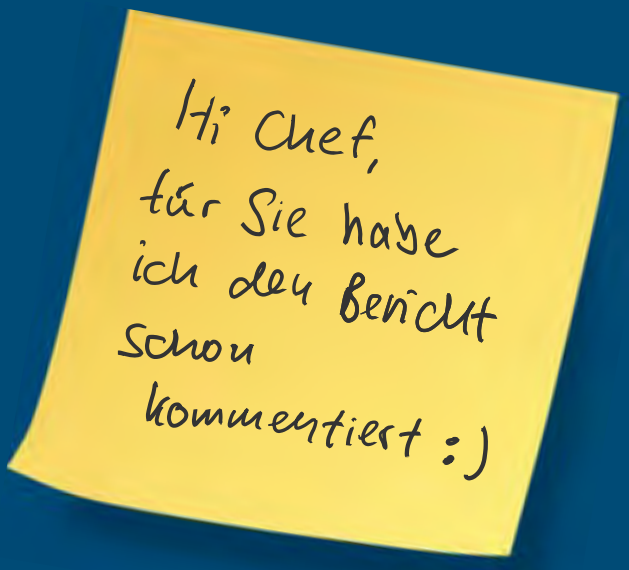
IT-Sicherheit
IN DER WIRTSCHAFT

CYBERANGRIFFE GEGEN UNTERNEHMEN

Ergebnisse einer repräsentativen Unternehmensbefragung

in Deutschland 2018/19



Kurzbericht
Hannover, 2020

KRIMINOLOGISCHES FORSCHUNGSINSTITUT NIEDERSACHSEN E.V.

Leibniz Universität Hannover

LBS

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Zusatzförderung durch:

pwc

VHV STIFTUNG

Zitierung: KFN (2020): Cyberangriffe gegen Unternehmen. Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland 2018/2019. Kurzbericht. Hannover

Herausgeber: Kriminologisches Forschungsinstitut Hannover e.V. (KFN)

Redaktion: Arne Dreißigacker
Bennet von Skarczinski

Mitarbeit: Lukas Boll
Niels Grote

Druck: DruckTeam Druckgesellschaft mbH, Hannover

© Kriminologisches Forschungsinstitut Niedersachsen e.V., 2020
Lützerodestraße 9, 30161 Hannover
Tel. +49 (0)511 34836-0, Fax: +49 (0)511 34836-10
E-Mail: kfn@kfn.de, Internet: www.kfn.de

Printed in Germany
Alle Rechte vorbehalten

INHALT

01 AUSGANGSPUNKT DER STUDIE 3

02 VORGEHEN BEI DER BEFRAGUNG 7

03 VERBREITUNG VON CYBERANGRIFFEN 11

04 MÖGLICHE RISIKOFAKTOREN 17

05 FOLGEN DES SCHWERWIEGENDSTEN ANGRIFFS 21

06 MÖGLICHE SCHUTZFAKTOREN 27

07 FAZIT 33

GLOSSAR 37

01

„Cyberkriminalität und deren Auswirkung stellt ein unternehmerisches Risiko dar, das unter anderem aufgrund der fehlenden verlässlichen Datenbasis nur schwer eingeschätzt, bewertet und gesteuert werden kann.“

AUSGANGSPUNKT DER STUDIE

Die Digitalisierung in der Gesellschaft bietet Privatpersonen wie Unternehmen vielfältige Chancen und Möglichkeiten, stellt sie aber auch gleichzeitig vor Risiken. Um ihre Wettbewerbsfähigkeit langfristig zu sichern, müssen sich Unternehmen mit der Digitalisierung ihrer Prozesse, ihrer Organisation und den eingesetzten Technologien auseinandersetzen.

Cyberkriminalität und deren Auswirkung stellt dabei ein unternehmerisches Risiko dar, das unter anderem aufgrund der fehlenden verlässlichen Datenbasis nur schwer eingeschätzt, bewertet und gesteuert werden kann.

Die Aussagekraft amtlicher Statistiken wie die Polizeiliche Kriminalstatistik (PKS) leidet vor allem an einer sehr geringen Anzeigequote. Daneben kann aufgrund des Vorgehens bei der Erfassung nicht zwischen Privatpersonen und Unternehmen als Betroffenen unterschieden werden. Zudem bleiben Cyberangriffe mit politischer oder nachrichtendienstlicher Motivation und ohne erkennbare Anhaltspunkte für eine innerdeutsche Tathandlung unberücksichtigt.[1]

in 2018 wurden nur 86.000 Fälle gemeldet ... bei 3,5 Mio Unternehmen und 83 Mio Einwohnern

Studien kommerzieller Herausgeber müssen sich nicht nach wissenschaftlichen Standards richten, sind demzufolge hinsichtlich ihrer Erhebungsmethoden häufig intransparent und neigen mitunter zu einer tendenziösen Darstellung im Sinne der jeweiligen wirtschaftlichen Ausrichtung. Die Stichprobengrößen verfügbarer Erhebungen sind zudem häufig relativ klein und erlauben oft nur

[1] Vgl. Bundeskriminalamt (2016): Cybercrime. Bundeslagebild 2015. Wiesbaden, S. 5.

2. B. eine Umfrage auf der eigenen Website oder unter eigenen Kunden

allgemein beschriebene Ergebnisse, die nicht selten zu widersprüchlichen Ergebnissen führen. Im Falle von willkürlich bestimmten Stichproben ist zudem eine Verallgemeinerbarkeit der Ergebnisse so gut wie ausgeschlossen, da die Stichprobenzusammensetzung kaum kontrolliert werden kann.

Daneben fallen offene Fragestellungen auf, die bisher nur selten oder nicht ausreichend präzise adressiert wurden. Dazu zählen insbesondere differenzierte Auswirkungen einzelner Angriffsarten auf Technik, Prozesse, Organisation und Beschäftigte von Unternehmen sowie die Art und Höhe entstehender Kosten infolge von Cyberangriffen und nicht zuletzt Risiko- und Schutzfaktoren, die sich auf die Betroffenheit von Cyberangriffen auswirken.

Um einen Beitrag zur Beantwortung solcher Forschungsfragen zu leisten, wurde das Forschungsprojekt „Cyberangriffe gegen Unternehmen" vom Kriminologischen Forschungsinstitut Niedersachsen e.V. (KFN) in Zusammenarbeit mit dem Forschungszentrum L3S der Leibniz-Universität Hannover initiiert. Gefördert wird dieses Projekt durch die Initiative „IT-Sicherheit in der Wirtschaft" des Bundesministeriums für Wirtschaft und Energie (BMWi). Eine Zusatzförderung erfolgt von der Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers (PwC) sowie der VHV Stiftung.

Abbildung 1: Initiative IT-Sicherheit in der Wirtschaft

IT-Sicherheit IN DER WIRTSCHAFT

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

Im Rahmen des Forschungsprojektes „Cyberangriffe gegen Unternehmen“ wurde eine repräsentative Unternehmensbefragung von 5.000 Unternehmen durchgeführt. Die Ergebnisse dieser Studie liegen im Form eines ausführlichen Forschungsberichtes vor und werden in dieser Kurzfassung für Verantwortliche und Entscheider*innen insbesondere kleiner und mittlerer Unternehmen zusammenfassend beschrieben.

#152 zu finden unter kfn.de/publikationen Sehr zu empfehlen :)

Der Kurzbericht ist folgendermaßen aufgebaut:

- Nach dieser kurzen Einführung folgt in **Abschnitt 02** eine knappe Beschreibung des methodischen Vorgehens und der zugrundeliegenden Stichprobe. Diese gibt Auskunft darüber, auf welche Unternehmen die vorgestellten Ergebnisse bezogen werden können und welche Punkte bei der Interpretation und beim Vergleich mit anderen Studien zu beachten sind.
- In **Abschnitt 03** wird die Verbreitung von Cyberangriffen gegen Unternehmen dargestellt. Dabei wird nach Unternehmensgröße, Cyberangriffsart und Branche differenziert.
- In **Abschnitt 04** werden weitere Unternehmensmerkmale als mögliche Risikofaktoren in Beziehung zur Betroffenheit von Cyberangriffen gesetzt.
- **Abschnitt 05** geht auf die Folgen der schwerwiegendsten Cyberangriffe der letzten zwölf Monate ein. Dazu werden die entstandenen direkten Kosten, die Anzeigebereitschaft und die Bewertung der polizeilichen Ermittlung beleuchtet.
- In **Abschnitt 06** stehen die technischen und organisatorischen IT-Sicherheitsmaßnahmen als mögliche Schutzfaktoren im Mittelpunkt.
- Und in **Abschnitt 07** wird ein zusammenfassendes Fazit gezogen.

Im **Glossar** am Ende des Kurzberichtes finden sich kurze Erläuterungen zu den verwendeten englischen Begrifflichkeiten.

02

„Diese Unternehmensbefragung zählt derzeit zu den größten und aussagekräftigsten Studien zum Thema Cyberangriffe gegen Unternehmen, die unabhängig, nach wissenschaftlichen Gütekriterien durchgeführt und transparent dokumentiert wurde."

VORGEHEN BEI DER BEFRAGUNG

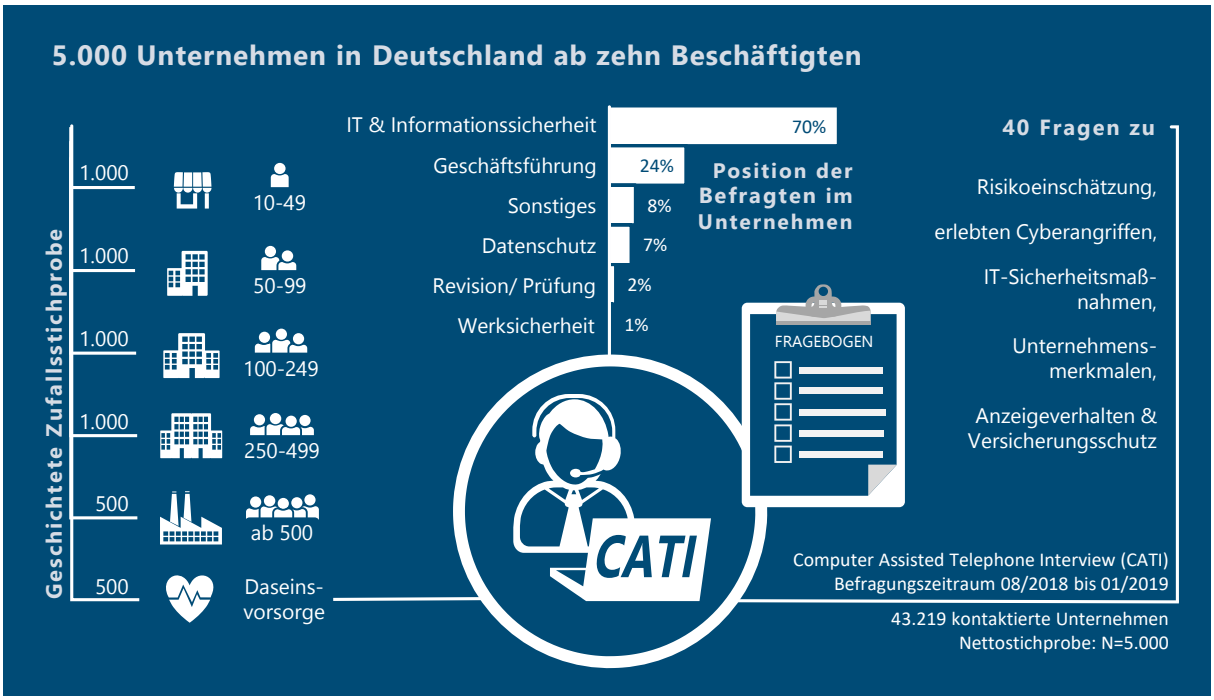
Die Befragung der 5.000 Unternehmen wurde im Rahmen eines wissenschaftlichen Forschungsprojektes konzipiert und per computergestützten Telefoninterviews (CATI) zwischen August 2018 und Januar 2019 vom Umfrageinstitut Kantar EMNID durchgeführt. Sie basiert auf einer geschichteten Zufallsstichprobe aus den kommerziellen Unternehmensdatenbanken Bisnode und Heins & Partner und umfasst Unternehmen ab zehn Beschäftigten nahezu aller Branchen der offiziellen Klassifikation der Wirtschaftszweige (WZ08-A bis S).

