Cyber Security in Österreich

Studie
IT Advisory

Mai 2022

Österreichs Unternehmen
in einer Welt voller
Abenteuer

Sicherheitsforum
Digitale Wirtschaft
Österreich

kpmg.at/cyber

Welt voller Abenteuer

»Unternehmen müssen längst überfällige Hausaufgaben dringend abarbeiten.«

Michael Schirmbrand
KPMG Partner

Andreas Tomek
KPMG Partner

Gert Weidinger
KPMG Partner

Wir agieren in einer Umgebung unglaublicher Herausforderungen: von vorhersehbaren Entwicklungen wie Artificial Intelligence, Machine Learning und Digitalisierung – bis hin zu nahezu unvorstellbaren Wendepunkten wie der globalen Pandemie oder zwischenstaatlichen Konflikten und Kriegen. All das hat nicht nur Auswirkungen auf unseren Lebensalltag, sondern auch auf unser Cyber Security-Gefüge.

Auf neuem Kurs

Diese Entwicklungen zwingen Unternehmen dazu, ihre Reiseroute durch den ohnehin aufregenden Cyber Security-Ozean abzuändern. Sie müssen umdenken und sich neu organisieren. Die Meeresschildkröte begleitet uns ganz bewusst grafisch durch die aktuelle Ausgabe unserer Cyber Security Studie 2022. Denn das Reptil hat im Laufe der Geschichte so einiges überstanden: Meteoriteneinschläge, Naturkatastrophen und Eiszeiten. Seit Millionen von Jahren passt sich das Tier an veränderte Rahmenbedingungen an, trotzt allen Widrigkeiten und stürzt sich täglich in ein Meer voller Abenteuer.

Gegen die Strömung

Unser Ziel ist und bleibt die Cyberresilienz. Suchen wir gemeinsam nach strategischen Antworten auf neue Security-Fragestellungen. Vergessen wir dabei aber auch nicht, Antworten auf alte Fragestellungen zu liefern. Denn einerseits vollziehen Unternehmen gerade einen Paradigmenwechsel in Sachen Cyber Security – beschleunigt unter anderem durch die Cloud – andererseits müssen sie längst überfällige „Hausaufgaben" – Stichwort Basishygiene – dringend abarbeiten.

Bereits zum siebten Mal veröffentlicht KPMG die Studie „Cyber Security in Österreich" gemeinsam mit dem Sicherheitsforum Digitale Wirtschaft des Kompetenzzentrum Sicheres Österreich. Die Studie bietet aktuelle Zahlen unserer Umfrage, an der sich rund 550 österreichische Unternehmen beteiligt haben. Gleichzeitig gibt sie einen umfassenden Überblick über aktuelle Trends und neue Abenteuer!

Wir wünschen Ihnen eine spannende Lektüre. Sollten Fragen offenbleiben, melden Sie sich gerne. Wir freuen uns von Ihnen zu hören!

Erwin Hameseder
KSÖ-Präsident

Die Entwicklungen der vergangenen zwei Jahre haben uns in dramatischer Weise die Verwundbarkeit unserer staatlichen, wirtschaftlichen und gesellschaftlichen Systeme vor Augen geführt. Die Kombination aus Pandemie, Terrorangriffen und einem realen Krieg in Europa machen uns einerseits menschlich betroffen, zeigen uns aber auch deutlich, dass Gesundheit, Wohlstand und Sicherheit im 21. Jahrhundert bei weitem nicht selbstverständlich sind.

Die durch die weltweite Covid-Pandemie beschleunigte Digitalisierung hat gerade in Zusammenhang mit Cyberkriminalität für eine neue Dynamik gesorgt. Ein Anstieg von Cyberangriffen und immer neue Angriffsvektoren setzen uns vor neue Herausforderungen, die nicht isoliert von einer Stelle alleine – weder vom Staat noch der Wirtschaft – gelöst werden können. Vielmehr braucht es eine gesamthafte Strategie und die Kooperation aller beteiligten Akteure. Genau hier setzt das KSÖ – früher „Kuratorium Sicheres Österreich", heute „Kompetenzzentrum Sicheres Österreich" an. Das KSÖ verbindet Wirtschaft, Wissenschaft, Verwaltung und Politik und steht als gemeinnützige Stakeholder-Plattform genau für diesen Anspruch.

Bereits zum siebten Mal erscheint eine breit angelegte Studie „Cyber Security in Österreich", die das KSÖ von Anbeginn gemeinsam mit KPMG durchführt. Einige Ergebnisse und Entwicklungen aus der aktuellen Studie möchte ich besonders hervorheben:

Erstens den Anstieg der Cyberangriffe durch vermutete staatliche Akteure. Cyberangriffe sind heute Teil des Repertoires staatlicher Aggression beziehungsweise staatlicher Handlungsoptionen geworden.

Zweitens bestätigt sich für mich ein zentrales Verständnis von Cyber Security: Cyber Security ist nicht nur ein Thema für Techniker und IT-Spezialisten, vielmehr brauchen Unternehmen eine ganzheitliche Vorgangsweise – von der technischen Komponente über Entscheidungs- und Informationsprozesse bis zur Awareness der MitarbeiterInnen.

Drittens weist die Studie auf eine weitere – große – Herausforderung für Wirtschaft wie Staat hin. Drei Viertel der Unternehmen haben Schwierigkeiten beim Rekrutieren von IT-Experten. Wir haben daher im Rahmen des KSÖ-Sicherheitsforums Digitale Wirtschaft gemeinsam mit Arbeitsminister Univ. Prof. Dr. Kocher einen Prozess initiiert, wo wir ausgehend von den Anforderungen und Bedarfslagen der Unternehmen Strategien zur Bekämpfung des Fachkräftemangels erarbeiten. Zudem steht das KSÖ-Arbeitsjahr 2022 unter anderem unter dem Thema „Digitale Fachkräfte". Wir wollen – begleitet von einer neuen KSÖ-Akademie – konkrete Qualifizierungsangebote bündeln, bzw neu ausrichten und mit dem Bedarf von Staat und Unternehmen abgleichen.

Angesichts dieser neuen Entwicklungen muss uns allen klar sein, dass Cyber Security aktueller denn je ist. Lesen Sie die vorliegende Studie, um sich zu informieren, nutzen Sie uns als Plattform, um sich bezüglich Maßnahmen zu vernetzen. Denn Cyber Security geht uns alle an.

Mag. Erwin Hameseder
Präsident, Kompetenzzentrum Sicheres Österreich

Inhalt

Interviewpartner
Gerhard Karner
Sönke Marahrens
Pascal Lamia
Björn Stahlhut
Matthias Wasinger
Sabine Herlitschka
Raphael Otto
Gerald Kortschak
Stanislava Saria

Round Table
Philipp Amann &
Wolfgang Rosenkranz

Auf stürmischer See

Unser Cyber Security-Umfeld ändert sich rasend schnell. Verlassen kann man sich dabei lediglich auf eines: die rücksichtslosen Attacken der Cyber-Kriminellen. Wohin die Reise gehen wird? Das weiß keiner ganz genau. Nur, dass wir alle mitschwimmen müssen – egal, ob großer Branchen-Fisch oder kleiner Meeresbewohner.

Robert Lamprecht
KPMG Director

Im Cyber-Ozean jagt ein Abenteuer das nächste. Die meisten Unternehmen fürchten die hohe See, sie sind auf der Suche nach einer sicheren Küste. Doch einfach abzutauchen und die Augen vor dem Sturm zu verschließen, geht nicht. Im Gegenteil: Das Tempo, mit dem der peitschende Ozean seine Strömungen ändert, verlangt einen neuen Cyber Security-Stil von Unternehmen: Angriffsflächen reduzieren, die wichtigsten operativen Prozesse im Unternehmen definieren und schützen und vor allem eines: handlungsfähig bleiben. Sowohl bei Angriffen als auch im Tagesgeschäft. Einige Entwicklungen im Überblick.

Konfliktherd Cyberspace: Schadsoftware bedroht Unternehmen

Der Ukraine-Russland-Konflikt macht sichtbar, was bisher nur Cyber Security-Experten am Radar hatten: Politische Spannungen werden auch virtuell ausgetragen. Anders ausgedrückt: Zwischenstaatliche Konflikte und Kriege finden ebenso im Cyberspace statt. Tendenz: steigend. Denn Nationalstaaten wollen zunehmend Kontrolle über „ihren" Cyberspace ausüben und nutzen den Raum des Gegners als Angriffsziel. Die staatlich geduldete oder gar unterstützte zielgerichtete Cyberkriminalität verstärkt sich – mit drastischen Folgen für Unternehmen und Gesellschaft – diplomatisch, sozial, wirtschaftlich. So werden etwa Unternehmen die Ausläufer zerstörerischer Schadsoftware zu spüren bekommen, die ursprünglich zur Austragung eines Konfliktes entwickelt wurde – ein aktuelles Beispiel: Wiper-Malware auf ukrainischen Computersystemen. Denn Malware ist nie vollständig unter Kontrolle zu halten und kann massiven Schaden quer über die Erdkugel verursachen. Dieser Krieg wird also vor allem jenen schaden, die sich bisher nicht gegen Cyberattacken geschützt haben.

Ransomware: Der Kokainhandel des 21. Jahrhunderts

Eine Szene professionalisiert sich und wird zum Schreckgespenst. Dahinter stecken nicht nur kriminelle Gruppierungen. Sogar Staaten versuchen immer öfter mithilfe von Ransomware-Angriffen an Devisen zu kommen, zB wenn sie einem Handelsembargo unterliegen. Geschätzte 60 Prozent der Attacken entstammen der Kategorie Ransomware as a Service, 20 Prozent von Ransomware-Gruppen wie Maze, Conti oder REvil, die restlichen 20 Prozent sind schwer zuzuordnen. Die Erpressungstaktiken werden immer ausgefeilter. Es entwickelt sich ein eigenes und sehr lukratives Wirtschaftssystem auf der „dunklen Seite". Die Cyber-Kriminellen haben klare Ziele: mit Ransomware-Attacken Systeme automatisiert zu verschlüsseln, Online-Backups zu zerstören und Organisationen zu erpressen. Die Folgereaktionen: Versicherer reduzieren ihr Portfoliorisiko angesichts der steigenden Kosten für die Zahlung von Lösegeldern. Regierungen stufen Cyberkriminalität als enorme Bedrohung für die nationale Sicherheit ein. Diskussionen über den Stopp der Verwendung von Kryptowährungen für die Auszahlung der Lösegelder werden lauter. Debatten darüber, ob die Zahlung von Lösegeld illegal werden soll, nehmen Fahrt auf. Der Frust über Länder, die solchen Gruppen Unterschlupf bieten, wird intensiver. Kurz gesagt: Es brodelt an allen Ecken und Enden.

Immer wieder die alte Leier: „Get the basics right"

Viele Unternehmen haben die „Sonntagspredigt" wohl schon satt – doch es hilft nichts. Wir werden nie darum herumkommen, unsere Basis-Hausaufgaben sorgfältig zu erledigen – Asset Management, Identitäts- und Zugangskontrolle, Protokollierung, etc. Denn Cyberbedrohungen sind Teil der Digitalisierung – durch Ignorieren verschwinden sie definitiv nicht. Ein entscheidender Teil der Cyber Security wird immer – heute und in Zukunft – darin bestehen, die Grundlagen auf standardisierte Weise umzusetzen. KI und Automatisierung werden einen großen Teil der manuellen Arbeit bei der Installation und Überwachung zukünftig überflüssig machen. Doch mangelnde Disziplin in diesen Bereichen ist und bleibt eine der Hauptquellen unserer Cyber Security-Probleme. Das Thema bekommt durch eine Entwicklung noch mehr Bedeutung: Der Großteil der IT-Umgebung befindet sich bereits heute außerhalb des Firmengebäudes. Denn die IT im eigenen Haus ist fast schon zum Relikt vergangener Tage geworden. Dieser Prozess beschleunigt sich durch die Umstellung auf hybrides Arbeiten und den rasanten Übergang zu Cloud-Diensten.

Eine Sisyphos-Arbeit: Schnell versus sicher in der Technologie

Die Geschwindigkeit der Digitalisierung wird zur Herausforderung: Das Rad dreht sich so schnell, dass es unmöglich wird, den seit Jahren aufgebauten Sicherheitsrückstand („technical debt") aufzuholen. Eine alte Bringschuld holt uns dabei ein: die Hersteller-Frage. Sicherheit müsste längst verpflichtend von Anfang an bei der Entwicklung mitgedacht werden. Nur so kann man Unternehmen so unempfindlich wie möglich gegen Angriffe machen. Die Realität sieht leider anders aus: Das nachträgliche Aufspüren von Sicherheitslücken und das Flicken derselben bleibt Mainstream. Anders gesagt: Wir müssen Schiffe bauen, die am Cyber-Ozean nicht untergehen können. Bisher liefern wir Schiffe aus und setzen erst dann Maßnahmen, damit möglichst wenige davon verloren gehen. Ähnliches gilt für die Sicherheit der Lieferkette – Schlagworte: Supply Chain und Third Party Risk Management. Hier sollte die Devise „Vertraue niemandem, kontrolliere alles" längst Standard in allen Bereichen sein. Außerdem muss der Austausch über Angriffe noch viel intensiver

»Die Cyber Security-Konzepte der Zukunft müssen sich klar auf ein Thema konzentrieren: Cyberresilienz.«

Robert Lamprecht

werden, ohne falsche Scham und ohne Grenzen Denn wir wissen immer noch zu wenig darüber, was gerade im Cyberspace passiert. All das erfordert viel mehr Aufmerksamkeit, um die Angriffsfläche der Unternehmen zu reduzieren.

Das Damoklesschwert: Cybersicherheit am Ende?

Eine neue Sorge macht sich angesichts dieser Tendenzen bedrohlich am Horizont breit: Ein mögliches Versagen der Cyber Security. Immer mehr Experten sind der Überzeugung, dass die digitalen Entwicklungen die Welt in den nächsten Jahren auf eine extrem harte Probe stellen werden: Neue Technologien, die zum Angriff genutzt werden können, die zum Teil überstürzte, jedenfalls aber schlagartige Digitalisierung vieler Bereiche, geopolitische Spannungen und ihr „Stellvertreterkrieg" im Cyberspace, die vorhin genannten Ransomware-Attacken und ihre besorgniserregenden Auswirkungen. Das alles beeinflusst den Betriebsalltag der Unternehmen enorm. Die Cyber Security-Konzepte der Zukunft werden sich deshalb klar auf ein Thema konzentrieren: Cyberresilienz. Widerstandsfähigkeit muss das Ziel jeder Organisation werden. Unternehmen erkennen, dass sie sich nicht gegen alles schützen können. Es braucht eine strategische Selektion: Welche meiner Bereiche garantieren meine Handlungsfähigkeit? Wie schütze ich sie bestmöglich? Und: Wie kann ich sie im Fall des Falles möglichst schnell wieder herstellen, ohne viel Zeit zu verlieren?

Eine Reise, die sich lohnt

Wir leben also in einer Welt voller neuer Cyber Security-Abenteuer. Das meiste klingt düster – wie kommen wir nun auf die helle Seite der See? Nehmen wir die Meeresschildkröte in unserer Studie mit auf eine abenteuerliche Reise. Sie ist nicht nur bildlicher Wegbegleiter, sondern auch Vorbild: Anpassungsfähig, schnell, gepanzert und mit allen Sinnen ausgestattet, die sie zum Urgestein der Tierwelt werden hat lassen.

Auch Unternehmen können es schaffen, sich an die rauen Cyber Security-Gegebenheiten anzupassen, den Umständen bestmöglich zu trotzen und allen voran handlungsfähig zu bleiben. Dabei helfen ein stabiler Schutzpanzer durch moderne Technologie (der „sechste Sinn"), schnelles Handeln durch die Menschen im Unternehmen und ein stetiges Mitwachsen und Umdenken der Organisation selbst. Und vor allem eines: das Lernen von anderen. Dazu soll diese Studie etwas beitragen.

