Cyber Security in Österreich

Studie
IT Advisory

Mai 2019

Strategien österreichischer Unternehmen im Kampf gegen Cyberkriminalität

Sicherheitsforum
Digitale Wirtschaft
Österreich

kpmg.at/cyber

Cyber Security ist die Grundlage für eine erfolgreiche Digitalisierung

Michael Schirmbrand
KPMG Partner

Andreas Tomek
KPMG Partner

Gert Weidinger
KPMG Partner

Das Meer birgt viele Gefahren für seine Bewohner: An jeder Ecke lauern angriffslustige Meerestiere. Doch Widerstand ist nicht zwecklos. Die auf den ersten Blick schwächeren Meeresbewohner haben ausgeklügelte Taktiken entwickelt, um sich zur Wehr zu setzen – durch gemeinsame Angriffe in Schwärmen, voluminöse Abschreckmethoden oder geschickte Ablenkungsmanöver.

Auf- statt Untertauchen

Auch die österreichischen Unternehmen beweisen einen langen Atem und leisten Widerstand gegen die Bedrohungen aus den Tiefen des Cyberraums – durch umfassende Strategien, Pläne für den Notfall und konzeptionelle Zusammenarbeit. Denn auch wenn die Zahl der Angreifer weiter zunimmt und die Methoden der Cyberkriminellen immer ausgeklügelter werden, zeigt sich: Österreichs Unternehmen tauchen in Sachen Cyber Security endlich an die Oberfläche.

Die Wichtigkeit des Themas ist unumstritten und Maßnahmen sowie Konzepte sind auf dem richtigen Weg. Dennoch halten viele Unternehmen noch die Luft an, wenn es darum geht, Attacken offen zu kommunizieren. Dabei würde genau das wesentlich zur Bewusstseinsbildung aller Beteiligter beitragen.

Reden statt Schweigen

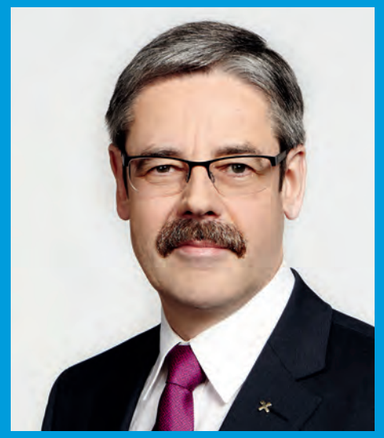
Bereits zum vierten Mal veröffentlicht KPMG die Studie „Cyber Security in Österreich“. Unsere Studie bietet in diesem Jahr nicht nur aktuelles Zahlenmaterial unserer Umfrage, an der sich mehr als 340 österreichische Unternehmen beteiligt haben. Gleichzeitig zeigen wir die wichtigsten Trends, die sich aus dem Vergleich der Jahre 2016 bis 2019 ergeben, und liefern Tipps für die Praxis.

Unsere Devise ist: Über Cybersicherheit müssen wir offen und ehrlich sprechen. Deshalb haben wir uns mit Cyberexperten der öffentlichen Verwaltung und von Aufsichtsbehörden an einen Tisch gesetzt und über ihre Einschätzung der Lage gesprochen. Darüber hinaus standen uns erneut zahlreiche Vertreter heimischer Unternehmen Rede und Antwort und teilten mit uns ihre Bedenken und Wünsche.

Österreichs Unternehmen sind 2019 besser vorbereitet, als noch vor vier Jahren. Die Rahmenbedingungen stellen Unternehmen vor immer neue Herausforderungen – unter anderem aufgrund der rasanten technologischen Entwicklung. Deshalb gilt es, Cyber Security von Beginn an in allen Projekten als elementaren Bestandteil miteinzubeziehen.

Oder anders gesagt: Unternehmen müssen sich so aufstellen, dass Cybersicherheit und Digitalisierungsinitiativen stets miteinander gedacht werden – nur so kann ein stabiles Wachstum gelingen.

Wir wünschen Ihnen viele Aha-Momente und neue Erkenntnisse beim Lesen unserer Studie. Sollten Fragen offen bleiben, gehen Sie bitte nicht auf Tauchstation. Wir freuen uns von Ihnen zu hören.



Sehr geehrte Damen und Herren,

bereits zum vierten Mal hat KPMG eine Cyber Security-Studie erstellt – das Ergebnis halten Sie in Ihren Händen. Als Präsident des Kuratorium Sicheres Österreich (KSÖ) ist es mir eine besondere Freude, dass wir die Studienerstellung in diesem Jahr mit dem „KSÖ Sicherheitsforum Digitale Wirtschaft Österreich" noch intensiver als in den Jahren zuvor mit unserer Expertise unterstützen konnten.

KPMG und das KSÖ verbindet ein gemeinsames Ziel: Ihre Aufmerksamkeit auf die aktuelle Cyber Security-Lage zu lenken und damit zu bewirken, dass die richtigen Maßnahmen zum Schutz der Bevölkerung, der Wirtschaft und der Behörden rechtzeitig eingeleitet werden, damit Cyberrisiken nicht zu Cybervorfällen werden.

Obwohl bereits ein messbares Umdenken stattgefunden hat und die Themen Cyber Security, IT-Sicherheit oder digitale Sicherheit immer öfter auf der Aufsichtsrats-, Vorstands- oder generell der Führungsebene diskutiert werden, ist der richtige Zugang zu dem Thema oft noch nicht gefunden.

Als Führungskräfte haben wir die Aufgabe, notwendige von übertriebenen Maßnahmen zu unterscheiden. Wir müssen Ressourcen so einsetzen, dass sowohl Wachstum als auch Schutz vor Gefahren abgedeckt werden, Organisationsaufgaben müssen dabei aber weiterhin erfüllt werden können.

Genau hier setzt die Cyber Security-Studie an. Denn das Wissen um die Bedrohungen ist genauso wichtig wie das Lernen von den Erfahrungen anderer. In der Ihnen vorliegenden Studie finden Sie sowohl Antworten auf die Fragen, wie andere Organisationen die Verantwortung für das Thema geregelt haben oder wie kritisch das Thema Fachkräftemangel inzwischen geworden ist. Sie finden aber auch Informationen von Experten und Beispiele für gelungene Kooperationen zwischen Wirtschaft und Behörden, die Ihnen als Anleitung für Ihre eigenen Maßnahmen dienen können.

Genau diese Kooperationen zwischen Akteuren, das voneinander Lernen und das miteinander Reduzieren von Gefahren ist es, was das „KSÖ Sicherheitsforum Digitale Wirtschaft Österreich", an dem auch KPMG als wesentlicher Partner teilnimmt, ausmacht. Es ist auszuschließen, dass jeder von uns für sich alleine die Sicherheitsherausforderungen, die mit dem Internet of Things, Industrie 4.0, Artificial Intelligence, 5G und vielen weiteren Themen, die auf uns zukommen, bewältigen kann. Nutzen Sie deshalb die Ergebnisse dieser Studie, um sich zu informieren. Entdecken Sie, wie es andere machen, wo Sie aufholen müssen und wo Sie bereits besser sind und anderen helfen können.

Ich wünsche Ihnen eine spannende Lektüre!

Erwin Hameseder
Präsident des Kuratorium Sicheres Österreich (KSÖ)

Inhalt

Zeit zum Auftauchen

Cybersicherheit an die Oberfläche bringen
Cyberkriminalität steht in Österreich nach wie vor auf der Tagesordnung: Zwei von drei heimische Unternehmen (66 Prozent) waren in den letzten zwölf Monaten von einer Cyberattacke betroffen. Schätzungen über zukünftige Schadenssummen und Höhe des Datendiebstahls klaffen weit auseinander, eine Erkenntnis teilen sie jedoch alle: Cyber Security gewinnt für die Wirtschaft und unsere Zivilgesellschaft immer mehr an Bedeutung.

Aktuelle Zahlen über den Status quo sind entscheidend, um einen Gesamtüberblick für ein Lagebild in Sachen Cyberangriffe und -sicherheit zu erhalten. Darum hat KPMG in Österreich bereits zum vierten Mal die vorliegende Umfrage durchgeführt. Die Ergebnisse verraten Trends und Veränderungen, machen deutlich, wo es Nachholbedarf gibt und in welchen Bereichen die heimischen Unternehmen bereits gut aufgestellt sind.

Von Cyber Security zu Cyber Resilience
Der detaillierte Blick auf Österreich zeigt: Cyber Security alleine reicht nicht mehr aus. Durch technologische und organisatorische Lösungen, die den „Faktor Mensch" gleichermaßen berücksichtigen, lassen sich zwar viele Angriffe abwehren. Doch die Palette der Angriffsmethoden ist zu groß, um sich gegen alle abzusichern.

Daher muss es das erklärte Ziel der Unternehmen sein, durch und durch widerstandsfähiger gegen Cyberattacken zu werden. Sie müssen sich zum einen vor Angriffen schützen, zum anderen auch betriebs- und funktionsfähig bleiben, um auch weiterhin ihre Geschäftsziele zu erreichen. Unternehmen brauchen daher genau jene Fähigkeit der Cyber Resilience: trotz widriger Umstände kontinuierlich ihre Leistung zu liefern. Cyber Resilience geht weit über reine Cyber Security hinaus und verfolgt einen umfassenden Ansatz zum Schutz der Organisation vor Cyberangriffen und zur Sicherstellung der Geschäftsprozesse nach erfolgten Angriffen. Das Thema Cyber Resilience muss zukünftig im Mittelpunkt jeder nachhaltigen Wachstumsstrategie eines Unternehmens stehen – vor allem aufgrund der Digitalisierung. Denn nur eine entsprechende Widerstandsfähigkeit gegen Gefahren aus dem Cyberraum kann zu Zuversicht und Vertrauen bei Kunden und Stakeholdern führen – der Schlüssel zum Unternehmenserfolg, speziell in der digitalen Welt.

Das Third Party-Risiko als verkannte Gefahr
In einem wirtschaftlichen Umfeld, das gerne als „hyper connected" bezeichnet wird, hängt die eigene Sicherheit stark von anderen ab, etwa vom Sicherheitsniveau der Zuliefererunternehmen. Geschäftspartner, Technologie-Provider, Outsourcing-Partner und andere – die Bedrohung aus dem Cyberraum kennt keine Grenzen. Mehr und mehr Risiken können nicht mehr direkt von den Unternehmen kontrolliert werden. Sie werden somit anfälliger für Angriffe.

Unternehmen müssen daher über die Cybersicherheit dieser Drittparteien Bescheid wissen und informiert darüber sein, welche Auswirkungen ein Angriff auf den eigenen Betrieb haben könnte. In der immer komplexer werdenden Wertschöpfungskette zählt jedes Glied – es reicht der Angriff auf das schwächste, um das gesamte System aus dem Gleichgewicht zu bringen.

Unsere Studie spiegelt eine Erkenntnis wider, die sich auch in unseren Nachbarländern zeigt: Mit dem Third Party-Risiko gehen Österreichs Unternehmen grob fahrlässig um. Das Fehlen eines systematischen Ansatzes zur Bewertung und Minderung des Third Party-Risikos kann jedoch gravierende Auswirkungen haben. Auch in Hinblick auf Merger & Acquisitions müssen Unternehmen nachrüsten, da hier das Third Party-Risiko ebenfalls schlagend werden kann. Die Lösung heißt Cyber Due Diligence und sollte zukünftig bei allen Übernahmen und Investitionen zum Standard werden, um Cyberrisiken rechtzeitig zu identifizieren.

Das NIS-Gesetz: Kritische Infrastruktur im Fokus
Immer noch schweigen viele Unternehmen, wenn sie angegriffen werden: Nur jedes dritte Unternehmen (33 Prozent) informierte öffentliche Stellen über einen Sicherheitsvorfall. Im Vorjahr waren es noch 40 Prozent der Unternehmen. Nur die großen Unternehmen handeln hier vorbildhaft: Fast die Hälfte (46 Prozent) wandte sich in den vergangenen zwölf Monaten an eine Behörde. Zu dieser Sensibilisierung bei großen Unternehmen hat wohl auch das Netz- und Informationssystemsicherheitsgesetz (NISG) beigetragen, welches Mitte Dezember 2018 vom Nationalrat beschlossen wurde, sowie die Datenschutzgrundverordnung (DSGVO) und entsprechende Regulatorien für die Finanzwirtschaft.

Das NISG verpflichtet Unternehmen zur Einrichtung umfangreicher Sicherheitsmaßnahmen und zum Nachweis von deren Wirksamkeit. Das heikle Thema „Kritische Infrastruktur"rückt dadurch in Österreich verstärkt ins Rampenlicht: Staatliche Stellen sowie Aufsicht und Regulatoren lassen der Materie eine ganz besondere Wichtigkeit zukommen. Bei Nichteinhaltung der Anforderungen aus dem NISG drohen Strafen und ein Reputationsverlust. Im Fokus der NIS-Richtlinie stehen die sogenannten „Betreiber wesentlicher Dienste". Doch der „frische Wind" durch das Gesetz ist österreichweit zu spüren: Das Thema Cybersicherheit wurde erneut aufgewertet. Eine positive Entwicklung, immerhin führt das NISG zu mehr Stabilität in Unternehmen und stärkt somit in weiterer Folge die gesamte heimische Wirtschaft.

Nur nicht treiben lassen
Die Ergebnisse unserer Studie zeigen, dass die österreichischen Unternehmen in Sachen Cybersicherheit immer weiter auftauchen. Dennoch dürfen sie sich nicht entspannt zurücklehnen. Denn einerseits fehlt es oft noch an den Basisstrukturen – Stichwort: CIAM (Customer Identity Access Management) – andererseits kommen die neuen Herausforderungen mit einer noch nie da gewesenen Geschwindigkeit – Stichwort: Künstliche Intelligenz. Die Digitalisierung schlägt hohe Wellen und fordert neues Denken, neues Handeln und neue Strategien von Österreichs Unternehmen.

Robert Lamprecht
KPMG Director

Key Findings

Biss mit Folgen

66%
der Unternehmen waren in den letzten 12 Monaten Opfer einer Cyberattacke

41%
erlitten aufgrund eines Cyberangriffs finanziellen Schaden

33%
informierten öffentliche Stellen über Sicherheitsvorfälle

Gemeinsam Zähne zeigen

7%
glauben, dass ihre Lieferanten ausreichende Sicherheitsmaßnahmen treffen

60%
sehen in der Einführung von Branchen-CERTs einen Mehrwert

73%
wünschen sich eine eindeutig definierte Anlaufstelle für Cyber Security

Volle Kraft voraus

65%
empfinden den Fachkräftemangel als Herausforderung

54%
haben einen Überblick über ihre IoT-Geräte

53%
sagen, dass Outsourcing die Sichtbarkeit und Kontrolle von Cyber Security verbessert

Widerstand leisten

19%
verfügen über eine Cyber-versicherung

53%
sind mit dem Angebot an Cyberversicherungen nicht zufrieden

68%
fühlen sich mit Incident Response-Plänen auf Angriffe gut vorbereitet

53%
betrachten Cyber Security nicht als fixen Bestandteil von Digitalisierungs-initiativen

64%
verfügen über eine mündliche (21 %) oder schriftliche (43 %) Berichterstattung

42%
verfügen über ein dezidiertes Cyber Security-Team

Quallen haben lange Tentakel mit Nesselzellen, die sie zum Fang von Beutetieren und zur Verteidigung benutzen.

Biss mit Folgen

Cyber Security im Jahresrückblick

66%

der Unternehmen waren in den letzten 12 Monaten Opfer einer Cyberattacke

56%

sind davon überzeugt, den Angriff innerhalb von 48 Stunden erkannt zu haben

47%

der Cyberattacken waren Phishing – gleiches gilt für Malware

41%

erlitten aufgrund eines Cyberangriffs finanziellen Schaden

33%

informierten öffentliche Stellen über Sicherheitsvorfälle

Haie beißen bei einem Angriff oft nur einmal zu und warten, bis ihr Opfer genügend Blut verloren hat, um es dann in geschwächtem Zustand erneut anzugreifen.

Cyberattacken sind in Österreich zum Daily Business geworden und stellen seit mehreren Jahren eines der größten Geschäftsrisiken für Unternehmen dar. Doch egal welche Maßnahmen die Unternehmen setzen: Einen 100%igen Schutz vor Cyberkriminellen gibt es nicht. Hacker suchen nach immer kreativeren und ausgeklügelteren Wegen, um Systeme anzugreifen und daraus Profit zu lukrieren. Daher müssen Unternehmen nicht nur in die Prävention und Abwehr von Angriffen investieren, sondern auch in Strategien nach einem Vorfall.

Strategische Maßnahmen zur Cyber Security und die Schaffung einer entsprechenden Widerstandsfähigkeit (Cyber Resilience) sorgen dafür, dass Unternehmen in diesem rauen Umfeld die Oberhand behalten. Sie brauchen eine ganzheitliche Strategie zur Stärkung ihrer Widerstandskraft gegen Angriffe auf die Informationssicherheit. Denn: Ein solider Schutz gegen Cyberangriffe wird immer mehr zur Voraussetzung, damit Unternehmen in der daten- und technologiebasierten Wirtschaft Erfolg haben können. Cyber Security soll und muss deshalb ein unabdingbarer Bestandteil jeder nachhaltigen unternehmerischen Wachstumsstrategie sein. Das stellt eine tägliche Herausforderung für die Führungskräfte dar: Der Bereich der Cybersicherheit wandelt sich aufgrund neuer Technologien, Möglichkeiten und Herausforderungen laufend.

Die harten Fakten: Angriffe auf Unternehmen

Cyberangriffe finden 365 Tage im Jahr und 24 Stunden am Tag statt. Auch hier halten die Automatisierung und zunehmende Professionalisierung mittels künstlicher Intelligenz Einzug: 2 von 3 österreichischen Unternehmen (66 Prozent) waren in den letzten zwölf Monaten Opfer einer Cyberattacke. Das sind fünf Prozent mehr als im Vergleich zur Vorjahresstudie (61 Prozent), 2016 war lediglich jedes zweite Unternehmen (49 Prozent) betroffen. Dies bedeutet einerseits einen Anstieg der Angriffe seit der ersten Cyber Security-Studie von KPMG in Österreich, zeigt aber auch, dass Unternehmen gelernt haben, die Ereignisse besser zu klassifizieren und zuzuordnen. Oder anders gesagt: Österreichische Unternehmen erliegen keiner „Schockstarre", was aber noch kein Grund sein darf sich zurückzulehnen. Denn von den Attacken aus dem Cyberraum sind österreichische Unternehmen jeder Größenordnung betroffen. Im Visier der Angreifer standen im letzten Jahr 59 Prozent der kleineren, 71 Prozent der mittleren und 76 Prozent der großen Unternehmen. In zahlreichen Unternehmen herrscht nach wie vor eine gewisse Unwissenheit darüber, ob die eigenen Systeme angegriffen wurden. So ist noch immer jedem zehnten Unternehmen (10 Prozent) hierzulande nicht bekannt, ob es von Attacken betroffen war oder nicht. Eine Zahl, die in den letzten Jahren nahezu unverändert geblieben ist. Besonders hoch ist die Unklarheit bei großen Unternehmen mit 23 Prozent. Diese verhältnismäßig hohe Zahl hat unterschiedliche Ursachen: Einerseits sorgen die komplexen und gewachsenen IT-Systeme mit ihren zahlreichen Benutzern oft dafür, leicht den Überblick zu verlieren. Andererseits erschwert die aktuelle Dynamik der Digitalisierung es großen Unternehmen besonders, Altlasten in den IT-Strukturen zu bereinigen.

Der unsichtbare Feind: Die Angriffsarten

Phishing und Malware sind und bleiben die häufigsten Angriffsarten aus der virtuellen Welt. Knapp die Hälfte der befragten Unternehmen (jeweils 47 Prozent) kamen mit diesen Attacken in Berührung. Hier lässt sich ein klarer Anstieg zum Vorjahr erkennen: 2018 waren 22 Prozent der Unternehmen von Malware und 24 Prozent von Phishing betroffen. In beiden Kategorien machen sich die Angreifer die Gutgläubigkeit und Neugierde von Mitarbeitern zunutze. Unreflektiertes Handeln öffnet Cyberkriminellen nach wie vor Tür und Tor: Die Dynamik des Alltages erleichtert den Cyberkriminellen ihr Vorhaben. Die Abgelenktheit durch die zahlreichen Einflüsse der Arbeitsumgebung sowie der Irrglaube, multitaskingfähig zu sein, verleitet oft zu Fehlentscheidungen, die den Cyberkriminellen einen erfolgreichen Eintritt ins Unternehmen ermöglichen. Bewusstseinsbildung muss daher in Unternehmen weiterhin einen hohen Stellenwert einnehmen.