Neben 1.000 kleinen Unternehmen mit 10-49 Beschäftigten und 3.000 mittleren Unternehmen mit 50-499 Beschäftigten sind auch 500 große Unternehmen ab 500 Beschäftigten als Vergleichsgruppe enthalten. Zusätzlich wurden weitere 500 Unternehmen der Daseinsvorsorge (z.B. Energie- und Wasserversorgung, Gesundheitswesen, Verkehrsbetriebe) anvisiert, die sich auf alle Größenklassen verteilen (siehe Abbildung 2).

Als vorrangige Zielpersonen der Befragung galten Personen, die für den Bereich IT- & Informationssicherheit verantwortlich waren. Wenn derartige Positionen in den Unternehmen nicht existierten, wurden Beschäftigte befragt, in deren Zuständigkeitsbereich das Thema IT- & Informationssicherheit fiel.

Die Befragung wurde durch professionelle Interviewer*innen anhand eines standardisierten Fragebogens mit 40 Fragen zur Risikoeinschätzung, zu erlebten Cyberangriffen, zu IT-Sicherheitsmaßnahmen, Unternehmensmerkmalen, zum Anzeigeverhalten und zum Versicherungsschutz durchgeführt.

Abbildung 2: Unternehmensbefragung



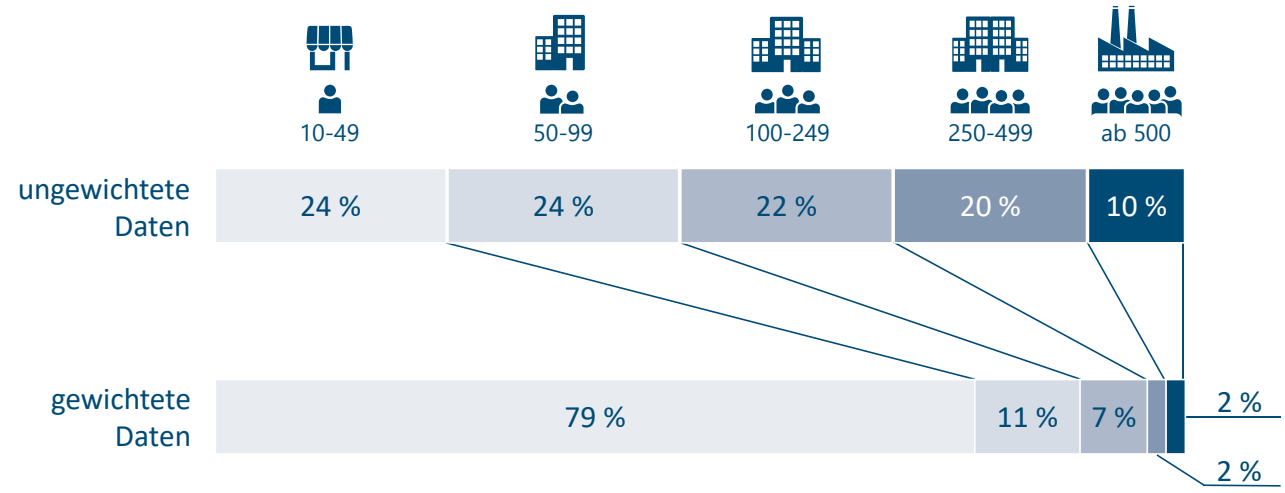
Durch eine nachträgliche Gewichtung der geschichteten Zufallsstichprobe nach Beschäftigtengrößenklasse und Wirtschaftszweig entspricht die Verteilung der Zusammensetzung aller Unternehmen ab zehn Beschäftigten in Deutschland im Jahr 2018, womit verallgemeinerbare Aussagen möglich sind.

Bei der Interpretation der Ergebnisse, die sich im Folgenden auf alle Unternehmen der Stichprobe beziehen, ist zu berücksichtigen, dass Unternehmen mit 10-49 Beschäftigten den größten Anteil (79 %) bilden, wohingegen Unternehmen mit mehr als 500 Beschäftigen lediglich 2 % der gewichteten Stichprobe ausmachen (Abbildung 3). Gesamtergebnisse über alle Unternehmensgrößen hinweg sind dementsprechend stark von den Angaben der kleinen Unternehmen beeinflusst und weichen in Hinblick auf die differenzierten Ergebnisse deutlicher von der Gruppe der großen Unternehmen ab.

Mögliche Ursache, warum das Bauchgefühl derer die viel mit großen Unternehmen arbeiten, manchmal täuscht

ab hier also nur noch gewichtete Daten

Abbildung 3: Verteilung der Beschäftigtengrößenklassen in der Stichprobe



Darüber hinaus ist zu berücksichtigen, dass Befragungsstudien allgemein verschiedenen Einschränkungen unterliegen, die deren Aussagekraft beeinträchtigen. Hier sind dies im Wesentlichen Unsicherheiten hinsichtlich der Vollständigkeit der Firmendatenbanken, aus der die Stichprobe gezogen wurde, sowie etwaige Erinnerungs- und Wissenslücken der Befragten, die mit ihren Aussagen jeweils ein Unternehmen repräsentieren. Wie bei anderen Befragungsstudien auch besteht die Möglichkeit, dass die Befragten Antworten gegeben haben, die sich tendenziell eher daran orientierten, wie es sein müsste, als daran, wie es ist. Zudem konnten mit dieser Erhebungsmethode keine Informationen zu unbemerkt gebliebenen Cyberangriffen (absolutes Dunkelfeld) gesammelt werden und der Detailgrad der Fragen, z.B. zu Qualität und Reifegraden von IT-Sicherheitsmaßnahmen, war aufgrund zeitlicher Grenzen beschränkt.

es wurde also nur gefragt, was vorhanden ist

Trotz der genannten Restriktionen zählt diese Unternehmensbefragung derzeit zu den größten und aussagekräftigsten Studien zum Thema Cyberangriffe gegen Unternehmen, die unabhängig, nach wissenschaftlichen Gütekriterien durchgeführt und transparent dokumentiert wurde. Damit bietet sie eine sehr gute Grundlage für Einschätzungen zu diesem Themenbereich.

03

„Etwa zwei Fünftel der Unternehmen waren in den letzten zwölf Monaten von mindestens einem Cyberangriff betroffen.

Neben der Unternehmensgröße stehen auch die Branche bzw. die Wirtschaftszweigzugehörigkeit im Zusammenhang mit der Betroffenheit.“

VERBREITUNG VON CYBERANGRIFFEN

Definition

Bezogen auf die Frage, ob die Unternehmen in den letzten zwölf Monaten von Cyberangriffen betroffen waren, auf die sie reagieren mussten, wurde zwischen verschiedenen Angriffsarten unterschieden (siehe Abbildung 4). Zusätzlich konnte jeweils angegeben werden, wie häufig dies der Fall war. Mehrfachnennungen waren möglich und bei kombinierten Angriffsarten innerhalb eines zusammenhängenden Cyberangriffs auch erwünscht.

E-Mails im Spam-Filter gelöscht also nicht dazu

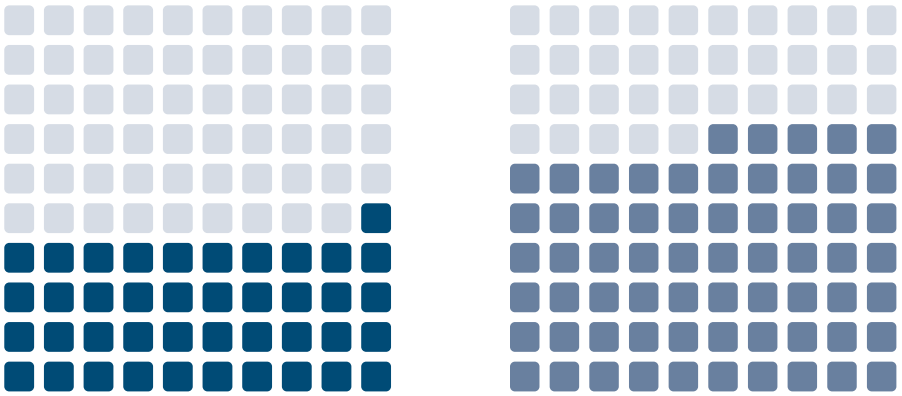
ein Angriff kann also mehrere Angriffsarten beinhalten

Abbildung 4: Angriffsarten

Wenn kein Cyberangriff in den letzten zwölf Monaten erlebt wurde, konnte angegeben werden, ob dies jemals der Fall war.