The Dark side of Digitalization

Stefan Fink
ist KPMG Chief Economist und Professor für Finanz- und Risikomanagement an der FH OÖ Campus Steyr

Die Palette an volkswirtschaftlichen Risikofaktoren befindet sich, vor allem seit Ausbruch der COVID-Pandemie im März 2020, in einem Prozess der stetigen Ausweitung. Der Einmarsch Russlands in die Ukraine im Februar 2022 hat dieser Palette neue Facetten hinzugefügt. Lieferkettenprobleme in Vorleistungen und Rohstoffen, Energiepreisanstiege und Inflationsproblematik, Konjunktur- und Zinsrisiken. Der Grad der Unsicherheit ist so hoch, dass unternehmerische Planungen immer mehr einer integrierten mikro- und makroökonomischen Szenariotechnik gleichen müssen. Was kann passieren? Wo ist mein Break-even, wo meine Worst-Cases?

Im Zuge der kriegerischen Auseinandersetzungen werden Cyberattacken zwar medial immer wieder kurz genannt, die Dominanz der makroökonomischen Schocks drängt – zumindest in der Wahrnehmung – die Bedrohung durch Cyberrisiken jedoch manchmal in den Hintergrund.

Während m globalen Risikoreport des World Economic Forum im Jahr 2021 noch knapp 40 Prozent (Risiko auf 0-2 Jahre) bzw 50 Prozent (Risiko auf 3-5 Jahre) der Unternehmen Cyberrisiken als global kritisches Risiko identifizierten, waren dies im Report 2022 nur noch knapp 20 Prozent (0-2 Jahre) bzw 15 Prozent (3-5 Jahre). Und in diesen Daten ist der Impact des Ukraine-Konflikts noch nicht enthalten.

Dabei sind die Größenordnungen an volkswirtschaftlichem Schaden, der durch diese Bedrohungen hervorrufen werden kann, mehr als signifikant. So beziffert eine Studie von McAfee den Schaden durch Cyberkriminalität auf 1 Billion USD, was über 1 Prozent der globalen Wirtschaftsleistung ausmachte. Cyber Security Ventures geht in einer Analyse von noch höheren Kosten aus. So wird für 2021 ein Schaden von 6 Billionen USD (über 6 Prozent des globalen BIP) geschätzt, mit einer Prognose von über 10 Billionen USD 2025. Das sind Größenordnungen, die auch aus volkswirtschaftlicher Sicht keine vernachlässigbare Größe mehr darstellen.

Was hier passiert, ist einer der größten Vermögenstransfers in der Geschichte, und damit auch ein signifikantes Risiko – reduzieren Cyberrisiken doch Anreize für Innovationen und Investments, den Grundbausteinen strukturellen und langfristigen Wirtschaftswachstums. Gerade in den innovations- und investitionsintensiven Branchen, wie im Hightechsektor wiegen diese Risiken besonders schwer. So schätzte das Handelsblatt in einem Report aus 2019 den entgangenen Umsatz von Hightechunternehmen zwischen 2019 und 2023 auf 753 Mrd USD.

Angesichts dieser Zahlen können wichtige Schlussfolgerungen sowohl auf mikro- als auch auf makroökonomischer Ebene abgeleitet werden.

Für Unternehmen bedeutet allein das monetäre Ausmaß des Risikos, dass das Cyber-Risikomanagement eine ganz zentrale Rolle im Enterprise Risk Management einnehmen muss, und dass Absicherungsstrategien nicht nur für Zinsen oder Wechselkurse, sondern auch für die Absicherung von Cyberrisiken implementiert werden sollten.

Auf makroökonomischer und nationalökonomischer Ebene bedeuten diese Zahlen, dass die Bekämpfung der Risiken auf nationaler, vor allem aber konzertiert auf internationaler Ebene, stärker in den Fokus rücken muss. Der volkswirtschaftliche Schaden, der hier entsteht, ist das, was als toter Wohlfahrtsverlust in der Ökonomie bestens bekannt ist. Und auch die Notwendigkeit, Wohlfahrtsverluste nach Möglichkeit entschlossen und nachhaltig zu reduzieren.

Zusammenarbeit auf EU-Ebene muss vertieft werden

Bundesminister Gerhard Karner im Gespräch über die Chancen und Herausforderungen der Digitalisierung und die österreichische Strategie für Cybersicherheit.

Die Gesamtkriminalität ist 2021 gesunken. Eigentumsdelikte sind erneut zurückgegangen. Radikalisierung und Cyberdelikte waren hingegen die größten Herausforderungen für die Polizei. Wie bereitet sich das BMI auf eine mögliche weitere Steigerung von Cybervorfällen vor?
Cyberkriminalität ist tatsächlich der am stärksten wachsende Bereich in der Kriminalstatistik. So sind im Jahr 2021 die angezeigten Straftaten in diesem Bereich um 28,6 Prozent gestiegen, während die Gesamtkriminalität rückläufig ist. Dank der hervorragenden Arbeit unserer Polizistinnen und Polizisten konnte aber auch die Aufklärungsquote im Cyberbereich auf 36,9 Prozent gesteigert werden. Die zunehmende Verlagerung der Kriminalität in den Cyberraum verlangt von uns natürlich auch Anpassungen und Vorbereitungen. So wird etwa das C4, das Cyber Crime Competence Center im Bundeskriminalamt sowohl strukturell als auch technisch angepasst und personell verstärkt. Kompetenzen werden aufgebaut, auch in neuen Fachbereichen wie Delikten in Zusammenhang mit Kryptowährungen und die Zusammenarbeit mit Social Media- und Online-Providern professionalisiert und intensiviert. Aber auch auf Landes- und Bezirksebenen sollen im Zuge der aktuell laufenden Kriminalitätsdienstreform verstärkt Cyberexperten, sogenannte „Cyber-Cops" zum Einsatz kommen.

Denken Sie, dass die Corona-Pandemie nicht nur einen Schub der Digitalisierung ermöglicht hat, sondern auch zu einer höheren Sensibilisierung der BürgerInnen für die Gefahren im Internet beigetragen hat? Wird Cyber Security Ihrer Meinung nach bei Behörden und in der Wirtschaft jetzt anders wahrgenommen und werden wir vermehrt die Bereitschaft zum präventiven Setzen von Maßnahmen in diesem Bereich sehen?
Ich denke tatsächlich, dass die Sensibilisierung der Menschen in Österreich insgesamt zugenommen hat – auch bedingt durch die zahlenmäßige Steigerung der Vorfälle. Delikte wie Internet- und Bestellbetrug, Erpressung von Unternehmen und Privatpersonen durch Verschlüsselung der Daten durch Ransomware oder Ausspähen von Passwörtern durch sogenannte „Flu-Bot-SMS", wie die gefälschten SMS von Paketdiensten genannt werden, betreffen mittlerweile eine große Anzahl von Firmen aber auch Privatpersonen. Ich bin überzeugt davon, dass hier Prävention ein ganz wichtiger Ansatz ist, um die Sensibilisierung weiter zu erhöhen und die Scheu vor der Anzeige dieser Straftaten zu reduzieren. Hier leistet unter anderem die Initiative „Gemeinsam.Sicher" wichtige Arbeit.

Können Sie uns sagen, ob der Krieg in der Ukraine bereits das Geschehen im Cyberbereich verändert und wenn ja, können Sie uns ein Beispiel dafür geben?
Grundsätzlich kann man sagen, dass die digitale Kriegsführung deutlich zugenommen hat. Vor allem die Ukraine und Russland sind seit dem Beginn des Krieges massiven Angriffen verschiedener Gruppen ausgesetzt – auch Firmen, die in den jeweiligen Staaten aktiv sind, wurden bereits Opfer von Attacken. In Österreich ist die Lage derzeit als stabil zu bezeichnen. Es ist ein leichter Anstieg von DDoS-Attacken zu beobachten, also das Überfluten von IT-Systemen, wie zum Beispiel Websites, mit Anfragen mit dem Ziel, sie lahmzulegen. Allerdings ist erhöhte Wachsamkeit das Gebot der Stunde, um bei eventuellen Angriffen schnell und effizient reagieren zu können. Als besonders wichtig ist hier die Vernetzung zu sehen. Vernetzung einerseits national zwischen Behörden und Unternehmen, andererseits auch international unter den Staaten, vorrangig natürlich innerhalb der Europäischen Union.

Für den stetigen Anstieg von Cyberangriffen braucht es hochqualifizierte Fachkräfte. Welche Bemühungen setzt das BMI, um in diesem Ringen um die „besten Köpfe" im Bereich der Cybersicherheit eine Chance zu haben?
Tatsächlich ist die Rekrutierung von IT-Fachkräften eine Herausforderung, allerdings nicht nur für den öffentlichen Dienst, sondern auch für die Wirtschaft. Neben dem Ansatz einer finanziellen Attraktivierung der Tätigkeit ist auch das Aufzeigen der weiteren immateriellen Vorteile eines Jobs im öffentlichen Dienst wichtig – ein Posten bei uns ist ein sehr sicherer Arbeitsplatz mit spannenden, zukunftsorientierten Aufgaben am Puls der Zeit und vielfältigen Entwicklungsmöglichkeiten in alle Richtungen. Ich denke, dass wir hier auch früh im Entscheidungsprozess der einzelnen Person ansetzen müssen – in den Schulen, den Unis und FHs.

Gerhard Karner
ist seit 6. Dezember 2021 Bundesminister für Inneres.

FOTO © BMI (KARL SCHOBER)

»Prävention ist ein ganz wichtiger Ansatz, um die Sensibilisierung weiter zu erhöhen und die Scheu vor der Anzeige von Cyberattacken zu reduzieren.«

Die österreichische Bundesregierung hat mit der „Österreichische Strategie für Cybersicherheit 2021" ein aktualisiertes Konzept zur Schaffung eines sicheren Cyberraums veröffentlicht. Was sind die wesentlichen Änderungen zur Strategie von 2013?
Die neue Österreichische Strategie für Cybersicherheit besteht aus einem allgemeinen Teil, der ergänzt wird durch konkrete Maßnahmen der Ressorts, die einem regelmäßigen Monitoring unterworfen sind. Das Thema Cybersicherheit bewegt sich in einem sehr agilen Umfeld, daher ist diese Loslösung der Maßnahmen eine ausgezeichnete Möglichkeit, um die Verfolgung der einzelnen Ziele aktuell zu halten. Dies ist eine wesentliche Veränderung im Vergleich zur Österreichischen Strategie für Cybersicherheit aus dem Jahr 2013. Das BMI hat sofort nach Veröffentlichung der österreichischen Strategie für Cybersicherheit, im Dezember 2021 Maßnahmen formuliert, die unter anderem den Ausbau des Cyber Crime Competence Center (C4) zu einer modernen High-Tech Einheit oder den Aufbau von Cyber Cops-Bezirks- IT Ermittlern fördern werden.

Ebenso hervorheben möchte ich, dass sich die Österreichische Strategie für Cybersicherheit nun auch in den europäischen Rechts- und politischen Rahmen im Bereich Cybersicherheit nahtlos einfügt. Sie schafft es so, sowohl einen Beitrag zur eigenen Sicherheit als auch zur europäischen Sicherheit zu leisten, um einen offenen, stabilen und sicheren Cyberraum zu garantieren.

Auf der Ebene der EU wird derzeit an der NIS 2-Richtlinie gearbeitet, können Sie uns einen Einblick auf mögliche, für die Cybersicherheit relevante Änderungen geben?
Die NIS 2-Richtlinie verfolgt das Ziel, das Cybersicherheitsniveau in der gesamten EU zu erhöhen. Es ist von entscheidender Bedeutung, dass die Widerstandsfähigkeit gegen Cyberangriffe unionsweit steigt und dass die Mitgliedsstaaten die Zusammenarbeit auf EU-Ebene verbessern und vertiefen,

»Die NIS 2-Richtlinie ist ein großer Schritt vorwärts im Bereich Cybersicherheit «

Gerhard Karner

insbesondere im Falle von groß angelegten Vorfällen oder Cyberkrisen.

Die Cybersicherheitspolitik muss weiterhin mit dem Ziel gestaltet werden, das Vertrauen der Nutzerinnen und Nutzer in digitale Produkte und Dienstleistungen zu stärken und einen stabilen und effektiven digitalen Binnenmarkt zu ermöglichen. Geschehen soll dies durch eine Verbesserung der Cybersicherheitskapazitäten, die verstärkte Zusammenarbeit zwischen den Mitgliedstaaten und die Verbesserung der Cyberresilienz öffentlicher und privater Einrichtungen.

Die NIS 2-Richtlinie ist ein großer Schritt vorwärts im Bereich Cybersicherheit. Die Neuerungen der Richtlinie werden zu mehr Resilienz im Bereich der Cybersicherheit führen, wenn wir es schaffen die Vorgaben rasch umzusetzen. Wir bereiten uns im Innenressort daher bereits jetzt aktiv auf die Umsetzung der NIS 2-Richtlinie vor.

„Fake News", „Verschwörungstheorien" oder auch „Hassreden" sind in einem anonymen, digitalen Raum leicht möglich. Die jüngste Vergangenheit hat mit den Anti-COVID-Demonstrationen und den entsprechenden Begleiterscheinungen in den digitalen Medien gezeigt, dass diese Herausforderung real ist. Können Sie uns einen Überblick über die Maßnahmen geben, die das BMI gesetzt hat, um an dieser Stelle zu einem besseren gesellschaftlich-digitalen Miteinander zu kommen, als auch jenen mit denen klare Straftaten von Seiten des BMI bekämpft werden, denn die Abgrenzung zwischen vermeintlicher „Bagatelle" und „Straftat" wird nicht selten von TäterInnen in diesem Raum bewusst adressiert?
Die Digitalisierung unserer Gesellschaft, die durch die Covid-19-Pandemie noch an Geschwindigkeit zugenommen hat, führt zu einer raschen Zunahme von Phänomenen wie Hass im Netz, Fake News und Deepfakes.

Strafrechtliche Bestimmungen gelten im digitalen Raum ebenso wie offline. Im „Hass im Netz"-Paket, das gemeinsam mit dem Bundesministerium für Justiz und dem Bundeskanzleramt auf den Weg gebracht wurde, erfolgten einerseits strafrechtliche Verschärfungen und andererseits Erleichterungen für die Verfolgung. Aktuell liegt der Schwerpunkt der Aktivitäten auf der Verfestigung der Schulung der Organe der Sicherheitsexekutive und dem Ausbau der Kooperationen mit der Zivilgesellschaft zur Sensibilisierung und Erhöhung der Anzeigebereitschaft.

Deepfakes, also verschiedene Formen der audiovisuellen Manipulation mittels einer auf Künstlicher Intelligenz-basierten Technologie und Fake News stellen eine besondere Bedrohung für unsere Demokratie und das soziale Gefüge dar. In Deepfakes können Personen Aussagen in den Mund gelegt oder Handlungen unterstellt werden, die in Wirklichkeit nie stattgefunden haben. Deepfakes und Fake News bergen ein erhebliches sicherheitspolitisches Risiko. Daher arbeiten wir in enger Zusammenarbeit mit dem Bundesministerium für Justiz und dem Bundeskanzleramt, dem Bundesministerium für Landesverteidigung und dem Bundesministerium für Europäische und internationale Angelegenheiten an einem Aktionsplan zum Thema Deepfakes, der demnächst vorgestellt wird.

Key Findings Studie 2022

20% finanzieller Schaden durch Cyber-Kriminelle.

36% erwarten in den nächsten 12 Monaten eine Verschlechterung im Cyber Security-Bereich.

