Cyber Security in Österreich

Studie
IT Advisory

April 2016

Herausforderungen und Maßnahmen österreichischer Unternehmen hinsichtlich Cyberkriminalität

kpmg.at/cyber

Inhalt

Mit Strategie gegen Cyberkriminalität 5

Aktuelle Situation in Österreich 6

Key findings 8

Cyberkriminalität: Willkommen in der Realität 10

Cyberabwehr: Das Wertvolle schützen 14

Cyberattacken: Der unsichtbare Feind 18

Cyber Security: Die richtige Strategie 22

Umfragemethodik 32

Cyber Security bei KPMG 33

Publikationen 34

“Das Bewusstsein für Cyber Security ist durchaus vorhanden, was fehlt sind strategische Maßnahmen.”

Mit Strategie gegen Cyberkriminalität

Medienberichte über Cybervorfälle gibt es heute fast täglich. Egal ob öffentliche Institution oder privatwirtschaftliches Unternehmen, ob großer Konzern oder Ein-Personen-Betrieb: Cyberkriminalität macht vor niemandem halt. Die Angreifer sind hoch professionell, gut organisiert und scheinen uns immer einen Schritt voraus zu sein.

Vorfälle der letzten Zeit haben gezeigt, dass der finanzielle Schaden enorm sein kann. Dazu kommt der Reputationsverlust eines Unternehmens. Es versteht sich von selbst, dass Unternehmen ihre digitalen Vermögenswerte angemessen schützen müssen.

Cyber Security erfordert daher einen prominenten Platz auf der Agenda des Managements. Das Bewusstsein dafür ist in Österreich durchaus vorhanden. Vielen Unternehmen gelingt es allerdings noch nicht, diesem Bewusstsein strategische Maßnahmen folgen zu lassen. Es ist nicht zielführend, Cyber Security nur reaktiv und aus Angst vor den Folgen eines Angriffs anzugehen.

Das bringt uns zu der Frage: Welche ist die beste Strategie mit Bedrohungen durch Cyberkriminalität umzugehen? Und wie gehen österreichische Unternehmen mit dieser Herausforderung konkret um? Vor diesem Hintergrund hat KPMG die vorliegende Studie durchgeführt, an der 94 Experten für Cyber Security von österreichischen Unternehmen teilnahmen. Ergänzt wird sie durch sieben Interviews mit Unternehmensvertretern und Branchenexperten.

Das Fazit der Umfrage: Unternehmen benötigen eine ganzheitliche Perspektive, um sich den Herausforderungen der Cyberkriminalität wirksam stellen zu können. Gefragt ist ein integrierter und ausgewogener Ansatz, der Menschen und Prozesse ebenso berücksichtigt wie Technologien. Das Wichtigste: Cyber Security muss endlich „Chefsache“ werden. Nur so können sich Unternehmen langfristig gegen Cyberkriminalität wehren.

Wir wünschen Ihnen eine anregende Lektüre und freuen uns darauf, Ihre Fragen persönlich mit Ihnen zu erörtern.

Michael Schirmbrand
KPMG Partner

Gert Weidinger
KPMG Partner

Aktuelle Situation in Österreich

Leben und Wirtschaft im Cyberraum

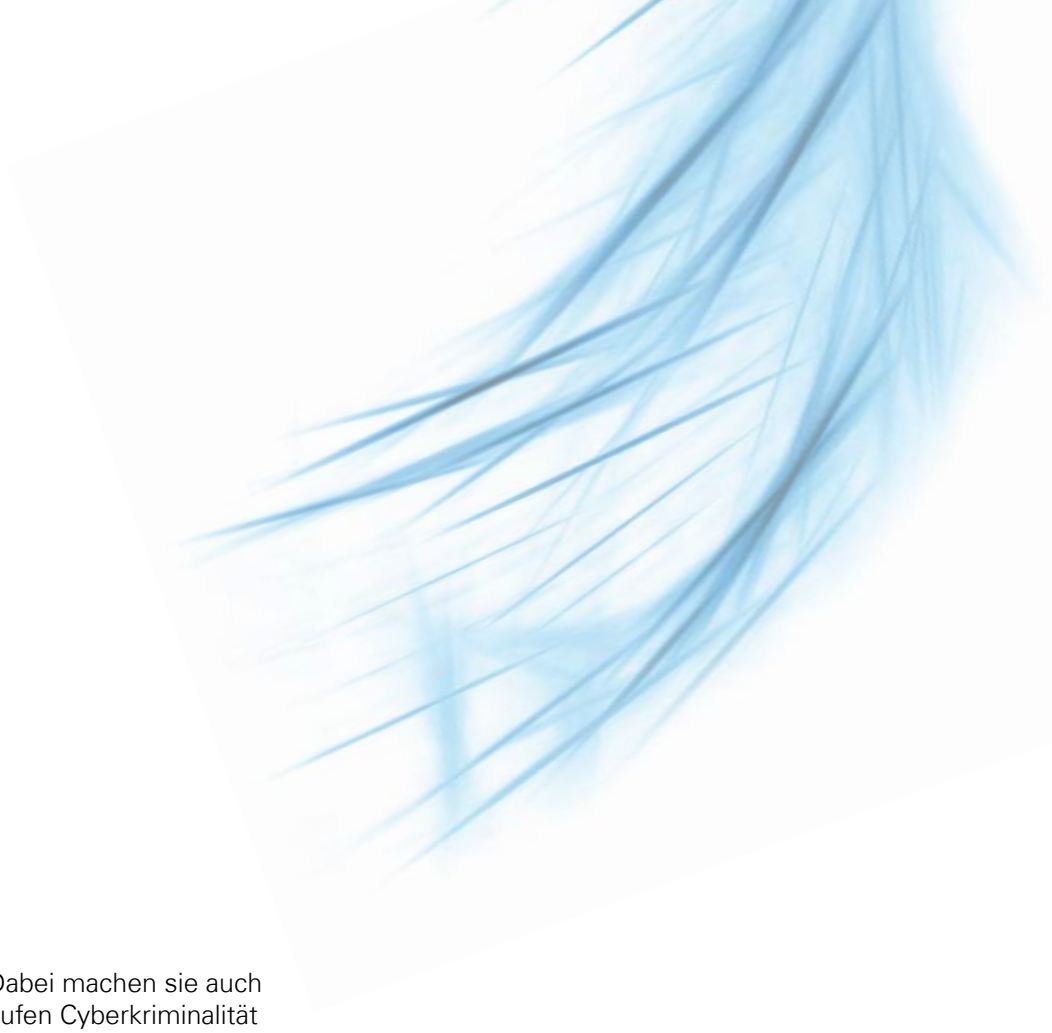
Wir leben in einer Zeit, in der alle Bereiche der Gesellschaft von zunehmender Digitalisierung geprägt sind. Die rasche Weiterentwicklung digitaler Technologien hat das wirtschaftliche und gesellschaftliche Leben grundlegend verändert. Der Cyberraum bietet einerseits völlig neue Chancen, andererseits liefert er viele neue Angriffspunkte für kriminelle Handlungen. Aufgrund unserer Abhängigkeit von einer funktionierenden digitalen Infrastruktur stellen Cyberangriffe ein ernstzunehmendes Risiko dar.

Finanzielle Schäden und Imageverlust

Digitale Technologien machen wirtschaftliche Prozesse schneller und effizienter. Die daraus resultierende Informationsüberflut ist jedoch nur schwer zu überblicken. Cyberkriminelle wissen genau, wie sie ihren Vorteil aus dieser Situation ziehen können. Unternehmen weltweit und auch in Österreich berichten von steigenden Kosten durch Cyberkriminalität. Die Schäden reichen von finanziellen Verlusten durch Daten- und Informationsdiebstahl über schwerwiegende Schädigung der Reputation bis hin zum Stillstand der Geschäftsprozesse.

Bedrohung des Wirtschaftsstandortes Österreich

Österreich ist ebenso von dieser Entwicklung betroffen. Die Anzahl an Cyberattacken steigt jährlich. Für Unternehmen steht im Zusammenhang mit Cyberkriminalität sehr viel auf dem Spiel. Kritische Infrastruktur, geistiges Eigentum und Geschäftsgeheimnisse von österreichischen Banken und Versorgungsunternehmen sowie Industrie- und Handelsunternehmen



stehen im Fokus der Angreifer. Dabei machen sie auch nicht vor KMUs halt. Experten stufen Cyberkriminalität mittlerweile als ernsthafte Bedrohung für den Wirtschaftsstandort Österreich ein.

Unternehmen nicht ausreichend gewappnet

Zwar ist man sich in Österreich der Gefahr bewusst, es gelingt den Unternehmen jedoch nur bedingt, dieses Bewusstsein in konkrete Maßnahmen umzuwandeln. Unternehmen, die vorwiegend auf den österreichischen Binnenmarkt ausgerichtet sind, schätzen Cyberrisiken eher als gering ein. Internationale Konzerne sind sich hingegen der Risiken stärker bewusst. Insbesondere kleine und mittlere Unternehmen unterschätzen die Gefahr durch Cyberrisiken. Aufgrund fehlender Sicherheits- und Reportingsysteme wissen viele nicht einmal, dass sie Opfer eines Angriffs wurden. Die aktuelle Situation zeigt deutlich, dass die meisten Unternehmen noch nicht ausreichend auf Cyberkriminalität vorbereitet sind.

Cyber Security im 21. Jahrhundert

Wie können sich österreichische Unternehmen vor Schäden durch Cyberangriffe schützen? Voraussetzung dafür ist eine ganzheitliche Betrachtung der Informationssicherheit auf höchster Führungsebene. Rein technologische Lösungsansätze alleine reichen nicht aus. Besonders wichtig ist die Schärfung des Bewusstseins der Mitarbeiter für Cyberkriminalität. Ebenso relevant ist die Entwicklung geeigneter Präventions- und Reaktionspläne für den Ernstfall. Eine zuverlässige Cyber Security zählt zu den wesentlichen Aufgaben der Unternehmensführung des 21. Jahrhunderts.

Key findings

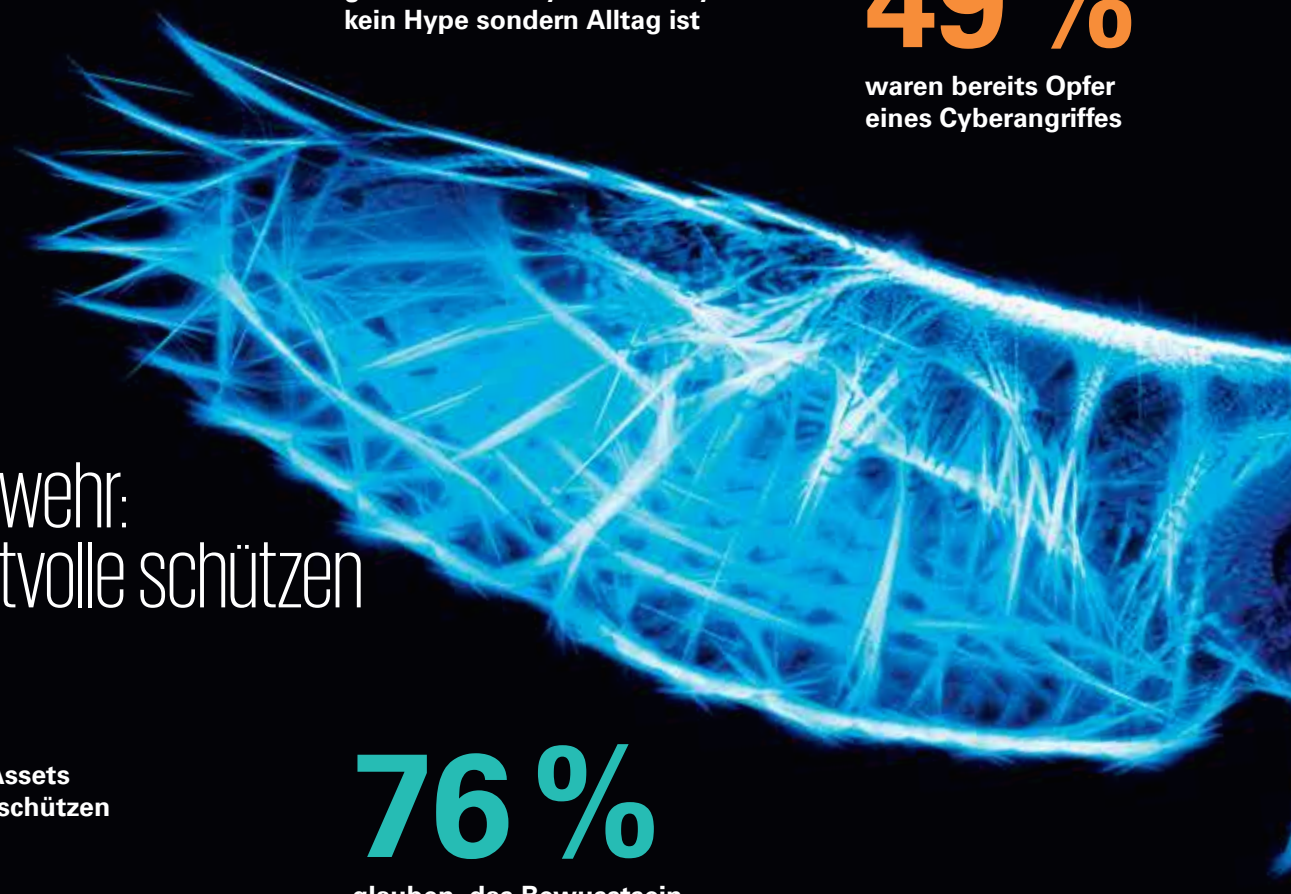
Cyberkriminalität: Willkommen in der Realität

