Cyberangriffe und Datendiebstahl: virtuelle Gefahr – reale Schäden

Eine Befragung von 200 österreichischen Unternehmen

Building a better working world

Inhalt

VORWORT

Gottfried Tonweber
Leiter Cybersecurity und Data Privacy
bei EY Österreich

Drazen Lukac
Leiter Risk IT und Cybersecurity
bei EY Österreich

Benjamin Weissmann
Leiter Cyberforensik
bei EY Österreich

Thomas Breuss
Rechtsanwalt und Director
bei EY Law Österreich

> Österreichs Unternehmen dürfen das Thema Cybercrime nicht unterschätzen: Sie müssen jederzeit mit einem Angriff rechnen, denn der Schatz in Form von Kundendaten und Know-how ist zu verlockend.“

Cyberangriffe und Datendiebstahl im Jahr 2019 – ein Evergreen, den man nicht mehr hören kann? Ganz und gar nicht! Heutzutage gibt es Unternehmen, die bereits wissen, dass sie Opfer von Cyberangriffen bzw. Datendiebstahl waren, und Unternehmen, die das noch feststellen werden. Eines können wir mit Gewissheit sagen: Für eine Vielzahl von Unternehmen besteht Handlungsbedarf – auch für diejenigen, die die Gefahr durch Cyberkriminalität als hoch einstufen und schon ein beachtliches Gefahrenbewusstsein innerhalb der letzten Jahre entwickelt haben. Wie hat es bereits Konfuzius gesagt? „In allen Dingen hängt der Erfolg von den Vorbereitungen ab.“ Unternehmen fühlen sich durch eigene Vorkehrungen ausreichend abgesichert, um der zunehmenden Kriminalität im digitalen Zeitalter die Stirn zu bieten. Doch Achtung! Diese Unternehmen wiegen sich möglicherweise in falscher Sicherheit und unterschätzen die Bedrohung durch Cyberangriffe bzw. Datendiebstahl.

Neben den technischen Aspekten ist der Faktor Mensch ein weiteres Risiko. Klassische Sicherheitsmaßnahmen in Form von Antivirensoftware, Firewalls und Passwortschutz greifen nicht, wenn eigene oder ehemalige Mitarbeiter Daten weitergeben.

Die Ergebnisse unserer Befragung zeigen, dass die Täter der registrierten Cyberangriffe und von Datenklau meist unerkannt bleiben. In den letzten Jahren ist es deutlich schwerer geworden, den tatsächlichen Täterkreis zu ermitteln. Sprich: In den meisten Fällen werden die Verantwortlichen nicht gefasst und treiben weiterhin ihr Unwesen.

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.

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. 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.

Zu einer erfolgreichen Cyber- und Spionageabwehr gehören nicht nur die technischen Vorkehrungen; auch ein Krisenreaktionsplan sollte im Unternehmen ausgearbeitet, implementiert und vor allem „geübt“ werden. Bei jeder Form von Angriff und Datenklau kommt es darauf an, schnell und systematisch reagieren zu können. Die Reaktionsfähigkeit muss regelmäßig trainiert werden. (Viel) Üben hilft. Qualifizierte Krisenmanager sind reaktionsfähiger als ad hoc eingesetzte Amateure. Auch eine passgenaue Kommunikation spielt intern und extern eine wesentliche Rolle. Denn der Schaden, der im Fall von Cyberangriffen und Datendiebstahl droht, kann für Unternehmen immens sein: Die Täter haben es mittlerweile überwiegend auf Kundendaten und Know-how abgesehen – und beides gehört mit zu den wichtigsten Werten eines Unternehmens.

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

Ergebnisse auf einen Blick

27 % der Unternehmen haben in den vergangenen fünf Jahren konkrete Hinweise auf Cyberangriffe bzw. Datendiebstahl erhalten, 15 % sogar mehrfach.

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

41 % 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 **81 % der befragten Führungskräfte** eine steigende Gefahr durch Cyberangriffe und Datendiebstahl, mehr als jede vierte Führungskraft (27 %) sieht sogar ein stark steigendes Risiko.

32 % fürchten Angriffe durch organisierte Verbrechergruppen, 29 % sehen ihr Unternehmen durch Hacktivisten wie Anonymous gefährdet.

Konkrete Hinweise auf Cyberangriffe bzw. Datendiebstahl gab es zuletzt am häufigsten bei Unternehmen im Bereich Handel und Konsumgüter sowie bei Versicherungsunternehmen. Hier berichten jeweils **40 % der befragten Führungskräfte** von Hinweisen auf Angriffe.

Die mit Abstand meisten Angriffe sind Hackerangriffe auf die IT-Systeme (54 %): In **fast jedem fünften Unternehmen (17 %)** gab es eine Attacke, die auf das vorsätzliche Lahmlegen dieser Systeme abzielte.

Bei jedem zweiten Fall (47 %) konnten Spionageangriffe durch das interne Kontrollsystem identifiziert werden. Durch unternehmensinterne Hinweise wurden 27 % der Angriffe aufgedeckt. Jedoch wird trotz interner Kontrollmechanismen und anderer Aktivitäten immer noch **fast jeder fünfte Angriff (19 %)** rein zufällig entdeckt.

Unternehmen setzen weiterhin auf konventionelle Sicherheitsvorkehrungen. **Mehr als 90 % der befragten Unternehmen** haben in Antivirensoftware, Firewalls und einen Passwortschutz investiert. Ein deutlicher Zuwachs kann bei Investitionen in Intrusion-Prevention-/Intrusion-Detection-Systeme verzeichnet werden: 37 % der Unternehmen investieren jetzt in solche Systeme.

57 % der befragten Unternehmen verfügen über Krisenpläne, die das Vorgehen im Falle eines entdeckten Datendiebstahls definieren. Dabei geben 25 % an, dass diese Abläufe nie geübt worden seien.

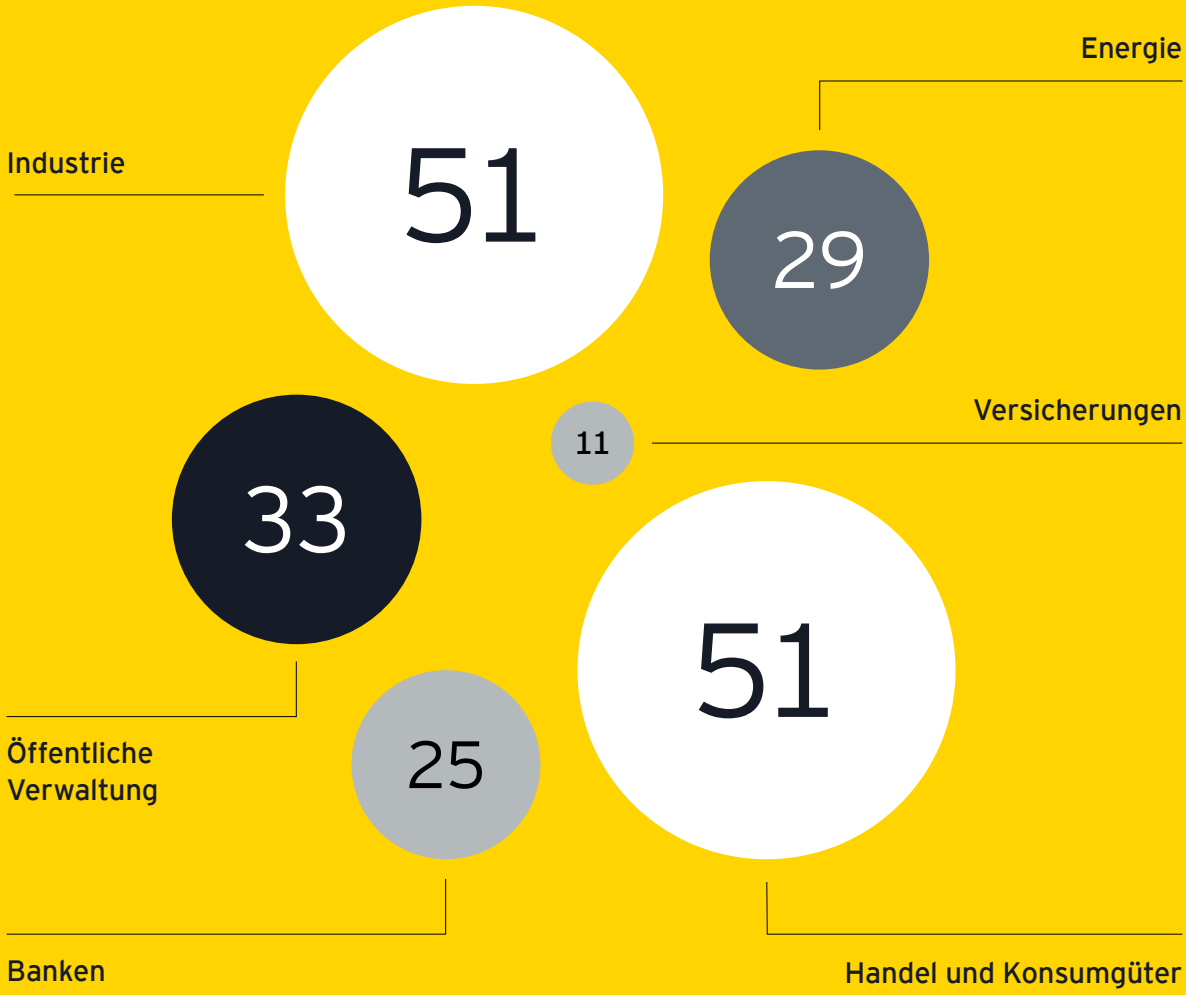
86 % der Unternehmen geben an, dass im Falle eines entdeckten Cyberangriffs bzw. Datendiebstahls eine fallbegleitende interne und externe Kommunikation wichtig oder sogar sehr wichtig sei. Hingegen erachten 14 % der Unternehmen eine solche Kommunikation im Ernstfall als nur bedingt oder gar nicht wichtig.

Design der Studie

Die nachfolgende Studie beruht auf den Ergebnissen einer repräsentativen telefonischen Befragung von 200 Führungskräften österreichischer Unternehmen ab 20 Mitarbeitern. Es wurden Geschäftsführer, Leiter Konzernsicherheit oder Leiter IT-Sicherheit von Unternehmen verschiedenster Größe (gemessen an Mitarbeiterzahl und Umsatzstärke) zum Thema Datenklau befragt.

Durchgeführt hat die Befragung das unabhängige Marktforschungsinstitut market Marktforschungs GmbH & CoKG, Linz im Jänner 2020. Die Ergebnisse sind repräsentativ für die folgenden Branchen:

Anzahl befragter Unternehmen je Branche



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

1

1.1

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

41 % der Manager bereitet die Informationssicherheit des eigenen Unternehmens Sorgen – weniger als vor zwei Jahren

Abbildung 1

Mehr als zwei von fünf Managern bewerten 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 vor zwei Jahren leicht gesunken ist. Viele Manager erwarten, dass sie ihre gesteigerten Investitionen in Cybersicherheit unverwundbar machen. Dabei werden Angreifer immer professioneller und unauffälliger.

Je größer das Unternehmen, desto größer das Risiko: Etwa jedes fünfte größere Unternehmen (21 %) mit mehr als 100 Mitarbeitern schätzt das Risiko, Opfer von Cyberangriffen bzw. Datendiebstahl zu werden, als sehr hoch ein; bei den mittleren und kleineren Unternehmen sind es 13 % bzw. 4 %.

Besonders gefahrenbewusst zeigen sich die Energie- und die Versicherungsbranche. Hier sehen 21 % bzw. 20 % der befragten Führungskräfte ein sehr hohes Risiko, Opfer von Cyberangriffen bzw. Datenklau zu werden, im Banken- und Industriebereich sind es jeweils 16 %.

Größere Unternehmen sehen ein höheres Risiko

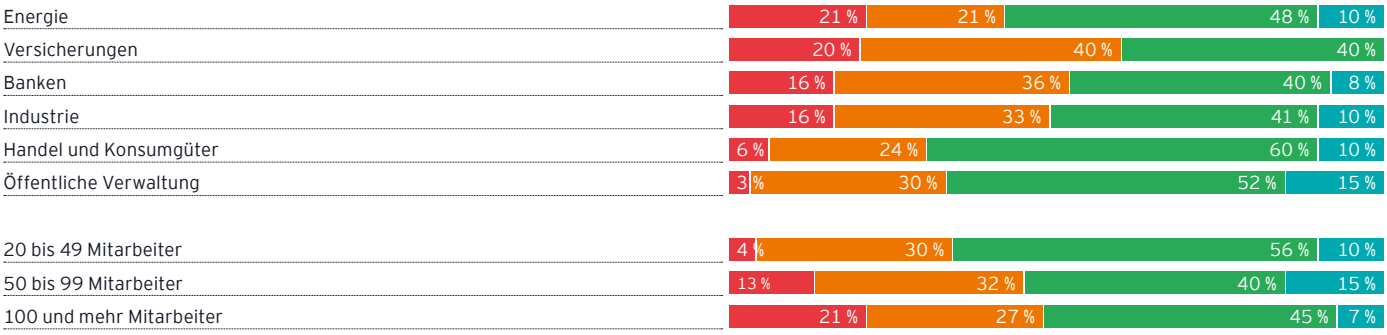


Abbildung 2 | Risikowahrnehmung je Branche und Unternehmensgröße

1.2

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

Immer noch rechnen 81 % der Unternehmen mit einer Verschärfung des Problems

Abbildung 3 | Einschätzung der zukünftigen Entwicklung — Steigt stark an — Steigt etwas an — Geht etwas zurück — Geht stark zurück

Auch in der aktuellen Umfrage gehen immer noch 81 % der Befragten davon aus, dass die Gefahr für Unternehmen, Opfer von Cyberangriffen bzw. Datendiebstahl zu werden, weiterhin zunehmen wird. Mehr als jede vierte Führungskraft sieht sogar ein stark steigendes Risiko. 2017 waren die Zukunftsaussichten noch deutlich pessimistischer.

