Datenklaustudie 2023

Virtuelle Gefahr – reale Schäden

Eine Befragung von über 500 deutschen Unternehmen zur aktuellen Lage

EY
Building a better working world

Inhalt

04 Vorwort

06 Kernaussagen der Studie im Überblick

07 Design der Studie

08 Kapitel 01
Einschätzung: Wie groß ist die Gefährdung – jetzt und in Zukunft?

- Neuer Höchststand: Risiko von Cyberangriffen ist aus Sicht der C-Suite groß wie nie
- Unternehmen aus Technologie, Medien und Telekommunikation sehen sich besonders gefährdet
- Niemand rechnet damit, dass die Gefahr geringer wird

14 Exkurs
Eingekaufte Cyberrisiken: Wie sich Investoren bei Übernahmen schützen

16 Kapitel 02
Spionagegefahr aus dem In- und Ausland

- Drei Tätergruppen besonders gefürchtet: organisiertes Verbrechen, Hacktivisten und ausländische Geheimdienste
- Russland mit neuem Rekordwert, China gleichbleibend: Beide gelten nach wie vor als größte Gefahrenherde

20 Interview
Heli Tiirmaa-Klaar, Director des Digital Society Institute an der ESMT Berlin

24 Kapitel 03
Konkrete Erfahrungen: Wer wurde Opfer? Wer sind die Täter?

- Hinweise auf Cyberangriffe sinken zwar – das Niveau bleibt dennoch hoch
- Mehr Homeoffice führt nicht zu deutlich mehr Cyberkriminalität
- Häufigstes Ziel von Cyberattacken: Finanzabteilungen
- IT-Abteilung als Aufklärer

34 Kapitel 04
Prävention: Schützen sich die Unternehmen ausreichend?

- Automotive und Pharma fühlen sich am wenigsten geschützt
- Firewall/VPN und Virenschutz werden zur Regel in der IT-Sicherheit
- Fast alle Arbeitsverträge enthalten Verpflichtungen zur Geheimhaltung
- Fast jedes zweite Unternehmen versichert sich gegen digitale Risiken

44 Kapitel 05
Reaktion auf Datenklau: Krisenpläne und Kommunikation

- Unternehmen bereiten sich immer besser auf den Krisenfall vor
- Die Branche Technologie, Medien und Telekommunikation probt den Ernstfall am häufigsten
- Mehr als die Hälfte aller Unternehmen hat kein etabliertes Krisenteam
- Kommunikation nach innen und außen: für jedes zweite Unternehmen bei Datenklau relevant

50 Exkurs
Kommunikation in der Krise: Jeder sollte vorbereitet sein

52 Fazit und Ausblick

54 Cyber Incident Response: passgenaue Lösungen im Kampf gegen Datenklau

56 Was wir für Ihr Unternehmen tun können

56 Ansprechpartner

Vorwort

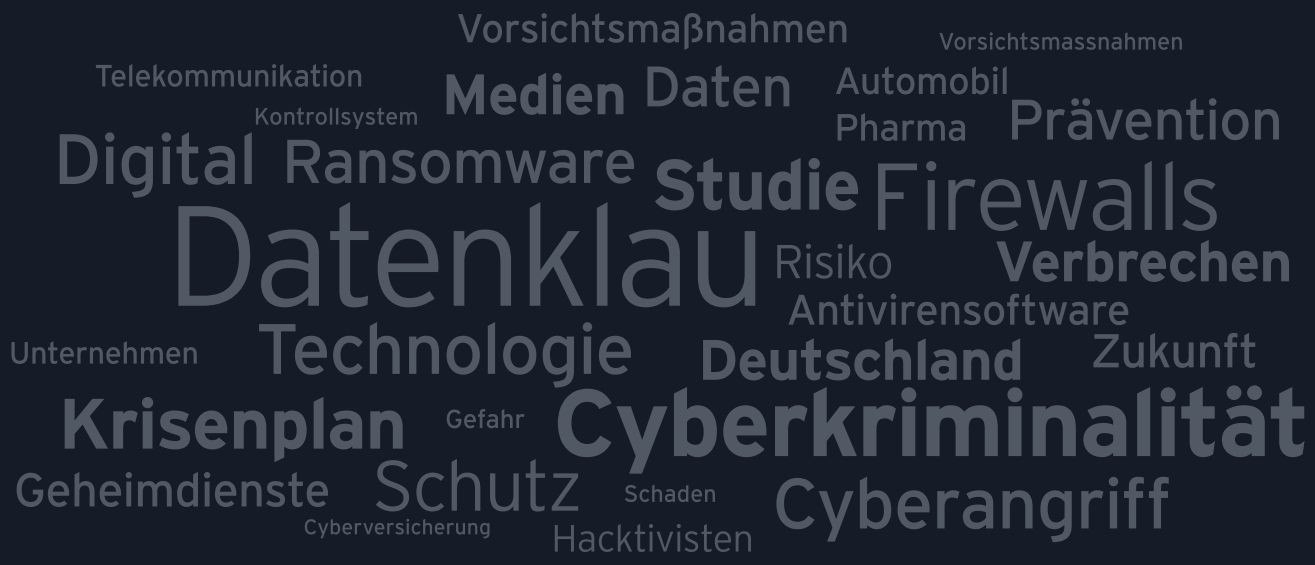
Bodo Meseke
Partner
Forensic & Integrity Services
EY Global Forensics Cyber Response Leader

Der forensische Technologieexperte kämpft weltweit gegen Wirtschaftskriminalität und Cyberattacken und hilft Kunden dabei, ihren Unternehmenswert und ihr geistiges Eigentum zu schützen. Bevor er zu EY kam, war er als Cybercrime-Ermittler für das Bundeskriminalamt tätig und gründete ein Unternehmen für digitale Forensik. Er leitet große IT-forensische Untersuchungen von Cybercrime oder Datenmissbrauch und bietet innovative IT-Forensik-Lösungen an. Darüber hinaus entwickelt er mit Kunden individuelle präventive IT-Forensik-Strategien und hilft, den Schaden bei Cyberangriffen zu begrenzen.

Thomas Koch
Partner
Forensic & Integrity Services
Digital Forensics & Incident Response (DFIR) Service Leader

Die Aufklärung von Cyberkriminalität ist das Hauptaufgabengebiet des zertifizierten Computerforensikers (GCFA) und IT Auditors (CISA). Seine langjährige Berufserfahrung hat der Informatiker schwerpunktmäßig in den Bereichen IT-Prüfung, Cybersicherheit und Digitalforensik gesammelt und dabei internationale Mandate von Kunden unterschiedlichster Größen, Industriezweige und Sektoren betreut. Er ist verantwortlich für den Bereich Digital Forensics & Incident Response (DFIR), und als direkter Ansprechpartner in Fällen von Cyberangriffen unterstützt er unsere Mandanten unmittelbar in den Bereichen Krisenmanagement, Analyse und Aufarbeitung von Datendiebstählen sowie Wiederherstellung des operativen Betriebs betroffener IT-Infrastrukturen.

> “
>
> Wie sich zeigt, hat das Bewusstsein für die Gefahren und Risiken durch Cyberangriffe und Datenklau erneut zugenommen. Und wer der Gefahr ins Auge blickt, kann auch Vorsichtsmaßnahmen treffen, um Ransomware-Attacken, Geschäftsunterbrechungen und andere Angriffe zu verhindern oder die Schäden zu minimieren.



Fast drei von vier Befragten sagen, das Gefährdungsrisiko für das eigene Unternehmen habe in den vergangenen beiden Jahren zugenommen. Alle Befragten rechnen damit, dass die Gefahr, Opfer von Cyberangriffen und Datenklau zu werden, in Zukunft zunehmen wird. Der Trend zur Cyberkriminalität, den wir mit dieser Studie seit 2011 dokumentieren, ist ungebrochen.

Darin liegt tatsächlich auch etwas Positives, denn vor allem im ersten Teil der Studie gehen wir den persönlichen Einschätzungen der Befragten auf den Grund. Wie sich zeigt, hat das Bewusstsein für die Gefahren und Risiken noch einmal zugenommen. Und wer der Gefahr ins Auge blickt, kann auch adäquate Vorsichtsmaßnahmen treffen.

Bei den Tätergruppen nimmt das organisierte Verbrechen erneut den Spitzenplatz ein, auch Hacktivisten und ausländische Geheimdienste spielen eine große Rolle. Dass die Täter vor allem in Russland und China vermutet werden, hat auch mit der aktuellen Weltlage und der medialen Berichterstattung zu tun. Denn Cyberkriminelle gibt es weltweit, beispielsweise agieren mittlerweile auch vom afrikanischen Kontinent aus einige maßgebliche Gruppen.

Fragt man die mit IT-Sicherheit betrauten Führungskräfte, gibt nur ein kleiner Teil konkrete Cyberangriffe auf das eigene Unternehmen zu: 37 Prozent der Befragten gaben an, bereits mindestens einmal digital attackiert worden zu sein. Ziel der Angreifer ist am häufigsten das Finanz- und Rechnungswesen: 42 Prozent der mit dem Thema vertrauten Führungskräfte gaben an, dass hier konkrete kriminelle Handlungen stattfanden. Dahinter folgen Angriffe auf Vertrieb (37 Prozent) und das Management (32 Prozent). Am häufigsten nutzten die Kriminellen hierbei die IT-Systeme direkt (53 Prozent) oder störten diese (25 Prozent).

Doch wie sieht es mit der Prävention aus? Zu den verstärkten Maßnahmen zählen die Klassiker wie Firewalls, VPN-Zugänge und Antivirensoftware. Weniger oft berücksichtigt werden die Multifaktor-Authentifizierung oder Zero-Trust-Umgebungen. Und obwohl die meisten entdeckten Angriffe vom internen Kontrollsystem erkannt wurden, und dabei meist vom Security Operations Center (SOC), hat ein solches nur ein Viertel der Unternehmen eingerichtet.

Das Bewusstsein für die Gefahr ist also vorhanden, aber die sich daraus ergebende Chance wird nicht in vollem Umfang genutzt. Deutlich mehr Führungskräfte als 2021 finden das eigene Unternehmen nicht ausreichend geschützt, insbesondere in der Automobil- und Pharmaindustrie sowie bei Technologie-, Medien- und Telekommunikationsunternehmen.

Möglicherweise ist so zu erklären, warum der Anteil der gegen Cyberrisiken Versicherten deutlich gestiegen ist. Mittlerweile hat fast jedes zweite Unternehmen eine solche Police. Ein Drittel derer, die noch keine haben, planen den Abschluss einer Cyberversicherung, die dann greift, wenn der Ernstfall eingetreten ist. Dazu passt, dass in deutlich mehr Unternehmen Krisenpläne vorhanden sind als noch vor zwei Jahren.

Die Zahlen der Studie, begleitet von Erläuterungen, Expertenmeinungen und Berichten aus der Praxis, finden Sie auf den nächsten Seiten.

Kernaussagen der Studie im Überblick

68%

... der befragten Führungskräfte
schätzen das Risiko für ihr Unternehmen, Opfer von Cyberangriffen/Datenklau zu werden, als sehr hoch oder hoch ein.

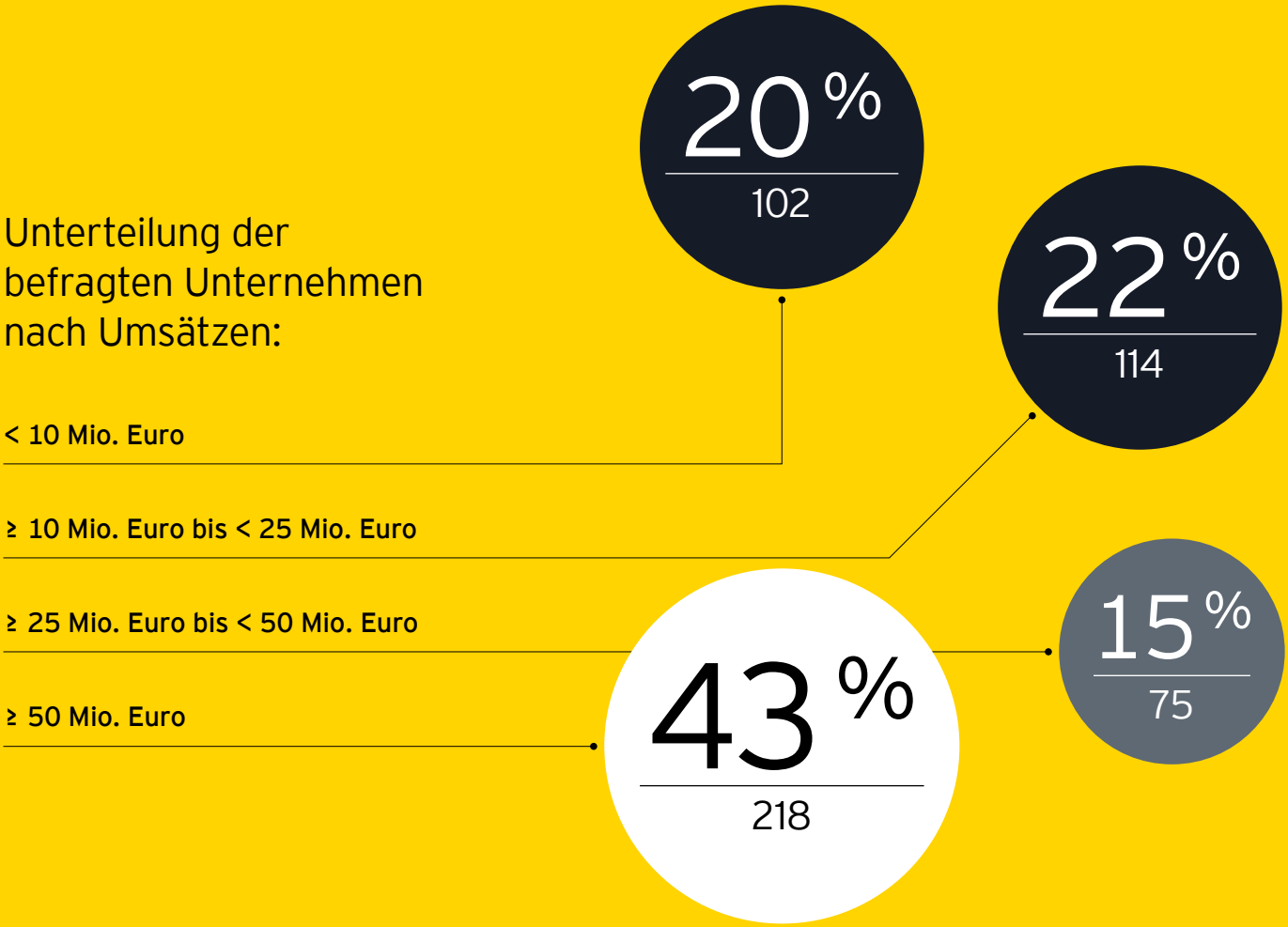
- Fast drei von vier Unternehmen sagen, das Risiko, Opfer von Cyberangriffen beziehungsweise Datenklau zu werden, sei in den vergangenen zwei Jahren gestiegen.
- Alle Unternehmen gehen davon aus, dass die Zahl der Cyberattacken weiter steigen wird, die Hälfte der Befragten erwartet sogar eine starke Verschärfung des Problems.
- Das organisierte Verbrechen wird als die bei Weitem gefährlichste Tätergruppe gesehen, an zweiter Stelle folgen die Hacktivisten. Ausländische Geheimdienste, Konkurrenten und Mitarbeitende spielen eine deutlich kleinere Rolle.
- Als die mit Abstand bedrohlichste Weltregion gilt jetzt Russland, das China als Zweitplatzierten in dieser Hinsicht überflügelt hat. Die Bedrohung aus den USA wird als deutlich geringer als noch 2021 wahrgenommen.
- Die flächendeckende Verbreitung des Arbeitens im Homeoffice hat erkennbar sicherheitsrelevante Auswirkungen. Immerhin stellen 16 Prozent der Unternehmen dadurch eine höhere Zahl von Cyberangriffen fest.
- Die mit Abstand meisten registrierten Attacken sind mit 53 Prozent Hackerangriffe auf die IT-Systeme. Das vorsätzliche Stören oder Lahmlegen der Geschäftstätigkeit oder der IT-Systeme wurde am zweithäufigsten beobachtet.
- Bei jedem dritten registrierten Cyberangriff wurden personenbezogene Daten entwendet, allerdings war nach Meinung der Befragten nur in einem knappen Viertel der Fälle eine Reaktion entsprechend der DSGVO nötig.
- Mit der Aufklärung der Angriffe wurde stärker als vor zwei Jahren die eigene IT-Abteilung beauftragt.
- Um ihre Sicherheit zu optimieren, investieren Unternehmen stark in Firewalls, VPN und Antivirensoftware. Weniger stark berücksichtigt werden Multifaktor-Authentifizierung, Zero-Trust-Umgebungen oder Information-Security-Management-Systeme.
- Deutlich gestiegen ist in den letzten zwei Jahren der Anteil der Unternehmen, die eine Cyberversicherung abgeschlossen haben: von 36 auf 46 Prozent. Jedes dritte nicht versicherte Unternehmen plant den Abschluss einer solchen Police.
- Krisenpläne haben sich deutlich stärker durchgesetzt als noch vor zwei Jahren. Mittlerweile verfügen 70 Prozent der Unternehmen darüber. Besonders stark ist dabei die Finanzbranche, gefolgt von der Automobilindustrie. Jedes zweite Unternehmen mit Krisenplan übt die Umsetzung mindestens einmal im Jahr.

Design der Studie

Für die vorliegende Studie wurden 509 Führungskräfte deutscher Unternehmen zum Thema Datenklau und Cybersecurity telefonisch befragt. Dazu zählen Geschäftsführerinnen und Geschäftsführer, Leiterinnen und Leiter Konzernsicherheit oder Leiterinnen und Leiter IT-Sicherheit.

Die Befragung wurde im März 2023 von dem unabhängigen Marktforschungsinstitut teleResearch GmbH, Ludwigshafen am Rhein, durchgeführt.

Unterteilung der befragten Unternehmen nach Umsätzen:



Die befragten Unternehmen lassen sich folgenden Branchen zuordnen:

71 Unternehmen
Pharma, Gesundheit und Chemie

63 Unternehmen
Finanzsektor

59 Unternehmen
Bau-, Immobilien- und Gastgewerbe

55 Unternehmen
Energie-/Metallverarbeitung

54 Unternehmen
Transport-/Logistikbranche

47 Unternehmen
Handel und Konsumgüter

47 Unternehmen
Technologie, Medien und Telekommunikation

40 Unternehmen
Automobilindustrie

40 Unternehmen
Sonstige Industrie
(vor allem Maschinenbau)

33 Unternehmen
Sonstiges

Einschätzung: Wie groß ist die Gefährdung – jetzt und in Zukunft?

1

1.1

Wie hoch schätzen Sie das Risiko für Ihr Unternehmen ein, Opfer von Cyberangriffen bzw. Datenklau zu werden?

Neuer Höchststand: Risiko von Cyberangriffen ist aus Sicht der C-Suite groß wie nie

Die Unternehmen fühlen sich klar zunehmend bedroht: 2021 erreichte die Einschätzung, dass das Risiko für Cyberangriffe und Datenklau „eher hoch" bis „sehr hoch" ist, bereits einen damaligen Höchststand von 63 Prozent. In diesem Jahr bewerten bereits 68 Prozent der befragten Manager das Risiko als hoch, Opfer von Cyberattacken zu werden. Besonders gestiegen ist dieser Wert seit 2017: Bis 2015 schätzte nur ein Drittel der Führungskräfte das Risiko als hoch ein. Parallel dazu ist der Anteil derer, die die Gefahr als „niedrig" einstufen, seit 2011 von 71 auf heute 32 Prozent stark gesunken.

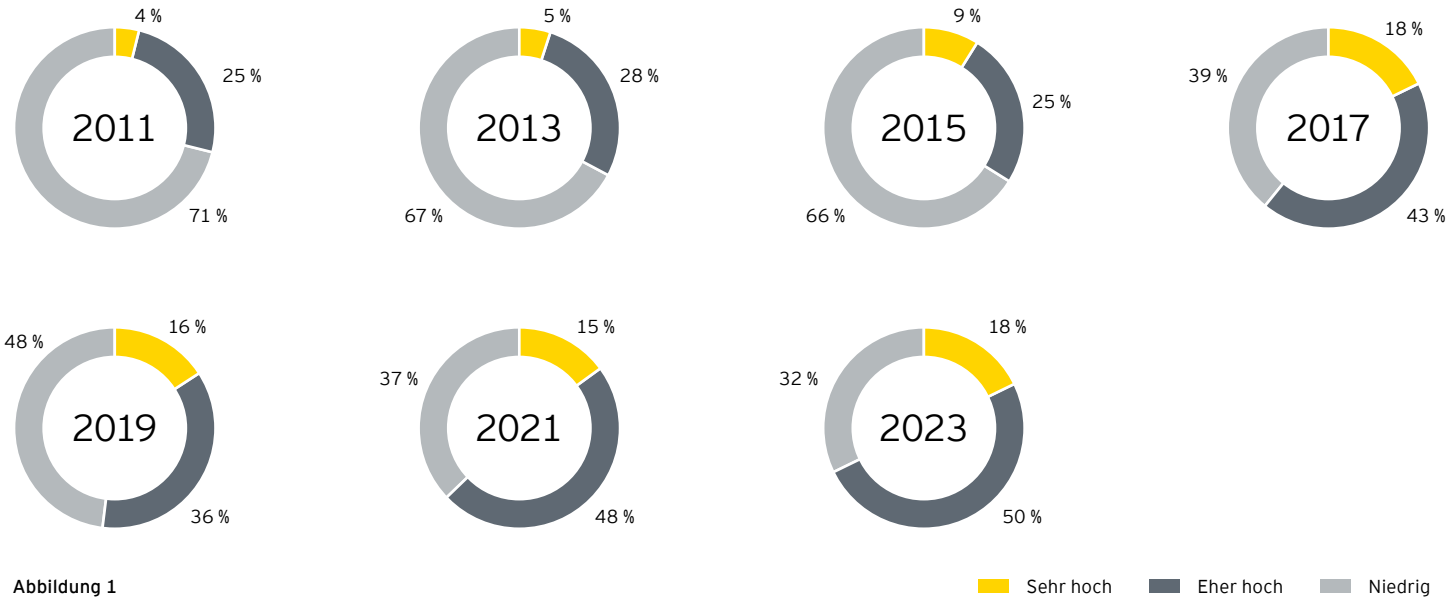


Abbildung 1

77 %

der Unternehmen mit digitalem Schwerpunkt in den Bereichen Technologie, Medien und Telekommunikation sehen sich am stärksten von Cyberangriffen und Datenklau bedroht.