30 %
erlitten bereits einen Schaden durch Cyberangriffe

40 %
sehen sich als attraktives Ziel für Angriffe

92 %
glauben, dass Cyber Security kein Hype sondern Alltag ist

49 %
waren bereits Opfer eines Cyberangriffes



Cyberabwehr: Das Wertvolle schützen

16 %
geben an, ihre Assets ausreichend zu schützen

76 %
glauben, das Bewusstsein der Mitarbeiter unzureichend geschärft zu haben

60 %
können Auswirkungen von Cyberangriffen nicht messen

57 %
glauben, über ihre Assets Bescheid zu wissen

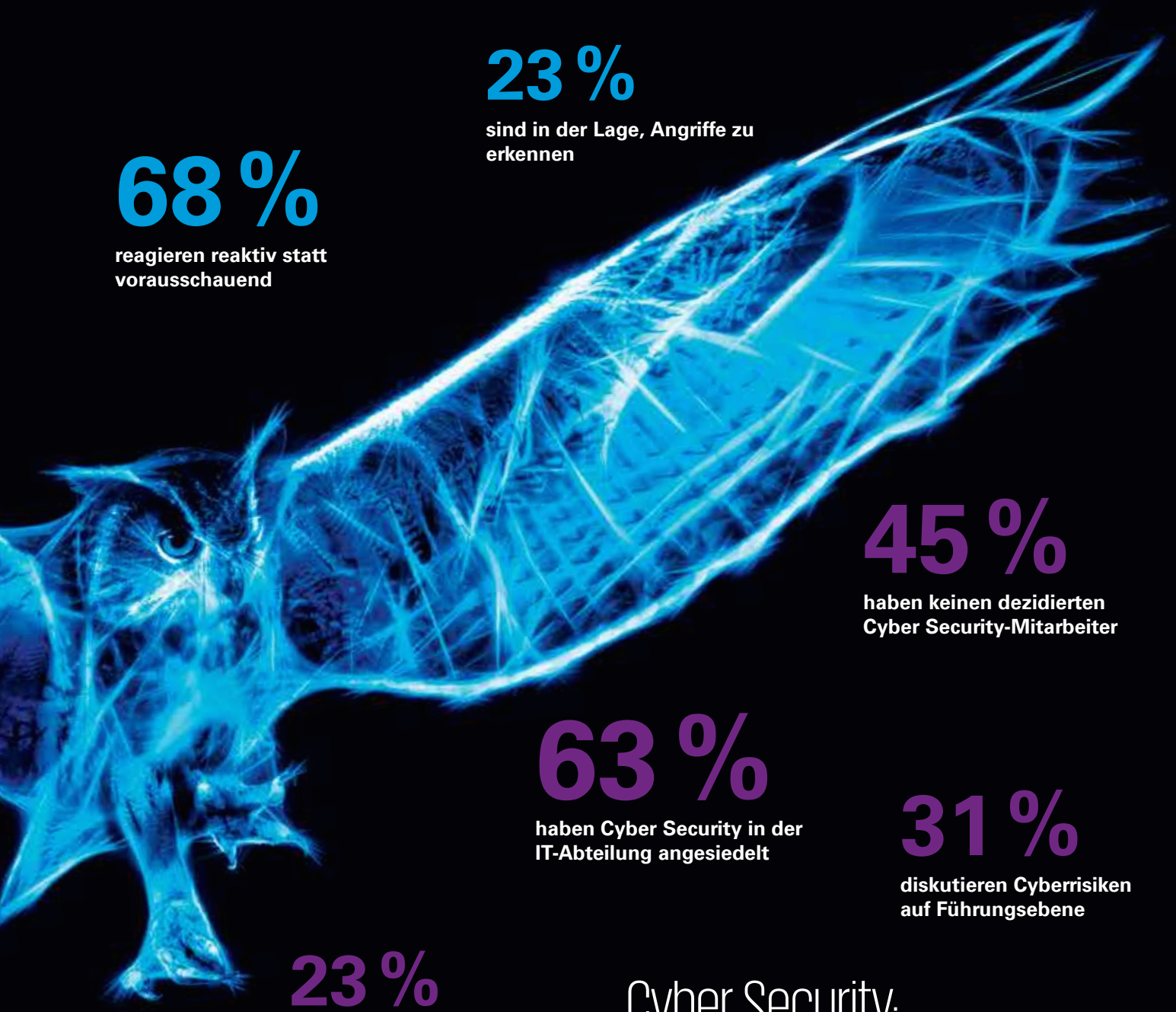
Cyberattacken: Der unsichtbare Feind

71 %
glauben, Cyberangriffe nicht ganz verhindern zu können

18 %
können wirksam auf Cyberattacken reagieren

23 %
sind in der Lage, Angriffe zu erkennen

68 %
reagieren reaktiv statt vorausschauend



45 %
haben keinen dezidierten Cyber Security-Mitarbeiter

63 %
haben Cyber Security in der IT-Abteilung angesiedelt

31 %
diskutieren Cyberrisiken auf Führungsebene

23 %
der Unternehmen haben keine Berichterstattung von Cyberangriffen

Cyber Security: Die richtige Strategie

Cyberkriminalität: Willkommen in der Realität

Alltagsgefahr statt exotischer Hype

Cyberbedrohungen sind längst in unserem realen Leben angekommen. Die KPMG-Studie „Cyber Security" verdeutlicht das eindrucksvoll: Knapp die Hälfte der befragten österreichischen Unternehmen war bereits Opfer von Cyberkriminalität. Auch jene, die bisher verschont blieben, erkennen die reale Bedrohung aus der virtuellen Welt an: 92 Prozent der Unternehmen sind sich der Gefahr von Cyberangriffen bewusst. Die Zeiten, in denen Cyberkriminalität und Cyber Security belächeltes Wording von Fach-Exoten waren, sind vorbei.

> "Gegen Cyberkriminalität muss man gemeinsam an einem Strang ziehen."
>
> Andreas Teischl
> Unicredit Bank Austria AG

Gefahr im Großen und Kleinen

Bei Cyberkriminalität sprechen wir längst nicht mehr nur von Hackern, die eine Unternehmenswebsite lahm legen. Cyberkriminelle sind hoch-professionell, gut vernetzt und global organisiert. Das World Economic Forum zählt Cyberangriffe heute zu den gefährlichsten Sicherheitsrisiken. Die ökonomischen und finanziellen Aspekte sind enorm. Vor allem aber steht ein Bedrohungsszenario im Raum: Die Gefährdung der sozialen und gesellschaftspolitischen Stabilität und Ordnung. Cyber Security steht daher bei vielen politischen Entscheidungsträgern weit oben auf der Agenda.

Unternehmen haben hingegen oft Probleme damit, genau einzuschätzen und zu messen, inwieweit sie gegen Cyberangriffe gewappnet sind. Eine strategische Herangehensweise ist jedoch unerlässlich, um Cyberrisiken wirksam abzuwehren.

Gut verdrängt ist halb verloren

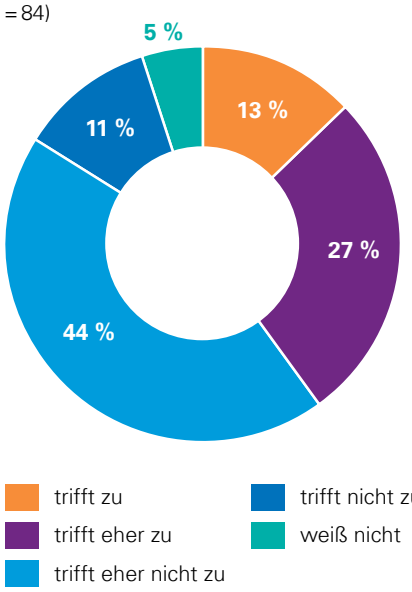
Auch wenn die Awareness für Cyberkriminalität bei österreichischen Unternehmen vorhanden ist, so lauert die Gefahr im Detail: Nur 40 Prozent der Unternehmen glauben, ein attraktives Ziel für Cyberangriffe zu sein. Große Unternehmen sehen sich tendenziell eher als Zielscheibe, kleinere und mittlere Unternehmen wiegen sich vermeintlich in Sicherheit.

Die Realität zeichnet jedoch ein anderes Bild: Nicht immer wählen Cyberkriminelle ihre Opfer nach wirtschaftlichen Kriterien. In vielen Fällen reicht es, eine leicht zu hackende Software zu verwenden – schnell wird man vom User zum Angegriffenen. Die Gefahr ist virtuell, die Auswirkungen real: Bei 41 Prozent der befragten Unternehmen resultierten Cyberattacken in der Unterbrechung von Geschäftsprozessen. Abseits der finanziellen Konsequenzen droht auch ein enormer Reputationsschaden.

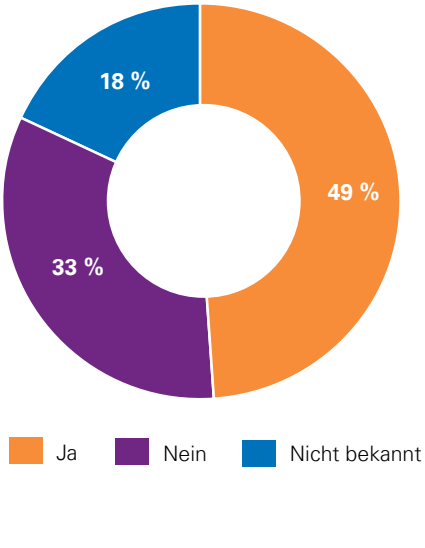
Der Mittelstand im Mittelpunkt

Kleinere und mittlere Unternehmen sind das Rückgrat der österreichischen Wirtschaft. Sie stehen für Know-how, Innovation und Erfindergeist. Der Fortbestand der Unternehmen hängt oft vom Schutz des geistigen Eigentums ab. Zwei Drittel der Cyberattacken betreffen mittlerweile KMUs. Cyber Security sollte daher auf der Agenda ganz oben stehen. Die Realität ist jedoch ernüchternd und bringt die Alarmglocken zum Läuten: Für den Großteil der österreichischen KMUs ist Cyber Security aktuell kein strategisch wichtiges Thema. Hier besteht eindeutig Handlungsbedarf.

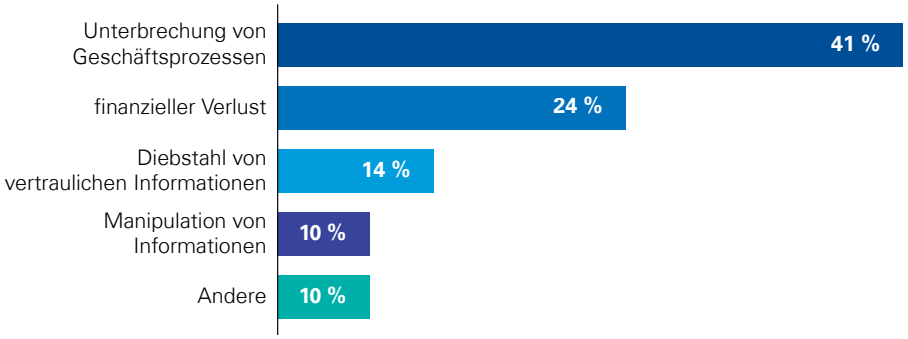
Unser Unternehmen ist ein attraktives Ziel für Angreifer.
(n = 84)



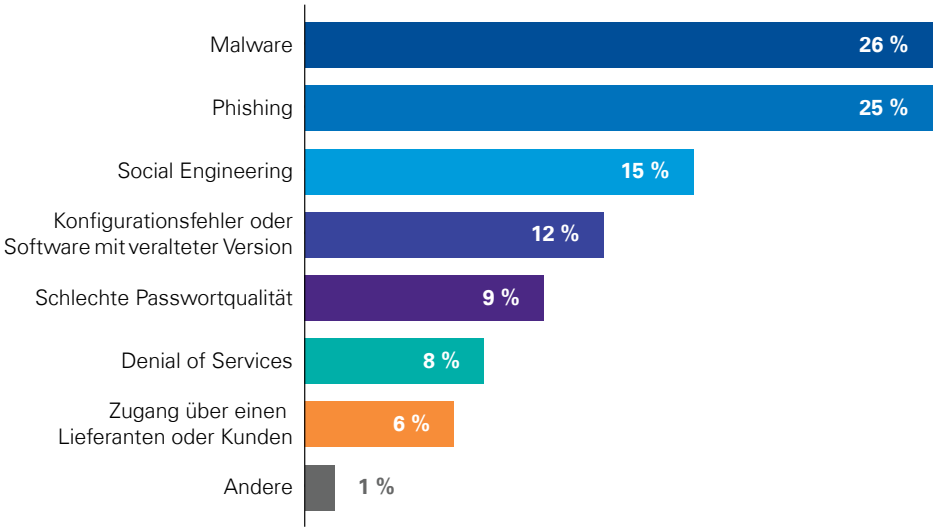
Wurden Sie schon Opfer eines Cyber Angriffes?
(n = 84)



Auswirkungen von Cyberangriffen
(n = 84)



Arten von Cyberangriffen
(n = 84)



92 %
glauben, dass Cyber Security kein Hype sondern Alltag ist
(n = 84)

49 %
waren bereits Opfer eines Cyberangriffes
(n = 84)

40 %
sehen sich als attraktives Ziel für Angriffe
(n = 84)

30 %
erlitten bereits einen Schaden durch Cyber-angriffe
(n = 84)

Cyberkriminelle sind meist einen Schritt voraus

Was sind aus Sicht der UniCredit Bank Austria die aktuell größten Bedrohungsszenarien, die beobachtet werden?
Cyberkriminalität ist ein großes Thema für uns. Im Bereich des Onlinebanking etwa ändern sich die Angriffsformen: weg vom ausschließlichen IT-Kanal hin zu einer Mischung aus Trojaner und Social Engineering. Die Awareness in der Bevölkerung ist mittlerweile so hoch, dass die Angreifer durch die alleinige Installation eines Schadprogrammes ihr Ziel nicht mehr erreichen.