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

Mehr als jedes dritte größere Unternehmen mit 100 Mitarbeitern oder mehr rechnet damit, dass sich die Problematik von Cyberangriffen bzw. Datendiebstahl weiter verschärfen wird. Bei kleineren Unternehmen steigt das Risikobewusstsein an.

Insbesondere Versicherungen sind alarmiert

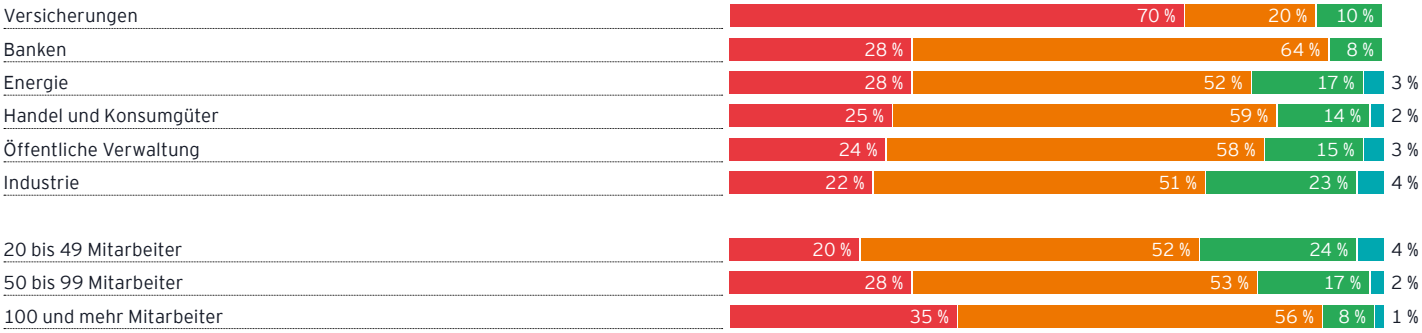
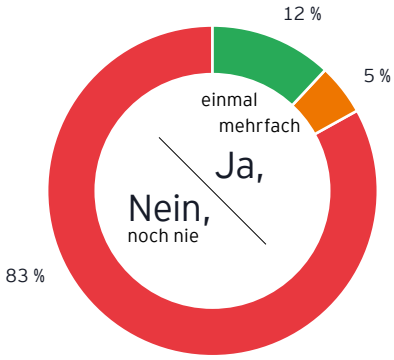


Abbildung 4 | Einschätzung der zukünftigen Entwicklung je Branche und Unternehmensgröße — Steigt stark an — Steigt etwas an — Geht etwas zurück — Geht stark zurück

1.3

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



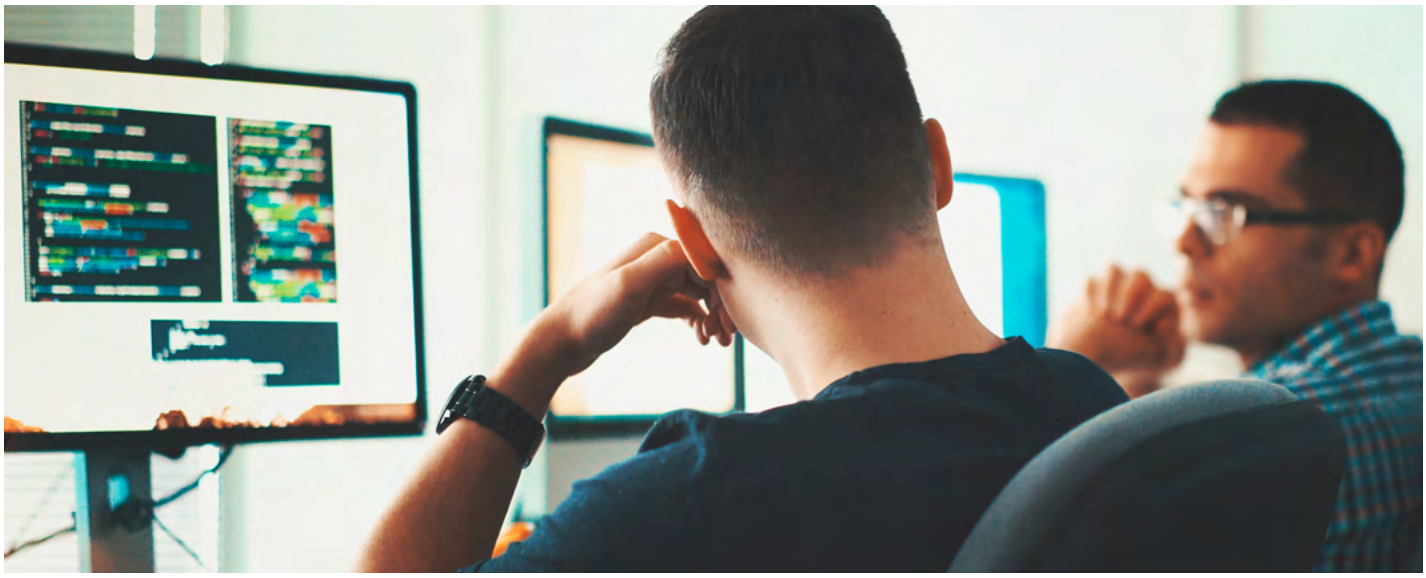
Fast jeder Fünfte war bereits Opfer eines Erpressungsversuchs

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 fordert der Angreifer Lösegeld.

17 % der Befragten waren bereits mit einem derartigen Angriff konfrontiert, jeder 20. sogar mehrfach. Für die Angreifer war dies jedoch selten von Erfolg gekrönt: Nur 3 % der Unternehmen haben gezahlt, 97 % haben dem Druck der Erpresser nicht nachgegeben.

Falls Ja, haben Sie bezahlt?

Abbildung 5 | Angaben zum Verhalten bei Erpressungsversuchen



Risikopotenziale und Tätergruppen

2

2.1

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

Besonders gefürchtet: organisierte Kriminalität

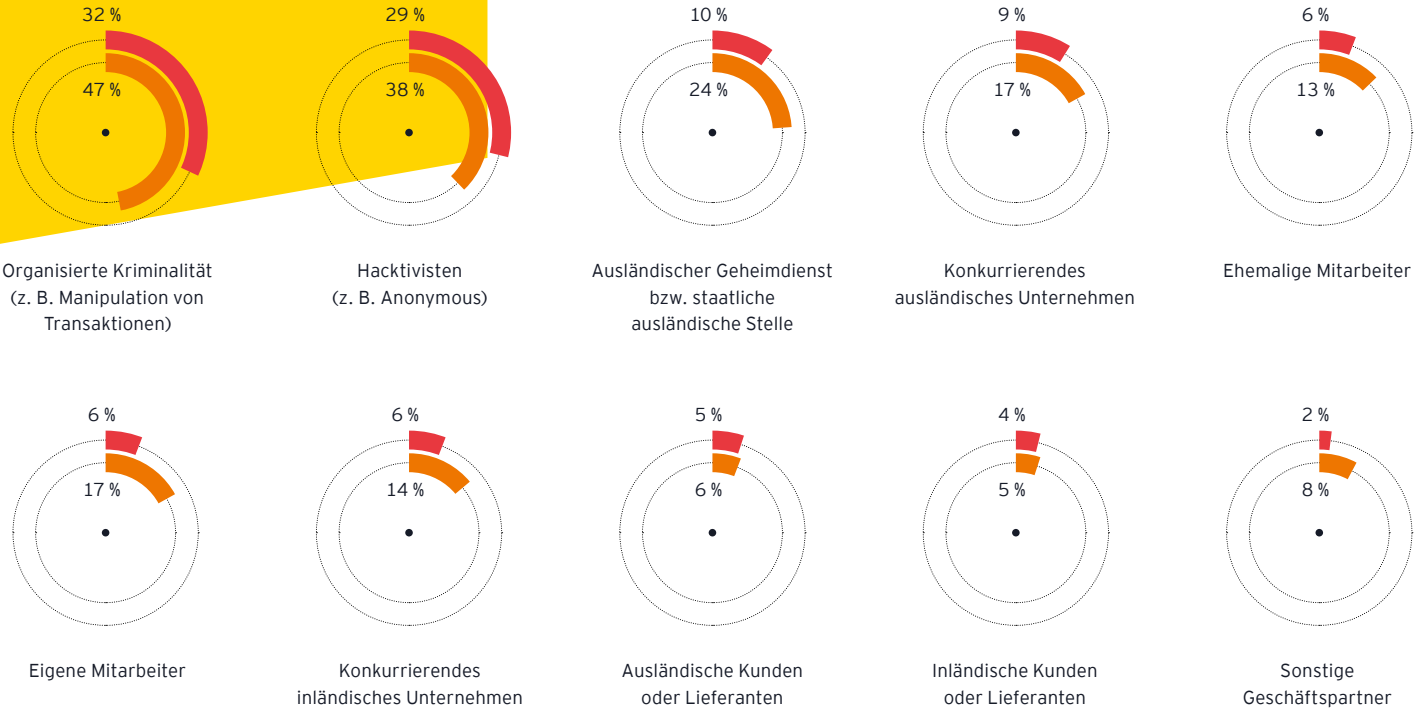


Abbildung 6 | Einschätzung des Risikos nach potenziellen Tätergruppen

Im Vergleich zu 2017 ist das Risikobewusstsein der österreichischen Unternehmen gesunken. Viele heimische Manager fühlen sich durch Investitionen in die Cybersicherheit besser gegen Angriffe gerüstet und schätzen die Gefahr als geringer ein. Die Reihenfolge der gefährlichsten Angreifer hat sich in den letzten beiden Jahren hingegen kaum geändert.

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 Hacktivisten oder ausländischen Geheimdiensten/staatlichen ausländischen Stellen geschädigt zu werden, wird vergleichsweise als hoch eingeschätzt.

Dabei ist die Risikobewertung für alle drei Tätergruppen im Vergleich zu 2017 gesunken.

Als deutlich weniger gefährlich als vor zwei Jahren stufen die Befragten hingegen den Datendiebstahl durch eigene Mitarbeiter ein. Der Anteil ist von 17 % auf 6 % gesunken. Hier scheinen die Manager davon auszugehen, dass die Weiterbildungen und Schulungen von Mitarbeitern zu einem stärkeren Bewusstsein geführt haben. Das gilt auch für ehemalige Mitarbeiter.

Warstory

Nichts geht mehr

Ablauf eines gezielten Ransomware-Angriffs

Montag
19.08.2019

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 haben nach eigenen Angaben interne Dokumente gestohlen und drohen mit Veröffentlichung. Neben Lösegeldforderung ist Mail-Adresse zur Kontaktaufnahme angegeben.

7.55 Uhr Weitere Mitarbeiter 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 des Unternehmens, aber auch wichtige Akteure wie IT, etwaige Krisenteams oder 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 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
19.08.2019

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 Server vom Unternehmensnetzwerk.

17.36 Uhr Krisenstab ist eingerichtet und beginnt mit 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 in dem hier beschriebenen Ransomware-Angriff weiterhin kritisch. Zentrale Daten-, Infrastruktur- und Back-up-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 Akteure 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 bezahlt 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 Kunden 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 Krisenmanagementteam einzubinden und sich auch in Sachen Öffentlichkeitsarbeit von erfahrenen Beratern unterstützen zu lassen. Parallel schaltet der Vorstand die Strafverfolgungsbehörden ein. Das zuständige Landeskriminalamt (LKA) entsendet umgehend Beamte, um den Sachverhalt aufzunehmen und das weitere Vorgehen zu besprechen.

Dienstag
20.08.2019

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

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

10.10 Uhr Krisenstab koordiniert an allen angebundenen Standorten Kontaktaufnahme mit Spezialfirmen, um 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 Beamten des LKA. 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 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 Kollegen 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 Kunden, beschließt der Vorstand, das geforderte Lösegeld zu bezahlen. Das LKA übernimmt die Kommunikation mit den Tätern. Am Nachmittag stehen die benötigten Bitcoins zur Verfügung. Nach der Übermittlung eines ersten Schlüssels zum Beweis, dass die Täter die Systeme auch tatsächlich entschlüsseln können, wird die Übertragung der Bitcoins veranlasst. Binnen zwei Stunden senden die Erpresser eine E-Mail mit einem ZIP-Archiv, das anscheinend alle benötigten Kryptoschlüssel enthält. Darüber hinaus geben die Täter an, keine weiteren internen Dokumente mehr veröffentlichen zu wollen.

Wer wurde Opfer? Wer sind die Täter?

