unternehmen erst nach dem Angriff eingeführt. Rund jedes sechste Unternehmen machte entsprechende Angaben. Etwa gleich viele haben diese Massnahme auch heute nicht eingeführt, rund zwei Drittel hatten sie jedoch bereits vor dem schwerwiegendsten Angriff. Geheimhaltungsverpflichtungen für Geschäftspartner haben rund 80% und dies bereits vor dem Angriff. Ein Unternehmen hat diese Massnahme irgendwann in der Zeit nach dem Angriff etabliert, rund jedes siebte Unternehmen setzt diese Massnahme nicht ein. Schriftlich fixierte Richtlinien zur ICT-Sicherheit sowie die Absicherung von Fernzugriffen auf Leitstelle und Steuerungsanlagen mit starker Authentisierung hatten rund drei Viertel der befragten Unternehmen bereits vor dem von ihnen berichteten Angriff und rund jedes 14. (Absicherung von Fernzugriffen mit starker Authentisierung) bzw. 20 (schriftlich fixierte Richtlinien zur ICT-Sicherheit) Unternehmen hat diese Massnahmen irgendwann in der Zeit zwischen dem Angriff und dem Befragungszeitpunkt eingeführt. Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen und ein Besuchermanagement bzw. Zutrittskontrollen hatten ebenfalls etwas mehr als 70% der Befragten bereits vor dem schwerwiegendsten Angriff. Jeweils drei Unternehmen haben die Massnahmen ebenfalls, aber diese erst seit dem Angriff ergriffen. Etwa jedes fünfte Unternehmen hat keine der beiden Massnahmen ergriffen. Bei regelmässigen Risiko- und Schwachstellenanalysen ist der Anteil Unternehmen, welche die Massnahme erst später, seit dem schwerwiegendsten Angriff eingeführt haben, besonders gross. Rund jedes sechste Unternehmen machte entsprechende Angaben. Physische Sicherheitsmassnahmen haben etwas mehr als 60%, vier Unternehmen führten diese Massnahme nach dem schwerwiegendsten Angriff ein und etwa jedes dritte Unternehmen verfügt nicht über physische Sicherheitsmassnahmen. Klare Regelungen für den Umgang mit vertraulichen Informationen haben ebenfalls fast 60% der Unternehmen, elf haben ein entsprechendes Konzept in der Zeit seit dem berichteten Angriff eingeführt, wiederum rund jedes dritte Unternehmen verfügt nicht über eine solche Schutzmass-

nahme. Ein kontinuierliches Monitoring sämtlicher Log-Daten in der Unternehmens ICT haben ebenfalls vergleichsweise viele Firmen erst nach dem schwerwiegendsten Angriff etabliert, etwa jedes siebte, dass über diese Massnahme verfügt. Knapp 50% hatten diese Massnahme bereits vor dem Angriff, rund ein Viertel hat sie bis heute nicht. Eine Verschlüsselung von Festplatten sowie eine Trennung der ICT-Netzwerke des Unternehmens, wie z.B. ein vom Internet getrenntes Netzwerk gab es in etwas mehr als der Hälfte der Unternehmen bereits vor dem berichteten Angriff. Acht Unternehmen (Verschlüsselung von Festplatten) sowie elf Unternehmen (Trennung der ICT-Netzwerke des Unternehmens) haben die Massnahme seit dem Angriff etabliert und etwa jedes dritte bis vierte Unternehmen verfügt nicht über eine der beiden Massnahmen. Schriftliche Massnahmen zum Notfallmanagement hatten gleich viele Unternehmen bereits vor dem Vorfall wie gar nicht (jeweils 40.4%). Etwa jedes siebte Unternehmen hat die Massnahme nach dem Vorfall eingeführt, was im Vergleich zu den Anteilen neuer Einführungen bei den anderen Massnahmen als eher viel zu bewerten ist. Ein Intrusion Detection System hatten ebenfalls rund 40% der Unternehmen bereits vor dem schwerwiegendsten Angriff, rund jedes zehnte Unternehmen verfügt ebenfalls über ein solches System, aber erst seit dem schwerwiegendsten Angriff und jedes fünfte Unternehmen hat kein solches System. Der Anteil derer, die nicht wissen, ob sie ein entsprechendes System haben, ist mit rund einem Viertel eher hoch. Eine eindeutige Kennzeichnung und Klassifizierung von Betriebsgeheimnissen haben 46% der Befragten, fünf davon seit dem schwerwiegendsten Angriff. 50% haben diese Massnahme nicht. Eine Kontrolle von veröffentlichten Informationen, wie z.B. auf der Homepage oder durch Mitarbeitende in sozialen Medien, nehmen etwas mehr als 40% der Unternehmen vor, wiederum fünf davon erst seit dem von ihnen berichteten Angriff. Etwas mehr als 50% nehmen eine entsprechende Kontrolle nicht vor. Die übrigen Massnahmen wurden jeweils von weniger als 40% der befragten Unternehmen als vorhanden angegeben. Die Anteile der Unternehmen, welche diese übrigen Massnahmen irgendwann in der Zeit nach dem Angriff neu eingeführt haben, ist mit Ausnahme des Verbots des Anschlusses privater Peripheriegeräte (fünf Unternehmen) und der Einführung eines Informationssicherheits-Managementsystems (16 Unternehmen) eher gering.