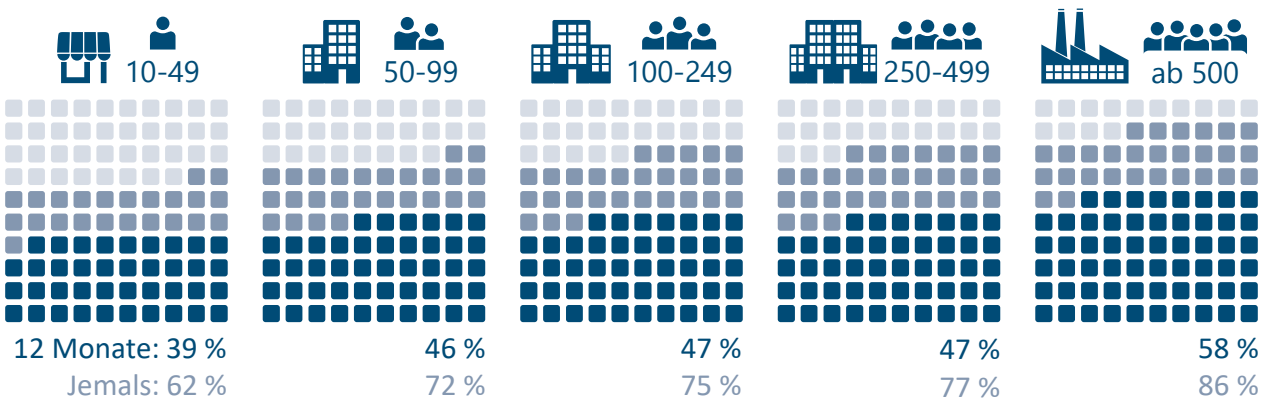
Über alle Angriffsarten hinweg waren etwa zwei Fünftel der Unternehmen (41 %) in den letzten zwölf Monaten von mindestens einem Cyberangriff betroffen. Dieser Anteil steigt auf rund zwei Drittel (65 %) bezogen auf die gesamte Vergangenheit (siehe Abbildung 5)

Abbildung 5: Betroffenheit von Cyberangriffen insgesamt



Große Unternehmen mussten anteilig deutlich häufiger auf Cyberangriffe reagieren als mittlere und kleine Unternehmen. Dies gilt für die letzten zwölf Monate als auch für die Vergangenheit insgesamt (siehe Abbildung 6).

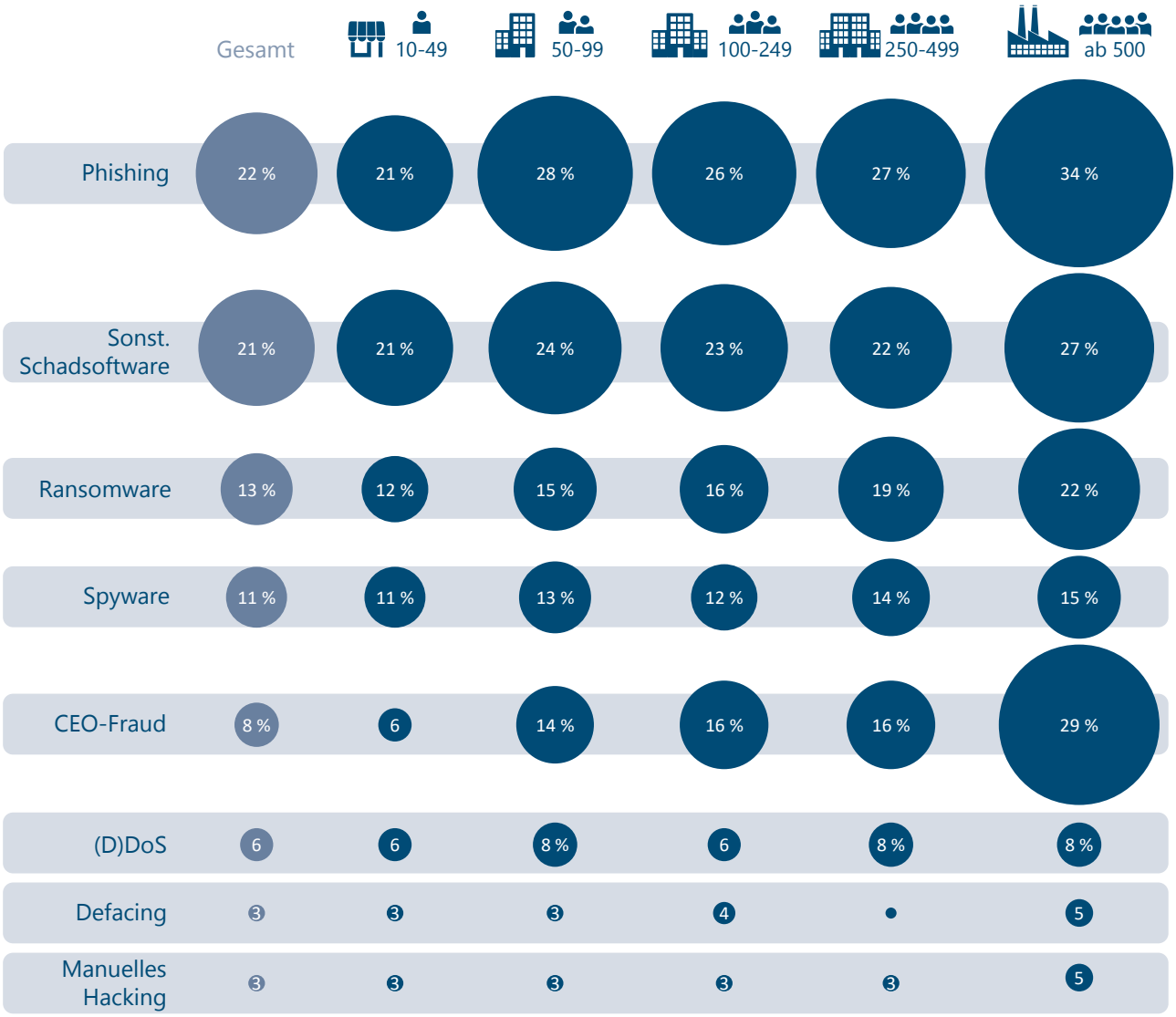
Abbildung 6: Betroffenheit von Unternehmen nach Größe



Unterschieden nach Angriffsarten zeigt sich, dass vergleichsweise viele Unternehmen in den letzten zwölf Monaten von Phishing und sonstiger Schadsoftware betroffen waren (siehe Abbildung 7). Im Vergleich der Unternehmen nach ihrer Größe fallen lediglich bei Ransomware, Phishing und CEO-Fraud deutliche Unterschiede auf. Große Unternehmen sind von diesen Angriffsarten anteilig häufiger betroffen als mittlere und kleine Unternehmen.

Spyware und sonstige Malware betraf alle in etwa gleich

Abbildung 7: Betroffenheit nach Angriffsart und Unternehmensgröße (letzte 12 Monate)

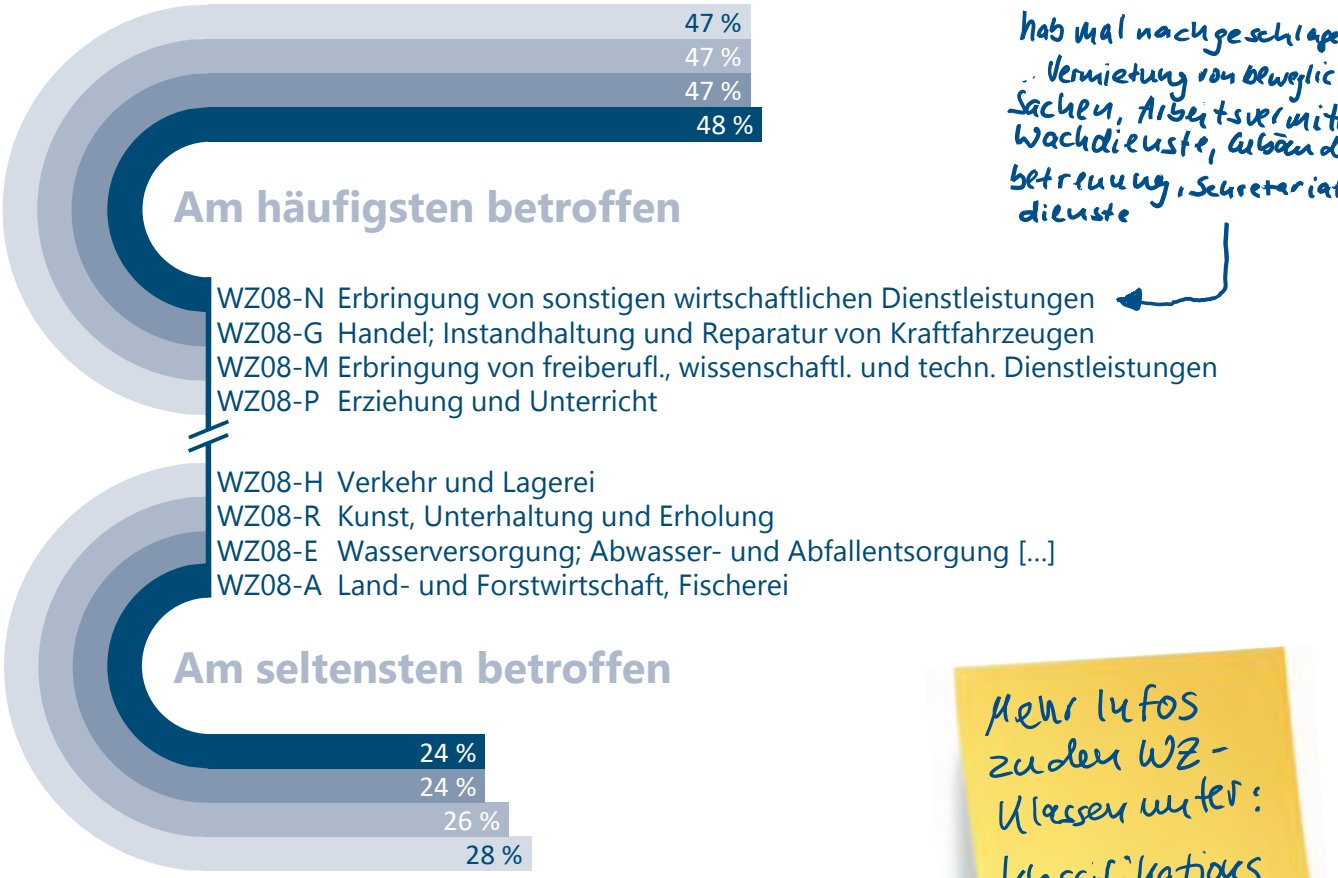


Im Forschungs-Bericht #152 ist das ausführlich beschrieben

Neben der Unternehmensgröße steht auch die Branche bzw. die Wirtschaftszweigzugehörigkeit im Zusammenhang mit der Betroffenheit von Cyberangriffen.

In Abbildung 8 werden die Wirtschaftszweige der ersten Ebene der WZ08-Klassifikation mit den vier größten und vier kleinsten Betroffenheitsanteilen dargestellt. Zu den am häufigsten betroffenen Wirtschaftszweigen zählen Unternehmen zur Erbringung von sonstigen wirtschaftlichen Dienstleistungen (48 %), Unternehmen des Handels inklusive Unternehmen zur Instandhaltung und Reparatur von Kraftfahrzeugen, Unternehmen zur Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen sowie aus dem Bereich Erziehung und Unterricht, jeweils mit Betroffenheitsanteilen von 47 %.