Ein Trend, der sich in der Praxis abzeichnet: Kompromittierte E-Mail-Konten und der Identitätsdiebstahl entwickeln sich zur meistverwendeten Taktik für erfolgreiche Phishingattacken. Derartige E-Mail-Konten werden vermehrt verwendet, um Phishing E-Mails an zusätzliche Benutzer im Unternehmen zu senden. Als besonders effektiv erweist sich die Methode in M&A-Situationen, da Mitarbeiter eine zusätzliche Kommunikation zwischen den Unternehmen erwarten. Der Vorteil für Cyberkriminelle: Phishing E-Mails, die innerhalb eines Unternehmens gesendet werden, umgehen eher eine Prüfung durch E-Mail Gateways. Aus Sicht der Cyberkriminellen ebenfalls sehr erfolgreich waren Angriffe auf Websites oder Website-Applikationen sowie die Verwendung von Cryptolocker mit jeweils 29 Prozent. Bei dieser Angriffsmethode zeigt sich allerdings eine rückläufige Tendenz. Der Grund: Die Lukrativität der Lösegeldforderungen ist aufgrund der aktuellen Kursentwicklung der Kryptowährungen für Angreifer nicht besonders vielversprechend. Besonders selten waren in den letzten zwölf Monaten Advanced Persistent Threats (APTs), die Ausnutzung von Hardware-Lücken (Spektre/Meltdown) sowie Angriffe auf Zulieferer- und Kundensysteme (jeweils nur rund zwei Prozent) – oder zumindest wurden sie als solche nicht identifiziert. Besonders im Bereich der APTs ist jedoch Vorsicht geboten: Das Erkennen von zielgerichteten und fortgeschrittenen Angriffen stellt Unternehmen vor enorme Herausforderungen. Insbesondere dann, wenn die eigentlichen Ziele Wirtschaftsspionage, Produktpiraterie und Know-how Diebstahl sind.

Die 3 wichtigsten Trends 2016 – 2019

- **Phising und Malware bzw Ransomware bleiben seit Jahren die Top-Angriffsarten.**
- **Immer weniger Unternehmen wenden sich nach einem Vorfall an die zuständige Behörde.**
- **Unternehmen sind immer öfter in der Lage, Cyberangriffe erfolgreich abzuwehren.**

Praxistipp

Bewusstseinsbildung ist einer der wichtigsten Bestandteile einer Sicherheitskultur und -strategie. Oft beschäftigen sich Unternehmen detailverliebt mit technischen Tools, vergessen aber auf den Faktor Mensch. Bewusstseinsbildung darf dabei keine einmalige Aktivität sein, sondern ein ständig stattfindender, gezielter und positiver Kommunikationsprozess.

Zeit ist Geld: Dem Täter auf der Spur

Am ehesten wurden Unternehmen in den letzten zwölf Monaten durch interne Sicherheitssysteme wie etwa Firewalls, IPS (Intrusion Prevention Systeme) oder SIEM (Security Information and Event Management) auf Angriffe aufmerksam (86 Prozent). Die entscheidenden Hinweise erfolgten in 65 Prozent der Fälle durch aufmerksame Mitarbeiter. In seltenen Fällen kam die wichtige Information von externen Zulieferern (zwei Prozent), Medien (vier Prozent) oder Behörden (drei Prozent). Eine schnelle Reaktion auf Cyberattacken ist entscheidend, um größere Schäden zu verhindern. Mehr als die Hälfte (56 Prozent) der Unternehmen gab an, dass sie den Angriff innerhalb von 48 Stunden erkennen konnten. Sechs Prozent der Befragten benötigten dafür laut

„Cyber Security wird zur permanenten Aufgabe des Staates werden."

GenMjr Mag. Rudolf Striedinger
Bundesministerium für Landesverteidigung (BMLV)

eigenen Angaben länger als eine Woche. Die Anzahl der Unternehmen, die den Zeitpunkt des Angriffes nicht bestimmen und somit keine Aussage über die Zeitdauer machen konnte, ist mit 28 Prozent verhältnismäßig hoch. Überdurchschnittlich gut schneiden hier große Unternehmen ab: 69 Prozent sind überzeugt, den Angriff innerhalb von 48 Stunden erkannt zu haben. Doch Experten vermuten, dass ein Cyberkrimineller zwischen 80 und 150 Tagen unerkannt im Unternehmen agieren kann.

Die vorliegende Umfrage zeichnet ein viel positiveres Bild für Österreich. Dies kann daran liegen, dass Unternehmen hierzulande Angreifer zu spät erkennen und den Zeitpunkt des Eindringens daher falsch bestimmen. Eine Falschinterpretation kann auch daher rühren, dass Unternehmen Commodity-Angriffe als Vorläufer oft nicht erkennen und erst die stark disruptiven Angriffe als Attacke klassifizieren. Fakt ist: Österreichs Unternehmen dürfen sich hier in keinster Weise in falscher Sicherheit wiegen.

Genau gerechnet: Der Schaden durch Angriffe

Die guten Neuigkeiten zuerst: Unternehmen sind immer öfter dazu in der Lage, mit Angriffen aus der virtuellen Welt umzugehen und Cyberangriffe erfolgreich abzuwehren. 59 Prozent der Unternehmen, die in den letzten zwölf Monaten Opfer einer Cyberattacke waren, entstand durch den Vorfall kein Schaden. Im Vorjahr gaben hingegen nur sechs Prozent der befragten Unternehmen an, in der Abwehr erfolgreich gewesen zu sein. Diese signifikante Zunahme gegenüber dem Vorjahr ist hauptsächlich dem Umstand geschuldet, dass Cyber Security endlich den Weg vom Fokusthema der IT-Spezialisten hin zum Risk Management-Thema der Geschäftsführung geschafft hat und entsprechende Maßnahmen Wirkung zeigen. Entscheidend ist hier auch die Einrichtung von entsprechenden Abläufen zur Vorfallsbehandlung. Denn nur mit einer grundlegenden Reaktions- und Handlungsfähigkeit sind Unternehmen in der Lage, den Angreifern Paroli zu bieten. Natürlich darf nicht angenommen werden, dass alle Angriffe vollumfänglich abgewehrt wurden und den Unternehmen kein Schaden entstanden ist. Die erfreuliche Professionalisierung des Themas in Österreichs Unternehmen sorgt jedoch für ein schwindendes Ohnmachtsgefühl und eine positive Grundstimmung.

Dennoch haben Cyberattacken enorme Konsequenzen für Wirtschaftstreibende im ganzen Land. Das Spektrum an Auswirkungen reicht dabei von finanziellen Schäden durch die Unterbrechung der Geschäftsprozesse bis hin zu geschäftsschädigendem Imageverlust. In den letzten zwölf Monaten sind bei rund 17 Prozent der Unternehmen Schäden von 1.000 bis 50.000 EUR entstanden und bei zehn Prozent mehr als 50.000 EUR. Anders sieht das bei großen Unternehmen aus. Hier waren die finanziellen Auswirkungen durch Cyberattacken stärker zu spüren: Bei 23 Prozent der befragten großen Unternehmen entstand ein Schaden zwischen 1.000 und 50.000 EUR, bei 38 Prozent war der Schaden höher als 50.000 EUR.

Die vermuteten Motive der Angreifer sind übrigens vielfältig: Zwei Drittel (67 Prozent) der befragten Unternehmen vermuten finanzielle Schadenszufügung als Motiv, 28 Prozent die Unterbrechung von Geschäftsprozessen, 23 Prozent eine geplante Beeinträchtigung der Reputation. Die Befürchtung einer absichtlichen finanziellen Schadenszufügung ist in den Bereichen Immobilien (83 Prozent), Energiewirtschaft (78 Prozent), Technologie (76 Prozent) und Industrie (95 Prozent) besonders hoch.

Der Tag danach: Reaktion auf Angriff

Die Auswirkungen von Cyberattacken lagen jahrelang im Dunkeln. Doch die Konsequenzen können mittlerweile von Unternehmen besser analysiert werden. Im Jahr 2017 war noch 36 Prozent der angegriffenen Unternehmen nicht klar war, welche konkreten Auswirkungen der Vorfall hatte. Diese Prozentzahl hat sich mittlerweile auf neun Prozent reduziert. Das bedeutet: Die meisten Unternehmen haben entsprechende Prozesse etabliert und Tools im Einsatz, um eine umfangreiche Schadensanalyse nach einem Angriff durchführen zu können.

Der Faktor „Zeit" spielt im Bereich Cybersicherheit eine entscheidende Rolle. Das ist den österreichischen Unternehmen bewusst: Der Großteil der Unternehmen (86 Prozent) hat nach Entdecken des Cyberangriffs umgehend mit der Analyse der technischen und organisatorischen Schwachstellen begonnen. Hier lässt sich eine eindeutig positive Entwicklung im Vergleich zum Vorjahr feststellen: 2018 reagierte nur ein Drittel (33 Prozent) der befragten Unternehmen mit einer sofortigen Analyse. Ein vergleichbarer Trend lässt sich auch in Bezug auf die forensische Untersuchung der Angriffe erkennen: Während 2018 nur 18 Prozent der Unternehmen interne und acht Prozent externe forensische Untersuchungen durchgeführt haben, waren es in diesem Jahr 46 Prozent (interne Untersuchungen) bzw 19 Prozent (externe Untersuchungen).

Ebenso eindeutig erkennbar ist folgende Tatsache: Alle Unternehmen (100 Prozent), die einen – wenn auch nur geringen – finanziellen Schaden durch einen Angriff erlitten haben, führen eine Analyse der technischen und organisatorischen Schwachstellen durch. Hingegen untersuchen nur 78 Prozent der Unternehmen, die Cyberattacken schadlos abwehren konnten, die Hintergründe des Angriffes. Große Unternehmen sind auf diesem Gebiet besonders engagiert: 100 Prozent analysieren die technischen und organisatorischen Schwachstellen und 71 Prozent setzen auf forensische Untersuchungen und/oder lassen durch externe Dienstleister Penetrationstests durchführen.

Hohe Dunkelziffer: Kein Vertrauen in Behörden

Eine fundierte Dokumentation von Cyberattacken ist sowohl für Unternehmen als auch die Allgemeinheit hilfreich. Dazu zählt auch das Melden des Vorfalles an Behörden. Nichtsdestotrotz prägt nach wie vor Verschwiegenheit das Bild: Immer weniger Unternehmen wenden sich nach einem Vorfall an die zuständige Behörde.

Nur ein Drittel der Unternehmen (33 Prozent) informierte öffentliche Stellen über Sicherheitsvorfälle, während im Vorjahr noch 40 Prozent der Unternehmen diesen Schritt setzten. Eine Ausnahme stellen hier große Unternehmen dar: Fast die Hälfte (46 Prozent) wendete sich in den vergangenen zwölf Monaten an eine Behörde. Zu dieser Sensibilisierung bei großen Unternehmen hat wohl auch das Netz- und Informationssystemsicherheitsgesetz (NISG) beigetragen, welches Mitte Dezember 2018 vom Nationalrat beschlossen wurde, sowie entsprechende Regulatorien für die Finanzwirtschaft.

Auffällig dabei: Nur ein Viertel der Unternehmen (22 Prozent), die einen Schaden durch einen Angriff verkraften mussten, meldete die Angriffe an die Polizei. Das Vertrauen in die Behörden in Bezug auf Cyberkriminalität ist nach wie vor nicht sehr hoch. Der Grund: Das Melden von Anomalien im Cyberraum ist eine große Vertrauensfrage. Jede Information darüber, dass man erfolgreich angegriffen wurde, kann, wenn sie öffentlich wird, imageschädigend sein. Darüber hinaus wünschen sich die betroffenen Unternehmen ein Mehr an Unterstützung von den Behörden. Hier entsteht das klassische Henne-Ei-Problem: Mit einem aktivieren Informationsfluss von Seiten der Unternehmen könnte ein klareres Lagebild in Sachen Cyberkriminalität für den Wirtschaftsstandort Österreich gezeichnet werden. Behörden könnten dadurch auch bessere Unterstützungsmöglichkeiten schaffen.

Cyber Security eröffnet neue Geschäftsmöglichkeiten für innovative Unternehmen in Österreich

Wie hat sich der Stellenwert von Cyber Security in der Industrie in den letzten Jahren geändert?
Cyber Security gewinnt in den letzten Jahren auch in der Industrie immer mehr an Bedeutung, da sie zu einem entscheidenden Wettbewerbsfaktor wird. Die Bedrohung für die österreichische Industrie ist real und richtet jährlich einen Millionenschaden an.

Insbesondere richten sich die Attacken gegen Unternehmen, deren Produkte und Dienstleistungen zu den innovativsten und qualitativ hochwertigsten zählen.

Dementsprechend wichtig ist es, den Industrie- und Wirtschaftsstandort Österreich stärker zu schützen. Dazu muss Österreich proaktiv agieren, sein Bewusstsein stärken, das vorhandene Potenzial schützen und die sich neu ergebenden Möglichkeiten aktiv für sich nutzen!

Wie sieht die Kommunikation und Kollaboration zwischen Unternehmen aus, auch im Hinblick auf Digitalisierung und Industrie 4.0?
Unsere Leitbetriebe sind Vorreiter auf dem Weg der Digitalisierung. Diese hohe Industrie 4.0-Readyness ist dabei nicht nur Grundvoraussetzung für die Leitbetriebe selbst, um auf den Weltmärkten bestehen zu können. Sie wird zum Ankerpunkt und Schrittmacher für ihre Kooperationspartner im digitalen Zeitalter.

800 bis 1.000 KMU sind mit jedem dieser Leitbetriebe verbunden. Somit können ganze Wertschöpfungsketten gesichert werden.

In diesem Kontext entstehen aber natürlich auch Gefahrenpotenziale, die ausgenützt werden können. Laut einer von uns mitbeauftragten Studie stammen fast die Hälfte aller Cyberangriffe von Mitbewerbern, knapp über zehn Prozent von Partnern entlang der Wertschöpfungskette. Je mehr Schnittstellen und Knotenpunkte entstehen, desto angreifbarer werden Unternehmen.

Wo sehen Sie die größten Handlungsfelder, um Cyber Security zu etablieren und weiter auszubauen?
Um die Cyber Security-Thematik effektiv zu adressieren, braucht man MINT-Fachkräfte. Diese haben eine strategische Bedeutung für die Industrie, deren Erfolgsgaranten seit vielen Jahren Forschung, Technologie und Innovation sind.

Daher benötigt die Industrie eine ausreichende Zahl von MINT-Qualifizierten. Die Rekrutierungssituation im MINT-Bereich war schon in den vergangenen Jahren sehr angespannt. Sie hat sich vor dem Hintergrund der positiven Konjunktur erneut zugespitzt. Knapp 60 Prozent der Unternehmen berichten im Bereich Technik & Produktion (inkl IT) von großen Rekrutierungsproblemen.

Ebenfalls wichtig wird sein, Österreich als einen führenden Technologiestandort zu etablieren. Die Industrie muss in Zukunft wettbewerbsfähig bleiben, um auf aktuelle Herausforderungen reagieren zu können und Zukunftsthemen in Österreich, beispielsweise Cyber Security, voranzutreiben. Dazu ist die öffentliche Hand gefordert, innovationsfördernde Rahmenbedingungen zu schaffen und F&E und Innovation zu stärken.

Welche Potenziale und neue Möglichkeiten ergeben sich durch Cyber Security?
Cyber Security eröffnet neue Geschäftsmöglichkeiten für innovative Unternehmen in Österreich. Die weltweiten Ausgaben für IT-Sicherheit betrugen im Jahr 2018 100 Milliarden Euro und sind im Vergleich zum vorherigen Jahr im zweistelligen Prozentbereich gestiegen. Das ergibt eine große Chance, die genutzt werden muss.

Wenn wir die Innovationen der Zukunft betrachten – von selbstfahrenden Autos über Heimautomatisierung – ist eine digital vernetzte Wirtschaft essenziell.

Diese Herausforderungen müssen nicht nur von den Unternehmen, sondern gemeinsam mit der öffentlichen Hand gelöst werden.

Wenn ein Unternehmen seine IT Security-Strategie ausweiten möchte, was empfehlen Sie den Führungskräften als nächste Schritte?
Ein wichtiger Punkt wird die Errichtung einer vertrauensvollen Kommunikations- und Austauschkultur zwischen Unternehmen und Behörden sein. Nur durch den gegenseitigen Austausch können Best Practice-Beispiele und mögliche Gefahrenstellen einander aufgezeigt werden.

Das Bewusstsein über Industriespionage muss nicht nur in Unternehmen, sondern vor allem auch in den zuständigen Behörden geschärft werden. Proaktive Weiterbildung muss nicht nur im Sinne der Prävention, sondern auch der Rechtslage und Nachverfolgung stattfinden.

Dafür ist eine enge und stetige Kooperation und Kommunikation zwischen Behörden und Betroffenen notwendig, die jedoch auf vertraulicher Basis stattfinden muss, um den Betroffenen die Bedenken in Bezug auf Reputationsverlust zu nehmen.

Ing. Mag. Peter Koren

Vize-Generalsekretär
der Industriellenvereinigung

Round Table

Die digitale Welt sicher machen

Der Cyberraum gewinnt für die öffentliche Verwaltung immer mehr an Bedeutung: Es gilt, Rahmenbedingungen für Unternehmen und Privatpersonen zu schaffen, um Menschen und Staat zu schützen. Dabei sind sowohl das Bundeskanzleramt (BKA), das Bundesministerium für Inneres (BMI) sowie das Bundesministerium für Landesverteidigung (BMLV) gleichermaßen gefragt. KPMG lud Experten aus den drei Behörden zu einer Diskussionsrunde.

Die Expertenrunde (v.l.n.r.):
Robert Lamprecht (KPMG), GenMjr Mag. Rudolf Striedinger (Bundesministerium für Landesverteidigung, BMLV), DI Philipp Blauensteiner (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, BVT), Erich Albrechtowitz (Bundeskanzleramt), Wolfgang Rosenkranz (KSÖ) und Andreas Tomek (KPMG)

Wolfgang Rosenkranz (KSÖ): Drei Behörden, ein Thema: Welche Aufgabe hat jedes Ihrer Ressorts in Hinblick auf Cyber Security?

Erich Albrechtowitz (BKA): Das Bundeskanzleramt hat die Aufgabe der gesamtstaatlichen Koordination, wozu ua auch die Schaffung von Cyber Security-Rahmenbedingungen zählt. Von uns kommen die Eckpfeiler und die Strategie. Die Umsetzung der operativen Aufgaben erfolgt weitgehend über die jeweiligen Ressorts. Ebenso unsere Aufgabe: Die internationale Koordination des Themas – Stichwort: europäische Rechtsprechung – sowie die Umsetzung des NIS-Gesetzes.

Rudolf Striedinger (Abwehramt/BMLV): In das Aufgabengebiet des Abwehramtes/BMLV fällt der Bereich der nationalen Cyber Defence. Dazu zählen alle Sicherheitsmaßnahmen der Informations- und Kommunikationstechnologie sowie die Abwehr von souveränitätsgefährdenden Cyberangriffen auf die Republik. Mit unseren Informationen tragen wir außerdem entscheidend dazu bei, ein möglichst realistisches Bild der Cyberlage des Landes zu zeichnen. Ebenso relevant: Unter dem Titel „Industrielle Sicherheit" beraten und zertifizieren wir als beauftragte Sicherheitsbehörde hinsichtlich militärischer Angelegenheiten österreichische Unternehmen, die an internationalen Aufträgen mit klassifizierten Informationen teilnehmen.

Philipp Blauensteiner (BVT/BMI): Die Cyber Security-Verantwortung des BMI ergibt sich aus der Bundesverfassung, die das Innenministerium als oberste Sicherheitsbehörde der Republik festlegt. Das BVT, das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, ist organisationsrechtlich in das BMI eingegliedert.

Das BMI hat auch die Aufgabe, die kritische Infrastruktur des Landes zu schützen, mit dem NIS-Gesetz wurde die operative NIS-Behörde im Innenministerium angesiedelt. Wir sind somit die Meldesammelstelle für alle Pflicht- aber auch für freiwillige Meldungen.

Wolfgang Rosenkranz (KSÖ): In welchem Ausmaß können Ihre Ministerien in Unternehmen eingreifen – Stichwort: NIS-Gesetz?

Rudolf Striedinger (Abwehramt/BMLV): Das NIS-Gesetz hat diesbezüglich keine Auswirkungen auf uns, da wir keinen Behörden-Status haben. Sollten wir einen Anlassfall orten, theoretisch in Richtung Wirtschaft aktiv werden zu müssen, dann geht dies nur im Wege der Assistenzleistung auf Anforderung des zuständigen Innenministeriums.

Philipp Blauensteiner (BVT/BMI): Das NIS-Gesetz verpflichtet Unternehmen zur Einhaltung von Mindestsicherheitsvorgaben. Das bedeutet, dass die Einhaltung auch überprüft werden muss und bei einem Verstoß die üblichen Schritte erfolgen. Natürlich gilt: Zuerst aufmerksam machen und beraten. Doch es besteht auch die Möglichkeit, Strafsanktionen zu setzen.

Erich Albrechtowitz (BKA): Das Bundeskanzleramt identifiziert grundsätzlich die Betreiber wesentlicher Dienste. Die Sicherheitsvorkehrungen werden in Form eines Bescheides vorgeschrieben und können dadurch auch einer staatlichen Überprüfung unterzogen werden.