Unternehmen aus Technologie, Medien und Telekommunikation sehen sich besonders gefährdet

Mit insgesamt 77 Prozent sehen sich Unternehmen mit digitalem Schwerpunkt in den Bereichen Technologie, Medien und Telekommunikation am stärksten von Cyberangriffen und Datenklau bedroht. Allerdings bleibt die Zahl derer, die davon das Risiko als „sehr hoch" einschätzen, im Vergleich zu 2021 konstant bei 26 Prozent. Vor zwei Jahren lag hier mit 69 Prozent der Sektor sonstige Industrie noch vorne, hier hat sich die Lage mit jetzt 65 Prozent offenbar etwas entspannt.

Auffällig gestiegen ist die gefühlte Bedrohungslage im Bereich Pharma/Gesundheit/Chemie von noch 69 Prozent im Jahr 2021 auf 75 Prozent in der aktuellen Untersuchung. Bei der Frage, wie sich das Problem Cyberangriffe künftig entwickeln wird, erreicht diese Branche mit 63 Prozent für „stark steigend" den höchsten Wert und zeigt sich damit als die am besorgteste. Gerade die in den letzten Jahren verbesserte IT-Sicherheitsinfrastruktur – bedingt durch den branchenspezifischen Sicherheitsstandard „B3S Pharma" – dürfte zu einer Sensibilisierung des Sektors für die tatsächliche Bedrohungslage geführt haben.

Von den befragten Unternehmensführungen sehen sich diejenigen mit mindestens 50 Millionen Euro Jahresumsatz beziehungsweise einem Jahresumsatz zwischen 25 und 50 Millionen Euro mit jeweils insgesamt 75 Prozent am stärksten der Gefahr von Cyberangriffen ausgesetzt. Unternehmen mit einem Jahresumsatz zwischen 10 und 25 Millionen Euro schätzen das Risiko mit 55 Prozent geringer ein.

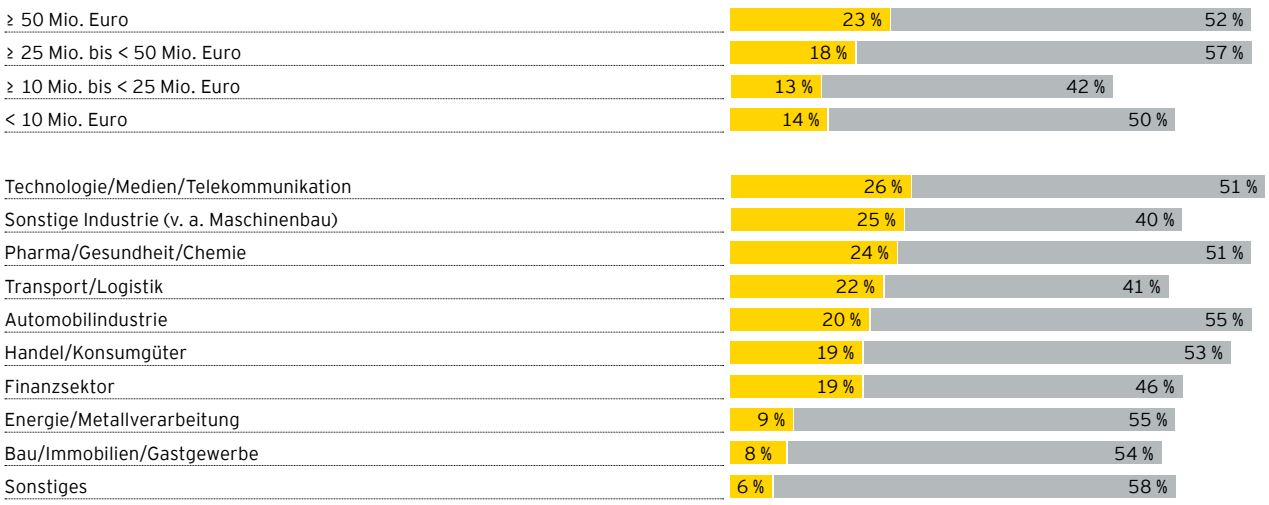


Abbildung 2

1.2

Hat das Risiko für Ihr Unternehmen, Opfer von Cyberangriffen/Datenklau zu werden, in den letzten zwei Jahren zugenommen?

Knapp drei Viertel sehen Anstieg des Risikos seit 2021

Überdeutlich zeichnet sich der Anstieg des Risikos von Cyberangriffen beziehungsweise Datenklau binnen der vergangenen zwei Jahre ab: 72 Prozent der Manager beobachten eine Zunahme der Gefährdung für ihr eigenes Unternehmen seit 2021, was mutmaßlich aus nachweisbaren Angriffsversuchen resultiert.

Analog dazu, dass sich Unternehmen aus dem Bereich Technologie, Medien und Telekommunikation insgesamt am stärksten bedroht fühlen, sehen auch vier von fünf Befragten ein gestiegenes Risiko innerhalb dieses Zeitraums. Damit nimmt dieser Sektor mit 83 Prozent hier die Spitzenposition ein. Knapp dahinter, mit 80 Prozent, liegen die Branchen Bau, Immobilien und Gastgewerbe.

Lediglich 18 Prozent der Führungskräfte sehen nicht, dass sich das Risiko eines Cyberangriffs seit 2021 verschärft hätte.

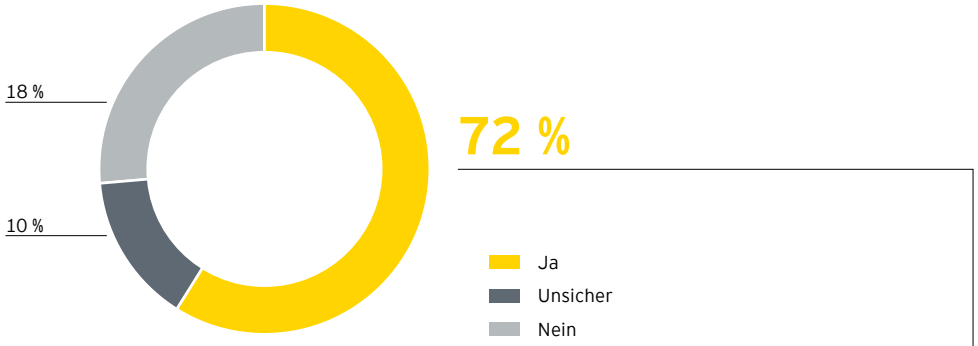


Abbildung 3

Anteil „Ja“ nach Branchen

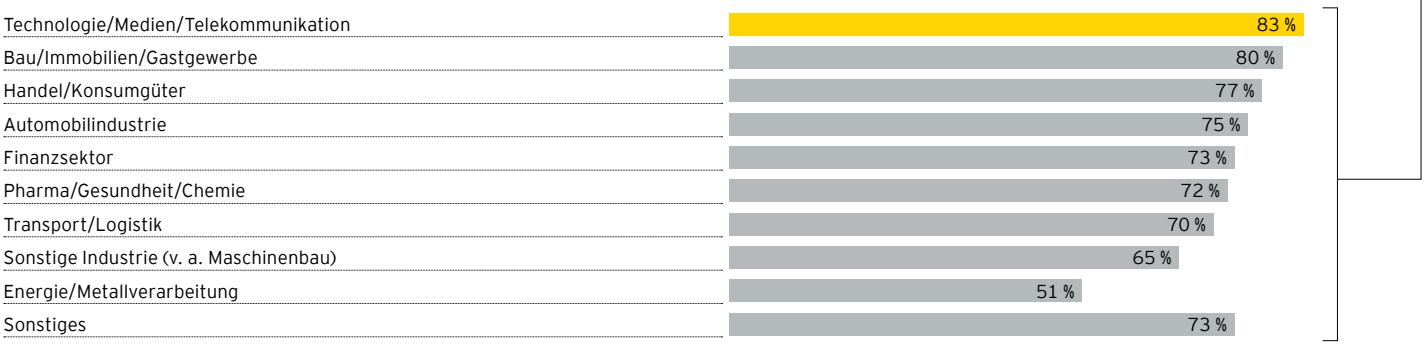


Abbildung 4

1.3

Wie wird sich die Bedeutung des Problems Cyberangriffe/Datenklau Ihrer Meinung nach künftig entwickeln?

Niemand rechnet damit, dass die Gefahr weniger wird

Nachdem fast drei Viertel der Befragten eine Zunahme des Risikos seit 2021 beobachten, scheint hier womöglich ein Scheitelpunkt erreicht zu sein. Denn es gehen wieder weniger Unternehmen davon aus, dass sich die Bedrohung noch weiter verschärft oder verschärfen kann: Mit 54 Prozent liegt die Zahl derer, die erwarten, dass die Bedeutung des Problems künftig weiter stark steigen wird, um 11 Prozentpunkte unter dem Wert von 2021. Wie bereits erwähnt befürchtet der Bereich Pharma, Gesundheit und Chemie am meisten eine stark steigende Tendenz der Bedrohung: 63 Prozent der Befragten aus diesen Branchen schließen sich dieser Auffassung an und lösen damit die sonstige Industrie (vor allem Maschinenbau) ab, die 2021 hier noch mit 72 Prozent votierte.

Mit jeweils 62 Prozent Zustimmung folgen Energie und Metallverarbeitung sowie Handel und Konsumgüter. Letztere erleben die Bedrohung ebenfalls deutlich intensiver: 2021 gingen nur 50 Prozent der Befragten aus dem Bereich Handel und Konsumgüter davon aus, dass das Problem Cyberangriffe und Datenklau stark steigen wird.

Überdurchschnittlich alarmiert zeigen sich insgesamt größere Unternehmen mit Jahresumsätzen mindestens 50 Millionen Euro.

Zum ersten Mal geht wiederum niemand mehr davon aus, dass die Thematik weniger relevant wird: Keiner der Befragten gibt inzwischen noch an, dass die Bedeutung leicht oder gar stark sinken wird. Das hebt die durchweg wahrgenommene Ernsthaftigkeit des Themas Cyberkriminalität hervor.

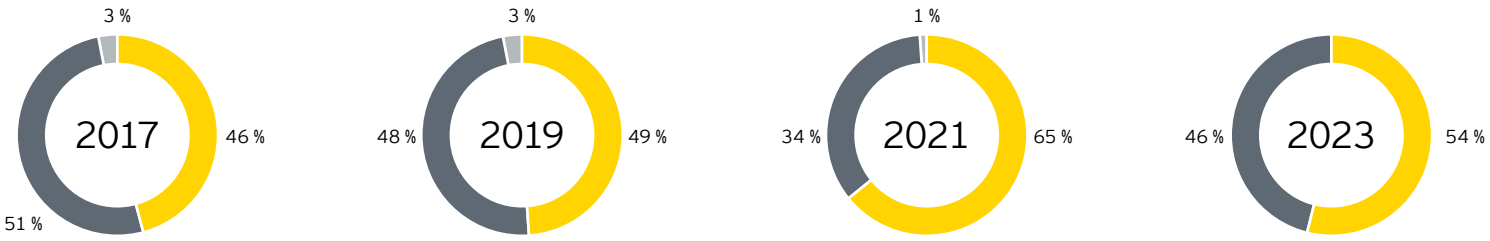
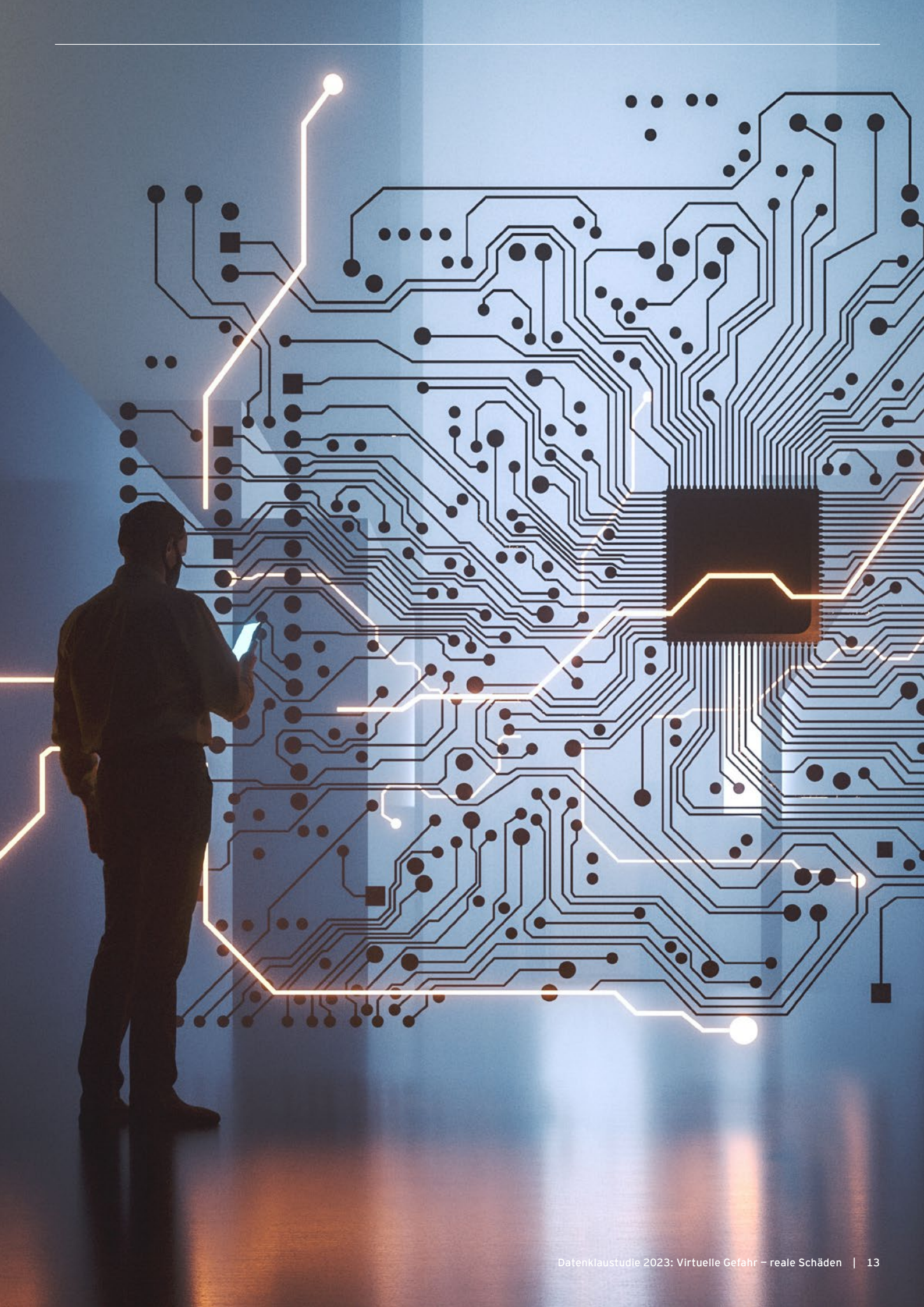


Abbildung 5



Eingekaufte Cyberrisiken: Wie sich Investoren bei Übernahmen schützen

Exkurs

Von Martin Hampel

Bei Firmenkäufen kann mangelnde Cybersecurity den Kaufpreis drücken oder sogar den Deal platzen lassen.

Cyberangriffe und Datenklau sind reale Bedrohungen für jedes Unternehmen. Verschlüsselte Daten, die nur gegen Lösegeld freigegeben werden, sensible Kundeninformationen im Darknet oder Wirtschaftsspionage: Angesichts der vielen öffentlich gewordenen Fälle in den letzten zwei Jahren halten circa 72 Prozent von EY im Rahmen der aktuellen Datenklaustudie befragten Führungskräfte Cyberattacken und Datendiebstahl für ein wachsendes Risiko für ihr Unternehmen.

Kein Wunder, dass Finanzinvestoren oder Firmen beim Kauf von Unternehmen oder Unternehmensteilen vermehrt darauf achten, wie es um deren Cybersicherheit bestellt ist. Bei solchen Übernahmen geht es um viel Geld. Schwächelt der Übernahmekandidat in Sachen Cybersecurity oder gibt es gar Sicherheitslücken, kann das zu einem Preisabschlag führen oder schlimmstenfalls den Verkauf platzen lassen.

Im Rahmen der Due Diligence versucht sich der potenzielle Käufer ein möglichst umfassendes Bild der Cybersecurity eines Übernahmekandidaten zu machen. Vorgaben, Firewalls, Tools und Prozesse werden überprüft, Verantwortliche interviewt. Am Ende entsteht eine Liste mit Risiken. Je länger diese Liste, desto lauter das Zähneknirschen beim Käufer.

Verkäufer versuchen häufig, Cyberrisiken im Kaufvertrag auf den Käufer abzuwälzen und keine Garantien und Gewährleistungen zu geben. Hat der Verkäufer eine gute Verhandlungsposition, weil es sich etwa um ein begehrtes Softwarehaus handelt, muss der Käufer die Risiken mehr oder weniger hinnehmen oder sich dagegen versichern, auch W&I-Versicherung (Warranty & Indemnity) genannt.

In der Praxis gehen strategische Investoren höchst unterschiedlich an die Due Diligence und die Integration von Unternehmen heran. Sind auf Käuferseite die Verantwortlichen für Cybersecurity und IT früh in die Übernahmeverhandlungen eingebunden, haben sie meist ein recht gutes Bild von der Sicherheitsarchitektur des Übernahmekandidaten und einen Fahrplan zur Integration. Investoren, die dem Thema vonseiten des Managements keine große Bedeutung zumessen oder es als isoliertes Problem der IT-Abteilung begreifen, kümmern sich meist erst später darum. Wenn sich eine bereits chronisch überlastete IT nun auch noch um die Systeme und die Sicherheit der neuen Gesellschaft kümmern muss, kann die Integration mitunter zu einem langjährigen Projekt werden. Hat auch der Übernahmekandidat Schwächen in der Security, können Sicherheitslücken über Jahre unerkannt bleiben, was Angreifer ausnutzen können.

Ein häufig unterschätzter Fakt: Unmittelbar nachdem eine Übernahme publik wird, ist die Gefahr professionell ausgeführter Cyberangriffe besonders hoch. Laut der Datenklaustudie sehen gut drei Viertel der befragten Unternehmen ein großes bis sehr großes Risiko, Opfer eines Cyberangriffs seitens des organisierten Verbrechens zu werden. Bei einer Übernahme steigt dieses Risiko zusätzlich. Die Logik der Angreifer ist simpel: Bei Unternehmenstransaktionen ist immer viel Geld im Spiel, ergo viel zu holen. Das gilt vor allem, wenn Finanzinvestoren im Spiel sind. Sie haben in den Augen der Cyberkriminellen besonders tiefe Taschen. Die gute Nachrichtenlage erleichtert den Angreifern die Recherche. Es gibt sogar Berichte von systematischen Attacken auf weitere Unternehmen im Portfolio von Finanzinvestoren, nach dem Motto: Wo eine Schwachstelle ist, sind auch weitere.

> Je länger die Liste der Cyberrisiken beim Übernahmekandidaten, desto lauter das Zähneknirschen beim Käufer.

Wollen Investoren Unternehmen abstoßen, wird im Vorfeld zudem gern der ein oder andere US-Dollar oder Euro gespart, auch bei der Cybersecurity, um den Gewinn zu steigern und so einen höheren Verkaufspreis zu erzielen. Aus der Beratungspraxis ist uns zumindest kein Finanzinvestor bekannt, der ein halbes Jahr vor einem geplanten Verkauf einer Firma ein neues Security-Team einstellt oder ein größeres Security-Projekt anstößt. Um die Cybersecurity eines Unternehmens ist es bei Eigentümerwechseln daher oft nicht zum Besten bestellt.

