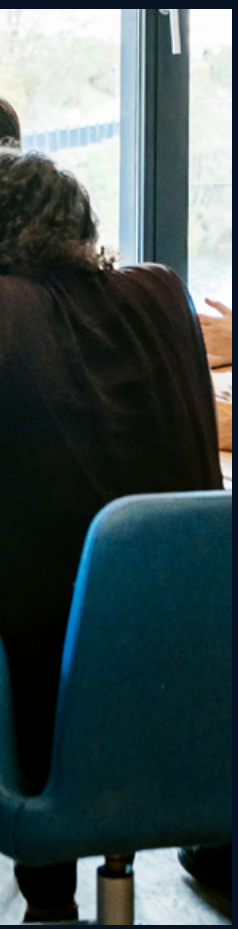
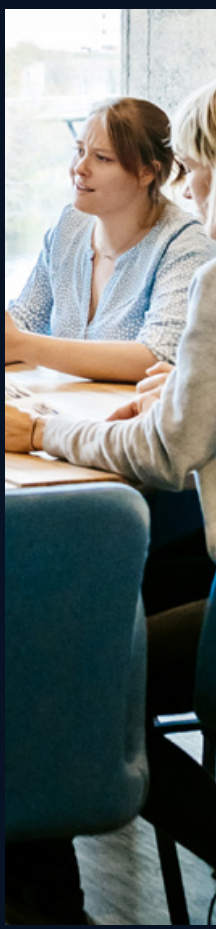
Cyberangriffe und Datendiebstahl: virtuelle Gefahr – reale Schäden

Eine Befragung von 200 österreichischen Unternehmen

Building a better working world

Inhalt





Vorwort

der Autoren von EY

Aufgrund der raschen Verbreitung von COVID-19 haben viele Unternehmen im letzten Jahr ohne entsprechende Vorbereitungszeit auf Telearbeit umgestellt. Das heißt, Tausende Menschen auf der ganzen Welt sind von einem Firmen- oder privaten Laptop aus mit dem Firmennetz verbunden. Diese Arbeitsweise kann für viele Unternehmen zum Risikofaktor werden: Neue Software musste installiert werden und private Laptops sind nicht mit derselben Software geschützt wie Firmen-PCs. Programme funktionieren nicht, IT-Mitarbeiter:innen versuchen, dies remote zu lösen, und dabei können Schwachstellen in der IT-Umgebung entstehen.

Cyberkriminelle können diese Situation ausnützen, vor allem über Betrugsszenarien wie Fake President, bei denen Betrüger:innen E-Mails mit Überweisungsaufträgen im Namen der vermeintlichen Chefetage verschicken. Die Mitarbeiter:innen sind einer Ausnahmesituation ausgesetzt und hinterfragen eventuell Mails und Anfragen nicht mehr; dies ist gerade für Phishing-Mails ein fruchtbarer Nährboden. Außerdem kann auch Malware jetzt über Schwachstellen ins Unternehmen kommen, diese könnte jedoch erst dann aktiviert werden, wenn wieder alles auf Normalbetrieb läuft.

Wie hat es bereits Konfuzius gesagt? „In allen Dingen hängt der Erfolg von den Vorbereitungen ab." Deshalb ist es so wichtig, bestmöglich vorbereitet und ausgerüstet zu sein. Bei jeder Form von Angriff und Datenklau kommt es darauf an, schnell und systematisch reagieren zu können. Die Reaktionsfähigkeit muss regelmäßig trainiert werden. Höchste Zeit also, dass sich Unternehmen die permanente Bedrohung bewusst machen und ihre Bemühungen um eine stabile und erfolgreiche Abwehr gegen Cyberangriffe und Datenklau verstärken. Denn auch Cyberkriminelle bereiten sich immer besser auf Angriffe vor. Oft werden Kunden über Tage und Wochen ausspioniert, um dann im entscheidenden Moment kontaktiert zu werden. Phishing-Mails enthalten bereits interne Informationen und sind immer öfter in perfektem Deutsch geschrieben.

Es ist alles andere als hilfreich, wenn Cyberangriffe und Datendiebstahl vertuscht und nicht ausreichend verfolgt werden, weil Unternehmen Angst vor negativen Folgen für das eigene Image haben. Denn der Schaden, der im Fall von Cyberangriffen und Datendiebstahl droht, kann für Unternehmen immens sein: Die Täter:innen haben es mittlerweile überwiegend auf Kundendaten und Know-how abgesehen – beides gehört zu den wichtigsten Werten eines Unternehmens. Hinzu kommt, dass die Bedrohungen aus dem Netz definitiv weiter ansteigen werden, wenn neue Technologien wie Blockchain und künstliche Intelligenz (KI) in unserem Arbeiten fest verankert sein werden; sie können sich sogar vervielfachen. Im Darknet wird schon länger mit „Crime as a Service" geworben und Kriminalität als Dienstleistung verkauft.

Mehr zum Thema Cyberkriminalität sowie alle Zahlen, Details und Expertenmeinungen finden Sie auf den nachfolgenden Seiten dieser Studie.

Thomas Breuss
Rechtsanwalt und Director
bei EY Law Österreich

Drazen Lukac
Leiter Technology Risk und
Cybersecurity bei
EY Österreich

Gottfried Tonweber
Leiter Cybersecurity
und Data Privacy bei
EY Österreich

Benjamin Weissmann
Leiter Cyberforensik
bei EY Österreich

Vorwort

KSÖ-Präsident Mag. Hameseder

Sehr geehrte Damen und Herren,

das Bundesministerium für Inneres (BMI) hat im März 2021 erste Zahlen zur Entwicklung der Kriminalität in Österreich im Jahr 2020 veröffentlicht. Diese lassen sich in einem klaren Satz zusammenfassen: Während die Gesamtkriminalität signifikant zurückgeht (minus 11,3 %), steigt die Cyberkriminalität dramatisch an (plus 26,3 %). Dies bestätigt einen schon über mehrere Jahre auffallenden Trend des spürbaren Anstiegs von Cyberkriminalität – 2020 verstärkt durch den Digitalisierungsturbo in Zeiten der Pandemie.

Als Präsident des KSÖ, das sich seit nunmehr 10 Jahren im Rahmen der Cybersicherheitsinitiative gemeinsam mit dem BMI mit den unterschiedlichsten Aspekten und Entwicklungen in der Cybersicherheit beschäftigt, sehe ich drei konkrete Handlungsfelder:

Erstens brauchen wir die besten technischen Instrumente und Lösungen für die Abwehr von Cyberangriffen. Dazu ist es wichtig, in Forschung und Innovation zu investieren und gerade auf europäischer Ebene die Möglichkeiten gemeinsamer Forschungs- und Entwicklungsprogramme zu nutzen.

Zweitens benötigen wir die Fachkräfte, die diese Instrumente und Technologien im konkreten unternehmerischen Umfeld anwenden können. Das Thema Fachkräfte ist seit langem Gegenstand intensiver Diskussionen von politisch Verantwortlichen und Expert:innen. Gerade in den Bereichen Cybersicherheit und sichere Digitalisierung ist der Fachkräftebedarf besonders dringend.

Drittens geht es um Vertrauen – Vertrauen der Kund:innen und Partner:innen, dass die Unternehmen bestmöglich auf Risiken und Herausforderungen vorbereitet sind. Das gilt insbesondere für die Cybersicherheit. Das KSÖ hat Anfang 2021 gemeinsam mit Partnern ein Cyber Trust Label präsentiert. Dieses Label ist das erste breit ausgerollte Gütesiegel für Cybersicherheit in Österreich. Es hilft Unternehmen – vor allem, aber nicht nur in der kritischen Infrastruktur –, die Cybersicherheit ihrer Lieferketten zu verifizieren und bietet KMU die Chance, ihre hohen Standards in den Bereichen Cybersicherheit, Business Continuity Management und Datensicherheit transparent und nachvollziehbar zu kommunizieren.

Mit der vorliegenden Studie „Cyberangriffe und Datendiebstahl" leistet EY einen wichtigen Beitrag, um Herausforderungen zu identifizieren, Probleme zu benennen und zugleich konkrete Lösungen aufzuzeigen. Das ist eine wesentliche Voraussetzung dafür, die Cybersicherheit insgesamt zu stärken und damit Österreich gerade in Zeiten der Krise widerstands- und wettbewerbsfähiger zu machen.

Mag. Erwin Hameseder
Präsident Kuratorium
Sicheres Österreich

Ergebnisse auf einen Blick

70 %

... der befragten Führungskräfte erwarten in Zukunft eine steigende Gefahr durch Cyberangriffe und Datendiebstahl

12 % der Unternehmen haben in den vergangenen fünf Jahren konkrete Hinweise auf Cyberangriffe bzw. Datendiebstahl erhalten, 12 % sogar mehrfach.

29 % der befragten Führungskräfte bereitet die Informationssicherheit des eigenen Unternehmens Sorgen und sie bewerten das Risiko, Opfer von Cyberangriffen bzw. Datendiebstahl zu werden, als eher oder sehr hoch.

Für die Zukunft ihres jeweiligen Unternehmens erwarten 70 % der befragten Führungskräfte eine steigende Gefahr durch Cyberangriffe und Datendiebstahl, mehr als jede vierte Führungskraft (21 %) sieht sogar ein stark steigendes Risiko.

35 % fürchten Angriffe durch organisierte Verbrechergruppen, 34 % sehen ihr Unternehmen durch Hacktivist:innen wie Anonymous gefährdet.

Konkrete Hinweise auf Cyberangriffe bzw. Datendiebstahl gab es zuletzt am häufigsten bei Industrieunternehmen (32 %) und Unternehmen der Energiebranche (30 %).

Die mit Abstand meisten Angriffe sind Hackerangriffe auf die IT-Systeme (40 %): In fast jedem fünften Unternehmen (17 %) gab es eine Attacke, die auf das vorsätzliche Lahmlegen dieser Systeme abzielte.

Bei jedem zweiten Fall (53 %) konnten Spionageangriffe durch das interne Kontrollsystem identifiziert werden. Durch unternehmensinterne Hinweise wurden 21 % der Angriffe aufgedeckt. Jedoch wird trotz interner Kontrollmechanismen und anderer Aktivitäten immer noch fast jeder neunte Angriff (11 %) rein zufällig entdeckt.

Während der Pandemie hat fast jedes dritte Unternehmen seine Cybersecurity-Maßnahmen verschärft, 12 % sogar sehr. Um sich während der Coronakrise vermehrt zu schützen, hat mehr als die Hälfte (59 %) der befragten Unternehmen ihre Mitarbeiter:innen sensibilisiert und neue organisatorische Regelungen aufgesetzt (54 %). Außerdem hat fast die Hälfte der Unternehmen auch ihre IT-Infrastruktur modernisiert (43 %).

Mehr als die Hälfte der Unternehmen hat während der Coronapandemie Ihre Mitarbeiter:innen sensibilisiert.

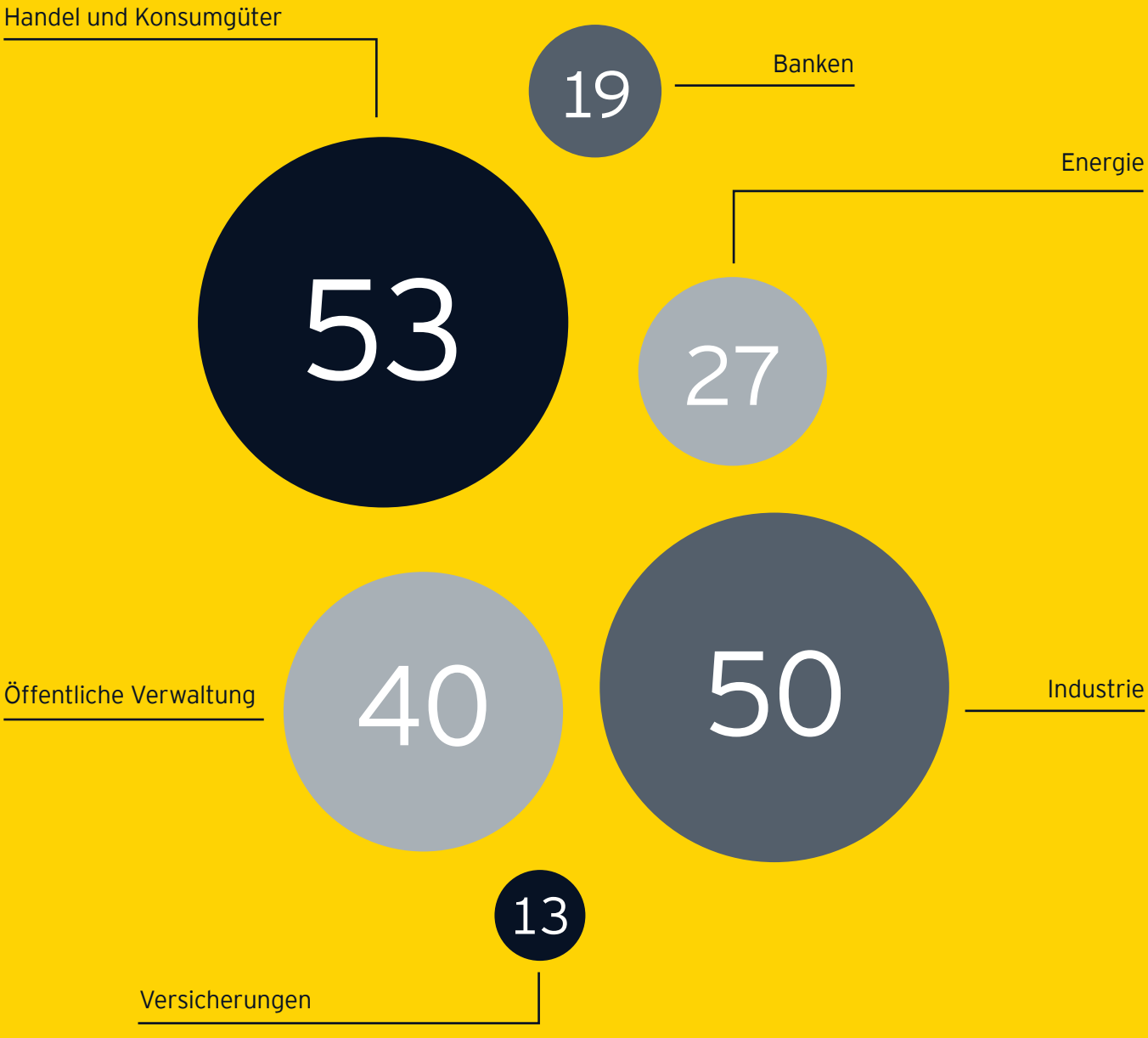
59 %

Design der Studie

Die nachfolgende Studie beruht auf den Ergebnissen einer repräsentativen telefonischen Befragung von 202 Führungskräften österreichischer Unternehmen ab 20 Mitarbeitende. Es wurden Geschäftsführer:innen, Leiter:innen Konzernsicherheit oder Leiter:innen IT-Sicherheit von Unternehmen verschiedenster Größe (gemessen an Mitarbeiterzahl und Umsatzstärke) zum Thema Datenklau befragt.

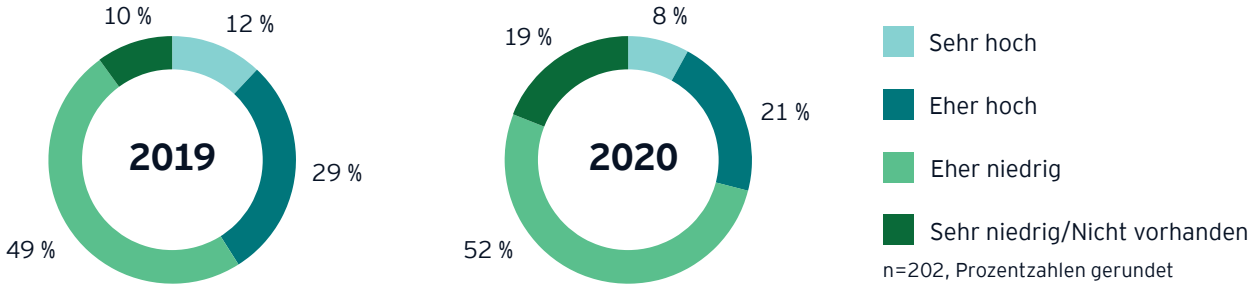
Durchgeführt hat die Befragung das unabhängige Marktforschungsinstitut market Marktforschungs-Ges.m.b.H. & Co.KG, Linz im Jänner 2021. Die Ergebnisse sind repräsentativ für die folgenden Branchen:

Anzahl der befragten Unternehmen je Branche



Einschätzung: Wie hoch ist die Gefährdung? Wie wird sie sich in Zukunft entwickeln?