3

3.1

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

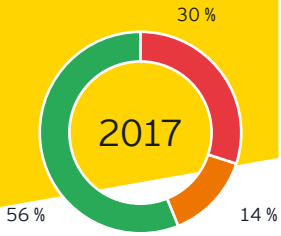
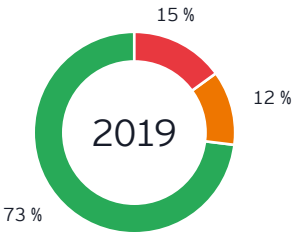


Abbildung 7 | Hinweise auf konkrete Cyberangriffe

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



Größere Unternehmen sind deutlich stärker betroffen

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

19 % 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.

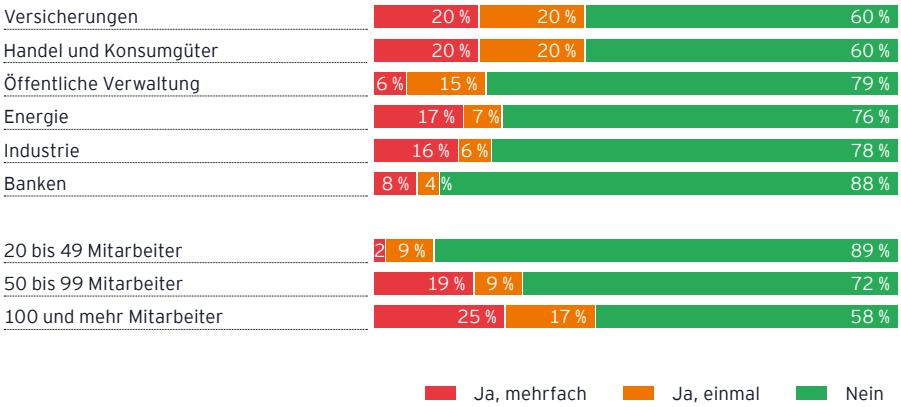


Abbildung 8 | Hinweise auf konkrete Cyberangriffe je Branche und Unternehmensgröße

Konkrete Hinweise auf Cyberangriffe bzw. Datendiebstahl gab es zuletzt am häufigsten bei Unternehmen aus den Bereichen Versicherung bzw. Handel und Konsumgüter. Hier berichten jeweils 40 % der befragten Führungskräfte von Hinweisen auf Cyberattacken.

Vor allem größere Unternehmen mit 100 Mitarbeitern oder mehr hat es besonders getroffen. In 42 % 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.

3.2

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

Der Vertrieb steht besonders im Visier von Datendiebstählen

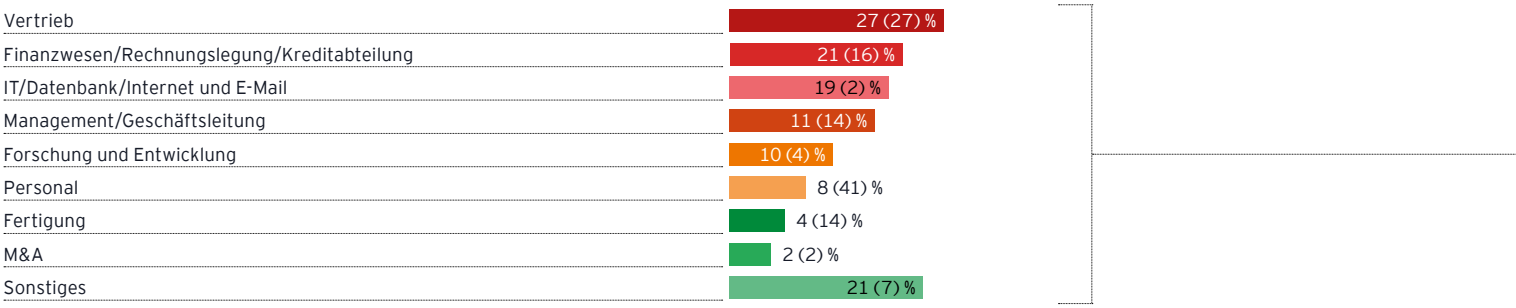


Abbildung 9 | Häufigkeit der Datendiebstähle je Unternehmensbereich (Mehrfachantworten möglich, Werte von 2017 in Klammern)

Besonders angriffsgefährdete Stellen im Unternehmen sind der Vertrieb, der in mehr als jedem vierten Fall betroffen war, aber auch das Finanzwesen. Hier gab es im Vergleich zu 2017 einen Zuwachs. Einen erheblichen Rückgang gab es jedoch bei Diebstählen von Personaldaten, von 41 % auf 8 %.

Branchenspezifisch zeigen sich große Unterschiede bei den Angriffszielen. Während gerade bei Handels- und Konsumgüterunternehmen sowie bei Banken die Kundendaten im Vertrieb besonders häufig angezapft werden, steht bei Industrieunternehmen der Bereich Forschung und Entwicklung – Stichwort Industriespionage – stärker im Fokus. Bei Versicherungen und Energieunternehmen sind insbesondere die IT-Systeme und Netzwerke im Visier der Angreifer.

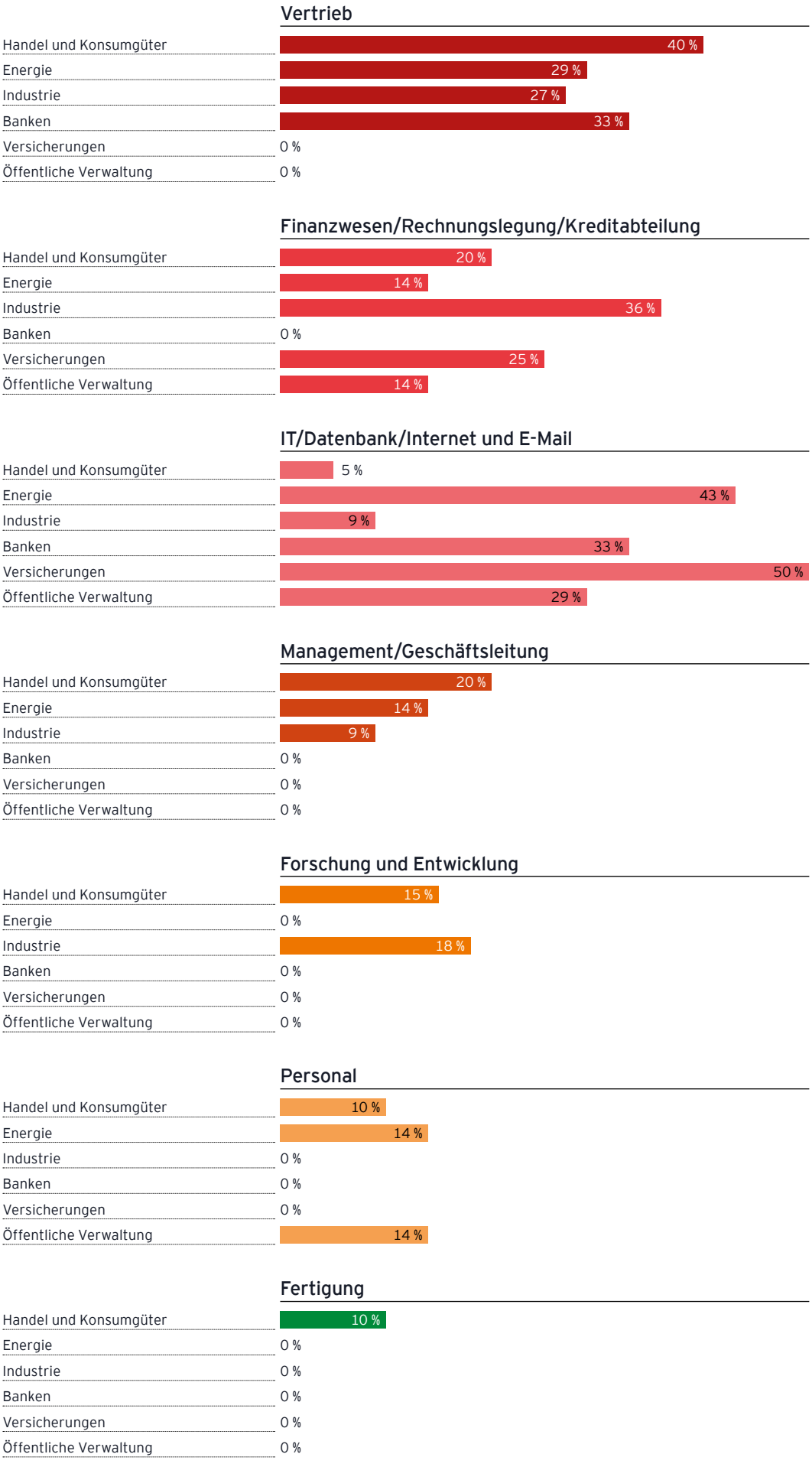


Abbildung 10 | Betroffene Bereiche je Branche

3.3

Welche konkreten Handlungen fanden statt?

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

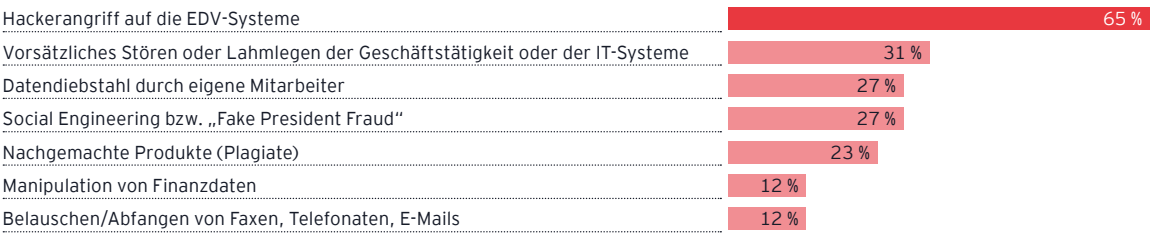


Abbildung 11 | Basis: Unternehmen, die bereits geschädigt wurden; Mehrfachnennungen möglich

Wie bereits in den Jahren zuvor sind die mit Abstand meisten Attacken Hackerangriffe auf die IT-Systeme (65 %). Zielte im Jahr 2017 noch jeder siebte Angriff auf das vorsätzliche Lahmlegen von IT-Systemen ab (14 %), so ist dies 2019 schon bei jedem dritten registrierten Angriff der Fall (31 %).

Dabei umfasst das vorsätzliche Stören oder Lahmlegen der Geschäftstätigkeiten oder der IT-Systeme auch die Verschlüsselung und den darauffolgenden Zugriffsverlust auf die eigenen Daten durch sogenannte Ransomware. Dabei handelt es sich um eine bösartige Schadsoftware (Malware), die den Zugriff auf Daten unmöglich macht und den Benutzer auf diese Weise sogar von seinem Gerät aussperren kann.

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.

Vor gerade einmal zwei Jahren 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 mit der Androhung einer Veröffentlichung der gestohlenen Daten ergänzt. Der tatsächliche Schaden für das Unternehmen lag deutlich über der Forderung der Täter.

Diese modernen Angriffsstrategien stellen Verantwortliche vor erhebliche 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 sind nicht ausreichend, Risikoszenarien müssen strategisch betrachtet und Maßnahmen ganzheitlich umgesetzt werden.

3.4

Wie wurden die kriminellen Handlungen aufgedeckt?

Rund jeder zweite Angriff wird durch das interne Kontrollsystem erkannt

Abbildung 12 | Basis: Unternehmen, die bereits geschädigt wurden; Mehrfachantworten möglich

Wie schon 2017 werden Angriffe in den häufigsten Fällen durch das interne Kontrollsystem identifiziert. Durch interne Routineprüfungen werden 26 % der Angriffe aufgedeckt; das ist eine Steigerung um 6 Prozentpunkte.

Die Dunkelziffer nicht aufgedeckter Angriffe wird höher sein, denn trotz interner Kontrollmechanismen und staatlicher Aktivitäten wird gut jeder siebte Angriff rein zufällig aufgedeckt.