In der Praxis fordern potenzielle Käufer häufig einen sogenannten Penetration Test beim Übernahmekandidaten, bei dem alle Netzwerke, IT-Systeme, Onlineshops, Kundenportale oder das Onlinebanking auf Schwachstellen untersucht werden. So nachvollziehbar dieser Wunsch ist, so schwierig ist er bei einem Verfahren mit mehreren Bietern umzusetzen. Zudem müssten die Softwareentwickler oder IT-Mitarbeiter eingebunden werden, was je nach Umfang mehrere Wochen dauert und den Tagesbetrieb stört. Verkäufer sind daher wenig geneigt, potenziellen Käufern über lange Zeit exklusiven Zugang zu ihren Mitarbeitern und Systemen zu gewähren.

Was also tun, wenn der Übernahmekandidat zwar bei der Cybersecurity schwächelt, betriebswirtschaftlich aber eine lohnende Ergänzung wäre? Die gute Nachricht ist, dass sich viele Probleme auch nach dem Kauf lösen lassen. Dazu gehören zum Beispiel der Aufbau eines Cybersecurity-Teams oder der Abschluss einer Cyberversicherung. Außerdem können Notfallpläne entwickelt und bestehende – und bekannte – Sicherheitslücken etwa auf Kundenportalen geschlossen werden. Die schlechte Nachricht ist, dass all diese Dinge natürlich Geld kosten – und deshalb unbedingt eingeplant werden sollten.

Fazit

Angesichts der gestiegenen Bedrohungslage und der Höhe der möglichen Schäden achten Investoren beim Kauf von Firmen oder Unternehmensteilen vermehrt auf deren Cybersecurity. Zeigt der Übernahmekandidat hier Schwächen, kann das zu einem Preisabschlag führen, den Verkauf platzen lassen oder eine Versicherung erfordern. Investoren sollten sich also vor dem Kauf der Risiken bewusst sein. ■

Martin Hampel
Director Strategy & Transactions,
EY-Parthenon

Spionagegefahr aus dem In- und Ausland

2

2.1

Wie bewerten Sie das Risiko, von folgenden Tätergruppen geschädigt zu werden?

Drei Tätergruppen besonders gefürchtet

Drei Tätergruppen sind seit der letzten Umfrage 2021 deutlich stärker ins Bewusstsein der Führungskräfte gerückt: 73 Prozent bewerten das organisierte Verbrechen als großes oder sehr großes Risiko (+5 Prozentpunkte), 47 Prozent Hacktivisten wie Anonymous (+5 Prozentpunkte) und 36 Prozent ausländische Geheimdienste (+6 Prozentpunkte).

Weniger bedrohlich eingeschätzt werden Tätergruppen wie ausländische Konkurrenz, ehemalige Mitarbeitende oder konkurrierende inländische Unternehmen. In allen drei Kategorien ist ein leichter Rückgang im Vergleich zu 2021 zu beobachten.

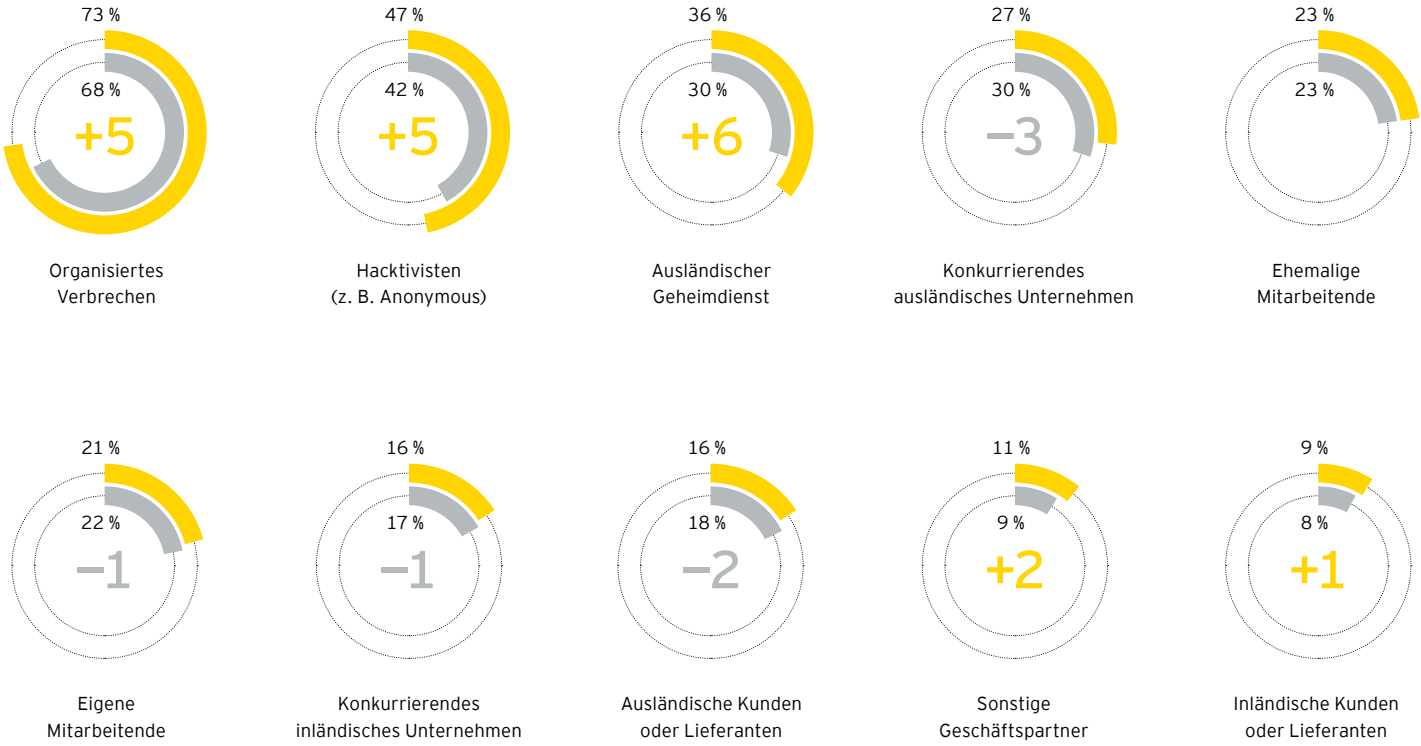


Abbildung 6

2021 2023

2.2

Gibt es Regionen, von denen aus Ihrer Sicht ein besonders hohes Gefährdungspotenzial hinsichtlich Cyberangriffen bzw. Datenklau ausgeht?

Russland mit neuem Rekordwert, China gleichbleibend: Beide gelten nach wie vor als größte Gefahrenherde

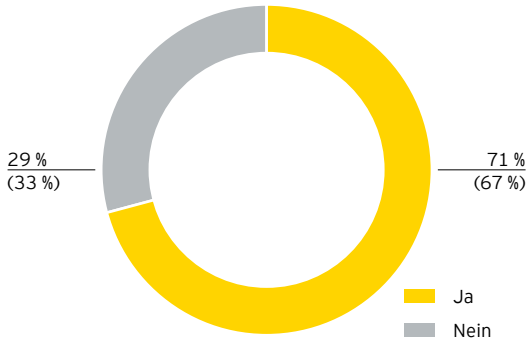


Abbildung 7 | Werte von 2021 in Klammern

Sieben von zehn Führungskräften halten bestimmte Regionen der Welt hinsichtlich drohender Cyberattacken für besonders gefährlich. Nach wie vor liegen hier Russland und China an der Spitze, Russland davon mit einem neuen Rekordwert: Mit jetzt 74 Prozent der Befragten, die das Land für besonders risikoreich halten, ist die Zahl im Vergleich zu 2021 um 18 Prozentpunkte gestiegen. Zahlenmäßig unverändert sehen 59 Prozent in China eine eklatante Bedrohung.

Mit deutlichem Abstand folgen Nordkorea (14 Prozent) und die USA (12 Prozent). Die Bedrohung aus dem Inland wird mit 2 Prozent weiterhin als sehr gering eingeschätzt.

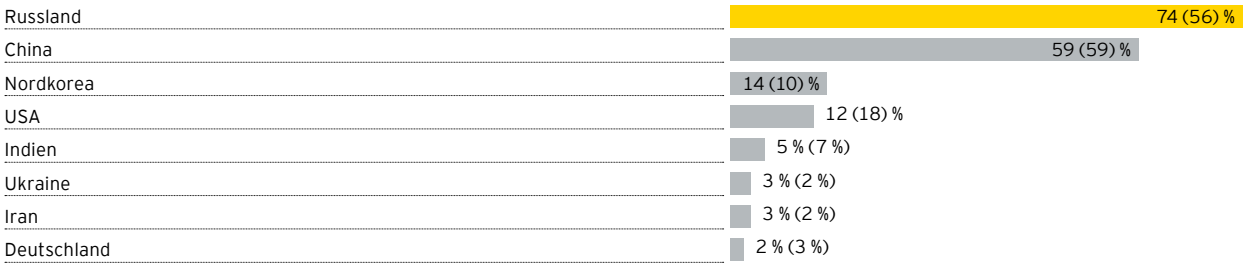


Abbildung 8 | Regionen mit hohem Gefährdungspotenzial | Werte von 2021 in Klammern | Mehrfachnennungen möglich

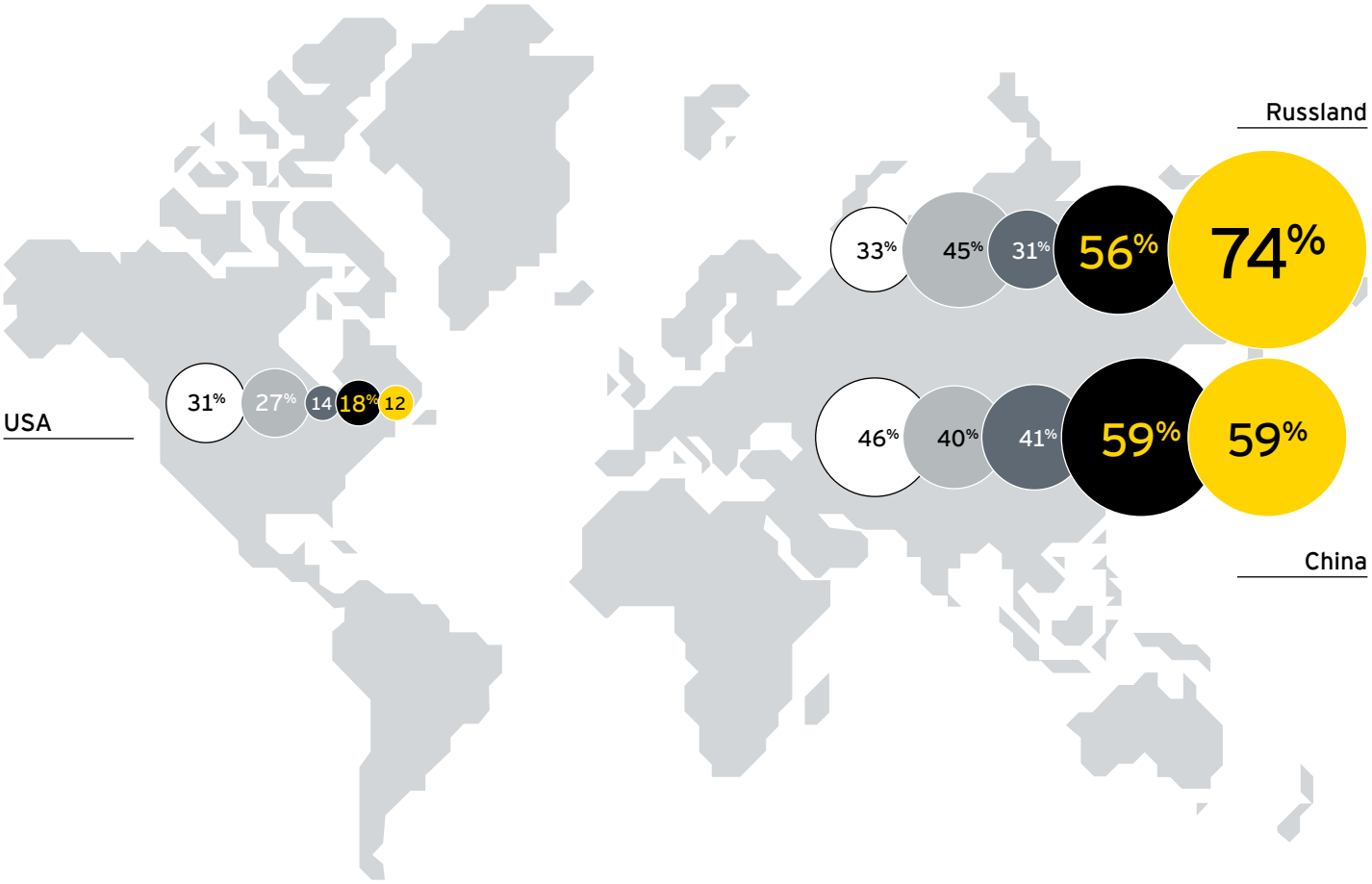


Abbildung 9 | Grundgesamtheit: Unternehmen, die eine Region nennen

2015 2017 2019 2021 2023

INTERVIEW

Heli Tiirmaa-Klaar

ist Direktorin des Digital Society Institute an der ESMT Berlin. Sie war Botschafterin für Cyberdiplomatie und Generaldirektorin der Abteilung für Cyberdiplomatie im estnischen Außenministerium und arbeitete in verschiedenen Funktionen in den Bereichen Cyberpolitik und Diplomatie im internationalen Bereich des NATO-Hauptquartiers, des European External Action Service und des estnischen Verteidigungsministeriums. Tiirmaa-Klaar ist zudem Autorin der Bücher „Botnets: How to Fight the Ever-Growing Threat on a Technical Level" und „Global and Regional Security Challenges: A Baltic Outlook" mit Tiago Marques.

Interview

Wir erleben eine Cybercrime-Pandemie und haben nur sehr wenige Ärzte

Egal ob UN-Sicherheitsrat, NATO-Hauptquartier, Europäische Union oder gleich mehrere Ministerien in ihrem Heimatland Estland: Heli Tiirmaa-Klaar hat weltweit an wichtigen Stellen zum Thema Cybersicherheit gearbeitet. Nun leitet sie das Digital Society Institute an der ESMT in Berlin mit dem Ziel, Privatsphäre, Vertrauen in die Digitalisierung und Bewahrung von Menschenrechten ins Zentrum der digitalen Transformation zu stellen. Sie analysiert die Ergebnisse der Datenklaustudie: Wie viel Angst sollten Organisationen vor den Herausforderungen durch Cyberverbrechen haben, worauf sollten sie sich vorbereiten und was ist von Gesetzgebern zu erwarten, die jetzt NIS2 implementieren?

Frau Tiirmaa-Klaar, unsere Umfrage zeigt, dass heute mehr Unternehmen als früher Cyberkriminalität als große Bedrohung wahrnehmen und dass sie organisierte Kriminalität, einschließlich professioneller Ransomware-Angriffe, als große Gefahr empfinden. Passt das zu Ihrer Berufserfahrung?

Es gibt definitiv eine anhaltende Bedrohung durch Ransomware, das ist nicht neu. Aber die kriminellen Unternehmungen haben definitiv aufgerüstet. Es gibt jetzt eine ganze Industrie um sie herum. Es gibt sogar kleinere Unternehmen, die Verhandlungen mit Kriminellen übernehmen, in manchen Fällen ist daran sogar die Polizei beteiligt. Grundsätzlich setzen die Angreifer ihre Methoden sehr effizient ein. Und sie profitieren davon, dass die Zusammenarbeit zwischen öffentlichen und privaten Stellen nicht immer reibungslos verläuft. Von zehn Fällen im Privatsektor werden neun nicht bei den Behörden gemeldet.

Wir brauchen in dieser Hinsicht mehr Zusammenarbeit, sowohl vor Ort auf lokaler Ebene als auch international. Der Informationsaustausch zwischen den verschiedenen Einheiten muss verbessert werden. Es gibt jetzt eine internationale Ransomware-Initiative, zu der Strafverfolgungsbehörden, Finanzministerien und auch Geldwäschebehörden gehören, weil die Kriminellen inzwischen häufig Bitcoin verwenden und sie sich das Geld irgendwo auszahlen lassen müssen. Es braucht generell einen Rahmen und ein Vorgehen für die Zusammenarbeit, wie dieses gute Beispiel ihn geschaffen hat.

Breiter diskutiert werden inzwischen auch Angriffe im Auftrag von Regierungen. Wie reagieren andere Staaten auf gegnerische Länder?

Wir sehen die Auswirkungen des russischen Krieges in der Ukraine auch im Cyberspace, wo bestimmte Länder und Branchen einer großen Anzahl von Angriffen ausgesetzt sind. Solche Attacken werden von manchen Staaten toleriert oder stehen unter dem Schutz feindlicher Regierungen.

Generell sind die meisten europäischen Nationen ständigen Angriffen aus dem Ausland ausgesetzt. Meistens kommt das nicht in den Nachrichten vor, weil unsere Cyberresilienz gut ist und wir uns selbst schützen können, aber auch weil nicht darüber berichtet wird.

Einige Umfrageergebnisse wirken widersprüchlich: Einerseits scheint es mehr Präventionsarbeit und mehr interne Prozesse zu geben, um mit Cyberangriffen umzugehen, andererseits berichten viele Teilnehmer auch von einem höheren Maß an wahrgenommenen Bedrohungen. Insgesamt fühlt es sich an, als gelinge nur ein sehr langsamer Fortschritt. Sie verfügen über großes Fachwissen auf diesem Gebiet: Stimmen Sie zu, dass wir keine geeigneten Schritte zum Umgang mit den Bedrohungen gehen?

Während meiner Karriere in der Cyberbranche haben sich die Dinge zum Besseren gewendet, aber ich glaube, wir sind noch nicht am Ziel. Unsere Reaktionen sind ein bisschen holprig und es gibt viele Gründe, warum wir uns in dieser Lage befinden: Digitale Ökosysteme sind sehr komplex, besonders in großen Unternehmen, die umfangreiche Altsysteme unterhalten, die schwer zu schützen sind. In dem Moment, in dem wir ein Problem beheben, tauchen mehrere andere auf, jetzt kommen Quantum-Technologie und KI ins Spiel, was auch wiederum den Guten, aber eben auch den Bösen helfen wird. Diese Technologien sind Maschinen, die einfach Wünsche ihrer Meister erfüllen.

Als langjährige Mitarbeiterin im staatlichen Dienst würde ich sagen, dass Schritte unternommen wurden, aber es ist sehr schwierig, sie vor Ort konkret umzusetzen. Wir erleben eine Cybercrime-Pandemie und haben nur sehr wenige Ärzte. Es gibt sehr wenige Experten und gleichzeitig ist es schwer zu definieren, wer überhaupt Experte ist, weil das Thema breit verstanden werden muss. In vielen Vorstandsetagen will die Führungsebene nicht über Cybersecurity diskutieren und dann erlebt man einen Einschüchterungseffekt im Management.

Gleichzeitig gilt Ihr Heimatland Estland oft als Vorreiter in Sachen Digitalisierung in der Zivilgesellschaft. Von welchen Erfolgsfaktoren könnten Ihrer Meinung nach andere Länder lernen?

Estland ist ein gutes Beispiel für Regierungsarbeit in diesem Bereich. Es ist ein Land, in dem das Cyberbewusstsein in den höheren Führungspositionen sehr ausgeprägt ist, weil es lange schon Tradition ist, Cyberbedrohungen ernst zu nehmen. In Estland können Sie beispielsweise Staatssekretäre treffen, die leidenschaftlich über die Notwendigkeit dis-

kutieren, Software ständig zu patchen, um Sicherheitslücken im Internet zu vermeiden. Beamte in Estland müssen sich zu digitalen Themen weiterbilden, denn das gesamte E-Government dort hängt von Cybersicherheit ab.

Auf internationaler Ebene haben wir aber ein Vertrauensproblem in Sachen Digitalisierung, weil wir in letzter Zeit so viele Probleme gesehen haben. Das wirft die Frage auf, wie wir Vertrauen in Digitalisierung messen und wie wir es steigern. Viele Offizielle glauben, dass es bei Vertrauen nur um Technologie und den Schutz vor Bedrohungen geht. Aber eine weitere Lehre aus Estland ist auch, dass die Regierung vor allem einige Dinge angestoßen hat. Das wurde dann zu einem Ökosystem, das sich selbst weiter aufbaute und von unten nach oben selbst regulierte. Digitalisierung kann man nicht von oben nach unten anordnen. Sie müssen den Menschen beibringen, wie sie es von unten nach oben aufbauen. Das schafft Vertrauen.

Eine Sache, die eine Regierung tun kann, ist, zuverlässig funktionierende Maßnahmen zu etablieren, um Vertrauen zu schaffen oder zu stärken. In Estland geschah das mit dem landesweiten digitalen elektronischen Personalausweis, den wir seit 20 Jahren haben. Es gibt keine persönlichen Informationen auf dieser Karte, aber mit einer Reihe von Nummern und dieser Karte authentifizieren sie Dienste, sogar zur Stimmabgabe bei Wahlen. Es hat einige Zeit gedauert, bis die Menschen dem vertraut haben, es gab auch Unterschiede zwischen den Generationen. Aber wir sehen inzwischen viele Senioren, die es nutzen, und Menschen aus allen Bildungsstufen. Es wurde zu einer Fähigkeit, die die Menschen gelernt haben und der sie nun vertrauen, weil sie sich bewährt hat.

Auf europäischer Ebene verpflichtet die zweite Richtlinie zur Netzwerk- und Informationssicherheit (NIS2) deutlich mehr Unternehmen zur Umsetzung von Cybersicherheitsmaßnahmen. Was sind für Sie besonders wichtige Änderungen für den deutschen Markt, die sich beim Übertragen in nationales Recht abzeichnen?