Abbildung 8: Betroffenheit nach Wirtschaftszweig (WZ08-Klassen, Ebene 1, Auszug)



hab mal nachgeschlagen: „Vermietung von beweglichen Sachen, Arbeitsvermittlung, Wachdienste, Gebäudebetreuung, Sekretariatsdienste

Mehr Infos zu den WZ-Klassen unter: klassifikationsserver.de

Zwischen diesen und den vier am seltensten betroffenen Wirtschaftszweigen: Verkehr und Lagerei (28 %), Kunst, Unterhaltung und Erholung (26 %), Wasserversorgung, Abwasser- und Abfallentsorgung und Beseitigung von Umweltverschmutzungen sowie Land- und Forstwirtschaft), Fischerei (jeweils 24 %) liegen bis zu 24 Prozentpunkte.

Noch deutlicher unterscheiden sich die Wirtschaftszweige auf der zweiten Ebene der WZ08-Klassifikation. Am häufigsten waren mit einem Anteil von 71 % Unternehmen des Verlagswesens in den letzten zwölf Monaten von Cyberangriffen betroffen und am seltensten Unternehmen zur Erbringung von sonstigen überwiegend persönlichen Dienstleitungen mit einem Anteil von 20 % (Abbildung 9).

Abbildung 9: Betroffenheit nach Wirtschaftszweig (WZ08-Klassen, Ebene 2, Auszug)

04

„Die Betroffenheitsraten kleiner und mittlerer Unternehmen erhöhen sich zum Teil deutlich, wenn sie z.B. mehrere Standorte in Deutschland oder mindestens einen zusätzlichen Standort im Ausland haben oder Güter bzw. Dienstleitungen exportieren.“

MÖGLICHE RISIKOFAKTOREN

Definition

Unternehmen = selbstständige juristische Einheit

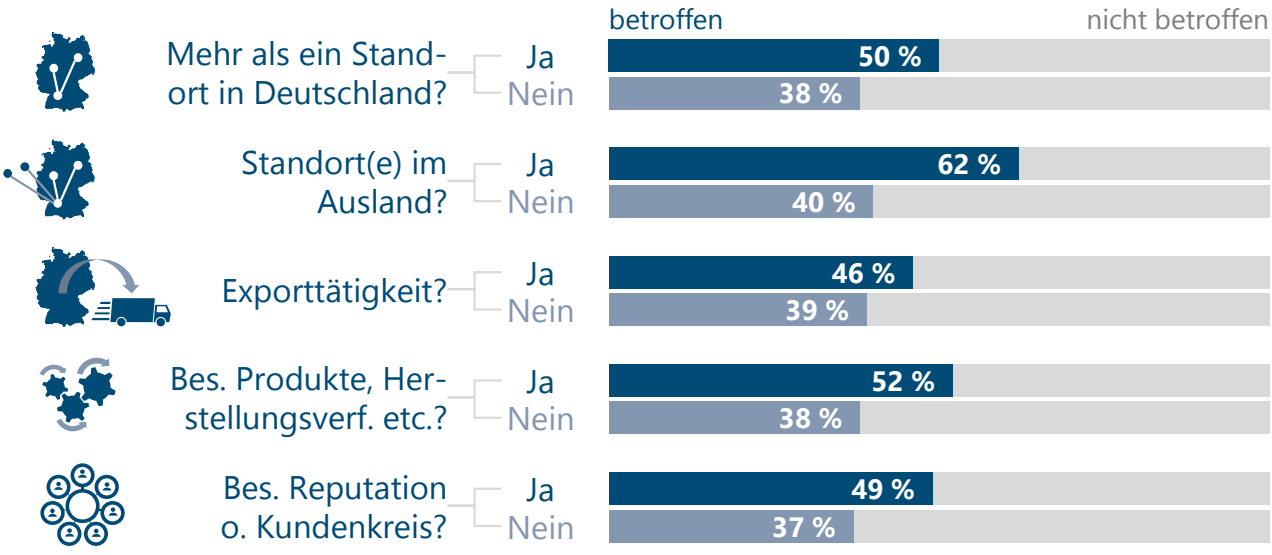
Beim Vergleich der Anteile von Unternehmen, die in den letzten zwölf Monaten von Cyberangriffen betroffen waren und bestimmte Merkmale aufweisen oder nicht, zeigen sich zum Teil weitere Unterschiede.

≠ gesamter Konzern

≠ einzelne Betriebsstätte

Die Hälfte der Unternehmen mit mehr als einem Standort musste im letzten Jahr auf mindestens einen Cyberangriff reagieren, während dies lediglich auf 38 % der Unternehmen mit nur einem Standort zutraf (Abbildung 10).

Abbildung 10: Anteile von Cyberangriffen betroffener Unternehmen nach ausgewählten Merkmalen



fett: statistisch bedeutsamer Unterschied

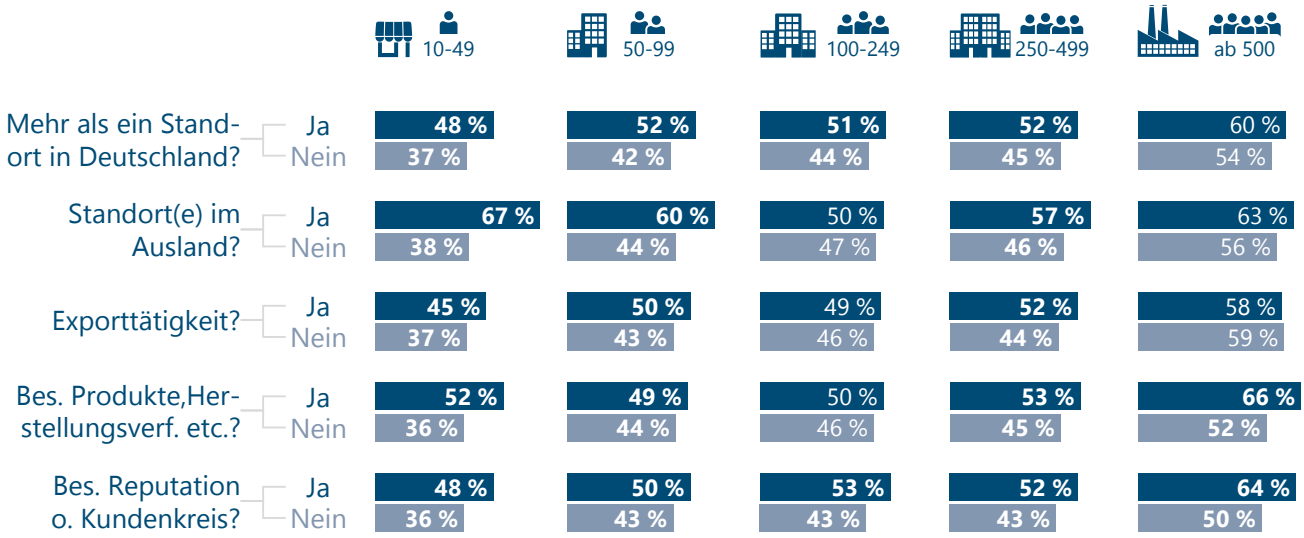
Noch deutlicher fällt der Unterschied zwischen Unternehmen mit und ohne Auslandsstandorten aus (62 % bzw. 40 %). Daneben sind bei Unternehmen, die Waren oder Dienstleistungen exportieren, die nach eigener Einschätzung über besondere Produkte,

Herstellungsverfahren, Dienstleistungen oder über eine besondere Reputation bzw. einen besonderen Kundenkreis verfügen, signifikant höhere Betroffenheitsraten festzustellen.

Zu erkennen ist, dass sich die Unterschiede der Betroffenheit von Cyberangriffen insbesondere zwischen kleinen, mittleren und großen Unternehmen unter Einbezug möglicher Risikofaktoren zumindest teilweise angleichen. Das bedeutet, dass diese Unternehmensmerkmale entscheidender sind als die Unternehmensgröße.

Also keine Entwarnung für UMU

Abbildung 11: Anteile von Cyberangriffen betroffener Unternehmen nach ausgewählten Merkmalen und Größe



fett: statistisch bedeutsamer Unterschied

Die Betroffenheitsraten kleiner und mittlerer Unternehmen erhöhen sich zum Teil deutlich, wenn sie z.B. mehrere Standorte in Deutschland oder mindestens einen zusätzlichen Standort im Ausland haben oder Güter bzw. Dienstleitungen exportieren.

Besonders sichtbar wird dies bei Standorten im Ausland. Kleine Unternehmen (10-49 Beschäftigte) mit Auslandsstandort(en) sind tendenziell sogar stärker betroffen als große Unternehmen (ab 500 Beschäftigte). Besondere Produkte, Herstellungsverfahren, Reputationen oder Kundenkreise wirken sich in ähnlicher Art und Weise aus.

Unternehmen der Daseinsvorsorge, d.h. Unternehmen, die die notwendige Grundversorgung der Bevölkerung mit existentiell wichtigen Gütern und Dienstleistungen gewährleisten (z.B. Wasser- und Stromversorger, Krankenhäuser u.ä.), waren mit einem Anteil von 31 % hingegen seltener betroffen als Unternehmen der anderen Wirtschaftszweige (42 %), was auf einen höheren Schutz solcher bedeutsamen Unternehmen hinweist. Dies zeigt sich insbesondere bei den kleineren Unternehmen (10-49 bzw. 50-99 Beschäftigten).

Es kann festgehalten werden, dass nicht alle Unternehmen das gleiche Risiko haben, von Cyberangriffen getroffen zu werden. In der Regel bieten große Unternehmen aufgrund ihrer höheren Komplexität in organisatorischer, personeller und technischer Hinsicht die größere Angriffsfläche für Täter*innen. Dies gilt besonders für Cyberangriffe, die Elemente des sogenannten Social Engineerings enthalten (z.B. CEO-Fraud oder Phishing). Hier wirkt sich wahrscheinlich die mit der Unternehmensgröße zunehmende Anonymität unter den Beschäftigten aus.

Dennoch gibt es für kleine und mittlere Unternehmen keinen Grund für Entwarnung. Unter Berücksichtigung verschiedener Unternehmensmerkmale, steigt deren Risiko von Cyberangriffen betroffen zu werden auf das Niveau der großen Unternehmen. Dies gilt z.B. dann, wenn sich die Anzahl der Standorte im In- und Ausland und damit auch die IT-Struktur vergrößert und die IT-Sicherheitsmaßnahmen daraufhin möglicherweise aufgrund fehlender Ressourcen nicht angepasst werden.

Auch Besonderheiten kleiner und mittlerer Unternehmen, z.B. besondere Herstellungsverfahren, Produkte etc. oder besondere Kundenkreise, steigern deren Risiko und damit die Notwendigkeit für zusätzlichen Schutz.

Cyber-Risiken können nicht nur durch Größe und Komplexität erklärt werden!

05

„Direkte Kosten infolge des schwerwiegendsten Angriffs entstanden bei 70 % der Unternehmen insbesondere im Zusammenhang mit Sofortmaßnahmen zur Abwehr und Aufklärung, mit der Wiederherstellung bzw. Wiederbeschaffung sowie mit externer Beratung.“

FOLGEN DES SCHWERWIEGENDSTEN ANGRIFFS

Um die Folgen von Cyberangriffen möglichst detailliert zu erfassen, sollten sich die Befragten nur auf den schwerwiegendsten Cyberangriff der letzten zwölf Monate beziehen. Zu den diesbezüglich am häufigsten genannten Angriffsarten zählen Phishing (27 %), sonstige Schadsoftware (24 %) und Ransomware (22 %). Anschließend folgen Spyware (8 %), (D)DoS (7 %), CEO-Fraud (7 %), manuelles Hacking (4 %) und Defacing (3 %).