1.1 Wie hoch schätzen Sie das Risiko für Ihr Unternehmen, Opfer von Cyberangriffen/Datendiebstahl zu werden?



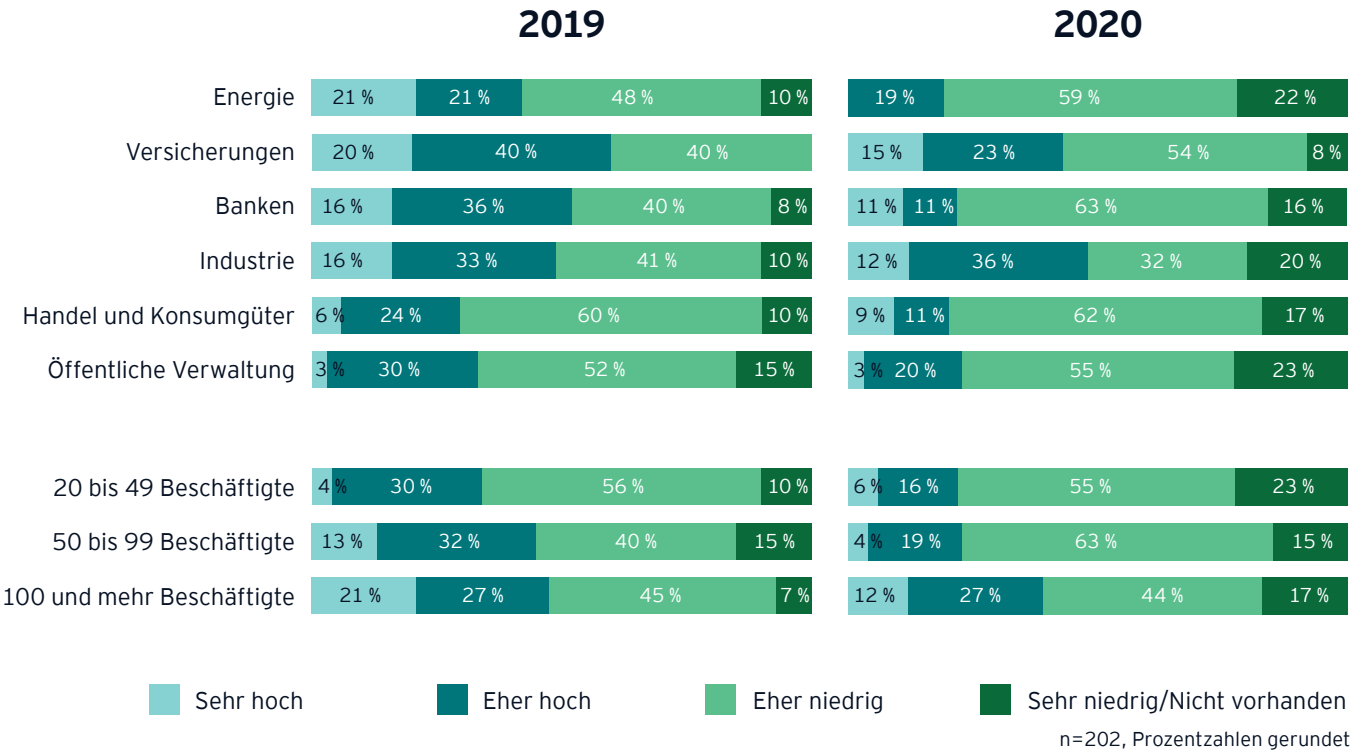
n=202, Prozentzahlen gerundet

Weniger als ein Drittel der Manager:innen bewertet das Risiko, Opfer von Cyberangriffen bzw. Datendiebstahl zu werden, als eher oder sehr hoch. Dabei zeigt sich, dass der Trend für dieses Gefahrenbewusstsein seit der letzten Befragung im vergangenen Jahr leicht gesunken ist. Viele Manager:innen erwarten, dass sie ihre gesteigerten Investitionen in Cybersicherheit unverwundbar machen. Dabei werden Angreifer:innen immer professioneller und unauffälliger. Je größer das Unternehmen, desto größer das Risiko: Etwa jedes achte größere Unternehmen (12 %) mit mehr als 100 Beschäftigten schätzt das Risiko, Opfer von Cyberangriffen bzw. Datendiebstahl zu werden, als sehr hoch ein; bei den mittleren und kleineren Unternehmen sind es 4 % bzw. 6 %.

Besonders gefahrenbewusst zeigen sich die Versicherungsbranche und Banken. Hier sehen 15 % bzw. 11 % der befragten Führungskräfte ein sehr hohes Risiko, Opfer von Cyberangriffen bzw. Datenklau zu werden, in der Industrie 12 %, in der Handels- und Konsumgüterbranche 9 %.

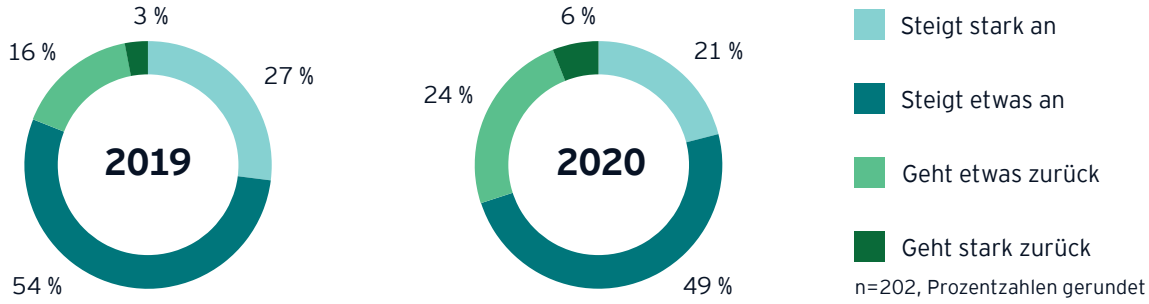
> 29 % der Manager:innen bereitet die Informationssicherheit des eigenen Unternehmens Sorgen – das sind weniger als im letzten Jahr.

Größere Unternehmen sehen ein höheres Risiko



n=202, Prozentzahlen gerundet

1.2 Was meinen Sie, wie wird sich die Bedeutung des Problems Cyberangriffe/Datendiebstahl künftig entwickeln?



n=202, Prozentzahlen gerundet

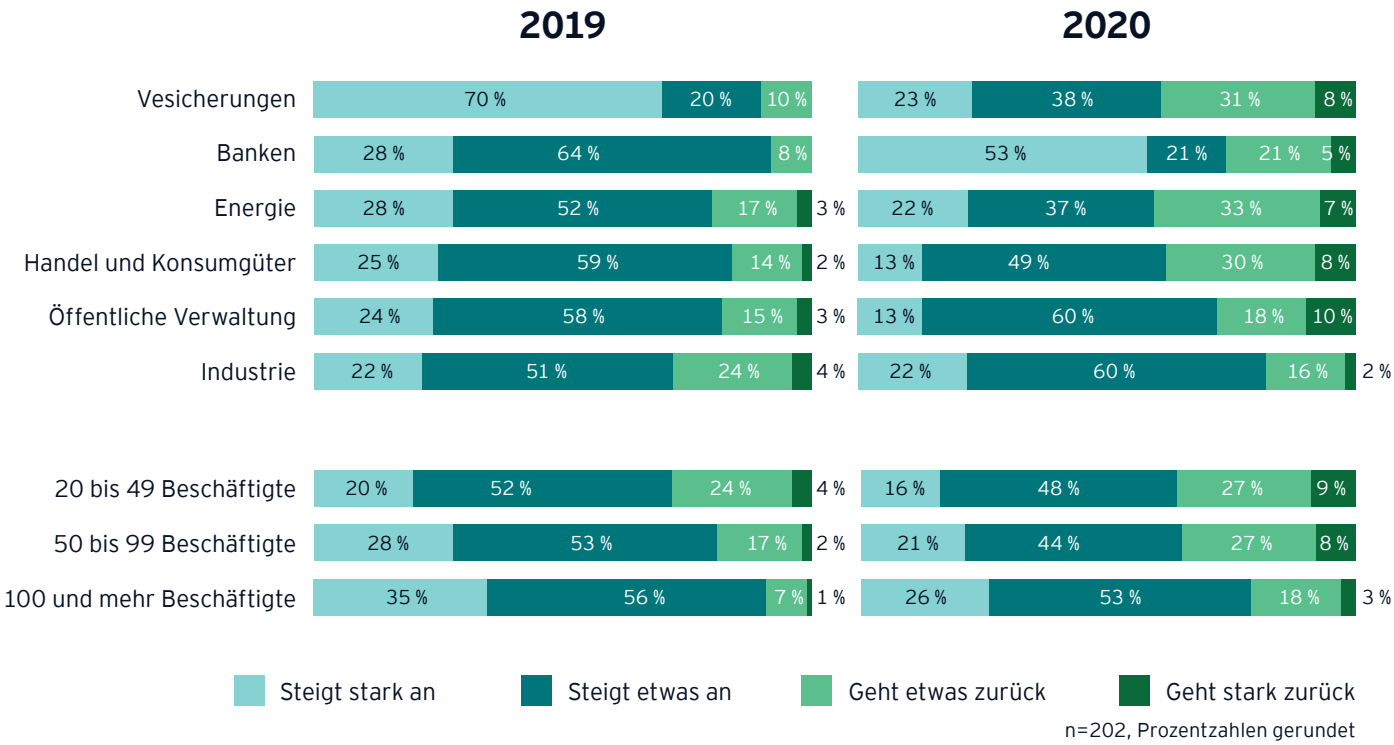
> Immer noch rechnen 70 % der Unternehmen mit einer Verschärfung des Problems.

Auch in der aktuellen Umfrage gehen immer noch 70 % der Befragten davon aus, dass die Gefahr für Unternehmen, Opfer von Cyberangriffen bzw. Datendiebstahl zu werden, weiterhin zunehmen wird. Fast jede vierte Führungskraft sieht sogar ein stark steigendes Risiko. 2019 waren die Zukunftsaussichten noch pessimistischer.

Wie bereits in den Jahren zuvor zeigen sich die Unternehmen alarmiert. Besonders Banken, die bereits jetzt ein verhältnismäßig hohes Risiko sehen, erwarten für die kommenden Jahre eine stark zunehmende Bedrohung.

Jedes vierte größere Unternehmen mit 100 oder mehr Beschäftigten rechnet damit, dass sich die Problematik von Cyberangriffen bzw. Datendiebstahl weiter verschärfen wird. Bei mittleren Unternehmen steigt das Risikobewusstsein an.

Insbesondere Banken sind alarmiert



n=202, Prozentzahlen gerundet

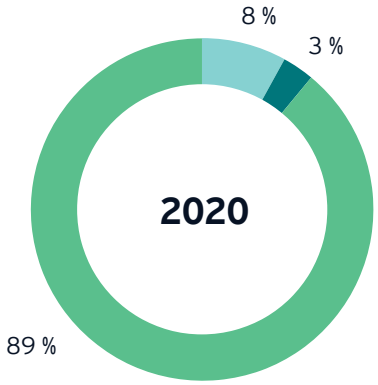
1.3 Gab es jemals Erpressungsversuche gegenüber Ihrem Unternehmen, also Angriffe, bei denen Geld gefordert wurde?

”

8 % der Befragten waren bereits mit einem derartigen Angriff konfrontiert, nur 3 % mehrfach. Für die Angreifer:innen war dies jedoch selten von Erfolg gekrönt.

Eine besondere Form des Cyberangriffs ist der Einsatz von Ransomware oder Erpressungssoftware. Das sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder den Zugriff auf das ganze Computersystem verhindern kann. Für die Entschlüsselung fordern die Angreifer:innen Lösegeld.

8 % der Befragten waren bereits mit einem derartigen Angriff konfrontiert, nur 3 % mehrfach. Für die Angreifer war dies jedoch selten von Erfolg gekrönt: 9 % der Unternehmen möchten nicht sagen, ob sie bezahlt haben, 91 % haben dem Druck der Erpresser:innen nicht nachgegeben.



Ja, einmal | Ja, mehrfach | Nein, noch nie

n=202, Prozentzahlen gerundet

Falls ja, haben Sie bezahlt?

Wie hoch war der durchschnittlich höchste Schaden pro Datendiebstahl?

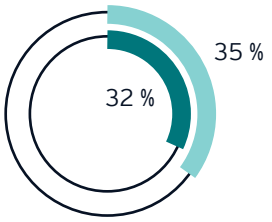
2019

n=202, Prozentzahlen gerundet

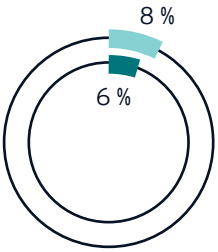
2 Risikopotenziale und Tätergruppen

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

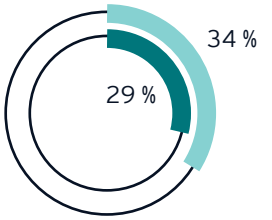
Besonders gefürchtet: organisierte Kriminalität



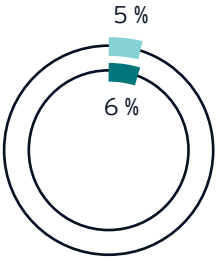
Organisierte Kriminalität
(z. B. Manipulation von Transaktionen)



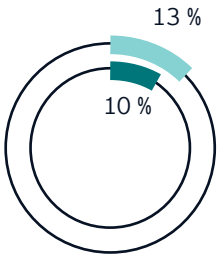
Eigene Mitarbeiter:innen



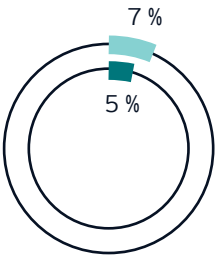
Hacktivist:innen
(z. B. Anonymous)



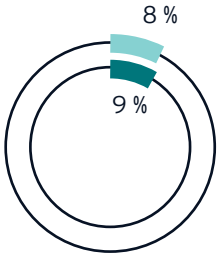
Konkurrierendes inländisches Unternehmen



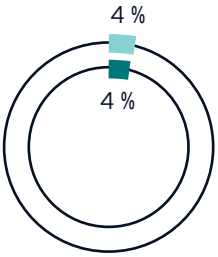
Ausländischer Geheimdienst bzw.
staatliche ausländische Stelle



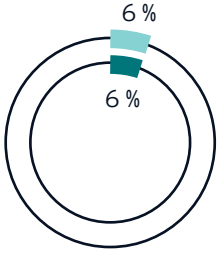
Ausländische Kund:innen
oder Lieferanten



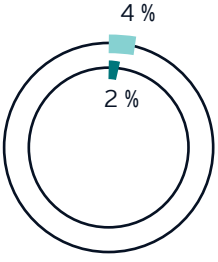
Konkurrierendes ausländisches
Unternehmen



Inländische Kund:innen
oder Lieferanten



Ehemalige Mitarbeiter:innen



Sonstige Geschäftspartner:innen

2019 2020

n=202, Prozentzahlen gerundet

> Österreichische Unternehmen fürchten insbesondere, Opfer von organisierter Kriminalität zu werden. So bewertet jede dritte Führungskraft dieses Risiko als hoch oder sehr hoch.

Im Vergleich zu 2019 ist das Risikobewusstsein der österreichischen Unternehmen teilweise gestiegen oder gleich geblieben. Viele heimische Manager:innen fühlen sich durch Investitionen in die Cybersicherheit besser gegen Angriffe gerüstet und schätzen die Gefahr als geringer ein.

Österreichische Unternehmen fürchten insbesondere, Opfer von organisierter Kriminalität zu werden. So bewertet jede dritte Führungskraft dieses Risiko als hoch oder sehr hoch.

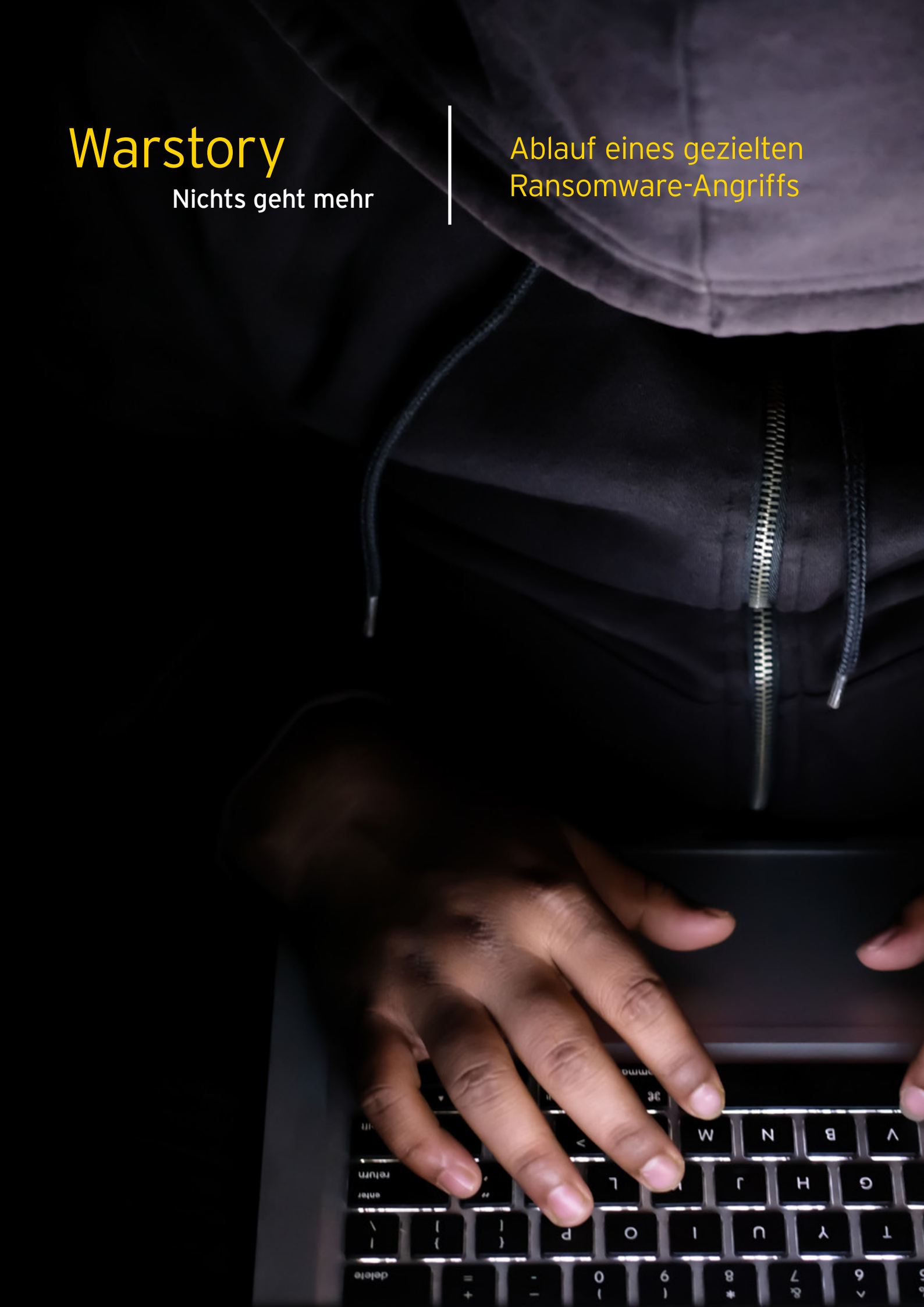
Auch das Risiko, von Hacktivist:innen oder ausländischen Geheimdiensten/staatlichen ausländischen Stellen geschädigt zu werden, wird als vergleichsweise hoch eingeschätzt.

Als gefährlich stufen die Befragten auch wieder den Datendiebstahl durch eigene Mitarbeiter:innen ein. Der Anteil ist von 6 % auf 8 % gestiegen. Die Weiterbildung und Schulung von Mitarbeitenden ist hier wichtig, um zu einem stärkeren Bewusstsein zu führen.