NIS2 muss als Richtlinie, im Gegensatz zu einer Verordnung, durch die Mitgliedsstaaten erst noch in nationales Recht umgesetzt werden.

Die gute Nachricht in Bezug auf Deutschland ist, dass es bereits einige Vorschriften und Gesetze zur Cybersicherheit gibt. Das deutsche IT-Sicherheitsrecht ist kein komplett unbeschriebenes Blatt, auch wenn viele Vorschriften sektorspezifisch sind und sich vor allem die Situation auf Landesebene – je nach Perspektive – als eine Mischung aus Dschungel und Flickenteppich beschreiben lässt.

Es gibt demnach bereits Vorgaben in unterschiedlicher Detailtiefe. Wir sehen folglich schon jetzt ein komplexes Regulierungsumfeld, das durch die Ausweitung der betroffenen Unternehmen durch NIS2, die in den Geltungsbereich von Cybersicherheitsverpflichtungen fallen, noch einmal an Komplexität gewinnt.

Das bedeutet aber auch, dass wir eine riesige Anzahl Experten benötigen. Unsere Umfrage hat aber auch gezeigt, dass in der akuten Phase nach einem Cyberangriff die unternehmenseigenen IT-Abteilungen häufiger als früher mit der Aufbereitung der Ergebnisse beauftragt werden. Externe Experten werden nun etwas weniger hinzugezogen, sodass am Ende noch mehr Fachkräfte gebraucht werden. Woher sollen die alle kommen?

Wir sehen definitiv, dass das erhöhte Bewusstsein zu einem größeren Bedarf an Experten führt. Gleichzeitig ist der Arbeitsmarkt für Cybersicherheit sehr teuer, weil es so wenig Fachleute gibt. Viele Unternehmen können sich diese in Zukunft möglicherweise nicht mehr leisten. Das kann dazu führen, dass Firmen nur die Kästchen in ihren Compliance-Frameworks abhaken, ohne intern die notwendigen Hausaufgaben zu erledigen.

Unsere öffentlichen Bildungssysteme sind nicht sehr schnell. Sie brauchen Zeit, um sich anzupassen, und es gibt generell ein geringes Interesse an MINT-Fächern. Mathematik, Informatik und Technik sind Themen, die in der Öffentlichkeit nicht sehr beliebt sind. In Deutschland hilft zwar das System der Fachhochschulen, aber die Volkswirtschaft ist auch sehr groß und benötigt viele Fachleute. Bildung ist zudem ein nationales Thema, das nicht von der EU gelenkt wird. Nicht alle Länder setzen so stark darauf wie Deutschland. Am Ende müssen 27 EU-Staaten ihre Hausaufgaben machen.

Am Ende gibt aber die Debatte über die Auswirkungen von NIS2 auch Hinweise darauf, was als Nächstes zu tun ist. Was halten Sie für wichtig?

Die EU-Staaten sollen nun jenen Unternehmen helfen, die zur Umsetzung von NIS2 verpflichtet sind. Die Auswirkungen werden von Land zu Land unterschiedlich sein. In Deutschland sollte zum Beispiel auf Länderebene mehr Bewusstsein für das Thema geschaffen werden und die Bundesländer sollten der Umsetzung von Cybersicherheitsthemen noch mehr Aufmerksamkeit schenken. Sie könnten ihre Bildungssysteme stärker darauf ausrichten, mehr Fachkräfte hervorzubringen. Länder, die bereits gut aufgestellt sind, sollten weiterhin daran arbeiten, die Zahl von Akteuren, die sich der gesellschaftlichen Auswirkungen von Cybersicherheit bewusst sind, noch weiter zu erhöhen.

Es ist wichtig, dass insbesondere Deutschland die Bedeutung von NIS2 erkennt, weil die Richtlinie Nationen mit vielen mittelständischen Unternehmen stärker treffen wird. In einigen südeuropäischen Ländern gibt es mehr landwirtschaftliche und weniger mittelständische Firmen. Mit der Stärke des deutschen Mittelstandes ist auch NIS2 ein größeres Thema. ■

Konkrete Erfahrungen: Wer wurde Opfer? Wer sind die Täter?

3

3.1

Gab es in Ihrem Unternehmen bereits konkrete Hinweise auf Cyberangriffe beziehungsweise Datenklau innerhalb der vergangenen zwei Jahre?

Die Hinweise auf Cyberangriffe beziehungsweise Datenklau sind in den vergangenen zwei Jahren weniger geworden. Das ist an sich eine gute Nachricht, sofern sie bedeutet, dass die Attacken wirklich abnehmen oder Unternehmen die Bedrohung besser im Griff haben und sich besser schützen. Sollten die Attacken nicht weniger, aber dafür unbemerkbarer erfolgen, wäre das Ergebnis weniger Anlass zur Freude.

Hinweise auf Cyberangriffe sinken zwar – das Niveau bleibt dennoch hoch

Immerhin: Die Zahl derer, die mindestens einmal oder sogar mehrfach Hinweise auf Spionageattacken erhielten, lag 2019 bei 40 und 2021 bei 44 Prozent und ist nun erstmals auf 37 Prozent gesunken. Damit hat immer noch jedes dritte Unternehmen seit 2021 Spuren von Cyberattacken verfolgt, jedes fünfte sogar öfter als einmal. Trotz des Rückgangs bleibt das Niveau also relativ hoch.

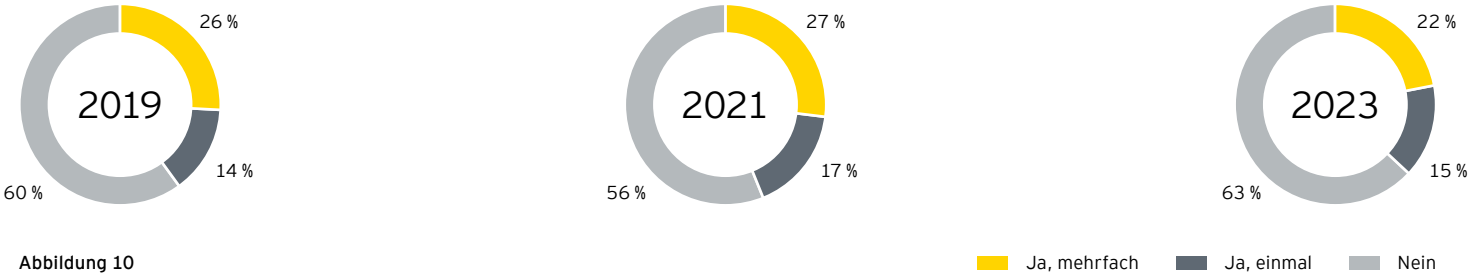


Abbildung 10

Unternehmen aus Technologie, Medien und Telekommunikation stellen die meisten Hinweise auf Cyberattacken fest

Mit 48 Prozent liegen Unternehmen mit den Geschäftsfeldern Technologie, Medien und Telekommunikation an der Spitze hinsichtlich einmaliger oder sogar mehrfacher konkreter Hinweise auf Cyberangriffe in den vergangenen zwei Jahren. Daraus erschließt sich, dass sich Unternehmen aus dieser Branche im ersten Kapitel „Wie groß ist die Gefährdung – jetzt und in Zukunft?“ auch als am stärksten von Datenklau bedroht wahrnehmen: Sie sind derzeit auch am meisten betroffen. Das war bereits 2021 so, als 40 Prozent der Unternehmen mit digitalem Geschäftsmodell von mehrfachen Angriffsversuchen berichteten. Mit 39 Prozent in diesem Jahr bleibt diese Zahl nahezu unverändert.

Insgesamt erfassen Unternehmen mit Jahresumsätzen zwischen 25 und 50 Millionen Euro häufiger Hinweise auf Cyberangriffe als sowohl kleinere als auch größere Unternehmen.

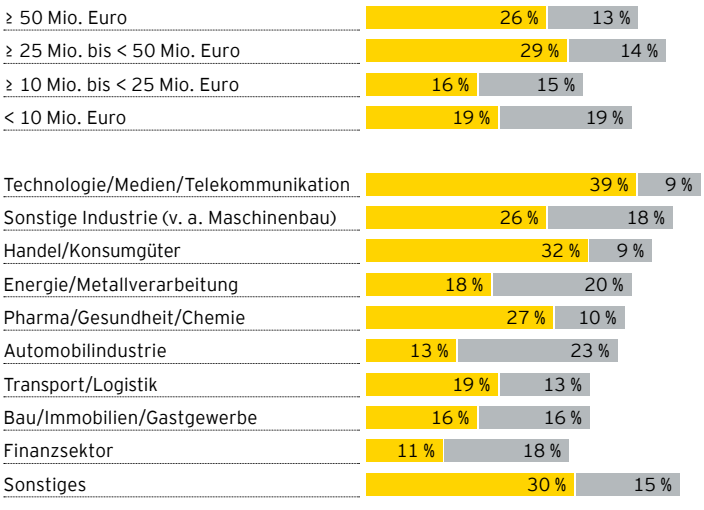


Abbildung 11

3.2

Hat sich die Anzahl an Angriffen gegen Ihr Unternehmen auf IT-Systeme und Daten seit der großflächigen Einführung von Homeoffice verändert?

Mehr Homeoffice führt nicht zu deutlich mehr Cyber-kriminalität

Mit 16 Prozent stellt jede sechste Führungskraft mehr Cyberattacken fest, seit durch die COVID-19-Pandemie erheblich mehr Tätigkeit ins Homeoffice verlagert wurde. Dem gegenüber steht allerdings eine große Mehrheit von 84 Prozent, die diesbezüglich keine Veränderung feststellen kann.

Den größten Anteil derer, die durch mehr Homeoffice eine Zunahme der Attacken erfassen, stellt mit 24 Prozent die Branche Pharma, Gesundheit und Chemie. Auch bei Technologie- und Medienunternehmen sowie im Sektor Handel und Konsumgüter ist der Anteil überdurchschnittlich hoch.

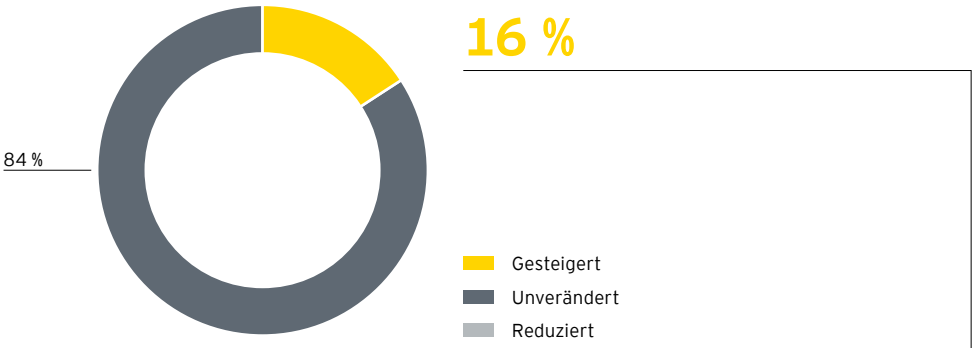


Abbildung 12

Anteil „gesteigert“ nach Branchen

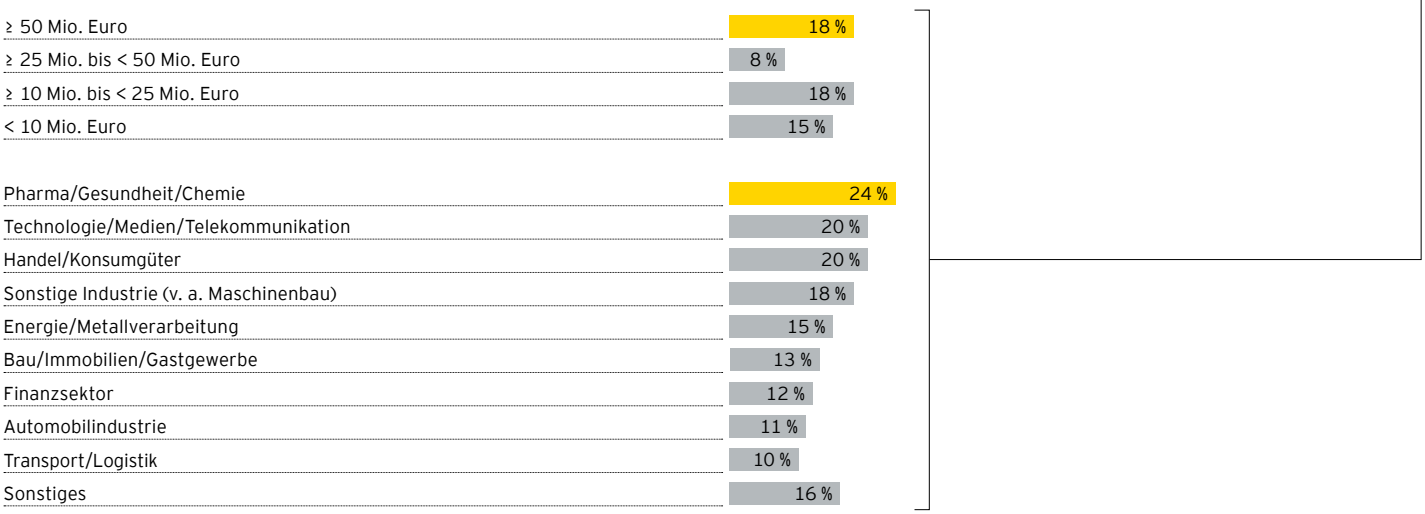


Abbildung 13

3.3

Welcher Bereich war vom Cyberangriff beziehungsweise Datenklau betroffen beziehungsweise wo ergab sich dieser Verdacht?

Häufigstes Ziel von Cyberattacken: Finanzabteilungen

Mit einem doch sichtbaren Vorsprung liegen Finanzabteilungen von Unternehmen an der Spitze der häufigsten Ziele von Cyberattacken beziehungsweise Datenklau: Mit 42 Prozent ist die Zahl zudem um einen Prozentpunkt im Vergleich zu 2021 gestiegen.

Deutlich erhöht haben sich mit 7 Prozentpunkten Attacken auf den Vertrieb mit jetzt 37 Prozent, auch die Managementebene war in fast jedem dritten Fall betroffen (32 Prozent).

Abbildung 14 | Häufigkeit der Datendiebstähle je Unternehmensbereich | Werte von 2021 in Klammern

3.4

Welche konkreten Handlungen fanden statt?

IT-Systeme werden mit Abstand am häufigsten attackiert

Wenig überraschend ist das Ziel, auf das sich die meisten Hackerangriffe richten: 53 Prozent betreffen IT-Systeme. Doch greifen anscheinend die Sicherheitsmaßnahmen der Unternehmen. Denn gegenüber 2021 (69 Prozent) sind nun 16 Prozentpunkte weniger Systeme betroffen.

Mit Abstand folgt dann mit 25 Prozent das vorsätzliche Stören oder Lahmlegen der Geschäftstätigkeit oder der IT-Systeme. Dagegen ist bei den Angriffen durch Phishing, Ransomware etc. ein Zuwachs von 21 Prozent 2021 auf jetzt 26 Prozent zu verzeichnen.

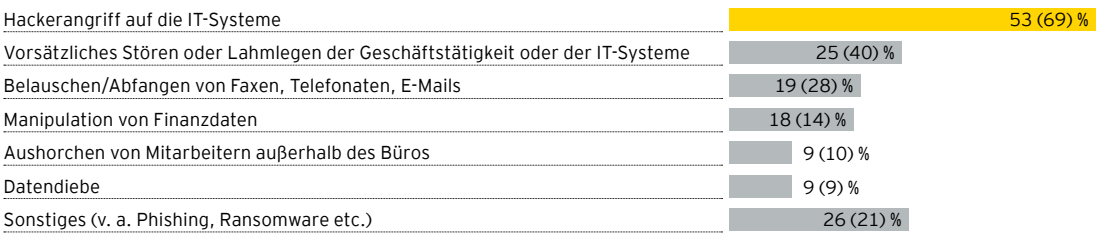


Abbildung 15 | Werte von 2021 in Klammern

3.5

Wurden personenbezogene Daten entwendet und war eine Reaktion entsprechend der Datenschutz-Grundverordnung (DSGVO) erforderlich?

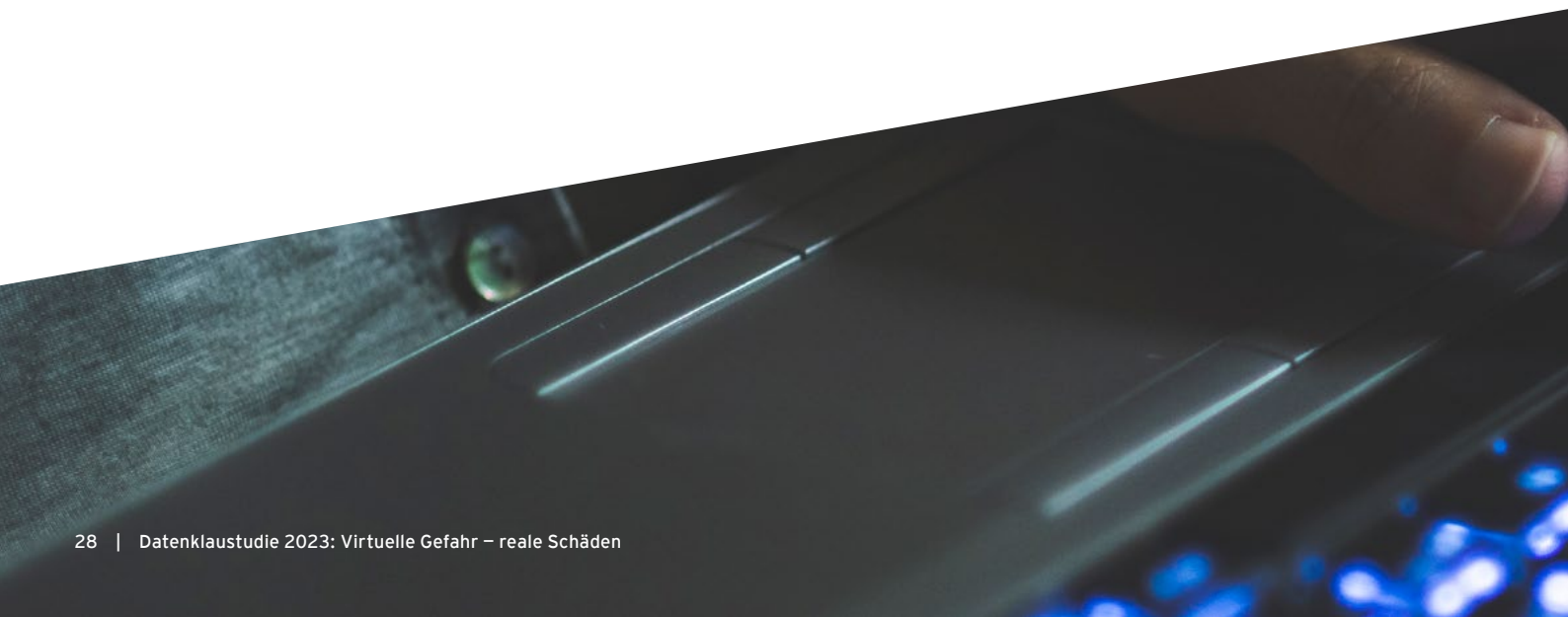
Personenbezogene Daten bei mehr als jedem dritten Angriff entwendet

In mehr als jedem dritten Fall (38 Prozent), in dem Unternehmen konkrete Hinweise auf eine Cyberattacke vorlagen, wurden personenbezogene Daten entwendet. Allerdings war nur in 13 Prozent dieser Fälle eine Reaktion entsprechend der Datenschutz-Grundverordnung erforderlich.

In 25 Prozent der Fälle hingegen war keine solche Reaktion erforderlich.

Abbildung 16

> Personenbezogene Daten sind bei Hackern ein beliebtes Angriffsziel. Kein Wunder also, dass bei mehr als jedem dritten registrierten Cyberangriff solche Daten entwendet wurden.



3.6

Von welchem Täterkreis ging die Gefährdung aus?

Tätergruppe Nummer eins: das organisierte Verbrechen, Tendenz steigend

Die vergleichsweise noch junge Form der Kriminalität, das organisierte Verbrechen im digitalen Raum, nimmt weiterhin zu: Mittlerweile steckt hinter jedem zweiten erkannten Cyberangriff (55 Prozent) das organisierte Verbrechen. Vor zwei Jahren lag der Anteil bei 49 Prozent, 2019 wurden gar nur 16 Prozent der Angriffe dieser Tätergruppe zugeschrieben.

Auf Rang zwei der Gruppierungen folgen Hacktivisten, also Hacker mit politischen oder ideologischen Zielen. Sie werden für 26 Prozent der registrierten Attacken verantwortlich gemacht, was wiederum acht Prozentpunkte mehr sind als noch 2021.