Attacken gegen ein Unternehmen selbst bewirken nicht nur einen finanziellen Schaden sondern wirken sich auch auf die Reputation aus. Vor einigen Jahren gab es einen Angriff auf eines unserer Test-Systeme, auf dem veraltete Daten gespeichert waren. Auch wenn mit den Daten in weiterer Folge keine Misswirtschaft betrieben wurde, so war der Imageschaden natürlich erheblich.

Die Awareness ist aus Ihrer Sicht bei den Bankkunden relativ hoch – steht das nicht im Widerspruch dazu, dass gerade Social Engineering stark im Kommen ist?
Es fällt auf, dass bei Kundenbesprechungen und -befragungen mittlerweile fast jeder zweite über Phishing-Mails spricht. Das ist eine signifikante Änderung: Früher war es einfacher für Phishing-Seiten, ihr Ziel zu erreichen. Durch die eingezogenen Barrieren ist das heute kaum mehr möglich: SMS-TAN, Überweisungslimits und verbesserte Awareness. Die Kriminellen haben also neue Strategien entwickelt und sich angepasst: weg von der reinen IT-Seite, hin zu Mustern, wie etwa: sich als Mitarbeiter der Bank auszugeben und zu behaupten: „Wir haben ein IT-Problem beim Onlinebanking, bitte machen Sie dieses und jenes...". Hier besteht noch Nachholbedarf in der Bewusstseinsbildung.

Kann man daraus den Umkehrschluss folgern, dass derzeit ein zu starker Fokus auf Technologie und noch zu wenig auf den Prozess mit den Menschen liegt?
Absolut! Die Tätergruppen sind uns in allen Lebensbereichen immer einen Schritt voraus, die Menschen leider oft zu gutgläubig – auch abseits der Cyberkriminalität. Nehmen Sie als Beispiel das Thema „Registrierkassenpflicht". Bereits wenige Tage nach Einführung des Gesetzes standen erste Kriminelle vor Einkaufszentren, gaben sich als Beamte des Finanzamts aus und „kontrollierten", ob die Menschen den Beleg dabei hatten. Dabei erbeuteten die Kriminellen bis zu 360 Euro pro Personen.

Welche Rolle nehmen die Kommunikation und der Austausch zwischen den Unternehmen selbst ein?
Eine Zusammenarbeit im Bereich Cybersicherheit ist unerlässlich. Es geht um eine gemeinsame Herangehensweise, der Konkurrenzgedanke ist hier vollkommen fehl am Platz. Gegen Cyberkriminelle muss man gemeinsam an einem Strang ziehen. Das ist auch die von uns gelebte Praxis. Es gibt einen Kommunikationsaustausch in der Branche in puncto Cybersicherheit. Wir kommunizieren sehr intensiv mit den Ansprechpartnern aus den anderen Banken.

Wie steht Österreich Ihrer Einschätzung nach im Vergleich zu anderen europäischen Ländern in Bezug auf Cyber Security da?
Große Unternehmen sind in dem Bereich bereits sehr nachhaltig aufgestellt, es wird viel in Security investiert. Bei mittelständischen Unternehmen ist Cyber Security zum Teil überhaupt kein Faktor. Es herrscht leider oft die Devise: „Es kostet etwas, daher interessiert es mich nicht". Wir organisieren immer wieder Veranstaltungen für Klein- und Mittelbetriebe, bei denen seit einiger Zeit auch immer ein Cybersicherheits- und Internetsicherheitsbaustein auf der Agenda steht. Das Thema wird dort interessiert aufgenommen.

Allerdings besteht noch großer Aufholbedarf. Ein Tischler mit fünf Angestellten macht sich nicht so viele Gedanken darüber, dass auch sein Unternehmen vernetzt ist: etwa durch Zahlungen mit Business-Net, durch Onlinebanking oder durch die Gehaltsverrechnung.

Interview mit Andreas Teischl, Chief Security Officer und Chief Information Officer, Unicredit Bank Austria AG

Andreas Teischl
Chief Security Officer und CIO,
Unicredit Bank Austria AG

Für Kriminelle ist er als Zielscheibe aber viel interessanter als ein klassischer Privatkunde, bei dem man bei einer Überweisung maximal ein paar tausend Euro erbeuten kann.

Wenn KMUs als Rückgrat der Wirtschaft im Bereich Cybersicherheit nicht ausreichend abgesichert sind, könnte man von einer Gefährdung des Wirtschaftsstandortes sprechen?
Darin sehe ich ein gewisses Risiko, ja. Die großen Corporates haben zum Teil eigene Security-Abteilungen, eigene Ressourcen, eigene Budgetierungen für Cybersicherheit. Bei KMUs sieht das vollkommen anders aus, das Thema wird stark vernachlässigt.

Stichwort „nächste Generation". Welche Möglichkeiten gibt es aus Ihrer Sicht, hier anzusetzen?
Bei diesem Thema besteht in jedem Fall großer Handlungsbedarf. Aus meiner Sicht müsste man das Thema Cybersicherheit in den Schulunterricht integrieren. In der Schule bekommt man auch Mindesets vermittelt wie etwa: Bei Rot über die Straße zu gehen ist gefährlich. Vergleichbares müsste für die Cyberwelt passieren, was jedoch aufgrund der Komplexität schwieriger ist.

Der EDV-Unterricht in den Schulen hat sich ja seit den 1980er Jahren kaum nachhaltig verändert. Die Kinder beschäftigen sich mit anderen Medien und Inhalten, als in der Schule vermittelt werden. Es müsste eine Bewusstseinsbildung stattfinden, die sich mit Fragen beschäftigt wie: Wie bewege ich mich in Social Media-Welten, was poste ich auf welcher Plattform, welche Inhalte sollte ich nur Freunden zugänglich machen und nicht der ganzen Weltöffentlichkeit? Denn: Bereits in Social Media-Räumen werden viele Kriminalitätsaktivitäten angebahnt. Der Cyber Crime des Privaten beginnt häufig im Social Media. Dieses Thema in den Schulen zu integrieren ist eine große Herausforderung.

Generell gefragt: Wie könnte der österreichische Staat verstärkt dazu beitragen, das Thema Cyber Security zu stärken?
Wichtig ist ein rechtlicher Rahmen. Es gibt bereits ein Cybersicherheitsgesetz bzw einen abgestimmten Entwurf. Hier müssen weitere Schritte gesetzt werden, auch hinsichtlich Strafverfolgung. Positiv zu erwähnen sind aus meiner Sicht die Aktivitäten in Richtung informelle, teilweise auch schon offizielle, Plattformen, bei denen man sich mit kritischer Infrastruktur auseinandersetzt. Es geht um Themen wie: Wie können wir die wesentlichen Säulen unseres Staates und unserer Infrastruktur sichern? Die Zusammenarbeit in diesem Bereich sollte noch stärker ausgebaut werden.

Cyberabwehr: Das Wertvolle schützen

Die Kronjuwelen bewachen

Geistiges Eigentum, Forschungsdaten, Patente, wichtige Rezepturen: der Schutz von Intellectual Property sollte für Unternehmen ganz oben auf der Agenda stehen. Denn Daten- und Informationsdiebstahl kann für Unternehmen weitreichende Folgen haben. Entscheidend ist daher, sich mit folgender Frage auseinander zu setzen: Was sind die wichtigsten Assets meines Unternehmens und wie schütze ich sie effektiv? 57 Prozent der befragten Unternehmen geben laut Studie „mit Sicherheit" an, dass sie über ihre wertvollsten Assets Bescheid wissen und wo diese gespeichert sind. Dieses Ergebnis ist erfreulich. Denn: Eine zielgerichtete Etablierung eines Abwehrsystems von Cyberangriffen ist nur unter solchen Voraussetzungen möglich.

Unbekannte Schwachstellen

Generell herrscht jedoch rund um das Thema Cyber Security große Unsicherheit: 82 Prozent der Unternehmen sind sich nicht sicher, ob sie wirklich in der Lage sind, wirksam auf einen Cyberangriff reagieren zu können. Nur 34 Prozent der Unternehmen sind überzeugt zu wissen, wie ihre Assets von Angreifern erreicht werden. Lediglich 16 Prozent der befragten Unternehmen können „mit Sicherheit" sagen, dass sie alle relevanten Ressourcen überwachen und ausreichend Schutz gewährleisten können. Unternehmen kennen also ihre wertvollsten Assets und wissen wo diese gespeichert sind. Sie sind sich aber nicht im Klaren darüber, wie Hacker bei einem Angriff vorgehen und wo sich Schwachstellen oder Angriffspunkte in ihren Systemen verbergen. Das bedeutet: Die Hacker sind den Unternehmen immer einen Schritt voraus.

Schutzmechanismen messbar machen

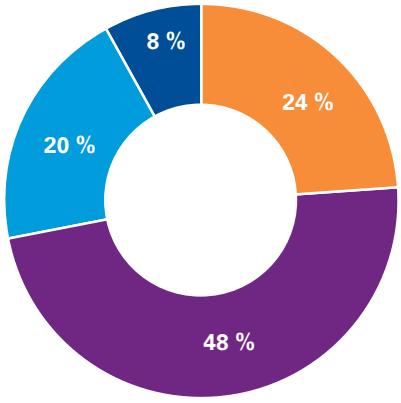
60 Prozent der befragten Unternehmen geben an, keine Methoden zur Messung der Auswirkungen von Cyberangriffen zu haben. Aufgrund fehlender Messinstrumente in den meisten Unternehmen kann folgende These in den Raum gestellt werden: Vielfach gibt es keinen ausreichenden Schutz gegen Cyberkriminalität. Denn: Es reicht nicht aus, die wichtigsten Assets der Unternehmen nach besten Wissen und Gewissen schützen zu wollen. Eine strategische Herangehensweise und eine Kontrolle der durchgeführten Maßnahmen sind entscheidend. Es muss überprüft werden können, ob die gewählten Aktionen ausreichend Schutz gewährleisten.

> "Attacken, die Unternehmensdaten zerstören oder verschlüsseln, sind existenzgefährdend."
>
> Thomas Stubbings
> Cyber Security Plattform der öster Bundesregierung

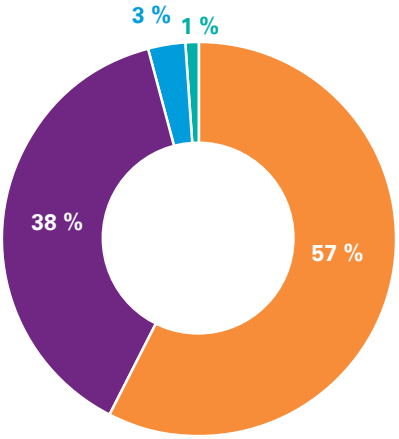
Maßgeschneiderte Lösungsansätze

Hinsichtlich Cyberabwehr besteht noch enormer Handlungsbedarf: Es braucht zuständige Mitarbeiter oder Berater, die Maßnahmen zur Beobachtung und Messung von Cyberangriffen einführen. Nur so können Angriffe erfolgreich abgewehrt werden. Awareness zu schaffen ist essentiell, alleine durch Bewusstseinsbildung kann die Gefahr der Cyberkriminalität aber nicht abgewehrt werden. Die Etablierung eines maßgeschneiderten Systems zur Abwehr von Angriffen ist unverzichtbar.