40% werben aktiv Sicherheitsexperten von anderen Unternehmen ab.

52% sagen, dass Cyberangriffe durch staatlich unterstützte Akteure für sie an Bedeutung gewonnen haben.

67% der befragten Unternehmen waren in den letzten 12 Monaten Opfer eines Cyberangriffs.

74% haben Schwierigkeiten beim Rekrutieren von IT-Experten.

1 — 2 — 3 — 4

Die Welt

Reise ins Unbekannte

10% sehen einen Zusammenhang zwischen der Unternehmenskommunikation und einem gezielten Cyberangriff.

22% geben an, dass APTs für sie mittlerweile zum Tagesgeschäft gehören.

52% sagen, dass Cyberangriffe durch staatlich unterstützte Akteure für sie an Bedeutung gewonnen haben.

Cyber Security kennt keine Staatsgrenze. Deshalb starten wir unsere Studie über Cyber Security in Österreich dieses Jahr etwas anders – nämlich mit einem Blick auf die weltweite Bedrohungslage.

Konflikte, wie jener zwischen Russland und der Ukraine, können die Cyber Security-Lage österreichischer Unternehmen ganz schnell und drastisch beeinflussen. Es geht also auf zu einer Reise, mit vielen Unbekannten. Wichtig dabei: Allen Umständen bestmöglich Paroli zu bieten und die Reise strategisch und gewappnet anzutreten.

Den Widrigkeiten trotzen

Willkommen in der vernetzten Welt: Cyberattacken und neue Formen von Kooperationen aufseiten der Kriminellen haben Auswirkungen auf die gesamte Gesellschaft. Das Damoklesschwert des „Cybersicherheitsversagens" schwebt seit jeher über der Welt – aktuell ist die Bedrohung aber besonders akut. Das hat Auswirkungen auf jedes einzelne Unternehmen in Österreich und zeigt auf, dass Cybersicherheit auf allen Ebenen neu gedacht werden muss.

Eines gleich vorweg: Den Kopf in den Sand zu stecken, ist keine Alternative. Denn das Rad muss trotz aller Widrigkeiten am Laufen gehalten werden: Unternehmen müssen die Widerstandsfähigkeit der Geschäftsprozesse sicherstellen, die in einer immer komplexeren Umgebung stattfinden. Die gute Nachricht: Auch in Zeiten wie diesen kann jede Organisation das Ziel der Cyberresilienz erreichen. Es braucht jedoch ein Umdenken.

Sorge um den Weltfrieden

Die Realität zeigt: Die weltweite Zunahme von staatlich unterstützten Angriffen (APTs) erschwert die Zusammenarbeit zwischen den Staaten, da man beginnt, manchen Ländern zu misstrauen. Die geopolitische Lage in der Ukraine und Russland erschüttert dieses Grundvertrauen zusätzlich. Bereits vor dieser kriegerischen Auseinandersetzung bereitete die Sorge um ein Cyber Security-Versagen vielen Experten Kopfzerbrechen. Denn die schnelle Digitalisierung in den meisten Volkswirtschaften durch die COVID-19-Pandemie hatte zu neuen Cyberschwachstellen geführt.

Ein „Versagen der Cybersicherheit" wurde vom World Economic Forum (WEF) in einer Umfrage als kritische, kurzfristige Bedrohung für die Welt identifiziert – das war vor den Angriffen Russlands auf die Ukraine. Die Befragten des „Global Risk Report" stufen Cybersicherheitsversagen unter die zehn größten Risiken ein, die sich seit Beginn der COVID-Krise am stärksten verschlechtert haben. Sie glauben, dass Cyber Security-Versagen die digitalen Systeme der Welt in den nächsten Jahren auf die Probe stellen werden: Jedes fünfte Unternehmen (20 Prozent) geht davon aus, dass ein Versagen der Cybersicherheit in den nächsten zwei Jahren kritisch für die Welt sein wird, 15 Prozent glauben, dies wird in zwei bis fünf Jahren der Fall sein.

» Deepfake-Videos sind eine gefährliche Propagandawaffe – wie der aktuelle Ukraine-Russland-Konflikt zeigt. Im März 2022 wurde auf die gehackte Webseite des ukrainischen Nachrichtensenders Ukraine 24 ein Deepfake-Video des ukrainischen Präsidenten Wolodymyr Selenskyj gestellt, das bald in zahlreichen Sozialen Medien kursierte. Darin rief das Staatsoberhaupt dazu auf, sich zu ergeben und die Waffen niederzulegen. «

Im Auftrag des Staates

Die institutionalisierte Kriminalität durch staatliche Stellen ist weltweit Realität geworden. Die Angst vor diesen zielgerichteten staatlich unterstützten Angriffen (APT – Advanced Persistent Threat bzw State Sponsored Attacks) steigt weiter. Die Akteure verfügen über entsprechende finanzielle Mittel, und Personal, sind bestens organisiert und haben ein konkretes Ziel vor Augen. In aller Regel werden solche Operationen von einer größeren Organisation (Staat bzw Geheimdienst) initiiert, die einen klaren Handlungsauftrag hat.

Vom Randthema zum Mainstream

Was vor zehn Jahren noch ein Exotenthema für die Rüstungs- oder Hochtechnologieindustrie war, ist nun auch in Österreich zur alltäglichen Herausforderung geworden. Für mehr als die Hälfte der befragten Unternehmen (52 Prozent) haben Cyberangriffe durch vermutlich staatliche oder staatlich unterstützte Akteure an Bedeutung gewonnen. Ein Viertel der befragten Unternehmen (22 Prozent) gibt gar an, dass APTs für sie mittlerweile zum normalen Tagesgeschäft gehören. Die Realität sieht aktuell wohl noch drastischer aus, denn unsere Umfrage wurde wenige Monate vor dem Ausbruch des Ukraine-Russland-Konfliktes durchgeführt. Aufgrund der aktuellen geopolitischen Lage hat sich die Situation verschärft. Es finden bereits Aktivitäten statt, die von gezielter Falschinformation in sozialen Netzwerken über Spionage in Systemen des Gegners und seiner Verbündeten bis hin zu Cyberangriffen auf kritische Infrastruktur und Industrieanlagen reichen können. Dabei müssen die Angreifer selbst nicht immer staatliche Akteure sein, sondern können auch von diesen geduldete, private Angreifer sein.

Ukraine-Russland-Konflikt

Die unsichere geopolitische Lage in der Ukraine und Russland hat auch Auswirkungen auf die Cyber Security weltweit. Die Befürchtungen vor Cybersicherheitsvorfällen und die Widerstandsfähigkeit kritischer Unternehmensdienste nehmen zu. Staaten und Unternehmen müssen ihre Anfälligkeit für Cybervorfälle neu bewerten. So hat etwa die russische Regierung ihre Abneigung gegen Unternehmen klar geäußert, die das Land verlassen wollen. Gleichzeitig stehen Unternehmen, die keine Waren mehr nach Russland liefern oder ihre Dienstleistungen von dort abziehen, auf der roten Liste. Auch in Österreichs Ministerien rechnet man mit russischen Vergeltungsaktionen gegen Unternehmen im Cyberspace.

Schauplatz Cyberspace

Es ist also mehr als wahrscheinlich, dass es im Zusammenhang mit dem Ukraine-Russland-Konflikt zu einer Zunahme an Cyberangriffen gegen Unternehmen und kritische Infrastruktur kommen könnte – und das nicht nur in den betroffenen Ländern, sondern auf der ganzen Welt. Dass diese Sorgen wohl schon Realität geworden sein könnten, zeigen ein paar aktuelle Beispiele: Das staatliche ukrainische Telekommunikationsunternehmen Ukrtelecom erlebte Ende März 2022 nach einem umfangreichen Cyberangriff eine Störung des Internetdienstes. Eine deutsche Tochtergesellschaft des russischen Energiekonzerns Rosneft meldet ebenso einen Cyberangriff. Das FBI warnte etwa zur gleichen Zeit davor, dass russische Hacker die Systeme von Energieunternehmen und anderen kritischen Infrastrukturen in den Vereinigten Staaten bereits gescannt haben. Während deutsche Regierungsvertreter über ein mögliches Embargo für Öl- und Gaslieferungen aus Russland diskutieren, melden der deutsche Windturbinenhersteller Nordex und die Enercon GmbH, der größte deutsche Hersteller von Windenergieanlagen, Cyber Security Incidents.

Gleichzeitig spielen nicht staatliche Akteure eine große Rolle bei Cyberoperationen, die gegen Russland gerichtet sind. Sie haben ein breites Spektrum von Opfern ins Visier genommen – russische Online-Zahlungsunternehmen, pro-russische Propa-

Die Hackergruppe Lapsus$ hatte ab Dezember 2021 innerhalb weniger Wochen gleich mehrere hochrangige Unternehmen wie Microsoft, Samsung und Nvidia sowie das brasilianische Gesundheitsministerium erfolgreich infiltriert und Daten gestohlen. Dabei wurde Ransomware eingesetzt und die Unternehmen erpresst und mit der Löschung oder Veröffentlichung der Daten gedroht. Vermutet wurden staatliche Hacker, die Wirtschaftsgeheimnisse stehlen wollten – die Hinweise deuten aber nun auf Teenager hin. (Stand April 2022).

ganda-Websites und vieles mehr. Unabhängig vom aktuellen Konflikt könnte dieses Niveau der Zusammenarbeit zwischen unabhängigen nicht staatlichen Akteuren gegen dasselbe Ziel eine neue Ära des Hacktivismus einläuten.

Fass ohne Boden

Eine weitere Gefahrenquelle: Zerstörerische Schadsoftware, die nicht vollständig unter Kontrolle zu halten ist, und somit massiven Schaden quer über die Welt verursachen könnte. Was Erinnerungen an die Ransomware-Software „NotPetya“ 2017 hervorruft, könnte sich im aktuellen Konflikt wiederholen. Sicherheitsexperten haben bereits mehrere Arten von neuer Wiper-Malware auf ukrainischen Computersystemen gefunden. Das einzige Ziel der Malware: Daten zu vernichten und so den Betrieb in den betroffenen Unternehmen und Organisationen zu stören. Auch „NotPetya“ hatte seinen Ursprung in einer ukrainischen Buchhaltungssoftware. Heute wird geschätzt, dass „NotPetya“ weltweit einen Schaden von mindestens zehn Milliarden US-Dollar verursacht hat.

Verunsicherte Gesellschaft

Hinzu kommen immaterielle Risiken: Desinformation und mangelnde digitale Sicherheit beeinträchtigen das Vertrauen der Öffentlichkeit in digitale Systeme. Cyber-Kriminelle haben Zugang zu sensibleren Informationen von Opfern, neue Technologien wie Deepfake ermöglichen es ihnen, Social Engineering-Methoden zu verbessern. Sie verbreiten Desinformationen – zB Deepfakes von politischen und wirtschaftlichen Entscheidungsträgern – und richten dadurch einen gesellschaftlichen Schaden an, der insbesondere das Vertrauen erschüttert – und das in Zeiten hoher Volatilität. All das wird das Misstrauen zwischen der Gesellschaft, den Unternehmen und den Regierungen vertiefen. Deepfakes könnten zum Beispiel dazu verwendet werden, Wahlen oder politische Ergebnisse zu beeinflussen – prognostiziert das WEF. Denn es gibt bereits einen boomenden Markt für Dienste, die darauf abzielen, die öffentliche Meinung zugunsten des Kunden zu manipulieren oder den Ruf des Rivalen zu schädigen.

Vom richtigen Zeitpunkt

Werfen wir einen Blick auf Österreich. Interessant ist hier der Zusammenhang zwischen Unternehmenskommunikation und einem gezielten Cyberangriff. Wie auch schon im Vorjahr sieht jedes zehnte heimische Unternehmen (zehn Prozent) hier eine Verbindung. Gerade Unternehmen, die im internationalen Kontext agieren, erzeugen Aufmerksamkeit und können aufgrund einer veröffentlichten Information zum Angriffsziel werden. Das zeigen auch internationale Vorfälle, die zumeist politisch motiviert sind. Kommuniziert ein Unternehmen beispielsweise seine Waren ab sofort nicht mehr in ein konkretes Land liefern zu wollen, kann dies eine gezielte Cyberattacke auslösen. Ein Aspekt, der angesichts der geopolitischen Lage enorm an Bedeutung gewinnt.

So gibt es in Bezug auf den aktuellen Konflikt eine täglich aktualisierte Liste der Universität Yale , die den Exodus der Konzerne aus Russland protokolliert. Gleichzeitig zeigt sie, welche rund 600 Unternehmen nach wie vor in Russland tätig sind. Die Liste hat sich nicht nur als „Hall of Shame “ einen Namen gemacht, sondern ist auch für Hackergruppen ein wichtiges Werkzeug geworden: Sowohl pro-russische als auch pro-ukrainische Cyber-Kriminelle finden auf dieser Liste ihre potenziellen Ziele für die nächsten Cyberattacken.

» Die Wichtigkeit von Cyber Security zieht sich durch das ganze Land. Österreichs Wirtschaftsministerin Margarete Schramböck kündigt im März 2022 ein Förderprogramm in Höhe von 2,3 Millionen Euro zur Stärkung der Cyber Security-Maßnahmen für KMUs an. Das Paket beinhaltet einen Zuschuss für Investitionen in die eigene IT-Sicherheit, aber auch Beratungen und Schulungen. Jedem Unternehmen steht eine maximale Fördersumme von 20.000 Euro zu. Innerhalb kürzester Zeit war der gesamte Förderrahmen vergeben. «

Durch hybride Aktivitäten wird ein Keil in die Gesellschaft getrieben

Hybride Bedrohungen sind ein Bereich, der schwer zu verstehen und zu fassen ist. Sönke Marahrens ist COI Director des Hybrid Center of Excellence in Helsinki und gibt Einblicke in diese umfangreiche Materie.

Können Sie uns die Funktionen und Aufgaben des Hybrid CoE grundsätzlich erklären?
Die EU hat gemeinsam mit der NATO beschlossen, den zunehmenden hybriden Bedrohungen entgegenzuwirken und 2018 das Hybrid CoE zu gründen. Österreich war einer der elf Gründerstaaten – heute haben wir 31. Hybrid CoE ist eine autonome, netzwerkbasierte internationale Organisation zur Bekämpfung hybrider Bedrohungen mit Sitz in Helsinki. Die Kernaufgabe: Die Fähigkeiten der Teilnehmerstaaten zur Bekämpfung hybrider Bedrohungen auszubauen und Resilienz aufzubauen.

Wie kann man sich das in der Praxis vorstellen?
Unter hybriden Bedrohungen versteht man konventionelle und unkonventionelle Methoden mit dem Ziel, unmittelbaren Schaden anzurichten und die Gesellschaften zu destabilisieren. So breit wie die Definition ist auch unser Aufgabenfeld. Wir sind einerseits im Bereich der Forschung und Analyse aktiv, bieten aber ebenso Trainings für Nationen an. Etwa: Wie schütze ich meine Wahlen vor hybrider Beeinflussung? Wie gehe ich mit Hybrid warfare um? Um nur ein paar Beispiele zu nennen.

Was versteht man unter hybriden Akteuren genau, haben Sie Beispiele?
Hybride Akteure agieren unterhalb eines Schwellenwertes, im Graubereich, um nicht als Angriff oder gar Kriegserklärung gewertet werden zu können. Man bezeichnet das als subthreshold. Das Hybrid CoE hat ein Grundlagendokument verfasst und darin in 13 verschiedenen gesellschaftlichen Dimensionen 30 Bereiche identifiziert, in denen wir hybride Akteure ermitteln konnten – sowohl auf staatlicher als auch auf nicht staatlicher Seite. Fakt ist: Sie können einen enormen Schaden anrichten. Eines der bekanntesten Beispiele ist Trollfactories: Eine institutionalisierte Gruppe von Internet-Trollen, die versucht, die politischen Meinungen zu steuern – Tastaturarmeen, um Propaganda zu verbreiten.