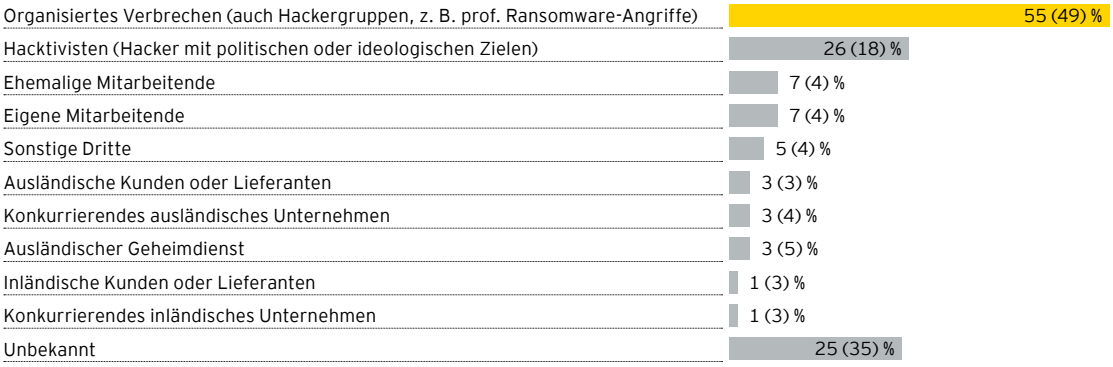


Abbildung 17 | Unternehmen, die bereits geschädigt wurden | Werte von 2021 in Klammern | Mehrfachnennungen möglich

3.7

Wie wurden die kriminellen Handlungen aufgedeckt?

Mehr als jeder zweite Angriff wurde vom internen Kontrollsystem erkannt

In mehr als jedem zweiten registrierten Fall (56 Prozent) half ein internes Kontrollsystem des Unternehmens bei der Aufdeckung der Cyberattacke, auch durch interne Routineprüfungen (37 Prozent) wurden kriminelle Handlungen entdeckt. Beide Werte sind nahezu identisch mit den Werten aus dem Jahr 2021. Hinweise unternehmensinterner Personen nahmen dagegen deutlich ab, liegen noch bei 36 Prozent.

Trotz aller Kontrollmechanismen und staatlichen Aktivitäten wird allerdings rund jeder siebte Angriff rein zufällig aufgedeckt.

Abbildung 18 | Unternehmen, die bereits geschädigt wurden | Werte von 2021 in Klammern | Mehrfachnennungen möglich

Wenn die kriminellen Handlungen durch das interne Kontrollsystem aufgedeckt wurden, um welche internen Kontrollsysteme handelte es sich dabei?

Interne Kontrollsysteme und Routineprüfungen decken die meisten Vorfälle auf

Mehr als jede zweite durch das interne Kontrollsystem aufgedeckte kriminelle Handlung (58 Prozent) wurde durch einen Alarm im Security Operations Center (SOC) oder Security Information and Event Management (SIEM) erkannt. Gut jeder dritte solche Fall wurde durch sonstige Auffälligkeiten im Information Security Management System (ISMS, 35 Prozent) beziehungsweise durch eine Regelprüfung wie zum Beispiel im Rahmen einer Überprüfung der Clean Desk Policy (34 Prozent) erkannt.

Abbildung 19 | Mehrfachnennungen möglich

3.8

Wer wurde mit der Aufklärung beauftragt?

IT-Abteilung als Aufklärer

Es ist an sich naheliegend und wird von den Zahlen bestätigt, dass die eigene IT-Abteilung erster Ansprechpartner bei der Aufklärung von Cyberangriffen beziehungsweise Datenklau ist: Mit 72 Prozent hat sich der mehrheitliche Anteil hierbei sogar noch um 6 Prozentpunkte im Vergleich zu 2021 erhöht Doch auch interne IT-Abteilungen benötigen im Ernstfall Hilfe von außen. Gerade neuartige Cyberbedrohungen bringen etablierte IT-Strukturen im Ernstfall schnell an ihre Kapazitätsgrenzen. So greifen dann auch 15 Prozent der befragten Unternehmen auf die Unterstützung von externen Spezialisten, wie zum Beispiel IT-Sicherheitsfachleute oder IT-Forensiker, zurück.

Abbildung 20 | Werte von 2021 in Klammern

Datenschutz-Grundverordnung (DSGVO) und „EU Trade Secrets“-Richtlinie

3.9

Ist Ihr Unternehmen mit den Regelungen der Datenschutz-Grundverordnung (DSGVO) und der EU-Richtlinie zum Schutz von Geschäftsgeheimnissen (EU Trade Secrets) vertraut?

99 Prozent der Unternehmen ist mindestens ein Regelwerk bekannt

Mit 61 Prozent ist die Mehrzahl der befragten Manager sowohl mit der Datenschutz-Grundverordnung (DSGVO) als auch mit der EU-Richtlinie zum Schutz von Geschäftsgeheimnissen (EU Trade Secrets) vertraut. 38 Prozent haben sich bisher nur mit der DSGVO beschäftigt.

Am besten kennen sich mit beiden Regelwerken die Automobilindustrie (73 Prozent) und der Finanzsektor (71 Prozent) aus, im Bereich Handel und Konsumgüter sind mit 49 Prozent die wenigsten Kenntnisse vorhanden.

Größere Unternehmen mit Jahresumsätzen von mindestens 50 Millionen Euro sind häufiger mit der DSGVO und der Richtlinie zum Schutz von Geschäftsgeheimnissen vertraut (68 Prozent) als kleinere Unternehmen.

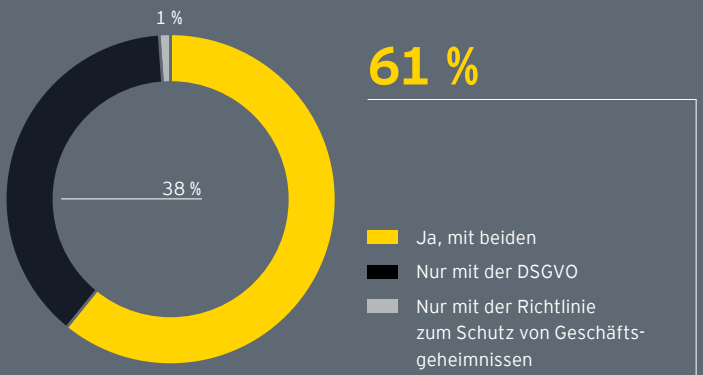


Abbildung 21

Anteil „Ja, mit beiden“ nach Branchen und Größenklassen

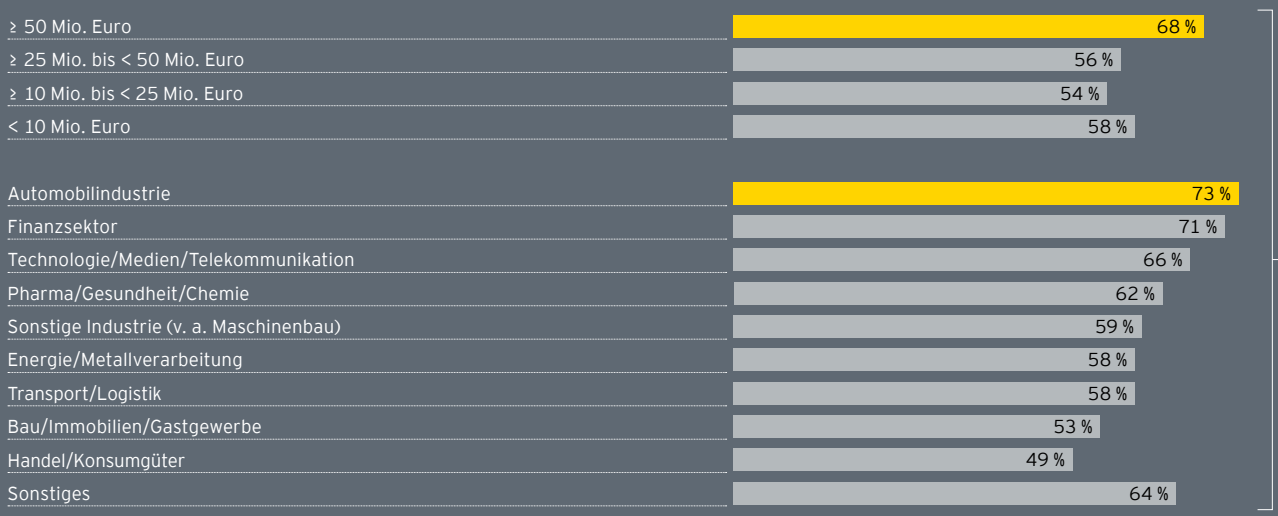


Abbildung 22

3.10

Welche Maßnahmen haben Sie ergriffen, um den Anforderungen der DSGVO beziehungsweise der EU-Richtlinie zum Schutz von Geschäftsgeheimnissen (EU Trade Secrets) gerecht zu werden?

Am häufigsten werden Schutzmaßnahmen festgelegt und durch Audits überprüft

Von den insgesamt 99 Prozent der befragten Führungskräfte, deren Unternehmen mit einem oder beiden Regelwerken vertraut sind, integrieren alle entsprechende Maßnahmen, um den Anforderungen der DSGVO beziehungsweise der EU-Richtlinie zum Schutz von Geschäftsgeheimnissen (EU Trade Secrets) gerecht zu werden.

Am häufigsten werden mit 82 Prozent Schutzmaßnahmen festgelegt, dahinter folgt mit 76 Prozent die Überprüfung implementierter Schutzmaßnahmen im Rahmen von Audits. Die Vorbereitung einer Reaktion auf detektierte bzw. erkannte Datenklauvorfälle liegt mit 75 Prozent an dritter Stelle.

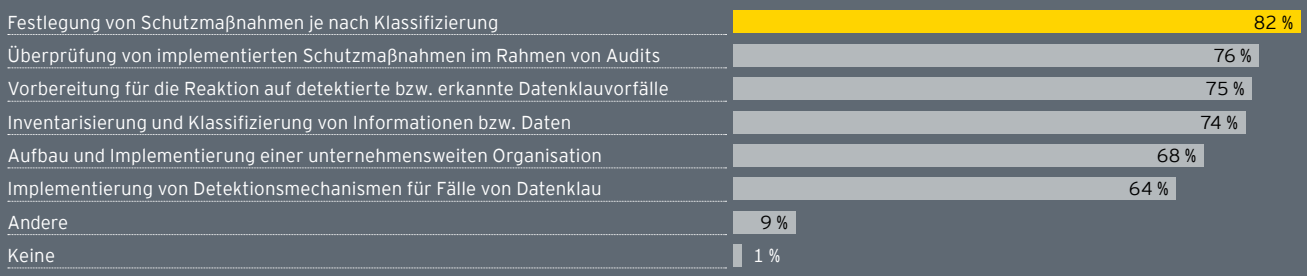
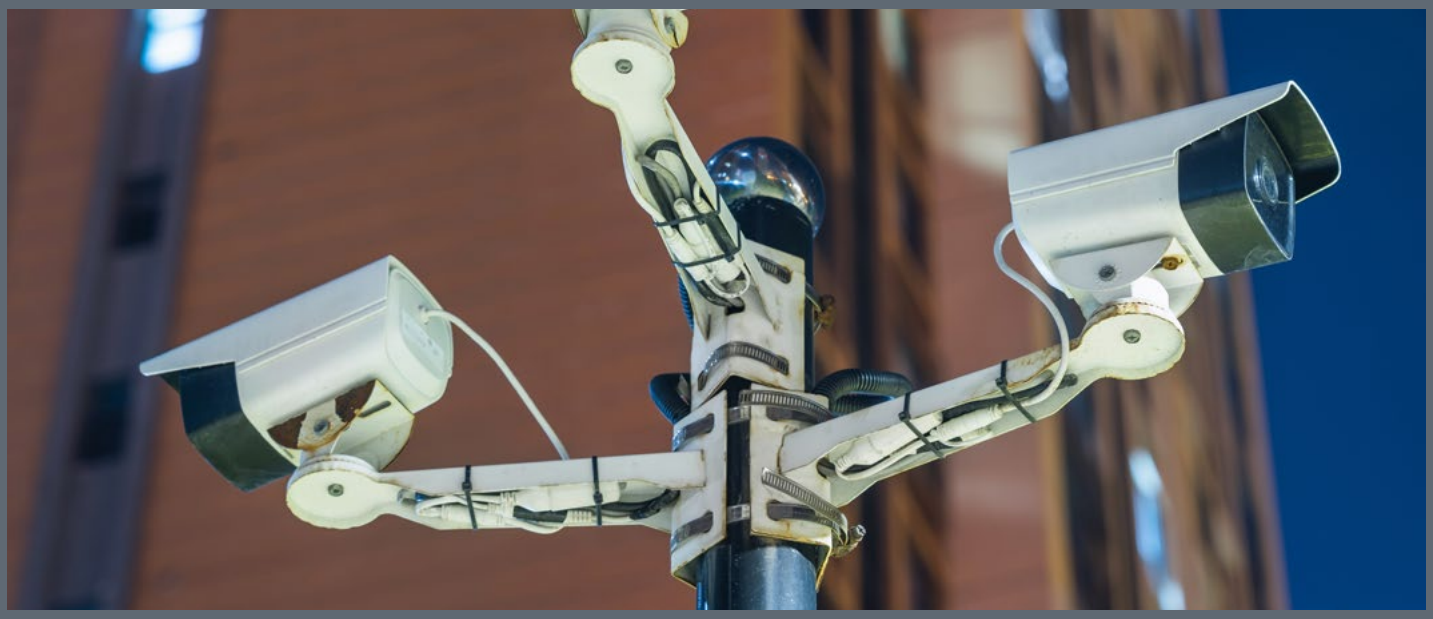


Abbildung 23 | Mehrfachnennungen möglich



Prävention: Schützen sich die Unternehmen ausreichend?

4

4.1

Sind aus Ihrer Sicht die präventiven Vorkehrungen im Unternehmen ausreichend, um sich wirkungsvoll gegen Informationsabfluss zu schützen?

Gut jedes dritte Unternehmen fühlt sich vor Spionage nicht ausreichend gesichert: Mit 33 Prozent sind das mehr als noch vor zwei Jahren (2021: 27 Prozent). Besonders skeptisch sind in dieser Hinsicht die Automobilindustrie und die Branchen Pharma, Gesundheit und Chemie mit jeweils 37 Prozent, dicht dahinter folgt der Bereich Technologie, Medien und Telekommunikation mit 36 Prozent. Letzterer stellte in den vergangenen zwei Jahren passend dazu auch die meisten Hinweise auf Cyberattacken fest.

Automotive und Pharma fühlen sich am wenigsten geschützt

Von den 67 Prozent der befragten Führungskräfte, die ihre Vorkehrungen gegen Informationsabfluss für ausreichend halten, stammt nahezu die Hälfte (45 Prozent) aus dem Bereich der sonstigen Industrie (vor allem Maschinenbau). Aufgeholt haben an dieser Stelle auch die Energie- und die Metallverarbeitungsunternehmen: 2021 war hier mit 39 Prozent die Sorge, nicht ausreichend geschützt zu sein, noch am stärksten ausgeprägt, jetzt ist der Wert auf 26 Prozent gesunken.

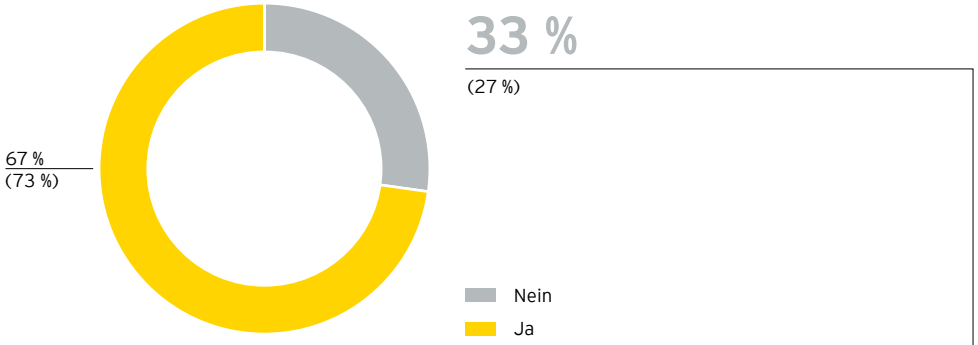


Abbildung 24 | Werte von 2021 in Klammern

Anteil „Nein“ nach Branchen

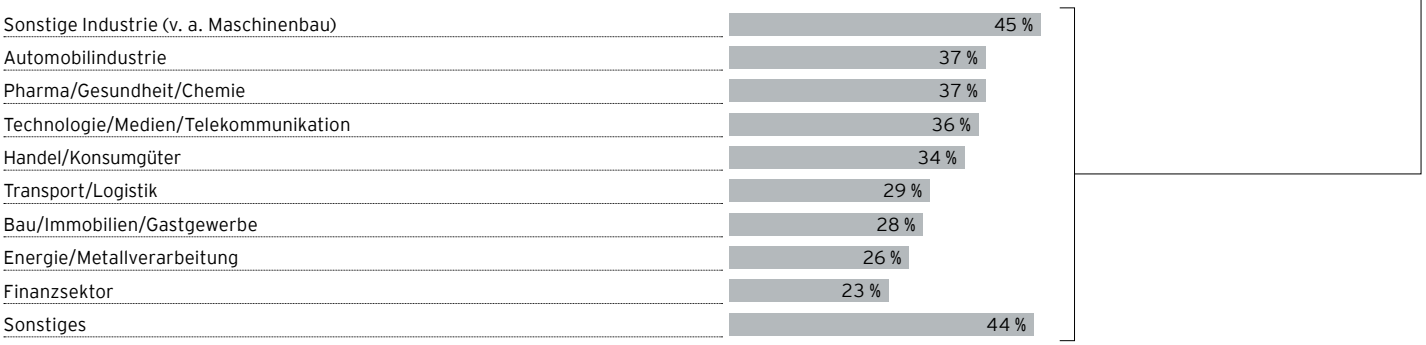


Abbildung 25

4.2

Wer kümmert sich im Unternehmen um die zentralen Belange des Schutzes sensibler Informationen beziehungsweise Daten?

Großteil der Verantwortung liegt bei Datenschutzbeauftragten

Erstmals haben wir in der Datenklaustudie nach Datenschutzbeauftragten gefragt: In 80 Prozent der Unternehmen ist diese Funktion für den Schutz sensibler Daten und Informationen zuständig, und bei 78 Prozent ist es die IT-(Security-)Abteilung.

Gleich geblieben ist mit 55 Prozent der Anteil derer, die externe Dienstleister für den Datenschutz einbinden. In immerhin 43 Prozent der Unternehmen (2021: 41 Prozent) ist Cybersecurity mittlerweile Chefsache.

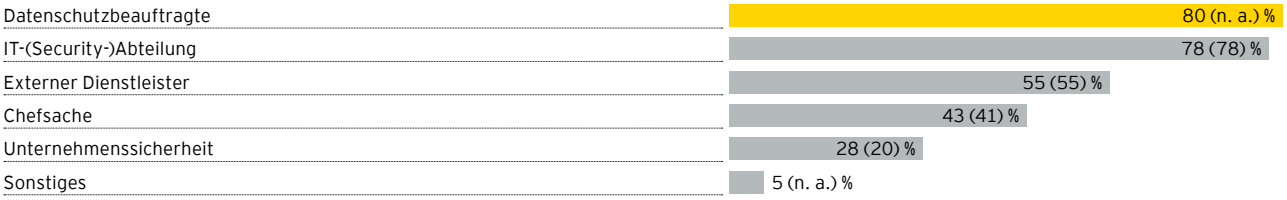


Abbildung 26 | Werte von 2021 in Klammern | Mehrfachnennungen möglich

4.3

In welche der folgenden Sicherheitsvorkehrungen im Bereich Objektsicherheit haben Sie in den vergangenen zwei Jahren investiert?

Zugangskontrollen und gesicherter Serverbereich als klassisch physischer Schutz

Ein besonders gesicherter Serverbereich steht auf der Prioritätenliste der Unternehmen nach wie vor ganz oben und hat mit 78 Prozent im Vergleich zu 2021 nochmals um 2 Prozentpunkte zugelegt. Die Zutrittskontrolle zum Firmenareal (74 Prozent) und die Überwachung besonders sensibler Bereiche (65 Prozent) liegen ebenfalls mit an der Spitze.

Nur noch 8 Prozent der befragten Manager haben im Bereich der Objektsicherheit zuletzt in neue Technologien wie Roboter und Drohnen investiert – vor zwei Jahren war dieser Anteil noch doppelt so hoch. Dagegen ist mehr Geld in die regelmäßige Untersuchung auf Abhöreinrichtungen durch Spezialisten geflossen: Hier hat sich der Anteil mit 10 Prozent mehr als verdoppelt.

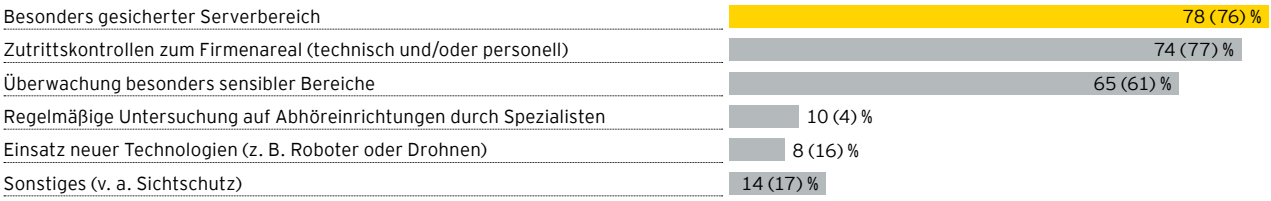


Abbildung 27 | Werte von 2021 in Klammern | Mehrfachnennungen möglich

4.4

In welche der folgenden Vorkehrungen im Bereich IT-Sicherheit haben Sie in den vergangenen zwei Jahren investiert?