Warstory

Nichts geht mehr

Ablauf eines gezielten Ransomware-Angriffs



Montag, 11. Jänner 2021

6.47 Uhr
Anruf Auslieferungslager Nord bei IT-Bereitschaft: PC-Arbeitsplätze gestört, keine Anmeldung möglich. Bereitschaftsmitarbeiterin bricht zur Zentrale auf. Unterwegs gehen weitere Meldungen ein.

7.19 Uhr
Bereitschaftsmitarbeiterin trifft in Zentrale ein. Kurze Prüfung ergibt: Server und PCs lassen keine Anmeldung mehr zu. Neustart des Domain-Controllers ohne Effekt. Abteilungsleiter nicht erreichbar. Bereitschaftsmitarbeiterin alarmiert IT-Team per Smartphone.

7.49 Uhr
Bei weiterer Prüfung der Server wird Nachricht entdeckt: Kriminelle haben System kompromittiert und Kontrolle übernommen. Wesentliche Bereiche der Systeme sind verschlüsselt. Täter:innen haben nach eigenen Angaben interne Dokumente gestohlen und drohen mit Veröffentlichung. Neben Lösegeldforderung ist eine Mail-Adresse zur Kontaktaufnahme angegeben.

7.55 Uhr
Weitere Mitarbeiter:innen der IT treffen ein und versuchen, Zugang zu Servern zu erlangen. Gelingt nur teilweise, essenzielle Daten scheinen tatsächlich verschlüsselt zu sein.

Ein solches oder ähnliches Szenario könnte heute praktisch jede Organisation treffen. Als Beispiel haben wir uns hier ein mittelständisches Unternehmen aus der Fertigungsindustrie ausgedacht. Das Unternehmen ist fiktiv, die Vorkommnisse sind es nicht. Was wir hier schildern, sind reale Ereignisse aus Krisensituationen, bei denen unser „Computer Emergency Response"-Team (CERT) und unser Krisenmanagementteam (KM-Team) Mandanten beraten und unterstützt haben.

Wird ein Unternehmen Opfer eines Ransomware-Angriffs, ist schnelles, aber bedachtes Handeln von entscheidender Bedeutung. Bereits in diesem frühen Stadium des hier beschriebenen Angriffs ist eine effiziente und strukturierte Kommunikation, intern wie extern, gefordert. Kundenbeschwerden, Fertigungsausfälle oder ein erheblicher Reputationsschaden könnten schon jetzt die Folge sein. Die Entscheidungsträger:innen des Unternehmens, aber auch wichtige Akteur:innen wie IT, etwaige Krisenteams oder die bzw. der Compliance-Beauftragte müssen umgehend über den aktuellen Sachverhalt informiert werden.

Darüber hinaus müssen zahlreiche Fragen beantwortet und Entscheidungen getroffen werden: Kann der Cyberangriff durch die eigenen IT-Teams abgewehrt und aufgeklärt werden? Muss die Internetverbindung getrennt werden? Ist die Unternehmenskommunikation den Anforderungen einer sich schnell entwickelnden Krisensituation gewachsen?

In vielen Fällen ist es sinnvoll, so früh wie möglich externe Unterstützung hinzuzuziehen. So können beispielsweise CERTs, KM-Teams und spezialisierte PR-Berater:innen wertvolle Unterstützung leisten und helfen, Folgen abzumindern und Fehler zu vermeiden. Auch eine spezialisierte Rechtsberatung kann essenziell sein, damit das Unternehmen im Umgang mit dem Angriff und seinen Folgen nicht in rechtliche Grauzonen gerät.

In unserem Beispiel entschließt sich der Vorstand nach der ersten Lagebesprechung, neben einem Fachanwalt auch ein DFIR-Team (Digital Forensics & Incident Response) hinzuzuziehen.

Montag, 11. Jänner 2021

14.10 Uhr
Eintreffen DFIR-Team. Leiter trifft Vorstand und Fachanwalt. Team beginnt Arbeit mit der IT-Administration zur Gewinnung eines aktuellen Lagebildes. Parallel starten weitere Teammitglieder mit Internet- und Darknet-Recherche zur Identifizierung möglicher Angriffsvektoren.

14.17 Uhr
CCO erhält Anruf eines Journalisten, der nach internen Dokumenten fragt, die angeblich auf einer Enthüllungsplattform aufgetaucht sind. Recherche ergibt: Zwei vertrauliche Vorstandsprotokolle wurden dort veröffentlicht. CCO informiert Vorstand.

14.28 Uhr
DFIR-Team beginnt forensische Sicherung befallener Systeme und Logdaten. Auswertung von Datensicherungen zur Analyse von Art und Umfang des Angriffs. Trennung des Servers vom Unternehmensnetzwerk.

17.36 Uhr
Krisenstab ist eingerichtet und beginnt mit der Koordination der Aktivitäten. IT-Plattform zur Herstellung und Aufrechterhaltung des Lagebildes vom KM-Team bereitgestellt.

19.11 Uhr
PR-Berater eingetroffen, beraten Krisenstab zur Kommunikationsstrategie. Zielgruppen werden analysiert. Mitteilungen für interne und externe Kommunikation werden erstellt, Media-Monitoring eingerichtet.

Die Lage bleibt bei dem hier beschriebenen Ransomware-Angriff weiterhin kritisch. Zentrale Daten-, Infrastruktur- und Backup-Server sind betroffen, fast alle wesentlichen Daten sind verschlüsselt. Es wurden aber auch erste Hinweise zur Angriffstechnik gefunden. Von einem Multifunktionsdrucker (MFD) im Vorstandssekretariat erfolgten verdächtige Anmeldungen. Die Daten dieses Geräts werden gerade forensisch gesichert. Außerdem wurde die eingesetzte Verschlüsselungstechnik analysiert.

Eine Entschlüsselung ohne Schlüssel scheint ausgeschlossen. Arbeiten in einer Krisensituation viele Akteur:innen zusammen, müssen Zuständigkeiten und Abläufe klar definiert sein. Erkenntnisse aus der fortlaufenden Untersuchung müssen kontinuierlich einbezogen und eine Fülle von Fragen beantwortet werden.

Soll das Lösegeld gezahlt werden? Falls ja, wie werden kurzfristig große Mengen Bitcoins beschafft? Welche rechtlichen Aspekte gibt es zu bedenken, beispielsweise Geldwäschevorschriften oder Sanktionsrecht? Wie gestaltet sich die Involvierung von Sicherheitsbehörden? Bis wann und in welchem Umfang muss die Meldung an Aufsichtsbehörden bzw. Regulatoren erfolgen? Welche Informationen werden wann und wie veröffentlicht, sei es innerhalb des Unternehmens, für die Kund:innen oder für die Öffentlichkeit?

In unserem Beispiel kommt erschwerend hinzu, dass sensible Dokumente auf einer Enthüllungsplattform aufgetaucht sind und weitere Veröffentlichungen drohen. Angesichts dieser neuen Dimension an Komplexität entschließt sich der Vorstand, ein professionelles KM-Team einzubinden und sich auch in Sachen Öffentlichkeitsarbeit von erfahrenen Berater:innen unterstützen zu lassen. Parallel schaltet der Vorstand die Strafverfolgungsbehörden ein. Das zuständige Bundeskriminalamt (BKA) entsendet umgehend Beamt:innen, um den Sachverhalt aufzunehmen und das weitere Vorgehen zu besprechen.

Dienstag, 12. Jänner 2021

9.50 Uhr
Die IT hat mit Unterstützung des DFIR-Teams einen vorläufigen Mailserver aufgesetzt. Notsystem ist getrennt vom aktuellen System, verfügt über eigene Sicherheitsinfrastruktur. Mails, insbesondere an unternehmenskritische Adressen, können wieder bearbeitet werden.

10.02 Uhr
CCO beginnt mit seinem Team und PR-Berater, die Fülle an zwischenzeitlich eingetroffenen Presseanfragen zu beantworten. KM-Team unterstützt bei Koordination.

10.03 Uhr
DFIR-Team hat ein Mobile-Incident-Response-System in Betrieb genommen und überwacht das Unternehmensnetzwerk auf verdächtige Aktivitäten. DFIR-Team und IT beginnen, Server und Arbeitsplätze auf Malware und Manipulationen zu überprüfen.

10.05 Uhr
Das Key-Account-Management beginnt, Kund:innen nach Kritikalität der Lieferbeziehung über Ausfälle zu informieren. Kritische Fälle erhalten eine spezielle Mail-Adresse zur Koordination der Notversorgung.

10.10 Uhr
Krisenstab koordiniert an allen angebundenen Standorten die Kontaktaufnahme mit Spezialfirmen, um eine Analyse besonderer Netzwerkgeräte (SCADA, Fertigungstechnik, Facility-Management etc.) zu veranlassen.

10.50 Uhr
IR-Team hat ersten möglichen Angriffsvektor identifiziert: Angebliche Zugangsdaten für Fernwartung des Industrieroboters werden im Darknet gehandelt. Rücksprache mit IT vor Ort bestätigt, dass gefundene Zugangsdaten aktuell sind. Betroffene Kennwörter werden geändert.

An diesem Morgen kommen Vorstand und Krisenstab zu einem weiteren Briefing durch die IT und den Leiter des DFIR-Teams zusammen. Anwesend sind auch die Beamt:innen des BKA. In der vorherigen Nacht wurden die Daten des MFD ausgewertet, der nach aktuellem Kenntnisstand tatsächlich als Angriffsplattform diente. Auf dem Gerät konnten verdächtige Zugriffe einer IP-Adresse identifiziert werden, die sich im Netzwerk eines ausländischen Fertigungsstandorts befindet. Eine entsprechende Anfrage an die dortige IT läuft bereits.

Auf dem MFD wurden zahlreiche Dateien gefunden. Es scheint sich um Kopien aller Dokumente zu handeln, die in den vergangenen zwei Monaten auf diesem Gerät kopiert, gefaxt oder ausgedruckt wurden. Es gibt Hinweise darauf, dass diese Dokumente an einen Server der Angreifer:innen gesandt wurden. Die Dokumente werden derzeit in das eDiscovery-System des DFIR-Teams importiert und mithilfe eines Vorstandsassistenten ausgewertet.

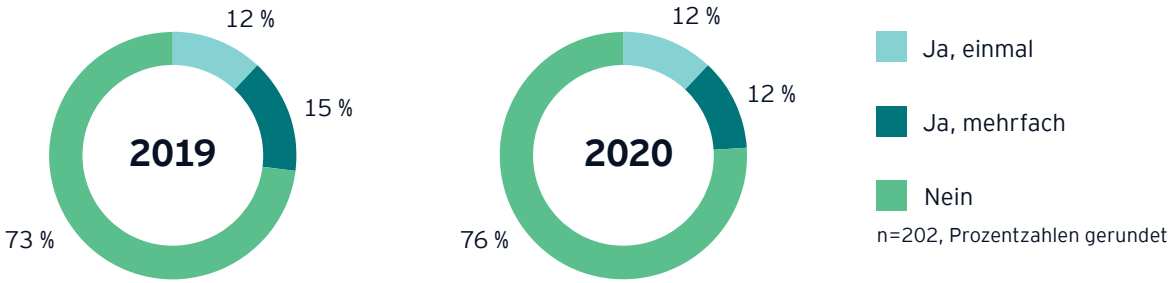
Am Vormittag kommt auch die Rückmeldung des ausländischen Standortes: Die verdächtige IP-Adresse gehört zu einem Steuerungsrechner eines Fertigungsroboters. Das DFIR-Team kontaktiert Kolleg:innen vor Ort und veranlasst eine forensische Sicherung des Geräts. Parallel nimmt der Krisenstab Kontakt mit dem Hersteller auf. Darüber hinaus werden die neuen Informationen mit in die Recherche zu möglichen Angriffsvektoren aufgenommen.

Angesichts der zunehmenden Komplexität und Kritikalität der Lage, verstärkt durch Probleme bei der Just-in-time-Versorgung der Kund:innen, beschließt der Vorstand, das geforderte Lösegeld zu bezahlen. Das BKA übernimmt die Kommunikation mit den Täter:innen. Am Nachmittag stehen die benötigten Bitcoins zur Verfügung. Nach der Übermittlung eines ersten Schlüssels zum Beweis, dass die Täter:innen die Systeme auch tatsächlich entschlüsseln können, wird die Übertragung der Bitcoins veranlasst. Binnen zwei Stunden senden die Erpresser:innen eine E-Mail mit einem ZIP-Archiv, das anscheinend alle benötigten Kryptoschlüssel enthält. Darüber hinaus geben die Täter:innen an, keine weiteren internen Dokumente mehr veröffentlichen zu wollen.

3

Wer wurde Opfer?
Wer sind die Täter:innen?

3.1 Gab es in Ihrem Unternehmen bereits konkrete Hinweise auf Cyberangriffe bzw. Datenklau innerhalb der vergangenen fünf Jahre?



n=202, Prozentzahlen gerundet

Bei einem Viertel der Unternehmen hat es in den vergangenen fünf Jahren konkrete Hinweise auf Cyberangriffe bzw. Datendiebstahl gegeben. Mehr als jedes achte Unternehmen hat sogar Hinweise auf mehrfache Attacken erhalten.

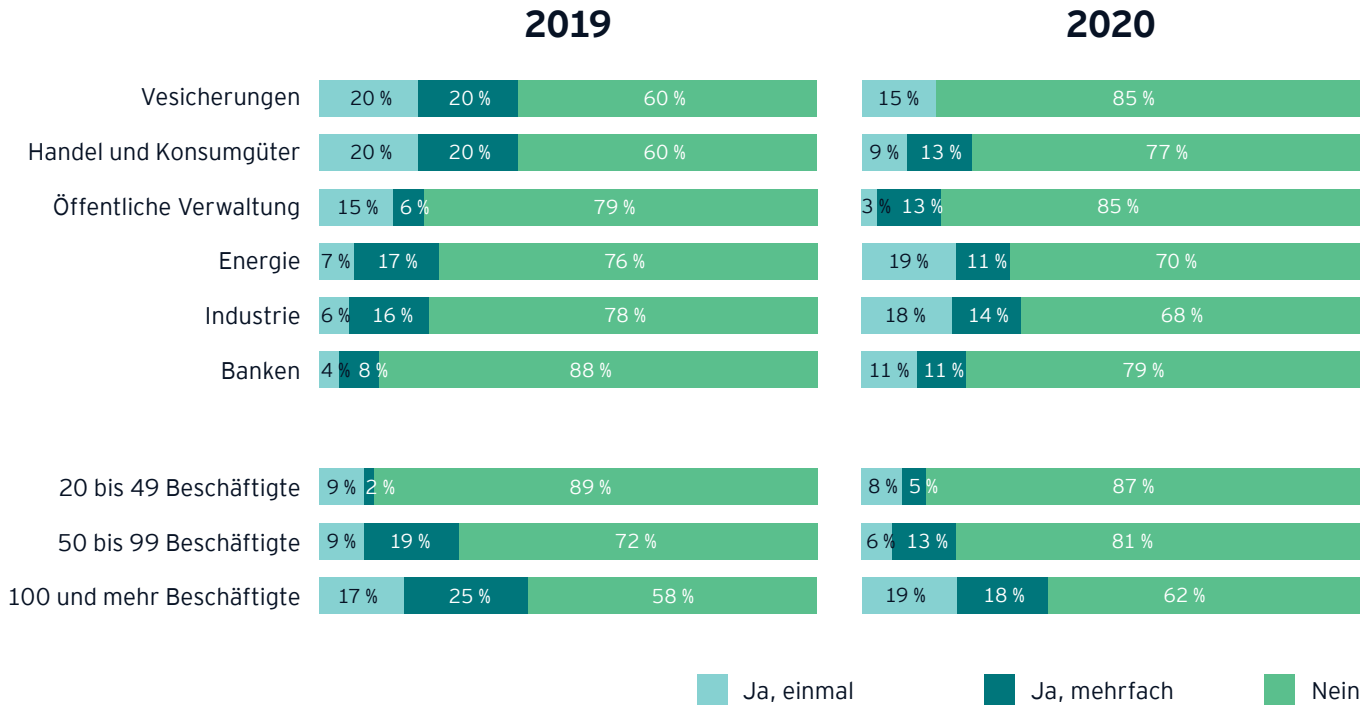
11 % der befragten Unternehmen gaben an, dass kriminelle Handlungen nur durch Zufall aufgedeckt worden seien. Die Dunkelziffer der tatsächlich erfolgten Fälle von Cyberangriffen bzw. Datenklau dürfte demnach deutlich höher sein.

Konkrete Hinweise auf Cyberangriffe bzw. Datendiebstahl gab es zuletzt am häufigsten bei Industrie- und Energieunternehmen. Hier berichten 32 % und 30 % der befragten Führungskräfte von Hinweisen auf Cyberattacken.

Vor allem größere Unternehmen mit 100 oder mehr Beschäftigten hat es besonders getroffen. In 37 % der Unternehmen dieser Größe gab es zuletzt Hinweise auf Attacken. An dieser Stelle ist zu berücksichtigen, dass mit der Größe des Unternehmens die Investitionsbereitschaft in Schutzmechanismen zunimmt. Erst durch diese bereits etablierten und erprobten Schutzmechanismen steigt die Wahrscheinlichkeit, Angriffe zu entdecken.