Wolfgang Rosenkranz (KSÖ): Inwiefern gibt es Kooperationen mit der Wirtschaft in Hinblick auf Cybersicherheit?

Philipp Blauensteiner (BVT/BMI): Im BVT bieten wir Betreibern kritischer Infrastruktur unsere Services proaktiv an. Statistisch betrachtet sind wir etwa einmal wöchentlich als Berater bei einem Betreiber einer kritischen Infrastruktur.

Im Entstehungsprozess zum NIS-Gesetz haben wir alle gesehen, dass die Zusammenarbeit zwischen Staat und Wirtschaft gut funktioniert.

Rudolf Striedinger (Abwehramt/BMLV): Einerseits gibt es eine Zusammenarbeit mit Unternehmen, wenn sie eine Facility Security Clearance benötigen.

Anderseits beraten wir Unternehmen in Hinblick auf allgemeine Sicherheitsthemen, so auch Cyber Security. Unser Wissen ist etwa im Bereich des Objektschutzes stark gefragt, um ein Beispiel zu nennen.

Erich Albrechtowitz (BKA): Cybersicherheit ist eine gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft. Wir veranstalten daher Round Tables mit Unternehmen, um uns auf partnerschaftlicher Ebene abzustimmen.

Andererseits haben wird die Cyber Security-Plattform, um einen kontinuierlichen Austausch zwischen Vertretern von Wirtschaft und Staat zu ermöglichen.

Robert Lamprecht
KPMG

Wolfgang Rosenkranz
Kuratorium Sicheres Österreich (KSÖ)

DI Philipp Blauensteiner
Leiter des Cyber Security Centers,
Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung (BVT)

GenMjr Mag. Rudolf Striedinger
Leiter Abwehramt,
Bundesministerium für
Landesverteidigung (BMLV)

Erich Albrechtowitz
Gruppenleiter der Gruppe I/B:
IT-Personalmanagement,
IKT-Sicherheit, IKT-Infrastruktur,
Bundeskanzleramt

Andreas Tomek
KPMG

Wolfgang Rosenkranz (KSÖ): Warum fällt es Unternehmen nach wie vor schwer, Cybervorfälle an Behörden zu melden?

Robert Lamprecht (KPMG): An dieser Stelle ein kurzer Input aus unserer Umfrage: Die Praxis zeigt, dass große Verschwiegenheit das Bild prägt. Nur jedes dritte Unternehmen informiert öffentliche Stellen über einen Sicherheitsvorfall, während im Vorjahr noch 40 Prozent diesen Schritt setzten. Es fehlt zum Teil an entsprechenden Strukturen für KMU, um ein Melden unkompliziert zu ermöglichen.

Erich Albrechtowitz (BKA): Staatliche Einrichtungen werden eher mit „behördlicher Verfolgung" als mit „Aufklärung und Bewusstseinsbildung" in Verbindung gebracht – das behindert den Informationsfluss. Das wesentliche Zauberwort in diesem Zusammenhang ist „Vertrauen". Behörden müssen ihre digitale Kompetenz besser nach außen kommunizieren. Gleichzeitig bauen wir sukzessive Strukturen auf, um den Informationsaustausch zu fördern, etwa durch die Gründung von CERTs sowie der Digitalisierungsagentur.

Philipp Blauensteiner (BVT/BMI): Unternehmen müssen einen Vorteil daraus haben, dass sie einen Vorfall melden. Etwa als Voraussetzung für eine Versicherungsleistung. Oder aber durch einen Mehrwert an Informationen: Die Meldungen müssen als gut aufbereitete Information der Wirtschaft wieder zur Verfügung gestellt werden. Hier sind wir auf einem guten Weg.

Wolfgang Rosenkranz (KSÖ): Aus staatlicher Sicht betrachtet: Wie sieht die Cyberbedrohung Österreichs aus?

Rudolf Striedinger (Abwehramt/BMLV): Man muss grundsätzlich zwischen Cyberkriminalität und Cyberterrorismus unterscheiden. Ersteres trifft früher oder später in irgendeiner Form jedes Unternehmen und viele Privatpersonen. Hier sind wir längst keine Insel der Seligen mehr. Cyberterrorismus wiederum zielt auf die staatliche Versorgung ab und findet aktuell in Österreich auf einem Niveau statt, mit dem wir gut zurechtkommen – hier sind wir zurzeit kein beliebtes Angriffsziel.

Wolfgang Rosenkranz (KSÖ): Wie weit darf und soll sich der Staat in die Wirtschaft einmischen – Stichwort: Cyber Security Act?

Erich Albrechtowitz (BKA): Hier treffen zwei Grundsätze aufeinander. Von staatlicher Seite soll in der Ökonomie nur geregelt werden, was wirklich notwendig ist. Andererseits muss der Staat Sicherheit auf staatlichem Raum gewähren – dazu zählt mittlerweile auch der digitale Raum. In Hinblick auf den Cyber Security Act bedeutet das: Wir müssen dafür Sorge tragen, den Wirtschaftsstandort Österreich und die staatliche Souveränität zu stärken. Oberste Prämisse ist es aber, die digitale Welt durch die Schaffung von Rahmenbedingungen sicher zu machen.

Wolfgang Rosenkranz (KSÖ): Wie schätzen Sie das Cyber Security-Bewusstsein der österreichischen Bevölkerung ein?

Rudolf Striedinger (Abwehramt/BMLV): Einerseits muss Cybererziehung und -hygiene von klein auf anerzogen werden – vom Elternhaus quer durch das ganze Schulsystem. Hier herrscht immenser Aufholbedarf. Andererseits muss der Staat dafür sorgen, dass bei Geräten automatisch die erforderlichen Sicherheitssysteme mitgeliefert werden: Ein User muss davon ausgehen können, dass sein Gerät sicher ist. Das entpuppt sich bei IoT-Geräten bisher als großes Problem.

Wolfgang Rosenkranz (KSÖ): Die Regulierung der Cyber Security – Geburtshelfer-Aufgabe oder staatliche Daueraufgabe?

Philipp Blauensteiner (BVT/BMI): Der Staat wird sich keinesfalls komplett zurückziehen können. Aktuell befinden wir uns in einer Phase, in der Sicherheit oft noch als Add-on am Ende eines Entwicklungsprozesses gesehen wird. Wir müssen durch gesamtstaatliche Initiativen und Vorgaben dafür sorgen, dass Sicherheit von Beginn an mitgedacht wird.

Erich Albrechtowitz (BKA): Der digitale Raum wird in seiner Bedeutung für den Staat als gesamtes mit dem physischen Territorium gleichziehen, ihn vermutlich sogar überholen.

Daher ist es für den Staat undenkbar, sich aus so einem wichtigen Teil seines Gefüges zurückzuziehen. Im Gegenteil: Der Staat wird noch mehr Verantwortung wahrnehmen müssen als in der Vergangenheit.

Rudolf Striedinger (Abwehramt/BMLV): Die Cyberbedrohung entwickelt sich laufend weiter, daher werden sich auch die Standards und Gesetze weiterentwickeln müssen. Cyber Security wird zur permanenten Aufgabe des Staates werden.

Tief Luft holen

Trends in der strategischen Verteidigung

64 %

verfügen über eine mündliche (21 %) oder schriftliche (43 %) Berichterstattung

65 %

verfügen über ausreichendes Cyber Security-Wissen

53 %

betrachten Cyber Security nicht als fixen Bestandteil von Digitalisierungsinitiativen

42 %

verfügen über ein dezidiertes Cyber Security-Team

34 %

betrachten Cyber Security als rein technische Angelegenheit

Kugelfische können sich bei Gefahr aufpumpen. Durch die enorme Volumsvergrößerung werden Angreifer abgeschreckt.

„Oberste Prämisse ist es, die digitale Welt durch die Schaffung von Rahmenbedingungen sicher zu machen."

Erich Albrechtowitz
Bundeskanzleramt

Der technologische Wandel und die Digitalisierung erfordern vollkommen neue Cyber Security-Strategien. Gefordert sind umfassende technologische und organisatorische Lösungen, die den „Faktor Mensch" gleichermaßen berücksichtigen und das Unternehmen widerstandsfähig gegen Angriffe machen. Um das Sicherheitsrisiko „Cyberkriminalität" strategisch zu managen, ist die Unternehmensführung am Zug – eine Aufgabe, die in keinster Weise delegierbar ist. Das Thema gewinnt zwar österreichweit auf oberster Ebene immer mehr an Bedeutung, doch nach wie vor herrscht auf Managementebene ein gewisser Mangel an Cyber Security-Wissen. Auch in Sachen Risikomessung haben die Unternehmen hierzulande noch Aufholbedarf. Die Umsetzung der DSGVO hat in den Unternehmen positive Spuren hinterlassen.

Chefsache: Cyber Security und Management

Im Kampf gegen Cyberkriminalität ist es von entscheidender Bedeutung, welche Rolle Cybersicherheit aus Sicht der Chefetage im Unternehmen einnimmt. Cyber Security ist eine Management-Aufgabe, die „top-down" organisiert und umgesetzt werden muss. Entscheidende Faktoren dabei sind eine offene Kommunikation und eine positive Kultur für das Thema. Denn der Cyberkriminalität kann man nur durch ein integriertes Security Management Herr werden.

In den letzten Jahren hat sich das Image von Cybersicherheit extrem gewandelt – vom absoluten Fokusthema der IT-Spezialisten hin zum Risk Management-Thema der Geschäftsführung. Nur mehr 34 Prozent der befragten Unternehmen betrachten Cyber Security als rein technische Angelegenheit. Im Vorjahr lag dieser Wert noch bei 70 Prozent. Laut Umfrage nimmt das Thema mittlerweile bei 56 Prozent der Unternehmensleitung einen hohen Stellenwert ein. 77 Prozent der österreichischen Unternehmen geben an, dass die Unternehmensleitung die Notwendigkeit zur Behandlung von Cyberrisiken aktiv kommuniziert.

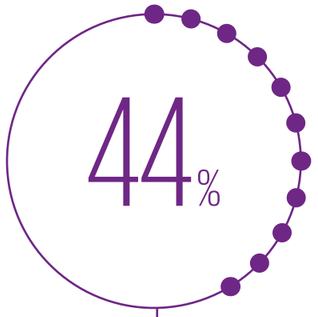
Cybersicherheit hat sich somit die strategisch wichtige Bedeutung und Unterstützung auf Führungsebene erarbeitet.

Dieser positive Trend darf jedoch nicht dazu verleiten, sich verfrüht auf die Schultern zu klopfen. Denn gleichzeitig herrscht ein enormer Widerspruch zwischen der Tatsache, dass Unternehmen über die Dringlichkeit des Themas Cybersicherheit Bescheid wissen, und der konkreten Umsetzung, um die Widerstandsfähigkeit des Unternehmens zu stärken. So stimmen etwa nur rund 40 Prozent der befragten Unternehmen der Aussage zu, dass die Unternehmensleitung alles tut, um das Unternehmen resilienter gegenüber Cyberangriffen zu machen.

Cyber Resilience ist eine wichtige Grundlage zur Förderung der Agilität in Unternehmen und einer der entscheidenden Bausteine für erfolgreiche Digitalisierungsvorhaben.

Auch in den Aufsichtsgremien hat das Thema noch nicht jenen Stellenwert, der im zustehen würde: Nach wie vor fordern die Hälfte der Aufsichtsräte (51 Prozent) aktiv keine Informationen zu Cyber Security ein.

Eine Zahl, die ebenso aufhorchen lässt: Für jedes zweite Unternehmen (53 Prozent) ist Security noch kein fixer Bestandteil in den Initiativen zur Digitalisierung. Digitalisierung muss jedoch gemeinsam mit Themen der Cybersicherheit gedacht werden und kann auch nur dann erfolgreich funktionieren. Hier besteht akuter Handlungsbedarf, wenn österreichische Unternehmen nicht ins Hintertreffen geraten wollen.



verfügen über keine Methode, um die Auswirkungen von Cyberrisiken mittels **Security KPIs** zu messen.

2017 waren es noch 57 Prozent.

Wissen ist Macht: Fehlender Informationsfluss

Das Bewusstsein über die Wichtigkeit von Cybersicherheitsthemen steht im Widerspruch zum Wissensstand der Entscheidungsträger: Nur zwei Drittel (65 Prozent) der befragten Unternehmen stimmen der Aussage zu, dass die Unternehmensleitung über ausreichendes Wissen im Bereich Cyber Security verfügt. Besonderen Aufholbedarf zeigen hier Familienunternehmen: Knapp die Hälfte (48 Prozent) der befragten Unternehmen gibt an, dass sie hier noch Handlungsbedarf sehen.

Besonders skeptisch zeigen sich die IT-Leiter: 53 Prozent der CIOs sind der Meinung, dass die Unternehmensleitung noch nicht über das notwendige Cyber Security-Wissen verfügt. Dies ist gleichzeitig ein Indiz dafür, dass der IT-Fachjargon eine ungestörte Kommunikation zwischen Fachexperten und der Führungsebene erschwert. Dadurch kommen entscheidende Botschaften oftmals nicht bei der Zielgruppe an: Unterschiedliche Sprachgebräuche behindern die Kommunikation und sind eine oftmals unterschätzte Hürde in der Zielerreichung.

Sattelfest sehen sich Österreichs Unternehmen hingegen bei den regulatorischen Rahmenbedingungen: 83 Prozent der Unternehmen geben an, dass ihnen die Regularien, wie die NIS-Richtlinie oder IKT-Sicherheitsleitfaden der Finanzmarktaufsicht (FMA), bekannt sind.

Ein wichtiger Indikator für strategische Cyber Security-Maßnahmen ist die Berichterstattung in Richtung Führungsebene. Dieses Reporting muss vorausschauend und institutionalisiert stattfinden, um Transparenz über alle Maßnahmen zu schaffen. 64 Prozent der Unternehmen verfügen mittlerweile über eine mündliche (21 Prozent) oder schriftliche (43 Prozent) Berichterstattung zu Cyber Security-Themen. Bei 36 Prozent der Unternehmen gibt es nach wie vor noch keinerlei Aktivitäten, um die Führung über Cyber Security zu informieren. Besonders uninformiert sind Aufsichtsräte, CFOs und der Finanzbereich: Jeweils 25 Prozent erhalten keine Berichterstattung zum Thema Cybersicherheit. Um die finanziellen Auswirkungen von Cybersicherheitsvorfällen einschätzen und beurteilen zu können, wäre eine Berichterstattung an diese Zielgruppen von entscheidender Bedeutung. Mangelndes Wissen tangiert auch das Risikomanagement in Unternehmen. Die Bedeutung von Kennzahlen ist in diesem Bereich unbestritten: Nur so können Sinnhaftigkeit und Wirksamkeit von Maßnahmen überprüft werden. Daher ist das Messen der Risiken entscheidend, um diese im Cyber Security-Bereich richtig steuern zu können.

Nach wie vor geben jedoch 44 Prozent der Unternehmen an, über keine Methoden zu verfügen, um die Auswirkungen von Cyberrisiken auf das Unternehmen messen zu können (Security KPIs). 2017 lag diese Zahl zwar mit 57 Prozent noch höher, dennoch kristallisiert sich klar heraus: In Sachen Risikobemessung herrscht enormer Aufholbedarf, da ansonsten die Grundlage für strategische Maßnahmen fehlt.

Volle Kraft voraus: Personelle Maßnahmen
Um im Kampf gegen Cyberkriminalität erfolgreich sein zu können, müssen Unternehmen neben der technischen Ausstattung auch die organisatorische und personelle Ebene angemessen auf Vordermann bringen. Denn um Security entsprechend authentisch im Unternehmen umsetzen zu können, benötigt es Personen, die sich ausschließlich um dieses Thema kümmern.

Ein Blick hinter die Kulissen verrät, dass Unternehmen noch viele Hausaufgaben zu erledigen haben. Lediglich 42 Prozent der Unternehmen geben an, über ein dezidiertes Cyber Security-Team zu verfügen. Noch dramatischer sind die Zahlen im Bereich der Familienunternehmen – 64 Prozent geben an, kein Team für Cyber Security zu haben – sowie im Handel: 3 von 4 Unternehmen (75 Prozent) haben keine personellen Ressourcen. 58 Prozent der befragten Unternehmen verfügen bereits über einen CISO (Chief Information Security Officer), der vorwiegend in der IT (50 Prozent) oder einer eigenen CISO- bzw Security-Abteilung (27 Prozent) angesiedelt ist. Nur bei acht Prozent der Unternehmen ist der CISO direkt dem Vorstand zugeordnet. Die Zuordnung zur IT ist aufgrund der Fachlichkeit grundsätzlich nachvollziehbar, doch wäre aufgrund der strategischen Herausforderung und zur Wahrung der Unabhängigkeit eine Ansiedlung an zentraler Stelle außerhalb der IT sinnvoller. Dafür sprechen auch die zunehmende Bedeutung für die erfolgreiche Umsetzung von Digitalisierungsvorhaben sowie die Verbesserung der Berichterstattung an die Unternehmensleitung.

Bei jenen Unternehmen, die über keinen CISO verfügen, werden die Sicherheitsagenden zumeist durch die IT-Leitung (50 Prozent) übernommen. 30 Prozent der befragten Unternehmen sehen keine Notwendigkeit eine derartige Stelle zu schaffen, 20 Prozent planen die Einführung einer CISO-Stelle in naher Zukunft. Auffällig ist, dass Familienunternehmen hier kaum Handlungsbedarf sehen: 69 Prozent geben an, keine vergleichbare Position im Unternehmen zu haben, 38 Prozent planen auch nicht, eine solche einzuführen. Gehandelt wird bei Österreichs Unternehmen hier zumeist erst reaktiv, also dann, wenn schon etwas passiert ist: 67 Prozent jener Unternehmen, die schon Opfer einer Cyberattacke geworden sind, verfügen über einen CISO.

Das liebe Geld: Cyber Security-Budgets
Cybersicherheit gewinnt an Bedeutung: Ein entscheidender Maßstab dafür ist die Höhe des Sicherheitsbudgets. Zahlreiche Aufsichtsbehörden und Regulatoren fordern mittlerweile eine entsprechende personelle und finanzielle Ausstattung des Bereiches Cyber Security in Unternehmen.

Unternehmen haben die Wichtigkeit eines Cyber Security-Budgets zwar erkannt, der Stellenwert spiegelt sich aber in der finanziellen Dotierung noch nicht klar wider. Bei rund einem Drittel der Unternehmen (32 Prozent) ist das Cyber Security-Budget im letzten Jahr zumindest leicht gestiegen. Aktuell liegt das Security-Budget bei 14 Prozent der befragten Unternehmen lediglich zwischen zwei und fünf Prozent des IT-Budgets. Nur fünf Prozent der Unternehmen geben mehr als zehn Prozent des IT-Budgets für Cybersicherheit aus. Rund jedes fünfte Unternehmen (21 Prozent) hat kein dezidiertes Budget für Cyber Security, bei Familienunternehmen liegt dieser Wert gar bei 37 Prozent. Insbesondere bei Familienunternehmen ist gegenüber dem Vorjahr keine Veränderung ersichtlich.

Eine Zahl, die aufhorchen lässt: 38 Prozent der Unternehmen geben an, nicht zu wissen, ob sie ein eigenes Cyber Security-Budget haben oder nicht. Die Gründe dafür können einerseits darin liegen, dass der Bereich nicht immer eindeutig identifizierbar ist. Oftmals spielen aber auch versteckte Kosten oder eine Kostenaufteilung auf unterschiedlichen Posten eine Rolle. Für eine umfassende Security Governance wäre es aber entscheidend, einen klaren Blick auf das Cyber Security-Budget zu haben. Nur so können Kosten und Wirksamkeit der einzelnen Maßnahmen sinnvoll beurteilt werden.

Nach dem gewünschten Ziel-Budget für Cyber Security gefragt, sind sich die Unternehmen uneins. Hier geben 17 Prozent der befragten Unternehmen an, dass zwei bis fünf Prozent des IT-Budgets der Idealzustand wären. Nahezu gleichviele Unternehmen (14 Prozent) plädieren für einen Anteil von fünf bis zehn Prozent. Auffällig dabei: Unternehmen, die vom NIS Gesetz direkt betroffen sind, erkennen die Notwendigkeit eines erhöhten Budgets zur Verbesserung der Cybersicherheitsmaßnahmen. Hier sind 25 Prozent der Meinung, dass ein Anteil von fünf bis zehn Prozent ein adäquates Budget wäre.

Im Wandel: DSGVO verändert Unternehmen
Die Datenschutz-Grundverordnung (DSGVO) hat im vergangenen Jahr mehr oder weniger alle Unternehmen jeglicher Größenordnung beschäftigt und ihre Spuren in den Organisationen hinterlassen. Bei 78 Prozent der Unternehmen zeigen sich in Bezug auf Prozesse und Werkzeuge wesentliche Veränderungen, knapp 8 von 10 Unternehmen (81 Prozent) verfügen aktuell über einen Datenschutzbeauftragten.