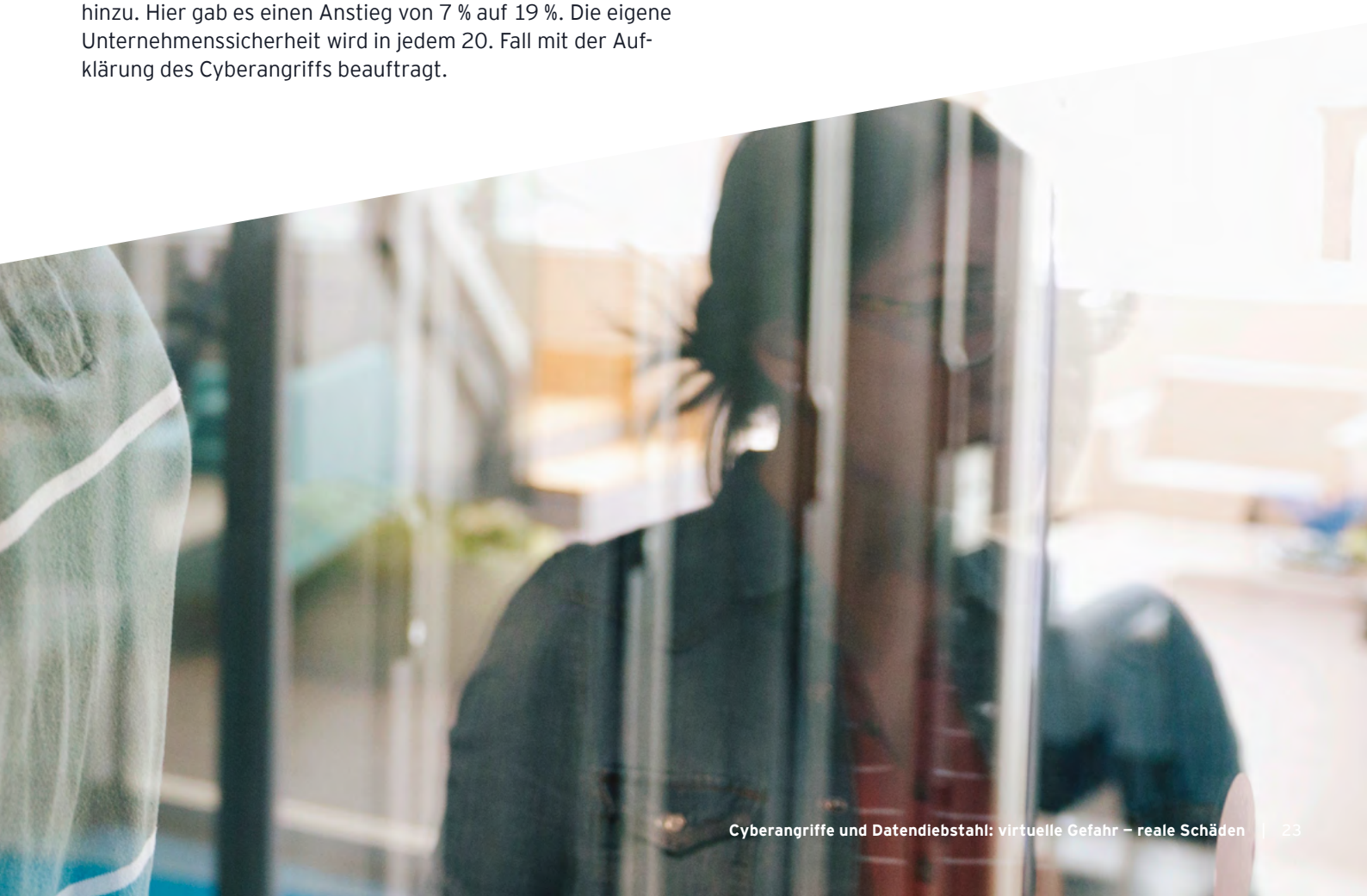
3.5

Wer wurde mit der Aufklärung beauftragt?

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

Abbildung 13 | Basis: Unternehmen, die bereits geschädigt wurden

Wird ein Cyberangriff bekannt, ist die IT-Abteilung in 63 % der Fälle die erste Anlaufstelle. Immer häufiger ziehen Unternehmen zur Aufklärung von Angriffen externe Dienstleister hinzu. Hier gab es einen Anstieg von 7 % auf 19 %. Die eigene Unternehmenssicherheit wird in jedem 20. Fall mit der Aufklärung des Cyberangriffs beauftragt.




© Christian Lendl

INTERVIEW

Die Vernetzung schafft schwer überschaubare Angriffsflächen

Margarete Schramböck, Bundesministerin für Digitalisierung und Wirtschaftsstandort, spricht im Interview über Vorteile und Risiken neuer Technologien, neue Kriminalitätsphänomene, die Gefahr zunehmender Vernetzung und über die Gründe, warum Cybersicherheit Schule machen sollte.

Interview

Frau Bundesministerin, die aktuelle EY-Studie Cybersecurity und Datendiebstahl zeigt eindeutig, dass Österreichs Führungskräfte das Gefahrenbewusstsein, Opfer von Cyberangriffen und Datendiebstahl zu werden, mehrheitlich als hoch einschätzen. Zudem erwartet der Großteil eine Verschärfung dieses Kriminalitätsphänomens. Wie bewusst müssen sich Unternehmen mit diesem Gefahrenpotenzial auseinandersetzen?

Die zunehmende Vernetzung im Umfeld der Digitalisierung macht Unternehmer immer anfälliger für Cyberangriffe und damit Datendiebstähle. Investitionen in die IT-Sicherheit heutzutage können noch nicht ganz mit einer Verschärfung der Bedrohungslage am Wirtschaftsstandort Österreich Schritt halten. Daher ist es unsere Aufgabe, Bewusstsein für solche Kriminalitätsphänomene zu schaffen. Das verstehen auch immer mehr Unternehmen.

Die Bundesregierung hat im Regierungsprogramm einen deutlichen Fokus auf die Themen Cyberkriminalität, -angriffe und -sicherheit gelegt, alleine diese Wörter kommen darin 35 Mal vor. Was sind die wichtigsten Schwerpunkte im Kampf gegen Cyberangriffe?

Für Cyberangriffe gibt es kein Allheilmittel. Vielmehr ist ein Mix aus vielen Maßnahmen gefragt, der kontinuierlich an sich verändernde Situationen angepasst werden muss. Wir haben eine Vielzahl an Initiativen im Regierungsprogramm vorgesehen. Zum einen müssen wir vorhandene Ressourcen bündeln, um damit effizienter im Cyber-Bereich werden zu können. Zum anderen brauchen wir neue effiziente Beratungs- und Informationsangebote, die auch Know-how liefern. Eine weitere Maßnahme den Wissenstransfer zwischen Bildung, Wissenschaft, Forschung und Wirtschaft zu stärken.

In den letzten Jahren gab es immer mehr Hinweise auf Cyberangriffe bzw. Datendiebstahl. Wie lässt sich dieser Anstieg erklären?

Gelegenheiten schaffen Täterinnen und Täter, zudem nimmt natürlich die Vernetzung von Computersystemen immer mehr zu. Dadurch entstehen schwer überschaubare Angriffsflächen. Und seit Jahren kann man eine höhere Anzahl an Schwachstellen in den Systemen erkennen. Gleichzeitig haben sich aber auch die Gegenmaßnahmen, um solche Schwachstellen einzudämmen, wesentlich verbessert. International lässt sich beobachten, dass nicht nur hochspezialisierte Technologie-Unternehmen oder Betreiber wesentlicher Dienste lohnenswerte Angriffsziele darstellen, sondern auch zunehmend Unternehmen, die beispielsweise Güter des täglichen Bedarfs herstellen.

Wie hoch ist die Aufklärungsrate bei Cyberangriffen und wer sind vorwiegend die Tätergruppen?

Laut dem Lagebericht Cybercrime 2019 des Bundesministeriums für Inneres sind die Anzeigen in der Kategorie Internetkriminalität von 2017 auf 2018 von 16.804 auf 19.627 gemeldete Fälle gestiegen. Die Aufklärungsquote lag 2018 bei 37,4 Prozent. Bei den Cybercrime-Delikten im engeren Sinn konnte 2018 ein Rückgang der Anzeigen um 13,4 Prozent festgestellt werden.

Wurde in den Jahren zuvor eher eine undefinierte Masse von Anwenderinnen und Anwendern attackiert, gerieten nun Klein- und Mittelunternehmen sowie Privatpersonen mit gezielten, aufwändigeren Angriffen in das Visier der Täter.

Steigt die Gefahr mit der zunehmenden Digitalisierung und Vernetzung der Wirtschaft und Gesellschaft?

Es stimmt, dass Veränderungen im Bereich der Digitalisierung rasch vor sich gehen. Diese Welle der Innovationen birgt weitreichende Potenziale, um neue Jobs zu schaffen und damit Wohlstand zu bilden. Starke Kooperationen zwischen der Wissenschaft und Forschung mit Unternehmen und dem Staat haben in der Vergangenheit die Durchdringung der Gesellschaft mit wegweisenden Technologien ermöglicht. Diese Technologien erleichtern unseren Alltag entscheidend. Gleichzeitig gehen damit aber natürlich auch Risiken einher. Das muss uns bewusst sein, sollte aber kein Grund sein, um sich zu fürchten. Für mich sind die Chancen klar im Vordergrund, und es ist unsere Aufgabe, ein Bewusstsein zu schaffen und alle für die Technologien zu wappnen.

Gibt es Branchen, die besonders im Fokus von Angreifern stehen?

Wie EY-Studie zeigt, gab es zuletzt konkrete Hinweise auf besonders häufige Cyberangriffe beziehungsweise Datendiebstahl bei Unternehmen im Bereich Handel und Konsumgüter sowie bei Versicherungsunternehmen. Insgesamt berichten dabei jeweils 40 Prozent der befragten Führungskräfte von Hinweisen auf Angriffe. Außerdem sind nach internationalen Erfahrungen auch Unternehmen im Bereich der Logistik besonders von Attacken betroffen. Cyberangriffe beschränken sich heutzutage nicht auf einzelne Branchen oder wenige Unternehmen. Das ist aber kein Grund, um der digitalen Revolution pessimistisch gegenüber zu stehen. Die Vorteile überwiegen. Demzufolge machen Cyberangriffe heutzutage nicht mehr vor einzelnen Branchen oder wenigen Unternehmen halt. Die digitale Revolution bringt eben neben einem Mehr an Chancen auch neue Risiken mit sich. Aber insgesamt überwiegen die Vorteile bei weitem.

Wie kann sich Österreichs Wirtschaft vor Cyberangriffen und Datendiebstahl schützen und wer trägt die Verantwortung dafür? Der Staat, die Unternehmen, die Bürgerinnen und Bürger – seit kurzem bietet das BKA ja z. B. Kurse für Cybersicherheit an?

Schutz bieten vor allem zukunftsweisende Kooperationen wie zwischen dem Staat und der EU, die mit einer Vorbildfunktion zwischen Wissenschaft und Forschung sowie zwischen den Unternehmen jeglicher Größe agieren sollten. Das setzt Mut voraus und den nötigen Einsatz, die auftretenden Herausforderungen gemeinsam anzugehen. Selbstverantwortung ist dabei ein bedeutsamer Aspekt. Der Staat bietet mit entsprechenden Instrumenten einen Rahmen und steht zur Seite. Auch Bürgerinnen und Bürger können sich an staatlichen Angeboten – wie etwa der Web-Plattform www.onlinesicherheit.gv.at oder Kursen des BKA – orientieren und Halt finden. Langfristig sollte Cybersicherheit bereits frühzeitig in der Schule behandelt werden, um ein Selbstverständnis für dieses Themenfeld zu entwickeln.

Die aktuelle EY-Studie unterstreicht, dass weiterhin in bestimmte technische und organisatorische Schutzmaßnahmen investiert wird. Worauf sollten Firmen achten, um sich gegen Cyberangriffe und Datenklau zu wappnen?

Die Unternehmen investieren bereits zielgerichtet in Maßnahmen gegen Cyberangriffe. Allerdings wird die Dynamik solcher Angriffe oft unterschätzt und Cybersicherheit spärlich als Prozess verstanden. Häufig wird Sicherheit nicht schon zu Beginn in IT-Systeme integriert und oft wird sie auch vergessen, wenn IT-Systeme nicht mehr benötigt oder durch neue Lösungen ersetzt werden. Vor diesem Hintergrund braucht es organisatorische Schutzmaßnahmen und die Umsetzung technischer Verfahren im gesamten Lebenszyklus von IT-Systemen.

Damit sich die Unternehmen auch in Zukunft schützen können, ist es auch wichtig, Expertinnen und Experten inhouse zu haben. Inwiefern wird hier die Ausbildung ausgebaut?

Ein ganz aktuelles Angebot stellt hier das BMDW gemeinsam mit der Wirtschaftskammer Österreich, mit der wir immer wieder Initiativen starten: So führen wir derzeit mit 20 Mio. Euro das erfolgreiche Programm KMU Digital weiter, mit dem die Unternehmen unter anderem ganz spezielle Unterstützung im Kampf gegen die Cyberkriminalität erhalten können. Unternehmenspraktika für Studierende im Security-Bereich sind ebenso besonders wertstiftend. Darüber hinaus wirkt die von meinem Ministerium und der Wirtschaft initiierte Fortbildungsplattform „fit4internet“ zum Ausbau der digitalen Kompetenzen – inklusive Cybersicherheit – der österreichischen Bevölkerung, wobei dieses Jahr auch noch spezielle Checks für Berufstätige angeboten werden.

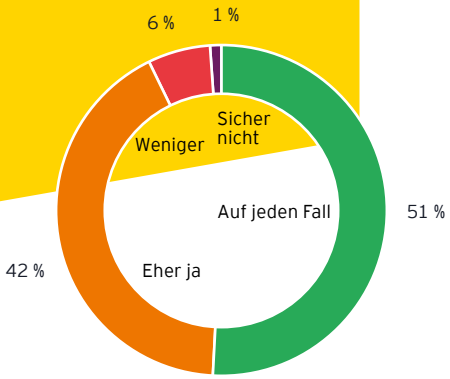
Frau Bundesministerin, vielen Dank für das Gespräch!

Prävention: Schützen sich die Unternehmen ausreichend?

4

4.1

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



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

Trotz der Bedrohung fühlen sich 93 % zumindest eher gut vor Cyberangriffen und Datendiebstahl geschützt. Vollkommen ruhig schlafen kann allerdings nur jeder zweite der Befragten. Jeder 14. hat nach eigener Aussage keine ausreichenden Vorkehrungen getroffen. Die gefühlte Sicherheit ist bei Unternehmen aller untersuchten Branchen und Größen vergleichbar hoch.

Zuständigkeit im Unternehmen für die zentralen Belange des Schutzes wichtiger Unternehmens-Assets

Abbildung 14 | Zuständigkeit nach Unternehmensbereich

Nach wie vor ist meist die interne IT-Abteilung mit dem Schutz sensibler Informationen und Daten betraut. 28 % der befragten Unternehmen nutzen externe Dienstleister für den Schutz sensibler Informationen. Im Vergleich zu 2017 ist das ein Zuwachs um 9 Prozentpunkte. Bei 13 % der befragten Führungskräfte wird der Schutz der sensitiven Daten als Chefsache gesehen – das ist ein leichter Zuwachs im Vergleich zu 2017 (10 %).