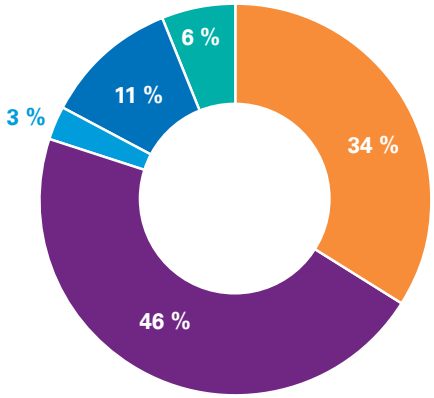
Unsere Mitarbeiter verfügen über ausreichendes Bewusstsein hinsichtlich Cyberangriffen.
(n = 85)



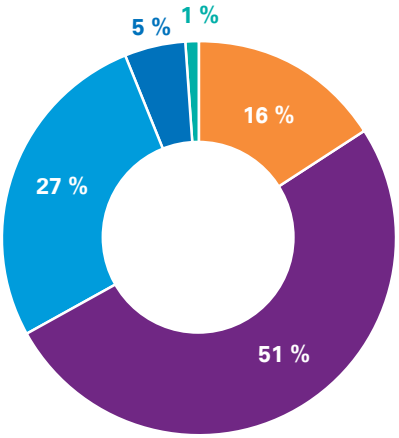
Wir kennen unsere wertvollsten Assets.
(n = 94)



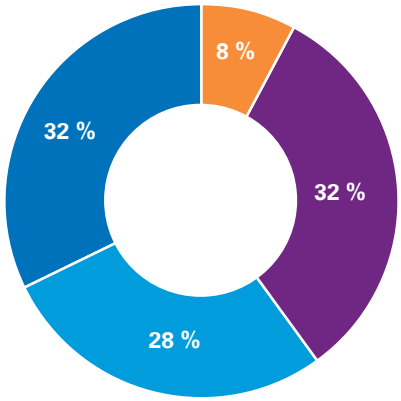
Wir haben ein klares Bild darüber, wie unsere Assets von Angreifern erreicht werden.
(n = 94)



Wir sind in der Lage, alle relevanten Ressourcen ausreichend zu schützen.
(n = 94)



Wir haben Methoden, um Auswirkungen von Cyberangriffen zu messen.
(n = 88)



76 %

glauben, das Bewusstsein der Mitarbeiter unzureichend geschärft zu haben
(n = 85)

60 %

können Auswirkungen von Cyberangriffen nicht messen
(n = 88)

57 %

glauben über ihre Assets Bescheid zu wissen
(n = 94)

16 %

glauben ihre Assets ausreichend zu schützen
(n = 94)

Risikomanagement ist essenziell

Sie vertreten als Vorsitzender die kritischen Infrastrukturen in der Cyber Security Plattform der österreichischen Bundesregierung. Was sind aus Ihrer Sicht die gefährlichsten Trends in Bezug auf Cyberattacken?
Kritisch sind vor allem Angriffe, die die Existenz ganzer Unternehmen betreffen. Durch eine solche Attacke kann etwa die Datenbasis eines Unternehmens zerstört oder böswillig verschlüsselt werden, um es damit zu erpressen. Ist ein Unternehmen nicht auf solche Szenarien vorbereitet, kann es dadurch seine Geschäftsgrundlage verlieren. Es gibt Fälle, in denen ein Unternehmen nach einem Cyberangriff out of business geht.

Industrieunternehmen fürchten vor allem die Unterbrechung von Geschäfts- und Produktionsabläufen, Banken- und Finanzdienstleister hingegen eher Daten- und Informationsdiebstahl. Wo sehen Sie das größte Risiko?
Daten- oder Informationsdiebstahl hat für das einzelne Unternehmen weitreichende Folgen: Verlust von Intellectual Capital, Haftungsthemen, Reputationsverlust. Aus gesamtstaatlicher Sicht ist jedoch die Verfügbarkeitsproblematik eine noch kritischere. Auch Unternehmen der kritischen Infrastrukturen sind vernetzt, setzen Systeme ein, die Schwachstellen enthalten können und angreifbar sind.

Es macht aber einen Unterschied, ob eine Schwachstelle in der Webseite eines Online-Marktplatzes ausgenützt wird oder bei den Steuersystemen einer Wasseraufbereitungsanlage. Hier geht es um Menschenleben und das Funktionieren der öffentlichen Ordnung. Naturgemäß sind Unternehmen der kritischen Infrastruktur besser aufgestellt, aber: das 100-prozentig sichere System gibt es nicht.

Der Mittelstand und kleine Unternehmen sind sich der Gefahr mehrheitlich nicht bewusst, obwohl bereits zwei Drittel aller Angriffe auf KMUs erfolgen. Wie kann man das Sicherheitsbewusstsein des Mittelstandes verbessern?
99 Prozent der österreichischen Unternehmen fallen in die Kategorie KMU, darunter auch einige der kritischen Infrastrukturen. Gerade hier ist der Nachholbedarf in Bezug auf Cybersicherheit am Größten. Viele Unternehmen haben sich noch nicht einmal ansatzweise mit dem Thema auf Geschäftsführungsebene beschäftigt. Hier geht es darum, sich überhaupt erst einmal strukturiert mit dem Thema Risikomanagement auseinanderzusetzen.

Einige Organisationen und Interessensvertretungen wie die WKÖ oder der KSÖ engagieren sich bereits stark im Bereich der Sensibilisierung. Doch hier sind alle Vertreter des Staates, der Wirtschaftsvertretungen und der Sicherheitsorganisationen gefragt.

KMUs sind derzeit nicht Teil der Cyber Security Plattform. In welcher Weise könnte eine verbesserte Einbindung in die Cyber Security Agenda der Bundesregierung erfolgen?
Es ist überlegenswert, auch für KMUs eine geeignete Plattform zu schaffen. In Deutschland gibt es die Allianz für Cybersicherheit, eine freiwillige Kooperationsplattform für KMUs, die ihnen Zugang zu Sicherheitsinformationen bietet und sie mit Herstellern und Dienstleistern vernetzt. Ein ähnliches Modell könnte durchaus auch in Österreich funktionieren.

Was kann auf europäischer Ebene unternommen werden, um das Thema Cybersicherheit zu verbessern und zu stärken?
Die NIS (Network and Information Security) Directive ist aus meiner Sicht ein wesentlicher erster Schritt, um die Wichtigkeit des Themas aufzuzeigen und zumindest für Unternehmen der kritischen Infrastrukturen die Umsetzung gewisser Mindeststandards zu fördern. Doch es muss noch darüber hinausgehen: Wir brauchen dringend eine Förderung eigener Infrastrukturen und Produkte europäischer Herkunft, die unter gesicherten und zertifizierten Mindeststandards arbeiten. Wir sind viel zu abhängig von außereuropäischen Anbietern, die aber im Bereich Datenschutz und Privacy ganz andere Standards haben. Wir müssen

Interview mit Dr. Thomas Stubbings, Vorsitzender der Cyber Security Plattform der österreichischen Bundesregierung

Thomas Stubbings
Vorsitzender der Cyber Security Plattform der österreichischen Bundesregierung

das Thema Digital Sovereignty ernst nehmen und uns eigene Alternativen schaffen, die unsere Sicherheitsvorstellungen erfüllen. Es geht hier nicht um Protektionismus, sondern darum, Produkte und Services zu fordern und zu fördern, die unserem Bedarf nach Sicherheit, Datenschutz und Privacy nachkommen.

Welche Aktionen müssten auf EU-Ebene gesetzt werden, um diesem Ziel näher zu kommen?
Es bedarf einerseits eines entsprechenden Angebotes, andererseits aber auch klar formulierter Anforderungen seitens des Marktes in Form von Standards oder anerkannten Zertifizierungen. Die EU Kommission arbeitet gerade daran, eine sogenannte „Contractual Public Private Partnership for Cybersecurity" zu etablieren, die europäische Anbieter auf EU-Ebene vernetzt. Das ist ebenfalls ein guter Schritt in die richtige Richtung. Im Rahmen der Agenda Horizon 2020 stehen über 700 Millionen Euro an Fördermitteln zur Verfügung. Wenn nur ein Teil davon für die Stärkung der europäischen IT-Industrie genutzt wird, würde uns das schon helfen.

Was sind Ihre wichtigsten Empfehlungen für österreichische Unternehmen für die kommenden zwölf Monate in Bezug auf Cyber Security?
Auf strategischer Ebene: die grundsätzliche Auseinandersetzung mit dem Thema. Jedes Unternehmen sollte sich die Frage stellen: Wo stehe ich heute? Welche Bedrohungen gibt es für mein Geschäftsmodell und wie kann ich darauf reagieren? Das müssen nicht immer die großen Attacken sein. Es geht um Szenarien, die jedes Unternehmen betreffen können, auch Ein-Personen-Unternehmen: Etwa eine Schadsoftware aus einer E-Mail, die alle Unternehmenslaufwerke verschlüsselt. Auf der operativen Ebene: Zumindest größere Unternehmen, die beispielsweise über spezielles Know-how, Intellectual Property oder kritische Produktionsprozesse verfügen, müssen sich die Frage stellen: Inwieweit sind wir in der Lage, komplexe Angriffe auf unsere Infrastruktur zeitnahe zu erkennen und effektiv darauf zu reagieren?

Die klassische Firewall und das Intrusion Prevention System reichen dafür schon lange nicht mehr aus. Es braucht eine geeignete Vernetzung aller Informationen, die Entwicklung von auf das Unternehmen und seiner Infrastruktur abgestimmte Use Cases und ein laufendes Monitoring durch speziell geschulte Mitarbeiter. Nur so kommt man überhaupt in die Lage, auch komplexere Angriffe zeitnah erkennen und darauf reagieren zu können. Und last but not least: Bewusstseinsbildung. Ein aufmerksamer und vorsichtiger Mitarbeiter kann durch keine Sicherheitstechnik der Welt ersetzt werden.

Cyberattacken: Der unsichtbare Feind

Wettlauf gegen die Zeit

Angreifer kann man nur abwehren, wenn man weiß, dass sie da sind. Die Messbarkeit von Cyberangriffen ist die Basis für die Einführung geeigneter Schutzmaßnahmen. Lediglich 23 Prozent der Unternehmen sind jedoch laut eigener Einschätzung in der Lage, Cyberangriffe überhaupt zu erkennen.

Die große Herausforderung: Unternehmen müssen in der Lage sein, Auffälligkeiten in ihren Datenflüssen schnell und frühzeitig zu erkennen. Entscheidend sind zwei Faktoren: die schnelle Erkennung eines Security Incidents und die rasche Behebung der Schwachstelle.

Kampf der Ohnmacht

Die österreichischen Unternehmen fühlen sich hilflos: Lediglich 18 Prozent der Unternehmen sind davon überzeugt, wirksam auf einen Cyberangriff reagieren zu können. 71 Prozent der befragten Unternehmen sind der Meinung, dass Cyberangriffe kaum bis gar nicht verhindert werden können.

Die Studie zeigt außerdem, dass Maßnahmen oft erst dann getroffen werden, wenn man bereits angegriffen wurde. Aus Angst vor den Folgen eines Angriffs aktiv zu werden, ist definitiv nicht der richtige Ansatz. Der bessere Weg: ein strategischer Ansatz zur Prävention von Cyberattacken. Und im Fall des Falles eine schnelle und effiziente Reaktion.

Prävention: alle Faktoren im Blick

Einen 100-prozentigen Schutz gegen Kriminalität gibt es weder in der realen Welt noch in der virtuellen Welt. Mit gut durchdachten Ansätzen können Unternehmen ihre Risiken jedoch wirkungsvoll reduzieren. Die vorausschauende Analyse von Bedrohungen ist enorm wichtig. Viele Unternehmen denken in erster Linie an Technologie, wenn es um die wirksame Abwehr von Cyberangriffen geht. Gefragt ist jedoch ein integrierter und ausgewogener Ansatz, der Menschen und Prozesse ebenso berücksichtigt wie Technologien.

Der Faktor Mensch

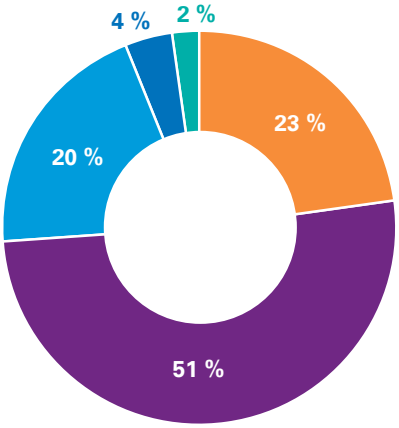
Wie bereits erwähnt, sind sensibilisierte Mitarbeiter noch wichtiger als eine fehlerfreie Sicherheitstechnik im Unternehmen. Auf der Firmenwebseite finden sich bisher unbekannte Bilder, ein Word- oder Excel-Dokument möchte plötzlich Makros aktivieren – Mitarbeiter müssen diese Abweichungen von der Norm erkennen und lernen zu hinterfragen. Einerseits sind sie ein interessantes Ziel für Angreifer, Stichwort „Social Engineering“, andererseits sind sie auch das wirksamste Präventionsmittel.

> “Die meisten Unternehmen unterschätzen, wie schnell sie zur Zielscheibe von Angriffen werden können.”
>
> Robert Schischka
> CERT.AT

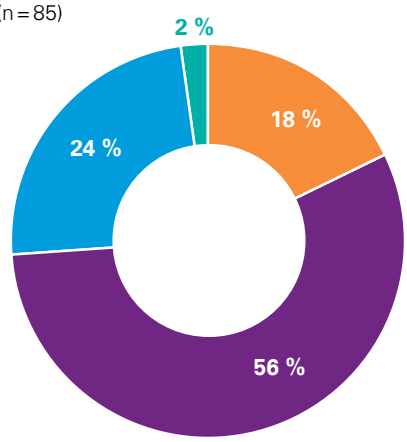
Schutz durch Bewusstseinsbildung

Bewusstseinsbildung ist das A und O: Der Schaden durch „CEO Fraud“ kann in Millionenhöhe gehen. CEO Fraud funktioniert nur durch die gezielte Beeinflussung des Menschen, technische Aspekte sind hier kaum relevant. Die meisten Cyberattacken sind nur durch die Ausnutzung der Schwachstelle Mensch erfolgreich – etwa durch den unreflektierten Klick auf den Link in einer E-Mail oder das Ausführen eines Makros in einem Word-Dokument. Auch die neue Angriffsform der „Zero-Day-Attacken“ arbeiten auf diese Weise.