Das klingt nach einer Materie, in der es schwer ist, den Überblick zu bewahren.
Bei dieser Komplexität an Problemstellungen zählen auf Verteidigungsseite, also auch bei uns im Hybrid CoE, vor allem Partnerschaften und Kooperationen. Alleine im Bereich hybrid Cyber haben wir rund 400 Experten, mit denen wir uns austauschen. Gleiches gilt für Bereiche wie gesellschaftliche Beeinflussung oder Militär etc. Dadurch können wir Trends schnell erkennen. Essenzieller Bestandteil den Überblick zu bewahren, sind natürlich auch unsere Forschungsaktivitäten.

Ist ein hybrider Konflikt immer gleich als solcher erkennbar?
Die Zuordnung ist sehr schwer. Nehmen wir Ransomware-Attacken auf Unternehmen als Beispiel. Eine Firma kann sowohl bewusst als auch zufällig Objekt eines Angriffes sein. Denken wir an „NotPetya“: Die weltgrößte Reederei Maersk wurde wohl bewusst attackiert, viele andere Unternehmen waren zufällig Opfer. Angriffe dieser Art erfolgen oft im Gießkannenprinzip. Sie beeinflussen die Gesellschaften aber enorm und richten einen großen Schaden an, egal ob gesteuert oder zufällig. Viel klarer einzuordnen sind etwa Wahlbeeinflussungen – man denke zB an Brexit. Hier ging es jeweils darum, durch hybride Aktivitäten einen Keil in die Gesellschaft zu treiben und eine Partei zu unterstützen bzw die andere zu schädigen.

Ein Unternehmen kommuniziert einen Exportstopp in ein Land und wird dann Opfer einer Cyberattacke. Ein hybrider Angriff?
Natürlich gibt es politische oder wirtschaftliche Interessen, Konkurrenten auszuschalten, Märkte zu beeinflussen oder virtuelle Vergeltungsschläge durchzuführen. Die Frage kann man aber nicht pauschal beantworten. Hier muss man eine Analyse im Einzelfall machen. Sie müssen sich den hybriden Akteur wie einen Zahnarzt vorstellen, auf der Suche nach jenem Nerv, der Schmerzen verursacht. In dem Moment, wo er die Schmerzstelle gefunden hat, sucht er weiter. Auch Cyber-Kriminelle suchen unsere Schwachstelle – natürlich im negativen Sinn. Oftmals finden sie diese zufällig, manchmal aber ganz bewusst.

Beispiel Shitstorms: Können sich Unternehmen eigentlich schützen?
Im Hinblick auf die Unternehmenskommunikation gilt: Man ist nie schutzlos ausgeliefert, muss aber alles überwachen und nichts einfach laufen lassen. Wenn wir an Social Media denken: Ein Shitstorm muss sofort eingefangen werden. Merkt ein Unternehmen, dass eine Desinformationskampagne gegen die Firma oder Marke läuft, muss früh mit Fakten entgegengewirkt werden, um die Kontrolle über die Kommunikation zu behalten. Vom Reagieren sofort ins Agieren kommen – denn sonst kann aus einem kleinen Feuer ein Flächenbrand werden.

FOTO © BUNDESWEHR

Sönke Marahrens
ist Direktor der Community of Interest für Strategie und Verteidigung am European Centre of Excellence for Countering Hybrid Threats in Helsinki.

Erfahren Sie mehr in unserem Podcast IMPULSE

»Menschen, deren Hobby ein enormes Potenzial für die Gesellschaft sein könnte und deren Engagement koordiniert werden müsste.«

»Moderne Unternehmen haben ihren Mitarbeitern gegenüber eine Fürsorgepflicht. «

Sönke Marahrens

Schlagwort: Social Media. Wie verhält sich ein Unternehmen hier seinen Mitarbeitern gegenüber? Moderne Unternehmen haben ihren Mitarbeitern gegenüber eine Fürsorgepflicht. Dafür braucht es einen strategischen Dialog, denn mit Maulkörben und Verboten kann man definitiv nichts erreichen. Das Konzept heißt auch hier: Awareness Building. Man muss Mitarbeitern klarmachen, dass sich ihre Meinungen auf das Unternehmen als Ganzes auswirken können. Auf der anderen Seite können Mitarbeiter das Image des Unternehmens ja auch extrem positiv beeinflussen. Es braucht in jedem Fall ein vertrauensvolles Miteinander.

Social Media und KI sind generell schwierige Terrains – Schutz der Bevölkerung versus Einschränkung der persönlichen Freiheiten?
Die nordischen Staaten haben bspw einen KI-Führerschein eingeführt. So sorgt man dafür, dass sich Menschen mit künstlicher Intelligenz auseinandersetzen und verstehen lernen, wie Algorithmen funktionieren. Sie lernen, warum ihnen bestimmte Dinge auf Facebook oder Twitter angezeigt werden. Es geht um eine Alphabetisierung im digitalen Bereich: Wie geht man mit diesen Medien um und was können mögliche Konsequenzen sein. Unser Ziel muss sein, Bürger gegen Falschinformationen resilient zu machen. Das Problem dabei: Desinformationskampagnen sind nicht immer so plump, wie man sich das vorstellt. Oft werden 95 Prozent richtige und überprüfbare Fakten geliefert und dann fünf Prozent Falschinformation dazwischen gestreut.

Schweden hat mit dem Aufbau einer staatlichen Agentur begonnen, die Desinformation und gezielte Gerüchte abwehren soll.
Genau. Die Behörde für psychologische Verteidigung beschäftigt sich damit, Desinformation zu erkennen, die sich gegen Schweden richtet. Das Institut wurde dem Justizministerium unterstellt, was eine sehr kluge Entscheidung ist: es genau den Wächtern der Gesetze zu unterstellen, die auch dafür verantwortlich sind, dass die Meinungsfreiheit gewahrt wird. So kann nie der Eindruck einer staatlichen Propaganda entstehen.

Im Ukraine-Russland-Konflikt agieren ja viele Freiwillige im Cyberraum – ein Konzept mit Zukunft?
Man kann dieses Phänomen auch als sehr positive Kraft sehen. Denn vielleicht brauchen wir in Zukunft eine Cyber-Hilfswehr, ähnlich wie die Freiwillige Feuerwehr. Menschen, deren Hobby ein enormes Potenzial für die Gesellschaft sein könnte und deren Engagement koordiniert werden müsste. Es bleibt natürlich das Restrisiko der Kontrolle: Woher wissen wir, was diese Menschen wirklich am Computer machen? Aber im positiven Sinn gesehen: Das Potenzial ist enorm und birgt viele kluge Ideen, die man für die Cyberverteidigung und den -schutz im 21. Jahrhundert nutzen muss.

Wie weit darf und soll sich da der Staat eigentlich in die Wirtschaft einmischen?
Eine heikle Grenzfrage. Natürlich ist die freie Marktwirtschaft ein großes Gut. Doch den Staat als Regulator abzulehnen und ihn gleichzeitig zu rufen, wenn man Verluste macht, ist auch nicht korrekt. Es braucht eine Balance, die wohl ähnlich kritisch ist wie jene zwischen freier Meinungsäußerung und Sicherheit. Wenn wir die Freiheit zugunsten der Sicherheit zu sehr einschränken, dann haben wir keine Freiheit mehr. Wenn wir aber die Sicherheit vernachlässigen, dann kann diese Freiheit missbraucht werden. Ähnliches gilt für den Marktbereich. Der Weg kann jedenfalls immer nur über Vernunft und nie über Zwang führen.

»Das Problem: Desinformationskampagnen sind nicht immer so plump, wie man sich das vorstellt.«

Sönke Marahrens

Man muss in Cybersicherheit investieren, sonst hat man verloren

Die Schweizer Cyberstrategie ist besonders, die Herausforderungen sind jedoch dieselben. Pascal Lamia vom NCSC (Nationales Zentrum für Cybersicherheit), und vom Kompetenzzentrum des Bundes für Cybersicherheit in der Schweiz, im Gespräch.

FOTO © PASCAL LAMIA PRIVAT

Pascal Lamia
ist Leiter für Operative Cybersicherheit im Nationalen Zentrum für Cybersicherheit (NCSC) und Stv. Delegierter des Bundes für Cybersicherheit in der Schweiz.

Erfahren Sie mehr in unserem Podcast IMPULSE

Welche Aufgaben hat das NCSC?
Unser Grundauftrag ist der Schutz der kritischen Infrastrukturen vor Cyberattacken in der Schweiz. Früher gab es MELANI, die Melde- und Analysestelle Informationssicherung des Bundes. Es wurde 2020 durch das NCSC, das Nationale Zentrum für Cybersicherheit, abgelöst. Wir haben unter anderem eine nationale Anlaufstelle für Bürgerinnen und Bürger oder kleine und mittlere Unternehmen, wo sie im Fall von Cyberattacken Unterstützung erhalten. Also eigentlich sind wir der Single Point of Contact auf staatlicher Seite, wenn es um Fragen der Cybersicherheit geht.

Es gibt in puncto Cybersicherheit so etwas wie ein „Schweizer Modell" – können Sie uns das erklären?
2004 gab es den Bundesratsentscheid, die Melde- und Analysestelle Informationssicherung aufzubauen, mit dem primären Ziel des subsidiären Schutzes kritischer Infrastruktur. Schon damals galt das Prinzip der Eigenverantwortung – Unternehmen müssen sich selbst um ihre Cyber- und Datensicherheit kümmern. 2012 und 2018 hat die Schweiz weitere Cyberstrategien erarbeitet, an diesem Grundprinzip wurde jedoch stets festgehalten. In der Schweiz gibt es drei Hauptsäulen im Cyberbereich: Erstens die Cyberstrafverfolgung – das ist Sache der Polizei. Zweitens die Cyber Defence – das ist der Bereich der Armee und des Nachrichtendienstes. Drittens die Cybersicherheit und hierfür ist das NCSC zuständig. Wir sind verantwortlich für die koordinierte Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS), für die Prävention und die Unterstützung primär bei kritischen Infrastrukturen im Krisenfall.

Ihre Arbeit ist sozusagen eine Assistenzleistung der Behörden?
Im Bereich der kritischen Infrastrukturen unterstützen wir Unternehmen beim Cybervorfall direkt. Es gibt eine Hotline und man ist sofort mit unserem GOVCERT, mit dem Computer Emergency Response Team der Schweiz, verbunden. Mit deren Unterstützung können Sofortmaßnahmen eingeleitet werden. Wir arbeiten Hand in Hand mit Strafverfolgungsbehörden, Polizei, externen Sicherheitsfirmen. Unsere Einsätze sind immer Hilfe zur Selbsthilfe: Das Problem lösen muss letztendlich das Opfer selbst, aber wir helfen, schnell das erste Feuer zu löschen. Sobald sich Erfolge einstellen oder Unternehmen externe Unterstützung gefunden haben, ziehen wir uns als Staat wieder zurück.

Machen Sie dabei einen Unterschied bei den Branchen?
Grundsätzlich behandeln wir alle kritischen Infrastrukturen gleich. Wenn wir aber Parallelangriffe haben – etwa gegen Energiesektor, Telekommunikation, Finanz, Gesundheitssektor – dann müssen wir natürlich priorisieren. Priorisieren heißt etwa: Wir alle brauchen Strom. Der Energiesektor ist somit ganz weit oben auf unserer Liste.

Wann und wie sehr soll Ihrer Meinung nach der Staat in die Cyber Security eines Unternehmens eingreifen?
Der Staat hat sich bisher nur im Bereich der kritischen Infrastruktur eingemischt. Eine Vielzahl an Ransomware-Angriffen hat dazu geführt, dass zahlreiche kleine und mittlere Unternehmen die Unterstützung des Staates nun vermehrt einfordern. Hier gilt es, die Balance zu halten. Natürlich muss der Staat helfen, wenn es um einen konkreten Vorfall geht und um Hilfe ersucht wird. Doch ein Mehr an Unterstützung ist aus meiner Sicht weder zielführend noch fair: Der Staat würde dann ja quasi mit Staatsgeldern all jene belohnen, die sich nicht ausreichend um ihre Cybersicherheit gekümmert haben. Nur in sehr kritischen Situationen sollte der Staat aktiv werden. Effizienter ist es, wenn sich die Unternehmen ihrer Eigenverantwortung bewusst sind und entsprechende Massnahmen umsetzen.

Im Bereich Cyber Security sitzt der Staat zwischen den Stühlen – Freiheit versus Compliance. Wo wird die Reise hingehen?
Eigenverantwortung auf der einen Seite, zusätzliche regulatorische Maßnahmen auf der anderen – das ist die Herausforderung. Grundsätzlich hat die Schweiz die Cyberstrategie als Zielniveau definiert. Das bedeutet: Wir überlassen den Firmen die Entscheidung, wie sie diesen Standard erreichen. Solange die Wirtschaft mitzieht und der Fortschritt sichtbar ist, will man dieses Modell weiterverfolgen. Doch auch in der Schweiz beginnt der Staat zusätzlich zu regulieren – so ist aktuell eine Meldepflicht für Betreibende von kritischen Infrastrukturen. Aufgrund der steigenden Bedrohungslage finde ich das richtig.

»Effizienter ist es, wenn sich die Unternehmen ihrer Eigenverantwortung bewusst sind und entsprechende Maßnahmen umsetzen.«

Wir brauchen eine gewisse Compliance, um einen definierten und verbindlichen Grundschutz zu erreichen.

Die Moral in puncto Cyberattacken-Meldung ist in Österreich ausbaufähig. Woher kommt diese Scheu, nicht darüber sprechen zu wollen?
Diese Herausforderung haben wir auch in der Schweiz. Unser Vorteil ist, dass der Staat seit 2004, seit MELANI, eine enge Zusammenarbeit mit den kritischen Infrastrukturbetreibern aufgebaut hat. Diese Unternehmen haben ein hohes Vertrauen in uns. Sie wissen, dass ihre Meldungen nicht automatisch an den Regulator, die Strafverfolgungsbehörde oder gar Journalisten geht. Kleinere Unternehmen haben diese Erfahrungen noch nicht. Daher überwiegt bei ihnen die Sorge eines Reputationsschaden. Sie fürchten, automatisch eine Anzeige zu bekommen, wenn der Grundschutz nicht eingehalten wurde oder besonders schützenswerte Personendaten betroffen sind. Wir haben im letzten Jahr über 22.000 Meldungen erhalten – über Angriffe und Angriffsversuche. Wir sammeln diese Daten, geben sie anonymisiert als Wochenrückblick auf unserer Website an die Öffentlichkeit weiter. Transparenz ist das A und O.

Was sind aus Ihrer Sicht die Grundsatzfragen, wenn es um eine Cyberstrategie in Unternehmen geht?
Die Kernaufgabe der Geschäftsleitung ist es zu wissen, welche Daten schützenswert sind. Und natürlich braucht es einen Cybergrundschutz – dieser muss eingehalten werden. Dazu gehören etwa das Einspielen von aktuellen Patches, eine Sensibilisierung der Mitarbeitenden. Niemals ausblenden darf man auch die Tatsache, dass Cybersicherheit Geld kostet – man muss heutzutage in diesen Bereich investieren, sonst hat man verloren.

Es werden heute nicht mehr nur die großen Unternehmen angegriffen ...
Richtig. Es werden jene Unternehmen angegriffen, in denen der Grundschutz nicht eingehalten wurde, jene in denen der Microsoft Exchange Server nach einem Jahr noch immer nicht richtig gepatcht ist, es offene VPN-Zugänge gibt und noch immer keine Mehrfachfaktorauthentifizierung. Die Aussage, dass KMUs seltener angegriffen werden, ist schlichtweg falsch. Cyber-Kriminelle suchen primär nach verwundbaren Systemen, dringen ein und schauen erst dann, ob und was sie für sich herausholen können. Cybersicherheit ist zum Wettbewerb geworden: Ich muss besser sein als viele andere, damit ich gar nicht erst in den Fokus der Cyber-Kriminellen komme.