Die 3 wichtigsten Trends 2016 - 2019

- **Cyber Security hat sich erfolgreich vom Fokusthema der IT-Spezialisten hin zum Risk Management-Thema entwickelt.**
- **Immer mehr Unternehmen messen Cyberrisiken, doch es herrscht nach wie vor Aufholbedarf.**
- **Unternehmen rüsten personell auf: Immer mehr beschäftigen Cyber Security-Mitarbeiter und verfügen über dezidierte CISOs.**

Welche Arten von Angriffen waren am erfolgreichsten?

47% **Malware**
Schadsoftware

47% **Phishing**
Identitätsdiebstahl über gefälschte Inhalte wie zB E-Mails mit der Aufforderung zur Durchführung einer Tätigkeit

29% **Cryptolocker**
Unbrauchbarmachen von Daten, um zur Wiederherstellung Geld in Form von Kryptowährungen zu erpressen

29% **Webseite oder Webapplikation**
wurde angegriffen

16% **Social Engineering**
zwischenmenschliche Beeinflussung, um so zB an vertrauliche Informationen zu gelangen

14% **Denial of Service bzw Distributed Denial of Service**
Ein Angriff bei dem Systeme so überlastet werden, dass diese nicht mehr erreichbar sind

Was waren die häufigsten Maßnahmen nach einem Angriff?

86% **Analyse**
der technischen und organisatorischen Schwachstellen

46% **Forensische Untersuchung**
zur Faktenfindung durch das eigene Unternehmen

36% **Penetrations-Test**
durch einen externen Dienstleister

28% **Penetrations-Test**
durch das eigene Unternehmen

28% **Überprüfung der Sicherheitsmaßnahmen**
durch externe Dienstleister

19% **Forensische Untersuchung**
zur Faktenfindung durch einen externen Dienstleister

Mehrfachnennungen waren möglich

Das Thema „Auskunftsrechte" hat die Unternehmen ebenfalls beschäftigt: 13 Prozent der heimischen Unternehmen wurden mit Anfragen kontaktiert.

Datenschutzverletzungen müssen innerhalb von 72 Stunden gemeldet werden. Um einen solchen Vorfall auch zu erkennen ist es notwendig, entsprechende Prozesse und Tools im Unternehmen zu etablieren. Nur so kann ein rasches Reagieren ermöglicht werden.

In Sachen „Erkennung eines Vorfalles" haben Unternehmen noch ein Stück des Weges vor sich. So geben nur 41 Prozent der Unternehmen an, hier die notwendigen Maßnahmen bereits getroffen zu haben. Natürlich wurden gewisse Aktivitäten umgesetzt, doch es fehlt häufig am strategischen Zusammenspiel der einzelnen Tools.

Auch bei der Sensibilisierung der Mitarbeiter und Dienstleister gibt es noch Aufholbedarf. „Im Fall des Falles" gilt es, den Datenschutzvorfall strukturiert abzuarbeiten. 58 Prozent der Unternehmen sind überzeugt, mit einem solchen Vorfall gut umgehen zu können und eine Erstmeldung an die Behörde innerhalb von 72 Stunden zu schaffen.

Besonders jene Branchen, die den täglichen Umfang mit Compliance-Vorschriften gewöhnt sind, punkten hier (Banken: 75 Prozent, Versicherungen: 78 Prozent, Energiewirtschaft: 90 Prozent), wohingegen im Bereich Handel und Lebensmittelerzeugung nur eine geringe Zustimmung vorliegt (jeweils 37 Prozent).

Praxistipp

Cybersicherheit gehört in das Zentrum gerückt: Cyber Security-Strategien und -Maßnahmen müssen ganzheitlich im Unternehmen verankert werden und einen entscheidenden Stellenwert in der Unternehmenskultur bekommen. Das geht nur, wenn das Thema „Chefsache" ist.

Dipl.-Ing. MMag. Peter Gerdenitsch

Peter Gerdenitsch ist Head of Group Information & Cyber Security der Raiffeisen Bank International AG (RBI). Das Risiko eines erfolgreichen Angriffs und dem damit verbundenen Reputationsverlust durch Cyberattacken beschäftigt die Branche der Finanzdienstleister wie keine andere. Kein Wunder also, dass Cyber Security auf der Board-Agenda der RBI ganz oben steht.

Entscheidend ist die richtige Balance zwischen Prävention und Reaktion.

Wann muss ein Unternehmen heutzutage mit einem Angriff durch Cyberkriminelle rechnen?
Die traurige Wahrheit: Wo ein Wille ist, da ist auch ein Weg. Man kann sich nie vollumfänglich vor Cyberkriminalität schützen. Als Unternehmen muss man rund um die Uhr darauf vorbereitet sein, angegriffen zu werden.

Organisierte Cyberkriminalität findet statistisch gesehen vermehrt abends und am Wochenende statt. Fakt ist: Bei den meisten Angriffen geht es längst nicht mehr darum, „es einmal zu probieren". Im Gegenteil: Über Ransomware, Trojaner oder vergleichbare Angreifer-Tools wollen Kriminelle auf illegale Art und Weise zu Geld kommen.

Wo liegen die Hauptrisiken von Cyberangriffen für Banken und Versicherer?
In einer Branche wie unserer, in der Vertrauen und Sicherheit eine ganz besonders große Rolle spielen, steht das Risiko des Reputationsverlustes ganz oben auf der Liste. Natürlich sind auch direkte finanzielle Schäden durch unerlaubte Transaktionen eine große Gefahr. Um das Vertrauen der Kunden aus prozessualer und technologischer Sicht rechtfertigen zu können, wurden von Banken und Versicherungen umfangreiche Cyber Security-Maßnahmen eingeführt.

Unsere Maßnahmen gehen dabei weit über die regulatorischen Vorgaben hinaus. Wir betrachten Cybersicherheit als ganzheitliche Thematik im Unternehmen und setzen entsprechende Schritte.

Was sind aus Ihrer Sicht die Kernpunkte einer guten Cyber Security-Strategie?
Das A und O ist das Commitment des Managements: Eine Cyber Security-Strategie kann nicht Bottom-up getrieben werden, sondern muss von der Geschäftsführung in der Unternehmenskultur verankert werden. Das Board hat die entscheidende Rolle, die C.I.A. der Daten zu gewährleisten: Confidentiality, Integrity, Availability, also Vertraulichkeit, Integrität, Verfügbarkeit.

Es braucht strategische Ziele, eine realistische und umsetzbare Roadmap sowie eine klare Kommunikation der Strategie. Zielgerichtete awareness-bildende Maßnahmen für unterschiedliche User-Gruppen sind dabei ebenso wichtig. Entscheidend ist es auch, den Mitarbeitern die Angst zu nehmen, Security hätte mit persönlicher Überwachung zu tun. Mitarbeiter müssen befähigt werden, gemeinsam mit Security-Experten sichere Lösungen für ihren Anwendungsfall zu finden.

Hier braucht es einen vollkommen neuen Denkzugang: Security soll kein Verhinderer sein, sondern lösungsorientiert arbeiten.

Antwortet man in Ihrem Unternehmen reaktiv auf Bedrohungen oder wird eine proaktive Cyberabwehr verfolgt?
Entscheidend ist die richtige Balance zwischen Prävention und Reaktion. In Sachen Prävention sollte man als Unternehmen unter anderem auf Threat Intelligence setzen, um potenzielle Bedrohungen frühzeitig zu identifizieren. Unverzichtbar ist der Informationsaustausch über Angriffs- und Bedrohungsmuster, den wir strategisch sowohl mit Feed-Providern als auch mit Banken innerhalb der Gruppe betreiben.

Nichtsdestotrotz: 100 Prozent Prävention ist illusorisch. Daher müssen Maßnahmen in Hinblick auf „Detect & Respond" laufend verstärkt werden, um Angreifer frühzeitig aufzuspüren und entsprechende Gegenmaßnahmen zu setzen. Wichtig ist auch, den Vorfall an die entsprechenden Stellen zu melden.

Schlagwort „Expertenmangel": Eine Herausforderung, die uns früher oder später zu schaffen machen wird. Wie geht Ihr Unternehmen aktuell damit um?
Generell gilt, dass Österreich verstärkt in Ausbildung investieren muss. Der Grundstein dafür sollte schon sehr früh in der Schulung der Digitalkompetenz gelegt werden. Bereits in der Volksschule sollten Kinder auf Gefahren aufmerksam gemacht werden. Für die Raiffeisen Bank International AG ist es im Moment noch verhältnismäßig leicht, technisch affine Leute als Mitarbeiter zu gewinnen. Der Stellenwert von Security in unserem Unternehmen ist sehr hoch, dieser Ruf ist unter den Stellensuchenden mittlerweile bekannt.

Hilfreich dabei ist natürlich auch die Marke Raiffeisen in jenen Ländern, in welchen wir tätig sind. Schwierigkeiten sehen wir aktuell weniger auf technischer Ebene als im Bereich Governance, also bei der Suche nach Personen, welche die regulatorischen Vorgaben auf Technologieseite umsetzen können.

Welches IT-Sicherheitsniveau haben österreichische Unternehmen im weltweiten Vergleich?
In Österreich sind die Finanzunternehmen sicherlich ein Vorreiter in Sachen Security. Allgemein sehe ich Österreich im internationalen Umfeld allerdings im hinteren Mittelfeld: Security hat in anderen Ländern einen wesentlich höheren Stellenwert. Die Wichtigkeit des Themas muss konsequent gefördert werden. Erste Fortschritte sind schon zu sehen, doch der Weg ist noch lang. Ganz besonderen Aufholbedarf orte ich im gesellschaftlichen Bereich, denn der „Faktor Mensch" ist in Sachen Cybersicherheit entscheidend. Die Technologie allein kann nie ausreichen. Ganz wichtig: Cyber Security ist kein kompetitives Wettstreitthema zwischen Unternehmen, sondern fordert gemeinschaftliches Denken und Handeln.

Das Silicon Valley ist und bleibt unglaublich attraktiv für internationale Talente. Denn: Talent attracts talent.

Mit „Open Austria“ haben das Außenministerium und die WKÖ 2016 gemeinsam ein eigenes Büro in San Francisco errichtet. Was ist das Resümee nach drei Jahren?
„Open Austria“ soll als österreichische Landezone für Unternehmen und Wissenschaftler im Silicon Valley dienen. Innovation und Wachstum funktionieren in Österreich und dem Silicon Valley sehr unterschiedlich.

Wenn Unternehmen anstreben, exponentiell zu wachsen, fehlt es ihnen hierzulande oftmals an Perspektive. Das Silicon Valley verfügt über eine unvergleichbar offene Innovationskultur, das ist für manches Hightech-Unternehmen eine einzigartige Chance. Open Austria unterstützt bei der Vernetzung mit potenziellen Geschäftspartnern in der Hightech-Hochburg. Insbesondere österreichischen Scale-up-Unternehmen bietet das Silicon Valley immense Perspektiven.

Es taucht oft die Kritik auf, das Silicon Valley sei zu abgehoben geworden. Dennoch wollen alle dorthin. Was macht das Silicon Valley so besonders?
Das Silicon Valley ist nach wie vor DIE Innovationsmetropole schlechthin, das Gravitationszentrum der digitalen Revolution. Ein einzigartiger Mix aus unvergleichbarem Ökosystem, anhaltendem Wachstum, Ansammlung vielseitiger Talente, risikofreudigen Kapitalgebern, einmaliger Ideenschmiede und vernetzten Mentoren. Und nicht zuletzt: Alle großen Player der Branche sind hier vertreten.

Natürlich hat die Region auch ihre Schattenseiten: Horrende Mieten und exorbitante Löhne für Mitarbeiter erfordern vielseitige Business-Konzepte. So empfehlen wir den Start-ups etwa in zahlreichen Fällen, das Software Development in Österreich zu belassen, die Kundenakquise jedoch im Valley zu etablieren.

Das Ende des Silicon Valley droht Ihrer Meinung nach also nicht?
Das Silicon Valley ist Teil eines zyklischen Prozesses, Rahmenbedingungen verändern sich. In einem Aufsehen erregenden Artikel hat das britische Wirtschaftsmagazin The Economist den „Peak Valley“ ausgerufen. Das Silicon Valley sei an seinem Zenit angekommen. Doch Totgesagte leben ja bekanntermaßen länger. Erkennbar ist, dass in der Technologie-Hochburg ein gewisses Maß an Korrektur kommen wird. Doch in welchem Ausmaß kann aktuell niemand vorhersagen. Momentan führt in Sachen Hightech nach wie vor kein Weg am Silicon Valley vorbei.

Nach erfolgreicher Gründung in Österreich: Welcher Schritt ist notwendig, um ins Silicon Valley zu expandieren?
Auf eigene Faust ins Silicon Valley zu starten ist ein sehr waghalsiges Unterfangen, denn dort herrschen eigene Spielregeln. Unser Programm „Go Silicon Valley“ eignet sich bestens dafür, um umfassende Einblicke zu gewinnen: Die Initiative ermöglicht es jährlich rund 15 Start-ups, ein bis drei Monate vor Ort ihre Geschäftsmodelle vorzustellen. Unter Mentorenbetreuung erhalten die Unternehmen Zugang zu Business-Netzwerken. Diese Herausforderung ist kein „Honigschlecken“. In Österreich sind Unternehmer nach wie vor nicht perfekt ausgebildet, um zu verkaufen, zu pitchen, zu überzeugen. Auf die Teilnahme an diesem Programm muss man sich intensivst vorbereiten.

Das Fehlen an Fachkräften ist eine allgegenwärtige Problematik. Wie begegnet man dieser Herausforderung im Silicon Valley und welche Empfehlungen lassen sich für Österreich ableiten?
Das Silicon Valley ist und bleibt unglaublich attraktiv für internationale Talente. Denn: Talent attracts talent.

Solche Rahmenbedingungen sind andernorts nur schwer herzustellen. Für Österreich entscheidend: Man muss die Vorteile, wie etwa die Lebensqualität oder die Lebenserhaltungskosten, ins Rampenlicht stellen.

Das allein reicht natürlich nicht. Es braucht langfristige, strategische Maßnahmen – etwa bei der Immigration: Österreich muss aktiv und systematisch internationale Talente suchen. Hier sollte man sich im Moment an Amerika kein Vorbild nehmen: Neue, strenge Einwanderungsgesetze hemmen den Zuzug.

Für das Silicon Valley ist so eine politische Entscheidung eine Katastrophe. Denn: Laut Statistik wurden mehr als die Hälfte der Toptech-Firmen der USA von Migranten oder deren Kindern gegründet.

Stichwort Datenschutz oder auch Künstliche Intelligenz: Im Silicon Valley gibt die Innovation das Tempo vor. Welches Konfliktpotenzial gibt es in Hinblick auf das Thema Regulierungsbedarf?
Überall dort, wo die Auswirkungen technischer Errungenschaften für die Gesellschaft nicht eindeutig vorhersehbar sind, herrscht Regulierungsbedarf. Ich sehe hier keinen Widerspruch zwischen Silicon Valley und Gesetzgebern, im Gegenteil.

Im Silicon Valley werden Chancen und Gefahren schon mitgedacht, Standards von diversen Plattformen schon gesetzt, bevor dies auf regulatorischer Ebene passiert. Hier gilt es, den politischen Entscheidungsträgern ausreichendes Faktenmaterial zur Verfügung zu stellen, damit sie ihre Entscheidung richtungsweisend treffen können.

Natürlich darf auch nicht vergessen werden: Zu viele Regulatorien hemmen Innovation.

Martin Rauchbauer

Martin Rauchbauer ist österreichischer Konsul in San Francisco und Co-Director von „Open Austria“. Die Initiative unterstützt österreichische Unternehmen dabei, im Silicon Valley Fuß zu fassen. An der Hightech- und Innovations-Hochburg führt, dem Experten zufolge, nach wie vor kein Weg vorbei. Doch die Antwort auf alle Fragen lautet keinesfalls „Silicon Valley“, warnt Rauchbauer.

Gemeinsam Zähne zeigen

Sicherheit der Eigen- und Fremdsysteme im Visier

23%

führen Red-Team Assessments durch

7%

glauben, dass ihre Lieferanten ausreichende Sicherheitsmaßnahmen treffen

28%

sichern sich das Recht, die Sicherheit der Lieferanten regelmäßig zu überprüfen

73%

wünschen sich eine eindeutig definierte Anlaufstelle für Cyber Security

60%

sehen in der Einführung von Branchen-CERTs einen Mehrwert

Piranhas sind aggressive und räuberische Fische mit sehr scharfen Zähnen. Sie fixieren zuerst die Beute und schießen dann blitzschnell auf sie zu um sie zu beißen.

„In Österreich – dem Land der KMU – müssen alle Unternehmen dazu ermutigt werden, Sicherheit als essenziellen Baustein zu sehen."

Dr. Michael Hysek
Finanzmarktaufsicht (FMA)

In den Bemühungen, ein unautorisiertes Eindringen von Cyberkriminellen in das Unternehmen zu verhindern, setzen Unternehmen je nach Branche und Unternehmensform unterschiedliche Schwerpunkte. Auch wenn die Wege oft unterschiedlich sind, so ist das Ziel immer das gleiche: die Sicherheitsniveaus von Systemen stetig zu verbessern.

Das Vertrauen in die Sicherheit der eigenen Systeme und jene von Lieferanten und Kunden kennt bei Österreichs Unternehmen zwar seine Grenzen. Dennoch agieren Unternehmen hierzulande im Umgang mit dem Third Party-Risiko, also jenen Risiken, die von Dienstleistern, Lieferanten und Partnern ausgehen, zum Teil fahrlässig.

Einer für alle? Die Zukunft der CERTs

CERTs (Computer Emergency Response Team) dienen als Ansprechpartner für IT-Sicherheit, vernetzen und koordinieren sicherheitsrelevante Information über Cyberangriffe und geben Warnungen und Alerts heraus. In der Diskussion um CERTs scheiden sich die Geister: Ein CERT für alle Unternehmen oder doch lieber Branchen-CERTs?

In Österreich ist CERT.at die erste Kontaktanlaufstelle für alle Belange der IT-Sicherheit mit Österreichbezug. Außerdem gibt es noch „Government-CERT (GovCERT)", das CERT der öffentlichen Verwaltung mit Fokus auf kritische Infrastrukturen, und ein milCERT für die militärische Landesverteidigung.

Österreich verfügt ebenso über ein brancheneigenes CERT, das Austrian Energy CERT (AEC), welches für die österreichische Elektrizitäts- und Erdgaswirtschaft zuständig ist.

Die KPMG Studie zeigt: Die Notwendigkeit eines klar definierten Ansprechpartners, egal ob nationaler CERT oder Branchen-CERT, ist sehr hoch. Knapp dreiviertel der Unternehmen (73 Prozent) wünscht sich eine eindeutig definierte Anlaufstelle für Cyber Security, insbesondere wenn sie schon Opfer eines Angriffes (82 Prozent) waren. Besonders hoch (86 Prozent) ist der Wunsch unter den Sicherheitsverantwortlichen innerhalb eines Unternehmens und in Unternehmen, bei denen das NIS-Gesetz Anwendung findet (88 Prozent). Vier Fünftel (82 Prozent) aller mittleren und großen Unternehmen sind vom Nutzen einer solchen Anlaufstelle überzeugt, während Start-ups (60 Prozent) und Familienunternehmen (67 Prozent) hier weniger Bedarf orten.

Unterschiede gibt es auch beim Detailblick auf die Branchen. Von der Einführung einer klar definierten Anlaufstelle sind insbesondere Unternehmen der Branchen Energiewirtschaft (100 Prozent), Healthcare (89 Prozent), Verkehr (100 Prozent) und Unternehmen im Handel und der Lebensmittelproduktion (88 Prozent) überzeugt. Unternehmen der Branchen Bildung sehen hingegen kaum eine Notwendigkeit (17 Prozent), unentschlossen zeigt sich der Dienstleistungssektor (55 Prozent).

Die Meinungen, ob ein Branchen-CERT einen Mehrwert darstellen würde oder nicht, sind zwar gespalten, die Tendenz geht jedoch in Richtung Branchenspezialisierung: 60 Prozent der Unternehmen orten in der Einführung von Branchen-CERTs einen Mehrwert – insbesondere Banken (77 Prozent) sowie Unternehmen der Branchen Energiewirtschaft (100 Prozent) und Healthcare (78 Prozent).

Die Vorteile eines Branchen-CERT liegen laut Sicherheitsexperten vor allem im fachspezifischen Wissen, dem gegenseitigen Vertrauen und der Berücksichtigung der Branchenspezifika. Skeptisch in Hinblick auf einen Branchen-CERT sind hingegen Unternehmen im Bereich Automotive, Landwirtschaft (jeweils 100 Prozent), Immobilien (jeweils 36 Prozent), Industrie (38 Prozent) sowie im Handel und der Lebensmittelproduktion (38 Prozent).