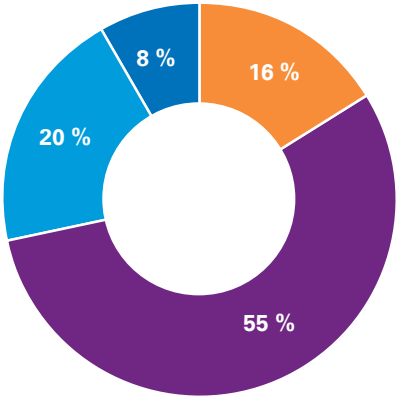
Unser Unternehmen ist in der Lage Cyberangriffe zu erkennen.
(n = 95)



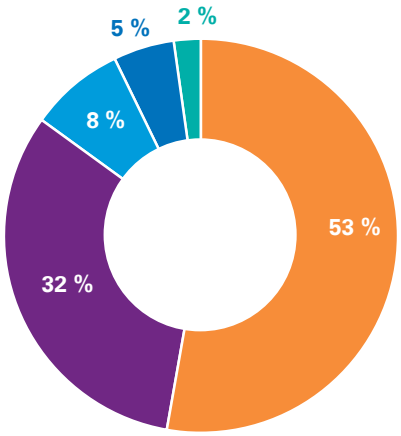
Unser Unternehmen ist in der Lage wirksam auf einen Cyberangriff zu reagieren.
(n = 85)



Cyberangriffe können nicht verhindert werden.
(n = 85)

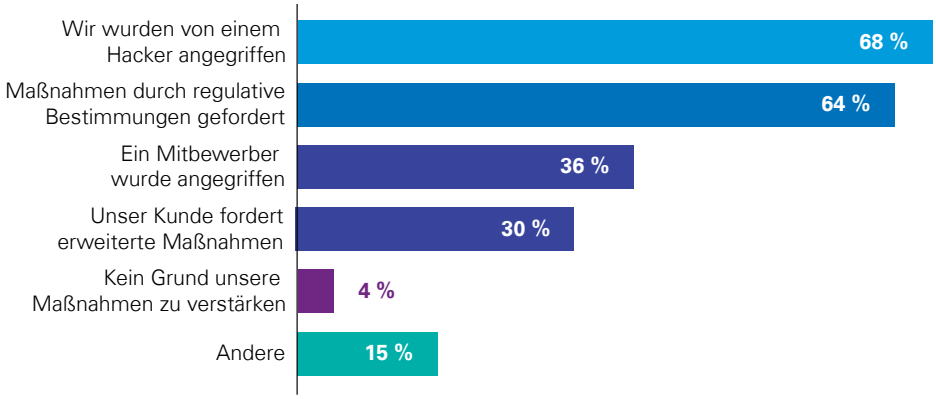


Die Zusammenarbeit mit anderen Unternehmen ist wichtig.
(n = 85)



trifft zu | trifft eher zu | trifft eher nicht zu | trifft nicht zu | weiß nicht

Treibende Kräfte, um Maßnahmen gegen Cyberkriminalität zu verstärken?
(n = 84)



71 %
glauben, Cyberangriffe nicht ganz verhindert zu können
(n = 85)

68 %
reagieren reaktiv statt vorausschauend
(n = 84)

18 %
können wirksam auf Cyberattacken reagieren
(n = 85)

23 %
sind in der Lage, Angriffe zu erkennen
(n = 95)

Cyberangriffe können jedes Unternehmen treffen

Was sind aus Ihrer Sicht die aktuellen Trends in Bezug auf Cyberattacken und Cyberkriminalität?
DDOS Angriffe (Distributed Denial of Service) in Kombination mit Erpressung nehmen derzeit stark zu. Davor warnen wir seit vielen Jahren. Viele Unternehmen haben sich gezielt darauf vorbereitet, die meisten erwischt es aber eiskalt. Viele Unternehmen machen sich keine Gedanken darüber, dass jemand gezielt ihre Webseite lahmlegen kann.

Ein zweiter großer Trend ist die verstärkte Orientierung der organisierten Kriminalität hin zu Firmenkunden. Hier wird hochprofessionell vorgegangen: Erhebung von Informationen im Vorfeld, gezielte maßgeschneiderte Phishing-Angriffe mittels Spear Phishing oder Waterholing. Auch die Beute wird gezielt einer Marktsegmentierung unterworfen: Man recherchiert, was das Unternehmen für einen Kontostand hat, welche Zeichnungsberechtigung es gibt, was die typischen Transaktionen und Überweisungsgrenzen sind. Ausgewählte Angriffsziele werden dann besonders „betreut". Der eigentliche Angriff ist nicht technisch, eine sehr ausgefeilte Variante von Social Engineering: Eine ganze Geschichte wird aufgebaut, entsprechende, glaubwürdig klingende E-Mails versendet, nachtelefoniert.

Die KPMG-Studie zeigt, dass über 90 Prozent der Unternehmen glauben, dass Angriffe nicht verhindert werden können. Interessanterweise ist gerade bei Unternehmen, die ein unterdurchschnittliches Sicherheitsbudget haben, das Vertrauen tendenziell größer…
Je mehr man sich mit der Thematik beschäftigt, desto kritischer sieht man die Unverwundbarkeit der eigenen Systeme. Man erkennt relativ rasch, dass man etwa gegen einen entsprechend motivierten Geheimdienst als Unternehmen chancenlos ist.

Die meisten Unternehmen unterschätzen, wie schnell sie zur Zielscheibe von Angriffen werden könnten. Man kann etwa allein deshalb ein Opfer werden, weil man das falsche Produkt einsetzt – etwa das falsche Content Management System: das System hat eine populäre Schwachstelle, wird gescannt, gefunden und automatisiert gehackt. Cyberangriffe passieren jedem Unternehmen – rein statistisch gesehen ist fast jedes irgendwann einmal betroffen. Zyniker sagen: es gibt jene, die es wissen, dass sie betroffen sind und jene, die es einfach nicht merken.

In letzter Zeit häufen sich Fälle von CEO Fraud, eine Kombinationsattacke aus Cyberkriminalität und klassischem Betrug, dem eine Reconnaissance-Phase voraus geht…
Ein Grundproblem ist, dass Informationen über Lebensdetails, Gewohnheiten, bis hin zu „ist jemand per Du mit einer Person?" heute leichter herauszufinden sind. In Kombination mit dem allgegenwärtigen Facebook-Exhibitionismus, sind solche Daten einfach zu erheben. Weiß ich solche Sachen über eine Person, habe ich einen entscheidenden Informationsvorsprung für zB CEO Fraud.

Brauchen wir also eine Bewusstseinsänderung in unserem Zugang zum Thema Vertraulichkeit versus Allgegenwärtigkeit von Informationen?
Das ist ein Thema, richtig. Das andere Thema ist: wir haben bis heute das Problem der Authentisierung, der Authentifikation des Gegenübers nicht gelöst. Es ist zu kompliziert geworden, wir haben zu viele Trust Center. Der Benutzer hat keine Kontrolle darüber, welchen Trust Centern vertraut wird. Das ist ein Riesenproblem für die zentrale Frage des Vertrauens in eine Technologie.

Es stellt sich die Frage, wie wir dieses Vertrauen wiederherstellen können. Was braucht es dafür?
Verlässliche Trusted Prozesse. Und ein weniger zerstrittenes Europa. Will man beispielsweise ein europäisches Firewall-Produkt kaufen, hat man eine sehr überschaubare Anbieterliste.

Würden europäische Standards helfen?
Ein stärkeres, europäisches Selbstbewusstsein würde schon helfen. Wir haben mit Sicherheit gute Wissenschaftler, gute Techniker. Betrachtet man aber die letzten zehn Jahre in der Informationstechnologie, spielen

Interview mit Mag. Robert Schischka, Leiter CERT.AT (Computer Emergency Response Team)

Robert Schischka
Leiter CERT.AT

europäische Konzerne kaum eine Rolle. Warum schaffen es US-Konzerne sehr wohl, heimische Firmen in der Beschaffung zu bevorzugen? Beim Sturmgewehr für das Militär kann ich laut Vergabegesetz entscheiden, dass bestimmte Hersteller zu bevorzugen sind. Für Sicherheitskomponenten im IT-Bereich geht sowas nicht.

Kann man sich als Unternehmen überhaupt noch auf irgendetwas verlassen?
Derzeit habe ich eher wenig Hoffnung. Man muss natürlich unterscheiden: wie sehr reden wir von „normaler" Kriminalität und wie sehr reden wir von staatlicher Aufklärung und Wirtschaftsspionage. Nur weil man sich gegen den Geheimdienst de facto nicht schützen kann, sollte man nicht vergessen, dass es sich trotzdem lohnt, angemessene Schutzmaßnahmen gegen den durchschnittlichen Angreifer einzusetzen.

Das heißt, Unternehmen müssen sich überlegen, wie sie ihre Sicherheitsstrategie ausrichten, etwa: Ein Schutz vor Geheimdiensten liegt außerhalb unserer Möglichkeiten, sehr wohl ist es uns aber möglich, uns gegen die übliche Cyberkriminalität zu rüsten.
Für das Unternehmen kann man das so sagen, ja. Wenn man ein Defense Contractor ist oder wirklich Leading Edge Research betreibt, dann sollte man versuchen, eine Stufe höher zu greifen. Um am Boden der Realität zu bleiben: Für die breite Masse an Unternehmen ist nicht der Geheimdienst der große Feind, sondern der normale Kriminelle, der routinemäßig klopft und schaut, ob ich geschützt bin.

Gerne wird auch auf die Gefahr von innen vergessen: nicht adäquate Zugriffsrechte im Unternehmen, nicht ordentliche Protokollierung von Dingen. Hier geht es um das Thema: Erkennen eines Angriffs. Wie schnell erkenne ich, dass ich gehackt bin, und wie sehr bin ich in der Lage, konsequent dagegen vorzugehen? Als Beispiel: bei komplexen Angriffen sind Fälle bekannt, bei denen der Täter fünf bis zehnmal innerhalb von wenigen Wochen wieder kam und über mindestens drei unterschiedliche Wege ins Unternehmen eindringen konnte.

Zusammenfassend heißt das, wir brauchen nicht nur mehr Bewusstsein, sondern wir brauchen auch mehr Budget?
Wir brauchen natürlich auch mehr Budget. Unternehmen müssen sich bewusst sein: wir haben hochkomplizierte Systeme und wir brauchen gut ausgebildete Leute, die das betreiben. Oder als Alternative: IT ist nicht mein Kerngeschäft, ich lagere es an einen verlässlichen Partner aus. Hier muss ich mich im Outsourcing-Prozess darum kümmern, dass mein Partner dieses Thema ernst nimmt.

Cyber Security: Die richtige Strategie

Verkannte Gefahr

Die Studie zeigt, dass die Befragten den unternehmerischen Gesamtkontext von Cyber Security noch nicht erkannt haben. Denn: 53 Prozent der Unternehmen sehen Cyber Security als technische Angelegenheit. 91 Prozent sehen das Thema als eine operative Angelegenheit und klassisches IT-Thema. Cybersicherheit ist in österreichischen Unternehmen somit noch nicht „Chefsache". Im digitalen Zeitalter muss das Thema jedoch unbedingt im Verantwortungsbereich der Unternehmensleitung liegen. Die Führungsebene muss sich ausreichend über Chancen und Risiken in der Cyberwelt informieren und das Thema als Fixpunkt auf die Agenda setzen.

Cyber Security managen

Diese Einstellung „Cybersicherheit ist IT-Thema" birgt große Gefahren: Technik alleine kann längst nicht mehr gegen Angriffe schützen, Cyberkriminalität gehört vielmehr zu den Top-Risiken im Unternehmen. Benötigt werden daher ein strategisches Gesamtkonzept sowie ein durchdachtes Cyber Security-Managementsystem. Ein derartiges System adressiert nicht nur technische Komponenten, sondern schafft organisatorische Voraussetzungen für den Kampf gegen Cyberkriminalität. Das Thema findet so seinen Platz in der Unternehmenskultur. Hier ist der Vorstand/die Geschäftsführung gefordert. Informationssicherheit darf kein Zufallsprodukt sein.

Unzureichende Berichterstattung

Ein wichtiger Indikator ist hier die Berichterstattung in Richtung Führungsebene. 23 Prozent der befragten Unternehmen haben noch keine derartige Berichterstattung zum Thema Cyber Security etabliert. Die Unternehmen werden erst aktiv, wenn bereits Angriffe stattgefunden haben: Mehr als 50 Prozent der Betriebe, die bereits einen Sicherheitsvorfall hatten, haben zumindest ein quartalsweises oder wöchentliches Reporting eingeführt. Die Maßnahmen sind nach wie vor reaktiv statt vorausschauend: Idealerweise sollte ein geeignetes Tool zur Berichterstattung bereits vor einem größeren Schaden eingeführt werden.

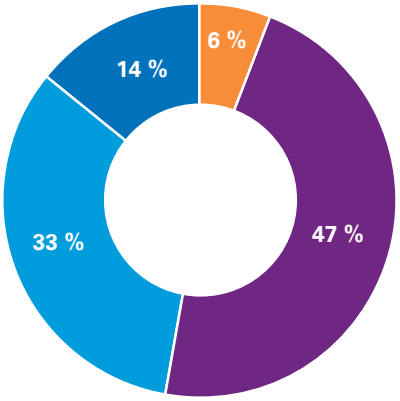
> "Im Cyberraum dreht sich sehr viel um das Thema Eigenverantwortung – jeder muss seinen Teil dieser Verantwortung wahrnehmen."
>
> Roland Ledinger
> Bundeskanzleramt

Bewusstsein für Cyberkriminalität stärken

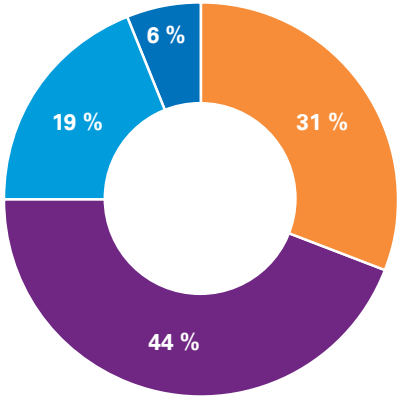
69 Prozent der Unternehmen sehen noch Verbesserungsbedarf in der Awareness auf der obersten Führungsebene. Nur 24 Prozent der Unternehmen sind überzeugt, dass bei ihren Mitarbeitern ausreichendes Bewusstsein für Cyberangriffe besteht. Eine der Ursachen: Es gibt keine oder nur sehr wenige für Cyber Security zuständige Mitarbeiter in den Unternehmen.