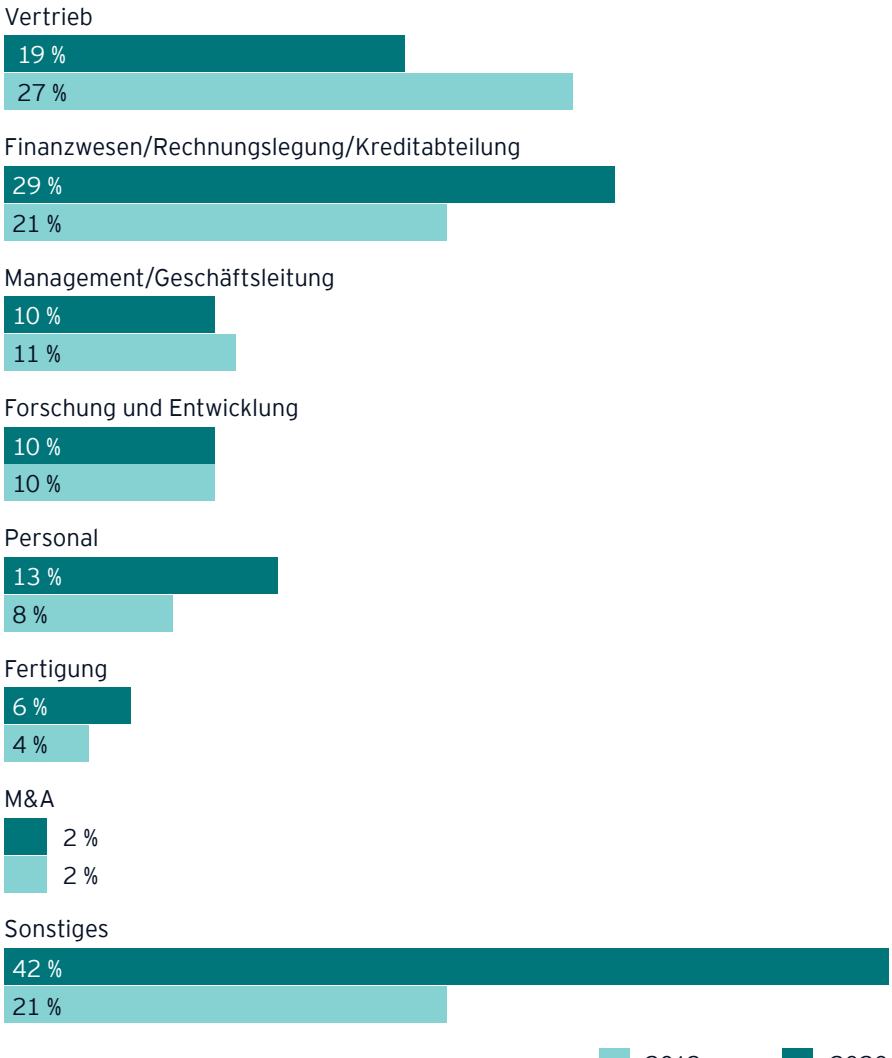
> In mehr als jedem vierten österreichischen Unternehmen gibt es konkrete Hinweise auf Cyberangriffe bzw. Datendiebstahl.

Größere Unternehmen sind deutlich stärker betroffen



n=202, Prozentzahlen gerundet

3.2 Welcher Bereich war vom Datendiebstahl betroffen bzw. wo ergab sich dieser Verdacht?



Häufigkeit der Datendiebstähle je Unternehmensbereich (Mehrfachantworten möglich)

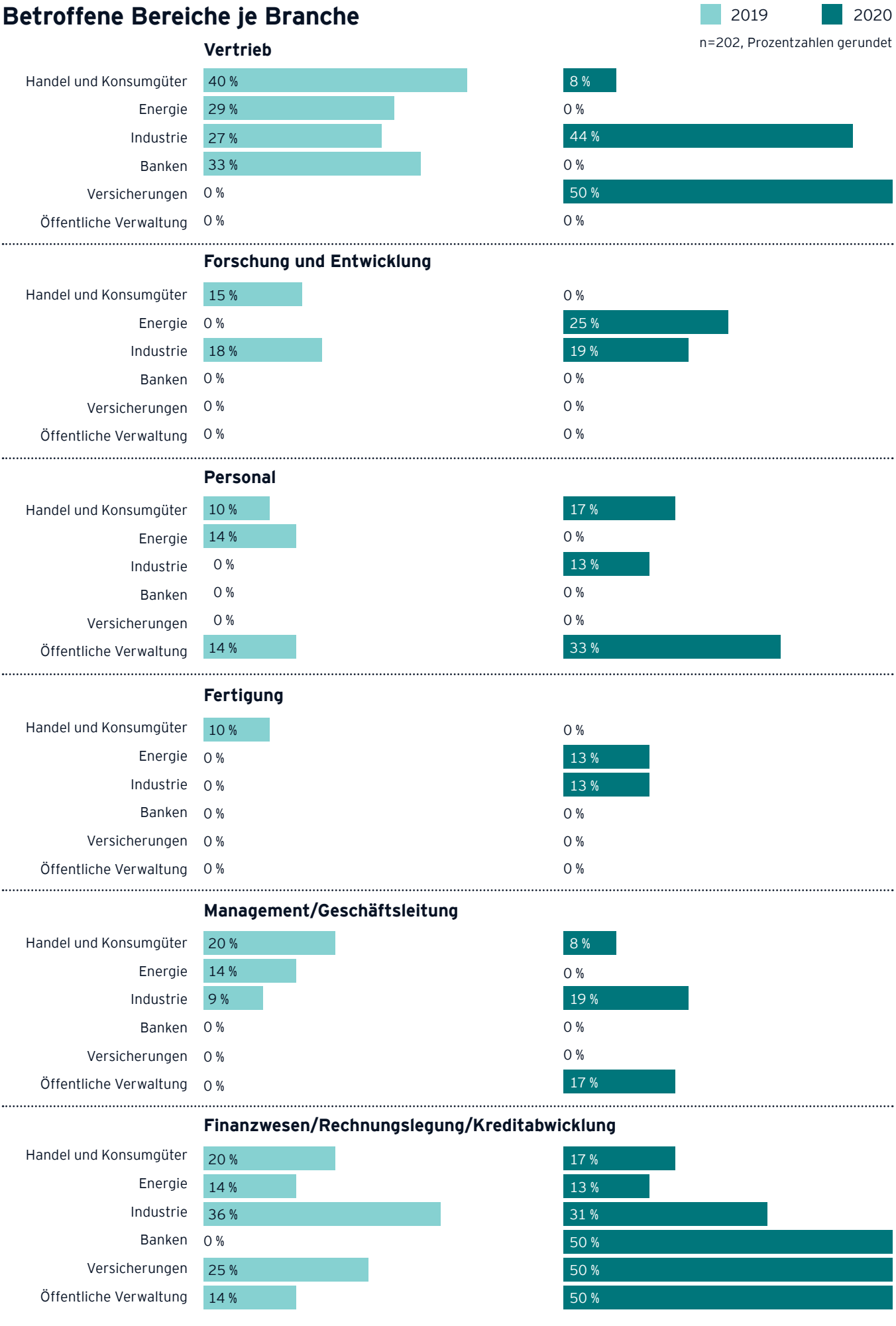
n=202, Prozentzahlen gerundet

> Durch alle Branchen hinweg gibt es ein beliebtes Angriffsziel – das Finanzwesen mit Rechnungslegung und Kreditabteilung.

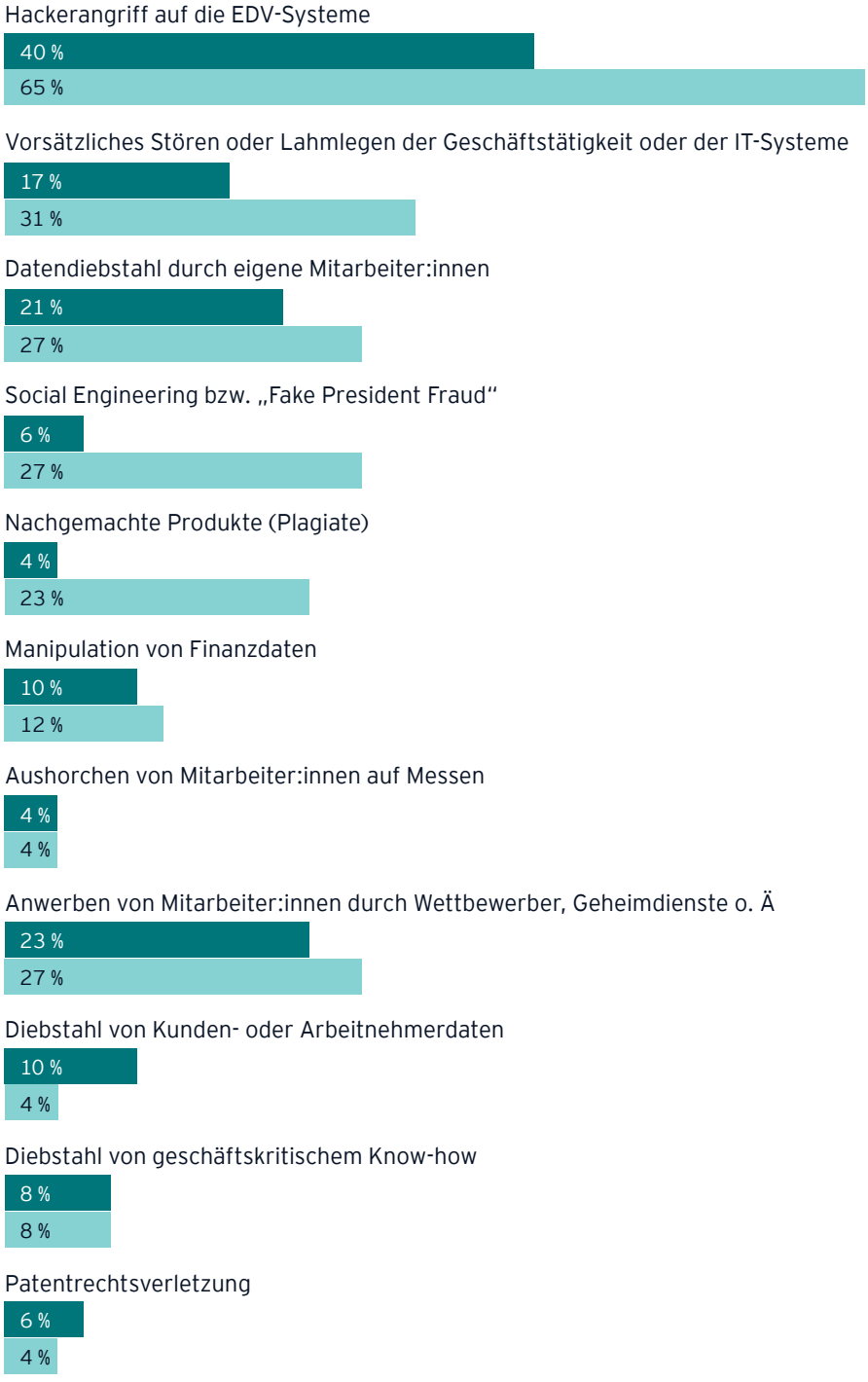
Besonders angriffsgefährdete Stellen im Unternehmen sind das Finanzwesen, das in mehr als jedem vierten Fall betroffen war, und der Vertrieb. Im Finanzwesen gab es im Vergleich zu 2019 einen Zuwachs. Einen erheblichen Rückgang gab es jedoch beim „Fake President Fraud", von 27 % auf 6 %.

Durch alle Branchen hinweg gibt es ein beliebtes Angriffsziel – das Finanzwesen mit Rechnungslegung und Kreditabteilung. Bei Industrieunternehmen und Versicherungen ist auch der Bereich Vertrieb inkl. Kundendaten betroffen. Bei Industrieunternehmen steht zudem der Bereich Forschung und Entwicklung – Stichwort Industriespionage – stärker im Fokus. In der Handel und Konsumgüter-Branche und in der öffentlichen Verwaltung sind auch Personaldaten vermehrt im Visier der Angreifer:innen.

Betroffene Bereiche je Branche

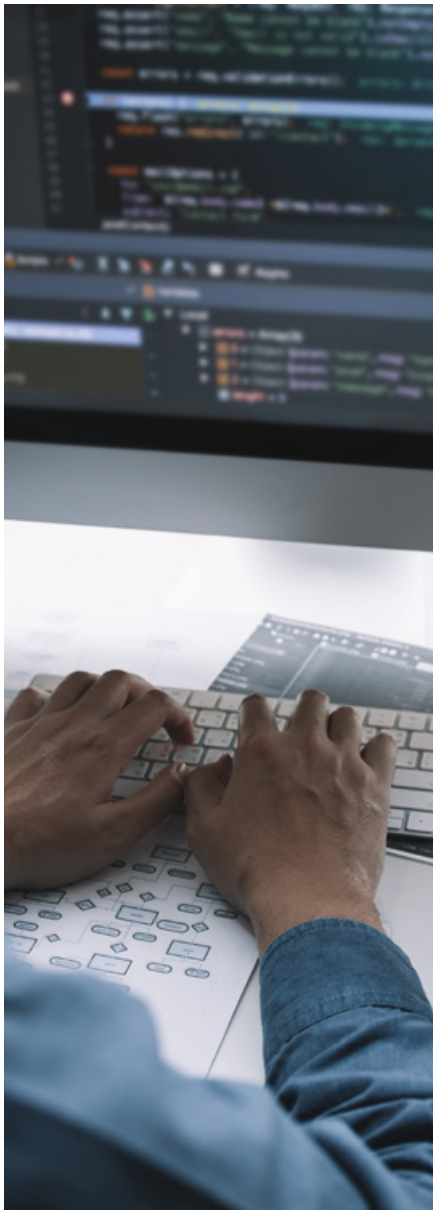


3.3 Welche konkreten Handlungen fanden statt?



n=202, Prozentzahlen gerundet

Basis: Unternehmen, die bereits geschädigt wurden; Mehrfachantworten möglich



Wie bereits in den Jahren zuvor sind die mit Abstand meisten Attacken Hackerangriffe auf die IT-Systeme (40 %). Auch wenn Hackerangriffe auf und das vorsätzliche Lahmlegen von IT-Systemen noch immer am meisten verbreitet sind, sind die Zahlen im Vergleich zum letzten Jahr eindeutig gesunken. Dabei umfasst das vorsätzliche Stören oder Lahmlegen der Geschäftstätigkeiten oder der IT-Systeme auch die Verschlüsselung und den darauf folgenden Verlust des Zugriffs auf die eigenen Daten durch sogenannte Ransomware. Dabei handelt es sich um eine bösartige Schadsoftware (Malware), die den Zugriff auf Daten unmöglich macht und Benutzer:innen auf diese Weise sogar vom Gerät aussperren kann.

> Fast jede dritte Attacke zielte auf vorsätzliches Stören der IT-Systeme ab.

Die Evolution von Ransomware

Aus der Praxis

Ransomware verwehrt Personen oder Unternehmen den Zugriff auf ihre Daten oder Systeme. Ziel dieses Angriffs ist es, anschließend Lösegeld zu erpressen. Die Konsequenzen dieser Attacke(n) sind aber weitreichender als gedacht, da durch die Verschlüsselung der Daten und IT-Systeme Ausfallzeiten in der Produktion auftreten können. Zudem kann ein Diebstahl personenbezogener Daten zu einer Verletzung der Datenschutz-Grundverordnung führen. Zudem müssen Unternehmen strenge Fristen bei Meldungen an den Datenschutz einhalten.

Im Jahr 2017 waren breit gestreute, hochgradig automatisierte Angriffe wie „WannaCry“ an der Tagesordnung, begleitet von als Ransomware getarnten Sabotageangriffen wie „NotPetya“. Heute werden Incident-Response-Teams vermehrt mit deutlich komplexeren Angriffsstrategien konfrontiert.

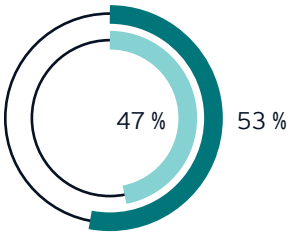
Angriffsziele werden dabei über Wochen und Monate hinweg gezielt ausgespäht. Der tatsächliche Angriff erfolgt schnell und systematisch. Derzeit werden dabei auch unterschiedliche Strategien kombiniert. In einem jüngeren Fall wurden nicht nur kritische Unternehmensdaten verschlüsselt, sondern gleichzeitig sensible Daten gestohlen. Die folgenden Lösegeldforderungen für die Herausgabe der Kryptoschlüssel wurden dann durch die Androhung einer Veröffentlichung der gestohlenen Daten ergänzt. Zusätzlich werden nicht nur die Opfer selbst, sondern auch deren Kund:innen, kontaktiert. Durch dieses Vorgehen erhoffen sich die Angreifer:innen eine höhere Quote an Zahlenden Opfern. Der tatsächliche Schaden für das Unternehmen lag deutlich über der Forderung der Täter:innen.

Diese modernen Angriffsstrategien stellen Verantwortliche vor erhebliche

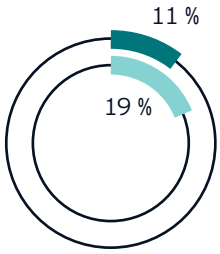
> „Rein technische Sicherheitslösungen reichen nicht aus, Risikoszenarien müssen strategisch betrachtet und Maßnahmen ganzheitlich umgesetzt werden.

Herausforderungen, da hierbei unterschiedlichste Methoden vom klassischen Hacking über maßgeschneiderte Malware bis hin zu Social Engineering eingesetzt werden. Psychologische Aspekte spielen dabei eine immer größere Rolle. Rein technische Sicherheitslösungen reichen nicht aus, Risikoszenarien müssen strategisch betrachtet und Maßnahmen ganzheitlich umgesetzt werden.

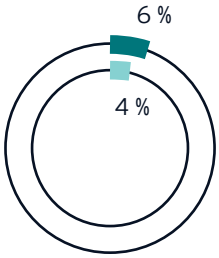
3.4 Wie wurden die kriminellen Handlungen aufgedeckt?