Auf Herz und Nieren: Sicherheitsüberprüfung

Unternehmen haben in Sachen Cybersicherheit ein großes Ziel: das unautorisierte Eindringen in das Unternehmen zu verhindern. Entscheidend dabei ist das Bereitstellen und die Überprüfung eines angemessenen Sicherheitsniveaus von Systemen. Besonders oft setzen Unternehmen Prozesse wie System Hardening, Patching oder Backups (97 Prozent) ein, um die Sicherheit der Systeme zu verbessern.

Auch das Durchführen von regelmäßigen Audits und Assessments zur Feststellung des aktuellen Sicherheitsstandes (80 Prozent) erfreut sich in Österreichs Unternehmerlandschaft größer Beliebtheit. Weniger Aufmerksamkeit wird Methoden wie Red-/Blue-/Purple-Team Assessments (23 Prozent) geschenkt. Maßnahmen im Bereich der internen (62 Prozent) und externen (65 Prozent) Penetrationstests und dem Review der gesetzlichen Rahmenbedingungen (62 Prozent) werden nicht einmal von zwei Drittel der befragten Unternehmen durchgeführt.

Auffällig ist, dass alle befragten Unternehmen im öffentlichen Bereich (100 Prozent), alle Personengesellschaften (100 Prozent) und nahezu alle Kapitalgesellschaften (98 Prozent) darauf bedacht sind, ihre Systeme regelmäßig zu patchen und zu sichern. Wohingegen nur zwei Drittel (67 Prozent) der Einzelunternehmen einen Nutzen in einem gehärteten und aktualisierten System sehen.

Noch gravierender ist der Unterschied im Bereich der regelmäßigen Audits: 100 Prozent der Personengesellschaften, 82 Prozent der Kapitalgesellschaften und 77 Prozent der öffentlichen Unternehmen führen regelmäßig Assessments durch, um etwaige Verbesserungsmaßnahmen zu identifizieren. Hingegen setzt nur ein Drittel der befragten Einzelunternehmen (33 Prozent) auf regelmäßige Assessments. Für Start-ups ist der Review der gesetzlichen Rahmenbedingungen (100 Prozent) wichtiger als System Hardening oder Penetrationstests (jeweils 50 Prozent). Große Unternehmen legen hingegen mehr Wert auf die Aktualität der Systeme und die Feststellung des aktuellen Sicherheitsstandes innerhalb des Unternehmens (jeweils 100 Prozent).

Der Detailblick auf Branchen eröffnet eine interessante Feststellung: Für alle Unternehmen im Handel und der Lebensmittelproduktion sowie dem Energiewirtschaftsbereich (jeweils 100 Prozent) und mehr als zwei Drittel aller Banken und Versicherungsunternehmen (jeweils 72 Prozent) ist es von entscheidender Bedeutung, die einzuhaltenden gesetzlichen Rahmenbedingungen regelmäßig zu reviewen und entsprechende Maßnahmen zu setzen. Überraschenderweise legt aber nur ein Drittel der Industrieunternehmen (33 Prozent) Wert darauf.

Gut behütet: Die internen Sicherheitssysteme

Das Vertrauen in die Sicherheit der eigenen Systeme kennt bei Österreichs Unternehmen seine Grenzen: Die Hälfte der befragten Dienstleistungsunternehmer (50 Prozent) und zwei Drittel der Unternehmen im Handel und der Lebensmittelproduktion (67 Prozent) sind davon überzeugt, dass ihre Informationssysteme ausreichend gesichert sind. Diese Meinung teilt hingegen nur knapp ein Viertel der befragten Unternehmen in den Bereichen Industrie (26 Prozent), Healthcare (25 Prozent), Energiewirtschaft (22 Prozent) und Bauwirtschaft (25 Prozent). In Bezug auf das Sicherheitsniveau der eigenen Systeme gegen externe Angreifer herrschen innerhalb der

Die 3 wichtigsten Trends 2016 – 2019

Das Sicherheitsrisiko durch Dritte, wie etwa Lieferanten oder Kunden, wird nach wie vor unterschätzt und ist ein lohnendes Ziel für Angreifer.

Immer mehr Unternehmen wünschen sich Branchen-CERTs als erste Anlaufstelle für Cybersicherheit.

Maßnahmen im Bereich der internen und externen Penetrationstests sind rückläufig.

Unternehmenshierarchie divergierende Meinungen. Ein Prinzip kristallisiert sich jedoch klar heraus: Personen, die mit den Systemen im Normalfall arbeiten, empfinden dieses eher als unsicher als Personen, die eine Führungsposition innehaben. So sind nur zwölf Prozent der Mitarbeiter ohne Führungsposition der Meinung, dass die Systeme im Unternehmen ausreichend geschützt sind, während durchschnittlich ein Viertel der IT-Leiter (30 Prozent) und Sicherheitsverantwortlichen (21 Prozent) und beinahe die Hälfte aller befragten Abteilungsleiter (46 Prozent) davon überzeugt sind.

Eine Ursache für dieses Auseinanderklaffen der Meinungen könnte sein, dass fachliche Mitarbeiter die alltäglichen Sicherheitsprobleme selten an ihre Vorgesetzten melden und diese daher ein vollkommen unterschiedliches Bild haben.

Österreichs Unternehmen wiegen sich auch bei einem anderen Thema zum Teil in falscher Sicherheit: Fast alle Unternehmen, die noch keinen Angriffsversuch auf ihr Unternehmen hinnehmen mussten, sehen ihre Systeme als ausreichend (45 Prozent) oder zumindest gut (44 Prozent) gegenüber Angreifern gesichert, die über den Weg der Kunden oder Lieferanten eindringen könnten.

Ein anderes Bild zeigt sich bei jenen Unternehmen, die bereits attackiert wurden: Nur ein Viertel betrachtet die Systeme als ausreichend gesichert (28 Prozent).

Gefährliche Partnerschaft: Third Party Risk

Im Umgang mit dem Third Party-Risiko agieren Unternehmen hierzulande allzu freizügig. Generell ist nur ein Bruchteil der befragten Unternehmen (sieben Prozent) der Meinung, dass ihre Lieferanten ausreichende Sicherheitsmaßnahmen gegen Risiken im Informationssicherheitsbereich treffen. Gleichzeitig sehen es Unternehmen nicht als ihre Pflicht an, Kunden und Lieferanten regelmäßig über neue Gefahren zu informieren (18 Prozent). Nur 28 Prozent der Unternehmen sichern sich das Recht, die Sicherheit der Lieferanten regelmäßig zu überprüfen.

Jene Unternehmen, welche die Sicherheitsmaßnahmen ihre Lieferanten in Punkto Cyber Security als ausreichend einstufen, haben auch großes Vertrauen in die eigene Sicherheitsstruktur: Fast alle (92 Prozent) sind davon überzeugt, dass die eigenen Systeme ausreichend gegen externe Angreifer gesichert sind. Gleichzeitig haben sich 58 Prozent davon das Recht gesichert, die Lieferanten einer Sicherheitsüberprüfung zu unterziehen, um sich so noch ein zusätzliches Bild über die Wirksamkeit der Maßnahmen zu verschaffen.

Zudem informiert ein Großteil ebenjener Unternehmen regelmäßig oder zumindest hin und wieder die Lieferanten und Kunden über neue Gefahren im Informationssicherheitsbereich (für 42 Prozent zutreffend bzw für 42 Prozent eher zutreffend).

Ein vergleichbares Bild zeigt sich bei jenen Unternehmen, die ihre Kunden und Lieferanten regelmäßig über neue Gefahren informieren. Hier haben sich knapp die Hälfte (47 Prozent) das Recht gesichert, eine Sicherheitsüberprüfung bei den Lieferanten durchzuführen. Gleichzeitig zeigen sie sich überzeugt davon, dass ihre eigenen Systeme ausreichend gesichert sind (47 Prozent). Umgekehrt zeigt die Studie: Jene Unternehmen, welche die Sicherheitsmaßnahmen ihrer Lieferanten im Informationssicherheitsbereich als unzureichend einstufen (sechs Prozent), informieren weder Kunden noch Lieferanten regelmäßig über neue Gefahren (80 Prozent). Auch haben sie sich kein Recht gesichert haben, die Lieferanten einer Sicherheitsüberprüfung zu unterziehen (50 Prozent).

Praxistipp

Die Kontrolle über Dritte wird zum Erfolgs- oder Misserfolgsfaktor, denn Angreifer kommen nie durch die Vordertür: In einem wirtschaftlichen Umfeld, in dem die Wertschöpfungskette immer komplexer wird, reicht ein einziges schwaches Glied, um die Widerstandsfähigkeit eines Unternehmens aufs Spiel zu setzen.

Mag. Julian Jäger

Vorstandsdirektor
der Flughafen Wien AG

Digitalisierung benötigt effiziente Rahmenbedingungen und eine breite Plattform, um maximale Synergieeffekte zu erzielen.

Ganz allgemein: Wie schätzen Sie den Umgang österreichischer Unternehmen mit Cyberrisiken ein?
Die vielfältigen Beispiele für Cyberangriffe in Österreich und weltweit haben definitiv zur Bewusstseinsbildung beigetragen – denken wir etwa an WannaCry, NotPetya oder Stuxnet. Die Bedrohung durch Cyberangriffe ist längst in den Chefetagen der österreichischen Unternehmen angekommen und es wird mittlerweile massiv in Cyber Security investiert.

Inwiefern haben sich die Angreifer und ihre Angriffsmethoden verändert?
Das wachsende Bewusstsein über Cyberrisiken hat dazu geführt, dass die Grundhygiene in den IT-Abteilungen sorgfältig hergestellt wird. Zeitgleich werden wirksame Abwehrsysteme gegen bekannte Angriffe geschaffen. Dieser „Basisschutz" lässt Cyberkriminelle zu neuen Strategien greifen, etwa die Individualisierung der Angriffe und die Verlagerung in Richtung Identitätsdiebstahl und Mitarbeitermanipulation (zB CEO Fraud). Gleichzeitig haben auch Regierungen die Wirksamkeit von Cyberangriffen erkannt und setzen diese gezielt ein.

Welche Vorkehrungen treffen Sie, um adäquat auf die ansteigenden Bedrohungen reagieren zu können?
Neben der laufenden Weiterentwicklung grundlegender Sicherheitsmechanismen investieren wir gezielt in die Stärkung der Cyber Security-Systeme und -Spezialisten. Sehr wichtig ist auch die Vernetzung mit Unternehmen und Behörden, wozu das KSÖ einen wichtigen Beitrag leistet. Denn den Kampf gegen Cyberkriminalität kann man nicht alleine gewinnen.

Was sollten Unternehmen tun, wenn sich herausstellt, dass es ein digitales Sicherheitsproblem gibt?
Als erstes muss das Problem so schnell wie möglich behoben werden. Sollten Dritte von den Sicherheitsproblemen direkt oder indirekt betroffen sein, ist eine klare Kommunikation wichtig, um die Auswirkungen für die Betroffenen zu minimieren. Am Flughafen Wien haben wir eigene Teams für solche Fälle etabliert, die sich aus den betroffenen Fachbereichen mit dem Senior Management zusammensetzen und sowohl die Aktivitäten als auch die Kommunikation koordinieren.

Der Schutz von Prozessen und Systemen: Was ist Ihrer Meinung nach hier die Rolle des Boards/Senior Managements?
Interne und externe Kontrollsysteme helfen, dass Prozesse eingehalten werden und Abweichungen erkannt und verhindert werden. Der Vorstand stellt sicher, dass die notwendigen Ressourcen für technische und organisatorische Kontrollmechanismen vorhanden sind. Diese Mechanismen werden laufend hinterfragt, deren Wirksamkeit wird geprüft und entsprechend nachgebessert. Nur wer die Kontrollen kontrolliert, kann sicherstellen, dass sie auch wirken.

Wie machen Sie Mitarbeiter auf die Risiken durch Phishing oder Ransomware aufmerksam?
Aktuell planen wir beispielsweise eine Phishing-Kampagne. Das Ergebnis zeigt uns, wo die Defizite liegen und ermöglicht die Ableitung gezielter Schulungsmaßnahmen. Zudem verteilen wir über unsere internen Medien regelmäßig Informationen bezüglich der Erkennung von Auffälligkeiten und das richtige Verhalten. Zuletzt zB über das Thema CEO-Fraud.

Wie wird das NIS-Gesetz den Umgang der Unternehmen und der Behörden mit Cybergefahren verändern?
Ich denke, dass sowohl Betreiber kritischer Infrastrukturen als auch Behörden mittlerweile ein gutes Risikobewusstsein entwickelt haben. Für viele Branchen existieren bereits Standards und Richtlinien, etwa für den Bereich Aviation der ICAO Annex 17. Der regelmäßig zu erbringende Nachweis über ausreichende Cybersicherheitsvorkehrungen wird, ähnlich dem „Pickerl" beim PKW, dazu beitragen, die Systeme laufend dem Stand der Technik anzupassen und Schwachstellen zu erkennen.

Wie hat sich das Inkrafttreten der DSGVO auf die Cyber Security-Lage Ihres Unternehmens ausgewirkt?
Die DSGVO verpflichtet Unternehmen, personenbezogene Daten mittels geeigneter technischer und organisatorischer Maßnahmen zu schützen. Durch die Umsetzung technischer Maßnahmen haben wir die Cyber Security weiter verbessert.

Darüber hinaus schärfen wir unsere Prozesse laufend nach, damit wir hier die strengen Anforderungen der DSGVO erfüllen.

Wie sieht die Kommunikation und Kollaboration branchenintern aus?
Im Rahmen der Mitgliedschaft in der Arbeitsgemeinschaft Deutscher Verkehrsflughäfen (ADV) tauscht sich der Flughafen Wien regelmäßig mit anderen Flughäfen aus. Diese Zusammenarbeit ist für uns seit jeher sehr positiv und trägt zu einem gemeinsamen Lagebild in unterschiedlichen Themengebieten, wie etwa Cyber Security, bei.

Wie sollen Unternehmen die Herausforderungen der Digitalisierung meistern?
Die Digitalisierung benötigt effiziente Rahmenbedingungen und eine breite Plattform, um Insellösungen zu vermeiden und maximale Synergieeffekte zu erzielen. Es ist wichtig, das Wesentliche im Auge zu behalten und keine Kompromisse bei Qualität und Sicherheit einzugehen.

Widerstand leisten

Notfallpläne und Cyberversicherungen für Unternehmen

45%
besitzen derzeit keine Versicherung gegen Cyberangriffe

53%
sind mit dem Angebot an Cyberversicherungen nicht zufrieden

57%
aktualisieren jährlich ihre Notfallpläne für Cyber Security

68%
fühlen sich mit Incident Response-Plänen auf Angriffe gut vorbereitet

19%
verfügen über eine Cyberversicherung

Oktopusse benutzen ihren Tintenbeutel, wenn sie sich bedroht fühlen. So können sie sich hinter einer farbigen Wasserwolke fluchtartig in Sicherheit bringen.

„Die Unternehmen müssen hinsichtlich Cyber Security ein großes Maß an Eigenverantwortung beweisen."

DI Christian Schönbauer
E-Control

Cyber Security-Strategien stellen den Schutz der wichtigen Daten des Unternehmens und die Sicherstellung der einwandfreien Funktionsweise der Geschäftsprozesse in den Fokus. Unternehmen konzipieren geeignete Schutzmaßnahmen, um Cyberkriminellen keine Angriffsfläche zu geben. Die Realität zeigt, dass immer mehr Unternehmen Angriffe abwehren können und sich die Bemühungen und Investitionen daher auszahlen.

Ebenso entscheidend ist es jedoch, sich nicht nur mit der Prävention und Abwehr von Angriffen zu beschäftigen, sondern auch Strategien nach einem Vorfall im Visier zu haben. Denn einen vollkommenen Schutz vor Kriminalität gibt es weder in der realen noch der virtuellen Welt.

Besonders dann, wenn kritische Infrastrukturen in den Fokus der Angreifer gelangen, ist ein rasches Reagieren und eine entsprechende Resilienz, besonders unterstützt auch durch das NIS-Gesetz, unabdingbar.

Gut geplant ist halb gewonnen: Krisenpläne

Das zukünftige Risiko in Hinblick auf Cyberattacken stufen Österreichs Unternehmen als bedrohlich ein. Fast drei Viertel der befragten Unternehmen (74 Prozent) befürchten, dass Cyberangriffe zunehmen werden. Einzig Start-ups sehen gelassener in die Zukunft: Sie sind zu einem großen Teil der Meinung, dass die Frequenz der Angriffe gleichbleiben wird (67 Prozent). Die zukünftige Bedrohungslage wird auch in den einzelnen Branchen unterschiedlich eingestuft. So rechnen etwa alle Befragten im Bereich der Automobilindustrie damit, dass die Anzahl der Angriffe gleichbleiben wird. Der Großteil der Unternehmen im Bereich Bildung und Telekommunikation (jeweils 90 Prozent) erwartet hingegen eine Zunahme.

Generell zeigen sich Österreichs Unternehmen zuversichtlich, für diese Bedrohungen entsprechend gerüstet zu sein. 68 Prozent fühlen sich mit Incident Response-Plänen auf Angriffe gut vorbereitet. Diese Pläne, auch Vorfallreaktionspläne genannt, sind eine Art schriftlicher Krisenplan, die Unternehmen dabei unterstützen, Angriffe zu entdecken und angemessen darauf zu reagieren. Denn besonders in Ausnahmesituationen, in denen sich Unternehmen nach einem Angriff befinden, ist ein strukturiertes Vorgehen entscheidend für die erfolgreiche Bewältigung.

In mehr als drei Viertel der befragten Unternehmen sind Notfallpläne vorhanden, die sich mit den Bereichen physischer Angriff auf Infrastruktur, Unerreichbarkeit von Systemen und Datendiebstahl, -manipulation, und -vernichtung befassen (jeweils 78 Prozent). Die Themen Cloud und Störung der geschäftskritischen Prozesse (jeweils rund ein Prozent) finden hingegen kaum Beachtung. Zwölf Prozent der Unternehmen gaben sogar an, dass sie derzeit überhaupt keine Notfallpläne im Einsatz haben. Drei Viertel (75 Prozent) davon sind jedoch dazu entschlossen, in Zukunft solche Pläne erstellen zu wollen.

Mit der Erstellung der Pläne alleine ist es jedoch nicht getan: Kaum ein Bereich ist so schnelllebig wie jener der Cyberkriminalität, denn auch hier hält die Digitalisierung der Abläufe Einzug. Eine regelmäßige Aktualisierung dieser Pläne und die Anpassung an die aktuellen Entwicklungen und unternehmerischen Gegebenheiten sind daher dringend anzuraten. Die Realität zeigt, dass dieser Handlungsanweisung viele Unternehmen Folge leisten: Die Aktualisierung der Notfallpläne erfolgt bei einem Großteil der Unternehmen (57 Prozent) jährlich oder öfter (insgesamt 14 Prozent), nur wenige Unternehmen aktualisieren die erstellten Notfallpläne seltener als jährlich (14 Prozent) oder gar nicht (vier Prozent). Die Beraterpraxis verdeutlicht, dass hier die Gefahr auch in einem anderen Detail schlummert: Die wenigsten Unternehmen üben die Umsetzung der Notfallpläne in der Praxis – eine Voraussetzung für ein schnelles und reibungsloses Reagieren im Fall des Angriffs. Die Pläne werden häufig erst dann aus der Schublade gezogen, wenn ein konkreter Vorfall den reibungslosen Ablauf im Unternehmen stört.

Die Praxis zeigt: Selbst wenn Übungen stattfinden, so sind sich Mitarbeiter in dieser Situation der Existenz der Pläne nicht bewusst und setzen ihre Handlungen im guten Glauben. Gefragt sind hier zielgerichtete, bewusstseinsbildende Maßnahmen und laufendes Trockentraining der Abläufe. Denn nur mit einem gewissen Grad an Perfektion in einem Übungsszenario können sich Unternehmen für den Ernstfall gut vorbereitet fühlen.

Ein Trend, der hinkt: Cyberversicherung

Die Nachfrage nach Cyberversicherungen nimmt seit Jahren zu. So prognostiziert die KPMG Studie „Neues Denken, neues Handeln" dem Versicherungsschutz für Cyberrisiken nicht nur enorme Wachstumschancen, sondern kommt sogar zu dem Schluss: Cyberversicherungen scheint die am schnellsten wachsende Sparte zu werden, die die Versicherungsbranche je gesehen hat.

Der Markt hat natürlich auch auf Gerichtsurteile in Folge der Windows-Malware „Notpetya" reagiert. Einige betroffene Unternehmen hatten Ausfall-Polizzen gegen Schäden aus Hackerangriffen abgeschlossen und Ausgleichszahlungen nicht oder nur zum Teil erhalten.

Versicherungen verwiesen auf einen „Akt kriegerischer Handlung". Hier bleibt nach der erstinstanzlichen Entscheidung abzuwarten, welche rechtlichen Entscheidungen getroffen werden und wie Unternehmen und Versicherungen darauf reagieren werden.