Bei einem Viertel der Unternehmen waren durch den schwerwiegendsten Cyberangriff unterschiedliche digitale Daten betroffen, insofern diese gelöscht, manipuliert, gestohlen/kopiert oder verschlüsselt wurden, wobei die Verschlüsselung am häufigsten vorkam.

Kosten

Bei 70 % der betroffenen Unternehmen entstanden direkte Kosten infolge dieser schwerwiegendsten Angriffe, wobei dieser Anteil bei kleinen Unternehmen (10-49 Beschäftigte: 72 %) etwas höher lag als bei den großen (ab 500 Beschäftigte: 65 %). Bei kleineren Unternehmen entstanden vergleichsweise häufig Kosten durch externe Beratung und die Wiederherstellung und Wiederbeschaffung, da sie in der in der Regel weniger eigene IT- oder sogar IT-Sicherheitsabteilungen haben und daher häufiger die Unterstützung Dritter zu Rate ziehen mussten. Insgesamt wurden am häufigsten Kosten für Sofortmaßnahmen zur Abwehr und Aufklärung angeführt (40 %). Von Kosten durch Schadensersatz/Strafen (1 %) und abgeflossene Gelder (2 %) wurde hingegen relativ selten berichtet.

Haben wir die Kosten des letzten Angriffes ermittelt ?

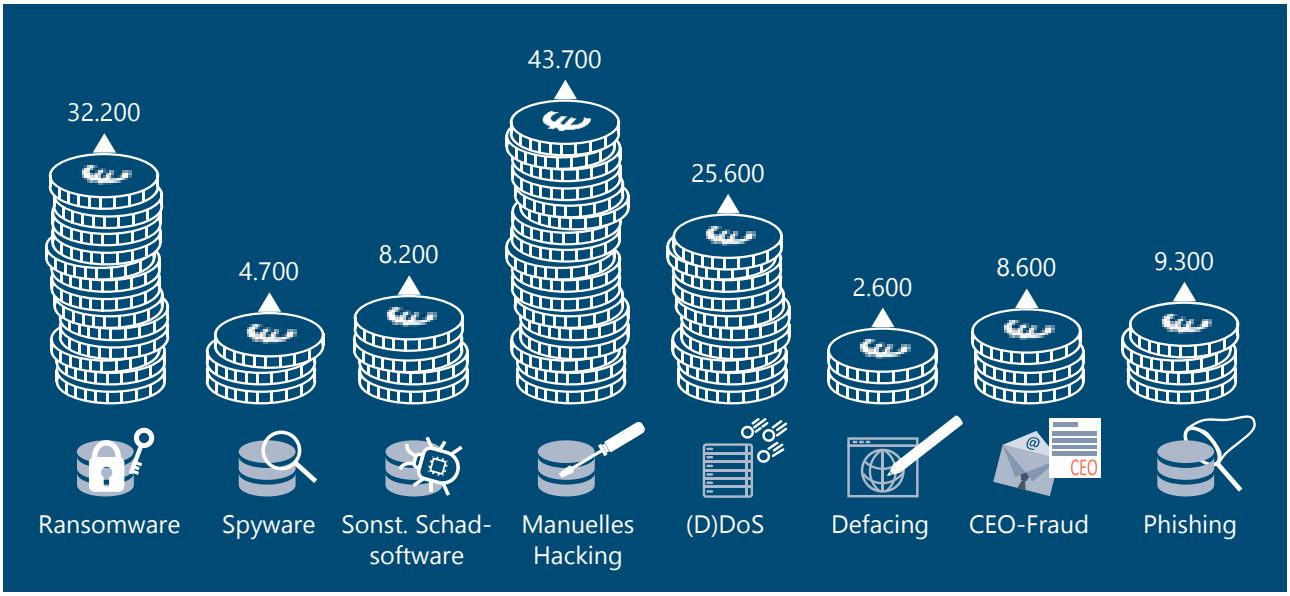
Die Höhe der direkten Gesamtkosten konnten bei 31 % der Unternehmen, bei denen Kosten entstanden sind, aufgrund fehlender Angaben nicht berechnet werden. Bezogen auf die übrigen Fälle reichten die unmittelbaren Gesamtkosten infolge der schwerwiegendsten Cyberangriffe bis 2 Mio. EUR. Im Durchschnitt wurden direkte Kosten von rund 16.900 EUR verursacht.

Mehr im Forschungs-Bericht

Allerdings lagen die berechneten Gesamtkosten bei über drei Viertel der Unternehmen (78,0 %) unter 5.000 EUR und nur sehr selten bei 50.000 EUR und mehr (3,4 %). Im Unternehmensgrößenvergleich fallen zumindest tendenzielle Unterschiede auf, insofern die durchschnittlichen direkten Gesamtkosten mit zunehmender Unternehmensgröße auf bis zu 31.200 Euro ansteigen. Zu den Angriffsarten, die die höchsten durchschnittlichen Kosten verursacht haben, zählen Ransomware-Angriffe, manuelles Hacking und (D)DoS-Angriffe (Abbildung 12).

zu beachten:
- Stichproben Zusammensetzung
- Schw. Vorfall der letzten 12 Monate
- nur direkte Kosten

Abbildung 12: Durchschnittliche direkte Kosten der schwerwiegendsten Cyberangriffe nach Angriffsart in €



Auch wenn die durchschnittlichen direkten Kosten erst einmal relativ gering erscheinen, darf nicht vergessen werden, dass diese

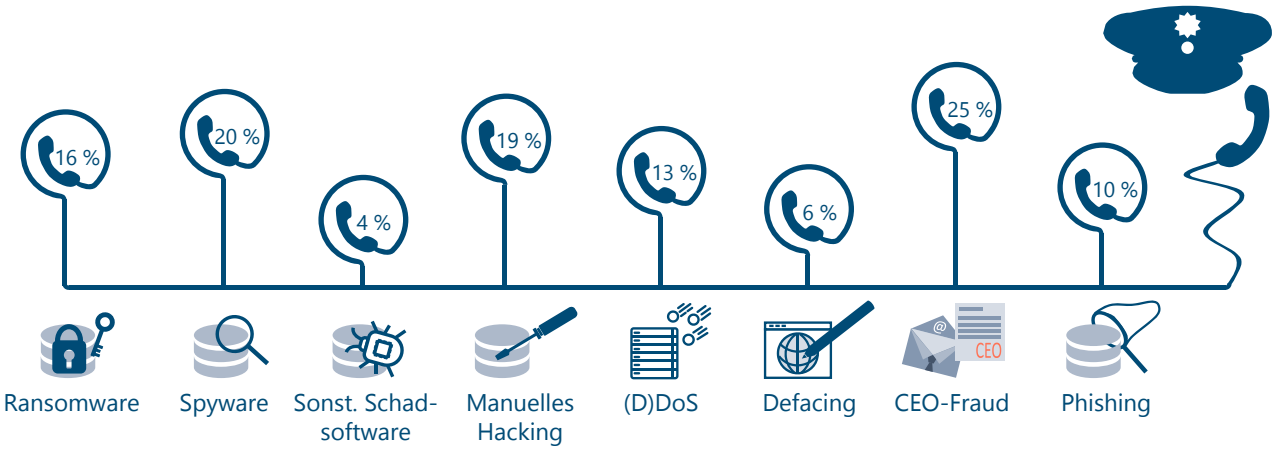
sich lediglich auf einen von möglicherweise mehreren Cyberangriffen im letzten Jahr beziehen. Daneben werden dabei auch Versuche mitumfasst, die vereitelt werden konnten und noch keine größeren Schäden verursacht haben. Mit Blick auf die höheren Werte der angegebenen Gesamtkosten können „erfolgreiche" Cyberangriffe gerade für kleine und mittlere Unternehmen ein bestandsgefährdendes Ausmaß annehmen. Hinzu kommt, dass mögliche indirekte Kosten, wie z.B. Umsatzverluste aufgrund von Imageschäden oder erfolgreicher Produktspionage, die noch Monate nach dem Cyberangriff anfallen können, hier unberücksichtigt bleiben.

Ergo:
Cyberangriffe bleiben ein Risiko, das durch geeignete Maßnahmen überwacht und reduziert werden muss

Anzeige

Lediglich 12 % der Unternehmen zeigten den berichteten schwerwiegendsten Cyberangriff polizeilich an, wobei größere Unternehmen (ab 500 Beschäftigte) mit 22 % häufiger Anzeige erstatteten als kleine Unternehmen (10-49 Beschäftigte) mit 11 %. Zu den am häufigsten angezeigten Angriffsarten zählen CEO-Fraud (25 %), Spyware (20 %) und manuelles Hacking (19 %; Abbildung 13). Demgegenüber wurden Angriffe mit sonstiger Schadsoftware und Defacing vergleichsweise selten angezeigt (4 % bzw. 6 %).

Abbildung 13: Quote der angezeigten schwerwiegendsten Cyberangriffe nach Angriffsart

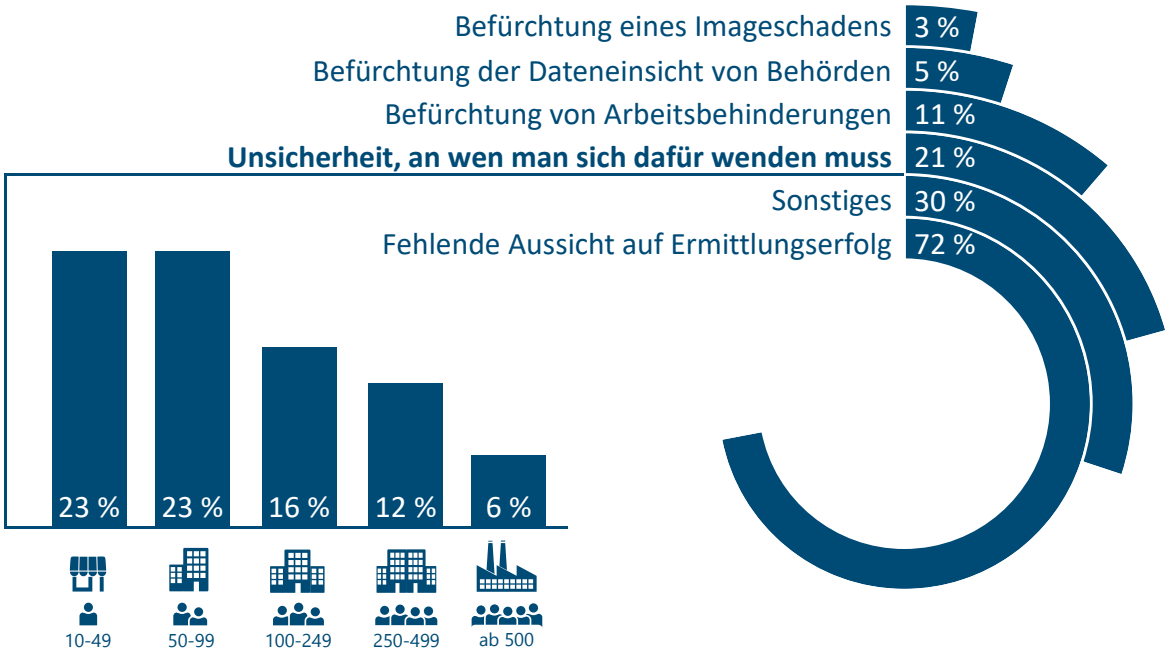


Die fehlende Aussicht auf einen Ermittlungserfolg wurde mit 72 % am häufigsten als Grund für die Nichtanzeige genannt (Abbildung 14). Über ein Fünftel (21 %) gab aber auch an, dass sie unsicher gewesen seien, an wen man sich dafür wenden muss.