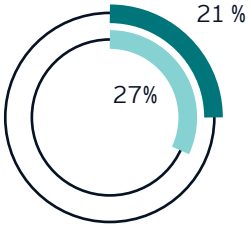
Internes Kontrollsystem



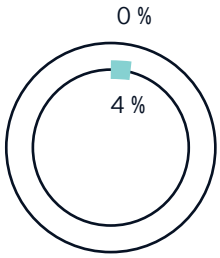
Zufall



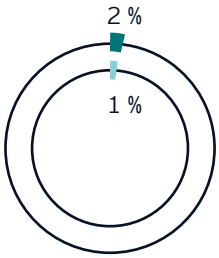
Sonderprüfung durch Dritte



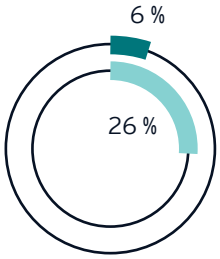
Unternehmensinterne Hinweise



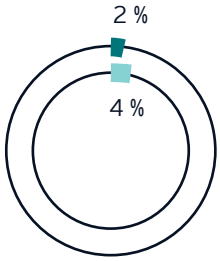
Unternehmensexterne Hinweise



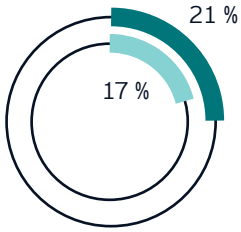
Strafverfolgungs- oder Aufsichtsbehörde



Interne Routineprüfung



Anonyme Hinweise



Sonstiges

2019 2020

n=202, Prozentzahlen gerundet

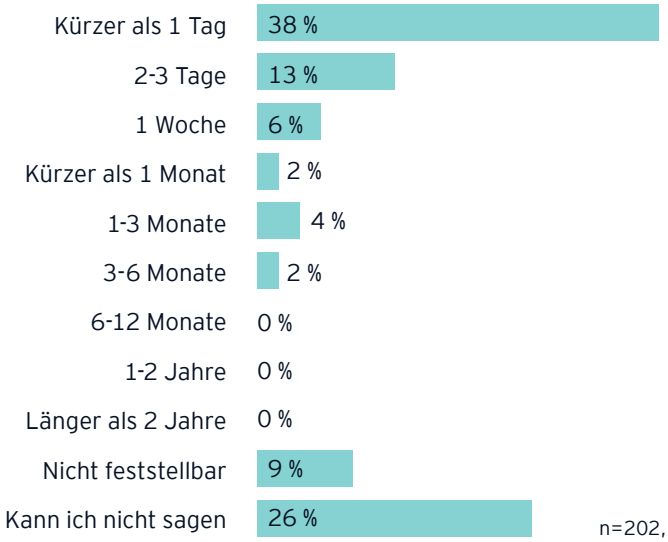
Basis: Unternehmen, die bereits geschädigt wurden; Mehrfachantworten möglich

Wie schon 2019 werden Angriffe in den häufigsten Fällen durch das interne Kontrollsystem identifiziert. Durch interne Routineprüfungen wurden im Vergleich zum letzten Jahr (26 %) nur mehr 6 % der Angriffe aufgedeckt. Die Dunkelziffer nicht aufgedeckter Angriffe wird höher sein, denn trotz interner Kontrollmechanismen und staatlicher Aktivitäten wird gut jeder siebte Angriff rein zufällig aufgedeckt.

”

Mehr als jeder zweite Angriff wird durch das interne Kontrollsystem erkannt.

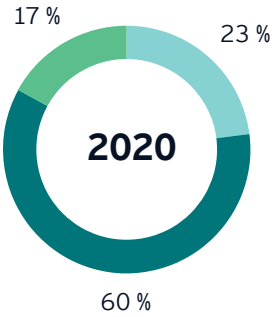
Wie lange war der Angreifer aktiv, bevor der Angriff erkannt wurde?



2020

n=202, Prozentzahlen gerundet

Ist der Angriff außerhalb der Organisation, z. B. bei Kund:innen oder Geschäftspartner:innen, bekannt geworden?



Ja
Nein
Weiß nicht

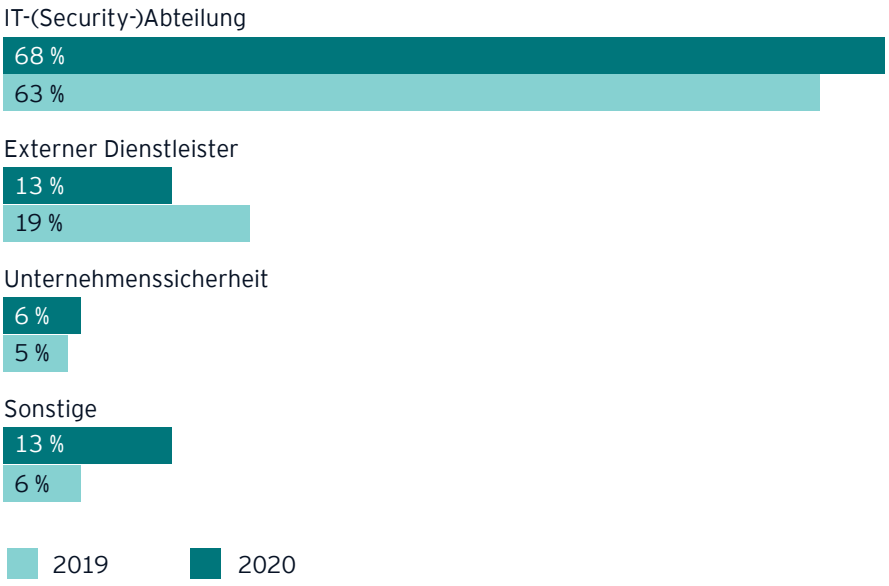
n=202, Prozentzahlen gerundet

3.5 Wer wurde mit der Aufklärung beauftragt?

”

Aufklärer Nummer eins ist die eigene IT-Abteilung, aber: Es wird vermehrt auf externe Dienstleister gesetzt.

Wird ein Cyberangriff bekannt, ist die IT-Abteilung in 68 % der Fälle die erste Anlaufstelle. Im Vergleich zum letzten Jahr werden weniger externe Dienstleister von Unternehmen zur Aufklärung von Angriffen hinzugezogen. Die eigene Unternehmenssicherheit wird in gut jedem 20. Fall mit der Aufklärung des Cyberangriffs beauftragt.

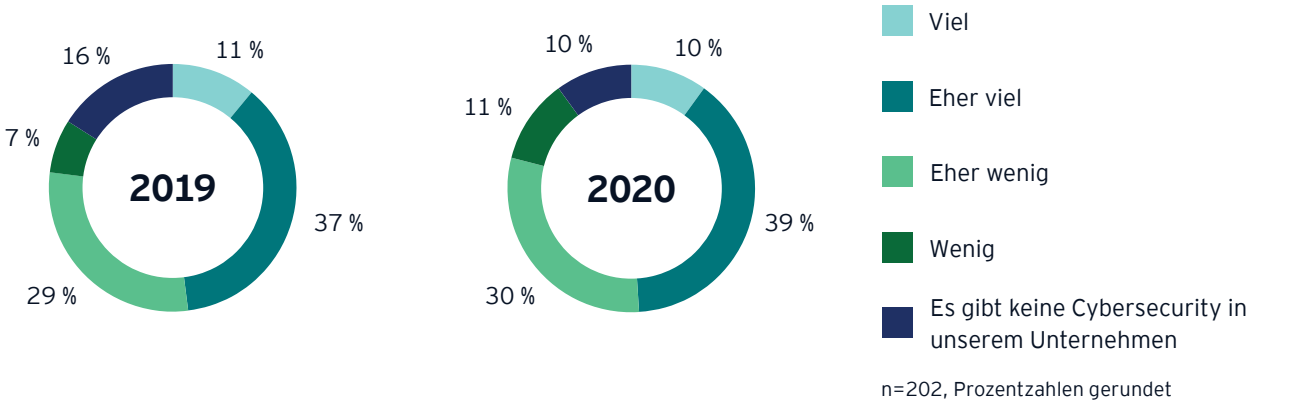


n=202, Prozentzahlen gerundet

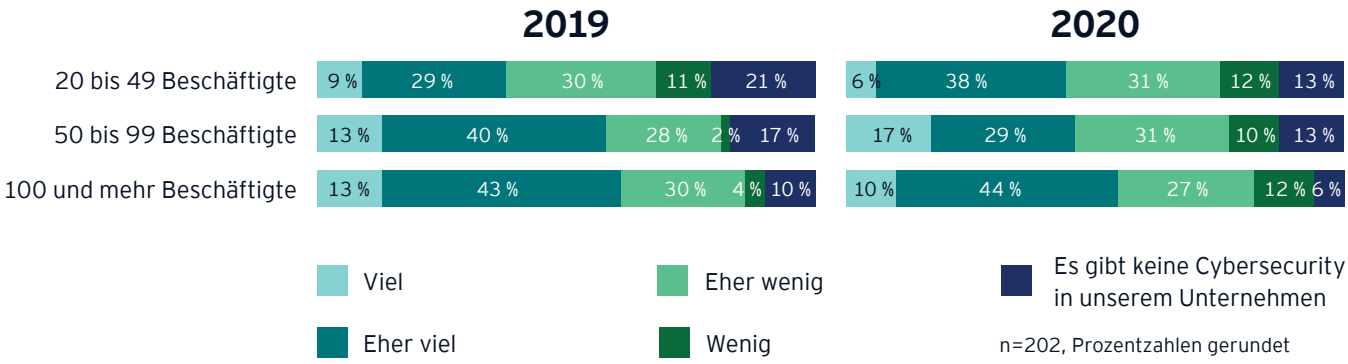
Basis: Unternehmen, die bereits geschädigt wurden

4 Prävention, Abwehr und Aufklärung: Schützen sich die Unternehmen ausreichend?

4.1 Wie viele Ressourcen (Personal, Mittel, Technologie, Budget) stehen Ihnen generell im Bereich Cybersecurity zur Verfügung?



n=202, Prozentzahlen gerundet



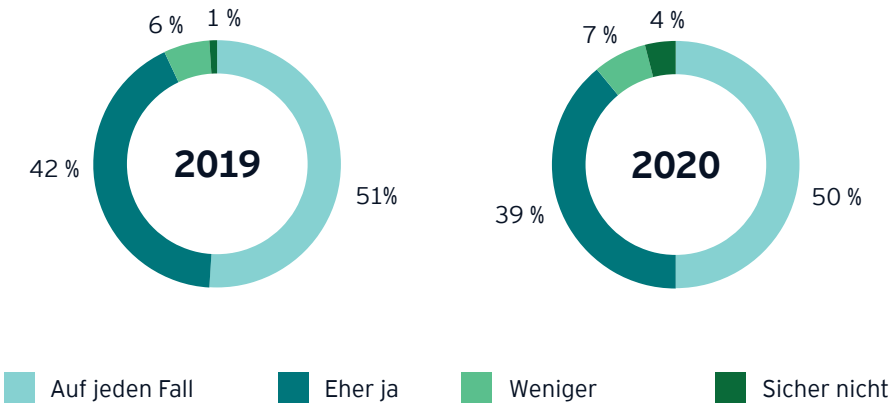
n=202, Prozentzahlen gerundet

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

”

Jedes zweite Unternehmen fühlt sich vollkommen sicher vor Cyberangriffen und Datendiebstahl – mehr als zwei von fünf immerhin „eher“ sicher.

Trotz der Bedrohung fühlen sich 89 % der Befragten zumindest eher gut vor Cyberangriffen und Datendiebstahl geschützt. Vollkommen ruhig schlafen kann allerdings nur jede:r zweite der Befragten. Jede:r neunte hat nach eigener Aussage keine ausreichenden Vorkehrungen getroffen. Die gefühlte Sicherheit ist bei Unternehmen aller untersuchten Branchen und Größen vergleichbar hoch.



n=202, Prozentzahlen gerundet

4.3 Wie hat die Kommunikation in Ihrem Unternehmen nach einem Angriff – insbesondere auch zwischen Abteilungen – funktioniert?

Sehr gut
60 %

Eher gut
40 %

Eher schlecht
0 %

Sehr schlecht
0 %

Für Unternehmen ist Datendiebstahl ein ernst zu nehmendes Risiko. Dabei ist es wichtig, dass die Kommunikation nach einem Angriff innerhalb des Unternehmens und im Bedarfsfall auch extern gut funktioniert. Für mehr als die Hälfte der Befragten ist die Kommunikation zwischen den Abteilungen nach einem Angriff gut gelaufen.

2020

n=202, Prozentzahlen gerundet

4.4 Wie ist die Wiederherstellung des Betriebs und der Sicherheit nach dem Angriff gelaufen?

Gut, der Neuaufbau konnte innerhalb weniger Tage erfolgen
75 %

Eher gut, der Neuaufbau konnte innerhalb einer Woche erfolgen
21 %

Eher schlecht, der Neuaufbau hat mehr als eine Woche in Anspruch genommen
4 %

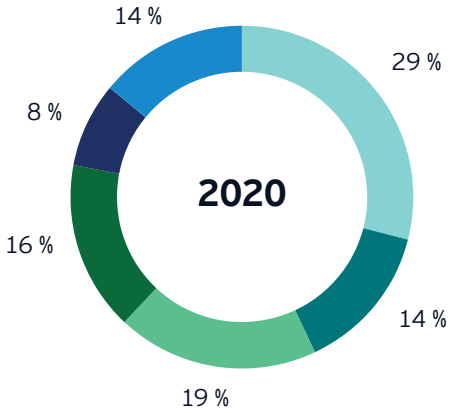
Schlecht, der Neuaufbau hat mehrere Wochen gedauert
0 %

Die Mehrzahl der befragten Unternehmen (75 %) konnte den Betrieb und die Sicherheit innerhalb weniger Tagen wiederaufbauen.

2020

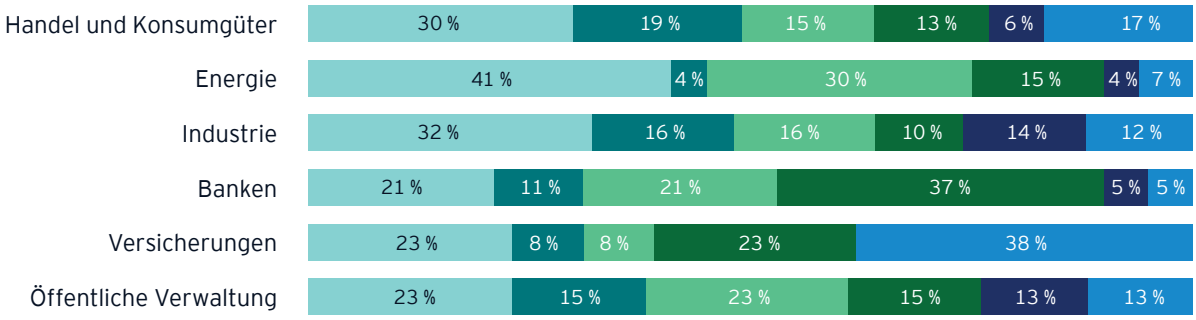
n=202, Prozentzahlen gerundet

4.5 Lässt sich Ihr Unternehmen regelmäßig (extern und/oder intern) auf Schwachstellen im Hinblick auf Cyberangriffe/ Datendiebstahl testen?



- Jährlich
- Halbjährlich
- Quartalsweise
- Monatlich
- Seltener
- Nie, haben wir noch nicht machen lassen

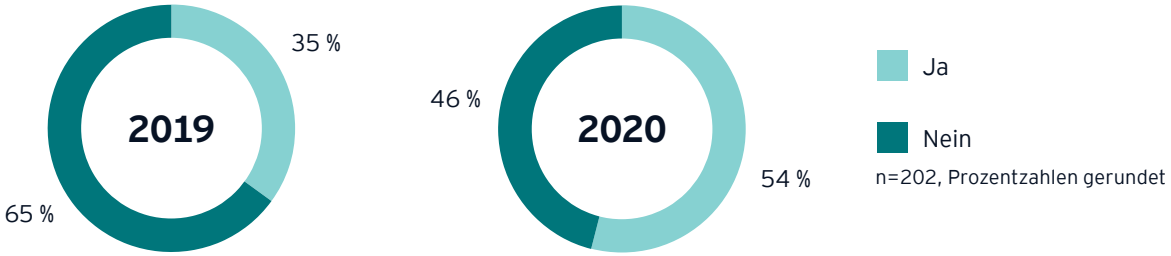
n=202, Prozentzahlen gerundet



- Jährlich
- Halbjährlich
- Quartalsweise
- Monatlich
- Seltener
- Nie, haben wir noch nicht machen lassen

n=202, Prozentzahlen gerundet

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



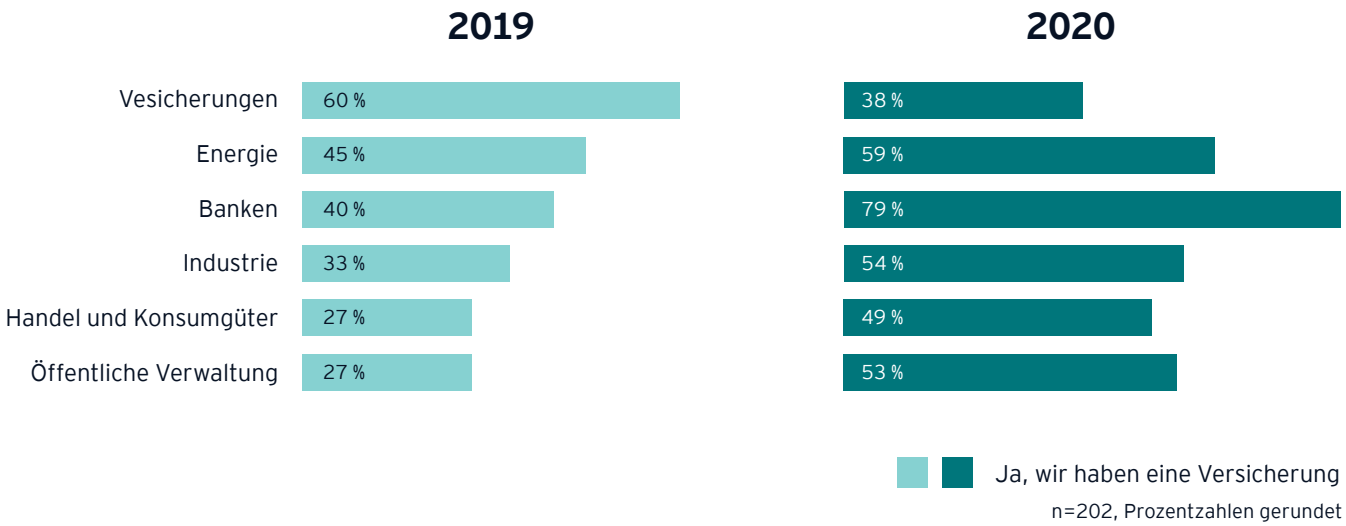
n=202, Prozentzahlen gerundet

”

Mehr als jedes zweite Unternehmen ist gegen digitale Risiken versichert.

Digitale Risiken sind für Unternehmen weiterhin nicht zu unterschätzen. Im Schadensfall können dabei Kosten in Millionenhöhe entstehen. Zum Schutz vor diesen schwerwiegenden Folgen schließen immer mehr Unternehmen Versicherungen gegen Cyberrisiken ab: 54 % der befragten Unternehmen haben inzwischen nach eigenen Angaben eine solche Versicherung abgeschlossen.