7 Zusammenfassung

7.1 Betroffenheit durch verschiedene Angriffsarten

Insgesamt war mit 80% die Mehrheit der befragten Unternehmen seit ihrem Bestehen von mindestens einer der abgefragten Angriffsarten betroffen. Im Durchschnitt wurde eine Betroffenheit durch 2.4 verschiedene Arten von Angriffen berichtet. Insgesamt 54 (20.0%) der 270 Unternehmen, welche die Frage nach der Betroffenheit durch die verschiedenen Arten von Angriffen seit Bestehen des Unternehmens beantwortet haben, waren noch nie von einer der abgefragten Angriffsarten betroffen. Weitere 44 (16.3%) Unternehmen berichten, seit dem Bestehen von einer Angriffsart betroffen gewesen

zu sein, 63 (23.3%) von zwei verschiedenen, 31 (11.5%) von drei verschiedenen 37 (13.7%) von vier verschiedenen usw. Zwei Unternehmen waren von neun verschiedenen Angriffsarten betroffen. Es zeigt sich also eine gewisse Mehrfachbetroffenheit durch unterschiedliche Angriffsarten bei vielen der befragten Unternehmen.

Besonders häufig waren Opferwerdungen durch CEO-Fraud, Phishing, sonstige Schadsoftware wie z.B. Viren, Trojaner oder Würmer) und Hackerangriffe. Eine ähnliche Verteilung zeigt sich für die Betroffenheit in den letzten zwei Jahren vor der Befragung. Auch in diesem Zeitraum berichten die Unternehmen besonders häufig von einem Angriff durch die zuvor genannten Angriffsarten. Insgesamt waren in den letzten 24 Monaten vor der Befragung 70.4% der befragten Unternehmen von mindestens einer Angriffsart betroffen, einige bis zu mehr als zwanzigmal. Eine so hohe Betroffenheit wurde insbesondere für Phishing berichtet. Aber auch von CEO-Fraud waren die Unternehmen häufig mehrfach betroffen. Ein Vergleich nach Unternehmensgrösse zeigt, dass insbesondere grosse Unternehmen mit 1000 und mehr Mitarbeitenden Opfer wurden. Dies gilt für die Mehrheit der verschiedenen Angriffsarten. Bei vielen Angriffsarten nimmt die Betroffenheit mit zunehmender Grösse des Unternehmens mehr oder weniger kontinuierlich zu. Dies gilt insbesondere für CEO-Fraud, sonstige Schadsoftware, Hackerangriffe, (D)DoS-Attacken und für den Diebstahl von Informationsmedien durch Einbruch. Deutlich häufiger Opfer geworden sind grössere Unternehmen mit mehr als 1000 Mitarbeitenden im Vergleich zu Unternehmen anderer Grösse durch Phishing-Angriffe. Insgesamt sind jedoch Unternehmen jeglicher Grösse insbesondere von CEO-Fraud, Phishing, von sonstiger Schadsoftware, wie Viren, Trojaner und Würmer sowie von Hackerangriffen betroffen.

7.2 Schwerwiegendster Angriff

Gefragt nach dem schwerwiegendsten Angriff in den letzten 24 Monaten vor der Befragung (diese Frage wurde nur denjenigen Unternehmen gestellt, die für die letzten 24 Monate mindestens einen Angriff angegeben haben), wurden insbesondere Angriffsarten genannt, die dem Bereich Cybercrime zugeordnet werden können. Am zweithäufigsten wurden Angriffe aus dem Bereich Social Engineering (CEO-Fraud oder sonstige Formen des Social Engineering) angegeben.

Der initiale Angriffspunkt des schwerwiegendsten Angriffs war insbesondere die Hauptniederlassung im Inland. Alle anderen potenziellen Angriffspunkte wie Zweigniederlassungen im Inland, Hauptniederlassungen im Ausland, Zweigniederlassungen im Ausland, Subunternehmer, Lieferanten, Dienstleister, wie z.B. Cloudanbieter oder Kundschaft wurden im Vergleich seltener genannt. Wenn ein Angriff bei einer Haupt- oder Zweigniederlassung im Ausland stattfand wurden vor allem die folgenden Länder als Ort der Niederlassung angegeben: Deutschland, USA, Indien, China, England und Italien. Es zeigten sich einige Unterschiede nach Unternehmensgrösse. Bei Unternehmen bis zu einer Grösse von

999 Mitarbeitenden war der initiale Angriffspunkt am häufigsten die Hauptniederlassung im Inland. Bei den befragten Unternehmen mit einer Grösse von mehr als 1000 Mitarbeitenden war dieser jedoch am häufigsten in einer Zweigniederlassung im Ausland. Bei Firmen mit mehr als 1000 Mitarbeitenden war auch eine Hauptniederlassung im Ausland im Vergleich zu Firmen anderer Grösse häufiger der initiale Angriffspunkt. Bezüglich der verschiedenen Angriffsarten unterscheiden sich die initialen Angriffspunkte kaum. Bei allen Angriffsarten gingen die Angriffe überwiegend von der Hauptniederlassung im Inland aus.