Firewall/VPN und Antivirenschutz werden zur Regel in der IT-Sicherheit

Im Jahr 2021 steuerten die Zahlen fast die 100-Prozentmarke an und auch jetzt rangieren Firewall und VPN-Zugänge mit 95 sowie Antivirensoftware mit 93 Prozent ganz oben bei den Investitionen in die IT-Sicherheit: Diese Schutzmaßnahmen zählen mittlerweile zum Standard. Auch die Multi-Faktor-Authentifizierung (MFA) gehört heute in mehr als zwei von drei Unternehmen (69 Prozent) zum Arbeitsalltag. Durchaus bemerkenswert: Von 30 Prozent 2021 auf jetzt 40 Prozent nahmen die Investitionen in Information-Security-Management-Systeme (ISMS) zu.

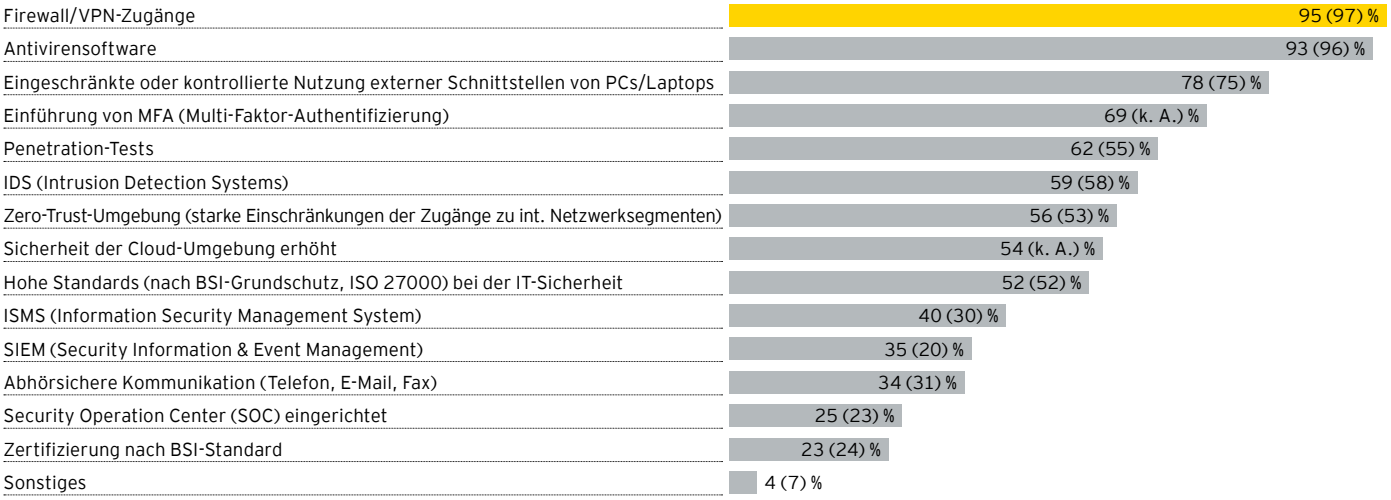
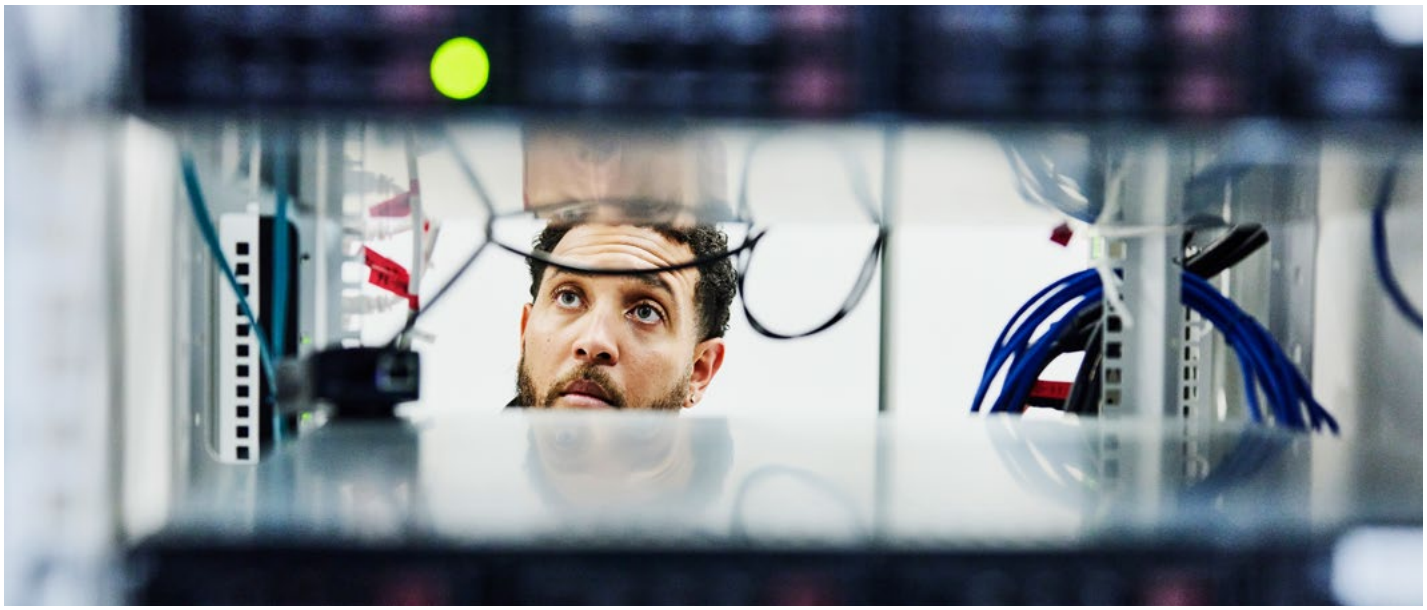


Abbildung 28 | Werte von 2021 in Klammern | Mehrfachnennungen möglich



4.5

Welche der folgenden Sicherheitsvorkehrungen haben Sie im Bereich Personal getroffen?

Fast alle Arbeitsverträge enthalten Verpflichtungen zur Geheimhaltung

Daten und Informationen können nicht allein durch Angriffe von außen geraubt werden, sondern auch von denen, die direkten und legitimierten Zugriff darauf haben – den Mitarbeitenden. Um dem vorzubeugen, schreiben 92 Prozent der Unternehmen Geheimhaltungsverpflichtungen in die Arbeitsverträge. Die Sensibilisierung der Mitarbeitenden für Spionagegefahren (89 Prozent) und personalfördernde Maßnahmen zur Steigerung der Verbundenheit mit dem Unternehmen (78 Prozent) sind die zweit- und drittwichtigsten Maßnahmen im Personalbereich. Alle drei unterliegen zahlenmäßig im Vergleich zu 2021 keinen größeren Schwankungen.

Jedoch zeigt sich eine wahrnehmbare Steigerung in zwei anderen Bereichen: Background-Checks vor der Besetzung sensibler Positionen führen inzwischen 41 Prozent der Unternehmen durch, 2021 waren es noch 34 Prozent. Noch stärker hat der Einsatz von Whistleblowing-Systemen zugenommen, von denen 2021 nur 20 Prozent und heute 32 Prozent Gebrauch machen.

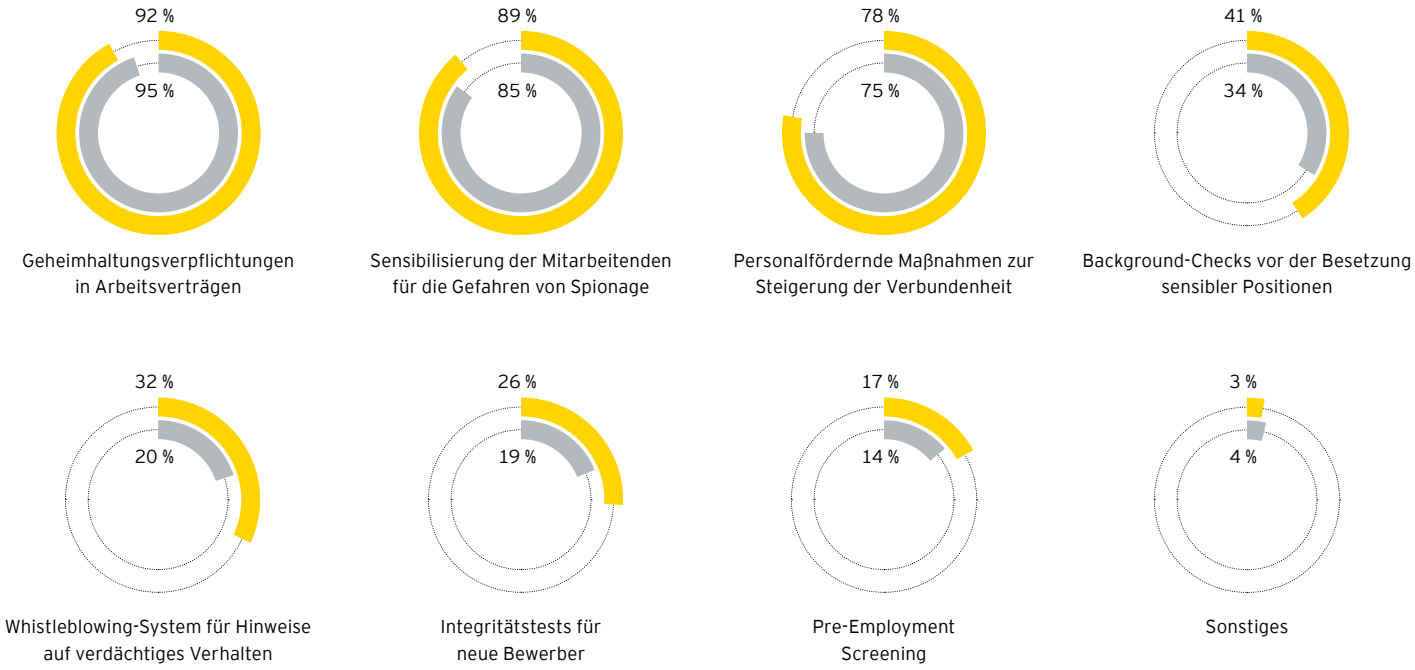


Abbildung 29 | Mehrfachnennungen möglich

4.6

Welche prozesstechnischen Vorkehrungen haben Sie getroffen, um sich vor Spionage zu schützen?

Klares Ergebnis für klare Regeln im Umgang mit sensiblen Informationen

Damit nicht nach außen dringt, was nur nach innen gehört, geben 90 Prozent der befragten Unternehmen klare Regeln für den Umgang mit schützenswerten Informationen vor, 87 Prozent verpflichten zudem ihre Geschäftspartner (ebenfalls) zur Geheimhaltung. Hierbei spielt für immer mehr Unternehmen auch die sorgfältige Auswahl der Geschäftspartner eine Rolle – ein Anstieg von 77 auf 81 Prozent. Vertrauen bleibt eben die Grundlage jeder funktionierenden Verbindung.

Dass es kein Unternehmen mehr gibt, das keinerlei prozesstechnische Vorkehrungen gegen Datenklau und Informationsabfluss trifft, zeigt, wie präsent das Risikobewusstsein hierfür mittlerweile ist. Dafür spricht auch der Anstieg der Nutzung Security-Incident-Management-Prozessen um 9 Prozentpunkte auf nun 45 Prozent.

Abbildung 30 | Mehrfachnennungen möglich

2021 2023

Cyberversicherung im Fokus

4.7

Hat Ihr Unternehmen eine Cyberversicherung gegen digitale Risiken (Hackerangriffe etc.) abgeschlossen?

Fast jedes zweite Unternehmen versichert sich gegen digitale Risiken …

Mit 10 Prozentpunkten mehr gegenüber der Datenklaustudie 2021 hat inzwischen fast jedes zweite Unternehmen eine Cyberversicherung abgeschlossen (46 Prozent). Am höchsten ist der Anteil mit 52 Prozent im Bereich Pharma, Gesundheit und Chemie, der auch zu den Sektoren gehört, die sich am stärksten bedroht fühlen. Auch im Finanzsektor sowie im Bereich Bau, Immobilien und Gastgewerbe liegt der Anteil der versicherten Unternehmen mittlerweile bei jeweils mehr als 50 Prozent.

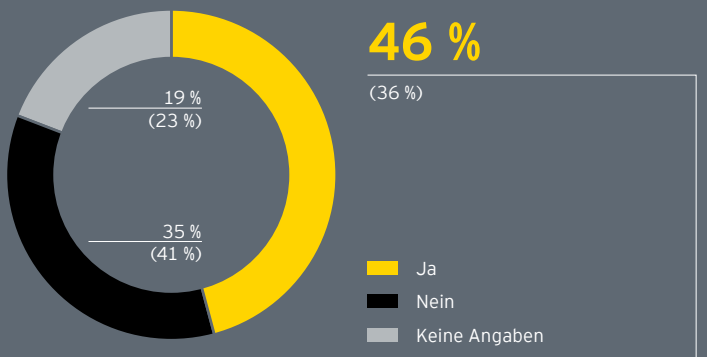


Abbildung 31 | Werte von 2021 in Klammern

Anteil „Ja“ nach Branchen

Abbildung 32

4.8

Unternehmen, die bisher keine Versicherung gegen digitale Risiken abgeschlossen haben: Planen Sie den Abschluss einer Cyberversicherung?

… jedes dritte noch nicht versicherte wird nachziehen

Von den 35 Prozent der befragten Unternehmen, die hingegen noch über keinen Versicherungsschutz gegen digitale Risiken verfügen, plant zumindest jedes dritte den Abschluss. Im Jahr 2021 hatten sich dies nur 20 Prozent vorgenommen.

Vor allem der Bereich Transport und Logistik (50 Prozent) und der Finanzsektor (47 Prozent) haben das Thema Cyberversicherung als baldigen Schritt auf der Agenda.

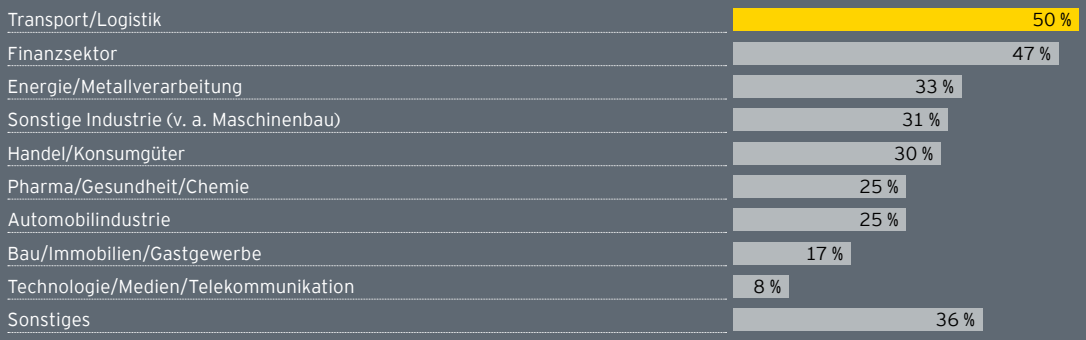


Abbildung 33

Cyberversicherung im Fokus

4.9

Unternehmen, die bereits eine Cyberversicherung abgeschlossen haben: Hat die Versicherung eine Prüfung und Feststellung des IT-Sicherheitsniveaus durchgeführt?

Versicherer checken in den meisten Fällen vorab das IT-Sicherheitsniveau

Mit der Prüfung und Feststellung des IT-Sicherheitsniveaus bewerten Versicherungen, wie effektiv und effizient die Informationssicherheit des Unternehmens bis dato gestaltet wurde – vergleichbar mit dem Gesundheitscheck für die Krankenversicherung. Diese Maßnahme ist für die Tarifberechnung ausgesprochen sinnvoll und hilft auch dem Unternehmen beim Risikomanagement.

Bei mehr als drei Viertel der Unternehmen (66 Prozent), die eine Cyberversicherung abgeschlossen haben, führte die Versicherung ein IT Security Maturity Assessment durch – ein deutlicher Anstieg: Vor zwei Jahren taten sie dies nur bei 58 Prozent der Unternehmen.

Am häufigsten wurden diese Bestandsaufnahmen in Unternehmen aus dem Bereich Technologie, Medien und Telekommunikation durchgeführt (90 Prozent), im Bereich Bau, Immobilien und Gastgewerbe dagegen nur bei zwei Dritteln (67 Prozent).

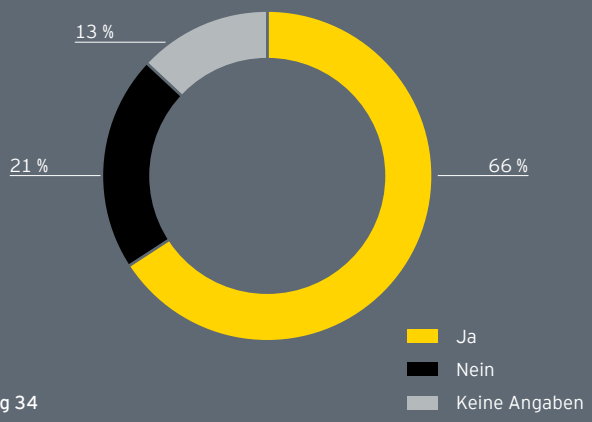


Abbildung 34

4.10

Hatten Sie in Ihrem Unternehmen bereits einen Fall, in dem Sie auf Ihre Cyberversicherung zurückgreifen mussten?

Versicherungsschutz wird bisher selten in Anspruch genommen

Bei der Cyberversicherung handelt es sich um ein noch recht junges Produkt, das erst seit einigen Jahren von Versicherern angeboten wird. Damit könnte es zusammenhängen, dass von den Unternehmen, die bisher eine solche Versicherung gegen digitale Risiken abgeschlossen haben, erst 8 Prozent diese in Anspruch nehmen mussten. Die meisten dieser Fälle traten in der Automobilindustrie auf.

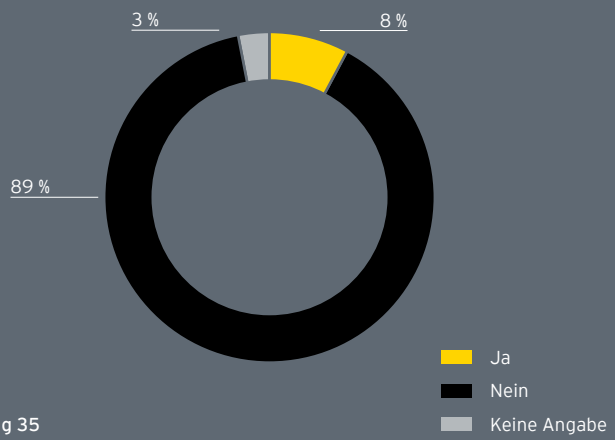


Abbildung 35

4.11

Welche Leistungen beinhaltet Ihre Cyberversicherung?

Diese Kosten übernehmen Cyberversicherungen

Top 7 von 2023

Die große Mehrheit der Cyberversicherungen beinhaltet die Kostenübernahme bei einem Eigenschaden (82 Prozent), für IT-Experten und -Forensiker greifen sie noch bei 79 Prozent. Die Zahlung von Lösegeld, wie sie bei Ransomware üblicherweise gefordert wird, gehört in der Regel nicht zu den Leistungen einer Cyberversicherung und bildet mit 46 Prozent das Schlusslicht. Fast jede zweite Cyberversicherung deckt dafür immerhin sogar die Beauftragung spezialisierter Anwälte ab.