4.2

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

Investitionen in gesicherte Serverbereiche bei mehr als der Hälfte der Unternehmen

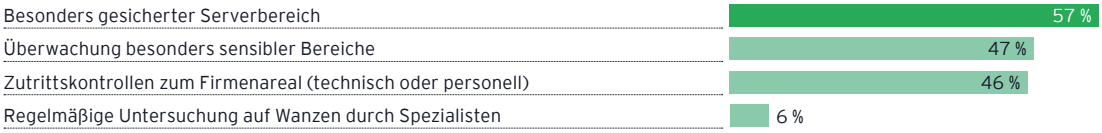


Abbildung 15 | Mehrfachantworten möglich

57 % der Unternehmen haben in einen besonders gesicherten Serverbereich investiert. Jeweils rund die Hälfte hat die Überwachung besonders sensibler Bereiche (47 %) sowie personelle Zutrittskontrollen zum Firmenareal (46 %) verbessert.

Eine regelmäßige Prüfung von Räumlichkeiten auf Abhörtechnik haben 6 % der Unternehmen in den vergangenen zwei Jahren durch Spezialisten durchführen lassen.

4.3

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

Unternehmen investieren in Passwortschutz, Antivirensoftware und Firewalls

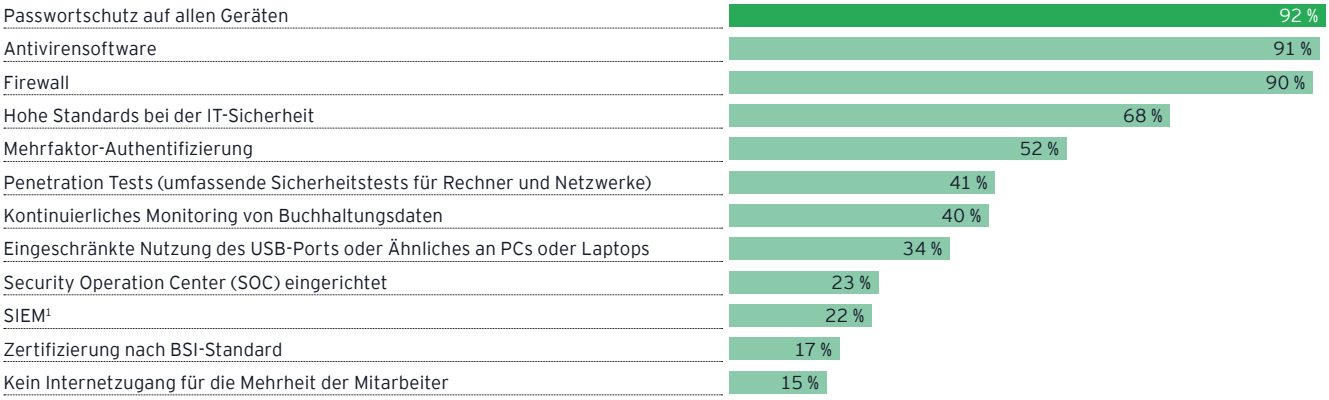


Abbildung 16 | Mehrfachantworten möglich

Unternehmen setzen weiterhin primär auf konventionelle Sicherheitsvorkehrungen. 90 % oder mehr der befragten Unternehmen haben in Passwortschutz, Antivirensoftware oder Firewalls investiert. Im Vergleich zu 2017 haben die Schutzvorkehrungen in den Unternehmen auch in anderen Bereichen zugenommen. 68 % der Unternehmen geben hohe Standards bei der IT-Sicherheit (2017: 54 %) und 41 % (2017: 28 %) Penetration Tests als Investitionsgrund an. Insbesondere Versicherungsunternehmen haben in den vergangenen beiden Jahren erheblich aufgerüstet bzw. nachjustiert.

1 „SIEM" steht für Security Information and Event Management. Es hilft, Unregelmäßigkeiten in IT-Systemen und im Netzwerk zu erkennen)

4.4

Welche der folgenden Sicherheitsvorkehrungen haben Sie im Bereich Personal getroffen?

Mehr als vier von fünf Unternehmen nutzen Geheimhaltungsverpflichtungen in Arbeitsverträgen

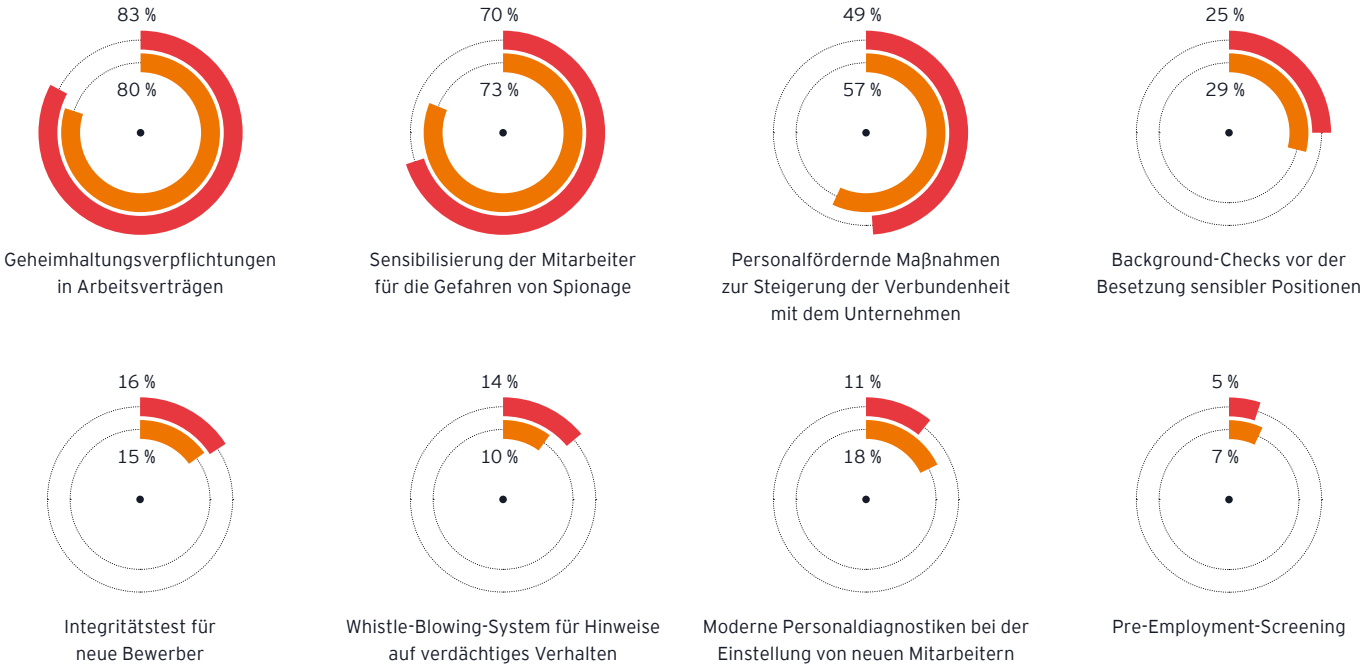


Abbildung 17 | Mehrfachantworten möglich

Die überwiegende Mehrheit der Unternehmen setzt auf Geheimhaltungsvereinbarungen in Arbeitsverträgen. Etwa sieben von zehn Unternehmen setzen auf eine Sensibilisierung ihrer Mitarbeiter für die Gefahren von Cyberangriffen bzw. Datendiebstahl. Dias ist definitiv eine gute Nachricht, denn derartige Maßnahmen, um das Sicherheitsbewusstsein jeder und jedes Einzelnen im Unternehmen zu erhöhen, sind ein unverzichtbarer Bestandteil erfolgreicher Sicherheitskonzepte.

Sicherheitsbewusstsein

Aus der Praxis

Die Wirksamkeit von Maßnahmen für das Sicherheitsbewusstsein („Awareness-Maßnahmen“) hängt von zahlreichen Faktoren ab: von der praktischen Umsetzbarkeit der Empfehlungen bis hin zur Kommunikations- und Führungskultur.

Die meisten Unternehmen führen regelmäßig Maßnahmen zur Sensibilisierung der Mitarbeiter in Bezug auf unterschiedliche Aspekte der Cybersicherheit durch. Zwei entscheidende Stellen im Unternehmen bleiben dabei nicht selten unberücksichtigt: das Sicherheitsmanagement und die IT selbst. Beide Gruppen benötigen spezifische Informationen und Fähigkeiten, um den heute verbreiteten, hochgradig integrierten Angriffstechniken wirkungsvoll begegnen zu können.

Neben Erfahrung und spezifischen technischen Fähigkeiten erfordern Design und Umsetzung wirkungsvoller Awareness-Maßnahmen auch Kenntnisse in anderen Fachgebieten, von effektiver Kommunikation über die richtige Präsentation bis hin zur Verhaltenspsychologie in der Unternehmenssicherheit.

Eine Awareness-Kultur sollte von innen nach außen aufgebaut werden. Sicherheitsverantwortliche wie Chief Security Officers (CSOs) und deren Teams und auch Sicherheitspraktiker wie die IT-Abteilung oder der User Help Desk sollten frühzeitig und umfassend geschult werden. Dadurch können gemeinsam Awareness-Maßnahmen (mit)gestaltet und implementiert werden, die praktisch umsetzbar und vollständig in die Unternehmensprozesse integriert sind.

Auf diese Weise werden Awareness-Maßnahmen zu einer gewinnbringenden Investition nicht nur in die Sicherheit, sondern auch in die Zukunft des eigenen Unternehmens.

4.5

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

Unternehmen setzen auf klare Regelungen zum Umgang mit schützenswerten Informationen

Abbildung 18 | Mehrfachantworten möglich

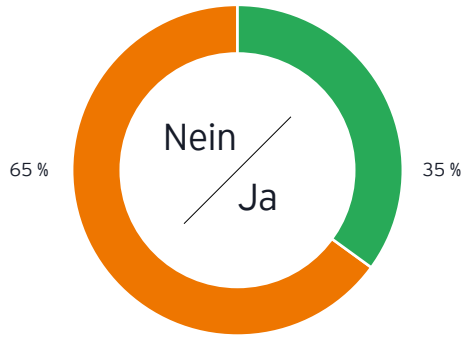
2019 2017

Die Mehrzahl der befragten Unternehmen (69 %) legt klare Regeln für den Umgang mit sensiblen Informationen fest. 58 % verpflichten ihre Geschäftspartner zur Geheimhaltung. 55 % haben einen Sicherheitsverantwortlichen bestellt. Immerhin jeder Vierte setzt bereits auf abhörsichere Kommunikation.

4.6

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

Mindestens jedes dritte 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: 35 % der befragten Unternehmen haben inzwischen nach eigenen Angaben eine solche Versicherung abgeschlossen.

Besonders hoch ist der Anteil der Unternehmen mit Versicherungsschutz in der Versicherungs-, der Energie- und der Bankenbranche.

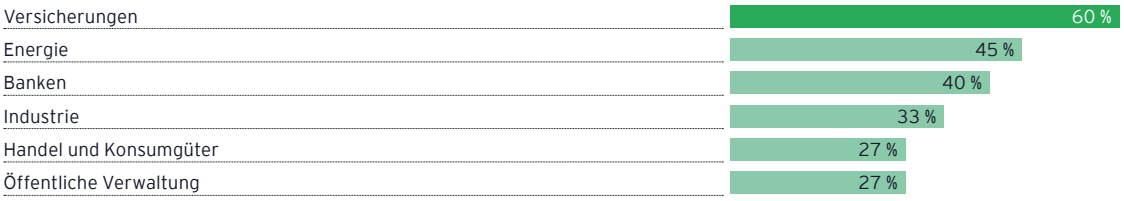


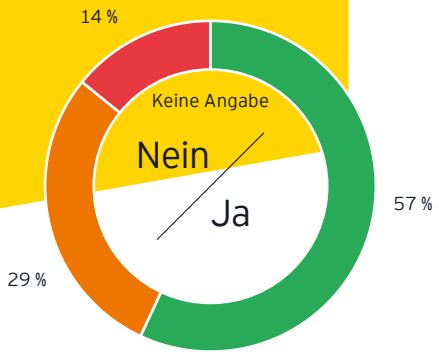
Abbildung 19 | Versicherung gegen digitale Risiken je Branche

Krisenpläne und Kommunikation

5

5.1

Hat Ihr Unternehmen Krisenpläne zur Reaktion auf Datendiebstahl-fälle vorbereitet?



57 % der Betriebe haben Krisenpläne

Für Unternehmen ist Datendiebstahl ein ernst zu nehmendes Risiko. Dabei verfügen 57 % der befragten Unternehmen nach eigenen Angaben über Krisenpläne, die das Vorgehen im Falle eines entdeckten Datenklaus definieren. Rund ein Drittel der Unternehmen hat bisher noch keinen Plan für ein Notfallszenario vorbereitet.

Bei Unternehmen aus der Versicherungs- und Bankenbranche liegt der Anteil mit Krisenplänen sogar bei 100 % bzw. 84 %. Bei Energieversorgern haben zwei Drittel einen Krisenplan für den Ernstfall vorbereitet.