Es zeigte sich ausserdem, dass in der überwiegenden Mehrheit der berichteten schwerwiegendsten Fälle, die Täterinnen bzw. Täter nicht bekannt waren. Wenn man nicht wusste wer es war, aber eine diesbezügliche Vermutung hatte, wurden besonders häufig Hacker als vermutete Täterinnen bzw. Täter genannt. Waren die Täterinnen bzw. Täter hingegen eindeutig bekannt, lässt sich kein eindeutiger Trend erkennen, wobei auch hier eher häufiger Hacker genannt wurden. Von Unternehmen mit mehr als 1000 Mitarbeitenden wurde im Vergleich zu den befragten Unternehmen anderer Grösse häufiger angegeben, dass die Täter bzw. Täterinnen unbekannt seien, dass es aber eine Vermutung gebe. Dass die Täter bzw. Täterinnen unbekannt seien wurde am häufigsten von Unternehmen mit einer Grösse von 50-249 und 250-999 Mitarbeitenden angegeben. Etwas weniger häufig von kleineren Unternehmen mit 1-49 Mitarbeitenden und am seltensten von Unternehmen mit mehr als 1000 Mitarbeitenden. Besonders häufig wurde in Bezug auf die Angriffsarten Cybercrime und Social Engineering angegeben, dass die Täter bzw. Täterinnen nicht bekannt seien. Beim Diebstahl von Informationsmedien, dem Diebstahl von digitalen Informationen oder sensiblen physischen Dokumenten durch Mitarbeitende und bei anderen als den vorgegeben Angriffsarten bzw. einer Kombination aus mehreren Angriffen war dies weniger häufig der Fall und die Täter bzw. Täterinnen häufiger bekannt.

Der berichtete schwerwiegendste Angriff wurde von mehr als der Hälfte der Unternehmen nicht als zielgerichtet wahrgenommen. Sie nehmen also an, dass sie eher als ein Unternehmen von vielen anderen attackiert wurden. Rund jedes fünfte Befragte Unternehmen gab jedoch an, dass sie zielgerichtet attackiert wurden. Ebenfalls etwa jedes fünfte Unternehmen weiss es nicht. Als Gründe für einen zielgerichteten Angriff wurden insbesondere ein hohes Erpressungs- und Ertragspotenzial sowie andere Gründe, wie finanzielle Bereicherung oder finanzielle Schädigung angegeben. Grössere Unternehmen gaben im Vergleich zu kleineren etwas häufiger an, dass der Angriff zielgerichtet erfolgt sei. Betroffene von Angriffen aus dem Bereich Cybercrime und Social Engineering berichten häufiger, dass sie eher als ein Unternehmen von vielen anderen attackiert wurden. Das Abfangen digitaler Kommunikation und der Datenabfluss durch Dritte, der Diebstahl von Informationsmedien sowie der Diebstahl von sensiblen Daten und Dokumenten durch Mitarbeitende wurden hingegen häufiger durch die Betroffenen als zielgerichtet wahrgenommen.

Etwa jedes dritte Unternehmen gab zudem an, dass der von ihnen berichtete schwerwiegendste Angriff nicht mit Folgen verbunden gewesen sei. Von den übrigen wurden eine oder mehrere Folgen genannt. Vergleichsweise häufiger entstanden Kosten durch Sofortmassnahmen zur Abwehr und Aufklärung, rund jedes dritte Unternehmen gab diese Folge an, gefolgt von Kosten für externe Beratung, die von rund jedem vierten Unternehmen benannt wurde. Ähnlich viele Unternehmen berichteten von Investitionen in Sicherheitsmassnahmen und spezielle Versicherungen. Etwa in jedem sechsten Unternehmen entstanden Kosten für die Wiederherstellung von Daten oder IT-Infrastruktur oder es kam zu einer Betriebsunterbrechung. Von einem Ausfall der Informatik als Folge berichtete rund jedes neunte Unternehmen. Die übrigen abgefragten Folgen wurden von weniger als zehn Prozent der Unternehmen angegeben, immerhin jedes elfte Unternehmen gab jedoch eine Erhöhung des Zusammenhalts unter den Mitarbeitenden als eine positive Folge des Angriffs an. Bezüglich der meisten Folgen zeigten sich keine eindeutigen Unterschiede nach Unternehmensgrösse. Mal waren grössere, mal mittelgrosse, mal kleinere Unternehmen von einzelnen Folgen stärker betroffen. Bezüglich der Angriffsart zeigten sich einige Unterschiede und bezüglich der besonders häufig genannten Folgen konnten folgende Unterschiede beobachtet werden: Kosten für Sofortmassnahmen zur Abwehr und Aufklärung wurden insbesondere von Unternehmen berichtet, die von Cybercrime, dem Abfangen digitaler Kommunikation und Datenabfluss durch Dritte, Social Engineering sowie einer anderen Angriffsart oder eine Kombination von Angriffsarten betroffen waren. Kosten für externe Beratung entstanden nur für Betroffene von Cybercrime, Social Engineering und einer anderen Angriffsart oder eine Kombination von Angriffsarten. Investitionen in Sicherheitsmassnahmen oder spezielle Versicherungen nannten hingegen mit Ausnahme von Opfern von Diebstahl von Daten/ Informationen durch eigene Mitarbeitende Opfer aller anderen Angriffsarten. Kosten für Wiederherstellung von Daten oder IT-Infrastruktur und auch Ausfälle der Informatik entstanden vorwiegend bei Unternehmen, die von Cybercrime betroffen waren. Betriebsunterbrechungen als Folge beichteten mit Ausnahme von Betroffenen von Diebstahl von Daten/Informationen durch eigene Mitarbeitende Betroffene aller anderen Angriffsarten. Als besonders schwerwiegende Folgen wurden der Ausfall der Informatik und Betriebsunterbrechungen bewertet, insbesondere auch dann, wenn sie eine von mehreren anderen Folgen gewesen sind. Vergleichsweise häufig wurden auch Kosten für Rechtsstreitigkeiten und Reputationsverluste als besonders schwerwiegende Folgen bewertet, jedoch insgesamt nur von vergleichsweise wenigen Unternehmen überhaupt als Folge genannt und diese haben zudem z.T. nur wenige verschiedene Folgen angegeben.