Dieser Grund wurde deutlich häufiger von den kleinen Unternehmen angegeben, was eine mögliche Erklärung für deren geringere Anzeigequote ist. Dies weist auf einen Informationsbedarf hin und bietet einen Ansatzpunkt zur Erhöhung der Anzeigequote, indem die Zentralen Ansprechstellen Cybercrime (ZAC) der Polizei für Wirtschaftsunternehmen an den Landeskriminalämtern der Bundesländer weiter verstärkt bekannt gemacht werden.

Mehr Infos zu den ZACs unter polizei.de

Abbildung 14: Nichtanzeigegründe



Einschätzung zur polizeilichen Ermittlung

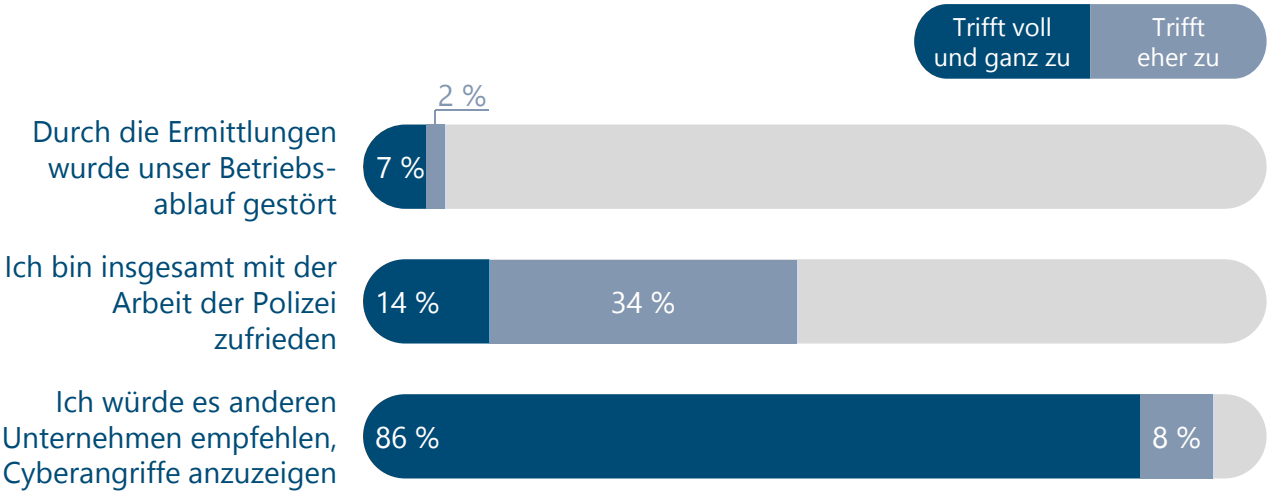
Wenn die befragten Unternehmen den schwerwiegendsten Cyberangriff der letzten zwölf Monate zur Anzeige gebracht haben, konnten lediglich in 8 % der Fälle Täter*innen ermittelt werden. Vor diesem Hintergrund ist es überraschend, dass trotzdem immerhin knapp die Hälfte (48 %) mit der Arbeit der Polizei insgesamt (eher) zufrieden ist und fast alle (94 %) die Anzeige von Cyberangriffen empfehlen würden (Abbildung 15).

Ziel der Anzeige dürfte bei diesen Unternehmen eben nicht nur die erfolgreiche Ermittlung sein, sondern möglicherweise auch die Erhöhung des gesellschaftlichen Problembewusstseins über zunehmende polizeilich registrieren Fallzahlen. Ein weiteres Ziel könnte in der Inanspruchnahme von Informations- und Beratungsmöglichkeiten der Polizei zum Schutz vor zukünftigen Cyberangriffen liegen.

Das stimmt! Wir sollten es nächstes Mal auch anzeigen

Dass die Ermittlungsarbeit der Polizei den Betriebsablauf gestört hätte, berichteten nur wenige Unternehmen (9 %). Damit kann entsprechenden Befürchtungen von bisher nicht anzeigenden Unternehmen entgegengetreten werden.

Abbildung 15: Einschätzung zur polizeilichen Ermittlung (nur Unternehmen die Anzeige erstatteten)



06

„Da technische Maßnahmen bereits weit verbreitet sind, geht es jetzt darum, sie noch besser in organisatorische Abläufe und Prozesse einzubinden und das Zusammenspiel von Mensch und Technik stärker in den Blick zu nehmen."

MÖGLICHE SCHUTZFAKTOREN

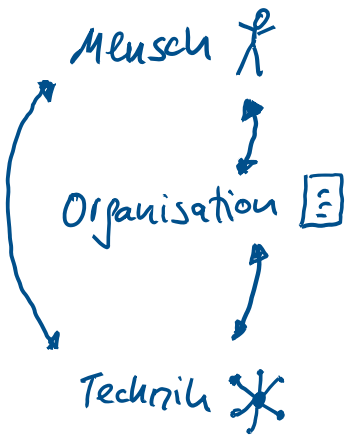
Um die Wirksamkeit von IT-Sicherheitsmaßnahmen zu testen, wurde das Vorhandensein verschiedener technischer und organisatorischer Sicherheitsmaßnahmen vor und nach dem schwerwiegendsten Cyberangriff in den letzten zwölf Monaten erfragt.

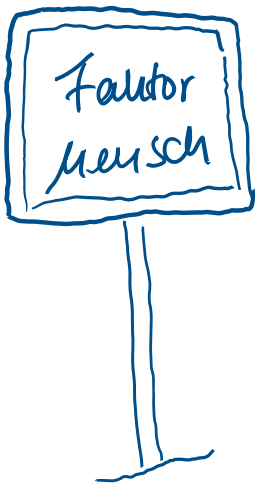
Technische IT-Sicherheitsmaßnahmen

Grundsätzlich lässt sich feststellen, dass viele technische Maßnahmen – z.B. regelmäßige Backups und deren physisch getrennte Aufbewahrung, aktuelle Antivirensoftware, regelmäßige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches sowie der Schutz der IT-Systeme mit einer Firewall – bei so gut wie allen Unternehmen vorhanden waren. Trotzdem waren viele dieser Unternehmen im letzten Jahr von mindestens einem Cyberangriff betroffen.

Hard- & Software allein kann das Problem also nicht lösen

Dieser Umstand weist darauf hin, dass die Wirkung technischer Maßnahmen mit weiteren Faktoren zusammenhängt. Neben der Qualität, dem Reifegrad sowie der sachgemäßen Konfiguration und Wartung der technischen Maßnahmen dürften dazu ebenso die Frage des Designs, der Nutzbarkeit und der Einbindung in organisatorische Abläufe und Prozesse zählen: Lassen sich z.B. die mit technischen Maßnahmen verbundenen Verhaltensregeln problemlos einhalten bzw. in die jeweilige Arbeitspraxis sinnvoll integrieren, ohne dass die eigentliche Arbeit darunter leidet? Oder führen sie sogar zu Missachtung und problematischen Ausweichhandlungen bei den Beschäftigten?



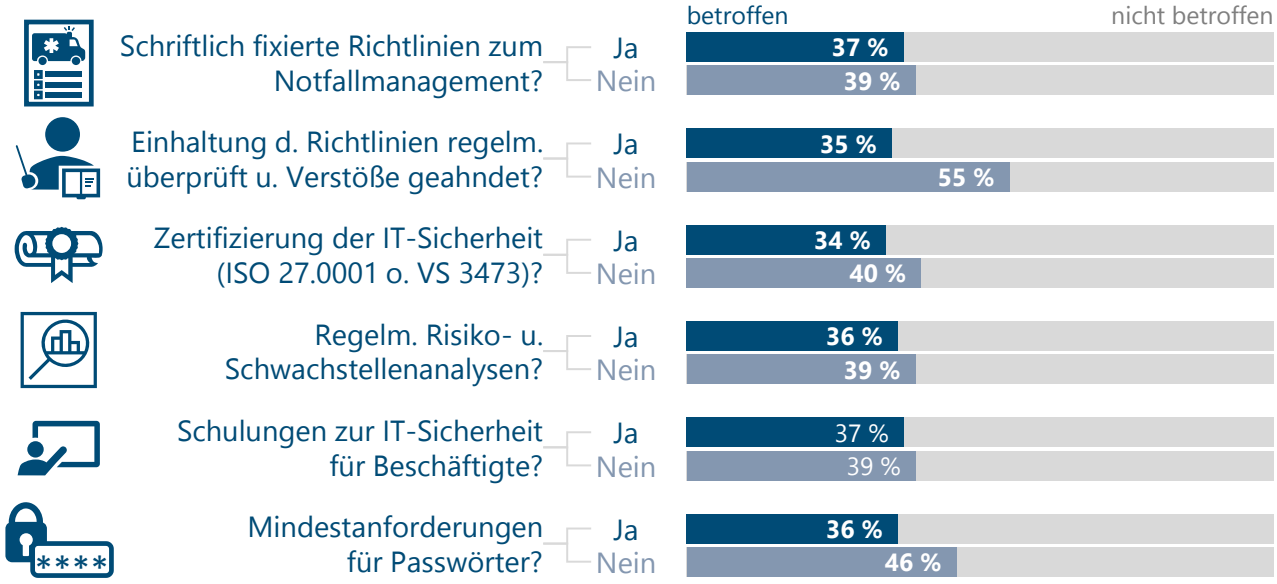


Organisatorische IT-Sicherheitsmaßnahmen

Organisatorische IT-Sicherheitsmaßnahmen waren demgegenüber weniger weit verbreitet, standen aber fast alle im Zusammenhang mit der Betroffenheit von Cyberangriffen. Insbesondere Unternehmen, die ihre Richtlinien zur IT-Sicherheit und zum Notfallmanagement regelmäßig überprüfen und Verstöße gegebenenfalls ahnden, waren signifikant seltener in den letzten zwölf Monaten von Cyberangriffen betroffen (35 %) als Unternehmen, die dies nicht taten (55 %; Abbildung 16).