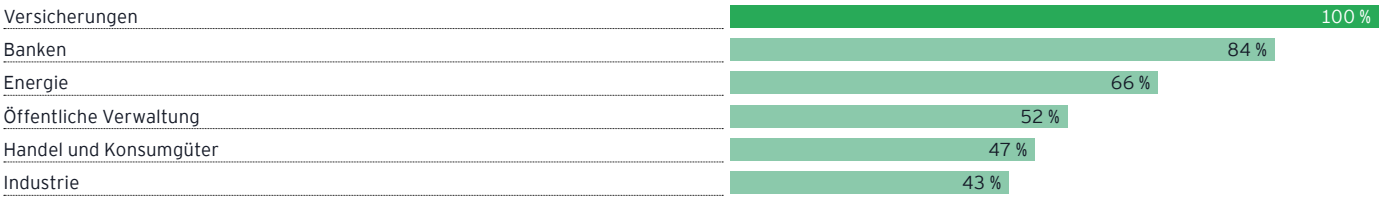
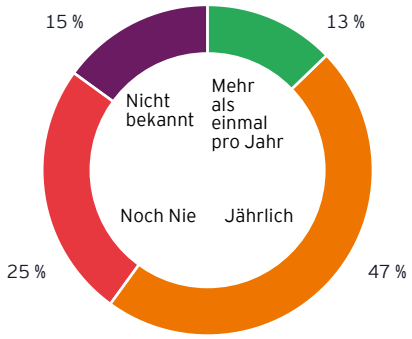


Abbildung 20 | Anteil „Ja“ nach Branche

5.2

Falls Ihr Unternehmen Krisenpläne zur Reaktion auf Datenklaufälle besitzt: Wie häufig werden die Abläufe des Krisenplans „Datendiebstahl“ geübt?

Nur 60 % üben Krisenpläne zumindest ein Mal im Jahr



Sobald ein Angriff auf IT und Daten erkannt wird, sollte ein Unternehmen möglichst schnell handlungsfähig sein. Hierfür ist eine Übung der Abläufe eines Krisenplans essenziell. So werden bei 60 % der Unternehmen mindestens einmal jährlich die Abläufe der Krisenpläne geübt, 25 % der befragten Unternehmen gaben hingegen an, die Abläufe noch nie geübt zu haben.

Mehr als zwei von drei größeren Unternehmen (68 %), die über Krisenpläne zur Reaktion auf Datenklaufälle verfügen, üben die Umsetzung dieser Pläne mindestens einmal pro Jahr. Bei den kleineren Unternehmen liegt der Anteil bei nur 52 %.

Abbildung 21 | Anteil „Mindestens einmal pro Jahr“

Krisenmanagement

Aus der Praxis

57 % der für diese Studie befragten Unternehmen haben einen Krisenplan für das Risiko/Notfallszenario „Datendiebstahl“ ausgearbeitet und implementiert. Im Grunde sollte diese Quote bei über 90 % liegen, denn Cyberangriffe und Attacken auf Daten können jede Organisation zu jeder Zeit treffen. Es kann nicht oft genug betont werden: Unternehmen müssen frühzeitig für mögliche Fälle von Cyberangriffen und Datendiebstahl vorsorgen.

Kommt erst im Ernstfall die Frage auf, wer eingebunden werden muss, wer welche Aktionen durchführen kann, wie die Arbeit strukturiert werden sollte und wie insbesondere die Kommunikation – nach innen wie nach außen – gestaltet wird, geht wertvolle Zeit verloren.

Die Studie zeigt, dass die akribische Vorbereitung auf Krisen in Österreich tendenziell immer noch eine Frage der Größe ist. Während fast zwei von drei größeren Unternehmen über Krisenpläne verfügen, ist es bei kleineren nur die Hälfte. Darüber hinaus gilt: Je größer das Unternehmen, desto intensiver und häufiger wird der Ablauf im Krisenfall geübt.

Die Vorbereitung auf den Ernstfall darf keine Frage der Größe sein. Wurde ein Angriff auf IT und Daten erkannt, kommt es darauf an, schnell und systematisch zu reagieren. Wie auch beim Sport lässt sich die Reaktionsfähigkeit trainieren. (Viel) Üben hilft. Qualifizierte Krisenmanager sind reaktionsfähiger als ad hoc eingesetzte Amateure.

Nur 43 % der befragten Unternehmen, also nicht einmal jedes zweite, gaben an, ein zentrales Krisenteam zu besitzen. Ob komplexe Cyberattacken oder anderweitige größere Vorfälle – Krisen können sich auf vielfältige Weise entwickeln. Viele Firmenlenker mögen nach dem Motto agieren, dass sie jeden Tag mit Krisen konfrontiert werden – und dann einfach die Ärmel hochkrempeln und handeln. Schließlich hat das bisher immer geklappt. Diese Einstellung mag pragmatisch sein, zu resilientem Krisenmanagement führt sie nicht.

Koordinieren qualifizierte Krisenteams von Anfang an Informationsflüsse, Entscheidungsprozesse und Maßnahmen, können unvorhergesehene Ereignisse wie Cyberangriffe bzw. Datenklau erfolgreicher bewältigt werden.

5.3

Existiert in Ihrem Unternehmen ein zentrales Krisenteam (unabhängig vom Thema Datendiebstahl)?

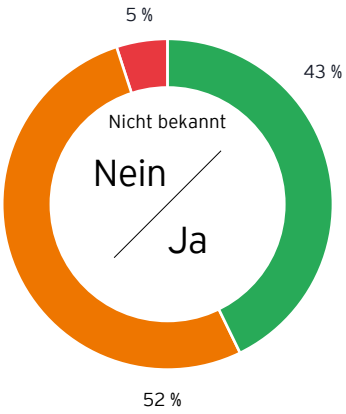


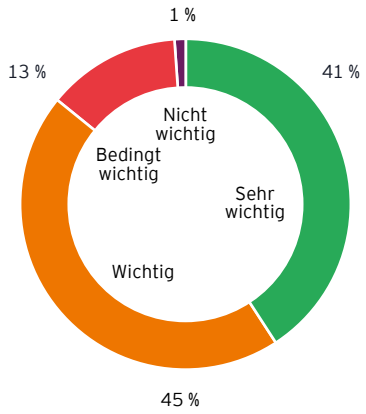
Abbildung 22 | Existenz eines zentralen Krisenteams

Mehr als die Hälfte hat kein zentrales Krisenteam etabliert

Qualifizierte Krisenteams sind ein wichtiger Bestandteil des Krisenmanagements bei einem Cyberangriff. Mit 52 % hat mehr als die Hälfte der befragten Unternehmen kein zentrales Krisenteam etabliert, 43 % der Unternehmen verfügen über ein solches.

5.4

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



Bei Datendiebstahl: Vier von fünf Unternehmen setzen auf fallbegleitende Kommunikation

Im Krisenfall spielt die Kommunikation, intern wie auch extern, eine bedeutende Rolle. Gut vier von fünf Unternehmen geben an, dass ihnen im Falle eines entdeckten Datenklaus eine fallbegleitende interne und externe Kommunikation wichtig oder sogar sehr wichtig sei. Lediglich 14 % der Unternehmen halten eine solche Kommunikation im Ernstfall für nur bedingt oder gar nicht wichtig.

Insbesondere Banken, Versicherungen und auch Unternehmen aus dem Bereich Handel und Konsumgüter halten die Kommunikation in der Krise für sehr wichtig.

Abbildung 23 | Relevanz einer fallbegleitenden Kommunikation je Branche

Die wichtigsten Ergebnisse

Spot on Sector

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:

Hacktivisten

Organisiertes Verbrechen

Ausländischer Geheimdienst/Staatliche Stelle

Angriffsfälle

entdeckten in den vergangenen fünf Jahren **einen Angriff** auf ihr Unternehmen.

wurden **mehrfach Opfer** von Angriffen. **Am häufigsten** angegriffen wurden: Vertrieb (40 %), Finanzwesen (20 %) und Management (20 %).

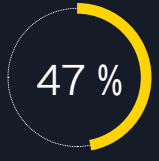
wurden bereits erpresst.

Prävention

sind sicher, dass die eigenen Präventionsmaßnahmen **wirkungsvoll** sind.

haben eine **Versicherung gegen digitale Risiken** abgeschlossen.

Krisenmanagement



haben **Krisenpläne** zur Reaktion auf Angriffe.

üben die Abläufe zumindest einmal im Jahr.

Interview Martin Unger

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

Interview

Wofür werden Daten im Handel und in der Konsumgüterindustrie genutzt und wie wichtig sind sie?

Kein anderer Sektor war durch die Möglichkeiten von „Big Data" mehr inspiriert als der Handel und die Konsumgüterindustrie. Die Sammlung von Daten – beispielsweise durch Clubmitgliedschaften – kann richtig eingesetzt zum Know-how-Hub in Bezug auf die eigene Kundenlandschaft, zur Anpassung des Produktsortiments und für Marketingmaßnahmen werden. Die zunehmende Präsenz von Online-Plattformen verstärkt diese Entwicklung massiv. Zusätzlich werden auch die Abläufe im Hintergrund systematisch digitalisiert, im Handel beispielsweise bei blockchainbasierten Lieferketten und vernetzten Kassensystemen, in der Konsumgüterindustrie durch Sensortechniken, die die produzierenden Geräte miteinander vernetzen.

Was macht Handels- und Konsumgüterunternehmen für Datendiebstahl und Cyberangriffe besonders interessant?

Vor allem die sehr breite Kundenbasis. Mit nur einem einzigen Cyberangriff kann eine hohe Anzahl Daten auf einmal gestohlen werden. Für Handelsunternehmen ist es deshalb unabdinglich, Daten sicher zu verwahren. Außerdem ist die Branche systemkritisch: Konsumgütererzeuger produzieren Lebensmittel, die von Handelsunternehmen verkauft werden – sie sind damit unentbehrlich für eine funktionierende Infrastruktur. Es ist gut, dass sich der österreichische Handel und die Konsumgüterindustrie dieser Verantwortung bewusst sind: Laut unserer Umfrage nehmen 85 Prozent der Handels- und Konsumgüterunternehmen eine steigende Gefahr von Angriffen auf ihr Unternehmen wahr – vor allem durch Hacker-Aktivisten oder organisiertes Verbrechen. Zwei von fünf Unternehmen haben in den letzten fünf Jahren sogar einen Angriff auf ihren Betrieb entdeckt. Am häufigsten betroffen waren die Unternehmensbereiche Vertrieb und Finanzwesen, aber auch das Management. Fast ein Fünftel der österreichischen Handels- und Konsumgüterunternehmen wurde sogar schon einmal erpresst.

Was ist in der Handels- und Konsumgüterbranche das Worst-Case-Szenario bei Cyberangriffen?

Das können ganz unterschiedliche Szenarien sein, deren Schadensausmaß sich im Vorfeld nicht genau ausmachen lässt und in jedem einzelnen Fall extreme Ausmaße annehmen kann. Durch die zunehmende Digitalisierung und die steigende Anzahl vernetzter Geräte werden sowohl die Produktion und die Lieferung als auch der Verkauf selbst zum interessanten Angriffsziel. Aus unserer Sicht am schwerwiegendsten sind aber eindeutig die Kundendaten. Durch die breite Kundenbasis können bei Datendiebstählen große Mengen an Daten von Tausenden Kunden gestohlen werden. Diese Datendiebstähle können nicht nur zu Rechtsstreiten führen, sie schmälern auch das Vertrauen der Kunden – und haben damit auch eine reale Auswirkung auf den Umsatz.

Was können Unternehmen tun, um sich besser auf Cyberangriffe vorzubereiten?

Sie kennen das Sprichwort „Vorsicht ist besser als Nachsicht"? Das trifft definitiv auf Cyberangriffe zu. Alles, was Sie im Vorfeld tun können, sollten Sie tun. Das hilft Ihnen dabei, im Ernstfall richtig zu reagieren und den Schaden zu minimieren. Ganz grundsätzlich sollte aber natürlich darauf geachtet werden, dass IT-Systeme immer den neuesten Standards entsprechen, kontinuierlich weiterentwickelt werden und auch mit simulierten Attacken auf ihre Resistenzfähigkeit getestet werden.

Die wichtigsten Ergebnisse

Spot on Sector | 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:

Organisiertes Verbrechen

Hacktivisten

Konkurrierendes ausländisches Unternehmen

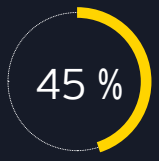
Angriffsfälle

entdeckten in den vergangenen fünf Jahren **einen Angriff** auf ihr Unternehmen.

wurden **mehrfach Opfer** von Angriffen. **Am häufigsten** angegriffen wurden: Finanzwesen (36 %), Vertrieb (27 %) und Forschung und Entwicklung (18 %).

wurden bereits erpresst.

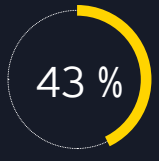
Prävention



sind sicher, dass die eigenen Präventionsmaßnahmen **wirkungsvoll** sind.

haben eine **Versicherung gegen digitale Risiken** abgeschlossen.

Krisenmanagement



haben **Krisenpläne** zur Reaktion auf Angriffe.

üben die Abläufe zumindest einmal im Jahr.

Interview Gerhard Schwartz

Gerhard Schwartz
Leiter Industrial Products
und Leiter Wirtschaftsprüfung
bei EY Österreich

Interview

Wofür werden Daten in der Industrie genutzt und wie wichtig sind sie?