Wie wurden Unternehmen auf einen Cyberangriff aufmerksam?

86%	**Interne Sicherheitssysteme** Firewall, SIEM, etc
65%	**Mitarbeiter**
23%	**Externe Dienstleister**
14%	**Kunden**
8%	**Angreifer** zB Hacktivisten
4%	**Medien**
3%	**Behörden**
2%	**Zulieferer**

Mehrfachnennungen waren möglich

Was waren die Motive der Angreifer?

67%	**Finanzielle Schadenszufügung**
28%	**Unterbrechung von Geschäftsprozessen**
25%	**Nicht bekannt**
23%	**Beeinträchtigung der Reputation**
17%	**Veröffentlichung vertraulicher Informationen von Kunden oder anderen Geschäftspartnern**
17%	**Manipulation von Informationen**
15%	**Veröffentlichung vertraulicher interner Informationen**
13%	**Unerlaubte Veröffentlichung von persönlichen Daten**
1%	**Erpressung**
1%	**Durchsetzung politischer Ziele**

Mehrfachnennungen waren möglich

Der Trend zu Cyberversicherungen ist zwar weltweit absehbar, hat sich am heimischen Markt jedoch noch nicht durchgesetzt. Denn beinahe die Hälfte der österreichischen Unternehmen besitzt derzeit keine Versicherung gegen Cyberangriffe (45 Prozent). Ein weiteres Drittel (36 Prozent) der Befragten ist sich nicht sicher, ob eine Versicherung in diesem Bereich vorhanden ist.

Knapp ein Viertel (23 Prozent) aller Unternehmen hat deshalb keine Cyberversicherung, weil die Risiken auf andere Art abgesichert werden. Weitere Gründe für das Fehlen einer Cyberversicherung: Unternehmen sind mit dem Angebot der Versicherung nicht zufrieden, da entweder die Prämie im Vergleich zur Deckung zu hoch ist (22 Prozent) oder der Deckungsumfang nicht angemessen ist (14 Prozent). Ebenfalls ein entscheidendes Thema ist die Tatsache, dass zwar Interesse bestehen würde, die Versicherung aber aus Sicht der Unternehmen derzeit kein passendes Angebot hat (17 Prozent). Dieser Punkt trifft insbesondere auf den Dienstleistungsbereich (33 Prozent) und den Bereich Familienunternehmen (30 Prozent) zu.

Große Unternehmen sind Vorreiter in Sachen Absicherung: 29 Prozent geben an, über eine Cyberversicherung zu verfügen. Außerdem betont die Hälfte der großen Unternehmen, die explizit keine Cyberversicherung hat, dass sie ihre finanziellen Risiken auf andere Art abgesichert hat.

Auch die Branchen gehen unterschiedlich mit dem Thema um: Besonders hoch ist der Anteil der versicherten Unternehmen unter den Befragten im Handel und der Lebensmittelproduktion (50 Prozent), im Bereich der Energiewirtschaft (30 Prozent), der Industrie (29 Prozent) und der Banken (25 Prozent). Hingegen verfügen 60 Prozent der Dienstleistungsunternehmen, 78 Prozent der Healthcare-Unternehmen und 80 Prozent der Logistikunternehmen über keine Versicherung.

Große Unterschiede gibt es auch in Bezug auf die Unternehmensform: So verfügen 69 Prozent der Einzelunternehmen und 54 Prozent der Unternehmen im öffentlichen Bereich über keine Cyberversicherung oder sind sich nicht im Klaren darüber, ob sie eine besitzen.

Überdurchschnittlich hoch ist hingegen der Anteil der versicherten Kapitalgesellschaften (23 Prozent). Erwähnt werden muss an dieser Stelle, dass zumindest die Unternehmen im öffentlichen Bereich zu einem großen Teil das Risiko auf eine andere Art absichern (43 Prozent).

Die 3 wichtigsten Trends 2016 – 2019

- **Notfall- und Krisenpläne setzen sich in immer mehr österreichischen Unternehmen durch.**
- **Cyberversicherungen sind zwar weltweit im Vormarsch, haben in Österreich aber noch keinen hohen Stellenwert.**
- **Große Unternehmen sind sowohl bei Notfallplänen als auch Cyberversicherungen Vorreiter.**

Praxistipp

Einen Notfallplan in der Schublade zu haben, reicht nicht aus. Auch mit der regelmäßigen Aktualisierung alleine ist es längst nicht getan. Entscheidend ist es, das Vorgehen im Fall des Falles auch kontinuierlich zu üben.

Nicht alles, was aus Fernost kommt, muss böse sein. Oder anders formuliert: Nicht alles, was aus den USA importiert wird, ist unbedenklich.

Wie schätzen Sie den Umgang österreichischer Unternehmen mit Cyberrisiken ein?
Großunternehmen haben in den letzten Jahren eindeutig ein erhöhtes Bewusstsein für Cyber Security erlangt. Im Bereich der kleinen und mittleren Unternehmen muss man die Sachlage differenziert betrachten: Hier findet man die gesamte Bandbreite von „Wir sind sehr gut geschützt" über „Das ist für kleine Betriebe zu komplex" bis zu „Mir kann das nicht passieren". Zahlreiche kleine Unternehmen werden außerdem hinsichtlich der sicherheitstechnischen Wartung ihrer IT-Systeme nicht optimal betreut und sind daher einem wesentlich höheren Cyberrisiko ausgesetzt. Gleichzeitig glauben sie allerdings, dass sie durch die IT- Betreuung gut geschützt sind. Von einer durchgängig soliden Basis kann man daher noch nicht sprechen.

Stellen Sie in den letzten Jahren Veränderungen in der Anzahl und Art der Attacken fest?
Ein eindeutiger Trend ist, dass Password Guessing-Massenangriffe zunehmen. Vor allem durch die zahlreichen Data Leaks der vergangenen Jahre – man denke etwa an Yahoo, mySpace, LinkedIn oder Twitter – wird von Seiten der Cyberkriminellen massiv versucht, Kundenkonten zu übernehmen.

Welche zentralen Motive würden Sie hinter einem Angriff auf Ihr Unternehmen vermuten?
Im Falle unseres Unternehmens, also der Österreichischen Lotterien, würde ich folgendes Ziel vermuten: Die Übernahme von Kundenkonten, um Zugriff auf deren Spielguthaben zu bekommen. Es werden also primär monetäre Ziele verfolgt, wie bei fast allen Cyberangriffen.

Wie gehen Management und Aufsichtsrat mit dem Thema Cyber Security bei Ihnen um?
Cyber Security ist ein eindeutiger Top-down-Prozess. Das spiegelt sich auch in der Berichterstattung wider. Cyberrisiken werden im Rahmen des strategischen Enterprise Risk Management dem Prüfungsausschuss des Aufsichtsrats schon seit Jahren proaktiv berichtet. In unregelmäßigen Intervallen werden auch für diese Ebene Berichte und Präsentationen erstellt, um die Awareness für das Thema zu fördern.

Wie wird das NIS-Gesetz den Umgang der Unternehmen und der Behörden mit Cybergefahren verändern?
Sofern ein Unternehmen nicht zu den „Betreibern wesentlicher Dienste" zählt, wird das Gesetz aus heutiger Sicht wenig unmittelbare Änderungen mit sich bringen. Dass auf nationaler Ebene die Behörde besser qualifiziert sein wird, um auf Cyberangriffe angemessener reagieren zu können, ist eine sehr positiv Entwicklung.

Diese Veränderung ist absolut essenziell für den Sicherheitsstandard in Österreich.

Welche Rolle soll der Staat/die EU aus Ihrer Sicht generell in Bezug auf Cyber Security in Zukunft übernehmen? Geht es um die Sicherung von Mindeststandards?
Für Betreiber von kritischer Infrastruktur macht eine Sicherung von Mindeststandards durchaus Sinn. Es stellt sich allerdings die Frage, wie die „unsicheren" Produkte definiert werden.

Plakativ ausgedrückt: Nicht alles, was aus Fernost kommt, muss böse sein – Stichwort Huawei. Oder anders formuliert: Nicht alles, was aus den USA importiert wird, ist unbedenklich – Stichwort NSA.

Sind die Cyber Security-Risiken in Ihrem Unternehmen Teil des Riskmanagement Framework?
Cyber Security-Risiken sind bei den Österreichischen Lotterien sowohl im operativen als auch im strategischen Enterprise Riskmanagement Framework enthalten.

Stichwort „Cloud Computing" und „User Security": Haben Sie Bedenken, wenn es um die Cloud geht oder überwiegen die Vorteile von Cloud-Lösungen?
Bedenken ergeben sich für mich einerseits aus der Einhaltung der Datenschutzbestimmungen und andererseits aus der Implementierung der Cloud-Lösungen durch den jeweiligen Anbieter.

Viele SaaS-Anbieter bedienen sich mittlerweile auch der großen Infrastruktur Cloud-Anbieter wie etwa AWS, Google, Microsoft, etc. Bei den großen und vielfach geprüften Anbietern habe ich weniger Sicherheitsbedenken hinsichtlich der infrastrukturellen Sicherheit.

Wenn der innovative SaaS-Anbieter seine Lösung allerdings unsicher designt, dann kann es zu Problemen kommen. Generell sehe ich den Vorteil von Cloud-Lösungen in der Erhöhung der Geschwindigkeit von Umsetzungen. Potenziell niedrigere Kosten müssen gegenüber gut gemanagten On-Premises-Lösungen erst erzielt werden.

Haben sie bereits ein Red-/Blue-/Purple-Team beauftragt?
Ja, wir setzen vor allem Red-Teams ein. Hauptgrund dafür ist der unabhängige Test der implementierten Schutzmaßnahmen und die Erkennung bzw die Reaktion auf die Angriffe durch die internen Security-Mitarbeiter.

In welcher Frequenz sollte eine solche Prüfung Ihrer Meinung nach wiederholt werden?
Das ist abhängig vom Risiko und den durchgeführten Veränderungen. Eine Prüfung sollte aber zumindest jährlich stattfinden.

Erich Schuster

Bereichsleiter IT
der Österreichischen Lotterien

Round Table

Die Aufsichtsbehörde als Informationsdrehscheibe

Finanzmarktaufsicht (FMA), E-Control und die Rundfunk und Telekom Regulierungs-GmbH (RTR): Alle drei haben behördlichen Charakter und gesetzliche Aufgaben in unterschiedlichen Branchen zu erfüllen – dem Finanz-, Energie- bzw Telekommunikationsbereich. Das Thema Cybersicherheit beschäftigt alle drei Aufsichtsbehörden gleichermaßen und immer intensiver. KPMG lud die Fachexperten zur Diskussionsrunde.

Die Expertenrunde (v.l.n.r.):
DI Christian Schönbauer (E-Control),
Dr. Michael Hysek (Finanzmarktaufsicht, FMA),
Robert Lamprecht, Andreas Tomek (beide KPMG),
Wolfgang Rosenkranz (KSÖ), Mag. Jan Weber und
Mag. Ulrich Latzenhofer (beide Rundfunk und
Telekom Regulierungs-GmbH)

Wolfang Rosenkranz (KSÖ): Wie würden Sie die Rolle der FMA, der E-Control und der RTR in Bezug auf Cyber Security beschreiben?

Michael Hysek (FMA): Die Kernaufgabe der FMA ist es, zu beaufsichtigen, ob Banken, Versicherungen und Wertpapierfirmen ihre Risiken angemessen begrenzen und managen. Dazu zählen nicht nur Kredit-, Markt- und Zinsänderungsrisiken, sondern auch operationelle Risiken, wie das Cyberrisiko. Das Thema hat sich immer stärker zum Aufsichtsschwerpunkt entwickelt, der Fokus der FMA liegt dabei klar in der Prävention.

Christian Schönbauer (E-Control): Als Regulierungsbehörde für Strom- und Gasversorgung haben wir den gesetzlichen Auftrag, uns auch um die Versorgungssicherheit zu kümmern. Der Cybersicherheit kommt daher eine große Rolle zu, Stichwort: Blackout nach einer Cyberattacke. Bereits 2012 startete die E-Control die „Cyber Security-Initiative für die österreichische Energiewirtschaft". Sollte es durch einen Cybervorfall zur Verknappung der Versorgung kommen, sorgt die E-Control gemeinsam mit dem Ministerium für die Energielenkung.

Ulrich Latzenhofer (RTR): Die RTR-GmbH besteht aus den Fachbereichen Medien sowie Telekommunikation und Post. Die RTR hat seit 2011 den gesetzlichen Auftrag, die Umsetzung von Mindestsicherheitsmaßnahmen bei den Telekommunikationsbetreibern zu beaufsichtigen. Wir sind außerdem Ansprechpartner bei Meldungen über Sicherheitsverletzungen innerhalb der Branche.

Darin sehen wir eine entscheidende Aufgabe aller Regulierungsbehörden: Es geht nicht nur darum, die Einhaltung der Vorgaben zu prüfen, sondern auch als Informationsdrehscheibe für betroffene Unternehmen zur Verfügung zu stehen.

Wolfang Rosenkranz (KSÖ): Wo sehen Sie die Grenzen der Regulierungsbehörden, in Sachen Cybersicherheit positiv einzuwirken?

Jan Weber (RTR): Das Ziel der RTR ist es, immer mit so wenigen Eingriffen wie möglich zu arbeiten, wir bauen auf Zusammenarbeit. Natürlich benötigen wir eine Rechtsgrundlage, um im Falle des Falles durchgreifen zu können. Als Regulierungsbehörde orientieren wir uns stark an der Technical Guideline on Incident Reporting der ENISA, der Europäischen Agentur für Netz- und Informationssicherheit.

Michael Hysek (FMA): Die Grenze einer Behörde ist immer der Gesetzestext: Aufgrund des Legalitätsprinzips können und dürfen wir uns nur im Rahmen der Gesetze bewegen. Natürlich gibt es auch die Möglichkeit via Soft Laws einzugreifen: Leitfäden, Maßnahmen, Empfehlungen, Risikoabschätzungen, Schulungen. So kann man als Regulator den Stellenwert der Thematik Cyber Security zusätzlich anheben.

Christian Schönbauer (E-Control): Spielregeln für Cyber Security zu definieren ist im regulatorischen Bereich besonders schwierig, da man sich ob der Schnelllebigkeit des Themas auf dem kleinsten gemeinsamen Nenner treffen muss. Oder anders ausgedrückt: Wir können nicht jede Detailanforderung ausformulieren. Die Unternehmen müssen hier ein großes Maß an Eigenverantwortung beweisen und sich des Themas proaktiv annehmen.

Wolfang Rosenkranz (KSÖ): Wie sieht denn die Zusammenarbeit zwischen den drei Regulierungsbehörden, also FMA, E-Control und RTR, aus?

Michael Hysek (FMA): Es gibt natürlich ähnlich gelagerte Themen im Finanz-, Energie- und Telekommunikationsbereich – denken wir etwa an die DSGVO oder Compliance-Bestimmungen. Es haben sich Fachrunden und Ad-hoc-Arbeitsgruppen gebildet, die gemeinsam versuchen, Themen voranzutreiben.

Eine intensivere Zusammenarbeit im Bereich Cyber Security wäre sicher sinnvoll, um unsere jeweiligen Erfahrungen auszutauschen. Beispielsweise veranstalten wir demnächst ein Cyber-Planspiel mit einigen Banken. Ich kann mir vorstellen, dass die Erkenntnisse daraus für die Kollegen interessant sein könnten.

Jan Weber (RTR): Die Zusammenarbeit wird sich aufgrund konkreter Fragestellungen, etwa neuer Rechtsvorschriften für Zahlungsdienstleister, immer mehr intensivieren. Eine enge Zusammenarbeit und der Austausch der Regulatoren ist aus meiner Sicht entscheidend für die Schaffung einer gemeinsamen Basis und zur Sicherung des Wirtschaftsstandortes Österreich.

Christian Schönbauer (E-Control): Die drei Behörden sind bereits derzeit zu IT-Sicherheitsthemen in Kontakt, haben regelmäßige IT-Treffen etwa quartalsweise.

Wolfang Rosenkranz (KSÖ): Wie schätzen Sie die Cyber Security-Lage in Österreich ganz allgemein ein?

Michael Hysek (FMA): Die Anzahl der Cyberattacken steigt an, die Cyberkriminellen agieren immer professioneller. Der Finanzsektor ist von jeher eines der beliebtesten Angriffsziele. Mit dem Ansteigen der Angriffe steigt aber auch das Bewusstsein für die Materie in den Unternehmen radikal. Entscheidend für Erfolg oder Misserfolg ist, wie das Management dem Thema Cyber Security gegenübersteht.

Christian Schönbauer (E-Control): Ohne Strom geht gar nichts mehr. Die Awareness im Energiebereich ist deshalb von jeher groß. Cyber Security wird immer mehr zum Daily Business, in großen Unternehmen ist der Grad an Cyber-Professionalität besonders hoch. Besonders berücksichtigen sollte man auch mittlere und kleine Energieversorgungsunternehmen, die hier noch hinterherhinken. Die Gefahr dabei: Sie sind genauso vernetzt wie die großen, ein Angriff kann das Gesamtsystem daher ebenso gefährden.

Ulrich Latzenhofer (RTR): Die Betreiber im Telekommunikationssektor sind sich der Wichtigkeit des Themas Cyber Security klar bewusst. Trotz des enormen Verantwortungsgefühls können sie aber nur für die Sicherheit im Netz bis zum Netzabschlusspunkt sorgen. Sicherheitsprobleme beim Kunden können nicht vom Betreiber behoben werden. Dem stehen teilweise auch rechtliche Erfordernisse, zB im Bereich der Netzneutralität, entgegen.

Wolfang Rosenkranz (KSÖ): Die Flut an immer neuen Regulatorien verursacht den Unternehmen Kosten. Gibt es hier viele Beschwerden?

Michael Hysek (FMA): Regulatorische Vorgaben versus regulatorische Kosten – natürlich ein Dauerbrenner im Finanzbereich. Doch die Reputations- und wirtschaftlichen Folgen können durch Cyberattacken in astronomische Höhen gehen. Daher legen wir hier besonderes Augenmerk auf die Risikominimierung. Auf oftmaliges Jammern folgt nahezu immer Verständnis.

Ulrich Latzenhofer (RTR): Die gesetzlichen Vorgaben zur Sicherheit hängen immer vom jeweiligen Risiko ab. Dieses ist bei großen Telekombetreibern naturgemäß größer als bei kleinen. Sie sind sich in Österreich dieser Verantwortung sehr bewusst und akzeptieren, dass Sicherheit auch kostet.

Wolfang Rosenkranz (KSÖ): Inwiefern hat das EnergieCERT die Branche in Hinblick auf Cybersicherheit verändert? Es ist ja in Österreich momentan noch das einzige Branchen-CERT.

Christian Schönbauer (E-Control): Durch das Austrian Energy CERT ist ein branchenspezifischer Informationsfluss entstanden, den es sonst nicht geben würde. Daraus werden entsprechende Empfehlungen abgeleitet. Ein solcher Austausch wäre auch für andere Branchen zu forcieren: Er schafft Vertrauen innerhalb der Branchen in Hinblick auf die Informationsweitergabe bei Cybersicherheitsvorfällen.

Wolfang Rosenkranz (KSÖ): Wo wird sich die Regulierung in Sachen Cybersicherheit hin entwickeln? „Geburtshelfer" oder Daueraufgabe?

Michael Hysek (FMA): Mit einer reinen Geburtshelferfunktion ist es bei der FMA bestimmt nicht getan. Im Sinne der Bewusstseinsbildung ist aktuell besonderes Engagement notwendig. Die FMA hat mit den beaufsichtigten Unternehmen ein gemeinsames Interesse: Dass der Finanzmarkt und alle seine Teilnehmer bestmöglich gegen Cyberattacken gewappnet sind. In Österreich, dem Land der KMU, müssen generell alle Unternehmen dazu ermutigt werden, Sicherheit als essenziellen Baustein zu sehen.

Christian Schönbauer (E-Control): Die Cyber Security-„Chaosphase", in der alles neu und ungeregelt war, haben wir hinter uns, da das Thema ja nicht mehr ganz neu ist. Aktuell befinden wir uns in einer Übergangsphase, in der es gilt, Bewusstsein zu schärfen, Standards zu erheben, Regeln zu optimieren. Aus meiner Sicht für die E-Control eine Daueraufgabe.

Ulrich Latzenhofer (RTR): Ich sehe die RTR als Prozessbegleiter. Die EU ändert die gemeinsamen Vorschriften zur Regelung der Telekommunikationsbranche, und zwar mit dem European Electronic Communications Code. Der Kodex setzt den Begriff des Kommunikationsdienstes umfassender an, sodass zukünftig auch die Over the Top-Dienste, zB WhatsApp, dazuzählen. Cybersicherheit ist und bleibt daher eine Daueraufgabe.