Bei mehr als 60 Prozent der Unternehmen ist Cyber Security in der IT-Abteilung angesiedelt. Bei 25 Prozent der Befragten gibt es eine eigene Organisationseinheit. Die Entwicklung hin zu eigenen, von der IT ausgegliederten Abteilungen wäre der Idealzustand. Eine solche Investition lohnt sich in jedem Fall, um das Bewusstsein für Cyberkriminalität zu stärken und dadurch Angriffe abzuwehren.

Wir betrachten Cyber Security als technische Angelegenheit.
(n = 88)

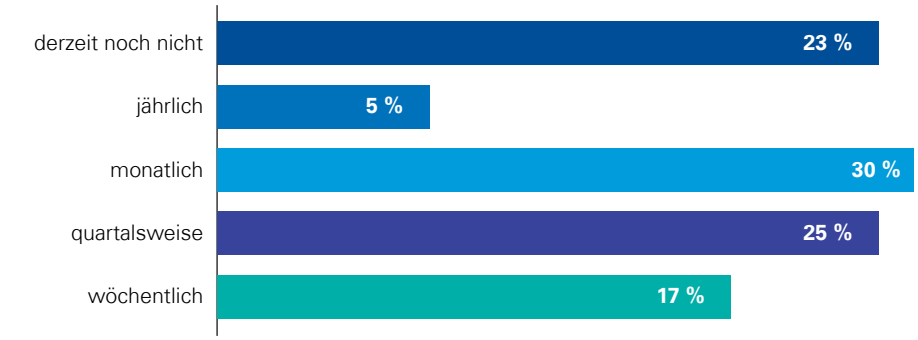


Cyberrisiken werden bei uns auf oberster Ebene (Vorstand, Geschäftsführung) diskutiert.
(n = 88)

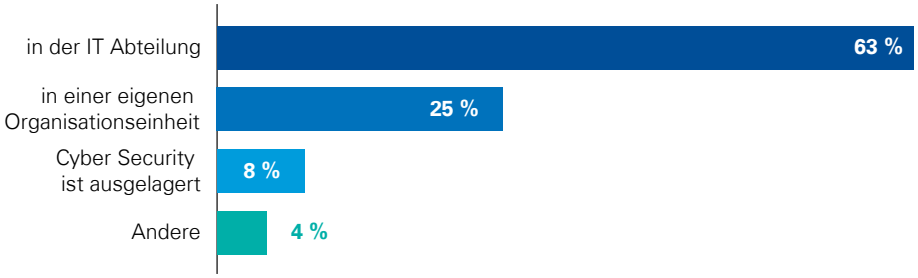


trifft zu | trifft eher zu | trifft eher nicht zu | trifft nicht zu | weiß nicht

Reporting von Cyberangriffen
(n = 87)



Wo ist Cyber Security in Ihrem Unternehmen angesiedelt?
(n = 91)



63 %
haben Cyber Security in der IT-Abteilung angesiedelt
(n = 91)

45 %
haben keinen dezidierten Cyber Security-Mitarbeiter
(n = 89)

31 %
diskutieren Cyberrisiken auf Führungsebene
(n = 88)

23 %
der Unternehmen haben keine Berichterstattung von Cyberangriffen
(n = 87)

Cyber Security sollte im Kindergarten beginnen

Die KPMG-Studie zeigt, dass eine absolute Mehrheit, also über 50 Prozent der Befragten, glaubt, dass Cyberangriffe nicht verhindert werden können. Überrascht Sie das?
Das überrascht mich grundsätzlich nicht. Auch in der realen Welt kann man durch Alarmanlagen oder Polizeipräsenz zwar Verbrechen eindämmen, aber verhindern kann man sie trotzdem nicht. So ist es auch im Cyberraum. Man kann durch Prävention viel verhindern, aber eine 100-prozentige Sicherheit wird es nie geben.

KMUs glauben mehrheitlich, als Ziel nicht attraktiv zu sein. Das widerspricht einer Studie von Symantec: demnach betreffen zwei Drittel der Cyberangriffe KMUs. Wie kann man dieses Awareness-Gap schließen?
Es liegt letztlich an uns allen und an den Maßnahmen der Interessensvertretungen und auch der Bundesregierung, die Awareness zu heben. Von Seiten des Wirtschaftsressorts, der Wirtschaftskammer und teilweise auch in unserem Bereich gibt es entsprechende Programme. Oft ist es allerdings schwierig, KMUs, für die IKT (Informations- und Kommunikationstechnik) nicht zum Kerngeschäft gehören, für das Thema zu begeistern.

Müsste man beim Thema Cyber Security bereits viel früher ansetzen, bei Schule und Ausbildung?
Grundsätzlich bin ich der Meinung, man sollte im Kindergarten beginnen. Das Thema sollte Bestandteil der Elementarerziehung sein, genauso wie Kinder die Regeln des Straßenverkehrs kennen lernen. Kinder müssen rechtzeitig lernen, sich in der digitalen Welt korrekt zu verhalten. Wir haben schon vor Jahren mit Programmen begonnen, diese Sicherheitsfragen auch in Kindergärten zu adressieren.

85 Prozent der Unternehmen haben in der Studie betont, dass sie die Zusammenarbeit zwischen den Unternehmen als besonders wichtig einstufen. Kann das staatliche Umfeld dazu beitragen, dass diese Zusammenarbeit noch verstärkt wird?
Plattformen wie der Austrian Trust Circle sind enorm wichtig: Branchen tun sich hier zusammen und tauschen sich aus. Man kann in einer vertrauenswürdigen Umgebung auf gleichem Niveau sprechen. Wir fördern diese Entwicklungen seit vielen Jahren. Reichert man solche Aktivitäten dann noch durch CERT-Strukturen (Computer Emergency Response Team) an, dann ist der Erfahrungsaustausch noch wesentlich größer.

Welche Art von Reporting wäre aus Ihrer Sicht notwendig, um zu einem aussagekräftigen Lagebild auf staatlicher Ebene im Sinne der NIS Directive (Network and Information Security Directive) zu kommen?
Man müsste sicherstellen, dass die auf Ebene der Organisation gesammelten qualifizierten Informationen bereits in ein gemeinsames Lagebild eingespeist werden. Aus meiner Sicht macht es keinen Sinn, dass alle noch nicht verifizierten Incidents, irgendwo an einer zentralen Stelle gesammelt werden. Ich persönlich bin überzeugt, dass das nur das Branchen-CERT oder die Branche selbst machen können. Nur mit dieser Qualifizierung macht es Sinn, auf der nächsten Ebene ein Lagebild zu erstellen.

Ansonsten befinden wir uns auf der Ebene der Google- und Microsoftberichte, die im Netz viel sehen und zusammenfassen. Das ist natürlich auch wichtig, aber das sagt noch nichts über die Möglichkeit der Einschätzung: Wie ist unsere Lage wirklich?

Zwei Drittel der befragten Unternehmen haben angegeben, nach einem schwerwiegenden Vorfall die Behörden zu involvieren – obwohl es keine gesetzliche Verpflichtung gibt?
In den letzten Jahren konnte ein gewisses Grundvertrauen aufgebaut werden, das ist positiv. Niemand vermutet mehr, dass der Staat diese Informationen missbraucht. Natürlich geht es hier aber nicht nur um die Meldung der Vorfälle, sondern auch um die Frage der Strafverfolgung. In weiterer Folge geht es um die Einschätzung, wie sehr die Geschäftsführung bzw die

Interview mit Ing. Roland Ledinger, Leiter Bereich IKT Strategie des Bundes, Bundeskanzleramt

Roland Ledinger
Leiter Bereich IKT Strategie
des Bundes, Bundeskanzleramt

Verantwortlichen die notwendigen Vorkehrungen getroffen haben, um ihre Haftungsfrage klären zu können. Da ist die Einbindung der Behörde ein guter Indikator.

Über 80 Prozent der Studienteilnehmer geben an, dass ihrer Meinung nach österreichische Behörden, die Wirtschaft nicht oder nur wenig effektiv vor Cyberangriffen schützen. Was kann verbessert werden?
Im Cyberraum dreht sich sehr viel um das Thema Eigenverantwortung – jeder muss seinen Teil dieser Verantwortung wahrnehmen. Es gibt noch immer die falsche Vorstellung, dass die Polizei oder die Behörden, mich vor allem schützen könnten – das funktioniert in der realen Welt nicht und im Cyberraum schon gar nicht. Weder Unternehmen noch Privatpersonen können von der Polizei vor Cyberangriffen geschützt werden. Diese Stellen können nur aufzeigen, was zu tun ist, damit das Risiko eines Angriffes reduziert wird.

Was könnte man auf europäischer Ebene tun, um das Thema Cybersicherheit noch weiter voranzutreiben?
Vernetzung ist hier das A und O. Die öffentlichen Stellen sind schon gut vernetzt – bei den Branchen besteht noch Aufholbedarf. Ein guter Ansatz wäre, Public-Private-Partnerships, so wie wir es in der Cyber Sicherheits-Plattform betreiben, über ganz Europa auszubreiten. Auch im Bereich der Standardisierung müsste einiges passieren. Wenn ich verschiedenste IT-Systeme für elektronische Identitäten habe, dann habe ich überall Sicherheitsbrüche zwischen den verschiedenen Staaten. Für sicherheitsrelevante Systeme müsste man eine Harmonisierung finden.

Wie lautet Ihre Einschätzung: Wie steht Österreich im europäischen Vergleich zum Thema Cybersicherheit da?
Wir haben eine ganz gute strategische Grundlage und gute Strukturen. Aufholbedarf besteht im Bereich der Investments in die Sicherheit.

Österreich ist sehr gut aufgestellt im Krisenmanagement über SKKM (Staatliches Krisen- und Katastrophenschutzmanagement), wenn es um klassische Krisen wie Hochwasser oder Lawinen geht. Inwiefern wurde dies bisher in den Cyberraum übertragen?
Das funktioniert bereits bestens. Ein Thema wird solange im Experten-Cyber-Arbeitskreis behandelt, solange es keine Krise ist. Sobald es über die IT-Mechanismen hinausgeht, wird sofort das SKKM eingebunden. Letztlich ist es ja sekundär, ob die Stromversorgung wegen einer Naturkatastrophe oder wegen eines Cyberangriffs ausfällt. Bisher musste das SKKM aber noch nicht im Cyberbereich tätig werden.

Angriffe können nicht immer verhindert werden

Was sind aus Ihrer Sicht derzeit die drei wichtigsten Trends in Bezug auf Cyberattacken und Cyberkriminalität?
Erstens: Angriffe auf kritische und strategische Infrastrukturen. Es handelt sich hierbei um Angriffe auf Wasserkraftwerke, Hafenanlagen, Hochöfen bis hin zu Atomkraftwerken. Solche Vorfälle werden nur selten bekannt. Ein durch diese Angriffe ausgelöster digitaler Stillstand ist jedoch ein wesentliches Thema für das Militär. Hier geht es um die Landesverteidigung im Cyberraum.

Zweitens: die Cyberspionage. Sie kann gegen Unternehmen, Wissensinstitutionen oder Forschungseinrichtungen gerichtet sein, die ihre Assets nicht ordentlich schützen. Dadurch wird Cyberspionage sogar zu einem volkswirtschaftlichen Problem. Es gibt eine österreichische Studie aus dem vergangenen Jahr, die belegt: hochgerechnet haben wir jährlich mindestens 1,6 Milliarden Euro Schaden durch Wirtschaftsspionage. Für Deutschland spricht man von 50 Milliarden Euro. Aktuell laufen Erpressungsangriffe mit Verschlüsselungsprogrammen wie „Locky" gegen Unternehmer, Behörden und Einzelpersonen. Gleichzeitig gibt es eine Welle von gezielten Angriffen mit Betrugsabsicht gegen CEOs und wichtige Unternehmensmitarbeiter.

Drittens: Der Missbrauch personenbezogener Daten. Dazu zählt auch die Manipulation von bestimmten Methoden wie Forecast Analytics.

Ist Cyberspionage ausschließlich gegen die gesamtstaatliche Souveränität ausgerichtet oder zielt sie auch auf einzelne Unternehmen ab?
Cyberspionage zielt natürlich ebenso auf Unternehmen ab. Hier geht es in erster Linie darum, Know-how zu stehlen. Der Markt ist groß: Es gibt Informationsanbieter wie zum Beispiel „Cyber Söldner", die andere ausspionieren und das Wissen dann verkaufen. Cyberspionage gegenüber Unternehmen kann auch von staatlichen Diensten anderer Länder ausgehen – mit dem Ziel, die eigene Wirtschaft zu stützen.

Sie hat die gleiche Zielsetzung wie die klassische Spionage in der analogen Welt – nur die Mittel und Wege sind neu. Cyberspionage ist weltumspannend möglich. Die Folgen: Es gibt Werke in Fernost, die durch Firmenspionage zum Teil bis zum halben Preis oder für 20 Prozent der ursprünglichen Kosten produzieren können. Das wird für den Staat gefährlich.