Besonders hoch ist der Anteil der Unternehmen mit Versicherungsschutz bei Banken, in der Energiebranche und in der Industrie.



n=202, Prozentzahlen gerundet

5 Auswirkungen der Coronapandemie

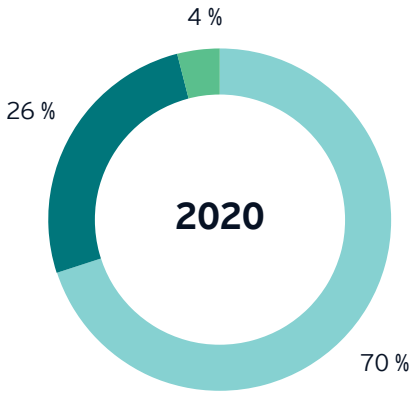
5.1 Haben Ihre Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet?

Ja

Nein

Bei uns ist grundsätzlich kein Homeoffice möglich

n=202, Prozentzahlen gerundet



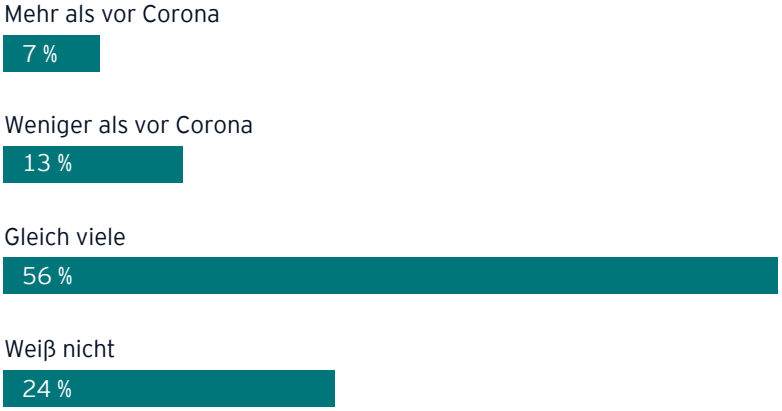
Aufgrund der raschen Verbreitung von COVID-19 haben viele Unternehmen ohne entsprechende Vorbereitungszeit auf Telearbeit umgestellt. Bei sieben von zehn Unternehmen haben die Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet.

5.2 Haben Sie in der Folge der Coronakrise und des Lockdowns Ihre Cybersecurity-Maßnahmen verschärft?

Das Homeoffice kann für viele Unternehmen zum Risikofaktor werden: Neue Software musste installiert werden und private Laptops sind nicht mit derselben Software geschützt wie Firmen-PCs. Programme funktionieren nicht, IT-Mitarbeiter:innen versuchen, dies remote zu lösen, und dabei können Schwachstellen in der IT-Umgebung entstehen. Daher hat etwa jedes dritte Unternehmen seine Cybersecurity-Maßnahmen verschärft, 12 % sogar sehr.

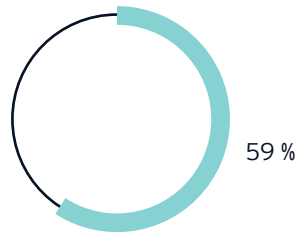
n=202, Prozentzahlen gerundet

5.3 Haben Sie seit dem Ausbruch der Coronakrise und den damit verbundenen Maßnahmen wie vermehrtes Homeoffice eine Veränderung bei Security Incidents bzw. Cyberangriffen (z. B. Phising Mails, SPAM) festgestellt?

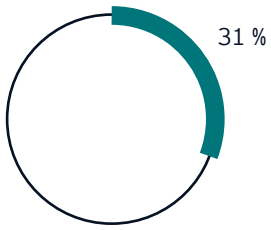


n=202, Prozentzahlen gerundet

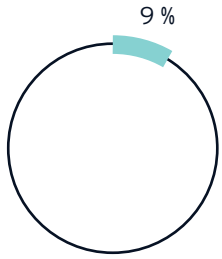
5.4 Wie haben die verstärkten Cybersecurity-Maßnahmen ausgesehen?



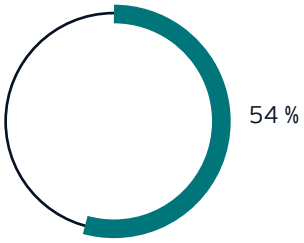
Sensibilisierung der Mitarbeiter:innen



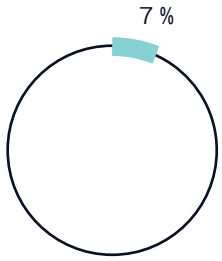
Verschärfung der Sicherheitsrichtlinien/-settings



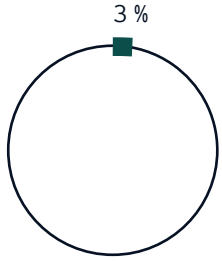
Papierloses Büro bis zum Umzug in die Cloud



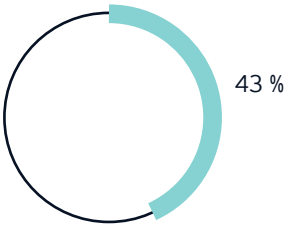
Neue organisatorische Regelung (Policies)



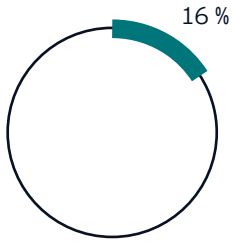
Prozessuale Anpassungen



Andere Maßnahmen



Modernisierung der IT-Insfrastruktur (z. B. neue Tools/Überwachungs-mechanismen)



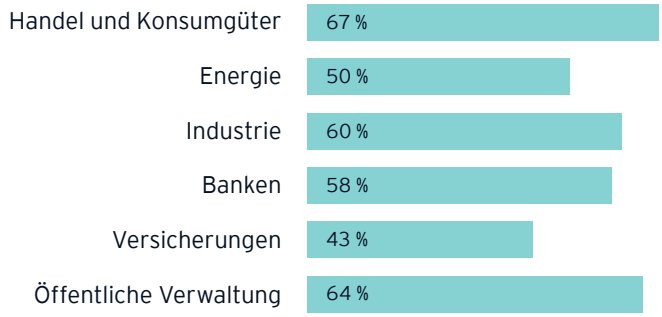
Zusätzliche Software wie Mehrfakto-renauthentifizierung; Intrusion-Preven-tion-/-Detection-Systeme (Systeme, die Hackerangriffe erkennen/abwehren)

n=202, Prozentzahlen gerundet

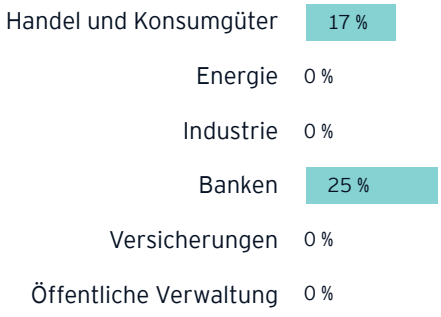
Um sich während der Coronakrise vermehrt zu schützen, haben mehr als die Hälfte (59 %) der befragten Unternehmen ihre Mitarbeiter:innen sensibilisiert und neue organisatorische Regelungen aufgesetzt (54 %). Außerdem hat fast die Hälfte der Unternehmen auch ihre IT-Infrastruktur modernisiert (43 %).

> Über die Hälfte der Unternehmen hat ihre Mitarbeiter:innen während der Coronakrise sensibilisiert und neue organisatorische Regelungen aufgesetzt.

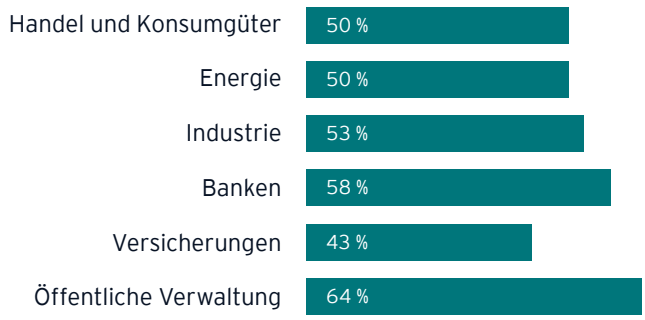
Sensibilisierung von Mitarbeiter:innen



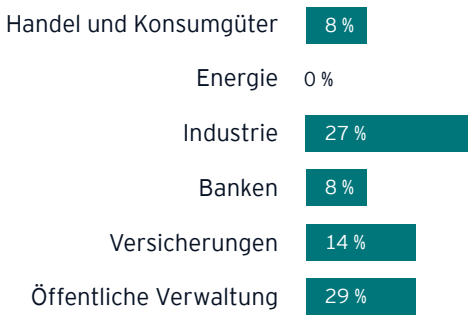
Prozessuale Anpassungen



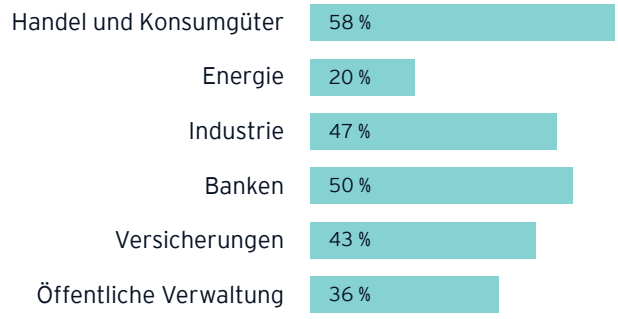
Neue organisatorische Regelungen (Policies)



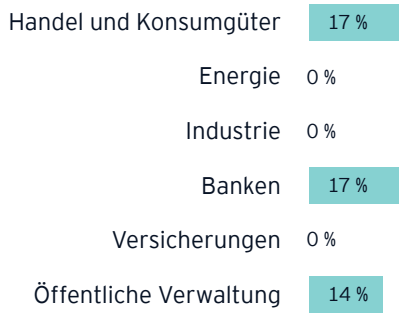
Zusätzliche Software wie Mehrfaktorauthentifizierung; Intrusion-Prevention-/-Detection-Systeme (Systeme, die Hackerangriffe erkennen/abwehren)



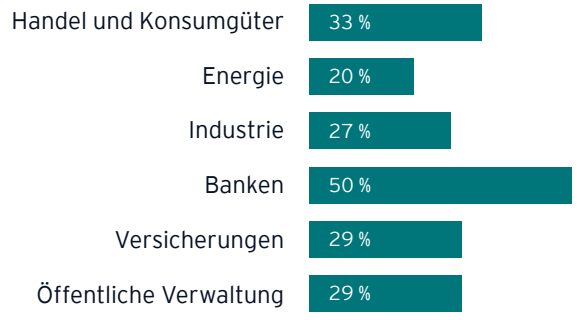
Modernisierung der IT-Infrastruktur (z. B. neue Tools/Überwachungsmechanismen)



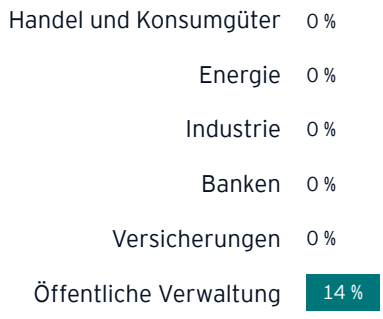
Papierloses Büro bis zum Umzug in die Cloud



Verschärfung der Sicherheitsrichtlinien/-settings



Andere Maßnahmen



2020

n=202, Prozentzahlen gerundet

Spot on Sector
Die wichtigsten Ergebnisse

Handel und Konsumgüterindustrie

Gefahrenpotenzial

schätzen das Risiko, Opfer eines Cyberangriffs zu werden, als (sehr) hoch ein

erwarten, dass die Gefahr von Angriffen auf ihr Unternehmen steigen wird

Tätergruppen

Von diesen Tätergruppen geht aus Sicht der Befragten die größte Gefahr aus:

Hacktivist:innen

Organisiertes Verbrechen

Ausländischer Geheimdienst/ Staatliche Stelle

Angriffsfälle

Am häufigsten angegriffen wurden: Finanzwesen (17 %), Personal (17 %) und Vertrieb (8 %)

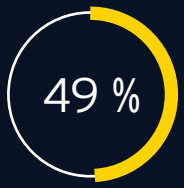
entdeckten in den letzten fünf Jahren einen Angriff auf ihr Unternehmen

wurden mehrfach Opfer von Angriffen

wurden bereits erpresst

Prävention

sind sicher, dass die eigenen Präventionsmaßnahmen wirkungsvoll sind



haben eine Versicherung gegen digitale Risiken abgeschlossen

Corona

geben an, dass ihre Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet haben

konnten seit Ausbruch der Coronakrise einen Zuwachs an Cyberangriffen feststellen

haben ihre Cybersecurity-Maßnahmen als Folge der Coronakrise und des Lockdowns verschärft

2020 n=53, Prozentzahlen gerundet

Interview

Martin Unger

> Cyberangriffe gehen daher meist auch mit einem Imageschaden und somit Markenwertverlusten einher. Unternehmen müssen dem vorbeugen und ihr wichtigstes Gut, die Marke, auch durch Cybersicherheitsmaßnahmen ausreichend schützen.

Martin Unger
Leiter Konsumgüter und Handel
bei EY Österreich und Leiter EYCarbon

Was ist in der Handel-und-Konsumgüter-Branche das Worst-Case-Szenario bei Cyberangriffen?
Sie kennen das doch bestimmt: Wenn Sie in den Supermarkt gehen, kaufen Sie meist dieselben Produkte von denselben Herstellern. In einer komplexen Welt mit Milliarden an Kommunikationspunkten und Wahlmöglichkeiten brauchen Konsument:innen Orientierung. In unserer westlichen Zivilisation übernehmen Marken diese Aufgabe. Wir kaufen die Produkte in der Erwartung einer bestimmten Leistung, wir vertrauen darauf und reduzieren somit die Komplexität ein Stück weit. Ein Cyberangriff, bei dem die Daten der Konsument:innen oder kompromittierende Informationen über das Unternehmen gestohlen werden, reduziert dieses Vertrauen. Cyberangriffe gehen daher meist auch mit einem Imageschaden und somit Markenwertverlusten einher. Unternehmen müssen dem vorbeugen und ihr wichtigstes Gut, die Marke, auch durch Cybersicherheitsmaßnahmen ausreichend schützen.

Wer will die Daten von Handels- und Konsumgüterunternehmen stehlen?
Grundsätzlich sehen Unternehmen aus der Branche die größte Gefahr von organisierten Verbrecher:innen und auch von Hacktivist:innen. Von organisierten Verbrecherbanden hat man oft finanzielle Hintergründe zu befürchten. Daten werden dann gestohlen, um beispielsweise Lösegeld zu erpressen. Hacktivist:innen sehen darin die technische Herausforderung, also einfach die Möglichkeit, in die Datenbanken großer Unternehmen eindringen zu können. Oft haben sie aber auch ein moralisch oder gesellschaftlich begründetes Ziel. Hier wird es gefährlich, wenn man mit falschen Karten spielt.

Hat COVID-19 das Cyberrisiko für Handels- und Konsumgüterunternehmen erhöht?
Rund zwei Drittel der Befragten aus der Branche nehmen an, dass die Gefahr durch Cyberangriffe steigen wird – auch wenn nur ein verschwindend geringer Teil der Unternehmen einen Zuwachs von Cyberangriffen seit Ausbruch der Pandemie im März 2020 feststellen konnte. Zwei Drittel der Betriebe hatten im Lockdown Mitarbeiter:innen im Homeoffice – oft ohne genügend Vorbereitungszeit. So steigt natürlich auch das Risiko, Ziel eines Angriffs zu werden.

Was können Handels- und Konsumgüterunternehmen tun?
Prävention ist nach wie vor das oberste Gebot. Unternehmen müssen ihre gesamte IT so gut es geht gegen Angriffe von außen absichern. Dabei ist es neben der Sicherheit von Systemen mindestens genauso wichtig, die eigenen Mitarbeiter:innen richtig zu schulen und sie auf Gefahrenquellen hinzuweisen. Aber nicht nur in Richtung Cybersicherheit muss einiges getan werden, sondern auch in Richtung Transparenz für die Stakeholdergruppen. Durch Digitalisierung werden Produktionsprozesse und Lieferketten transparenter – auch für Dritte. Wer sich hier besser darstellt, als er ist – was zum Beispiel die Einhaltung von Menschenrechten oder Umwelt- und Klimaneutralität betrifft –, steht spätestens nach einem gezielten Cyberangriff, bei dem erdrückende Beweise gestohlen wurden, als Verlierer da.

Spot on Sector
Die wichtigsten Ergebnisse

Industrie

Gefahrenpotenzial

schätzen das Risiko, Opfer eines Cyberangriffs zu werden, als (sehr) hoch ein

erwarten, dass die Gefahr von Angriffen auf ihr Unternehmen steigen wird

Tätergruppen

Von diesen Tätergruppen geht aus Sicht der Befragten die größte Gefahr aus:

Hacktivist:innen

Organisiertes Verbrechen

Ausländischer Geheimdienst/ Staatliche Stelle

Angriffsfälle

Am häufigsten angegriffen wurden: Vertrieb (44 %), Finanzwesen (31 %), und Management und Forschung & Entwicklung (jeweils 19 %)

entdeckten in den letzten fünf Jahren einen Angriff auf ihr Unternehmen

wurden mehrfach Opfer von Angriffen

wurden bereits erpresst

Prävention

sind sicher, dass die eigenen Präventionsmaßnahmen wirkungsvoll sind

haben eine Versicherung gegen digitale Risiken abgeschlossen

Corona

geben an, dass ihre Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet haben

konnten seit Ausbruch der Coronakrise einen Zuwachs an Cyberangriffen feststellen

haben ihre Cybersecurity-Maßnahmen als Folge der Coronakrise und des Lockdowns verschärft

2020 n=50, Prozentzahlen gerundet

Interview

Gerhard Schwartz

”

Der Bereich Forschung und Entwicklung ist neben dem Finanzwesen, dem Vertrieb und dem Management am häufigsten von Attacken auf österreichische Industrieunternehmen betroffen.