DI Christian Schönbauer
Koordination Versorgungssicherheit, E-Control

Andreas Tomek
KPMG

Wolfgang Rosenkranz
Kuratorium Sicheres Österreich (KSÖ)

Mag. Jan Weber
Rechtlicher Experte, Rundfunk und Telekom Regulierungs-GmbH

Mag. Ulrich Latzenhofer BA
Technischer Experte, Rundfunk und Telekom Regulierungs-GmbH

Dr. Michael Hysek
Bereichsleiter, Finanzmarktaufsicht

Robert Lamprecht
KPMG

Volle Kraft voraus

Cyber Security
auf dem Weg zum
nächsten Level

65%
empfinden den Fachkräftemangel als eine Herausforderung

54%
haben einen Überblick ihre IoT-Geräte

37%
haben ein Customer Identity Access Management-System (CIAM) im Einsatz

57%
planen, auf Machine Learning und KI basierende Sicherheitslösungen einzusetzen

53%
sagen, dass Outsourcing die Sichtbarkeit und Kontrolle von Cyber Security verbessert

Meeresschildkröten können beim Tauchen ihren Stoffwechsel stark herabsetzen und so ihre Beute mit großer Ausdauer jagen.

Emerging Technologies, wie zB Künstliche Intelligenz, IoT oder autonome Systeme, bieten Unternehmen enormes Potenzial für Wachstum. Doch auch die Kehrseite der Medaille ist entscheidend: Die modernen Technologien vergrößern gleichzeitig die Möglichkeiten für Cyberattacken. Cyber Security war daher noch nie so wichtig wie heute und kann für den Erfolg oder Misserfolg eines Unternehmens entscheidend sein. Unternehmen, die derartige Technologien einsetzen, müssen daher die Sicherheitsmaßnahmen entsprechend erhöhen und anpassen.

Back to the roots: CIAM

Obwohl wir in diesem Kapitel von „Emerging Technologies" sprechen, ist der Einstieg in die Materie ein altbekannter. Denn: Eine der wichtigsten Basismaßnahmen für Unternehmen ist es, digitale Identitäten von Kunden, Partnern und Mitarbeitern sicher zu verwalten. Ein sogenanntes „Customer Identity Access Management"-System (CIAM) ist hier das notwendige Werkzeug und eine Herausforderung, die Unternehmen aller Größenordnungen in unterschiedlichen Varianten seit mehr als zehn Jahren beschäftigt: War er früher nur für die eigenen Mitarbeiter von Bedeutung, so erstreckt sich nun der Fokus aufgrund der Digitalisierung auch auf die Customer-Perspektive und so wird aus IAM nun CIAM. Doch bevor CIAM-Basics nicht auf Schiene gebracht sind, ist jede Aktivität von Unternehmen in Richtung Emerging Technologies fahrlässig.

Erschreckend dabei: Nur 37 Prozent der befragten Unternehmen gaben an, ein CIAM im Einsatz zu haben. Besonderen Aufholbedarf haben Familienunternehmen: Nur 20 Prozent haben ein CIAM im Einsatz, wohingegen die Nutzung in großen Unternehmen verhältnismäßig hoch ist (56 Prozent). Ein interessantes Detail am Rande: Alle befragten Start-Ups gaben an, ein CIAM zu verwenden. Ebenso interessant: Nur 30 Prozent der Unternehmen, die bereits Opfer eines Angriffsversuchs waren, verwenden ein CIAM. Hingegen haben mehr als die Hälfte (52 Prozent) der Unternehmen, die noch nicht angegriffen wurden, ein solches Tool im Einsatz.

Der Großteil der befragten Unternehmen verwendet zur Absicherung nach wie vor die klassischen Authentifizierungsmöglichkeiten wie Benutzername/Passwort (43 Prozent) oder Mehrfaktorauthentifizierung (40 Prozent).

Nur 18 Prozent der Unternehmen haben Zertifikate oder Bürgerkarte/Handysignatur im Einsatz. Besonders hoch ist die Akzeptanz von Bürgerkarte/Handysignatur oder Zertifikaten in öffentlichen Unternehmen, bei Dienstleistern und im Healthcare-Bereich mit jeweils 33 Prozent.

Vorreiter in Sachen CIAM sind die Branchen Banken (52 Prozent), Telekommunikation (55 Prozent), Retail (67 Prozent), Healthcare (67 Prozent) und Versicherungen (63 Prozent). Insbesondere Banken, in deren Branche Vertrauen und Sicherheit eine ganz besonders große Rolle spielen, zeigen sich hier vorbildlich. 71 Prozent der Banken setzen bei CIAM Mehrfaktorauthentifizierungen ein, während Versicherungsunternehmen (72 Prozent) und Retail (100 Prozent) nach wie vor an der herkömmlichen Username/Password-Kombination festhalten.

In der Zukunft wird vor allem dem Kunden eine größere Bedeutung zukommen. Das zeigt auch die KPMG Studie „Was Kunden begeistert".

Ein kritischer Blick:
Die Blockchain-Technologie

Die Skepsis gegenüber der Blockchain-Technologie ist in Österreich noch relativ hoch. Dies betrifft insbesondere diverse Einsatzbereiche innerhalb des Unternehmens.

Eine Blockchain wird dabei, vereinfacht ausgedrückt, als ein dezentrales Protokoll für Transaktionen zwischen Parteien definiert, das jede Veränderung transparent erfasst. Ein Großteil der befragten Unternehmen ist nicht der Meinung, dass der Einsatz von Blockchain ein Risiko für das Unternehmen darstellt (69 Prozent).

Doch auch die Chance einer potenziellen Schutzfunktion wird nicht gesehen: Nur fünf Prozent sind bisher überzeugt, dass Blockchains und andere verteilte Datenbanken dabei helfen können, das Unternehmen auch tatsächlich zu schützen.

Große Unternehmen sind hier besonders skeptisch: Mehr als die Hälfte (56 Prozent) der großen Unternehmen glaubt nicht, dass Blockchains beim Schutz des Unternehmens hilfreich sein können. Durchschnittlich waren nur 19 Prozent aller Unternehmen dieser Meinung.

Ein Blick auf die Branchen zeigt: Im Einzelhandelsbereich wird der Technologie mehr zugetraut als überall sonst. 67 Prozent der Unternehmen dieser Branche stimmen der Aussage zu, dass Blockchains und verteilte Datenbanken helfen können, das Unternehmen zu schützen.

Langsamen Schrittes:
Machine Learning und KI

Immer mehr Zuspruch erhält hingegen eine andere moderne Technologie. Im Bereich Machine Learning und Künstliche Intelligenz (KI) überlegen derzeit mehr als die Hälfte (57 Prozent) der österreichischen Unternehmen, darauf basierende Sicherheitslösungen einzusetzen: 18 Prozent wissen bereits sicher, dass sie sich des Themas annehmen werden, 39 Prozent stimmen mit „eher ja" ebenfalls zu. Besonders hoch ist hier der Anteil bei den Einzelunternehmen (80 Prozent) und den Personengesellschaften (68 Prozent).

Die 3 wichtigsten Trends 2016 - 2019

Unternehmen reagieren oftmals zu sorglos im Umgang mit Internet of Things (IoT), sind aber am Weg der Besserung.

Österreichs Unternehmen haben immer weniger Bedenken vor unkontrolliertem Datenverlust bei Cloud-Lösungen.

Auf Künstlicher Intelligenz (KI) basierende Sicherheitslösungen nehmen in Österreich Schritt für Schritt zu.

Praxistipp

Einen Überblick über die eigenen IoT-Systeme zu haben, die Software aktuell zu halten und die Berechtigungen nicht aus den Augen zu verlieren, sind unerlässlich für eine funktionierende Basissicherheit.

„Cybersicherheit ist eine gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft."

Erich Albrechtowitz
Bundeskanzleramt

Nimmt man die einzelnen Branchen detaillierter unter die Lupe zeigt sich: Alle befragten Unternehmen der Automobilbranche (100 Prozent) und der Retailbranche (67 Prozent „ja" bzw 33 Prozent „eher ja") planen den Einsatz von maschinellem Lernen und Künstlicher Intelligenz.

In der Dienstleistungsbranche ist hingegen die Zeit dafür offensichtlich noch nicht reif: Österreichs Unternehmen orten aktuell noch kein Einsatzgebiet für diese Technologien (40 Prozent „nein" bzw 60 Prozent „eher nein").

Mangelndes Vertrauen: Cloudbasierte Lösungen

Skepsis herrscht auch in Hinblick auf cloudbasierte Sicherheitslösungen: 60 Prozent der Unternehmen geben an, cloudbasierte Sicherheitslösungen nur zusätzlich zu ihren eigenen Lösungen einsetzen zu wollen. Auf absoluten Widerstand stößt die Technologie bei 38 Prozent der Unternehmen: Sie verweigern den Einsatz vollkommen.

Eine absolute Ausnahme stellen hier Start-ups dar: Ein Drittel (33 Prozent) der aufstrebenden Newcomer setzt ausschließlich auf cloudbasierte Sicherheitslösungen, ein weiteres Drittel (33 Prozent) hat diese zusätzlich in Gebrauch.

Auch in diesem Bereich kristallisieren sich große Unternehmen als Vorreiter heraus, die neuen Technologien tendenziell aufgeschlossener gegenübertreten: 89 Prozent gaben an, Cloud-Lösungen zu verwenden. Zum Vergleich: 67 Prozent der mittleren und nur 54 Prozent der kleinen Unternehmen haben Cloud-Lösungen im Einsatz. Besonders kritisch gegenüber der Anwendung von cloudbasierten Sicherheitslösungen sind Dienstleistungsunternehmen und der öffentliche Sektor (60 bzw 61 Prozent nutzen diese nicht). Unternehmen aus dem Bereich Retail (100 Prozent), Immobilien (75 Prozent), Telekommunikation (82 Prozent), Versicherung (75 Prozent) und Industrie (85 Prozent) nutzen diese hingegen zusätzlich oder ausschließlich.

Ein klarer Vorteil: Outsourcing an Dritte

Beim Auslagern an Dritte sind Österreichs Unternehmen nach wie vor auf der Hut. Dennoch ist insgesamt ein positiver Trend in Richtung Outsourcing zu erkennen. Unternehmen orten zwischenzeitlich klar die Vorteile: 53 Prozent gaben an, dass sich durch die Auslagerung das Verständnis, die Sichtbarkeit und die Kontrolle von Cyber Security verbessert hat.

Während fast die Hälfte (45 Prozent) der Unternehmen im öffentlichen Bereich keine Auslagerung der Aufgaben planen, haben alle befragten Personengesellschaften bereits teilweise Aufgaben ausgelagert und dabei großteils positive Erfahrungen gemacht: 84 Prozent beurteilen das Outsourcing als Verbesserung.

Start-ups spielen auch hier in einer eigenen Liga: Drei Viertel (75 Prozent) haben Aufgaben ausgelagert und dabei ausschließlich positive Erfahrungen gemacht.

Betrachtet man die einzelnen Branchen genauer, lässt sich auch hier ein Outsourcing Trend erkennen: Alle befragten Unternehmen im Dienstleistungsbereich haben Aufgaben ausgelagert, 80 Prozent davon stufen diese Entwicklung als positiven Beitrag zur Entwicklung der Informationssicherheit im Unternehmen ein.

Auch in den Bereichen Logistik (75 Prozent), Industrie (65 Prozent) und Energiewirtschaft (60 Prozent) überwiegen die durchwegs guten Erfahrungen. Einzig die Unternehmen im öffentlichen Sektor stehen einer Auslagerung überdurchschnittlich skeptisch gegenüber (45 Prozent).

Vernetzte Welt: IoT-Sicherheit im Fokus

Bereits unsere Vorjahresstudie zeigte, dass Unternehmen im Umgang mit Internet of Things (IoT) am Weg der Besserung sind. Trotz oftmals zu sorglosem Umgang ist ein Umdenken deutlich spürbar: So steigerte sich die Zahl jener, die einen Überblick über alle IoT-Geräte im Unternehmen hatten, von 40 (2017) auf 48 (2018) bis hin zu 54 Prozent (2019).

Die diesjährige Studie zeigt: Auf die Basissicherheit von IoT-Geräten wird bei den befragten Unternehmen mittlerweile viel Wert gelegt. 83 Prozent der Unternehmen gaben an, dass die Geräte regelmäßig die neuesten Updates erhalten. 81 Prozent sind der Überzeugung, dass die potenziellen Angriffsflächen wie Devices, Netzwerk und Cloud ausreichend geschützt werden.

Deutlich geringer ist hingegen die Awareness in Bezug auf die Isolierung der Daten von anderen Systemen oder Diensten (62 Prozent) und bei der Kommunikation der „Dos and Don'ts" an die User (65 Prozent).

Nur wenige Unternehmen geben außerdem an zu wissen, welche Daten (33 Prozent) und wie diese Daten (24 Prozent) von den Devices verarbeitet werden. Lediglich bei 37 Prozent der Unternehmen wird die Integrität der verwendeten Software verifiziert.

Under Construction: Fachkräftemangel behindert Sicherheit

Eine immer größer werdende Herausforderung für Unternehmen in Hinblick auf Cybersicherheit ist der Fachkräftemangel: Fast zwei Drittel aller Unternehmen (65 Prozent) empfinden den Fachkräftemangel im Cyber Security-Bereich als eine Herausforderung.

Viele Unternehmen versuchen dieser Herausforderung durch Aus- und Weiterbildung der eigenen Mitarbeiter Herr zu werden: 41 Prozent geben an, ihre Mitarbeiter durch Schulungen für diesen Bereich zu qualifizieren.

Alarmierend hoch ist der Mangel an Cyber Security-Personal im Bereich Automotive und Energiewirtschaft: Alle befragten Unternehmen geben an, dringenden Bedarf an Fachkräften zu haben.

Etwas entspannter sieht die Lage in anderen Branchen aus: Unternehmen im Bereich Dienstleistung (55 Prozent), Healthcare (44 Prozent), öffentlicher Sektor (48 Prozent) und Retail (50 Prozent) geben an, großteils über ausreichend Fachkräfte zu verfügen und die fehlenden durch die Schulung der eigenen Mitarbeiter abdecken zu wollen.

In diesem Bereich sind Unternehmen verstärkt auf der Suche nach Lösungen: Als die effektivste Maßnahme, um den Fachkräftemangel innerhalb der nächsten zwei Jahre zu lösen, sehen viele Unternehmen (36 Prozent) interne und externe Schulungen und Ausbildungen.

Hierbei setzen Unternehmen sowohl auf Kooperationen mit Fachhochschulen und Universitäten, Lehrlingsausbildungen als auch auf relevante Security-Zertifizierungen.

Weitere Maßnahmen aus Sicht der Unternehmen: Einerseits der Aufbau eines dezidierten Security-Teams durch Rekrutierung von geeigneten Mitarbeitern innerhalb und außerhalb der EU, andererseits das Outsourcing in diesem Bereich.

Mag. Susanne Tischmann

Leiterin Technologie
bei ÖAMTC

DI (FH) Christoph Pertl

IT Security Officer
bei ÖAMTC

Der Einsatz von Red-/Blue-/Purple-Teams ist eine sinnvolle Maßnahme, um Sicherheitslücken aufzuspüren, bevor ein externer Dritter diese ausnutzen kann.

Cyberangriffe gehören in Österreich und weltweit mittlerweile zum Daily Business. Wie schätzen Sie den Umgang österreichischer Unternehmen mit diesen Angriffen ein?
Der Umgang mit Cyberrisken ist aus unserer Wahrnehmung als mittelmäßig gut zu bezeichnen. Es werden durchaus Maßnahmen zur Prävention und schnelleren Auffindung gesetzt, allerdings ist im Europavergleich keine Vorreiterrolle zu erkennen. Oder anders ausgedrückt: Das Bewusstsein für Cybersicherheit hat sich in Österreich in den letzten Jahren stark gewandelt, die Alpenrepublik befindet sich auf dem richtigen Weg – doch es besteht kein Anlassfall, sich auf den bisherigen Lorbeeren auszuruhen.

Stellen Sie in den letzten Jahren Veränderungen in der Anzahl und Art der Attacken fest?
Zahlreiche Studien belegen, dass sich die Anzahl der Attacken stetig steigert. Cyberkriminelle agieren 24 Stunden am Tag und 365 Tage im Jahr. Betroffen sind dabei Unternehmen aller Größenordnungen und Branchen. Besonders auffällig aus unserer Sicht ist, dass sich vor allem bei Phishing die Qualität der Anschreiben erheblich professionalisiert hat.

Denken Sie, dass Ihr Unternehmen gut gegen Cyberangriffe gewappnet ist?
Wir als ÖAMTC sind auf einem guten Weg und verfolgen unterschiedliche Maßnahmen, sowohl technologischer als auch organisatorischer Art. Ganz entscheidend in unserer Cyber Security-Strategie ist der Faktor Mensch. Das bedeutet: Wir versuchen mit zahlreichen Aktivitäten die Awareness der Mitarbeiterinnen und Mitarbeiter zu steigern. Denn wie auch die aktuelle KPMG Studie zeigt: Der Großteil der Cyberangriffe nutzt nach wie vor die Gutgläubigkeit der Menschen in Unternehmen aus. Wenn man hier ansetzt, kann man viele Vorfälle verhindern.

Wie gehen Management und Aufsichtsrat mit dem Thema Cyber Security bei Ihnen um?
Das Thema Cybersicherheit hat natürlich auch beim ÖAMTC längst einen wichtigen Platz auf der Agenda der Führungsebene eingenommen. Unser Management weiß, dass es sich dabei um keine reine technische Herausforderung handelt, sondern um eines der größten Risiken für Unternehmen, das strategisch und gezielt bearbeitet werden muss. Diverse Cyber Security-Themen werden sinnvoll mitgetragen und budgetäre Mittel zur Verfügung gestellt. Es existiert eine Gruppe, inklusive CEO, in der zyklisch die aktuellen Themen vorgestellt und besprochen werden.

Erwarten Sie sich von der Umsetzung des NIS-Gesetzes Veränderungen?
Die Umsetzung des Gesetzes wird definitiv dafür sorgen, dass Unternehmen und Behörden dem Thema Cybersicherheit gegenüber mit noch mehr Professionalität und Awareness auftreten. Das ist aus unserer Sicht eine sehr positive Entwicklung, denn im Kampf gegen Cyberkriminelle dürfen Unternehmen nie unachtsam sein. Durch das Gesetz wird sich auch der Umgang mit Vorfällen verbessern.

Welche Rolle soll der Staat/die EU generell in Bezug auf Cyber Security in Zukunft übernehmen? Geht es um die Sicherung von Mindeststandards oder sogar um Einfuhrbeschränkungen für unsichere Produkte?
Eine Einfuhrbeschränkung für unsichere Produkte ist schwer bis nicht umsetzbar. Allerdings sollten weltweit übergreifende Standards verhandelt und umgesetzt werden und die entsprechenden Strafverfolgungen auch in internationaler Zusammenarbeit umgesetzt werden.

Sind in Ihrem Unternehmen die Cyber Security-Risiken Teil des Risikomanagement-Framework?
Ja. Das effektive Management von operationellen Risiken gewinnt eine immer größere Bedeutung, nicht nur in stark regulierten Branchen wie Banken und Versicherungen.

Haben Sie Sicherheitsbedenken gegenüber Cloud Computing?
Einerseits bietet Cloud Computing enorme Chancen für Unternehmen aller Branchen, insbesondere in puncto Verfügbarkeit der IT-Infrastruktur, Leistungsfähigkeit, Aktualität und Reaktionsgeschwindigkeit. Doch die Sicherheitsbedenken bleiben auch aus unserer Sicht die größte Hürde. Die Hauptrisken liegen in der Gemeinsamkeit der Cloud-Technologien und darin, dass Angriffe viel breiter wirken können.

Haben Sie Red-/Blue-/Purple-Teams beauftragt und warum?
Der Einsatz von Red-/Blue-/Purple-Teams ist bei uns aktuell in Planung. Solche Teams sind eine sinnvolle Maßnahme, um Sicherheitslücken aufzuspüren, bevor ein externer Dritter diese ausnutzen kann. Gleichzeitig können Cybervorfälle geübt werden und man kann sich strategisch auf den Fall des Falles vorbereiten.

In welcher Frequenz sollte so eine Prüfung Ihrer Meinung nach wiederholt werden?
Wie bei Brandschutzübungen sollten derartige Prüfungen alle ein bis spätestens zwei Jahre wiederholt werden.

Es kann nicht mehr alles abgeschottet werden. Die Bedrohungen müssen in Echtzeit erkannt und Gegenmaßnahmen eingeleitet werden.

Welches sind die Risiken, mit denen Unternehmen im Bereich Cyber Security umgehen müssen?
Die R-IT hat eine Umfeldanalyse der aktuellen Bedrohungen unter Einbeziehung von Best Practices wie CIS oder ENISA und externer Beratung erstellt. Der Fokus als Service Provider im Finanzdienstleistungsbereich spielgelt sich für uns auch bei den identifizierten Risiken wider. Die drei wesentlichsten Risiken sind demnach: Dataloss/Databreach, Advanced Persistent Threat und Unmanaged Systems.