Der entstandene Schaden führte jedoch insgesamt bei der Mehrheit der befragten Unternehmen nicht zu starken Einschränkungen. Etwas mehr als zwei Drittel der Unternehmen gab an, der Schaden war kurzfristig behebbar und leicht verdaubar. Bei rund jedem sechsten Unternehmen führte der entstandene Schaden hingegen zu spürbaren Einschränkungen, bei zwei Unternehmen gefährdete er sogar

die Existenz des Unternehmens. Rund jedes siebte Unternehmen gab an, der durch den schwerwiegendsten Angriff entstandene Schaden zog keine Einschränkungen nach sich. Im Durchschnitt entstand den Unternehmen ein Schaden in Höhe von 205 142.86 CHF. Der kleinste angegebene Schaden betrug 0 CHF, der Grösste 2 000 000 CHF. Die Mehrheit der Unternehmen, die Angaben zum Schaden machten, beziffern diesen mit einer Summe von mehr als null bis zu 10 000 CHF (siehe Grafik 15). Dies trifft auf fast 40 Prozent der Unternehmen zu. Etwa bei einem Drittel entstand ein Schaden zwischen 10 000 und 100 000 CHF, bei rund jedem fünften befragten Unternehmen ein Schaden zwischen 100 000 und 1 000 000 CHF und bei fünf Unternehmen ein Schaden von mehr als 1 000 000 CHF. Unternehmen aller Grössen bewerteten den Schaden mehrheitlich als kurzfristig behebbar. Zu spürbaren Einschränkungen führte er weniger häufig in den kleinsten Unternehmen mit einer Mitarbeiterzahl von 1-49. Hohe Schadenssummen in Höhe von 1 000 000 CHF und mehr entstanden häufiger in grösseren Unternehmen mit 250-999 und mehr als 1000 Mitarbeitenden.

Im Vergleich zu Produktions- und Prozessdaten sowie Produkt und F & E Daten waren Kunden- und personenbezogene Daten häufiger beim schwerwiegendsten Angriff betroffen. Bei allen Arten von Daten zeigte sich, dass diese insbesondere verschlüsselt wurden und seltener gestohlen, manipuliert oder gelöscht. Eine Ausnahme bilden Kunden- und personenbezogene Daten. Diese wurden etwa ähnlich häufig bzw. geringfügig häufiger gestohlen als verschlüsselt. Bei allen Datentypen wurde zudem von sechs bis elf Prozent der Unternehmen angegeben, dass sie nicht wüssten, ob entsprechende Daten betroffen waren oder nicht.

Zusätzlich wurden die Unternehmen gebeten, anzugeben, zu welchen Akteurinnen und Akteuren sie nach dem von ihnen berichteten schwerwiegendsten Angriff Kontakt aufgenommen haben. Von den verschiedenen vorgegebenen Akteurinnen und Akteuren wurde am häufigsten angegeben, dass spezialisierte Dienstleister kontaktiert wurden. Rund eine Viertel der Unternehmen hatte zudem Kontakt zur Polizei aufgenommen. Kontakt zur Versicherung hatte rund jedes fünfte befragte Unternehmen. Etwa gleich viele kontaktierten zudem andere, nicht im Fragebogen genannte Akteurinnen und Akteure, wie z.B. die Bank, Beauftragte für Datenschutz, Behörden vor Ort, wenn der Angriff im Ausland stattgefunden hat, die eigene IT-Abteilung und IT-Sicherheitsberater, die interne Rechtsabteilung, den Betreiber des Rechenzentrums oder Vertriebspartner im Ausland. Kontakt zum Nationalen Zentrum für Cybersicherheit (NCSC) oder zum Nachrichtendienst des Bundes (NDB) oder einer ähnlichen Behörde im Ausland wurde vergleichsweise selten aufgenommen. Bei allen abgefragten Akteurinnen bzw. Akteuren erfolgte häufiger eine Kontaktaufnahme durch grössere im Vergleich zu kleineren Unternehmen. Spezialisierte Dienstleister wurden häufiger kontaktiert, wenn ein von einem Unternehmen ein schwerwiegendster Angriff aus dem Bereich Cybercrime, Diebstahl von Daten oder Informationen durch eigene Mitarbeitende oder eine andere Angriffsart bzw. Kombination von mehreren An-

griffsarten berichtet wurde. Betroffene von einem Abfangen digitaler Kommunikation und Datenabfluss durch Dritte, Diebstahl von Informationsmedien und einer anderen Angriffsart bzw. Kombination von mehreren Angriffsarten haben vergleichsweise häufiger die Polizei kontaktiert. Dies berichteten auch rund ein Viertel der von Cybercrime betroffene Unternehmen sowie jedes sechste von Social Engineering betroffene Unternehmen.