Unternehmen, die Mindestanforderungen an Passwörter stellten, waren ebenfalls signifikant seltener betroffen. Etwas weniger deutlich aber immer noch statistisch bedeutsam sind entsprechende Unterschiede hinsichtlich schriftlich fixierter Richtlinien zum Notfallmanagement, der Zertifizierung der IT-Sicherheit sowie der regelmäßigen Risiko- und Schwachstellenanalyse.

Abbildung 16: Anteile von Cyberangriffen betroffener Unternehmen nach IT-Sicherheitsmaßnahmen

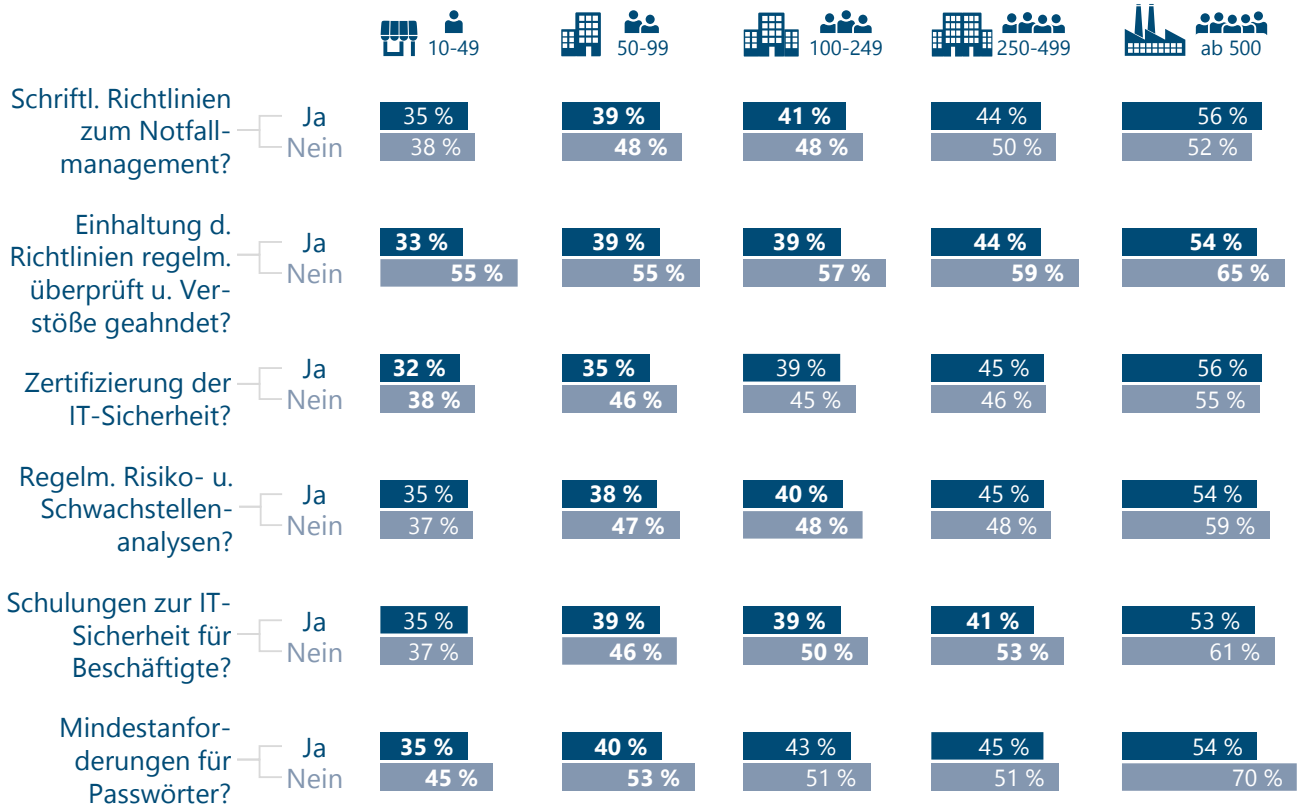


fett: statistisch bedeutsamer Unterschied

Der relativ große Unterschied zwischen Unternehmen, die ihre Richtlinien zur IT-Sicherheit und zum Notfallmanagement regelmäßig überprüfen und Verstöße gegebenenfalls ahnden, und

Unternehmen, die dies bislang nicht vorsahen, zeigt sich in sämtlichen Beschäftigtengrößenklassen und mit einem Unterschied von 22 Prozentpunkten am deutlichsten bei kleinen Unternehmen mit 10-49 Beschäftigten (Abbildung 17).

Abbildung 17: Anteile von Cyberangriffen betroffener Unternehmen nach IT-Sicherheitsmaßnahmen und Größe

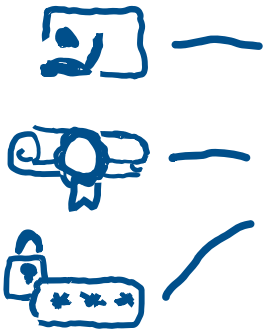


fett: statistisch bedeutsamer Unterschied

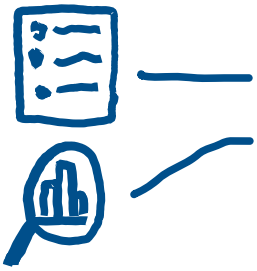
Die vergleichsweise großen Unterschiede dürfte damit zu tun haben, dass Richtlinien in der Regel verschiedene andere IT-Sicherheitsmaßnahmen voraussetzen und deren Wirkung damit indirekt mit umfassen. Es kommt also nicht nur darauf an, entsprechende Richtlinien und IT-Sicherheitsmaßnahmen zu haben, sondern diese auch innerhalb der Unternehmen „zu leben“. Neben der regelmäßigen Überprüfung der Einhaltung und der Ahndung etwaiger Verstöße dürften auch die Überprüfung der Aktualität und Umsetzbarkeit sowie die Förderung „richtiger“ Verhaltensweisen innerhalb der Unternehmen eine wichtige Rolle spielen.

Am Beispiel der Schulungen zur IT-Sicherheit für Beschäftigte ist zu erkennen, dass der Unterschied über alle Größenklassen hinweg zunächst eher klein ausfällt und auch statistisch gesehen nicht bedeutsam ist (Abbildung 16). Dieses Bild ändert sich bei der Betrachtung der einzelnen Größenklassen (Abbildung 17).

In der Gruppe der kleinen Unternehmen (10-49 Beschäftigte), die in der gewichteten Stichprobe am stärksten vertreten ist, findet sich weiterhin kein relevanter Unterschied in Hinblick auf Schulungen zur IT-Sicherheit, bei Unternehmen der anderen Größenklassen allerdings schon. Insbesondere mittlere Unternehmen, die ihre Beschäftigten zur IT-Sicherheit schulten, waren deutlich seltener von Cyberangriffen betroffen als die übrigen.



Zertifizierungen der IT-Sicherheit sowie Mindestanforderungen für Passwörter stehen demgegenüber eher bei den kleineren Unternehmen bis 99 Beschäftigte im Zusammenhang mit der Betroffenheit. Der hierbei erkennbare Unterschied bei großen Unternehmen (ab 500 Beschäftigte) ist statistisch nicht bedeutsam. Dies hat damit zu tun, dass die Gruppe großer Unternehmen, die keine Mindestanforderungen für Passwörter hat, sehr klein ist, was statistische Unsicherheiten mit sich bringt.



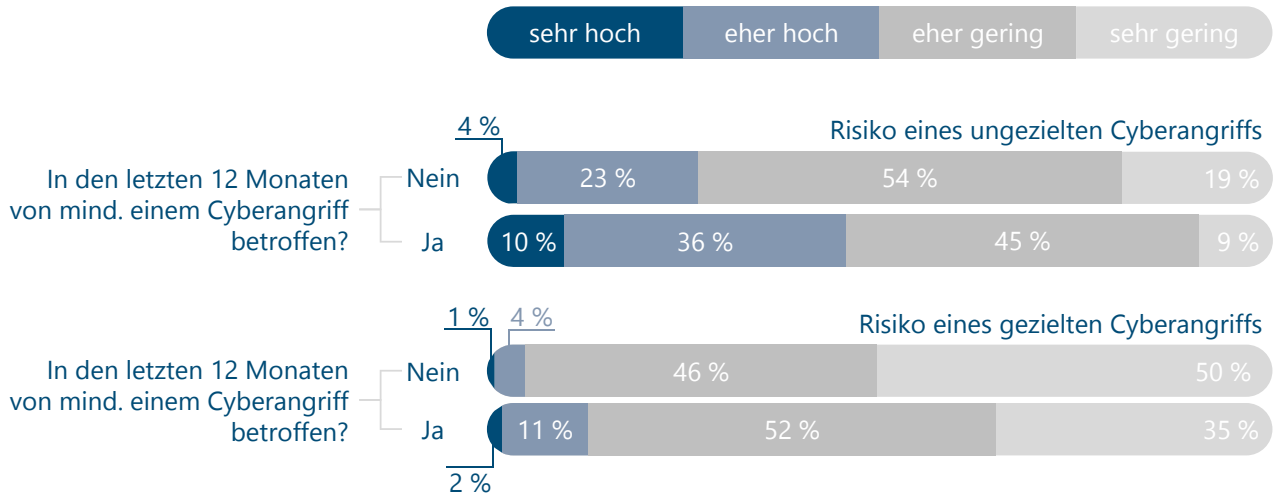
Schriftlich fixierte Richtlinien zum Notfallmanagement und regelmäßige Risiko- und Schwachstellenanalysen stehen mit einer Ausnahme in allen Größenklassen zumindest tendenziell im Zusammenhang mit einer niedrigeren Betroffenheit. Statistisch gesehen bedeutsam sind die Unterschiede in mittleren Unternehmen mit 50 bis 249 Beschäftigten. Der kleinere gegenläufige Unterschied bezüglich schriftlich fixierter Richtlinien bei großen Unternehmen (ab 500 Beschäftigten) könnte zufällig über die Stichprobenziehung zustanden gekommen sein, zumal die Gruppe großer Unternehmen, ohne derartige Richtlinien ebenfalls sehr klein ist.

Risikobewertung

Die IT-Sicherheit von Unternehmen hängt in vielerlei Hinsicht mit deren Risikoeinschätzung zu Cyberangriffen zusammen. Vor diesem Hintergrund wurde die Befragten gebeten, die Wahrscheinlichkeit, dass ihr Unternehmen in den nächsten zwölf Monaten durch einen (un)gezielten Cyberangriff geschädigt wird, einzuschätzen. Im Ergebnis wurde das Risiko eines gezielten Cyberangriffs deutlich geringer eingeschätzt als das eines ungezielten Angriffs, von dem auch viele andere Unternehmen betroffen werden.