Daten werden in der Industrie vor allem zur Steuerung von Industrieanlagen unter dem Stichwort Internet of Things genutzt. Geräte, Maschinen und ganze Produktionsprozesse werden zunehmend digitalisiert und sind über Sensoren miteinander vernetzt. So wird natürlich auch eine große Menge an Daten generiert. Wer diese Daten richtig analysiert und in den richtigen Zusammenhang setzt, kann beispielsweise notwendige Maschinenwartungen prognostizieren, Lieferengpässe vermeiden und insgesamt eine bessere Auslastung der Produktion ermöglichen. Gleichzeitig aber bietet diese Datenmenge und dessen Nutzung eine neue Angriffsflanke für Cyberkriminelle.

Was macht Industrieunternehmen für Datendiebstahl und Cyberangriffe besonders interessant?

Datendiebstähle und Cyberangriffe sind durch die zunehmende Digitalisierung der industriellen Produktion ein ernstzunehmendes Risiko. Sie bergen die Gefahr, dass Kundendaten oder Entwicklungspläne gestohlen werden, die gesamte Produktion stillsteht oder sogar mit Fehlern produziert und das Unternehmen in weiterer Folge erpresst wird. Die Industrie ist aus mehreren Gründen ein interessantes Ziel für Hacker: Zum einen gibt es Kunden- und Zahlungsdaten, die vermehrt in den Fokus solcher Attacken rücken. Zum anderen wird viel in die Forschung und Entwicklung von Produkten investiert. Wenn eben diese Entwicklungspläne gestohlen werden, könnten Kriminelle Lösegeld dafür fordern. Der Bereich Forschung und Entwicklung ist neben dem Finanzwesen und dem Vertrieb am häufigsten von Attacken auf österreichische Industrieunternehmen betroffen.

Was ist im Industriesektor das Worst-Case-Szenario bei Cyberangriffen?

Das Worst-Case-Szenario ist ein großer finanzieller Schaden. 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 Kundendaten gestohlen werden. Daraus könnten sich längere gerichtliche Prozesse und Schadensersatzforderungen ergeben. Der Diebstahl der eigenen Finanzdaten ist ebenfalls ein großes Risiko. Mitarbeiter sind ein potenzielles Gateway – Stichwort „Fake President Fraud". Solche Fälle gehen mit jahrelangen Rechtsstreitigkeiten, Entlassungen des Vorstandes und Einbrüchen des Aktienkurses einher.

Was können Industrieunternehmen tun, um sich besser auf Cyberangriffe vorzubereiten?

Genau das – Unternehmen müssen sich vorbereiten. Kein IT-System der Welt ist zu 100 Prozent vor Cyberangriffen sicher. Das ist das Risiko, das mit der Digitalisierung einher geht. Aber man kann sich gut drauf vorbereiten. Einerseits, indem man die Systeme selbst laufend testet und weiter optimiert. Andererseits, indem man die Mitarbeiter über Risiken aufklärt und über vorbeugende Maßnahmen informiert. Letztendes ist es auch wichtig, sich auf den Ernstfall vorzubereiten: Ein Krisenplan mit klar definierten Teammitgliedern, Kommunikationswegen und Entscheidungsketten ermöglichen im schlimmsten Fall ein schnelles und geordnetes Vorgehen.

Die wichtigsten Ergebnisse

Spot on Sector | 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:

Organisiertes Verbrechen

Hacktivisten

Ausländischer Geheimdienst/Staatliche Stelle

Angriffsfälle

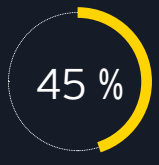
entdeckten in den vergangenen fünf Jahren **einen Angriff** auf ihr Unternehmen.

wurden **mehrfach Opfer** von Angriffen. **Am häufigsten** angegriffen wurden: IT-Systeme (43 %), Vertrieb (29 %) und Personalwesen (14 %).

wurden bereits erpresst.

Prävention

sind sicher, dass die eigenen Präventionsmaßnahmen **wirkungsvoll** sind.



haben eine **Versicherung gegen digitale Risiken** abgeschlossen.

Krisenmanagement

haben **Krisenpläne** zur Reaktion auf Angriffe.

üben die Abläufe zumindest einmal im Jahr.

Interview Stefan Uher

Stefan Uher
Leiter Energy bei EY Österreich

Interview

Wofür werden Daten in der Energiebranche genutzt und wie wichtig sind sie?

In der Energiebranche ist die Digitalisierung im vollen Gange. Smart Homes, Smart Meters, Smart Cities sind nur einige Schlagworte in dem Zusammenhang. Der Trend hin zum Digitalen eröffnet Kunden neue Möglichkeiten, ihren eigenen Verbrauch besser zu steuern, und auch die Energieversorgungsunternehmen selbst werden immer digitaler. Durch diese Trends werden große Mengen an Daten erzeugt, die Energieunternehmen und die Verbraucher selbst nutzen können.

Was macht Energieversorger und -dienstleister für Datendiebstahl und Cyberangriffe besonders interessant?

Energieunternehmen müssen sich bewusst sein, dass ihre Daten und Systeme ein interessantes Ziel für Cyberkriminelle sind. Ein Stromausfall kann schnell zum Desaster für ganze Regionen und Staaten werden. Das ist der Grund, warum die österreichische Energiebranche das Risiko von Cyberattacken sehr ernst nimmt. Derzeit gehen laut unserer Umfrage vier von fünf Energiedienstleister davon aus, dass das Risiko von Cyberangriffen zunimmt, mehr als 40 Prozent schätzen das Risiko sogar als sehr hoch bzw. hoch ein. Die Energiebranche sieht sich vor allem durch organisiertes Verbrechen bedroht. Ein Viertel hat in den letzten Jahren einen Angriff auf das eigene Unternehmen entdeckt. Jedes fünfte Energieunternehmen wurde sogar bereits erpresst.

Was ist in der Energiebranche das Worst-Case-Szenario bei Cyberangriffen?

Schwerwiegend wäre beispielsweise ein flächendeckender Stromausfall – also ein Blackout. Ein länger andauernder Stromausfall bedeutet, dass die gesamte Infrastruktur einer Stadt, einer Region oder eines Landes zum Erliegen kommt. Niemand kann Lebensmittel kaufen, niemand kann Geld abheben, Heizungen fallen aus, die Wasserversorgung und das Telefonnetz brechen zusammen, ganz zu schweigen vom vollkommenen Stillstand der gesamten Wirtschaft – immerhin ist heute so gut wie jeder Arbeitsplatz mit einem Computer ausgestattet und mit dem Internet verbunden. Auch die Manipulation von Smart Meters oder der Diebstahl von Kundendaten sind schwerwiegend für Energieversorger. Kundendaten sind insofern kritisch, als Cyberkriminelle oft mit Veröffentlichung drohen, um Lösegeld zu erpressen. Hinzu kommen sämtliche Szenarien, die alle Branchen gleichermaßen treffen können. Dazu zählt beispielsweise die Infiltrierung des Betriebs über E-Mail-Systeme und USB-Sticks. Auch die eigenen Mitarbeiter werden oft als Zutrittskarte missbraucht. Cyberkriminelle können über gefälschte E-Mail-Adressen als vermeintliche Vorgesetzte Arbeitsanweisungen erteilen und hohe Geldbeträge überweisen lassen.

Was können Unternehmen tun, um sich besser auf Cyberangriffe vorzubereiten?

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 wichtigsten Ergebnisse

Spot on Sector

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:

Hacktivisten

Organisiertes Verbrechen

Ausländischer Geheimdienst/Staatliche Stelle

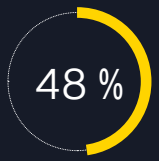
Angriffsfälle

entdeckten in den vergangenen fünf Jahren **einen Angriff** auf ihr Unternehmen.

wurden **mehrfach Opfer** von Angriffen. **Am häufigsten** angegriffen wurden: IT-Systeme (29 %), Finanzwesen (14 %) und Personal (14 %).

wurden bereits erpresst.

Prävention



sind sicher, dass die eigenen Präventionsmaßnahmen **wirkungsvoll** sind.

haben eine **Versicherung gegen digitale Risiken** abgeschlossen.

Krisenmanagement

haben **Krisenpläne** zur Reaktion auf Angriffe.

üben die Abläufe zumindest einmal im Jahr.

Interview Christoph Harreither

Christoph Harreither
Leiter Government & Public Sector
bei EY Österreich

Interview

Wofür werden Daten im öffentlichen Bereich genutzt und wie wichtig sind sie?

Der digitale Wandel wirkt sich nicht nur auf Städte und Gemeinden, sondern im gesamten öffentlichen Sektor aus. Österreich gehört zu Europas Vorreitern und belegt im aktuellen E-Government-Benchmarking der Europäischen Kommission den sechsten Platz von 34 untersuchten Ländern. Besonders gut schneidet Österreich in den Bereichen grenzüberschreitende Mobilität und benutzerorientierte Regierung ab. Darunter fallen die Online-Verfügbarkeit von Dienstleistungen, Online-Support und Help Services. Über all diese Kanäle werden neben den schon lange bestehenden Systemen, beispielsweise im Meldewesen, zusätzlich Daten gesammelt.

Was macht die Politik und den öffentlichen Sektor für Datendiebstahl und Cyberangriffe besonders interessant?

Der gesamte öffentliche Sektor ist für die Aufrechterhaltung der Infrastruktur verantwortlich. Das macht diesen Bereich natürlich zum interessanten Angriffsziel. Früher wurden die Kriege auf dem Schlachtfeld geführt, heute verlagern sich feindliche Angriffe vermehrt ins Netz. Natürlich steigt mit der zunehmenden 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 vier von fünf der Befragten aus der öffentlichen Verwaltung, dass die Gefahr von Cyberangriffen weiter steigen wird. Sie sehen sich vor allem durch Hacker-Aktivisten und das organisierte Verbrechen bedroht.

Was ist im öffentlichen Sektor das Worst-Case-Szenario bei Cyberangriffen?

Für Parteien und politische Entscheidungsträger 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 Patienten 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 Unbekannten steht, selbst wenn es sich „nur" um eine Meniskusoperation handelt. Aber auch Verkehrsnetze oder die Grundversorgung mit Wasser und Strom sind kritisch für die Aufrechterhaltung unseres Systems – eine Übernahme durch feindliche Angreifer kann zu sozialen Unruhen, sinkender Attraktivität des Wirtschaftsstandortes und Vertrauensverlusten in der Bevölkerung führen.

Was kann der öffentliche Sektor tun, um sich besser auf Cyberangriffe vorzubereiten?

Das richtige Schlagwort ist in diesem Zusammenhang Cybersicherheit, nicht Cyberangriffe. IT-Systeme und digital vernetzte Geräte müssen sicher sein und die Mitarbeiter der öffentlichen Verwaltung müssen sich der Gefahr von Cyberangriffen bewusst sein. Außerdem muss 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.

Die wichtigsten Ergebnisse

Spot on Sector | 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:

Hacktivisten

Organisiertes Verbrechen

Ausländischer Geheimdienst/Staatliche Stelle

Angriffsfälle

entdeckten in den vergangenen fünf Jahren **einen Angriff** auf ihr Unternehmen.

wurden **mehrfach Opfer** von Angriffen. **Am häufigsten** angegriffen wurden: Vertrieb (33 %) und IT-Systeme (33 %).

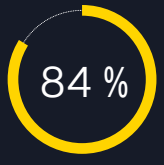
wurden bereits erpresst.

Prävention

sind sicher, dass die eigenen Präventionsmaßnahmen **wirkungsvoll** sind.

haben eine **Versicherung gegen digitale Risiken** abgeschlossen.

Krisenmanagement



haben **Krisenpläne** zur Reaktion auf Angriffe.

üben die Abläufe zumindest einmal im Jahr.

Interview Armin Schmitt

Armin Schmitt
Leiter Financial Services Banking
bei EY Österreich

Interview

Wofür werden Daten im Bankensektor genutzt und wie wichtig sind sie?

Das Bankgeschäft war schon immer ein Geschäft mit Daten. Und: Es wird immer digitaler. Geld überweisen oder Kredite beantragen – zwei von drei Bankkunden erledigen diese Aufgaben mittlerweile online oder über Apps. Mit der steigenden Digitalisierung werden natürlich noch mehr Daten generiert. Die Banken setzen alles daran, dass die hochsensiblen Finanzdaten ihrer Kunden geschützt werden.

Was macht Banken für Datendiebstahl und Cyberangriffe besonders interessant?

Die Bedrohung für Banken steigt zunehmend – oft werden die Kunden selbst durch betrügerische E-Mails und vermeintliche Sicherheitsabfragen Opfer von Cyberangriffen. Die österreichischen Banken sind sich durchaus bewusst, dass sie eine große Verantwortung tragen, und beobachten die Entwicklungen deshalb sehr genau. Derzeit gehen laut unserer Umfrage fast alle der befragten österreichischen Banken davon aus, dass die Gefahr von Angriffen weiter steigt – 92 Prozent, so viele wie in keiner anderen Branche. Mehr als die Hälfte schätzt das Risiko als hoch bzw. sehr hoch ein. Ein Großteil der Banken hat deswegen Krisenpläne zur richtigen Reaktion, fast drei Viertel üben die Abläufe im Falle eines Hackerangriffs zumindest einmal pro Jahr. Das sind schon sehr hohe Werte, die zeigen, wie wichtig dieses Thema für Österreichs Banken ist.