Schutz- und Interventionsmassnahmen

Insgesamt zeigte sich, dass alle befragten Unternehmen mindestens vier der abgefragten Schutz- und Interventionsmassnahmen etabliert haben. Fünf Unternehmen haben sogar für alle der abgefragten Massnahmen angegeben, dass sie diese einsetzen würden. Im Durchschnitt verfügten die Unternehmen über rund 25 von 35 Massnahmen. Mit mehr als einem Drittel hat die Mehrheit der Unternehmen angegeben, dass sie über 26-30 der abgefragten Massnahmen verfügen. Mehr als 30 Massnahmen hat rund jedes vierte befragte Unternehmen etabliert. In der Kategorie 21-25 Massnahmen ist es rund jedes siebte, in der Kategorie 16-20 Massnahmen rund jedes achte und in der Kategorie 10-15 rund jedes neunte befragte Unternehmen. Acht Unternehmen haben weniger als 10 Massnahmen etabliert. Zudem verfügen die Unternehmen mit zunehmender Grösse über mehr Massnahmen. Besonders häufig als vorhanden genannt wurden Regelmässige Backups/Datensicherungen, aktuelle Anitivirensoftware, Schutz der ICT-Systeme mit einer Firewall, eine regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches sowie eine physisch getrennte Aufbewahrung von Backups. Über diese Massnahmen verfügen fast alle der befragten Unternehmen. Ebenso über Geheimhaltungsverpflichtungen für Mitarbeitende, eine individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe, Mindestanforderungen für Passwörter, Geheimhaltungsverpflichtungen für Geschäftspartner, eine Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen, ein Besucher- und Besucherinnenmanagement bzw. Zutrittskontrollen, physische Sicherheitsmassnahmen wie z.B. Kameras, Alarme oder Badge-Schliesssysteme sowie klare Regelungen für den Umgang mit vertraulichen Informationen. Am seltensten genannt wurden ein Verbot des Anschlusses privater Peripheriegeräte, wie z.B. USB-Sticks oder Smartphones an das Firmennetzwerk oder die Verschlüsselung von E-Mails, beide Massnahmen jedoch immerhin noch von rund jedem dritten befragten Unternehmen. Besonders häufig erst nach dem berichteten schwerwiegendsten Angriff wurden Schulungen zur ICT-Sicherheit für Mitarbeitende eingeführt. Rund jedes sechste Unternehmen machte entsprechende Angaben. Etwa gleich viele haben diese Massnahme auch heute nicht eingeführt, rund zwei Drittel hatten sie jedoch bereits vor dem schwerwiegendsten Angriff. Auch bezüglich regelmässiger Risiko- und Schwachstellenanalysen, einem kontinuierlichen Monitoring sämtlicher Log-Daten in der Unternehmens ICT sowie schriftlich fixierte Richtlinien zum Notfallmanagement ist der Anteil Unternehmen,

welche diese Massnahmen erst nach dem Angriff eingeführt haben, vergleichsweise gross. Ob der berichtete Angriff der Anlass für die Etablierung dieser und anderer Massnahmen war, wurde jedoch nicht erfasst.

8 Quellenverweise

Barth M., Hellemann, N., Kob, T., Krösmann, C., Morgenstern, U., Tschersich, T., Ritter, T., Shulman, H., Trapp, D. & Wintergerst, R. (2020). Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt. Studienbericht 2020. Berlin: Bitkom.

Dreissigacker A., von Skarczinski B. & Wollinger G.R. (2020). Cyberangriffe gegen Unternehmen in Deutschland. KFN Forschungsbericht Nr. 152. Hannover: KFN.

Corporate Trust (2014). Studie: Industriespionage. Die Schäden durch Spionage in der deutschen Wirtschaft. München: Corporate Trust.

Mändli Lerch, K. & Repic, A. (2017). Cyberrisiken in Schweizer KMUs. Befragung von GeschäftsführerInnen Schweizer KMUs. Zürich: gfs-zürich.

Nationales Zentrum für Cybersicherheit NCSC (2021). Informationssicherung: Lage in der Schweiz und International. Halbjahresbericht 2021/I (Januar-Juni). Bern: NCSC.

Peter, M. K., Hölzli, A., Kaelin, A. W. Mändli Lerch, K., Vifian, P. & Wettstein, N. (2020). Digitalisierung, Home-Office und Cyber-Sicherheit in KMU: Ein Beitrag zum Verständnis und zur Stärkung von Schweizer KMU mit 4-49 Mitarbeitenden im Umfeld von Corona (COVID-19). Bern: Die Mobiliar, digitalswitzerland, FHNW Hochschule für Wirtschaft, SATW, gfs-Zürich.

Zwahlen, F., Marti, I., Richter, M., Konopatsch, C. & Hostettler, U. (2020). Wirtschaftsspionage in der Schweiz – Schlussbericht zuhanden des Nachrichtendienstes des Bundes (NDB). Bern: Universität Bern – Institut für Strafrecht und Kriminologie.