»Cybersicherheit ist zum Wettbewerb geworden.«

Pascal Lamia

Wie sehen Übungen mit Unternehmen in der Praxis aus?
Wir spielen seit vielen Jahren Übungen gemeinsam bei Unternehmen durch. Das können ganz einfache Tabletop-Übungen sein, bei denen NCSC, Regulatoren aber auch externer Berater dabei sind. Die Unternehmen lernen dabei dafür zu sorgen, dass ihre Kernprozesse weiterhin funktionieren. Bei ENISA-Übungen, also die European Union Agency for Cyber Security betreffend, holen wir auch private Firmen oder Spitäler dazu, sodass sie ihre Sichtweise einbringen können. Diese Lessons Learned sind für uns sehr wichtig – letztendlich profitieren alle davon. Das Wichtigste ist, als Unternehmen in einer Krise Köpfe zu kennen. Man muss wissen, wo man Unterstützung bekommt. Denn im Ernstfall gilt es, keine Zeit zu verlieren.

»Transparenz ist das A und O.«

Pascal Lamia

Hat der aktuelle geopolitische Konflikt das Thema Cyber Security verändert?
Was wir sehen ist, dass der Ukraine-Konflikt von den Cyber-Kriminellen als Thema aufgenommen wird – in Form von dubiosen Spendenaufrufen etwa. Aktuell sehen wir aber keine gezielten Angriffe gegen kritische Infrastrukturen in der Schweiz.

In Zusammenhang mit dem Ukraine-Russland Konflikt herrscht eine große Nervosität vor Cyberangriffen. Zurecht?
In der Vergangenheit wurde demonstriert, dass es enorme Cyberfähigkeiten wirklich gibt: Rund um den Computerwurm Stuxnet gab es zum Beispiel Angriffe gegen nukleare Anlagen im Iran. Und das schürt Angst. Speziell rund um den Ukraine-Russland-Konflikt gab es vermehrt Sorgen, dass man diese Fähigkeiten gegen ein Land oder Europa im Allgemeinen einsetzen könnte. Fakt ist: Momentan ist das noch nicht geschehen. So etwas kann aber jederzeit stattfinden, da bin ich überzeugt. Jedes Land muss sich entsprechend vorbereiten.

Bleibt es so ruhig? Denken wir an zielgerichtete Schadsoftware wie HermeticWizard oder HermeticWiper, die im Zuge des Konfliktes erstellt wurden.
Ich rechne mit einem baldigen Anstieg der gezielten Attacken gegen Unternehmen. Die Cyber-Kriminellen müssen ihre Kriegskassen bald wieder auffüllen und werden das ganze Internet nach verwundbaren Servern scannen, diese dann angreifen und Organisationen letztendlich erpressen.

Sollte es zu einem „Kalten Cyberkrieg" in Europa kommen, wie sollten wir heute schon vorsorgen?
Das Wichtigste ist, dass eine gewisse Kommunikation innerhalb Europas sichergestellt ist und optimiert wird. Hier müssen wir noch vereinter und besser zusammenarbeiten, insbesondere im Bereich des Informationsaustausches. Technische Informationen müssen grenzüberschreitend verfügbar sein, um weitere Schäden zu verhindern und Gegenmaßnahmen einleiten zu können. Diese Kooperationen funktionieren in Einzelfällen bereits gut, müssen aber definitiv noch vertieft werden.

Zum Abschluss: Welche Botschaft möchten Sie jedem Unternehmen mitgeben?
Schauen Sie, dass Sie Ihren Grundschutz unbedingt einhalten und umsetzen. Werden Sie jetzt aktiv. Analysieren Sie Ihre Systeme und Daten und überlegen, was Sie unbedingt schützen müssen. Jetzt haben Sie noch die Chance, sich vorzubereiten und Maßnahmen zu ergreifen. Denn Cyberkriminelle werden meiner Einschätzung nach bald nach neuen Wegen suchen, Geld zu machen. Die Zeit zu handeln ist jetzt.

1 — 2 — 3 — 4

Die Organisation

Das große Umdenken

36% erwarten in den nächsten 12 Monaten eine Verschlechterung im Cyber Security-Bereich.

53% vertrauen bei einem Cyber Security-Vorfall auf Externe.

73% geben als Ursache für den Budgetanstieg neue Bedrohungen an.

83% vertrauen ihren Schutzmaßnahmen im Fall eines Angriffes.

Österreichs Unternehmen vollführen eine Kehrtwende in Sachen Cyber Security. Das Schlagwort heißt Handlungsfähigkeit.

Die Geschwindigkeit, mit der sich der Cyberraum ändert, erfordert eine neue Einordnung des Begriffes Cyber Security: Die wichtigsten operativen Prozesse im Unternehmen müssen definiert und geschützt werden. Für Unternehmen liegt der Fokus heute zu gleichen Teilen auf der Verringerung der Angriffswahrscheinlichkeit und dem Folgenmanagement. Dafür braucht es mehr als „nur" Technologie. Es braucht eine Unternehmenskultur, die Cybersicherheit von A bis Z mitdenkt.

Priorität Nummer eins

Das Toprisiko: Cyber Security wird erfreulicherweise jedes Jahr mehr und mehr zur Chefsache in Unternehmen. Denn Maßnahmen zur Sicherung von IT-Systemen und Anwendungen – das betrifft auch die Cloud – bedürfen höchster Priorität und eines klaren Management Commitments. Nur so kann man kann man in sich schnell ändernden Gefährdungslagen sicher und situationsangepasst handeln. Eine weltweite KPMG Umfrage zeigt etwa: Technologieunternehmen definieren Cybercrime als größte Bedrohung für ihr Wachstum. 61 Prozent sind der Überzeugung, dass Informationssicherheit ein potenzieller Wettbewerbsvorteil ist.

Von 0 auf 100: Die Pandemie hat zusätzlich für noch mehr Risikobewusstsein in Sachen Cybersicherheit gesorgt, auch wenn diese sich nicht 1:1 im Sicherheitsbudget widerspiegelt: 59 Prozent der Unternehmen in Österreich stimmen der Aussage zu, dass sich die Bedeutung von Cyber Security durch die Pandemie in ihrem Unternehmen verändert hat.

Hauptverantwortlich ist dabei laut Unternehmensangaben der Trend zu hybriden Arbeitswelten. Etwas, das bei vielen Unternehmen vorher unvorstellbar war, wurde ihnen innerhalb kürzester Zeit direkt vor die Haustüre geliefert – aus Mangel an Alternativen. Diese hybriden Arbeitswelten werden in vielen Bereichen nicht mehr verschwinden.

Eine Frage der Kultur

In den Grundfesten: Österreichs Unternehmen adressieren Cybersicherheit aktiv im Rahmen ihrer Unternehmensstrategie. Dass sie diesen Sicherheitsaspekt mittlerweile als wesentlichen Bestandteil ihres Alltags sehen, spiegelt der sich langsam verbessernde Reifegrad heimischer Unternehmen wider. Ziel jedes Unternehmens muss es sein, echte Cyberresilienz zu schaffen. Cybersicherheit ist eine strategische Priorität, die in der Kultur, den Technologien und den Abläufen des Unternehmens verankert sein muss. Die KPMG Umfrage unter Technologieunternehmen kommt zu dem Schluss, dass für die meisten Unternehmen eine Cyber Security-Kultur mittlerweile genauso wichtig ist wie entsprechende Cyber Security-Technologien: 87 Prozent stimmen dieser Aussage weltweit zu. Für immer mehr Unternehmen steht Cyberresilienz , mit dem Fokus auf Cyberfähigkeiten und Cyberkultur also mittlerweile auf der To-do-Liste ganz oben.

Halbvoll oder halbleer

Die Stimmungslage in den heimischen Unternehmen ist ambivalent. Jedes dritte Unternehmen (36 Prozent) sieht pessimistisch in die Zukunft und erwartet in den nächsten zwölf Monaten Verschlechterungen im Cyber Security-Bereich. Ein Viertel (26 Prozent) blickt optimistisch auf das nächste Jahr. Analysiert man die Antworten nach der Funktion im Unternehmen, zeigt sich eine interessante Diskrepanz: Vorstände und Geschäftsführer sind weitestgehend eher pessimistisch, Sicherheitsverantwortliche tendieren zum fast schon überschwänglichen Optimismus.

Der Maßstab Budget

Das liebe Geld: Cybersicherheit wird von immer mehr Unternehmen im Land als geschäftskritisch bewertet, entsprechend wird agiert. Ein verlässlicher Indikator dafür ist die Höhe des Sicherheitsbudgets. 2022 gaben sieben von zehn Unternehmen (69 Prozent) an, dass ihr Cyber Security-Budget deutlich gestiegen ist. 24 Prozent haben kein dezidiertes Cyber Security-Budget. Bei einem Fünftel (19 Prozent) der Unternehmen macht das Cyber Security-Budget drei bis fünf Prozent des IT-Budgets aus, der momentane Spitzenreiter in unserer Studie.

Stetig nach oben

Strategie vor Pandemie: Auch wenn die Investitionen stetig steigen, so zeigt sich dennoch: Die Pandemie war kein entscheidender Treiber für das erhöhte Cyber Security-Budget. Das ist durchaus eine Überraschung – und widerspricht den viel verbreiteten Theorien. Diese Hypothese, die zu Beginn der Pandemie vielfach aufgestellt wurde, konnte durch unsere Umfrage nicht bestätigt werden. Nur jedes zehnte Unternehmen (neun Prozent) gibt als Grund für die Steigerung des Budgets die Pandemie an. Der Großteil beruft sich als Erklärung auf neue Bedrohungen (73 Prozent)

> In den USA sollen die Bundesausgaben von 17,9 Milliarden US-Dollar auf 20,3 Milliarden US-Dollar im Jahr 2022 steigen. Präsident Joe Biden hat in seinem neuen Infrastrukturgesetz Maßnahmen zur Cybersicherheit und deren Finanzierung verstärkt.

bzw auf die Unternehmensstrategie (57 Prozent). Hier gilt es jedoch ein psychologisches Phänomen zu beachten, ohne die Glaubwürdigkeit der Unternehmen infrage stellen zu wollen: Oftmals werden Entscheidungen nachträglich einer strategischeren Kategorie zugeordnet, um das Handeln in einem besseren Licht darzustellen.

Von Soll und Muss: Behördliche Vorgaben und Compliance-Erfordernisse sind die am dritthäufigsten genannten Gründe für die Budgeterhöhung und treffen auf jedes dritte Unternehmen (37 Prozent) zu. Gerade in hochregulierten Wirtschaftsbereichen wie Banken oder Versicherungen ist diese Zahl – wenig überraschend – mit 70 Prozent noch höher. Der Druck von außen auf diese Unternehmen stieg über die letzten Jahre hinweg kontinuierlich. Das Pendel der Digitalisierung hat zu Beginn die innovativen Aspekte in den Vordergrund gestellt, diese wurden später durch behördliche Vorgaben und Compliance-Erfordernisse wieder in geordnete Bahnen gebracht – das typische Governance-Phänomen. So können Regulatorien oftmals als Impulsgeber dienen, auch wenn nachträglich eine Prüfung über ihre Einhaltung und Umsetzung folgt. Unternehmen müssen auch diesen Aspekt klug in ihrer strategischen Planung berücksichtigen.

Die Kosten weltweit

Österreich entspricht hier dem weltweiten Trend. Denn: Je mehr Digitalisierung, desto mehr Cyberkriminalität, desto höhere Investitionen in Cybersicherheit. Einem Bericht von Bloomberg Intelligence zufolge werden die Ausgaben für Cybersicherheit 2024 jährlich 200 Milliarden Dollar übersteigen. Das World Economic Forum schätzt, dass die Kosten für Cyber Security für Unternehmen in allen Größen erheblich steigen werden. Dies könnte eine besondere Herausforderung für kleine und mittlere Unternehmen darstellen, die möglicherweise in naher Zukunft bis zu vier Prozent oder mehr ihrer Betriebsausgaben für Sicherheit aufwenden müssen. Für größere Organisationen liegt die WEF-Schätzung bei ein bis zwei Prozent.

Gelassenheit und Herausforderung

Zwischen Coolness und Panik: Interessant ist an dieser Stelle auch der Blick in das Daily Business der Unternehmen: So stufen 71 Prozent der Unternehmen Phishing mittlerweile als normales Tagesgeschäft ein. Ähnlich sieht die Realität beim Thema Social Engineering (63 Prozent), CEO Fraud (60 Prozent) bzw (D)DoS (56 Prozent) aus. Unternehmen haben gelernt, mit derartigen Gefahren umzugehen und sich bestmöglich darauf vorzubereiten. Auch Fake News und die Rufschädigung in sozialen Netzwerken bzw Identitätsdiebstahl lösen keine breite Panik mehr aus: Für fast die Hälfte der Unternehmen (51 bzw 49 Prozent) hierzulande gehören die Herausforderungen bereits zum normalen Alltagsgeschäft.

Anders sieht die Lage in Hinblick auf Ransomware/Erpressung und Data Leakage aus: Jedes zweite Unternehmen (49 bzw 45 Prozent) bezeichnet diese Thematiken als besondere Herausforderung. Nicht unwesentlich für den hohen Anteil ist wohl die mediale Berichterstattung der letzten Monate zu diesem Thema – Ransomware-Attacken sind und waren omnipräsent. Ein Teil der Furcht könnte also auf die mediale Präsenz zurückzuführen sein. Auch Angriffe auf Zulieferer- oder Kundensysteme (Supply Chain Attacks und Third Party-Risiken) treiben über einem Drittel der Verantwortlichen die Schweißperlen auf die Stirn (36 Prozent).

Nach dem Angriff ist vor dem Angriff

Das Vertrauen in die eigenen Maßnahmen ist ungebrochen hoch: 83 Prozent der Unternehmen fühlen sich im Fall eines Angriffes gewappnet – sie vertrauen ihren Schutzmaßnahmen sehr (21 Prozent) oder eher (62 Prozent). Die KPMG Umfrage unter Technologieunternehmen zeigt eine vergleichbare Zahl: Drei Viertel der Unternehmen (74 Prozent)

9% geben als Ursache für den Budgetanstieg die Pandemie an.

59% sagen, dass sich die Bedeutung von Cyber Security durch die Pandemie in ihrem Unternehmen verändert hat.

65% investieren nach einer Cyberattacke in zusätzliche Security Tools.

71% verzeichnen einen Anstieg des Cyber Security-Budgets.

71% stufen Phishing mittlerweile als normales Tagesgeschäft ein.

97% binden externe Dienstleister in die technische Vorfallsbehandlung ein.

sagen, sie sind auf eine zukünftige Cyberattacke gut vorbereitet.

Das Pferd von hinten aufzäumen: Seit Jahren zeigt unsere jährliche Umfrage, dass heimische Unternehmen zu sehr auf Reaktion statt Prävention setzen. In zu vielen Unternehmen gewinnt Cybersicherheit erst dann an Bedeutung, wenn ein Angriff stattgefunden hat. Zwei Drittel der Unternehmen (65 Prozent) investieren nach einer Cyberattacke in zusätzliche Security Tools und suchen nach Schwachstellen in ihren Systemen. Unternehmen reagieren also häufig auf Vorfälle statt vorab strategisch geplant zu agieren. Das bestätigt unsere oben genannte Theorie, dass die Unternehmensstrategie wohl nicht immer der ausschlaggebende Faktor für Budgeterhöhungen ist. Knapp die Hälfte (49 Prozent) verbessern nach einem Angriff außerdem die interne Krisenplanung für Cyberangriffe und holen sich externe Hilfe durch spezialisierte IT-Berater oder Dienstleister (47 Prozent). Für ein Viertel der Unternehmen (25 Prozent) ist der Cyberangriff Auslöser dafür, neue Mitarbeiter im Bereich Cybersicherheit einzustellen bzw in die Ausbildung der bereits bestehenden zu investieren.