Welche Basispräventionsmaßnahmen gegen übliche Cyberangriffe empfehlen Sie?
Ganz entscheidend sind Tools zur frühzeitigen Erkennung und Alarmierung im Fall eines Angriffs sowie ein erweiterter Distributed Denial of Service-Attackenschutz wie zB Srubbing Center. Nicht vergessen werden darf auf Advanced Threat Protection und das so wichtige Thema Awareness Building.

Welche Präventionsmaßnahmen sind bei neuen, unbekannten Angriffen empfehlenswert?
Die Schaffung eines Rahmens, damit der Paradigmenwechsel im Bereich Security möglich wird, ist von essenzieller Bedeutung. Denn: Es kann nicht mehr alles abgeschottet werden, die Bedrohungen müssen in Echtzeit erkannt und Gegenmaßnahmen eingeleitet werden. Hilfreich dabei sind Machine Learning und Deep Learning. Empfehlenswert ist auch ein Sensornetzwerk zum Ableiten von neuen Indicators of Compromise.

Warum sind Key Performance Indicators wichtig, um die Effektivität von Cyber Security zu messen?
Durch den Einsatz von KPIs werden komplexe Verfahren innerhalb der Cyberabwehr transparent und messbar gemacht. Das Top-Management erhält einen Überblick über die wesentlichen Sicherheitsthemen und ein aktives Steuerungsinstrument. Idealerweise fließen die wesentlichsten KPIs auch in die Balanced Score Card des Unternehmens ein.

Aus meiner Sicht sind folgende KPIs entscheidend: Vulnerability Management, Compliance Management, Awareness, Security Incidents, Testing sowie Indicators of Compromise.

Wie hat sich das Inkrafttreten der DSGVO auf die Cyber Security Ihres Unternehmens ausgewirkt?
Die Auswirkungen der Implementierung hielten sich für die R-IT in Grenzen. Durch die Erhebung der notwendigen Inhalte für das Verarbeitungs- und das Auftraggeberverzeichnis wurden alle Lieferanten und Kunden durchgehend geprüft und auf ein einheitliches Vertragsniveau gehoben. Die DSGVO Implementierung hatte eine überwiegend positive Auswirkung auf das Unternehmen.

Wie wird das NIS-Gesetz den Umgang der Unternehmen mit Cybergefahren verändern?
Aufgrund der Tatsache, dass sich das NIS-Gesetz an bestehende Vorgaben im Meldewesen hält, erwarten wir für unser Unternehmen nur unwesentliche Änderungen. Die R-IT unterstützt ihre Partner aktuell bereits bei PSD II-, ÖNB- und EZB-Meldungen. Die bestehenden Mechanismen werden auch für die NIS-Meldung, wie im Gesetz verankert, herangezogen.

Wie gehen Management und Aufsichtsrat mit dem Thema Cyber Security in Ihrem Unternehmen um?
Das Thema Cybersicherheit hat es längst auf die Agenda des Top-Managements geschafft. IT ist außerdem ein nicht wesentliches Element im täglichen Geschäftsablauf unserer Kunden, die R-IT ist Teil der kritischen Infrastruktur in Österreich geworden. Das Top-Management erhält regelmäßig Informationen zu aktuellen Sicherheitsrisiken: durch Jour Fixes mit der Geschäftsführung, Vorträge, Schulungen und die Behandlung der Sicherheitsthemen im Aufsichtsrat.

Was empfehlen Sie Unternehmen, die ihre IT Security-Strategie ausweiten möchte?
Unverzichtbar ist die notwendige Unterstützung des Top-Managements. Zu Beginn steht eine Analyse des Status quo, basierend darauf sollten entsprechende Maßnahmen abgeleitet werden. Damit wesentliche Aspekte nicht außer Acht gelassen werden, muss mit den Stakeholdern das Security Ambition Level definiert werden. Nur so erreicht man eine eindeutige Zielsetzung. Auch eine Analyse der IT Security-Strategie mit externen Sicherheitsexperten ist oft sinnvoll.

Welche Veränderungen sehen Sie in den nächsten fünf Jahren in Bezug auf IoT und Sicherheit?
In den nächsten fünf Jahren werden die Grenzen der IoT-Geräte verschwimmen. Die größten Herausforderungen sind Hardening, Idendity und Access Management, Patching und Verfügbarkeit. Denn die Systeme entsprechen häufig nicht dem klassischen IT-Operating Security Life Cycle. Der Grund: Viele Hersteller verzichten aus Kostengründen auf diese notwendigen Rahmenbedingungen. Langfristig müssen durch zentrale öffentliche Stellen Vorgaben definiert werden, damit wir diesem Umstand gemeinsam entgegenwirken können.

Haben Sie bereits einmal ein Red-/Blue-/Purple-Team beauftragt?
Ja. Als Vorbereitung auf das kommende TIBER-EU Framework sollte jedes betroffene Unternehmen im Eigeninteresse derartige Tests beauftragen. Wir als R-IT beschäftigen seit Jahren interne Security-Analysten, die uns in dem Bereich „Testing“ unterstützen.

Othmar Schöller

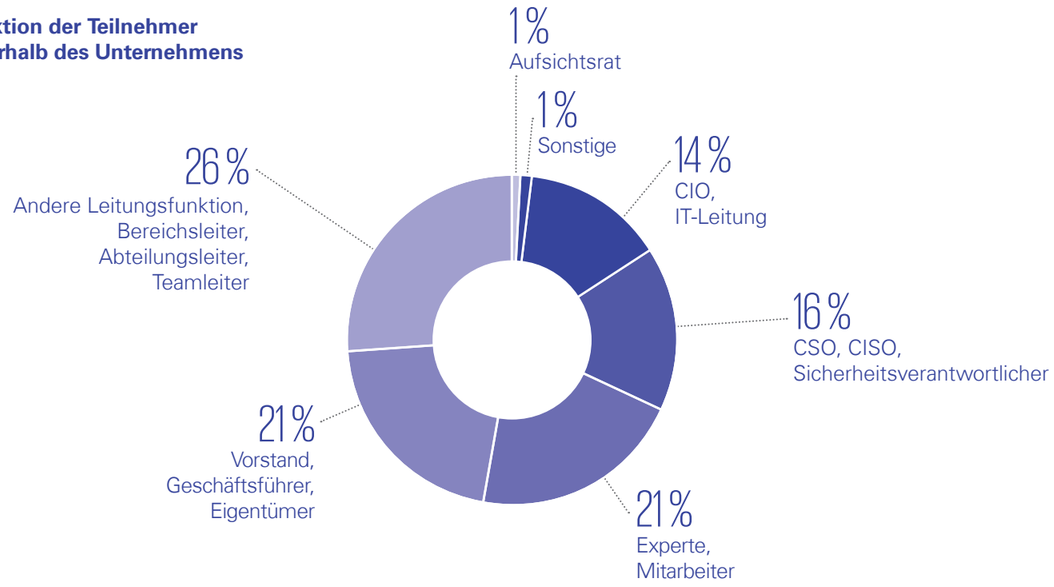
Chief Security Officer
bei Raiffeisen Informatik

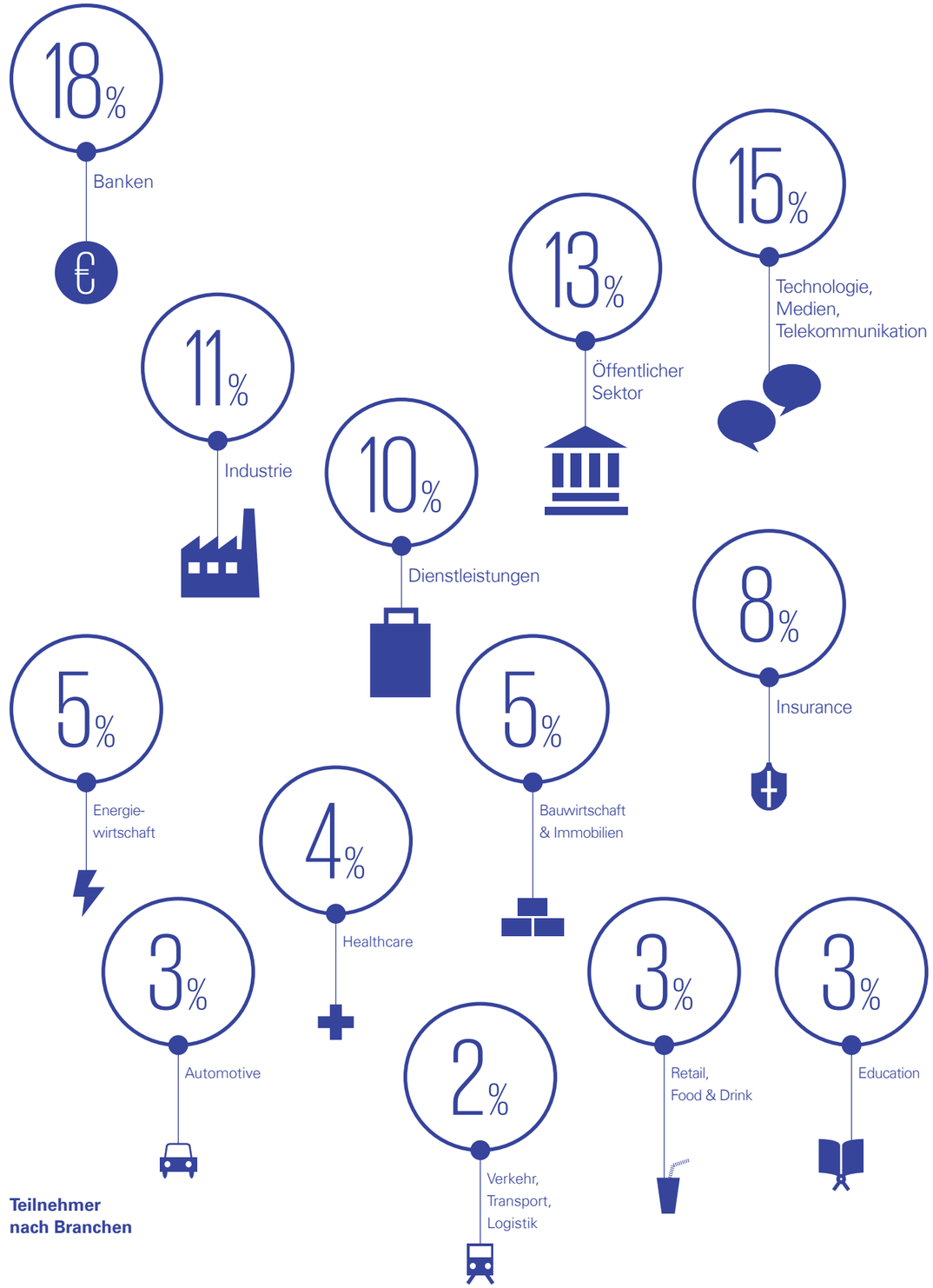
Umfragemethode

Die vorliegende KPMG Studie beschäftigt sich mit der Frage, wie österreichische Unternehmen den neuen Herausforderungen der Cyberkriminalität begegnen und welche Cyber Security-Maßnahmen getroffen werden. Die Umfrage zur Studie wurde im Februar und März 2019 unter 342 österreichischen Unternehmen von KPMG durchgeführt. Die Teilnehmer setzten sich aus kleinen und mittleren Unternehmen sowie Großunternehmen aus den Branchen Banken, Technologie, Medien & Telekommunikation, Öffentlicher Sektor, Industrie, Dienstleistung, Insurance, Energiewirtschaft, Bauwirtschaft & Immobilien, Healthcare, Automotive, Retail, Food & Drink, Education und Verkehr, Transport, Logistik zusammen.

Jeder Teilnehmer erhielt, seiner Funktion im Unternehmen entsprechend, einen Online-Fragebogen mit spezifischen Fragen. Für die Befragung wurde zwischen Innensicht/Leitungsebene (Experten, Bereichsleiter, CSO etc) und Außensicht/Steuerungsebene (Vorstand, Eigentümer, Aufsichtsrat) unterschieden. Die Ergebnisse wurden von einem KPMG Cyber Security-Expertenteam aus dem Bereich IT-Advisory ausgewertet. In persönlichen Interviews standen außerdem sieben Wirtschaftsvertreter und Cyber Security-Experten zum Thema Rede und Antwort. Bei zwei Round Tables diskutierten Vertreter von KPMG und dem KSÖ mit Expertenrunden über die Chancen und Herausforderungen hinsichtlich Cyber Security für den Wirtschaftsstandort Österreich.

Funktion der Teilnehmer innerhalb des Unternehmens





Teilnehmer nach Branchen

Kuratorium Sicheres Österreich

Das Kuratorium Sicheres Österreich (KSÖ) befasst sich seit seiner Gründung im Jahr 1975 mit Themen der inneren Sicherheit.

Im Jahr 2011 wurde das Themenspektrum um den Bereich der Cyber Security erweitert, indem gemeinsam mit dem Innenministerium eine „Cyber Security Initiative" ins Leben gerufen wurde. Das erste Produkt dieser Initiative war die Erstellung einer Cyber Security Risikomatrix.

KURATORIUM SICHERES ÖSTERREICH

Sicherheitsforum
Digitale Wirtschaft
Österreich

Diese Risikomatrix sollte eine gemeinsame Sicht von Wirtschaft, Behörden und Wissenschaft auf die damals wesentlichen Herausforderungen für Staat und Wirtschaft darstellen. Sie unterschied sich damit von Beginn an durch einen breiten, gesamtstaatlichen Ansatz, der sowohl technische Bedrohungen wie DDoS-Angriffe als auch (wirtschafts-)politische Themen wie die Abhängigkeit von ausländischen Sicherheitstechnologien beinhaltete.

Zum damaligen Zeitpunkt war das Thema Cyber Security immer noch ein Expertenthema. Edward Snowden war noch niemandem ein Begriff und exponentielle Entwicklungen wie Künstliche Intelligenz und das Internet of Things eine Zukunftsvision. Die Erstellung einer staatlich-privaten Cyber Security Risikomatrix war daher ungewöhnlich und aus dem gleichen Grund dringend notwendig. Denn schon damals zeigte sich, dass Cybersicherheit nicht nur ein technisches Thema war, sondern vor allem ein strategisches.

Blick auf 2011 und 2016

Fünf Jahre später, im Jahr 2016, erstellte das KSÖ diese Risikomatrix erneut und es zeigte sich, dass manche Risiken weiterhin unbehandelt bestanden – wie zB das mangelnde Sicherheitsbewusstsein. Als Ergänzung zur Risikomatrix von 2011 wurde 2016 auch abgefragt, wie sehr Staat und Wirtschaft auf die Risiken vorbereitet waren.

Damit konnte beispielsweise aufgezeigt werden, dass DDoS-Angriffe weiterhin ein Risiko darstellten, die IT Security-Industrie aber in der Zwischenzeit Maßnahmen entwickelt hatte, um mit diesem Risiko umgehen zu können. Da diese Maßnahmen aber nicht flächendeckend eingesetzt wurden, war das Risiko nicht vollständig eliminiert.

Da das Tempo der Digitalisierung einer exponentiellen Entwicklung entspricht, war es auch in kürzerem Abstand notwendig, die Cyber Security Risikomatrix zu erneuern.

Und so kontaktierte das KSÖ im Jahr 2019 erneut Experten aus unterschiedlichen Sektoren, um die Veränderungen der Risiken seit 2016 abzufragen. Die Methodik wurde großteils beibehalten und auch die Risiken wurde nur geringfügig den aktuellen Gegebenheiten angepasst. Dies sollte sicherstellen, dass die Entwicklung der Risiken seit 2011 in weiten Teilen nachverfolgbar blieb.

Wesentliche Erkenntnisse aus 2019

Die Cyber Security Risikomatrix 2019 zeigt einige sehr interessante Unterschiede zur Matrix von 2016. So ist das größte Risiko von 2016, die Abhängigkeit von ausländischen Sicherheitstechnologien, von der Spitze in das Mittelfeld gerückt. Als neues Top-Risiko werden staatliche und staatlich unterstützte Cyberangriffe gesehen, knapp gefolgt von fehlendem Fachpersonal bzw Sicherheitsexperten.

Cyberkriminalität ist im Vergleich zu 2016 in Bezug auf die Risikoeinschätzung fast unverändert geblieben. Das gleiche gilt auch für das mangelnde Sicherheitsbewusstsein seitens der Mitarbeiter, unsichere IoT-Systeme und fehlerhafte Software. Deutlich gesteigert hat sich das Risiko der Abhängigkeit von Cloud-Providern, was mit hoher Wahrscheinlichkeit auf die in den letzten Jahren ebenfalls immer häufigere Nutzung von Cloud-Diensten zurückzuführen ist.

Stark reduziert hat sich das Risiko, das von DDoS-Angriffen ausgeht. Etwas weniger stark aber immer noch verbessert hat sich das Empfinden in Bezug auf unklare Kompetenzlagen bei den Behörden. Dies kann eine direkte Auswirkung des Inkrafttretens des NIS-Gesetzes sein. Gespannt darf man sein, wie sich dieses Risiko bei der nächsten Risikomatrix verändert, wenn das Gesetz ausreichend Zeit hatte, um seine Wirkung zu entfalten.

Schlussfolgerungen

Auch wenn bereits 2016 durch die Snowden-Enthüllungen bekannt wurde, dass Staaten durch ihre Nachrichtendienste aktiv zu Cyberrisiken beitragen, so scheint sich dieses Empfinden 2019 nochmal gesteigert zu haben. Staatliche und staatlich unterstützte Cyberangriffe werden als genauso wahrscheinlich aber von ihrer Wirkung her als bedrohlicher angesehen als Cyberkriminalität.

In Verbindung mit dem ebenfalls als hochriskant angesehenen Fachkräftemangel hat die Wirtschaft, laut den Ergebnissen der Matrix, diesem Risiko noch nicht genug entgegenzusetzen – was sich auch in dem ebenfalls hoch bewerteten Risiko der mangelnden Erkennung von Angriffen durch Unternehmen bestätigt zeigt.

Die Bedrohungslandschaft ist seit 2016 also komplexer geworden. Das Kuratorium Sicheres Österreich begegnet diesem Trend seit langem durch die Vernetzung von Experten aus Staat, Wirtschaft und Wissenschaft.

Wesentliches Element dabei ist das Sicherheitsforum Digitale Wirtschaft, an dem wesentliche Vertreter der österreichischen Wirtschaft teilnehmen. Das Sicherheitsforum hat sich zum Ziel gesetzt, die Digitalisierung durch einen Fokus auf das Thema Sicherheit dauerhaft nutzbar zu machen – nach dem Motto „Digitalisierung – ja, aber sicher!"

www.kuratorium-sicheres-oesterreich.at

KSÖ Cyber Security Risikomatrix 2019

Die KSÖ Cyber Security Risikomatrix 2019 zeigt die von Vertretern von Behörden, Wirtschaft und Wissenschaft interpretierte Landschaft an strategischen und technischen Cyber Security-Risiken. Wesentlichste Risiken sind staatliche Angriffe und der akute Fachkräftemangel auf staatlicher und privatwirtschaftlicher Seite.

Gemeinsam Zukunft schreiben

Unternehmerische Zukunft sichern

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

Orientiert an den Geschäftszielen

Gemeinsam mit Ihnen wollen wir Ihr Unternehmen im Zeitalter der Digitalisierung voranbringen. Der positive Umgang mit Cyberrisiken hilft Ihnen nicht nur die Unsicherheit in Ihrem Unternehmen unter Kontrolle zu bringen. Sie können daraus auch einen echten strategischen Vorteil ziehen und sich im Digitalisierungs-wettrennen in das Spitzenfeld bringen.

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 in der 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 Zusammenarbeit und Begleitung beraten und fordern wir Sie, damit Sie die richtigen Entscheidungen treffen können – und zwar mit begründeter Zuversicht.

KPMG

Impressum

Cyber Security in Österreich

Herausgeber
KPMG Security Services GmbH

Für den Inhalt verantwortlich:
Michael Schirmbrand
M +43 664 816 09 69
mschirmbrand@kpmg.at

Andreas Tomek
M +43 664 816 09 95
atomek@kpmg.at

Gert Weidinger
M +43 664 304 60 11
gweidinger@kpmg.at

Fachliche Studienleitung:
Robert Lamprecht
M +43 664 816 12 32
rlamprecht@kpmg.at

Grafik und Satz:
Heidemarie Schalk
T +43 1 313 32-3960
hschalk@kpmg.at

Druck:
Ferdinand Berger & Söhne GmbH

KURATORIUM SICHERES ÖSTERREICH

Sicherheitsforum
Digitale Wirtschaft
Österreich

Die Studie wurde in Kooperation mit dem Sicherheitsforum Digitale Wirtschaft des Kuratorium Sicheres Österreich (KSÖ) durchgeführt. Das Sicherheitsforum Digitale Wirtschaft Österreich ist die Arbeitsplattform, wo Wirtschaft, Forschung und Behörden gemeinsam Verantwortung übernehmen und ihren Beitrag zur sicheren Digitalisierung leisten.