9 Anhang

9.1 Zusammenfassung der schwerwiegendsten Angriffe

- Cybercrime
    a. Hackerangriff (manuelles Hacking) auf IT-Systeme und Firmengeräte, d.h. die Manipulation von Hard- und Software ohne die Nutzung spezieller Schadsoftware
    b. Erfolgreicher Angriff mit Ransomware, bei dem Unternehmensdaten verschlüsselt wurden
    c. Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner
    d. Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten
    e. Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden
- Abfangen digitaler Kommunikation und Datenabfluss durch Dritte
    a. Abhören oder Abfangen digitaler Kommunikation, z.B. E-Mails, Telefonate, Besprechungen
    b. Unrechtmässiger Abfluss von Daten durch Dritte, z.B. Zulieferer, Dienstleister, bei Kundenanlagen
- Social Engineering
    a. «CEO-Fraud», wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitenden zu bewirken, z.B. Geldüberweisung
    b. Sonstiges «Social Engineering», bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken/Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen
- Diebstahl von Informationsmedien
    a. Diebstahl von Informationsmedien, z.B. Smartphones, Handy, PC, Laptop, Festplatten, Unterlagen, Muster, Maschinenteile durch einen Einbruch in Firmengebäude
    b. Diebstahl von Informationsmedien, z.B. Smartphones, Handy, PC, Laptop, Festplatten durch Personen, die Zugang zum Firmengelände haben/hatten, wie z.B. Mitarbeitende, Besucher u.ä.

- Diebstahl von sensiblen Daten/Informationen durch eigene Mitarbeitenden
    a. Diebstahl von sensiblen digitalen Daten bzw. Informationen durch eigene Mitarbeitende
    b. Physischer Diebstahl von sensiblen physischen Dokumenten, z.B. Unterlagen, Muster, Maschinen, Bauteile durch eigene Mitarbeitende
- Sabotage
    a. Digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen
    b. Physische Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen
- Andere Angriffsart oder Kombination aus mehreren Angriffsarten
    a. Ausnahmen: (1) bei einer Kombination aus Cybercrime und CEO-Fraud wurde, wurde der Angriff in die Kategorie Social Engineering eingeordnet; (2) wenn verschiedene Angriffsarten aus dem Bereich Cybercrime angegeben wurden, wurde der Angriff in die Kategorie Cybercrime eingeordnet

9.2 Fragenkatalog

Nummer	**Fragetext/Antwortoptionen/ggf. Ausprägungen der Fragenitems**
1 & 2	War Ihr Unternehmen (inklusive Tochtergesellschaften im In- und Ausland) jemals von einem oder mehreren der unten aufgeführten digitalen oder physischen Angriffe betroffen. Wenn ja, wie häufig in den letzten 24 Monaten vor der Befragung. (Seit Bestehen des Unternehmens: jemals passiert ja/nein; in den letzten 24 Monaten: Bitte Anzahl eintragen) - Hackerangriff (manuelles Hacking) auf IT-Systeme und Firmengeräte, d.h. die Manipulation von Hard- und Software ohne die Nutzung spezieller Schadsoftware - Erfolgreicher Angriff mit Ransomware, bei dem Unternehmensdaten verschlüsselt wurden - Erfolgreicher Angriff mit sonstiger Schadsoftware, z.B. Viren, Würmer, Trojaner

	- Denial of Service ((D)DoS) Attacken, die auf eine Überlastung von Web- oder E-Mail-Servern zielten - Phishing-Angriffe, bei denen Mitarbeitende mit echt aussehenden E-Mails oder Websites erfolgreich getäuscht wurden und z.B. sensible Unternehmensdaten erlangt wurden - Abhören oder Abfangen digitaler Kommunikation, z.B. E-Mails, Telefonate, Besprechungen - «CEO-Fraud», wobei eine Führungsperson des Unternehmens vorgetäuscht wurde, um bestimmte Handlungen von Mitarbeitenden zu bewirken, z.B. Geldüberweisung - Sonstiges «Social Engineering», bei dem Mitarbeitende gezielt und geschickt ausgefragt bzw. ausspioniert wurden, z.B. am Telefon, in sozialen Netzwerken/Internetforen, im privaten Umfeld, auf Messen oder sonstigen Veranstaltungen - Diebstahl von Informationsmedien, z.B. Smartphones, Handy, PC, Laptop, Festplatten, Unterlagen, Mustern, Maschinenteilen durch einen Einbruch in Firmengebäude - Diebstahl von Informationsmedien, z.B. Smartphones, Handy, PC, Laptop, Festplatten durch Personen, die Zugang zum Firmengelände haben/hatten, wie z.B. Mitarbeitende, Besucher u.ä. - Diebstahl von sensiblen digitalen Daten bzw. Informationen durch eigene Mitarbeitende - Physischer Diebstahl von sensiblen physischen Dokumenten, z.B. Unterlagen, Mustern, Maschinen, Bauteilen durch eigene Mitarbeitende - Unrechtmässiger Abfluss von Daten durch Dritte, z.B. Zulieferer, Dienstleister, bei Kundenanlagen - Digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen - Physische Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen - andere Angriffsart (Bitte angeben, um welche Art von Angriff es sich handelte)