Was ist für Banken das Worst-Case-Szenario bei Cyberangriffen?

„Hundertausende Kundendaten der Musterbank gestohlen" ist wohl nichts, was man morgens in der Zeitung lesen möchte – weder als Kunde noch als Vorstand dieser Bank. Cyberangriffe gehen gerade bei Banken immer mit hohen Strafzahlungen und einer massiven Imageschädigung einher. Für Banken, deren Geschäft vorwiegend auf Vertrauen basiert, ist das besonders tragisch, immerhin gehören die eigenen Finanzdaten für Bankkunden zu den sensibelsten Daten überhaupt. Deshalb ordnen wir „Phishing" als eine der schwerwiegendsten Cyberattacken auf Banken ein. Dabei werden Zugriffsdaten auf die Finanzportale der Kunden abgegriffen und das Geld der Kunden gestohlen. Oder die Bank wird zur Lösegeldzahlung erpresst, damit die Kundendaten 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.

Was können Unternehmen tun, um sich besser auf Cyberangriffe vorzubereiten?

Banken sind intensiv gefordert, alles zu tun, um Cyberattacken vorzubeugen und das Risiko zu minimieren. Dazu gibt es auch umfassende regulatorische Vorgaben, die umgesetzt und eingehalten werden müssen. Trotzdem bleibt ein gewisses Restrisiko, da sich nicht nur neue Technologien, sondern auch die möglichen Cyberattacken immer weiterentwickeln. Das Gute ist: Wer die richtigen Maßnahmen trifft, ist erstens schwer 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 kombiniert mit der richtigen Informationspolitik im Hinblick auf Mitarbeiter und Kunden.

Die wichtigsten Ergebnisse

Spot on Sector

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:

Hacktivisten

Organisiertes Verbrechen

Eigene Mitarbeiter

Angriffsfälle

entdeckten in den vergangenen fünf Jahren **einen Angriff** auf ihr Unternehmen.

wurden **mehrfach Opfer** von Angriffen. **Am häufigsten** angegriffen wurden: IT-Systeme (50 %) und Finanzwesen (25 %).

wurden bereits erpresst.

Prävention

sind sicher, dass die eigenen Präventionsmaßnahmen **wirkungsvoll** sind.

haben eine **Versicherung gegen digitale Risiken** abgeschlossen.

Krisenmanagement

haben **Krisenpläne** zur Reaktion auf Angriffe.

üben die Abläufe zumindest einmal im Jahr.

Interview Ali Aram

Ali Aram
Leiter Financial Services
Insurance Advisory Services
EY Österreich

Interview

Wofür werden Daten bei Versicherungen genutzt und wie wichtig sind sie?

Der Trend geht weg von der produkt- und in zur bedarfsorientierten Versicherung. Dementsprechend arbeiten Versicherer daran, ihre Kunden und deren Bedürfnisse durch Erfassung von Daten besser zu verstehen. Versicherungsdaten und Kommunikationsflüsse im Versicherungsbereich werden immer digitaler – über alle Altersklassen hinweg gewinnen „Online-Abschlüsse" zunehmend an Bedeutung. Für mehr als 50 Prozent der Österreicher ist die Verfügbarkeit sämtliche Informationen in allen Kanälen (u. a. Kundenportal) sehr oder sogar äußerst wichtig. So wird natürlich auch eine große Menge an Daten gesammelt, die gut genutzt, aber auch gut verwahrt werden müssen.

Was macht Versicherungen für Datendiebstahl und Cyberangriffe besonders interessant?

Die Daten und auch die digitalen Kommunikationswege bieten Cyberkriminellen viele Möglichkeiten, den Versicherungsunternehmen Schaden zuzufügen. Versicherungen haben sehr viele Kundendaten gespeichert. Ziel von Hackern ist oft die Erpressung von Lösegeld. Die österreichische Versicherungslandschaft ist sich der drohenden Gefahr durch Cyberangriffe bewusst: Laut unserer Umfrage erwarten 90 Prozent der befragten Versicherungen, dass die Gefahr von Angriffen auf ihr Unternehmen weiter steigen wird. Vor allem Hacker-Aktivisten und das organisierte Verbrechen ordnen sie als Tätergruppen mit dem höchsten Gefahrenpotenzial ein. Ein Fünftel hat in den letzten fünf Jahren einen Angriff auf das eigene Unternehmen identifiziert, genauso viele wurden bereits erpresst. Es ist aber erfreulich, dass alle befragten Versicherungen bereits Krisenpläne im Einsatz haben, die ihnen im schlimmsten Fall ein geordnetes Vorgehen ermöglichen.

Was ist in der Versicherungsbranche das Worst-Case-Szenario bei Cyberangriffen?

Wie in der Bankenbranche sind Versicherungen bei Cyberangriffen einem hohen Reputationsrisiko ausgesetzt. Kunden wollen ihre Finanzprodukte sicher verwaltet wissen. Zusätzlich werden in der Versicherungsbranche auch stark sensible Kundendaten verarbeitet (z. B. Gesundheitsdaten bei Zusatzversicherungen etc.). Werden Kundendaten gestohlen, kann das zu Lösegeldforderungen führen. Die Hacker 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.

Was können Unternehmen tun, um sich besser auf Cyberangriffe vorzubereiten?

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

Fazit und Ausblick

Cyberangriffe werden in Zukunft weiter zunehmen, darüber sind sich alle einig: Die überwiegende Mehrheit der Unternehmen in Österreich (81 %) geht davon aus, dass die Gefahren durch Cyberangriffe oder Datendiebstahl in Zukunft steigen werden. Experten bestätigen diesen Trend, der durch die fortschreitende Digitalisierung in allen Bereichen begünstigt wird. Diese bietet der Cyberkriminalität ein beinahe grenzenloses Wachstums- und Schadenspotenzial. Nahezu unkontrolliert und stark anonymisiert ist das Darknet ein Umschlagplatz für organisierte Kriminalität.

Die gute Nachricht: Das Gefahrenbewusstsein der Unternehmen ist inzwischen hoch. 41 % der Unternehmen sehen ein (erhöhtes) Risiko, selbst Opfer von Cyberangriffen und Datendiebstahl zu werden. Nicht zu Unrecht, denn 27 % 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 44 % jener Unternehmen, die ein geringes Risiko sehen, Opfer eines Angriffs zu werden, fühlen sich gut geschützt. Allerdings sind nur 48 % 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 50.000 Euro.

Hinzu kommt, dass rund ein Drittel der Unternehmen bislang keinen Krisenplan für ein Notfallszenario vorbereitet hat. Bei 60 % der Unternehmen, die einen Krisenplan ausgearbeitet haben, werden dessen Abläufe mindestens einmal jährlich trainiert. 25 % der befragten Unternehmen gaben an, dass die Abläufe noch nie geübt worden seien.

Es werden definitiv zu wenig Cyberkriminelle gefasst und noch immer werden viele Vorfälle auch nur zufällig entdeckt: In 47 % der Unternehmen griff das interne Kontrollsystem und deckte die kriminellen Handlungen auf. 19 % 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.

“

Es werden definitiv zu wenig Cyberkriminelle gefasst und noch immer werden viele Vorfälle auch nur zufällig entdeckt.

81 %

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. Aufdem Spiel stehen letzten Endes insbesondere auch wertvolle Kundendaten – denn darauf haben es die Täter 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!

81 % der Befragten erwarten,
dass Cyberangriffe auf österreichische Unternehmen weiter zunehmen.

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 und Fachleute für ausgewählte Themenbereiche zur Verfügung. So treffen etwa IT-Berater und Security-Fachleute auf Fachmitarbeiter aus den klassischen EY-Bereichen Wirtschaftsprüfung, Steuer- und Rechtsberatung, aber auch auf Kriminalisten und Soziologen.

Die über 7.200 global vernetzten Cyber-Professionals 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.

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, die Sie sich stellen sollten:

- Sind wir ausreichend vorbereitet, um gegen die zunehmenden Cyberbedrohungen zu bestehen?
- Ist unsere Cybersicherheitsstrategie zukunftsfähig?
- Sind die persönlichen Daten unserer Kunden, 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 Fragen rund um Cybersecurity und Krisenreaktion werden immer dringender. Unsere Leistungen liefern Antworten und Hilfestellungen für einen nachhaltigen Unternehmenserfolg.

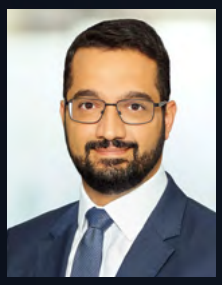
Die Cybersecurity- und Krisenmanagement-Services von EY im Überblick

Sicherheit für Ihr digitales Business

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

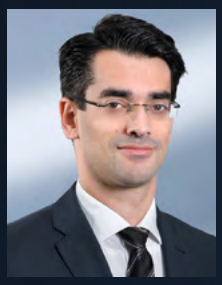
Damit das Vertrauen Ihrer Kunden, Mitarbeiter und Partner erhalten bleibt, helfen wir Ihnen, sich gegen neue und wiederkehrende Cyberbedrohungen zu schützen. Durch unsere integrierten Lösungen können wir Ihre digitale Transformation maßgeblich unterstützen.

Ansprechpartner



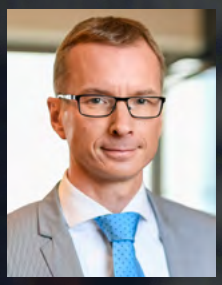
Ali Aram
Leiter Financial Services Insurance Advisory Services EY Österreich

Telefon +43 1 21170 1149
Ali.aram@at.ey.com



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

Telefon +43 1 26095 2113
thomas.breuss@eylaw.at

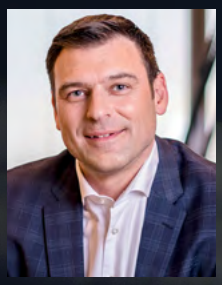


Christoph Harreither
Sector Leader Government & Public EY Österreich

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

Drazen Lukac
Leiter Risk IT und Cybersecurity EY Österreich

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

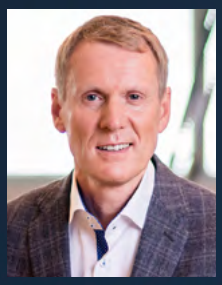


Gunther Reimoser
Sector Leader Financial Services (Banken und Versicherungen) EY Österreich

Telefon +43 1 21170 1032
gunther.reimoser@at.ey.com

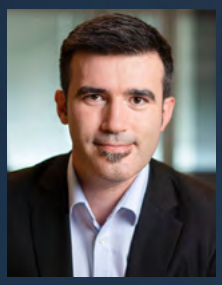
Armin Schmitt
Leiter Financial Services Banking EY Österreich

Telefon +43 1 211 70 1717
Armin.Schmitt@de.ey.com



Gerhard Schwartz
Sector Leader Industrie
EY Österreich

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



Gottfried Tonweber
Leiter Cybersecurity und
Data Privacy EY Österreich

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

Stefan Uher
Sector Leader Energiewirtschaft
EY Österreich

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

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

Telefon +43 1 21170 1903
martin.unger@parthenon.ey.com

Benjamin Weissmann
Leiter Cyberforensik
EY Österreich

Telefon +43 1 21170 1121
benjamin.weissmann@at.ey.com

Impressum

Konzept, Design and Realisation
MEDIENMASSIV, Stuttgart
www.medienmassiv.com

Bildquellen
Getty Images International
www.gettyimages.de

EY | Assurance | Tax | Transactions | Advisory

Die globale EY-Organisation im Überblick
Die globale EY-Organisation ist einer der Marktführer in der Wirtschaftsprüfung, Steuerberatung, Transaktionsberatung und Managementberatung. Mit unserer Erfahrung, unserem Wissen und unseren Leistungen stärken wir weltweit das Vertrauen in die Wirtschaft und in die Finanzmärkte. Dafür sind wir bestens gerüstet: mit hervorragend ausgebildeten Mitarbeiterinnen und Mitarbeitern, dynamischen Teams, einer ausgeprägten Kundenorientierung und individuell zugeschnittenen Dienstleistungen. Unser Ziel ist es, die Funktionsweise wirtschaftlich relevanter Prozesse in unserer Welt zu verbessern – für unsere Mitarbeiterinnen und Mitarbeiter, unsere Kunden sowie die Gesellschaft, in der wir leben. Dafür steht unser weltweiter Anspruch *Building a better working world*.

Die globale EY-Organisation besteht aus den Mitgliedsunternehmen von Ernst & Young Global Limited (EYG). Jedes EYG-Mitgliedsunternehmen ist rechtlich selbstständig und unabhängig und haftet nicht für das Handeln und Unterlassen der jeweils anderen Mitgliedsunternehmen. Ernst & Young Global Limited ist eine Gesellschaft mit beschränkter Haftung nach englischem Recht und erbringt keine Leistungen für Kunden. Informationen dazu, wie EY personenbezogene Daten erhebt und verwendet, sowie eine Beschreibung der Rechte, die Personen gemäß dem Datenschutzgesetz haben, sind über ey.com/privacy verfügbar. Weitere Informationen zu unserer Organisation finden Sie unter ey.com.

In Österreich ist EY an vier Standorten präsent. „EY" und „wir" beziehen sich in dieser Publikation auf alle österreichischen Mitgliedsunternehmen von Ernst & Young Global Limited.

GSA Agency
BKL 2004-012
ED None

ey.com/at