Verlässliche Wegbegleiter

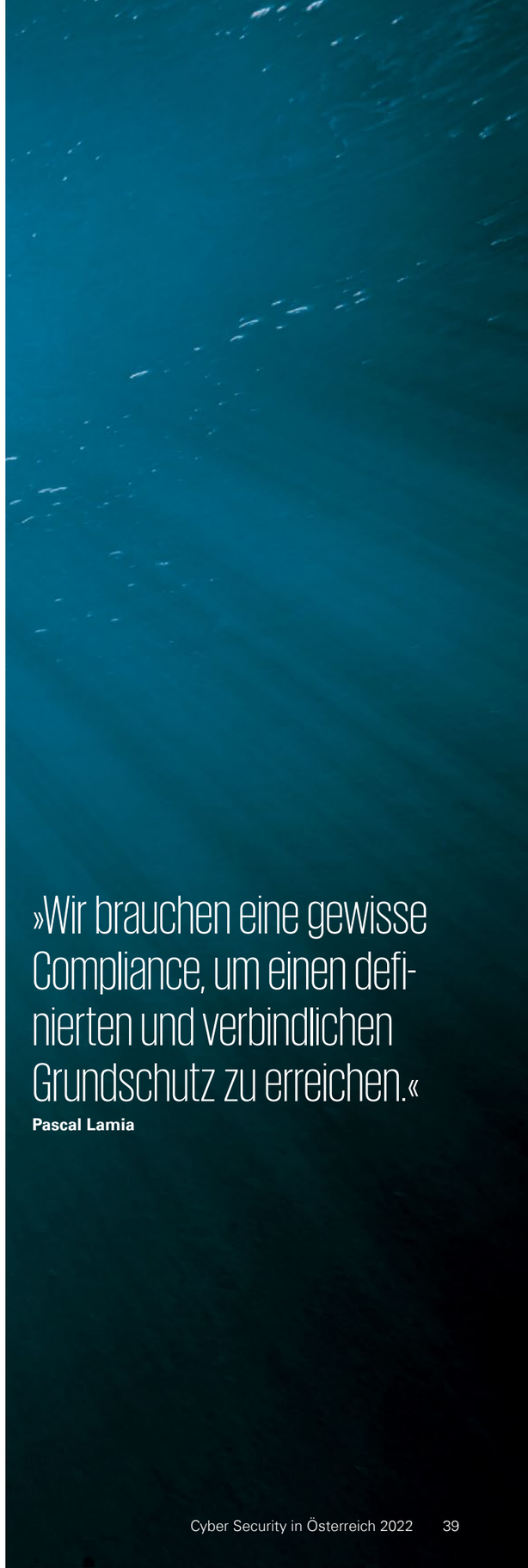
Hilfe von außen: Bei der Bearbeitung von Sicherheitsvorfällen setzen Österreichs Unternehmen auf externe Dienstleister. Mehr als die Hälfte (53 Prozent) vertraut bei einem Cyber Security-Vorfall auf Externe – der Großteil (79 Prozent) zieht nationale Experten zurate. Ein bereits bestehendes Kooperationsverhältnis ist dabei von großer Bedeutung – Unternehmen vertrauen in dieser heiklen Thematik großteils auf langjährige Geschäftspartner, die oftmals auch den IT-Betrieb für das Unternehmen durchführen. Nur sechs Prozent der Unternehmen taten sich schwer, einen passenden Dienstleister für die Problematik zu finden. Fast alle Unternehmen (97 Prozent), die einen externen Dienstleister zurate ziehen, binden ihn in die technische Vorfallsbehandlung ein, denn bei dieser Herausforderung brauchen alle professionelle Unterstützung. Etwas weniger als die Hälfte (43 Prozent) beauftragte auch Berater für die organisatorische Vorfallsbehandlung – etwa in den Bereichen Krisenmanagement und Organisation.

Langjährige Zusammenarbeit führt dabei zwar zu einer hohen Kundenzufriedenheit: Die große Mehrheit (83 Prozent) gab bei der Umfrage an, mit dem externen Dienstleister äußerst zufrieden bzw zufrieden zu sein. Ein wichtiger Aspekt dabei: Unternehmen suchen sich bereits vor einer möglichen Cyberattacke einen passenden Dienstleister und sorgen damit für den Tag X vor. Hier beweist sich – wie so oft beim Thema Cyber Security: Vorsorge ist besser als Nachsorge. Nichtsdestotrotz birgt langjährige Zusammenarbeit aber auch einen Interessenskonflikt: Schließlich ist der der externe IT-Dienstleister, der nun den Cybervorfall bearbeitet, auch der, der für Cyber Security hätte sorgen sollen und nun möglicherweise seine eigenen Mängel aufarbeiten muss. Hier kann zusätzliche Unterstützung herangezogen werden.

Drohender Stillstand

Aus dem Vorjahr wissen wir, dass etwa jedes dritte Unternehmen in Österreich (31 Prozent) eine Cyberversicherung abgeschlossen hat. Der Markt der Cyberrisikoversicherungen wird in Österreich mittlerweile als eher beschränkt beurteilt, was an den sehr unterschiedlichen Prämienhöhen und -leistungen festgemacht wird. Diese Vermutung wird auch von Analysen des World Economic Forum (WEF) unterstrichen: Angesichts der zunehmenden Häufigkeit und Schwere von Ransomware-Schäden stiegen die Preise für Cyberversicherungen in den USA im dritten Quartal 2021 um 96 Prozent, was den stärksten Anstieg seit 2015 und einen Anstieg von 204 Prozent im Vergleich zum Vorjahr darstellt. Die Bereitschaft, eine Versicherung abzuschließen, sinkt mit steigenden Versicherungsprämien. Ist der Selbstbehalt sehr hoch und die Höchstentschädigung zu niedrig, erscheint es vielen Unternehmen rentabler, den möglichen Schaden selbst zu bezahlen.

Die wachsende geopolitische Bedrohungslandschaft stellt die Grenzen des Cyberversicherungssystems auf eine zusätzliche Probe: So wird es im Umfeld des aktuellen Ukraine-Russland-Konflikts beispielsweise immer wieder Hackerangriffe auf Unternehmen geben, die als virtueller, staatlich motivierter Vergeltungsschlag gewertet werden können. Versicherungen möchten sich ihrerseits verständlicherweise gegen diese drohende finanzielle Gefahr rüsten und arbeiten an Klauseln zum Ausschluss von Cyberkriegen in Versicherungspolizzen. Eine Entwicklung, die für die Branche interessante Auswirkungen haben könnte. Es bleibt abzuwarten, wie Unternehmen darauf reagieren werden.



»Wir brauchen eine gewisse Compliance, um einen definierten und verbindlichen Grundschutz zu erreichen.«

Pascal Lamia

Wir brauchen eine Zieltrias aus Politik, Gesellschaft und Wirtschaft

Das Steckenpferd von Björn Stahlhut ist der Umgang mit Krisen. Im Gespräch gibt der Teamleiter des Generalsekretariats des deutschen Roten Kreuzes Einblicke in aktuelle gesellschaftliche Herausforderungen.

FOTO © NICOLE LEHMANN/PRIVAT

Björn Stahlhut
ist seit 2009 Teamleiter im Generalsekretariat Deutsches Rotes Kreuz, zuständig für gesundheitlichen Bevölkerungsschutz, Breitenausbildung und Rettungswesen. Davor war er Offizier bei der Bundeswehr.

Erfahren Sie mehr in unserem Podcast IMPULSE

Erzählen Sie uns etwas über Ihre Funktion und Ihr Buch „Gesamtstaatliche Sicherheitsvorsorge: gerüstet für den Ernstfall!?".
Einer meiner Themenbereiche im Generalsekretariat des deutschen Rotes Kreuz ist der gesundheitliche Bevölkerungsschutz. Im Buch zeigen wir auf, welche sicherheitspolitischen Herausforderungen durch die Corona-Pandemie entstehen. Herausforderungen von nationaler Tragweite, die zum Umdenken bewegen – in Europa und weltweit. Herausforderungen, die nicht vom Gesundheitswesen allein zu bewältigen sind, weil sie Themen der Gefahrenabwehr, Lieferketten etc auf den Plan rufen. Der Lessons Learned-Prozess in Hinblick auf die Pandemie ist europaweit noch kaum im Gange. Hier haben wir enormen Aufholbedarf.

Warum ist das so? Stecken wir den Kopf in den Sand?
Unser Krisenbewältigungsmechanismen ist zu sehr auf die berühmt berüchtigte „Road to Zero" ausgerichtet – also die Fragestellung: Wie bringe ich die Corona-Fallzahlen auf null? Experten gehen davon aus, dass uns eine vergleichbare Situation in den nächsten fünf bis zehn Jahren in ähnlicher Form wieder bevorstehen kann. Wir müssen die Krisenbewältigungsmechanismen daher schnell weiterentwickeln. Auch in Bezug auf Autarkie der Lieferketten – denken wir an Rohstoffe für die Medikamentenproduktion. Wir brauchen am Ende eine Zieltrias, die Politik, Gesellschaft und Wirtschaft miteinander verknüpft. Noch denken und agieren wir zu säulenhaft und konzentrieren uns nur auf die Optimierung einzelner Bereiche. Die Herausforderungen von heute lassen sich nicht mehr nur mit Ressortzuständigkeiten bewältigen. Die Erfahrungen der Geschichte geben uns hier nicht die Antworten für die Zukunft.

Stichwort Cyberangriffe: Auch das IKRK musste hier leider vor kurzem Erfahrungen machen.
Zu Beginn des Jahres wurde ein Server des internationalen Komitees vom Roten Kreuz mit personenbezogenen Daten von über 500.000 Menschen weltweit in einem ausgeklügelten Cyberangriff gehackt. Brisant dabei ist die Art der Daten: Sie enthielten Angaben über Vermisste und Inhaftierte auch aus aktuellen Konflikten sowie ihre Familien – alles sensible Daten von höchst schutzbedürftigen Personen. Das IKRK hat rund 200 nationale Gesellschaften – 60 davon waren betroffen, auch Deutschland. Wir wissen aber mittlerweile, dass der Angriff zielgerichtet war. Was kann man mit solchen Daten anfangen? Sie lassen Rückschlüsse auf Familienangehörige zu, Menschen können dadurch auf unmenschlichste Weise erpressbar werden. Das ist eine ganz neue und verachtenswerte Art und Weise der Cyberkriminalität.

Durch hybride Methoden wird die Zivilgesellschaft in Konflikte hineingezogen – kann man das so sagen?
Das muss man unter dem Summenstrich so festhalten, ja. Wir haben dadurch eine erhöhte Betroffenheit der Zivilbevölkerung. Stichwort: Manipulation oder auch Fake News. Es wird immer häufiger versucht, Menschen und Stimmungen zu beeinflussen – pro Regierung, contra Regierung. Das wird zukünftig bei der Vorbereitung eines potenziellen Krieges eine wesentliche Rolle spielen.

Braucht es neue Rahmenbedingungen aufgrund der neuen Gegebenheiten?
Auf jeden Fall. Welche Regeln gelten etwa in einem Raum, der kein Staatsgebiet ist, in dem Teile eines bewaffneten Konfliktes mit hybriden Mitteln ausgetragen werden? Wir haben heute immer noch eine Krisenbewältigungsstrategie, die auf das Territorium zielt. Das beruht natürlich auf unserer Staatlichkeit – wir reden über ein Staatsvolk, über ein Staatsgebiet. Es braucht jedoch immer mehr Maßnahmen – insbesondere auch bei der Cybersicherheit –, die sich nicht auf territoriale Grenzen festlegen lassen. Es werden einige Neudefinitionen erforderlich und das wird eine der wesentlichen Herausforderungen auch für das humanitäre Völkerrecht.

Braucht die Gesellschaft einen generalistischeren Ansatz, um aktuelle Herausforderungen zu meistern?
Wir haben uns in den letzten Jahrzehnten an das Ausbleiben von Krisen gewöhnt, genauso sind wir nun auch aufgestellt und strukturiert. Es braucht eine Rekultivierung des strategischen Ansatzes, denn wir haben verlernt, generalistisch und über unsere Generation hinaus zu denken. Weg von der Einzellösung, hin zu einer Gesamtlösung innerhalb der genannten Zieltrias aus Politik, Gesellschaft und Wirtschaft. Wir sprechen immer von Resilienz und Autarkie. Das mag im Einzelfall relativ gut funktionieren, aber in der allgemeinen Krisenbewältigung hinken wir dem Idealbild stark hinterher. Wir müssen unser Ambitionslevel überdenken. Der Wunschgedanke der hundertprozentigen Sicherheit – egal in welchem Bereich – ist meiner Meinung nach dabei zu hinterfragen.

»Es braucht jedoch immer mehr Maßnahmen – insbesondere auch bei der Cybersicherheit –, die sich nicht auf territoriale Grenzen festlegen lassen.«

Da kommen viele Herausforderungen auf unsere Gesellschaft zu ...
Richtig. Wir sind weit davon entfernt „unser altes Leben zurückzubekommen" – eine Formulierung, die wir oft hören. Ich sage Ihnen: Das werden wir nicht wieder kriegen! Den Wert der Freiheit bekommen wir wieder, wir werden aber auch lernen müssen, ihn mit mehr Inhalt zu befüllen. Wir müssen als Gesellschaft umdenken und nicht alles immer sofort mit Euphorie, Aufgeregtheiten oder totaler Lethargie zur Kenntnis zu nehmen. Sondern bestimmte Dinge im Sinne einer neuen Normalität annehmen und gestalten – dazu gehören leider auch Krisen.

Unternehmen erkennen, dass Cybersicherheit ein Wettbewerbsvorteil ist

Zwei Cyberprofis am KPMG Round Table: Philipp Amann von Europol und Wolfgang Rosenkranz von CERT.AT über aktuelle Trends und die Rolle der Cybersicherheit für unsere Gesellschaft.

Herr Amann, können Sie uns einen Überblick darüber geben, welche Aufgaben Europol hat?
Amann: Ich arbeite für das europäische Zentrum zur Bekämpfung der Cyberkriminalität, das ist Teil der Europol, die in Den Haag sitzt. Wichtig dabei: Wir starten nicht unsere eigenen Ermittlungsverfahren, sondern unterstützen die EU-Mitgliedsstaaten bei ihren. Wir stellen Expertise und Services zur Verfügung und haben ein Netzwerk an Verbindungsbeamten, aber auch Netzwerke mit Industriepartnern, Universitäten und der CERT Community. Weil die Frage oft auftaucht: Im Gegensatz zu Europol hat Interpol einen globalen Auftrag mit mehr Mitgliedsstaaten – wir agieren primär innerhalb der EU.

Herr Rosenkranz, CERT.at ist das nationale Computer Emergency Response Team Österreichs – wie kann man sich die Tätigkeiten vorstellen?
Rosenkranz: CERT.at ist die österreichische Institution für Cybersicherheit. Leute verwenden gerne die Feuerwehr-Analogie, wenn sie über uns sprechen: Wenn es brennt, dann kommen wir. Das ist in puncto Cyberattacken auch richtig, aber im Tagesgeschäft sind wir vor allem auch eine Informationsdrehscheibe und fördern den Informationsaustausch. CERT.at ist Schnittstelle zwischen den unterschiedlichen Organisationen – von Behörden bis Unternehmen, von national bis international.