Gerhard Schwartz
Leiter Industrial Products
bei EY Österreich

Was ist in der Industrie das Worst-Case-Szenario bei Cyberangriffen?
Datendiebstähle und Cyberangriffe sind durch die zunehmende Digitalisierung der industriellen Produktion ein ernst zu nehmendes Risiko. Durch die zunehmende Vernetzung von Produktionsprozessen und Maschinen kann die Produktion lahmgelegt werden. Das resultiert in Lieferengpässen, stornierten Aufträgen und Reputationsschäden, was sich direkt auf den Umsatz auswirkt. Weniger offensichtlich, aber umso schwerwiegender sind Angriffe auf Daten im Bereich Forschung und Entwicklung. Stellen Sie sich vor, Sie investieren jahrelang mehrere Millionen Euro in die Entwicklung eines neuen Produkts. Wenn letzten Endes die gesamten Entwicklungspläne gestohlen werden, hat das schwerwiegende Konsequenzen. Genauso problematisch ist es, wenn Kund:innendaten gestohlen werden. Daraus könnten sich längere gerichtliche Prozesse und Schadensersatzforderungen ergeben. Der Diebstahl der eigenen Finanzdaten ist ebenfalls ein großes Risiko. Mitarbeiter:innen sind ein potenzielles Gateway – Stichwort „Fake President Fraud“. Solche Fälle gehen mit jahrelangen Rechtsstreitigkeiten, Entlassungen des Vorstandes und Einbrüchen des Aktienkurses einher.

Wer will die Daten von Industrieunternehmen stehlen?
Industrieunternehmen sehen sich vorrangig durch Hacktivist:innen bedroht. Die Industrie ist auch aus mehreren Gründen ein interessantes Ziel für Hacker:innen. Zum einen gibt es Kund:innen- und Zahlungsdaten, die vermehrt in den Fokus solcher Attacken rücken. Zum anderen wird viel in die Forschung und Entwicklung von Produkten investiert. Wenn diese Entwicklungspläne gestohlen werden, könnten Kriminelle Lösegeld dafür fordern. Der Bereich Forschung und Entwicklung ist neben dem Finanzwesen, dem Vertrieb und dem Management am häufigsten von Attacken auf österreichische Industrieunternehmen betroffen.

Hat COVID-19 das Cyberrisiko für die Industrie erhöht?
Wegen COVID-19 haben viele Betriebe ihre Mitarbeiter:innen ins Homeoffice geschickt – in der Industrie waren es 70 %. Oft war die Vorbereitungszeit auf diese Umstellung unzureichend, wir haben sogar von Unternehmen gehört, die Mitarbeiter:innen von Privatlaptops aus arbeiten ließen. Problematisch und für Cyberangriffe anfällig sind dann natürlich auch die noch nicht für das Teleworking angepassten Arbeitsprozesse. Das erhöht beispielsweise auch das Risiko für einen „Fake President Fraud“ oder andere Attacken, bei denen Mitarbeiter:innen als Eintrittskarte genutzt werden. Insgesamt konnte aber nur jeder zehnte Industriebetrieb einen Zuwachs an Cyberangriffen feststellen. Aber: Nur weil keine Attacke entdeckt wurde, heißt das natürlich nicht, das keine stattgefunden hat. Insgesamt haben wir in den letzten Monaten eine steigende Gefahr durch Cyberangriffe beobachtet.

Was können Industriebetriebe tun?
Wir raten Unternehmen, sich umfassend vorzubereiten, auch wenn kein IT-System der Welt zu 100 Prozent vor Cyberangriffen schützen kann. Das ist das Risiko, das mit der Digitalisierung einhergeht. Aber man kann sich gut drauf vorbereiten: einerseits indem man die Systeme selbst laufend testet und weiter optimiert, andererseits indem man die Mitarbeiter:innen über Risiken aufklärt und über vorbeugende Maßnahmen informiert. Am meisten profitiert man davon, wenn man sich auf den Ernstfall vorbereitet: Ein Krisenplan mit klar definierten Teammitgliedern, Kommunikationswegen und Entscheidungsketten ermöglicht im schlimmsten Fall ein schnelles und geordnetes Vorgehen.

Spot on Sector
Die wichtigsten Ergebnisse

Energie

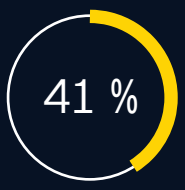
Gefahrenpotenzial

schätzen das Risiko, Opfer eines Cyberangriffs zu werden, als (sehr) hoch ein

erwarten, dass die Gefahr von Angriffen auf ihr Unternehmen steigen wird

Tätergruppen

Von diesen Tätergruppen geht aus Sicht der Befragten die größte Gefahr aus:



Hacktivist:innen

Organisiertes Verbrechen

Ausländischer Geheimdienst/ Staatliche Stelle

Angriffsfälle

Am häufigsten angegriffen wurden: Forschung und Entwicklung (25 %), Finanzwesen (13 %) und Fertigung (13 %)

entdeckten in den letzten fünf Jahren einen Angriff auf ihr Unternehmen

wurden mehrfach Opfer von Angriffen

wurden bereits erpresst

Prävention

sind sicher, dass die eigenen Präventionsmaßnahmen wirkungsvoll sind

haben eine Versicherung gegen digitale Risiken abgeschlossen

Corona

geben an, dass ihre Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet haben

konnten seit Ausbruch der Coronakrise einen Zuwachs an Cyberangriffen feststellen

haben ihre Cybersecurity-Maßnahmen als Folge der Coronakrise und des Lockdowns verschärft

2020 n=27, Prozentzahlen gerundet

Interview

Stefan Uher

> Energieunternehmen müssen sich bewusst sein, dass ihre Daten und Systeme ein interessantes Ziel für Cyberkriminelle sind. Schwerwiegend wäre beispielsweise ein flächendeckender Stromausfall — also ein Blackout.

Stefan Uher
Leiter Energy & Resources
bei EY Österreich und Co-Leiter EYCarbon

Was ist in der Energiebranche das Worst-Case-Szenario bei Cyberangriffen?
Smart Homes, Smart Meters, Smart Cities – die Haushalte und auch die Realwirtschaft werden immer elektrifizierter und damit digitaler. Durch diese Trends werden große Mengen an Daten erzeugt, die Energieunternehmen und die Verbraucher:innen selbst nutzen können. Genau hier liegt auch die größte Gefahr, denn alles, was digital ist, kann auch gehackt werden. Energieunternehmen müssen sich bewusst sein, dass ihre Daten und Systeme ein interessantes Ziel für Cyberkriminelle sind. Schwerwiegend wäre beispielsweise ein flächendeckender Stromausfall – also ein Blackout. Niemand kann Lebensmittel kaufen, das Auto auftanken oder Geld abheben, Heizungen fallen aus, die Wasserversorgung und das Telefonnetz brechen zusammen, bis zum vollkommenen Stillstand der gesamten Wirtschaft – immerhin ist heute so gut wie jeder Arbeitsplatz mit einem Computer ausgestattet und mit dem Internet verbunden. Das ist der Grund, warum die österreichische Energiebranche das Risiko von Cyberattacken sehr ernst nimmt.

Wer will die Daten von Unternehmen in der Energiebranche stehlen?
Energieversorger sehen sich vor allem durch Hacktivist:innen und auch durch das organisierte Verbrechen bedroht. Angriffe von ausländischen Geheimdiensten bzw. auch von staatlichen Stellen werden von den wenigsten erwartet.

Hat COVID-19 das Cyberrisiko für die Energiebranche erhöht?
Derzeit gehen laut unserer Umfrage sechs von zehn Energiedienstleistern davon aus, dass das Risiko von Cyberangriffen zunimmt, jeder fünfte schätzt das Risiko sogar als sehr hoch bzw. hoch ein. Wegen COVID-19 setzen viele Energieversorger auf Homeoffice, 85 Prozent haben ihre Mitarbeiter:innen zumindest während der Lockdowns auf Remote Work umgestellt. Das und weitere Faktoren erhöhen natürlich das Risiko – auch wenn zumindest zwei von fünf der befragten Unternehmen in der Energiebranche ihre Cybersecurity-Maßnahmen infolge der Coronakrise verschärft haben.

Was können Energieunternehmen tun?
Grundsätzlich sollten sich Energieversorger der Gefahr durch Cyberangriffe bewusst sein und schon im Vorfeld geeignete Maßnahmen ergreifen, um die eigenen Systeme und Prozesse möglichst sicher zu gestalten. Trotzdem bleibt auch dann ein gewisses Restrisiko. Deshalb ist es notwendig, Krisenpläne zu erarbeiten, damit im Notfall Chaos vermieden wird und strukturiert vorgegangen werden kann.

Die Anforderungen an die Cybersicherheit bei kritischen Infrastrukturbetreibern hat der Gesetzgeber im NIS-Gesetz geregelt und ich freue mich, dass wir als EY unsere Kund:innen nicht nur bei der Umsetzung der Anforderungen unterstützen können, sondern als sogenannte „qualifizierte Stelle" die implementierten Sicherheitsmaßnahmen und Prozesse auch abnehmen bzw. prüfen dürfen.

Spot on Sector
Die wichtigsten Ergebnisse

Öffentliche Verwaltung

Gefahrenpotenzial

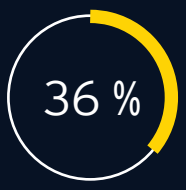
schätzen das Risiko, Opfer eines Cyberangriffs zu werden, als (sehr) hoch ein

erwarten, dass die Gefahr von Angriffen auf ihr Unternehmen steigen wird

Tätergruppen

Von diesen Tätergruppen geht aus Sicht der Befragten die größte Gefahr aus:

Hacktivist:innen



Organisiertes Verbrechen

Ausländischer Geheimdienst/ Staatliche Stelle

Angriffsfälle

Am häufigsten angegriffen wurden: Finanzwesen (50 %), Personalwesen (33 %) und Management (17 %)

entdeckten in den letzten fünf Jahren einen Angriff auf ihr Unternehmen

wurden mehrfach Opfer von Angriffen

wurden bereits erpresst

Prävention

sind sicher, dass die eigenen Präventionsmaßnahmen wirkungsvoll sind

haben eine Versicherung gegen digitale Risiken abgeschlossen

Corona

geben an, dass ihre Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet haben

konnten seit Ausbruch der Coronakrise einen Zuwachs an Cyberangriffen feststellen

haben ihre Cybersecurity-Maßnahmen als Folge der Coronakrise und des Lockdowns verschärft

2020 n=40, Prozentzahlen gerundet

Interview

Christoph Harreither

> Sie würden bestimmt nicht wollen, dass der Roboter, der Sie gerade operiert, plötzlich unter der Kontrolle eines oder einer Unbekannten steht, selbst wenn es sich „nur“ um eine Appendektomie handelt.

Christoph Harreither
Leiter Government & Public Sector
bei EY Österreich

Was ist im öffentlichen Sektor das Worst-Case-Szenario bei Cyberangriffen?
Für Parteien und politische Entscheidungsträger:innen ganz sicher die Möglichkeit der Wahlfälschung. Zusätzlich ist der Staat auch Eigentümer von Einrichtungen, die kritisch für unsere Infrastruktur sind. Werden beispielsweise Krankenhäuser gehackt, kann auf die Gesundheitsdaten von Patient:innen zugegriffen werden. Lösegeldforderungen sind in diesem Zusammenhang nicht unwahrscheinlich. Auch ein feindlicher Zugriff auf medizinische Geräte ist nicht auszuschließen – bei der zunehmenden Technologisierung der Chirurgie kann das lebensgefährlich werden. Sie würden bestimmt nicht wollen, dass der Roboter, der Sie gerade operiert, plötzlich unter der Kontrolle eines oder einer Unbekannten steht, selbst wenn es sich „nur“ um eine Appendektomie handelt. Aber auch Verkehrsnetze oder die Grundversorgung mit Wasser und Strom sind kritisch für die Aufrechterhaltung unseres Systems – eine Übernahme durch feindliche Angreifer:innen kann zu sozialen Unruhen, sinkender Attraktivität des Wirtschaftsstandortes und Vertrauensverlusten in der Bevölkerung führen.

Wer will die Daten von öffentlichen Unternehmen stehlen?
Der gesamte öffentliche Sektor ist für die Aufrechterhaltung der Infrastruktur verantwortlich. Das macht diesen Bereich zum interessanten Angriffsziel. Die größte Bedrohung sieht die öffentliche Verwaltung von Hacktivist:innen und auch vom organisierten Verbrechen. Beobachtet man die aktuelle politische Weltbühne, in der fast jede Wahl zur Spaltung der Nation führen kann, ist das eine durchaus realistische Einschätzung. Werte haben an Bedeutung zugenommen, das zieht auch politisch motivierte Hacktivist:innen an.

Hat COVID-19 das Cyberrisiko für den öffentlichen Sektor erhöht?
Natürlich steigt mit der durch COVID-19 angeheizten Digitalisierung aller Bereiche der öffentlichen Verwaltung die Gefahr von Cyberangriffen. Die digitalen Kommunikationswege und die Online-Verfügbarkeit von Daten öffnen auch die Türen für Cyberkriminelle. Dieses Risiko hat die öffentliche Verwaltung von Österreich natürlich im Blick. Laut unserer Umfrage erwarten drei Viertel der Befragten aus der öffentlichen Verwaltung, dass die Gefahr von Cyberangriffen weiter steigen wird.

Was kann der öffentliche Sektor tun?
Es ist elementar, dass sich öffentliche Organisationen richtig auf Cyberangriffe vorbereiten. IT-Systeme und digital vernetzte Geräte müssen sicher sein und die Mitarbeiter:innen der öffentlichen Verwaltung müssen sich der Gefahr von Cyberangriffen bewusst sein. Außerdem müssen die öffentliche Verwaltung und jeder öffentliche Betrieb schon im Vorfeld klären, wer zum Krisenstab im Falle eines Cyberangriffs gehört und wer dabei welche Rolle spielt. Nur dann kann man den Schaden möglichst minimal halten.

Spot on Sector
Die wichtigsten Ergebnisse

Banken

Gefahrenpotenzial

schätzen das Risiko, Opfer eines Cyberangriffs zu werden, als (sehr) hoch ein

erwarten, dass die Gefahr von Angriffen auf ihr Unternehmen steigen wird

Tätergruppen

Von diesen Tätergruppen geht aus Sicht der Befragten die größte Gefahr aus:

Hacktivist:innen

Organisiertes Verbrechen

Ausländischer Geheimdienst/ Staatliche Stelle

Angriffsfälle

Am häufigsten angegriffen wurde: Finanzwesen (50 %)

entdeckten in den letzten fünf Jahren einen Angriff auf ihr Unternehmen

wurden mehrfach Opfer von Angriffen

Es gab noch keine Erpressungsversuche

Prävention

sind sicher, dass die eigenen Präventionsmaßnahmen wirkungsvoll sind

haben eine Versicherung gegen digitale Risiken abgeschlossen

Corona

geben an, dass ihre Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet haben

konnten seit Ausbruch der Coronakrise einen Zuwachs an Cyberangriffen feststellen

haben ihre Cybersecurity-Maßnahmen als Folge der Coronakrise und des Lockdowns verschärft

2020 n=19, Prozentzahlen gerundet

Interview

Armin Schmitt

> Vom gehackten Bankomaten über Fehlüberweisungen bis hin zur teils stillgelegten Bank ist schon alles vorgekommen.

Armin Schmitt
Leiter Banking bei EY Österreich

Was ist in der Bankenbranche das Worst-Case-Szenario bei Cyberangriffen?
Banken sind die „Verteilzentren" der weltweiten Finanztransaktionen. Transaktionen rund um den Globus sind in den Systemen der Banken gespeichert, Konten aller Art werden bei ihnen verwaltet. Da ist es klar, dass ein Worst-Case-Szenario bei einem Cyberangriff zu einem erheblichen finanziellen Schaden für Banken bzw. deren Kund:innen führen würde. Deshalb gibt es für Banken auch sehr weitreichende Vorschriften, was die Sicherheit ihrer IT-Systeme betrifft. Die Schwachpunkte sind oft die Kund:innen selbst, wenn sie beispielsweise ihre Bankdaten unsicher verwalten oder weitergeben. Deshalb ordnen wir „Phishing" als eine der schwerwiegendsten Cyberattacken auf Banken ein. Dabei werden Zugriffsdaten auf die Finanzportale der Kund:innen abgegriffen und deren Geld gestohlen. Oder die Bank wird zur Lösegeldzahlung erpresst, damit die Kund:innendaten nicht ihren Weg in die Öffentlichkeit finden. Grundsätzlich ist aber kein Szenario auszuschließen und wirklich jedes einzelne kann weitreichende Folgen haben. Vom gehackten Bankomaten über Fehlüberweisungen bis hin zur teils stillgelegten Bank ist schon alles vorgekommen.

Wer will die Daten von Banken stehlen?
Von Hacktivist:innen und vom organisierten Verbrechen geht wohl die größte Gefahr aus, das sehen auch die Banken so. Über ein Viertel der Banken befürchtet aber auch Angriffe durch ausländische Geheimdienste bzw. staatlichen Stellen – mehr als in jeder anderen Branche. Das Interesse dürfte durchaus von allen Seiten gegeben sein, immerhin sind Banken wegen ihrer zentralen Rolle in der Geldversorgung der Schlüsselsektor einer jeden Volkswirtschaft.

Hat COVID-19 das Cyberrisiko für die Bankenbranche erhöht?
Jede zehnte Bank hat seit Ausbruch der Krise einen Zuwachs von Cyberangriffen beobachtet. Im Branchenvergleich ist das der höchste Wert überhaupt. Das ist eine realistische Einschätzung der aktuellen Lage – immerhin wirkt COVID-19 als Digitalisierungsbooster und hat dem Onlinehandel massiven Aufschwung gegeben. Dort wiederum ist es für Hacker:innen und Cyberkriminelle natürlich möglich, Bankdaten abzugreifen – auch wenn es einem die Banken keinesfalls leicht machen.