3	**Frage 3 wurde nur denjenigen Befragten angezeigt, die angegeben haben, in den letzten 24 Monaten vor der Befragung von mindestens einer Angriffsart betroffen gewesen zu sein.** Sie haben für die unten aufgeführten Angriffsarten angegeben, dass Ihr Unternehmen in den letzten 24 Monaten von diesen betroffen war. Welcher dieser Angriffe war aus Ihrer Sicht der schwerwiegendste? Sie können mehrere Angriffsarten auswählen, wenn mehrere Angriffsarten zusammen aufgetreten sind. Im Online-Fragebogen wurden die Angriffsarten aus Frage 1 & 2 angezeigt, für die mindestens ein Vorfall in den letzten 24 Monaten angegeben wurde.
4	**Frage 4 bis Frage 15 wurde nur denjenigen Befragten angezeigt, die einen schwerwiegendsten Angriff angegeben haben.** Wo war der initiale Angriffspunkt des von Ihnen angegebenen schwerwiegendsten Angriffs? - Hauptniederlassung im Inland - Hauptniederlassung im Ausland (bitte Land eintragen) - Zweigniederlassung im Inland - Zweigniederlassung im Ausland (bitte Land eintragen) - Subunternehmer - Lieferanten - Dienstleister, z.B. Cloudanbieter - Kundschaft - Sonstiger Ort (bitte eintragen)
5	Sind die Täterinnen und Täter des von Ihnen angegebenen schwerwiegendsten Angriffs bekannt bzw. gibt es eine Vermutung? - Die Täterinnen und Täter sind bekannt (polizeilich ermittelt/gerichtlich festgestellt) - Die Täterinnen und Täter sind bekannt (auf sonstigem Wege) - Die Täterinnen und Täter sind unbekannt, aber es gibt eine Vermutung - Die Täterinnen und Täter sind unbekannt

6	**Frage 5 wurde nur denjenigen Befragten angezeigt, die bei Frage 5 angegeben haben, die Täterinnen und Täter seien bekannt oder sie seien unbekannt, aber es gebe eine Vermutung.** Wer waren Ihrer Kenntnis oder Ihrer Vermutung nach beim von Ihnen angegebenen schwerwiegendsten Angriffs die Täterinnen bzw. Täter? (Mehrfachnennungen) - Hacker (einzeln, im Kollektiv oder Organisierte Kriminalität) - Kunden - Lieferanten - Eigene aktuelle oder ehemalige Mitarbeiter - Dienstleister/Berater - Staatlicher Nachrichtendienst - Andere Täter und Täterinnen (bitte eintragen)
7	Was denken Sie: Wurde Ihr Unternehmen bei dem von Ihnen angegebenen schwerwiegendsten Angriff bzw. den zusammengehörigen Angriffen … - zielgerichtet attackiert/ausgewählt (z.B. gezielter Spionageangriff)? - als ein Unternehmen von vielen anderen attackiert (z.B. bei massenhaft versendeter Schadsoftware, Ransomwareangriffen oder dem Ausnützen von technischen Schwachstellen)? - Weiss nicht
8	**Frage 8 wurde nur denjenigen Befragten angezeigt, die bei Frage 7 angegeben haben, sie wurden zielgerichtet attackiert.** Was denken Sie: Warum wurde Ihr Unternehmen bei diesem schwerwiegendsten Angriff zielgerichtet attackiert? (Mehrfachnennungen möglich, Antwortkategorien: „ja“, „nein“, „weiss nicht“) - Diebstahl von Produkten, Herstellungsverfahren oder Dienstleistungen, Know how z.B. aufgrund spezieller Technik, Design, Materialien, Innovation - Schädigung der Reputation, z.B. wegen besonders gutem Image der Firma, wegen hohem Sicherheitsstandard, besonderer Vertrauenswürdigkeit - Hohes Erpressungs-/Ertragspotenzial - Sabotage - Anderer Grund (bitte eintragen)

9	Zu welchen Folgen hat der genannte schwerwiegendste Angriff bzw. die zusammengehörigen Angriffe geführt? (Mehrfachnennungen möglich) - Ausfall der Informatik - Diebstahl oder Schädigung von IT- oder Kommunikationsgeräten - Betriebsunterbrechung (d.h. vollständiger oder teilweiser Ausfall der Produktion und Administration) - Erpressung mit den verschlüsselten Daten - Erpressung mit entwendeten Daten - Kosten für Sofortmassnahmen zur Abwehr und Aufklärung - Kosten aufgrund von Lösegeldzahlungen - Kosten für Wiederherstellung von Daten oder IT-Infrastruktur (Hardware und Software) - Kosten für externe Beratung - Kosten für Rechtsstreitigkeiten, Schadensersatz, Strafen - Investitionen in Sicherheitsmassnahmen und spezielle Versicherungen - Negative Auswirkung auf die Geschäftsentwicklung - Kundenverluste/Auftragsverluste - Umsatzeinbussen durch nachgemachte Produkte (Plagiate) - Verletzung von Schutzrechten (Geistiges Eigentum) - Verlust von personenbezogenen Daten, z.B. Kundendaten, Daten von Mitarbeitenden - Reputationsverluste/Negative Presse - Interne Reorganisationskosten - Entlassung von Mitarbeitenden - Höhere Mitarbeitendenfluktuation, z.B. Verlust von kompetenten Arbeitskräften - Positive Reaktionen (z.B. von Kundinnen und Kunden) auf den raschen und resilienten Umgang mit dem Angriff - Erhöhung des Zusammenhalts unter den Mitarbeitenden - Keine Folgen