Ist es durch Cyberspionage für die Spione einfacher geworden in Unternehmen einzudringen als früher?
Wenn von einem Unternehmen die richtigen Schutzmaßnahmen getroffen werden, dann braucht es immer noch eine Person, die einbricht, um dem Unternehmen etwa die Festplatte zu entwenden. Ist die Festplatte dann auch noch verschlüsselt und das Passwort nicht bekannt, muss man wiederum die Menschen direkt ausspionieren. Man darf also nicht glauben, dass es die ursprüngliche Form der Spionage nicht mehr gibt.

Große Konzerne, die für das Thema sensibilisiert sind und das Gefahrenpotenzial kennen, machen viel für ihren Schutz, etwa durch Verschlüsselungen. Ist für Angreifer die Verschlüsselung nicht zu knacken, wird direkt auf die Zielperson abgezielt, etwa durch Verwanzung. Eine Verschlüsselung allein ist also nicht ausreichend. Die Spione von heute sind technisch top.

Wie schätzen Sie die Situation bei den österreichischen Unternehmen ein? Sind sich die Unternehmen dieser Bedrohungen bewusst?
Wir führen Sicherheitsüberprüfungen für Unternehmen durch, die eine solche gegenüber ausländischen Dienststellen vorweisen müssen. In den von uns beratenen Unternehmen sind zum Großteil sicherheitsbewusste Mitarbeiter angestellt, die auf die Gefahren sensibilisiert sind.

Es wäre aber falsch daraus zu schließen, dass alle Unternehmen so gut aufgestellt sind. Meine Erfahrung ist, dass der Großteil der kleinen und mittleren Unternehmen wenig bis gar nichts für die Sicherheit tut.

Interview mit Obst dG Mag. Walter Unger, Leiter der Abteilung C im Abwehramt, Bundesministerium für Landesverteidigung und Sport

Walter Unger
Leiter der Abteilung C im Abwehramt

Bei Bankinstituten herrscht meiner Einschätzung nach ein relativ hohes Niveau, weil die Branche permanent im Fokus der Angreifer steht. In der Sicherheitscommunity weiß man heute, dass Angriffe nicht zu 100 Prozent verhindert werden können. Man muss damit rechnen, angegriffen und geschädigt zu werden. Wichtig ist es, eine entsprechende Sicherheitsorganisation zu haben, die sofort eingreifen kann. Dazu gehört auch die Bewusstseinsbildung unter den Mitarbeitern. Awareness zu vermitteln ist durch zum Teil hohe Mitarbeiterfluktuationen eine Daueraufgabe.

Über 80 Prozent der Befragten sind der Meinung, dass österreichische Behörden (wie die Polizei) die Wirtschaft nicht oder nur wenig effektiv vor Cyberangriffen schützen. Warum?
Der Staat ist auf allen Ebenen im Rückzug. Wir wollen ja einen kostengünstigen Staat – daher sind auch die Elemente für den Schutz im Bereich Cyber Security klein und beschränken sich im Wesentlichen auf die Strafverfolgung. Die Unternehmen müssen hier ihre Einstellung ändern und selbst gute Schutzmaßnahmen treffen. Der Staat selbst kann etwa aktuelle Lagebilder liefern. Wir erhalten Meldungen über Schwachstellen bevor diese veröffentlicht werden. Das gibt den Betroffenen Zeit, das Problem zu lösen bevor eine Attacke auf die vorhandene Schwachstelle stattfindet.

Zusammenarbeit, Vernetzung und Austausch sind Kernelemente im Bereich Cyber Security. Kann der Staat den Wissensaustausch und die Vernetzung fördern?
Immer nur so weit, wie es die Unternehmen zulassen. Wenn sich ein Unternehmen nicht in die Karten schauen lassen möchte, dann kann auch der Staat nicht helfen.

Ziel muss eine vertrauensvolle Zusammenarbeit zwischen Staat und Unternehmen sein. Der Staat kann außerdem Vorschriften für Sicherheitsmaßnahmen in Unternehmen festlegen. In Deutschland sind diese Maßnahmen etwa per Gesetz vorgeschrieben: Somit werden die Unternehmen gezwungen, ein gewisses Maß an Sicherheit zu gewährleisten.

Was sind aus Ihrer Sicht die wichtigsten Trends oder Herausforderungen im Bereich Cyber Security in den nächsten Jahren?
Sicherheit muss erstens leistbar sein. Das gelingt, wenn man geeignete Systeme und Methoden entwickelt und diese auch gelebt werden. Zweitens muss für den Fall eines Angriffes ein Incident-Management eingeführt werden. Drittens sollte Sicherheit als Business Enabler erkannt werden.

Das Schlagwort heißt: Awareness!

Welche Bedeutung hat Informationssicherheit für Ihr Unternehmen?
Der Schutz von Daten unseres Unternehmens und unserer Kunden hat für uns einen sehr hohen Stellenwert. Natürlich muss man ergänzen, dass Informationssicherheit in anderen Branchen eine noch zentralere Rolle spielt – nämlich überall dort, wo Datenverwaltung zum Kerngeschäft gehört. Als Beispiel könnte man Mobilfunkanbieter oder Bankinstitute nennen.

Glauben Sie, dass der Lebensmittelbereich ein interessantes Ziel für Cyberangreifer ist?
Das würde ich eher verneinen. Unser Unternehmen hat keine Geschäftsgeheimnisse im Sinne von Patenten oder Rezepturen. Das macht uns in Hinblick auf „Datenklau" für Angreifer uninteressant. Es ist uns natürlich bewusst, dass niemand vor Wirtschaftskriminalität per se geschützt ist. Bei vielen Cyberangriffen geht es weniger um die Branche als um die Außenwirksamkeit, die Größe und das Markenimage. Alles in allem sehen wir uns aber nicht als vorrangige Zielscheibe.

Welches Bedrohungsszenario erscheint Ihnen am ehesten realistisch?
Das Blockieren von Abläufen und Prozessen durch einen gezielten technischen Angriff von Hackern auf Unternehmenssysteme. Wobei ich auch hier die Eintrittswahrscheinlichkeit für unser Unternehmen als eher gering einstufen würde. Wenn solche Angriffe jedoch erfolgreich sind und der Zugriff zu Kernsystemen eines Unternehmens ermöglicht wird, sind die Folgen weitreichend: von finanziellen Auswirkungen angefangen bis hin zu noch größeren Auswirkungen auf die Reputation eines Unternehmens.

Welche Rolle schreiben Sie den Mitarbeitern in einem Unternehmen in puncto Cyberkriminalität zu?
Eine ganz entscheidende. Wir versuchen in der Prävention in erster Linie die Menschen zu adressieren. Firewalls und technische Systeme, um Angriffe zu verhindern sind natürlich enorm wichtig. Das Schlagwort heißt hier aber eindeutig: Awareness. Die Mitarbeiter werden durch Schulungen auf die Gefahren von Cyberkriminalität sensibilisiert. Unser Hauptaugenmerk liegt in der Bewusstseinsbildung der Mitarbeiter, der Erziehung des mündigen Users.

Auch die Nutzung von Webmail-Diensten und privaten Devices durch Mitarbeiter birgt ein gewisses Gefahrenpotenzial. Es kommt etwa in Unternehmen häufig vor, dass das eine oder andere geschäftliche E-Mail über Webmail-Dienste verschickt wird. Die Handhabung von privaten Geräten wie etwa Handys im Unternehmen spielt eine große Rolle, weil dadurch viele Angriffspunkte entstehen. Sollte wiederum ein Mitarbeiter selbst dolose Handlungen begehen, ist ein Nachweis kaum möglich, da sich das Gerät im Eigentum des Mitarbeiters befindet.

Die Gefahr kann ja nicht nur von außen kommen, sondern auch von innen. Wie beurteilen Sie dieses Bedrohungsszenario?
Aus unserer Sicht ist für Unternehmen der Datendiebstahl durch einen Innentäter die oft größere Gefahr als ein Angriff von außen. Das kann im ganz kleinen Rahmen geschehen: Mitarbeiter nehmen häufig Unternehmensdaten von einem Arbeitgeber zum nächsten mit, von Gehaltsdaten angefangen bis Kalkulationen oder die GuV. Es geht selten darum diese Daten an Dritte zu verkaufen oder einen direkten finanziellen Vorteil daraus abzuleiten. Viel mehr will man sich selbst durch diese Daten einen Vorteil verschaffen, sich „wertvoller machen". Dennoch darf das keinesfalls als Kavaliersdelikt gewertet werden!

Wo liegen Ihrer Meinung nach die größten Herausforderungen für Cyber Security in der Zukunft?
Die zunehmende Vernetzung ist eine enorme Chance, birgt aber auch ein hohes Risiko. Datenmengen werden immer größer, sowohl die interne als auch die externe Vernetzung der Daten nimmt kontinuierlich zu. Einzelne Prozesse bis hin zur gesamten Wertschöpfungskette werden in Unternehmen digital abgebildet und mit Dritten verknüpft – als Beispiel könnte man

Im Rahmen eines anonymen Interviews gibt ein Vertreter der Lebensmittelbranche Einblick in den unternehmensinternen Umgang mit Informationssicherheit.

den Fakturenversand nennen. Durch diese vernetzten Prozesse steigt in weiterer Folge der Kontrollaufwand und die Transparenz sinkt. Im Fall des Falles steigt die Schadenshöhe dann exponentiell an, weil man Beeinträchtigungen nicht so schnell erkennen kann.

Die Vernetzung von Daten ist aus dem Arbeitsalltag nicht mehr wegzudenken. Sehen Sie das auch so?
Natürlich. Die Abhängigkeit besteht nicht nur gegenüber anderen Unternehmen, sondern auch gegenüber dem öffentlichen Bereich: ohne die Erfüllung von gewissen Formvorschriften oder das Absetzen von Meldungen bei der jeweiligen Aufsichtsstelle, darf der Geschäftsprozess eines Unternehmens oftmals nicht weiter fortgesetzt werden. Die Kernprozesse sind heute ohne eine funktionierende IT kaum mehr umsetzbar.

Wie wichtig sind hier Kontrollmechanismen?
Sehr wichtig. Die Effizienz, die man heute durch automatisierte Abläufe gewinnt, muss man zu einem gewissen Grad wieder für die Kontrolle aufwenden. Wenn man so wie früher mit der Schreibmaschine Rechnungen schreibt, kann auch nur in kleinerem Ausmaß manipuliert werden. Verschickt jedoch ein zentrales System alle Rechnungen und es gelingt, hier einzugreifen, ist der angerichtete Schaden natürlich viel größer.

Holen Sie sich bei diesem Thema Rat von außen?
Ja. Wichtig für Unternehmen ist es, bei solch heiklen Themen auch auf externe Expertise zu vertrauen. Wir arbeiten etwa mit externen Dienstleistern zusammen, die uns bei der Analyse von verdächtigen Dateien unterstützen.

Welche Informationen sind aus Sicht der Geschäftsführung von Bedeutung, um einen Überblick im Unternehmen zu bewahren?
Als CFO kann man sich nicht um jedes Detail kümmern. Die Inhalte müssen von den fachlichen Experten auf ein allgemeines, verständliches Level gehoben werden. Ein CFO möchte in gefilterter Form wissen, welche Angriffe und Vorkommnisse es gab, welche Vorkehrungen und Maßnahmen getroffen worden sind sowie Informationen über deren Wirksamkeit. Ein externes Audit ist hier sehr hilfreich: die externen Experten können Gefahrenpotenziale professionell einstufen und Lösungsvorschläge liefern.

"Durch vernetze Prozesse steigt der Kontrollaufwand – die Transparenz sinkt."

Unternehmen stehen unter Handlungsdruck

Was sind aus Ihrer Sicht die aktuellsten Entwicklungen zum Thema Datenschutz, besonders in Hinblick auf rechtliche Standards?
Ab 2018 wird die Datenschutzreform der EU in Kraft treten – das ist sicherlich die größte und wichtigste Neuerung. Der wichtigste Punkt dabei ist die Erhöhung des Strafrahmens. Das Strafhöchstmaß kann bis vier Prozent des globalen Konzernumsatzes betragen. Das setzt Unternehmen unter enormen Handlungsdruck.

Die Unterschiede im Datenschutz zwischen Europa und den USA sind enorm. Ist hier eine Angleichung zu erwarten? Das „Safe Harbour"-Abkommen wurde unter Ihrer Mithilfe zu Fall gebracht – hat das neue Abkommen „Privacy Shield" Zukunft?
Die Nachfolge-Regelung „Privacy Shield", die den Datentausch zwischen EU und USA regeln soll, ist zum Großteil eine 1:1-Kopie des „Safe Harbour"-Abkommens. Dieses wurde aber vom EuGH gekippt, insbesondere aus zwei Gründen. Die Massenüberwachung persönlicher Daten von EU-Bürgern. Der EuGH hat geurteilt, dass es diese Art der Überwachung von Daten nicht geben darf. Im „Privacy Shield"-Text wird jedoch ausdrücklich festgehalten, dass es Massenüberwachung gibt. Also ein eindeutiger Konflikt mit dem EU-Recht.

Das zweite große Thema war das ungleiche Schutzniveau im privaten Bereich. US-Unternehmen können am europäischen Markt auftreten, ohne jenen Datenschutz zu bieten, den europäische Unternehmen nach europäischem Recht bieten müssen. Mit ein paar Sätzen in einer Datenschutz-Richtline können Unternehmen die Regelungen umgehen und am Ende mit den Daten machen, was sie wollen. Der EuGH hat jedoch judiziert, dass der Schutz „der Sache nach" gleich dem EU-Recht sein muss.