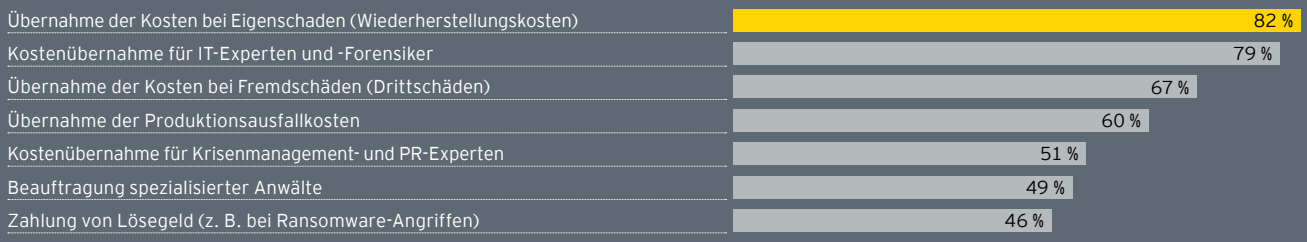
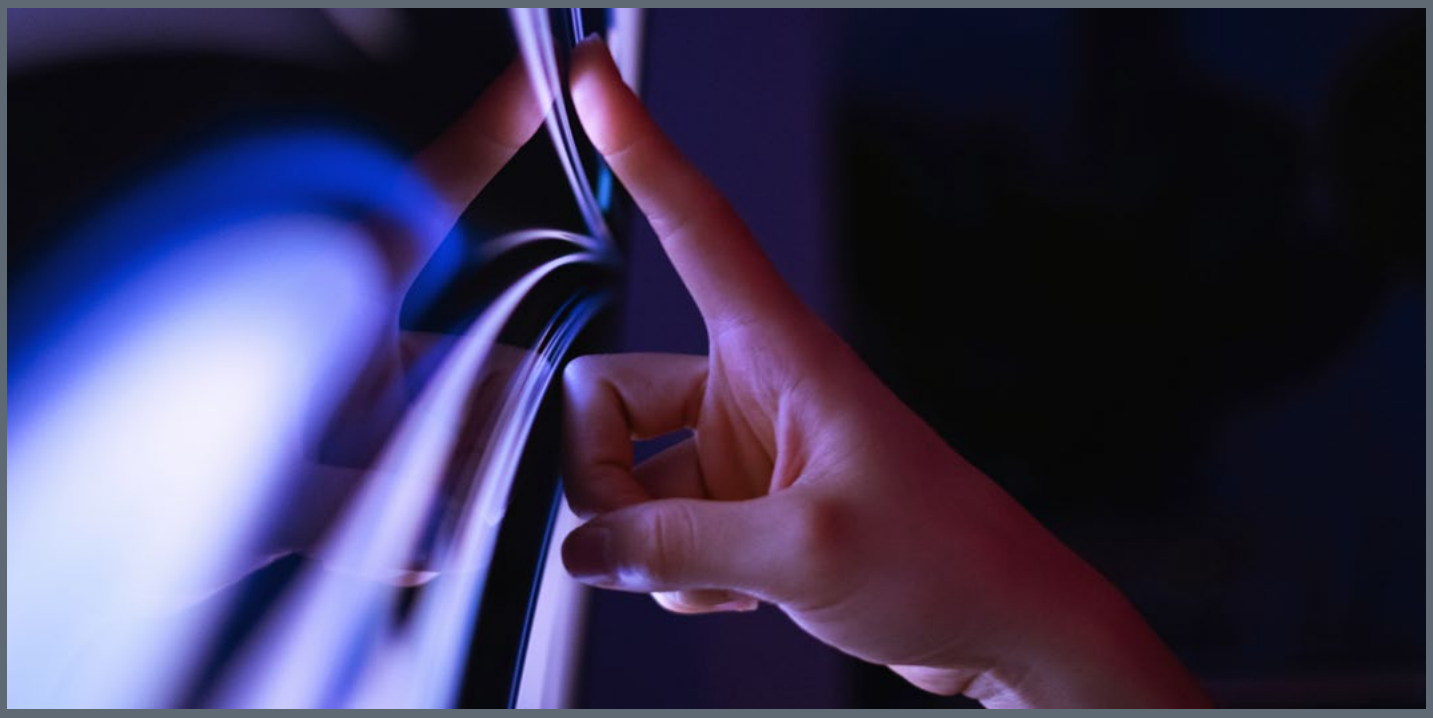


Abbildung 36



Reaktion auf Datenklau: Krisenpläne und Kommunikation

5

5.1

Hat Ihr Unternehmen Krisenpläne zur Reaktion auf Datenklaufälle vorbereitet?

Unternehmen bereiten sich zunehmend besser auf den Krisenfall vor

Das geschärfte Risikobewusstsein für Cyberattacken und Datenklau hat einen Sprung in der Vorbereitung bewirkt: Mit 70 Prozent verfügen sieben von zehn Unternehmen über einen Krisenplan, der das Vorgehen im Falle eines festgestellten Angriffs definiert – das sind 18 Prozentpunkte mehr als noch vor zwei Jahren (52 Prozent). Der Finanzsektor und die Automobilindustrie sind an dieser Stelle mit 83 bzw. 75 Prozent führend.

Nur noch 17 Prozent der Unternehmen haben bisher keine Krisenpläne für den digitalen Notfall parat, diese Zahl ist von 26 Prozent im Jahr 2021 gesunken. 13 Prozent der befragten Führungskräfte wollten hierzu keine Angabe machen.

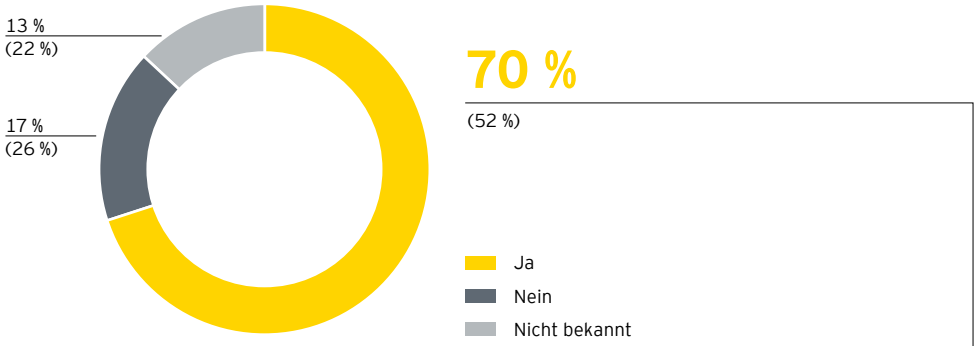


Abbildung 37 | Werte von 2021 in Klammern

Anteil „Ja“ nach Branchen

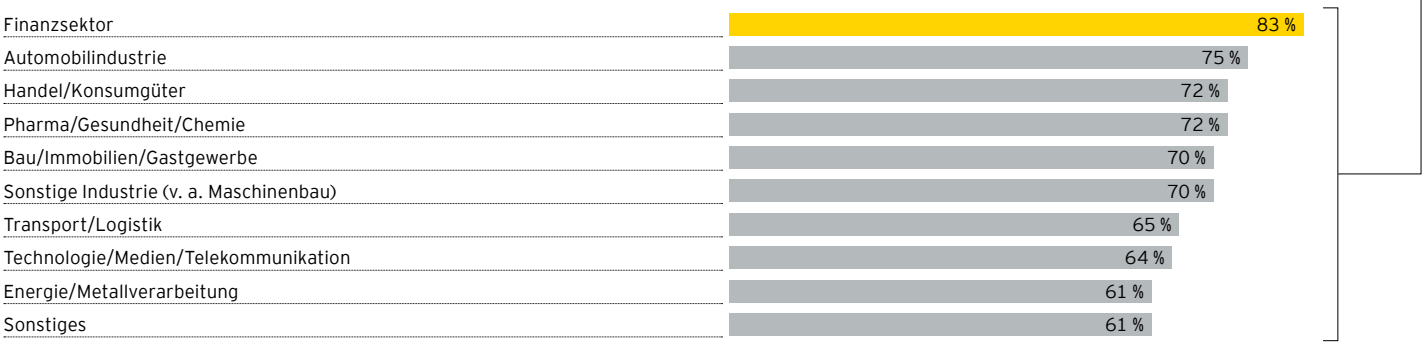


Abbildung 38

5.2

Falls Ihr Unternehmen Krisenpläne zur Reaktion auf Datenklaufälle besitzt: Wie häufig werden deren Abläufe geübt?

Ein Krisenplan allein ist ein guter Anfang – noch besser ist es, wenn die betreffenden Personen ihn kennen und aufeinander eingespielt sind. Daher ist es wichtig, die Umsetzung regelmäßig zu üben. Von den befragten Unternehmen, die über Krisenpläne für den Fall einer Cyberattacke verfügen, üben 45 Prozent den Ernstfall einmal pro Jahr, 13 Prozent sogar mehrmals im Jahr. Am häufigsten spielen Unternehmen aus Technologie, Medien und Telekommunikation das Szenario durch (76 Prozent) – die Branche ist aktuell auch am häufigsten von Cyberangriffen betroffen. Doch auch die Energie und Metallverarbeitung ist an dieser Stelle mit 69 Prozent sehr aktiv.

Pharma, Gesundheit und Chemie fühlen sich zwar am stärksten vom Datenklau bedroht, allerdings übt nur die Hälfte der Unternehmen, die aus diesem Sektor einen Krisenplan erstellt haben, diesen auch. 27 Prozent aller Unternehmen mit Krisenplänen haben dessen Ausführung noch nie geprobt.

Die Branche Technologie, Medien und Telekommunikation probt den Ernstfall am häufigsten

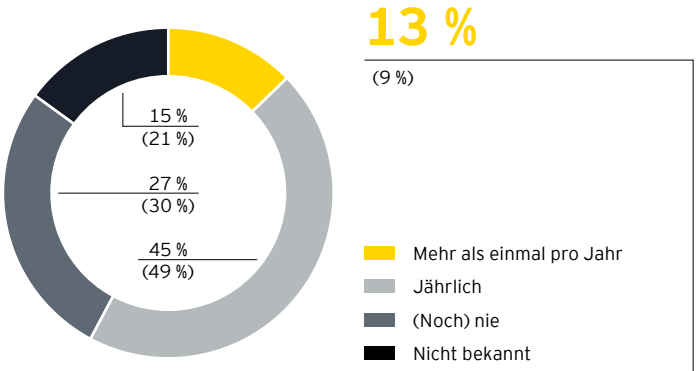


Abbildung 39 | Werte von 2021 in Klammern

Anteil „Mindestens einmal pro Jahr" nach Branchen

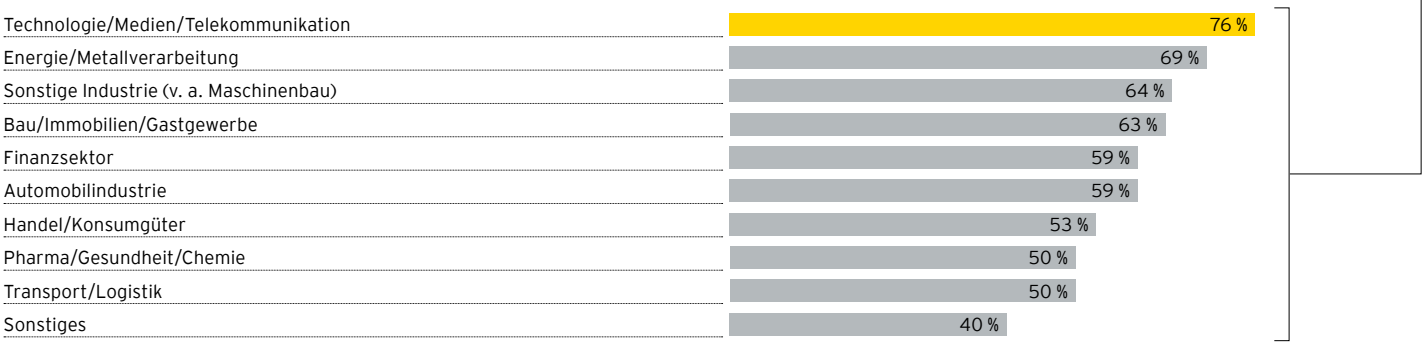


Abbildung 40

5.3

Falls Ihr Unternehmen keine Krisenpläne zur Reaktion auf Datenklaufälle besitzt oder es Ihnen nicht bekannt ist: Existiert in Ihrem Unternehmen ein zentrales Krisenteam?

Mehr als die Hälfte aller Unternehmen hat kein etabliertes Krisenteam

Obwohl allein die Sicherheitsvorkehrungen in technischer Hinsicht aufgrund der Bedrohungslage steigen, etablieren die befragten Unternehmen weniger häufig ein Krisenteam. Womöglich verlassen sie sich verstärkt auf die Technik. Diese allein ersetzt jedoch kein Team, das im Krisenfall weiß, welche Prozesse anzuschieben sind, und dessen Mitglieder sich aufeinander verlassen können.

Nur noch 33 Prozent (2021: 51 Prozent) geben an, dass es im Unternehmen ein zentrales Krisenteam gibt, verneinen tun dies 56 Prozent (2021: 41 Prozent). In den Fällen, in denen ein Krisenteam besteht, ist dieses zum Großteil (72 Prozent) auch bei Vorfällen im Bereich der Cyberkriminalität zuständig.

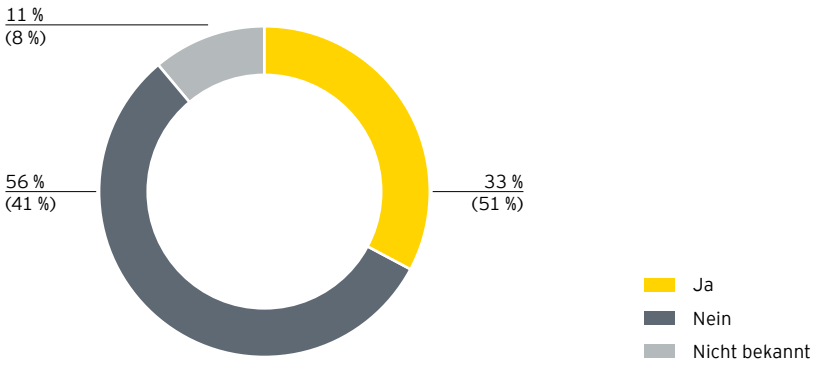
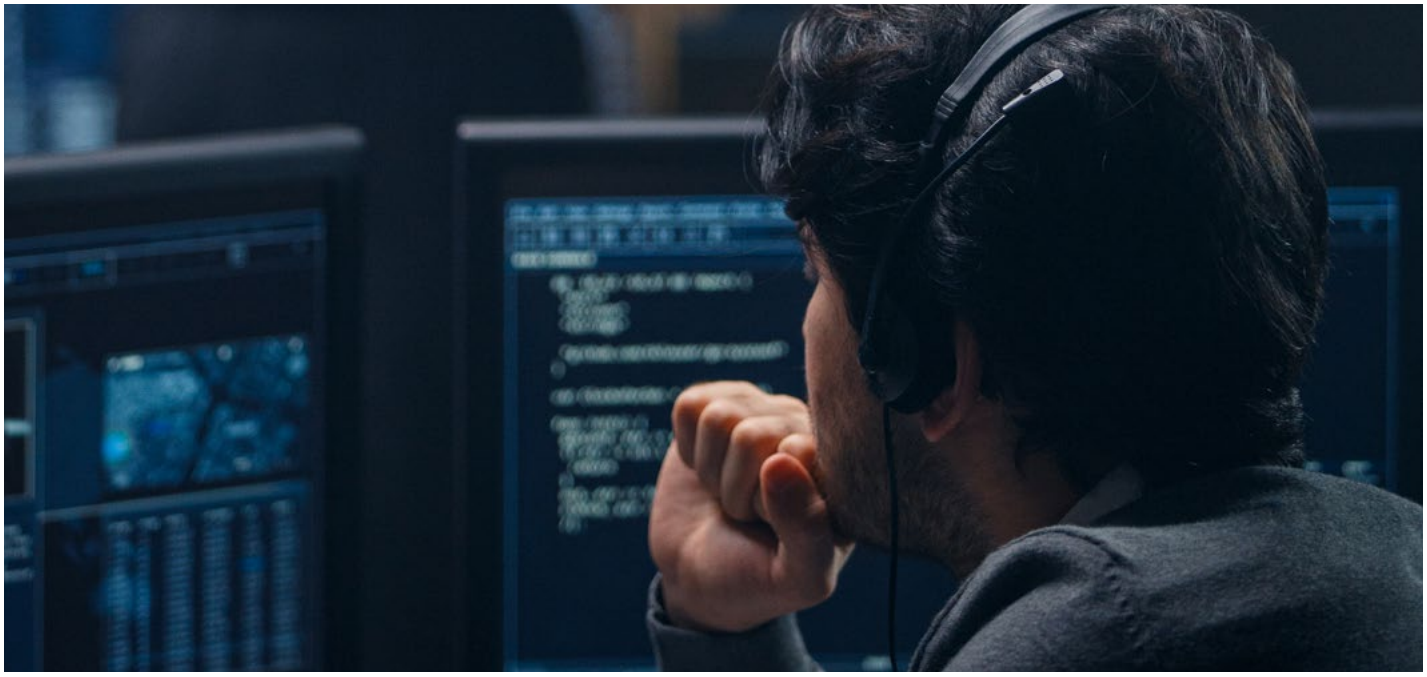


Abbildung 41



5.4

Falls ein zentrales Krisenteam vorhanden ist: Ist dieses Team auch für Vorfälle im Bereich Cybersecurity verantwortlich?

Meist ist das zentrale Krisenteam auch für die Cybersecurity verantwortlich

Bei gut sieben von zehn der Unternehmen, die über ein zentrales Krisenteam verfügen, ist dieses auch für Vorfälle im Bereich der Cybersecurity verantwortlich.

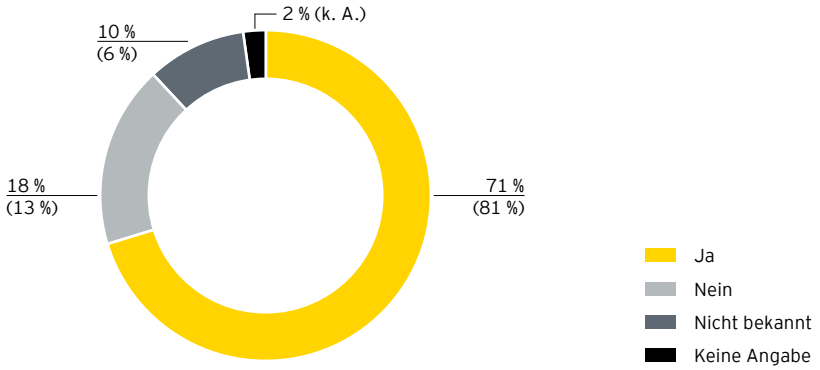
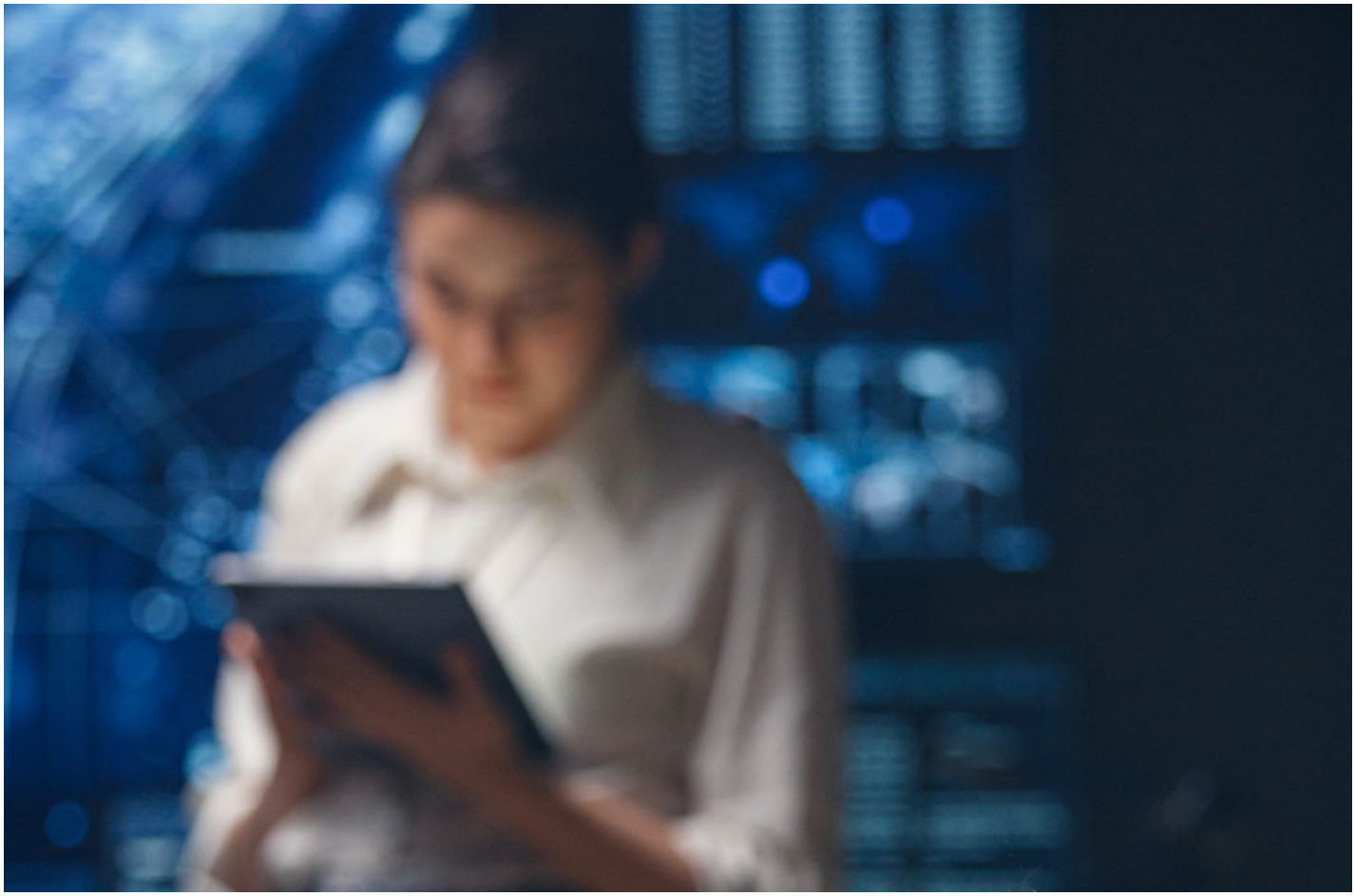


Abbildung 42 | Werte von 2021 in Klammern

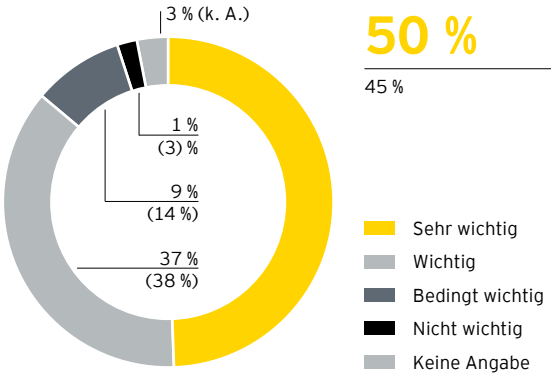


5.5

Im Falle von Datenklau: Wie wichtig ist für Sie eine fallbegleitende interne wie auch externe Kommunikation?