Daneben ist aber auch erkennbar, dass Unternehmen, die in den letzten zwölf Monaten von Cyberangriffen betroffen waren, das Risiko bezogen auf gezielte und ungezielte Angriffe deutlich höher sehen (Abbildung 18).

Abbildung 18: Risikoeinschätzung für die nächsten 12 Monate



Diese Unterschiede finden sich ebenfalls in den einzelnen Unternehmensgrößenklassen. Zusammen mit dem Befund, dass die Hälfte der Unternehmen die Wahrscheinlichkeit schädigender Cyberangriffe eher/ sehr gering einschätzt, weist dies darauf hin, dass es sinnvoll ist, das Risikobewusstsein insbesondere von bisher noch nicht betroffenen kleinen und mittleren Unternehmen zu steigern.

07

„Es kommt nicht nur darauf an, verschiedene IT-Sicherheitmaß-nahmen zu haben, sondern diese auch innerhalb des Unter-nehmens zu leben.“

FAZIT

Cyberkriminalität stellt ein unternehmerisches Risiko dar, das nur schwer eingeschätzt, bewertet und gesteuert werden kann. Vor diesem Hintergrund wurde vom Kriminologischen Forschungsinstitut Niedersachsen e.V. (KFN) und dem L3S Forschungszentrum der Leibniz Universität Hannover das Forschungsprojekt „Cyberangriffe gegen Unternehmen" initiiert, um belastbare Erkenntnisse zur Verbreitung von Cyberangriffen gegen Unternehmen, den Folgen und möglichen Risiko- und Schutzfaktoren zu gewinnen. Gefördert wird dieses Projekt im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft" des Bundesministeriums für Wirtschaft und Energie sowie über eine Zusatzförderung von der Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers und der VHV-Stiftung.

Ein zentraler Bestandteil dieses Projektes ist eine umfangreiche deutschlandweite Unternehmensbefragung, die derzeit zu den größten und aussagekräftigsten Studien zum Thema Cyberangriffe gegen Unternehmen zählt und deren Ergebnisse in einem umfangreichen Forschungsbericht und dem vorliegenden Kurzbericht beschrieben werden.

Zu den zentralen Ergebnissen zählen folgende Befunde:

- **Viele Unternehmen sind von Cyberangriffen betroffen**
  Etwa zwei Fünftel der Unternehmen mussten in den letzten zwölf Monaten auf mindestens einen Cyberangriff reagieren. Aber nicht alle Unternehmen waren gleichermaßen betroffen.
- **Große Unternehmen sind häufiger betroffen als kleine**
  Dies zeigt sich vor allem bei Ransomware-Angriffen, CEO-

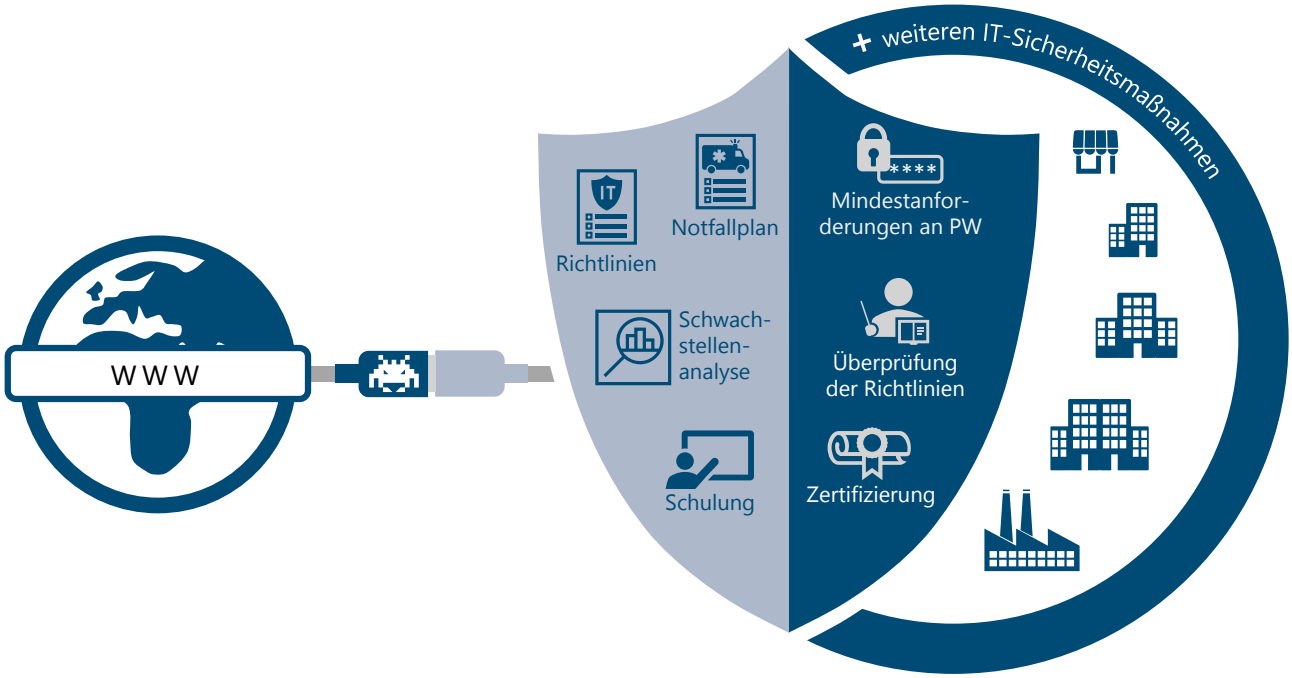
Fraud und Phishing, bei denen einzelne Beschäftigte von den Tätern*innen getäuscht werden (Social Engineering).

- **Die Unternehmensgröße allein ist nicht entscheidend**
  Wenn bestimmte Risikofaktoren wie z.B. mehrere Standorte im In- oder Ausland, Exporttätigkeit oder besondere Schutzgüter hinzutraten, dann lagen auch die Betroffenheitsraten kleiner und mittlerer Unternehmen deutlich höher und reichten zum Teil an das Niveau der großen Unternehmen heran. Das bedeutet, dass besonders kleine und mittlere Unternehmen, auf die diese Merkmale zutreffen, ein höheres Risiko haben und zusätzlicher Schutzmaßnahmen bedürfen.

- **Verursachte direkte Kosten sind sehr unterschiedlich**
  Die durchschnittlichen direkten Kosten der schwerwiegendsten Cyberangriffe erscheinen mit rund 16.900 Euro erst einmal relativ gering. Dabei darf nicht vergessen werden, dass sich diese Kosten lediglich auf einen Cyberangriff im letzten Jahr beziehen und auch Versuche mitumfasst sind, die vereitelt werden konnten. „Erfolgreiche" Cyberangriffe können gerade für kleine und mittlere Unternehmen bestandsgefährdende Kosten nach sich ziehen, worauf die große Spanne von bis zu 2 Mio. Euro hinweist.

- **Technik allein bietet keinen ausreichenden Schutz**
  Die meisten der erfragten technischen IT-Sicherheitsmaßnahmen wurden von fast allen Unternehmen aller Größenklassen eingesetzt. Trotzdem waren viele dieser Unternehmen im letzten Jahr von mindestens einem Cyberangriff betroffen. Dieser Umstand weist nicht auf deren Nutzlosigkeit hin, sondern auf weitere Faktoren, die mit deren Wirksamkeit zusammenhängen. Neben der Qualität, dem Reifegrad sowie der sachgemäßen Konfiguration und Wartung der technischen Maßnahmen dürften dazu ebenso die Frage des Designs und der Nutzbarkeit im Alltag der Beschäftigten zählen.

- **Organisatorische Maßnahmen machen einen Unterschied**
  Zum einen sind organisatorische IT-Sicherheitsmaßnahmen deutlich weniger weit verbreitet als technische. Zum anderen standen davon fast alle im Zusammenhang mit einer signifikant geringeren Betroffenheit. Zudem zeigt sich, dass es nicht nur darauf ankommt, verschiedene IT-Sicherheitsmaßnahmen zu haben, sondern diese auch innerhalb des Unternehmens „zu leben".



- **Anzeigeerstattung macht Sinn**
  Nur 12 % der betroffenen Unternehmen zeigten den schwerwiegendsten Cyberangriff der letzten 12 Monate an. Davon würden aber fast alle die Anzeige anderen betroffenen Unternehmen empfehlen. Denn neben möglichen Ermittlungserfolgen könnten höhere offizielle Fallzahlen das gesellschaftliche Problembewusstsein steigern. Die Zentralen Ansprechstellen Cybercrime für die Wirtschaft (ZAC) in den Landeskriminalämtern beraten und nehmen Anzeigen auf.

GLOSSAR

CEO-Fraud

Form des Betrugs (engl. fraud) durch Vortäuschung der Identität einer vorgesetzten Person z.B. aus der Geschäftsführung (engl. Chief Executive Officer, kurz CEO), um Beschäftigte per E-Mail so zu manipulieren, dass diese z.B. eine Geldüberweisung veranlassen

Defacing

Unbefugte Veränderung/ Verfälschung (engl. defacement) von Webseiten und deren Inhalten

Distributed Denial of Service (DDoS)

Mutwillige Überlastung von Web- oder E-Mail-Servern durch massenhafte Anfragen oder E-Mail-Sendungen, die zu deren Dienstverweigerung (engl. denial of service) führt und oft verteilt (engl. distributed) über mehrere zusammengeschaltete Rechner erfolgt

Phishing

Täuschung mit echt aussehenden E-Mails oder Webseiten, um z.B. Passwörter oder andere sensible Daten zu erlangen (engl. password harvesting/ fishing)

Ransomware

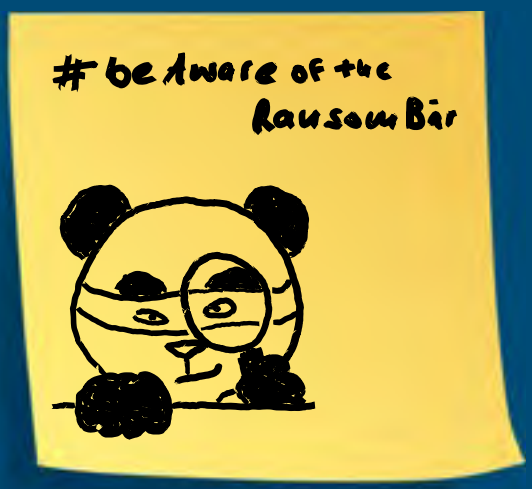
Schadsoftware, die Daten verschlüsselt, um z.B. ein Lösegeld (engl. ransom) für deren Entschlüsselung zu erpressen

Social Engineering

Sammelbezeichnung für verschiedene Formen der kommunikativen Beeinflussung von Personen, um diese zu bestimmten Handlungen zu verleiten, z.B. zur bereitwilligen Herausgabe von Passwörtern

Spyware

Schadsoftware zur Spionage (engl. spying), um unbemerkt Nutzeraktivitäten oder andere sensible Daten zu erlangen


#beaware of the
RansomBär