Insgesamt sind die neuen Regeln aus meiner Sicht rechtlich nicht sehr stabil. Viele Unternehmen behelfen sich daher mit Standardvertragsklauseln und anderen Rechtsgrundlagen, um Daten in die USA zu schicken, statt auf „Privacy Shield" zu vertrauen, da das neue Regelwerk am Ende vielleicht wieder vom EuGH aufgehoben werden wird.

Vorschriften für US-Unternehmen sind also weniger streng als jene für europäische Unternehmen. Was können europäische Provider tun, um sich mittelfristig gegen amerikanische Anbieter durchsetzen zu können?
Der große Pluspunkt ist die Sicherheit – das kann zu einem wesentlichen Vorteil am Markt führen. „Geht der Anbieter ordnungsgemäß mit den Daten um? Ist er ordentlich zertifiziert? Wer haftet? Welche Folgen hat es für mich als europäisches Unternehmen, wenn der Provider in den USA die Bestimmungen nicht einhält?" – solche Fragen fallen bei europäischen Anbietern in viel kleinerem Maß an.

Auch bei Fragen der „Massenüberwachung" ist man bei europäischen Providern auf der sichereren Seite. Man darf bei diesem Thema auch die Gefühlsebene nicht außer Acht lassen: vielen Usern ist es einfach lieber, die E-Mails in Österreich liegen zu haben statt irgendwo in einer anonymen US-Cloud. Wettbewerbsnachteile sind oft die Usability und die Kosten – hier sind die großen amerikanischen Serviceanbieter im Vorteil.

Zur Umsetzung der neuen EU-Datenschutz-Verordnung in Österreich: Gibt es Möglichkeiten für lokale Gesetzgeber, Anpassungen vorzunehmen?
Die Datenschutzverordnung ist im Prinzip unmittelbar anwendbar. Allerdings wirkt sie in vielen Bereichen eher wie eine Richtlinie, wo national noch angepasst werden kann.

In Österreich wird es eine Art „Datenschutzverordnungsbegleitgesetz" geben, das verschiedene Möglichkeiten für Anpassungen vorsieht. Bisherige Sonderparagraphen – wie etwa in der Gewerbeordnung, zu Direktmarketing oder zu Bonitätsdatenanbie-

Interview mit Mag. Max Schrems, österreichischer Jurist und Datenschutzaktivist

Max Schrems
Jurist und Datenschutzaktivist

tern – werden wahrscheinlich auch zukünftig bestehen bleiben. Bei vielen dieser Sondergesetze muss überprüft werden, ob sie mit der Verordnung kompatibel sind.

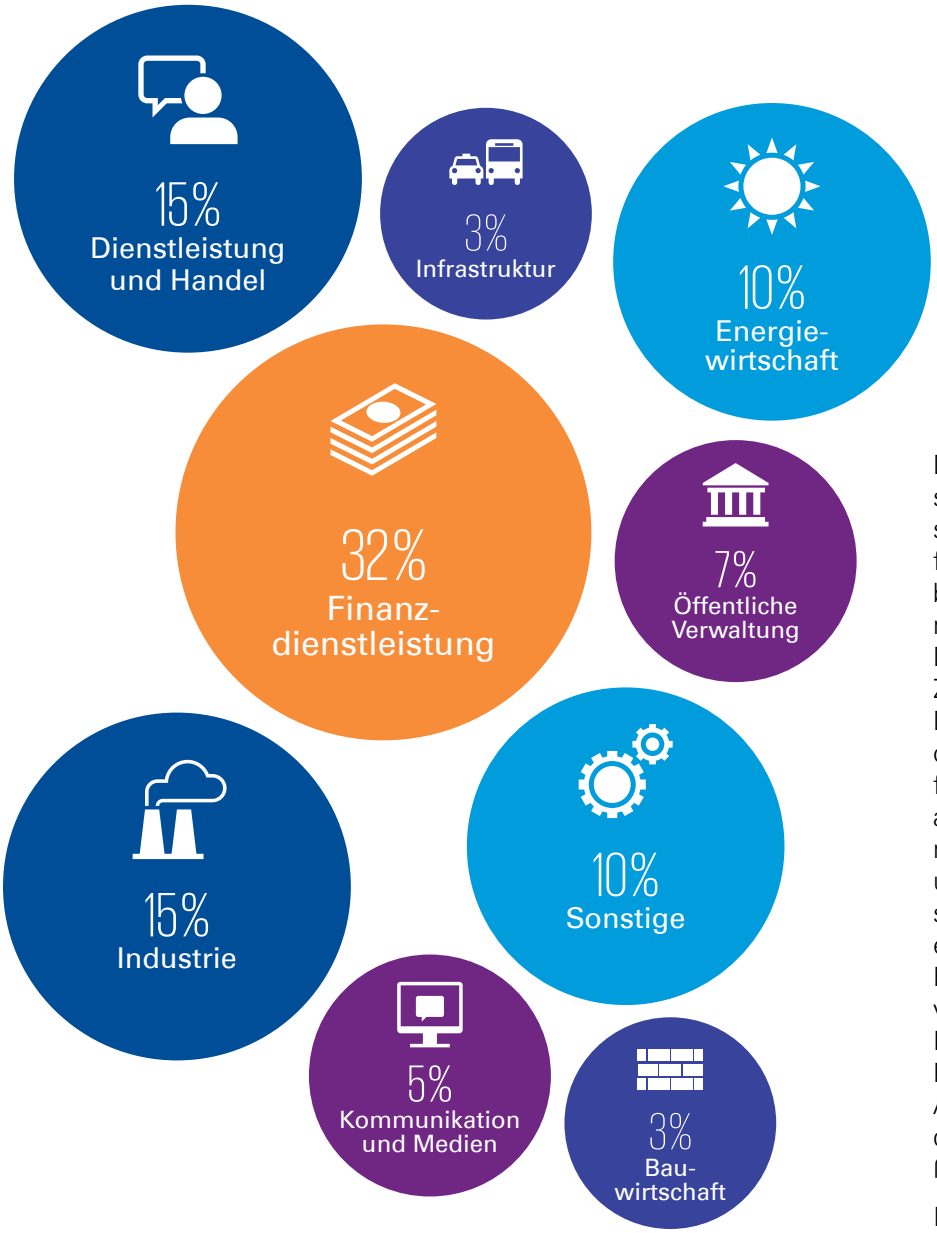
Was kann man österreichischen Unternehmen raten, um die neuen EU-Regelungen zu erfüllen?
Unternehmen haben bis 2018 Zeit zu evaluieren, ob und wie sie ihren Datenschutz anpassen müssen, um den neuen Anforderungen zu entsprechen. Es ist empfehlenswert, die Unternehmenssysteme rechtzeitig und genau zu überprüfen, denn ab 2018 drohen heftige Strafen wenn Datensätze falsch verarbeitet werden. In vielen Fällen werden nur kleinere Anpassungen vorgenommen werden müssen, um gesetzeskonform zu agieren. Viele Unternehmen haben den Bereich aber bisher vernachlässigt. Das erklärte Ziel des Gesetzgebers: es soll zu Änderungen und mehr Compliance in der Praxis kommen.

Um auf den Endnutzer zu sprechen zu kommen: Wo besteht hier Handlungsbedarf?
Man muss jedenfalls im Bereich der Ausbildung ansetzen, hier gibt es viel Nachholbedarf – niemand erklärt einem Kind in der Schule, was ein Cookie ist. Gleichzeitig muss man eingestehen, dass die Materie für den durchschnittlichen Endnutzer viel zu komplex ist, sodass manche Themen nicht in der Ausbildung vermittelt werden können.

Wie könnten Enduser und Konsumenten geschützt werden?
Die Etablierung einer glaubwürdigen Zertifizierung, einer glaubwürdigen Marke wäre meiner Meinung nach ein erster wichtiger Schritt. Weiters eine Art Datenschutz-Durchsetzungsvereinigung aufzustellen – damit beschäftige ich mich aktuell. Also eine Vereinigung, die Produkte testet, aber auch etwas gegen Unternehmen unternimmt, die sich nicht an die Gesetzte halten. Dadurch entsteht auch ein gewisser Druck, sich an Vorgaben zu halten.

Wird die EU-Datenschutz-Verordnung große Veränderungen herbeiführen?
Datenschutz war bisher eher ein stiefmütterliches Thema. Nun sind wir aber unwiderruflich in einer Informationsgesellschaft angekommen, in der Informationen die größten Assets für Unternehmen sind. Viele Unternehmen haben sich bisher nicht an Datenschutzbestimmungen gehalten – nicht unbedingt aus Bösartigkeit, sondern weil es für sie einfach kein wichtiges Thema war. Die Zeit ist nun reif, um „klar Schiff" zu machen, um bis zum Inkrafttreten der EU-Datenschutz-Verordnung gesetzeskonform zu sein.

Umfragemethodik



Die vorliegende Studie beschäftigt sich mit der Frage, wie österreichische Unternehmen den Herausforderungen der Cyberkriminalität begegnen und welche Cyber Security-Maßnahmen getroffen werden. Die Umfrage zur Studie wurde im Zeitraum von 9. November bis 4. Dezember 2015 unter 94 österreichischen Unternehmen durchgeführt. Die Teilnehmer setzen sich aus kleinen und mittleren Unternehmen sowie Großunternehmen unterschiedlicher Branchen zusammen. Jeder Teilnehmer erhielt einen Online-Fragebogen mit 25 Fragen. Die Ergebnisse wurden von einem Expertenteam aus dem Bereich IT Advisory ausgewertet. Fehlende Werte wurden bei der Auswertung ausgeschlossen. Dadurch variieren die Stichprobengrößen der einzelnen Variablen.

In persönlichen Interviews standen außerdem sieben Wirtschaftsvertreter und Cyber Security-Experten zum Thema Rede und Antwort.

Cyber Security

Unternehmerische Zukunft sichern

Finden Sie gemeinsam mit KPMG die richtige Strategie zur Umsetzung Ihres Cyber Security-Ansatzes. Mithilfe unseres Know-hows und unserer jahrelangen Erfahrung entwickeln wir Lösungen für eine verlässliche Cyber Security in Ihrem Unternehmen.

Orientiert an den Geschäftszielen

Gemeinsam mit Ihnen wollen wir Ihr Unternehmen voranbringen. Der positive Umgang mit Cyberrisiken hilft Ihnen nicht nur, die Unsicherheit in Ihrem Unternehmen unter Kontrolle zu bringen. Sie können daraus einen echten strategischen Vorteil ziehen.

Gestochen scharfe Analysen

Die rasante Digitalisierung mit immer neuen Möglichkeiten und Bedrohungen erfordert von Ihnen flexibles Handeln und einen sicheren Rückhalt. Unsere Spezialisten kennen sich sowohl mit Cyber Security als auch in Ihrem Markt aus. So vermitteln wir Ihnen wertvolle Erkenntnisse, überzeugende Ideen sowie bewährte Lösungen und schaffen die Basis dafür, dass Sie sicher handeln können.

Experten an Ihrer Seite

Cyberrisiken erzeugen oft Unsicherheit. Deshalb arbeiten wir Hand in Hand mit Ihnen. Im Sinne einer langfristig angelegten Partnerschaft beraten und fordern wir Sie, damit Sie die richtigen Entscheidungen treffen – und zwar mit begründeter Zuversicht.

kpmg.at/cyber

Publikationen

Sie suchen eine Studie oder Publikation von KPMG? Gerne helfen wir Ihnen weiter – senden Sie uns Ihre Anfrage unter **publikationen@kpmg.at**

Dimensionen

Die KPMG Kundenzeitschrift bietet dreimal jährlich fachliche Neuigkeiten aus den Bereichen Wirtschaftsprüfung und Beratung. Im Juni erscheint die nächste Ausgabe unter dem Schwerpunkt Cyber Security.

ACNews

Die Informationsbroschüre von KPMG enthält aktuelle Fragestellungen rund um das Audit Committee, Corporate Governance im Allgemeinen und die Internationale Rechnungslegung. Die ACNews erscheint zweimal im Jahr.

kpmg.at/publikationen

Impressum

Cyber Security in Österreich

Herausgeber:
KPMG Austria GmbH

Für den Inhalt verantwortlich:
Michael Schirmbrand
T +43 1 31332-3590
mschirmbrand@kpmg.at

Gert Weidinger
T +43 732 6938-2152
gweidinger@kpmg.at

Fachliche Studienleitung:
Robert Lamprecht
T +43 1 31332-3409
rlamprecht@kpmg.at

Koordination:
Iris Bauer
T +43 1 31332-3175
irisbauer@kpmg.at

Grafik und Satz:
Mirjam Schweigkofler
T +43 1 31332-3586
mschweigkofler@kpmg.at

Druck:
Ferdinand Berger & Söhne GmbH

© 2016 KPMG Austria GmbH Wirtschaftsprüfungs- und Steuerberatungsgesellschaft, österreichisches Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Printed in Austria.

KPMG und das KPMG-Logo sind eingetragene Markenzeichen von KPMG International. Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs, oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte auf Grund dieser Informationen handeln, ohne geeigneten fachlichen Rat eingeholt zu haben. Die in dieser Zeitschrift vorhandenen personenbezogenen Bezeichnungen sind aufgrund der besseren Lesbarkeit und Verständlichkeit des Textes zumeist in der männlichen Form angegeben, beziehen sich aber selbstverständlich geschlechtsneutral sowohl auf die weibliche als auch auf die männliche Form. Wir danken für Ihr Verständnis.