An dieser Stelle herrscht weitestgehend Einigkeit: Fast neun von zehn Unternehmen (87 Prozent) ist eine fallbegleitende interne und externe Kommunikation im Falle eines Datenklaus wichtig oder sogar sehr wichtig. Hervor sticht hierbei am stärksten der Finanzsektor, der diesen Punkt von allen Branchen und mit Abstand für am relevantesten hält (64 Prozent). 10 Prozent der befragten Unternehmen messen der Kommunikation im Ernstfall wenig bis gar keine Bedeutung zu.

Kommunikation nach innen und außen: für jedes zweite Unternehmen bei Datenklau relevant



50 %

45 %

Abbildung 43 | Werte von 2021 in Klammern

Anteil „Sehr wichtig“ nach Branchen

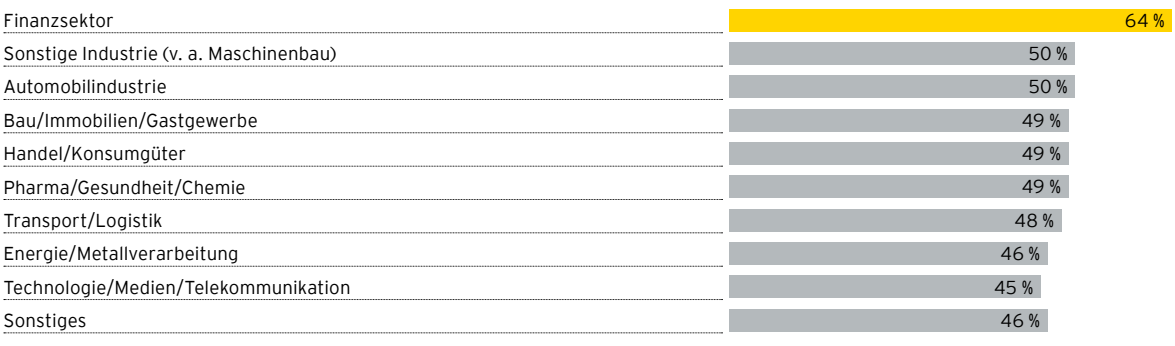


Abbildung 44

Kommunikation in der Krise:
Jeder sollte vorbereitet sein

Exkurs

Interview mit Marcus Ewald, Geschäftsführender Gesellschafter Dunkelblau GmbH & Co. KG

Cyber Incidents können jedes vernetzte Unternehmen trotz aller Schutzmaßnahmen treffen. Worauf es bei der Bewältigung von Cyberattacken nach innen wie nach außen ankommt, weiß Krisenmanager Marcus Ewald.

Mancher Satz von Marcus Ewald schrammt nur knapp am Kalenderspruch vorbei: „Es gibt für jede Krise eine richtige Entscheidung. Manchmal zwar keine gute, aber immer eine, die die am wenigsten schlechte ist", ist sein Leitspruch. Mit seiner Leipziger Agentur „Dunkelblau" steht er Unternehmen als Krisenmanager und -kommunikator in schweren Zeiten zur Seite. Mehr als 100 Organisationen leistete das Team bereits Erste Hilfe, der Anteil an Cyberkrisen nimmt dabei zu.

Ransomware-Angriffe und andere Cyberattacken sind eine noch relativ junge Form organisierter Kriminalität, die jedoch jedes digital vernetzte Unternehmen trotz aller Schutzmaßnahmen treffen kann – mit drastischen Auswirkungen. Erste Maßnahme im Krisenfall ist darum ein Lagebild. „Bei Cyber Incidents ist zu Beginn häufig nicht klar, wie genau der Angriff erfolgte und wann der Schaden behoben sein kann. Dennoch müssen die Stakeholder davon erfahren und auch, was unternommen wird", sagt Ewald. Das verschaffe in der unsicheren Situation etwas Sicherheit – für alle Beteiligten. Denn neben der Krisenbewältigung betreibt Marcus Ewald auch „Enttäuschungsmanagement" beim Kunden und seinen Stakeholdern: In der Regel dauert die Wiederherstellung der Systeme mindestens zwei bis vier Wochen, sogar wenn Back-ups vorliegen und/oder das Lösegeld schnell gezahlt wurde. Das dauert deutlich länger als in der Vorstellung vieler Betroffener.

Zu den größten und häufigsten Fehlern zählen an dieser Stelle nach Erfahrung des Krisenmanagers falsche Versprechen und voreilige Zusagen. „Es ist verständlich, dass man seine Kunden beruhigen möchte und sagt: ‚Nächste Woche können wir wieder liefern.' Doch nie gelingt alles reibungslos, und wenn das Unternehmen solche Versprechen mehrfach nicht einhalten kann, erodiert das Vertrauen spürbar. Wir müssen jeden Tag den konkreten Stand der Arbeitsfähigkeit und einen Zeitplan vermitteln, aber bei allen Prognosen sollte immer mitkommuniziert werden: Zu wie viel Prozent

> Einen vernünftigen Plan zu entwickeln und einzuhalten macht gutes Krisenmanagement aus. Dann ziehen auch Mitarbeitende und externe Stakeholder mit.

ist das sicher? Das erfordert auch, unangenehme Dinge auszusprechen." Der Umgang mit der Krise spiele eine entscheidende Rolle. Misslinge er, könne daraus eine Krise zweiter Ordnung entstehen. Das richtige Krisenmanagement beuge dem vor, indem aus der volatilen Lage heraus Szenarien abgeleitet und im Anschluss die richtigen Entscheidungen gefällt würden. „Einen vernünftigen Plan zu entwickeln und einzuhalten macht gutes Krisenmanagement aus. Dann ziehen auch Mitarbeitende und externe Stakeholder mit."

Ein signifikantes Risiko entsteht dann, wenn die Organisation in der Krise beginnt, sich mit sich selbst zu beschäftigen. Unter hohem Druck entstehen schnell Schuldzuweisungen, die selten zutreffen und noch weniger weiterhelfen. Die Aufgabe des Dunkelblau-Teams besteht in diesen Fällen darin, Ruhe und Gelassenheit in die Situation zu bringen und rasch erste Lösungsansätze aufzuzeigen. In jedem Fall hält Ewald es für eine unternehmerische Pflicht, auf eine (Cyber-)Krise vorbereitet zu sein. „Unternehmen müssen belegen können, dass sie sich vorbereitet haben. Cybersecurity, Krisenmanagement, Krisenkommunikation, Business Continuity: Im Ernstfall geht es darum, dass Menschen wissen, wie sie zusammenarbeiten, und auch kommunizieren können, was die nächsten Schritte und Verbesserungen sind." Dabei geht es nicht um Millionenprojekte, sondern darum, Szenarien vorher zu durchdenken und Zuständigkeiten festzulegen. Vorsorge war schon immer besser als Nachsorge – das gilt für die Handlungsfähigkeit im Krisenfall einmal mehr. ■

Fazit und Ausblick

Auch in dieser Ausgabe der Datenklaustudie kann von Entwarnung keine Rede sein. Es ist nicht übertrieben, Cyberangriffe und Datenklau als Normalität in deutschen Unternehmen zu bezeichnen, wenn 100 Prozent der Befragten damit rechnen, dass sich die Lage in den nächsten zwei Jahren noch verschlimmern wird.

Zu dieser Wahrnehmung trägt nicht nur das eigene Erleben bei, sondern auch die mediale Verarbeitung der Situation. Auch außerhalb der Fachmedien gehört die Berichterstattung über gewaltige Datenlecks, Lösegeldforderungen in mehrstelliger Millionenhöhe und wochenlange Unterbrechungen in Betrieben und der Verwaltung zum Alltag.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) kam in seinem Lagebericht 2022 zu einer entsprechenden Bewertung: Die zuvor angespannte Lage habe sich weiter zugespitzt, die Bedrohung im Cyberraum sei so hoch wie nie. Insbesondere für Unternehmen liege die Hauptbedrohung weiterhin in den Ransomware-Angriffen und den damit verbundenen Lösegeldforderungen.

Wie intensiv, professionell und effizient Cyberkriminelle ihrer „Arbeit" nachgehen, zeigt auch die Zahl der Varianten von Schadprogrammen: Laut BSI haben sich diese zwischen Juni 2021 und Mai 2022 um rund 117 Millionen vermehrt. Die in unserer Studie befragten Führungskräfte können das nur bestätigen, denn sie vermuten hinter einem Großteil der Angriffe das organisierte Verbrechen als Tätergruppe.

Dementsprechend lautet eine zentrale Erkenntnis der Studie, dass das Wissen über die aktuelle Gefahrenlage, darüber, welche Schäden potenziell drohen und wie sich Unternehmen schützen können, deutlich zugenommen hat. Angriffstechniken sind ebenso bekannt wie die vielen wirkungsvollen Verteidigungsmechanismen.

Dennoch scheint gerade die Prävention nicht der Bedrohung zu folgen. Noch immer investieren die Unternehmen überwiegend in die Klassiker der IT-Sicherheit, in Firewalls, VPN-Zugänge oder Antivirensoftware. Schon die Multifaktor-Authentifizierung fällt deutlich ab, noch stärker Maßnahmen wie Zero-Trust-Umgebungen.

Starke Zuwächse sind dort zu beobachten, wo es um die Reaktion auf einen erfolgreich durchgeführten Angriff geht. Deutlich mehr Unternehmen als 2021 sind jetzt gegen Cyberrisiken versichert, viele weitere planen den Abschluss einer solchen Police. Auch Krisenpläne für den Fall der Fälle sind öfter vorhanden: 2021 verfügten 52 Prozent darüber, 2023 sind es bereits 70 Prozent. Nur beim Einüben hapert es noch etwas, nicht einmal zwei Drittel trainieren den Ernstfall.

> Cyberangriffe und Datenklau gehören zur neuen Normalität in deutschen Unternehmen.

Was bedeutet das für die Zukunft?

Vor allem Ransomware-Attacken werden auch in Zukunft zu den größten Cyberrisiken gehören, denn diese Form des Angriffs ist – man kann es nicht anders ausdrücken – ein funktionierendes Geschäftsmodell. Mit der Hilfe neuer Technologien und Kriminellen, die nicht selbst die Angriffe führen, sondern die Mittel dazu entwickeln und feilbieten, wird sich der Täterkreis vergrößern und die Zahl der Angriffe erhöhen.

Die Täter sitzen außerdem in mehrfacher Hinsicht am langen Hebel. Wer Daten erbeutet hat, kann erstens Lösegeld für die Entschlüsselung fordern, zweitens mit Veröffentlichung drohen – was wieder mit Geld abgewendet werden kann – und drittens die Kunden des gehackten Unternehmens bedrohen.

Vor diesem Hintergrund wundert es nicht, dass die Zahl der Führungskräfte gesunken ist, die ihr Unternehmen für ausreichend gegen Cyberangriffe und Datenklau abgesichert halten. Damit ist die Hausaufgabe für die Unternehmen klar: mehr in Prävention investieren und dort Hilfe hinzuziehen, wo es zu aufwendig wäre, die Expertise selbst aufzubauen. Bereits gut die Hälfte der Unternehmen hat Dienstleister mit dem Schutz vor Informationsabfluss betraut.

Und wenn es zum Ernstfall kommen sollte, gehört mit zur Wahrheit, dass es nicht genügt, Krisenpläne zu haben. Unternehmen sollten auch in der Lage sein, sie routiniert umzusetzen.

Wir sind jetzt schon auf die Ergebnisse unserer nächsten Studie gespannt.

100%

… der Befragten gehen davon aus,
dass die Gefahr für ihr Unternehmen, Opfer von Cyberangriffen/Datenklau zu werden, steigen wird.

Cyber Incident Response
Passgenaue Lösungen im Kampf gegen Datenklau

Um Cybersecurity kommt kein Unternehmen herum

Doch wo anfangen? Zunächst sollten Sie sich folgende Fragen stellen:

- Sind die persönlichen Daten Ihrer Kunden und Ihr Kern-Know-how geschützt?
- Wissen Sie, was wirklich in Ihren Netzwerken vorgeht?
- Kennen Sie die ersten Schritte und Maßnahmen für eine rasche Krisenreaktion?
- Betreiben Sie ein systematisches Informationssicherheitsmanagement?
- Treffen Sie bei Unsicherheit und hohem Zeit- und Handlungsdruck die richtigen Entscheidungen?

Je öfter Sie mit Nein antworten müssen, desto dringender sollten wir uns unterhalten.

EY ist seit vielen Jahren ein weltweit führender Anbieter für Cybersicherheit sowie für digitale Forensik und Investigation und bündelt die Kompetenzen eines globalen Netzwerks. Transparenz, Integrität und Effizienz – darum muss es bei der Prävention, der Detektion und der Reaktion in Bezug auf Krisensituationen gehen. Dafür stehen unsere Leistungen und darauf zielen sie ab, ganz gleich ob wir dabei Routinetätigkeiten übernehmen oder Sie aktiv bei der Abwehr von Angriffen unterstützen.

Krisen managen, Vertrauen stärken

Zur Etablierung eines erfolgreichen Krisenmanagements helfen wir Ihnen, relevante Risiken zu identifizieren und zu bewerten. Unsere Fachleute erstellen gemeinsam mit Ihnen geeignete Präventionskonzepte, bauen eine effektive Krisenmanagementorganisation auf und qualifizieren Ihre Funktions- und Entscheidungsträger.

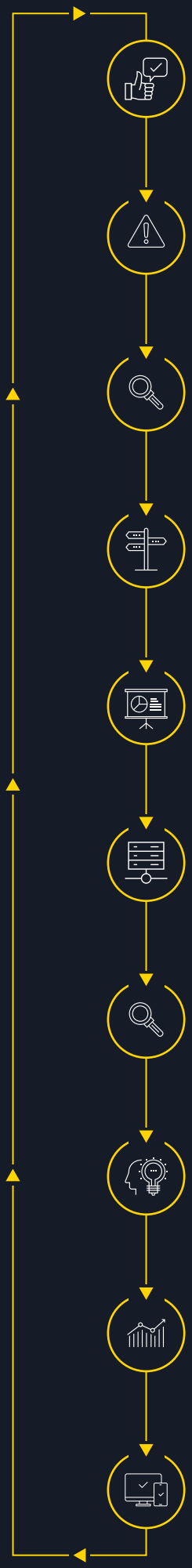
Unser Ziel ist es, Risiken zu minimieren, Ihre Krisenfestigkeit zu erhöhen, Ihnen im Ernstfall Stabilität zu geben und Vertrauen aufzubauen. Wir möchten, dass Sie auf unerwartete Ereignisse mit Schadenspotenzial schnell und effektiv reagieren und sich so Wettbewerbsvorteile sichern können. Außerdem beraten wir Sie natürlich auch umfassend während konkreter Krisenereignisse und danach.

Wie wir Ihnen bei der Abwehr digitaler Attacken helfen – Schritt für Schritt

Wir begleiten Cybersicherheitsvorfälle von Anfang bis Ende, in enger Abstimmung mit den Kunden und vielen internen Ansprechpartnern – je nach Dringlichkeit auch rund um die Uhr.

Der folgende typische Ablauf zeigt, wie genau die Ad-hoc-Reaktion mit den Auftraggebern funktioniert.

Der zehnte Schritt ist idealerweise auch der vorgeschaltete erste Schritt, denn ein prophylaktisch abgeschlossenes Master Service Agreement verkürzt die Reaktionszeit im Ernstfall immens. ■



0. Ideale Vorbereitung (optional)

Mit Abschluss eines Rahmenvertrags können wir im Falle eines Cybervorfalls noch schneller reagieren. Zur idealen Vorbereitung gehören auch Workshops, in denen wir Ihr Unternehmen, Ihr Krisenteam und Ihre IT-Infrastruktur besser kennenlernen.

1. Meldung des Cybersicherheitsvorfalls an EY

Der Anruf geht bei der EY-Incident-Response-Hotline ein und wird an einen Spezialisten weitergeleitet.

2. Scoping-Prozess

Es erfolgt ein erster Lagebild-Anruf, um die Situation einschätzen zu können und festzustellen, wie EY Sie am besten unterstützen kann.

3. In Transit

Während unser Cyber-Incident-Response-Team anreist, unterstützen Sie unsere Kollegen aus dem Fachbereich bereits zusätzlich per Telefon/Video.

4. Planung

Gemeinsam entwickeln wir eine Strategie, um das Unternehmen zu schützen und den Geschäftsbetrieb aufrechtzuerhalten.

5. Datensicherung

Die Datensicherung relevanter Systeme wird forensisch fundiert durchgeführt und dokumentiert.

6. Analyse und Eindämmung

Die gesicherten Daten und Systeme werden zielgerichtet analysiert, Strategien zur Eindämmung werden entwickelt und umgesetzt.

7. Gewonnene Erkenntnisse

Anhand der gewonnenen Erkenntnisse werden Maßnahmen zur Optimierung der IT-Sicherheit identifiziert und ausgearbeitet.

8. Bericht

Es wird ein umfassender Bericht mit den gewonnenen Erkenntnissen erstellt.

9. Wiederherstellung (optional)

Wir unterstützen Sie auch nach dem Vorfall, zum Beispiel bei der Wiederherstellung der Systeme oder der Optimierung/Neustrukturierung der IT-Infrastruktur.

Als qualifizierter

BSI APT-Response-Dienstleister

im Sinne § 3 BSIG hilft Ihnen unser erfahrenes Team, erste Maßnahmen bei komplexen Cyberangriffen zu ergreifen und sicher durch die Krisensituation zu navigieren.

24/7-Hotline für schnelle Hilfe bei einem Cyberangriff:

0800 2323 273

ir@de.ey.com

Was wir für Ihr Unternehmen tun können

Unser erfahrenes Team zur Bekämpfung von Cybervorfällen hilft Ihnen, erste Maßnahmen bei komplexen Cyberangriffen zu ergreifen und sicher durch die Krisensituation zu navigieren – von der technischen Untersuchung über die Begleitung von möglichen Gerichtsverfahren bis hin zu regulatorischen Maßnahmen (z. B. Meldepflichten).

Erfahren Sie mehr über unsere Leistungen:

Reaktion und Datenschutz bei Cybervorfällen

https://www.ey.com/de_de/assurance/privacy-cyber-response

Unser Portfolio:

- Just-in-Time-Unterstützung vor Ort oder remote zur zügigen Identifizierung von Cyberangreifern, einer schnellen Eindämmung des Angriffs sowie Verdrängung der Angreifer aus dem IT-Netzwerk – auch als Retainer-Service
- Post Breach Support: Identifikation und Klassifikation geleakter Daten, um erforderliche datenschutzrechtliche Maßnahmen richtig, vollumfänglich und zeitgerecht durchführen zu können
- ERP Health Check zur Prüfung der Betroffenheit Ihres zentralen ERP-Systems, um nachhaltige Störungen auszuschließen und das Vertrauen in die Finanzsysteme aufrechtzuerhalten
- PMO-Support zur Abwicklung der komplexen Krisenlage eines Cyber-Incidents und Orchestrierung der relevanten Stakeholder wie C-Suite, IT, Legal Department, HR, Public Relations und anderer
- Unterstützung bei der Zusammenarbeit/Kommunikation mit einzubindenden Regulatoren, Strafverfolgungsbehörden oder auch Nachrichtendiensten
- Vorschlag verbesserter Abwehrmaßnahmen zur Steigerung der IT-Sicherheit und Verringerung des Risikos weiterer Cyberangriffe

Ansprechpartner

Bodo Meseke
Partner
Forensic & Integrity Services
EY Global Forensics Cyber Response Leader

Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Mergenthalerallee 3-5
65760 Eschborn

+49 6196 996 22174
bodo.meseke@de.ey.com

Thomas Koch
Partner
Forensic & Integrity Services
Digital Forensics & Incident Response (DFIR) Service Leader

Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Mergenthalerallee 3-5
65760 Eschborn

+49 681 2104 17324
thomas.s.koch@de.ey.com

Impressum

Konzept, Design and Realisation
MEDIENMASSIV, Stuttgart (medienmassiv.com)

Bildquellen
Getty Images International (gettyimages.de)
Unsplash (unsplash.com)

EY | Building a better working world

Mit unserer Arbeit setzen wir uns für eine besser funktionierende Welt ein. Wir helfen unseren Kunden, Mitarbeitenden und der Gesellschaft, langfristige Werte zu schaffen und das Vertrauen in die Kapitalmärkte zu stärken.

In mehr als 150 Ländern unterstützen wir unsere Kunden, verantwortungsvoll zu wachsen und den digitalen Wandel zu gestalten. Dabei setzen wir auf Diversität im Team sowie Daten und modernste Technologien in unseren Dienstleistungen.

Ob Assurance, Tax & Law, Strategy and Transactions oder Consulting: Unsere Teams stellen bessere Fragen, um neue und bessere Antworten auf die komplexen Herausforderungen unserer Zeit geben zu können.

In Deutschland finden Sie uns an 20 Standorten.

Creative Design Germany | BKL 2305-006
ED None

de.ey.com/eyforensics