Was können Banken tun?
Gerade weil sich das Risiko während der Pandemie spürbar erhöht hat, haben die Banken in den Ausbau ihrer Cyberabwehr investiert. Banken sind intensiv gefordert, alles zu tun, um Cyberattacken vorzubeugen und das Risiko zu minimieren – auch wegen der bestehenden regulatorischen Vorgaben, die umgesetzt und eingehalten werden müssen. Trotzdem bleibt ein gewisses Restrisiko, da sich nicht nur neue Technologien, sondern auch die Möglichkeiten für Cyberkriminelle immer weiterentwickeln. Das Gute ist: Wer die richtigen Maßnahmen trifft, ist erstens schwerer zu knacken und kann zweitens im Krisenfall viel besser und schneller reagieren. Der Schaden kann so nicht vermieden, aber zumindest minimiert werden. Das richtige Maßnahmenportfolio ist ein Mix aus technischen Sicherheitsvorkehrungen in den IT-Systemen und der richtigen Informationspolitik im Hinblick auf Mitarbeiter:innen und Kund:innen.

Spot on Sector
Die wichtigsten Ergebnisse

Versicherungen

Gefahrenpotenzial

schätzen das Risiko, Opfer eines Cyberangriffs zu werden, als (sehr) hoch ein

erwarten, dass die Gefahr von Angriffen auf ihr Unternehmen steigen wird

Tätergruppen

Von diesen Tätergruppen geht aus Sicht der Befragten die größte Gefahr aus:

Hacktivist:innen

Organisiertes Verbrechen

Ausländischer Geheimdienst/ Staatliche Stelle

Angriffsfälle

Am häufigsten angegriffen wurden: Finanzwesen (50 %) und Vertrieb (50 %)

entdeckten in den letzten fünf Jahren einen Angriff auf ihr Unternehmen

Niemand wurde mehrfach Opfer von Angriffen

Es gab noch keine Erpressungsversuche

Prävention

sind sicher, dass die eigenen Präventionsmaßnahmen wirkungsvoll sind

haben eine Versicherung gegen digitale Risiken abgeschlossen

Corona

geben an, dass ihre Mitarbeiter:innen im Lockdown vermehrt im Homeoffice gearbeitet haben

konnten seit Ausbruch der Coronakrise einen Zuwachs an Cyberangriffen feststellen

haben ihre Cybersecurity-Maßnahmen als Folge der Coronakrise und des Lockdowns verschärft

2020 n=13, Prozentzahlen gerundet

Interview

Ali Aram

> Die Gefahr durch Cyberkriminalität und damit auch das Interesse an Versicherungen ist durch die Coronapandemie gestiegen. Cybercrime kann für Versicherungen deshalb zum Geschäftsmodell werden.

Ali Aram
Leiter Versicherungen bei EY Österreich

Was ist in der Versicherungsbranche das Worst-Case-Szenario bei Cyberangriffen?
Versicherungen sind bei Cyberangriffen einem hohen Reputationsrisiko ausgesetzt. Kund:innen wollen ihre Finanzprodukte sicher verwaltet wissen. Zusätzlich werden in der Versicherungsbranche auch sensible Kund:innendaten verarbeitet, zum Beispiel Gesundheitsdaten bei Zusatzversicherungen. Werden Kund:innendaten gestohlen, kann das zu Lösegeldforderungen führen. Die Hacker:innen drohen dann mit Veröffentlichung der Daten und wollen eine meist nicht unwesentliche Summe Geld erpressen. Natürlich sind auch die immer digitaler werdenden Arbeitsprozesse und Abläufe oft Ziel einer Cyberattacke. Cyberkriminelle dringen dabei in die IT-Infrastruktur des Unternehmens ein und richten dort Schaden an. Es ist möglich, damit das ganze Unternehmen zumindest kurzfristig außer Gefecht zu setzen.

Wer will die Daten von Versicherungen stehlen?
Versicherungen fühlen sich vorrangig durch Hacktivist:innen, aber auch durch das organisierte Verbrechen bedroht. Die Daten und auch die digitalen Kommunikationswege bieten Cyberkriminellen viele Möglichkeiten, den Versicherungsunternehmen Schaden zuzufügen. Versicherungen haben sehr viele Kund:innendaten gespeichert. Ziel von Hacker:innen ist oft die Erpressung von Lösegeld.

Hat COVID-19 das Cyberrisiko für die Versicherungsbranche erhöht?
Die österreichische Versicherungslandschaft ist sich der drohenden Gefahr durch Cyberangriffe bewusst: Laut unserer Umfrage erwarten rund 60 % der Befragten, dass die Gefahr von Angriffen auf ihre Versicherung weiter steigen wird. Fast jede:r siebte hat in den letzten fünf Jahren einen Angriff auf das eigene Unternehmen identifiziert. COVID-19 hat das Risiko nochmals erhöht, auch wenn nur 8 % der Versicherungen seit Ausbruch der Coronakrise einen Zuwachs von Angriffen auf ihre Systeme beobachtet haben. Versicherungen beugen aber vor: Mehr als die Hälfte hat ihre Cybersecurity-Maßnahmen infolge der Coronakrise und der Lockdowns verschärft.

Was können Versicherungen tun?
In erster Linie ist bei der zunehmenden digitalen Transformation des Unternehmens darauf zu achten, parallel auch die Cybersicherheit weiterzuentwickeln. Prozesse und Systeme müssen von vornherein robust konstruiert werden, um Attacken standhalten zu können. Auch Mitarbeiter:innen müssen entsprechend geschult werden, damit sie nicht als trojanische Pferde missbraucht werden. Das alles ist wichtig und notwendig; trotzdem wird man damit nicht jedes Risiko ausschließen können. Auch die Techniken der Hacker:innen und Cyberkriminellen entwickeln sich weiter. Deshalb müssen schon im Vorfeld alle notwendigen Prozesse und Verantwortlichkeiten im Falle eines Angriffs festgelegt werden.

Grundsätzlich muss man aber sagen, dass Cyberkriminalität für Versicherungen auch zum Geschäftsmodell werden kann. Rund die Hälfte der Unternehmen aller Branchen hat derzeit eine Cyberversicherung abgeschlossen, das ist ein Zuwachs um 20 % im Vergleich zum Vorjahr. Das bedeutet, dass das Interesse an solchen Versicherungsprodukten massiv wächst, gleichzeitig aber noch genügend Potenzial am Markt vorhanden ist. Dies ist eine Chance für viele Versicherer, sich hier ein zusätzliches Marktsegment zu sichern.

Fazit und Ausblick

Cyberangriffe werden in Zukunft weiter zunehmen, darüber sind sich alle einig: Die überwiegende Mehrheit der Unternehmen in Österreich (70 %) geht davon aus, dass die Gefahren durch Cyberangriffe oder Datendiebstahl in Zukunft steigen werden. Expert:innen bestätigen diesen Trend, der durch die fortschreitende Digitalisierung und durch vermehrtes Homeoffice in Zeiten der Pandemie in allen Bereichen begünstigt wird. Diese bietet der Cyberkriminalität ein beinahe grenzenloses Wachstums- und Schadenspotenzial. Während der Pandemie hat fast jedes dritte Unternehmen seine Cybersecurity-Maßnahmen verschärft, 12 % sogar sehr. Um sich zu schützen, haben mehr als die Hälfte (59 %) der befragten Unternehmen ihre Mitarbeiter:innen sensibilisiert und neue organisatorische Regelungen aufgesetzt (54 %). Außerdem haben mehr als zwei Fünftel der Unternehmen auch ihre IT-Infrastruktur modernisiert (43 %).

Die gute Nachricht: Das Gefahrenbewusstsein der Unternehmen ist inzwischen hoch. 29 % von ihnen sehen ein (erhöhtes) Risiko, selbst Opfer von Cyberangriffen und Datendiebstahl zu werden. Nicht zu Unrecht, denn 24 % der Befragten haben laut eigenen Angaben in den letzten fünf Jahren einen Angriff auf ihr Unternehmen entdeckt – die Dunkelziffer ist deutlich höher.

Aber: Trotz der zunehmenden Gefahr durch Cyberkriminalität fühlen sich die meisten Unternehmen gut abgesichert. Immerhin 50 % der Unternehmen, die ein geringes Risiko sehen, Opfer eines Angriffs zu werden, fühlen sich gut geschützt. Allerdings sind nur 49 % mit den personellen und finanziellen Ressourcen im Bereich Cybersicherheit zufrieden. Bei der Mehrheit der Befragten liegt das Jahresbudget für den Schutz vor Cyberangriffen bei unter 25.000 Euro.

Es werden definitiv zu wenig Cyberkriminelle gefasst und noch immer werden viele Vorfälle nur zufällig entdeckt: In 53 % der Unternehmen griff das interne Kontrollsystem und deckte die kriminellen Handlungen auf. 11 % der befragten Unternehmen gaben an, dass kriminelle Handlungen nur durch Zufall aufgedeckt worden seien. Die Dunkelziffer der tatsächlich erfolgten Cyberangriffe und Datendiebstahl dürfte demnach deutlich höher sein. Auch bleiben die Verantwortlichen meist unerkannt.

Kriminalität muss in der virtuellen Welt genauso verfolgt werden können wie in der analogen. Ob die Unternehmen für diese Herausforderung gewappnet sind, ist fraglich. Ein wichtiger Schritt in die richtige Richtung wäre es, die Investitionen in eine erfolgreiche Cyberabwehr zu erhöhen und wirkungsvolle Maßnahmen für das Sicherheitsbewusstsein in allen Unternehmensbereichen umzusetzen. Auf dem Spiel stehen letzten Endes insbesondere auch wertvolle Kund:innendaten – denn darauf haben es die Täter:innen vermehrt abgesehen. Für manche Organisationen bedeutet dies eine kontinuierliche Verbesserung bestehender Maßnahmen, für andere vielleicht sogar eine komplette Neuausrichtung.

In jedem Fall ist es wichtig und notwendig, ein systematisches und umfassendes Vorgehen zur Prävention und zum Umgang mit Krisensituationen zu etablieren und sich die entsprechenden externen Hilfen zu holen. Es gilt schließlich, der Gefahr durch Cyberkriminalität auf Augenhöhe begegnen zu können, um das eigene Unternehmen weiter auf Kurs zu halten. Die Verantwortlichen sollten sich definitiv auf stürmische Gewässer einstellen!

”

Es gilt schließlich, der Gefahr durch Cyberkriminalität auf Augenhöhe begegnen zu können, um das eigene Unternehmen weiter auf Kurs zu halten. Die Verantwortlichen sollten sich definitiv auf stürmische Gewässer einstellen!

Digitalisierung hat ihre Tücken

Passgenaue Lösungen sind gefragt

Wir liefern die Antworten auf dringende Fragen

EY ist seit vielen Jahren ein weltweit führender Anbieter für Cybersicherheit sowie für digitale Forensik und Investigation und bündelt die Kompetenzen eines globalen Netzwerks. In fast jedem Land der Welt sind unsere Projektteams rund um die Uhr für Sie einsatzbereit. Ganz nach Ihren individuellen Bedürfnissen und für konkrete Aufgabenstellungen stehen Ihnen Branchenkenner:innen und Fachleute für ausgewählte Themenbereiche zur Verfügung. So treffen etwa IT-Berater:innen und Security-Fachleute auf Fachmitarbeiter:innen aus den klassischen EY-Bereichen Wirtschaftsprüfung, Steuer- und Rechtsberatung, aber auch auf Kriminalist:innen und Soziolog:innen.

Die über 7.200 global vernetzten Cyberprofessionals von EY, unterstützt durch zwölf weltweit verteilte Security-Center, betrachten Risiken aus wirtschaftlicher und geopolitischer Perspektive. Dies verhilft Ihnen zu einem realistischen und umfassenden Risikoverständnis, auf dessen Basis Sie intelligente und zukunftssichere Entscheidungen treffen können.

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, krisenmanagementrelevante 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:innen. 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 können und sich so Wettbewerbsvorteile sichern. Außerdem beraten wir Sie natürlich auch umfassend während und nach konkreten Krisenereignissen.

Jede unserer Leistungen hat das Ziel, Antworten auf dringende Fragen rund um Cybersecurity und Krisenmanagement zu finden. Folgende Fragen sollten Sie sich stellen:

- Sind wir ausreichend vorbereitet, um gegen die zunehmenden Cyberbedrohungen zu bestehen?
- Ist unsere Cybersicherheitsstrategie zukunftsfähig?
- Sind die persönlichen Daten unserer Kund:innen, aber auch unser Kern-Know-how geschützt?
- Was geht wirklich in unseren Netzwerken vor?
- Wie können wir das Krisenpotenzial von Ereignissen und Entwicklungen schnell erkennen und analysieren?
- Was sind erste Schritte und Maßnahmen für eine rasche Krisenreaktion?
- Wie wird ein systematisches Informationsmanagement betrieben?
- Wie können bei Unsicherheit und hohem Zeit- und Handlungsdruck Entscheidungen getroffen werden?

Die Cybersecurity- und Krisenmanagement-Services von EY im Überblick

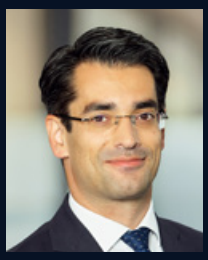
Sicherheit für Ihr digitales Business

Damit das Vertrauen Ihrer Kund:innen, Mitarbeiter:innen und Partner:innen erhalten bleibt, helfen wir Ihnen, sich gegen neue und wiederkehrende Cyberbedrohungen zu schützen. Durch unsere integrierten Lösungen können wir Ihre digitale Transformation maßgeblich unterstützen.

Wir beraten Sie passgenau in allen Fragen zur Cybersicherheit und zum Krisenmanagement – von der Bestandsaufnahme bis hin zur Planung, Umsetzung und Optimierung.

Ansprechpartner

Autoren



Thomas Breuss
Rechtsanwalt und Director EY Law, Pelzmann Gall Größ Rechtsanwälte GmbH

+43 1 26095 2113
thomas.breuss@eylaw.com

Drazen Lukac
Leiter Technology Risk und Cybersecurity EY Österreich

+43 1 21170 1029
drazen.lukac@at.ey.com

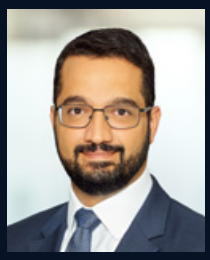
Gottfried Tonweber
Leiter Cybersecurity und Data Privacy EY Österreich

+43 1 21170 1145
gottfried.tonweber@at.ey.com

Benjamin Weissmann
Leiter Cyberforensik EY Österreich

+43 1 21170 1862
benjamin.weissmann@at.ey.com

Sektorenleiter



Ali Aram
Sector Leader Versicherungen EY Österreich

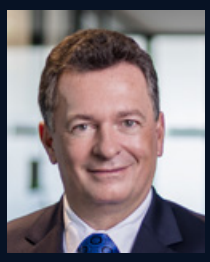
+43 1 21170 1149
ali.aram@at.ey.com

Christoph Harreither
Sector Leader Government & Public EY Österreich

+43 1 21170 1171
christoph.harreither@at.ey.com

Stefan Uher
Sector Leader Energy & Resources EY Österreich

+43 1 21170 1213
stefan.uher@at.ey.com



Martin Unger
Sector Leader Handel und Konsumgüter EY Österreich, Leiter Strategieberatung Contrast EY Parthenon

+43 1 21170 1845
martin.unger@parthenon.ey.com

Armin Schmitt
Sector Leader Financial Services
EY Österreich

+43 1 21170 1717
armin.schmitt@at.ey.com

Gerhard Schwartz
Sector Leader Industrie
EY Österreich

+43 1 21170 1136
gerhard.schwartz@at.ey.com

Impressum:

Eigentümer, Herausgeber und Medieninhaber:
Ernst & Young Wirtschaftsprüfungsgesellschaft
m. b. H. („EY"), 1220 Wien
Inhaltliche Gesamtverantwortung: Thomas Breuss,
Drazen Lukac, Gottfried Tonweber und Benjamin Weissmann
Redaktion: Sarah Mauracher, Nina Eggenberger
Lektorat: Text+Design Jutta Cram
Design: Tanja Maria Allgäuer
Bildmaterial: Gettyimages, Eva Kelety, EY Österreich

Wir sind eine NIS-qualifizierte Stelle

Die europäische NIS-Richtlinie (Netz- und Informationssystemsicherheit) wurde Ende 2018 in das österreichische NISG (Netz- und Informationssystemsicherheitsgesetz) überführt. Ziel ist es, das Sicherheitsniveau für kritische Infrastruktur in Betrieben zu erhöhen beziehungsweise zu gewährleisten. Dazu wurden entsprechend strenge Sicherheitsauflagen für die betroffenen Unternehmen definiert.

Die regelmäßige Überprüfung und die Nachweiserstellung (Prüfberichte) müssen durch akkreditierte „qualifizierte Stellen" durchgeführt werden. Wir helfen als qualifizierte Stelle unseren Kund:innen mit fachlicher Expertise im Bereich Informationssicherheit bei der Absicherung ihrer IT-Netzwerke durch Beratung und Überprüfung aller NISG beziehungsweise von der NISV betroffenen Unternehmensbereiche. Unsere langjährige Prüferfahrung und Expertise bei Zertifizierungsprozessen, beispielsweise bei ISMS (Information Security Management Systems) und DSGVO, sowie eine Vielzahl von Security-Fachleuten ermöglichen uns eine strukturierte Prüfung der geforderten Maßnahmen und Prozesse. Unsere Expertise ermöglicht es uns, die Anwendungen des NISG mit Blick auf die ISO 27001 zu prüfen.

Inhaltlich fordern NISG und NISV großteils identische Sicherheitsmaßnahmen wie die internationale Norm für Informationssicherheit ISO 27001. Wir berücksichtigen von Anfang an den zukünftigen Einsatz von NIS-Tools und richten unsere Handlungsempfehlungen an einer integrierten Umsetzung mit bestehenden Security-Prozessen aus.

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 die Nutzung von Daten und modernsten Technologien bei der Erbringung unserer Dienstleistungen.

Ob Wirtschaftsprüfung (Assurance), Steuerberatung (Tax), Strategie- und Transaktionsberatung (Strategy and Transactions) oder Unternehmensberatung (Consulting): Unsere Teams stellen bessere Fragen, um neue und bessere Antworten auf die komplexen Herausforderungen unserer Zeit geben zu können.

Das internationale Netzwerk von EY Law, in Österreich vertreten durch die Pelzmann Gall Größ Rechtsanwälte GmbH, komplettiert mit umfassender Rechtsberatung das ganzheitliche Service-Portfolio von EY.

In Österreich ist EY an vier Standorten präsent.

GSA Agency | TAL 2104-000
ED None

ey.com/at