Was waren die einprägsamsten Ereignisse in den letzten 12 Monaten in puncto Cyberbedrohungen?
Amann: Ransomware ist und bleibt leider eine der Hauptbedrohungen und wurde vonseiten der Kriminellen perfide angepasst: Es erfolgen mehrschichtige Angriffe: Daten werden verschlüsselt, Unternehmen erpresst, Daten weiterverkauft – es ist leider ein lukratives kriminelles Geschäftsmodell geworden. Die Cybersicherheitsaspekte von Ransomware-Angriffen gehen weit über den finanziellen Schaden hinaus. Insbesondere mit Blick die kritische Infrastruktur kann man sagen: Ransomware kann zu einem Risiko für Leib und Leben werden. Neben Ransomware hat aber auch mobile Schadsoftware hat im letzten Jahr einen signifikanten Anstieg erlebt.
Rosenkranz: Man kann festhalten: Cyber-Kriminelle passen auf ihrer Seite an, sobald neue Sicherheitsmaßnahmen eingeführt werden. Sie agieren businessmäßig – die Zeiten der Script-Kiddies sind längst vorbei. Wir reden nicht mehr von Einzelpersonen, die versuchen dadurch ein paar Euro zu verdienen, sondern tatsächlich von organisierter Kriminalität.

Nur 14 Prozent der österreichischen Unternehmen wurden Opfer einer Ransomware-Attacke. Passiert in Österreich wirklich so wenig?
Rosenkranz: Unsere Erfahrung zeigt, dass es generell zu wenige Zahlen gibt. Selbst als CERT.at bekommen wir Angriffe oft erst mit, wenn Angreifer im Darknet damit prahlen. Es vertraut uns mittlerweile der Großteil der Unternehmen, aber oft regiert dennoch die falsche Scham. Und das erschwert das Arbeiten. Im Hinblick auf Ransomware glaube ich aber, dass die Zahlen durchaus stimmen könnten. Die kriminellen Gruppen gehen eher selektiv vor – sie suchen sich lukrative Opfer ganz bewusst aus.
Amann: Diesem Grundproblem des Zahlenmangels stimme ich zu. Zu zuverlässigen Daten zu kommen, den finanziellen Schaden zu beziffern – all das ist im Zusammenhang mit Cybercrime eine besondere Problematik. Das hat damit zu tun, dass Unternehmen einfach nicht berichten oder es unterschiedliche Standards gibt. Und zum Thema Ransomware: Es gibt Gruppen, die sich nur auf die „großen Fische" konzentrieren, aber die kleineren an andere Akteure weiterreichen. KMUs sind unserer Erfahrung nach somit genauso im Fadenkreuz der Angreifer.

Bringt es Unternehmen etwas, Lösegeldforderungen zu bezahlen?
Amann: Wir vertreten ganz klar die Position: Auf keinen Fall Lösegelder zahlen. Einerseits befeuert man damit das kriminelle Geschäftsmodell, andererseits hat man keinerlei Garantie, die Daten zurückzubekommen. Im schlimmsten Fall – und da gibt es zahlreiche Fälle – habe ich gezahlt, meine Daten verloren und trotzdem eine Betriebsunterbrechung. Natürlich sind die Gründe der Unternehmen für uns nachvollziehbar – man kann in so einem Fall durchaus vom wirtschaftlichen Nahtoderlebnis bei betroffenen Unternehmen sprechen. Eine solche Attacke kann den wirtschaftlichen Ruin bedeuten und man versucht natürlich alles, um dem zu entgehen.
Rosenkranz: Ein spannender Aspekt ist, dass so manche kriminelle Organisation mittlerweile so viel Geld mit ihren Machenschaften verdient, dass sie sich Angriffswerkzeuge leisten können, die früher staatlichen Stellen – also zB Nachrichtendiensten – vorbehalten waren. Durch das Zahlen von Lösegeldforderungen fördert man dieses System und schaufelt sich sozusagen sein eigenes Grab. Die Situation eskaliert immer mehr – und das ist eigentlich das Hauptproblem.

Philipp Amann
ist Head of Strategy beim European Cybercrime Centre (EC3) von Europol in Den Haag. Vor 2014 und seiner Tätigkeit bei Europol war Philipp Amann unter anderem beim Internationalen Strafgerichtshof, der Organisation for the Prohibition of Chemical Weapons und der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) tätig.

»Würden alle Unternehmen ihren Cybergrundschutz ordnungsgemäß einhalten, wäre ein riesiger Schritt getan.«

Wolfgang Rosenkranz
leitet das nationale Computer-Notfallteam „CERT.at". Davor war er als Cyber Security Koordinator des Kuratorium Sicheres Österreich (KSÖ) für die Organisation von Planspielen, Rechts-Technologie-dialogen und für das KSÖ Sicherheitsforum verantwortlich.

»Unternehmen vertrauen uns zwar, aber beim Austausch zu Cybervorfällen regiert immer noch sehr oft falsche Scham.«

Kann man diese Aufwärtsspirale der Cyberkriminalität überhaupt irgendwie stoppen?
Rosenkranz: Ich konzentriere mich in meiner Antwort jetzt einmal rein auf den Aspekt der Kooperation als Abwehrtool. Denn es muss irgendwann hoffentlich eine völkerrechtliche Antwort auf Cyberkriminalität geben. Länder müssen soweit verbindlich zusammenarbeiten, dass sie kriminelle Gruppen in ihrem Land zumindest nicht mehr schützen. Das wäre einer der wichtigsten Schritte. Leider ist das de facto noch nicht Realität.
Amann: Rechtliche Kooperationen müssen definitiv verbessert werden – damit meine ich sowohl Ermittlungsbehörden als auch Unternehmen oder Forschungsinstitute. Andererseits ist die Antwort oft auch simpel: Würden alle Unternehmen ihren Cybergrundschutz ordnungsgemäß einhalten, wäre ein riesiger Schritt getan. Wir müssen immer wieder darauf aufmerksam machen, dass man mit Prävention und Bewusstseinsbildung einen entscheidenden Schritt dazu beitragen kann. Es gibt viele einfache Mittel – klassisches Beispiel: Multi-Faktor-Authentifizierung –, um Daten effizient zu schützen. Es ist natürlich auch die Industrie gefragt – Stichwörter: Security by Design, Privacy by Design.

Muss man denn überhaupt noch darauf hinweisen, dass Cyber Security Aufgabe jedes Unternehmens ist?
Rosenkranz: Tatsächlich bin ich selbst oft irritiert, dass wir diese Basisgespräche ab und zu noch führen müssen. Aber leider: Ja, wir müssen. Dabei gibt es so viele Stellen, die mit Informationen auf Unternehmen zugehen: Polizei, Wirtschaftskammer, Industriellenvereinigung, Europol, CERT.at, etc. Es muss endlich in die Köpfe jedes noch so kleinen Unternehmers, dass Cybersicherheit keine Zusatzaufgabe ist, sondern essenzieller Teil der Digitalisierung. Es geht nicht nur um mich und mein Geschäft, es geht auch um eine kollektive gesellschaftliche Verantwortung.
Amann: Viele Unternehmen erkennen bereits, dass Cybersicherheit ein entscheidender Wettbewerbsvorteil ist. Natürlich ist Cyber Security mit Kosten und Mehraufwand verbunden, vor dem sich viele Unternehmen scheuen. So wie wir im Einkauf nicht immer auf den billigsten Produzenten setzen dürfen, so ist es auch bei der Sicherheit: Das entscheidende Bewertungskriterium externer Anbieter darf nicht der Preis alleine sein.

Ganz allgemein: Geht die Digitalisierung in die richtige Richtung?
Amann: Man muss die Entwicklung schon an manchen Stellen hinterfragen – ganz besonders wenn es um das Internet der Dinge geht. Muss wirklich jeder Kühlschrank und jeder Toaster mit dem Internet verbunden sein – und das unter dem Deckmantel der Digitalisierung? Dadurch werden natürlich viel mehr – und zum Teil unnütze – Angriffsflächen für Cyber-Kriminelle geschaffen. Manche Bereiche sollten vielleicht besser analog bleiben. Grundsätzlich aber bietet die Digitalisierung viel positives Potenzial.
Rosenkranz: Digitalisierung und Auditierung hängen stark zusammen und das ist richtig so. Es müssen entsprechende Rahmenbedingungen geschaffen werden. Die EU NIS-Direktive regelt im europäischen Raum die Cyber Security für kritische Infrastrukturen. Die neue EU NIS2 erweitert Sektoren und Cyber Security-Pflichten deutlich. Die Grundidee ist, mehr Unternehmen in die gemeinsame Aufsicht und Rechenschaftspflicht einzubinden. Der Aufwand ist sicher hoch, aber das lenkt die Digitalisierung ein Stück weit in die richtige Richtung.

Wann werden wir als Gesellschaft Cyber Security in unsere DNA integriert haben?
Rosenkranz: Das Sicherheitsbewusstsein steigt von Generation zu Generation. So wie wir von klein auf lernen, auf der Straße nach links und rechts zu schauen, bevor wir sie queren, so haben werden wir auch im Cyberraum immer vorsichtiger werden. Das geht natürlich nicht von alleine. Eine Herausforderung ist sicher, dass wir diese Form der Kriminalität immer noch nicht richtig fassen können – vielen Menschen ist Cybercrime zu abstrakt.

Provokant formuliert: Braucht Cybercrime mehr Leichen im Keller, um die Menschen zu sensibilisieren?
Amann: Je weniger Schaden an Leib und Seele, desto besser, natürlich. Aber ganz abstrakt ist all das nicht. Denken wir an die Fälle gehackter Kinderspielzeuge oder Herzschrittmacher. Mit etwas Fantasie kann man weiterspinnen, wie eine solche Geschichte zum echten Kriminalfall werden kann. Cyberkrimis helfen zwar dabei, die Leute zu sensibilisieren und wachzurütteln – am besten bleiben sie aber nur fiktiv!

Wenn wir uns in einem Jahr wieder treffen: Welche Dinge werden wir uns wünschen, getan zu haben?
Rosenkranz: Eine unserer größten Herausforderungen ist der Fachkräftemangel. Hier müssen wir strategisch aktiver werden. Wenn wir großflächige Angriffe haben, werden wir jede einzelne ausgebildete Person brauchen. Eine solche Ausbildung dauert entsprechend lange. Wir werden uns in einem Jahr wünschen, wirklich alles daran gesetzt zu haben, noch mehr Menschen für Cyber Security zu begeistern.
Amann: Wir werden uns wünschen, Theorie und Empfehlungen wirklich in die Praxis umgesetzt zu haben. Als nicht nur zu wissen, dass wir Cybersicherheit erhöhen müssen, sondern konkrete Maßnahmen abgeschlossen zu haben, um resilienter zu werden: im Ausbildungsbereich, in der Prävention, im Awareness Building, in der Technologie. Und wir werden uns wünschen, uns wirklich um unsere Basissicherheit gekümmert zu haben. Gemeinsam können wir es schaffen, die Digitalisierung sicher zu machen, ihre Vorteile zu nutzen und damit so manches gesellschaftliche Problem zu lösen.

Erfahren Sie mehr in unserem Podcast IMPULSE

Die strategischen Autonomie ist die Achillesferse der EU

Matthias Wasinger ist Gründer des Onlinejournals Defence Horizon mit sicherheits- und verteidigungspolitischem Fokus. Im Gespräch über Cyber Security aus militärwissenschaftlicher Sicht.

Erzählen Sie uns etwas über Ihren Zugang zu Cybersicherheit!
Ich beschäftige mich seit über zwei Jahrzehnten mit dem gesamten Spektrum der Sicherheits- und Verteidigungspolitik, sowohl national als auch international. Weiters bin ich Gründer des „The Defence Horizon Journals“: ein Open Source Onlinemagazin mit sicherheits- und verteidigungspolitischem Fokus.

Welche Ziele verfolgen Sie mit Ihrem Journal?
Ich möchte damit dem Staatsbürger globale Themen der Sicherheits- und Verteidigungspolitik aus unterschiedlichen Perspektiven näherbringen. Der Staat und internationale Organisationen stellen dem Bürger ein „Sicherheitsbecken“ zur Verfügung. Dieses muss er in der Lage sein, zu verstehen und zu beurteilen. Dafür gilt es, Wissen aus unterschiedlichen Perspektiven zu beleuchten – und das versuchen wir mit dem Journal. „The Defence Horizon“ ist ein Sammelsurium an unterschiedlichen Sichtweisen, eine Plattform, auf der Wissen generiert wird, um die Zusammenhänge besser zu verstehen.

Wie beurteilen Sie den Ukraine-Russland-Konflikt aus Cybersicht?
Es taucht immer wieder die Formulierung „neue Realität“ auf. Ich widerspreche dem sehr vehement, denn die Realität ist gleichgeblieben – sie hat sich nur am 24. Februar sehr brutal in unser Bewusstsein gedrängt. Cyber Security spielt dabei eine wichtige Rolle: Russische Cyberattacken auf die ukrainische Infrastruktur finden bereits seit Jahren statt. Diese rufen das Thema der strategischen Autonomie der Europäischen Union auf den Radar – die Achillesferse des Kontinents. Wenn wir strategische Autonomie als Fähigkeit definieren, eigene außen- und sicherheitspolitische Entscheidungen zu treffen, dann ist Cyber Security in Wahrheit ohne diese Autonomie sehr schwer.

Wie stufen Sie die europäische Handlungsfähigkeit in Sachen Cloud ein?
Europa ist hier sehr eingeschränkt. Niemand hat heute seine Server zur Datenspeicherung im eigenen Bürogebäude, alles läuft über die Cloud. Blickt man auf die Top 10 Cloud-Anbieter weltweit, wird man darunter keinen einzigen europäischen Konzern finden. Wenn am Ende des Tages alle Daten in einer Cloud gespeichert werden, die entweder über dem Atlantik oder in China disloziert sind und dort auch die eigentlichen gewerblichen Rechte liegen, wieviel Handlungsspielraum kann ich dann in puncto IT-Sicherheit haben? Wir haben hier einen enormen Aufholbedarf und wir landen wieder beim Stichwort: strategische Autonomie der Europäischen Union.

Geht Österreich in puncto Cybersicherheit den europäischen Weg?
Die österreichische Sicherheitsstrategie bekennt sich klar dazu, diese im Rahmen der Europäischen Union umzusetzen. Doch wie könnte die EU die Fähigkeit aufbauen, Daten geschützt und ohne Externe transferieren und speichern zu können? Schauen wir auf die USA: Der Staat hat dort einen Teilbereich der Cloud von Amazon angekauft und quasi teilverstaatlicht. Somit sind die Daten nicht mehr am gewerblichen Markt verfügbar, sondern Eigentum der US-Regierung. Ein Weg, der auch für die EU denkbar wäre. So ein Prozess geht nicht über Nacht – man muss derartige Dinge über zehn bis 15 Jahre planen und umsetzen.

Schlagwort: hybride Bedrohungen. Was ist Ihre Einschätzung dazu?
Von einem hybriden Konflikt spricht man salopp, wenn er unterhalb der Schwelle des bewaffneten Konfliktes beginnt, mehrere Instruments of Power einsetzt, oft nicht klar attribuierbar ist und manchmal dann auch im konventionellen Krieg endet. Man spielt Angriffe also quasi „über die Bande“. Bricht ein zwischenstaatlicher Konflikt aus, werden hybride Angriffe weiterhin fortgesetzt und verschwinden deshalb nicht. Die Mehrheit aller Handlungen findet heutzutage wohl genau dort statt. Entscheidend ist dabei auch der Faktor der Plausible Deniability, also der glaubhaften Abstreitbarkeit. Durch die Schaffung des hybriden Raums kann ich sagen: Das war ich gar nicht! Und das macht diese Herangehensweise natürlich attraktiver als der Einsatz von Streitkräften.