10	**Frage 10 bis Frage 13 wurde nur denjenigen Befragten angezeigt, die bei Frage 9 mindestens eine Folge angegeben haben.** Sie haben die unten aufgeführten Folgen für den von Ihnen berichteten schwerwiegendsten Angriff angegeben: Bitte bringen Sie diese in eine Rangfolge nach ihrer Schwere, indem Sie diese entsprechend anordnen (drag and drop). Ganz oben soll die schwerste Folge stehen, auf Platz zwei die zweitschwerste usw. Im Online-Fragebogen werden nur die negativen Folgen angezeigt, die sie bei Frage 9 angekreuzt haben. Diese sollten dann in eine Rangfolge gebracht werden.
11	Bitte ergänzen Sie: Der durch den schwerwiegendsten Angriff erfolgte Schaden… - war kurzfristig behebbar und leicht verdaubar - führte zu spürbaren Einschränkungen - gefährdete die Existenz des Unternehmens - zog keine Einschränkungen nach sich
12	Bitte geben Sie an, welche Kosten durch den von Ihnen angegebenen schwerwiegendsten Angriff entstanden sind. (Bitte schätzen Sie, falls die Kosten nicht genau beziffert werden können und tragen ganze Zahlen ein.)
13	Gab es bei diesem schwerwiegendsten Angriff eine Lösegeldforderung? (Antwortkategorien „ja“, „nein“, „weiss nicht“, „keine Angabe“)
14	Waren bei dem genannten schwerwiegendsten Angriff die folgenden Daten betroffen? Wenn ja, wurden diese gelöscht, manipuliert, gestohlen oder verschlüsselt? (Sie können mehrere Antwortmöglichkeiten ankreuzen) (Antwortkategorien „nein“, „ja, sie wurden ge-löscht“, „ja, sie wurden manipuliert“, „ja, sie wurden gestohlen“, „ja, sie wurden verschlüsselt oder blockiert“, „weiss nicht“) - Kunden- und personenbezogene Daten - Produktions- und Prozessdaten - Produkt und F & E Daten - Betriebswirtschaftliche Daten - Andere Daten (bitte eintragen)

15	Zu welchen der unten aufgeführten Akteure wurde nach dem von Ihnen genannten schwerwiegendsten Angriff Kontakt aufgenommen? (Mehrfachnennungen möglich) - Polizei - Nachrichtendienst des Bundes (NDB) oder vergleichbare Behörden im Ausland - Versicherung - spezialisierter Dienstleister - Nationales Zentrum für Cybersicherheit (NCSC) oder vergleichbare Behörden im Ausland - Andere (bitte eintragen)
16	Welche der folgenden Schutzmassnahmen gibt es derzeit in Ihrem Unternehmen? (Antwortkategorien „ja“, „nein“, „weiss nicht“; für diejenigen, die einen schwerwiegendsten Angriff angegeben hatten, wurden anstelle der Antwortkategorie „ja“ die beiden Antwortkategorien „ja und bereits vor dem schwerwiegendsten Angriff“, „ja, aber erst nach dem schwerwiegendsten Angriff“ angezeigt) - Aktuelle Anitivirensoftware - Schutz der ICT-Systeme mit einer Firewall - Regelmässige Backups/Datensicherungen - Physisch getrennte Aufbewahrung von Backups - Regelmässige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches - Mindestanforderungen für Passwörter/Multifaktor-Authentifikation - Verschlüsselung von E-Mails - Verschlüsselung von Festplatten - Kein Anschluss privater Peripheriegeräte (USB-Sticks, Smartphones etc.) an das Firmennetzwerk - Intrusion Detection System (IDS) - Schriftlich fixierte Richtlinien zur Informations- bzw. ICT-Sicherheit - Schulungen zur ICT-Sicherheit für Mitarbeitende - Individuelle Vergabe von Zugangs- und Nutzungsrechten je nach Aufgabe - Trennung der ICT-Netzwerke der Firma, wie z. B. ein vom Internet getrenntes Netzwerk

	- Alle Fernzugriffe (für Wartung und Administration) auf Leitstelle und Steuerungsanlagen sind mit starker Authentisierung abgesichert - Kontinuierliches Monitoring sämtlicher Log-Daten in der Unternehmens ICT - Regelmässige Risiko- und Schwachstellenanalysen - Übungen oder Simulationen für den Ausfall wichtiger ICT-Systeme - Schriftlich fixierte Richtlinien zum Notfallmanagement - Einführung eines Informationssicherheits-Managementsystems (ISMS) - Klare Regelungen für den Umgang mit vertraulichen Informationen (Informationssicherheitskonzept) - Eindeutige Klassifizierung/Kennzeichnung von Betriebsgeheimnissen - Geheimhaltungsverpflichtungen für Mitarbeitende - Geheimhaltungsverpflichtungen für Geschäftspartner - Weisungen für die Mitnahme von vertraulichen Informationen bei Auslandsreisen - Weisungen für das Verhalten bei Messen und Ausstellungen - Besuchermanagement/Zutrittskontrollen - Background-Checks von Geschäftspartnern (Lieferanten, Dienstleister, Berater etc.) - Anpassung der Rekrutierungsprozesse, z.B. persönliche Sicherheitsüberprüfungen, Straf- und Betreibungsregisterauszüge, zusätzliche Unterlagen bei ausländischen Bewerbern - Clean-Desk-Policy - Regelmässige Kontrollen (der Arbeitsplätze, der Mitarbeitenden etc.) in Bezug auf die Einhaltung von Vorschriften - Physische Sicherheitsmassnahmen, z.B. Kameras, Alarme, Badge-Schliesssysteme - Festlegung von Zugriffsrechten für bestimmte Räume im Unternehmen - Kontrolle der veröffentlichten Informationen, z.B. auf Homepage /durch Mitarbeitende in den sozialen Medien - Weitere Massnahmen (bitte eintragen)

17	Wie viele Mitarbeitende hat Ihr unternehmen? - 1 – 49 - 50 – 249 - 250 – 999 - über 1000