Können Unternehmen ein angemessenes Sicherheitsniveau gegen Cyberattacken etablieren?
Kein Unternehmen kann sich so schützen, dass es kein Einfallstor gibt. Dementsprechend wäre die Ableitung: Man muss Redundanzen aufbauen. Cyberattacken richten sich zumeist nicht auf die Attraktivität des Ziels, sondern über die Leichtigkeit des Zugriffes. Je leichter der Zugriff, desto wahrscheinlicher

Matthias Wasinger
ist Gründer des Onlinejournals The Defence Horizon Journal.

FOTO © MATTHIAS WASINGER PRIVAT

Erfahren Sie mehr in unserem Podcast IMPULSE

»Wenn wir strategische Autonomie als Fähigkeit definieren, eigene außen- und sicherheitspolitische Entscheidungen zu treffen, dann ist Cyber Security in Wahrheit ohne diese Autonomie sehr schwer.«

der Angriff. Es braucht also eine bestmögliche Mischung aus Redundanzen, Strategie und Abschreckung.

Stichwort Datenaustausch: Wie motiviert man Unternehmen, Cybervorfälle zu melden?
Es wird nicht nur durch rechtliche Verpflichtungen gehen. Unternehmen müssen den klaren Mehrwert ihres Handelns erkennen, um Informationen einzubringen. Es ist ein klassisches Give and Take. Doch das wird nicht nur durch rechtliche Verpflichtungen gehen. Unternehmen müssen ihren Nutzen sehen, dann werden sie die Karten auf den Tisch legen. Dafür braucht es einen strategischen und langfristigen Plan.

Österreich und die EU – haben wir unsere Cyberziele ausreichend definiert?
Die strategischen Dokumente der Republik Österreich bieten eine rechtlich gut erarbeitete und auch ambitionierte Ausgangsposition. Ziele erledigen sich jedoch nicht von alleine. Auch rechtlich gesehen muss man die Landesverteidigung in Bezug auf Cyberbedrohungen durch zusätzliche Aspekte im Bundesverfassungsgesetz wohl irgendwann ergänzen – man denke etwa an hybride Konflikte. Ich kann heutzutage die umfassende Landesverteidigung nicht auf die wirtschaftliche, geistige, militärische und zivile beschränken. Im Großen und Ganzen bin ich jedoch der Überzeugung, dass das österreichische Konstrukt passt.

Haben wir in einem Jahr einen kalten Cyberkrieg mit Russland?
Ich denke, den haben wir bereits heute. Rückblickend hätten wir bereits vor 15 Jahren beginnen sollen, ein besseres Sicherheitskonstrukt in Österreich aufzubauen, um uns selbst schützen zu können. Eines, das einerseits kompatibel mit unseren europäischen Partnern ist, andererseits unserer Neutralität Rechnung trägt. Eine Cyberstrategie, die eine Abhaltewirkung auf gewisse Zeit hat, sodass sich

»Wir haben hier einen enormen Aufholbedarf und wir landen wieder beim Stichwort: strategische Autonomie der Europäischen Union.«

Matthias Wasinger

Cyber-Kriminelle lieber auf ein leichter anzugreifendes Land konzentrieren. Doch wir können auch jetzt noch handeln – und das tun wir auch.

In unserer Umfrage haben mehr als 50 Prozent der befragten Unternehmen gesagt, dass sie gerade in puncto Cyber Security stärkere Unterstützung durch den Staat wünschen – was könnte der Staat hier für Unternehmen bereitstellen?
Es gibt unterschiedliche Herangehensweisen. Das eine ist das oft geforderte gesamtstaatliche Lagezentrum, eine Art gesamtstaatliches Führungszentrum in dem alle unterschiedlichen Akteure und Stakeholder eines Staates und auch die Instruments of Power vertreten sind – hier zählen auch Kernbetriebe im staatlichen, teilstaatlichen und rein privatwirtschaftlichen Bereich dazu –, die man einbindet, damit ein möglichst gesamtheitliches Lagebild generiert werden kann, um so Entscheidungen nicht nur fundiert treffen zu können, sondern auch entsprechend an die Stakeholder kommunizieren zu können, um einen Entscheidungsvorteil zu haben. Aber natürlich muss das ganzheitlich gesehen werden. Denn in einer verbundenen EU, in einem Kontinent, in dem die Arbeit frei, die Bewegung frei und alles frei zugänglich vernetzt ist, wird es auch nicht reichen, wenn Staaten als Insellösungen diese Entscheidungsvorsprünge erarbeiten. Man wird das nur gesamtheitlich lösen können und das führt uns dann wieder zurück zur österreichischen Sicherheitsstrategie.

1 — 2 — 3 — 4

Die Technologie

Mit enormer Geschwindigkeit

20% entsteht finanzieller Schaden durch Cyberkriminelle.

51% der Angriffe sind Phishingattacken.

67% der befragten Unternehmen waren in den letzten 12 Monaten Opfer eines Cyberangriffs.

Cyberkriminalität hat sich zu einer gewinnorientierten Industrie entwickelt. Und nahezu täglich tauchen neue Bedrohungen am Cyberhorizont auf – von auf AI basierenden Deepfake-Methoden bis hin zu Geschäftsmodellen wie „Cyber Crime as a Service“ oder „Ransomware as a Service“.

Auf Seite der Unternehmen wird ebenso investiert – mittlerweile verstärkt in Managementthemen (zB Business Continuity Management und Krisenmanagement) statt in reine Technologie-Aspekte. Und das ist gut so. Denn die Steigerung der digitalen Widerstandsfähigkeit ist für Unternehmen aller Größenordnungen essenziell.

Die Bestandsaufnahme

Fass ohne Boden: Aus unseren Umfragen der letzten Jahre wissen wir: Rund zwei von drei österreichischen Unternehmen sind jedes Jahr mit Cyberattacken konfrontiert, ein Großteil davon wird gleich mehrmals angegriffen. 2021 lag die Anzahl der Betroffenen bei 60 Prozent, bei unserer ersten Umfrage vor sieben Jahren waren 49 Prozent Opfer eines Angriffs. Die Dunkelziffer dürfte weit höher sein. So oder so: Der Trend geht nach oben und hält beständig an.

Die Ursachen dafür sind vielfältig: Auf der einen Seite die Professionalisierung und Hightechausstattung der Cyber-Kriminellen, kombiniert mit ihren immer kreativeren und aggressiveren Angriffsmethoden. Auf der anderen Seite oft lückenhafte Cyber Security-Strategien der Unternehmen und ihr Mangel an Cybersicherheitsexperten. Diese müssen in gewachsenen Organisationen und Strukturen für Ordnung sorgen und dabei mit ständig neu aufkommenden Bedrohungen und Schwachstellen umgehen.

Teamwork der Bösen

Gemeinsam statt einsam: Auf Seiten der Kriminellen tut sich ein besonders lukratives Geschäftsmodell auf: das illegale Angebot von „Cyber Crime as a Service“ im Allgemeinen und „Ransomware as a Service“ im Speziellen. Besonders letzteres hat im Jahr 2021 einen enormen Aufschwung erlebt. Cyber-Kriminelle setzen dabei auf Arbeitsteilung und stellen diese Tools als Service zur Verfügung. Das ermöglicht es auch technisch nicht so versierten Kriminellen, Angriffe auszuführen – ein Trend, der sich mit dem Aufkommen künstlicher Intelligenz (KI) noch verstärken könnte. Darüber hinaus ermöglichen Kryptowährungen den Kriminellen die Risiken der Entdeckung oder gar Rückforderung des Lösegeldes gering zu halten. Dieser gefährliche Mix verschärft das Risiko, angegriffen zu werden, weltweit – und auch in Österreich.

Angriff mit Auswirkungen

KMUs im Fokus: Dieses Jahr haben wir in unserer Österreich-Analyse den Fokus auf den erlittenen Schaden gelegt. Das Ergebnis: Jedem fünften attackierten Unternehmen (20 Prozent) entsteht durch Cyber-Kriminelle ein finanzieller Schaden. Am häufigsten entstehen den betroffenen Firmen Schäden in der Höhe von bis zu 10.000 Euro (46 Prozent). Darin nicht enthalten sind Investitionskosten in Technologien und Kosten für externe Dienstleister, die bei der Abarbeitung des Sicherheitsvorfalls unterstützen. Die Kosten in der Höhe von bis zu 10.000 Euro spiegeln auch die österreichische Unternehmenslandschaft wider, die von kleinen und mittelständischen Unternehmen geprägt ist. Die Zahl unterstreicht einmal mehr, dass auch sie im Fokus stehen. Dass die Schäden auch in Österreich bis zu fünfhunderttausend Euro (10 Prozent) und sogar in Millionenhöhe (2 Prozent) gehen können, darf dabei nicht außer auch gelassen werden, wie auch die Ergebnisse unserer diesjährigen Studie zeigen.

Ein interessanter Aspekt: Nach wie vor kann ein Viertel der Unternehmen (23 Prozent) die Höhe entstandener Schäden nach einer Cyberattacke nicht beziffern. Keine Überraschung ist dabei, dass große Unternehmen besser auf Cyberkriminalität vorbereitet sind als kleinere. Sie räumen Cyber Security seit vielen Jahren die notwendige Priorität und Strategie ein und sind daher besser geschützt. Die Kehrseite der Medaille: Oftmals weichen Cyber-Kriminelle auf leichter zu attackierende Ziele aus und konzentrieren sich auf Klein- und Mittelbetriebe, denen es an finanziellen oder personellen Ressourcen für Cybersicherheit fehlt. Oftmals fehlt ihnen auch das Wissen über aktuelle Bedrohungen, da das Thema bei ihnen noch nicht den entscheidenden Stellenwert besitzt. Gerade diese Unternehmen stellen einen wesentlichen Teil der heimischen Volkswirtschaft dar und bedürfen zukünftig einer besonderen Aufmerksamkeit und Unterstützung. Sie müssen auf einen sicheren Weg am Pfad der Digitalisierung begleitet werden – und das mit fachkundigen Experten, die es verstehen, zielgruppengerecht Wissen zu vermitteln und Unterstützung zu bieten. Hochkomplexe Erklärungen und das Schüren von Ängsten sind hier fehl am Platz!

Im Mai 2021 wurde der amerikanische Energieversorger Colonial Pipeline von einer Ransomware-Attacke heimgesucht. Diese zwang das Unternehmen dazu, seinen Betrieb vorübergehend einzustellen, um die Infektion zu isolieren. Die Probleme mit der Ölversorgung führten zu Panikkäufen in einigen Städten in den USA. Der Angriff wurde jedoch auch zu einer Erfolgsgeschichte der US-Justiz: 2,3 Millionen Dollar des Lösegeldes, das Colonial an DarkSide gezahlt hatte, konnte beschlagnahmt werden.

Die Methoden der Kriminellen

Auf der Überholspur: Ein Blick auf die weltweite Realität zeigt, dass die Bedrohungslage im Cyberraum kontinuierlichen Änderungen unterworfen ist und demgemäß auch rasant ansteigt. Folgende Zahlen verdeutlichen diese Entwicklung sehr plakativ: Im Jahr 2020 erhöhte sich die Anzahl der Angriffe durch Malware und Ransomware weltweit um 358 bzw 435 Prozent – Tendenz steigend. Auch in Österreich nehmen Attacken zu – die häufigsten Angriffsarten bleiben jedoch gleich. Die internationalen Konflikte bestätigen ebenfalls diese Entwicklungen.

Oldies but Goldies: An erster Stelle rangieren auch dieses Jahr Phishingattacken (51 Prozent), dicht gefolgt von Business E-Mail Compromise bzw CEO/CFO Fraud (41 Prozent) und Denial of Service Attacken (DoS, 41 Prozent). Auch Malware-Angriffe sind mit 39 Prozent unter den Top-Angriffsarten hierzulande. Für sie alle gilt: Die Angriffsvektoren werden immer perfider (zB ein anscheinend entgangener Anruf mit einer Sprachnachricht in MS Teams) und gezielter (zB das vemeintliche Office Dokument, das mit mir geteilt wird) und erfolgen oft in Kombination mit anderen zeitgleich durchgeführten Attacken. Ein äußerst raffinierter Ansatz des Cyberbetrugs sind dabei Deepfakes, also Phishing mittels hochtechnischer Manipulation. Durch den Einsatz von KI werden Stimme und Aussehen einer Person imitiert. Die Endresultate sind Audio- oder Videoaufnahmen, die teilweise kaum von der Realität zu unterscheiden sind. Gerade durch die verstärkte Nutzung von online Kollaborations- und Kommunikationstools ist vieles möglich – und so findet ein Gespräch mit dem vermeintlichen Vorgesetzten oder Kollegen statt, ohne zu wissen, dass man eigentlich mit einer fremden Person spricht. Für einige mag das nach Sicence Fiction klingen – doch aus Science Fiction wurde schon vor langem Science Facts.

Trends über Trends

Aus der Tasche gezogen: Zur Herausforderung für immer mehr Unternehmen wird der Bereich Data Breach. Darunter versteht man den Verlust von personenbezogenen, sensiblen und besonders schützenwürdigen Daten (zB Geschäftsgeheimnisse) eines Unternehmens. Verbuchten im Vorjahr nur neun Prozent der Unternehmen einen solchen Angriff, geben mittlerweile schon 14 Prozent an, davon betroffen gewesen zu sein. Kein Wunder, denn laut COVEWARE beinhalten mittlerweile über 84 Prozent der Ransomware-Angriffe weltweit neben der Dateiverschlüsselung auch den Diebstahl von Unternehmensdaten.

Dahin geht die Reise: Europol skizziert folgende Tendenzen: Phishing und Social Engineering sind nach wie vor die Hauptbetrugsarten im Zahlungsverkehr und nehmen sowohl an Umfang als auch an Raffinesse zu. Ransomware-Operationen konzentrieren sich zunehmend auf Unternehmen und ihre Lieferketten, während Social Engineers ihre Aufmerksamkeit auf die oberen Führungsebenen verlagern.

Ransomware: Die große Bedrohung

In die Mangel genommen: Weltweit gelten Ransomware-Angriffe, bei denen Daten verschlüsselt und nur gegen Zahlung eines Lösegeldes wieder freigegeben werden, bedauerlicherweise als gut funktionierendes Geschäftsmodell für Cyber-Kriminelle. War es oft möglich, sich mit guten Back-up- und Restore-Prozessen zu schützen, haben die Cyber-Kriminellen längst ihr Erpressungsrepertoire um die Veröffentlichung von Daten bei Nichtbezahlung des Lösegeldes erweitert. Laut World Economic Forum (WEF) betonen 85 Prozent der befragten Meinungsführer, dass Ransomware zu einer wachsenden Bedrohung wird und ein großes Problem für die öffentliche Sicherheit darstellt. Rund 44 Prozent der Ransomware-Angriffe weltweit betreffen aktuell Unternehmen mit 101 bis 1.000 Mitarbeitern. Im Durchschnitt sind diese anschließend mit 20 Tagen

10% verzeichneten Schäden in der Höhe von bis zu 500.000 Euro.

14% der Angriffe hatten einen Data Breach.

14% der Unternehmen sind von Ransomware betroffen betroffen.

41% der Angriffe sind Business E-Mail Compromise bzw CEO/CFO Fraud und Denial of Service-Attacken.

46% davon erleiden Schäden in der Höhe von bis zu 10.000 Euro.

Betriebsunterbrechungen konfrontiert. Die durchschnittlichen Lösegeldzahlungen im 4. Quartal 2021 betrugen rund 322.000 Dollar.

(K)eine Pandemie in Österreich

Gegen den Strom: Bei der Erpressersoftware scheint Österreich aktuell dem Trend noch zu trotzen. Lediglich 14 Prozent geben an, mit dieser Angriffsmethode in Berührung gekommen zu sein. Ist Österreich also eine Insel der Seligen? Wohl eher nicht. Die Angriffe finden in Österreich tendenziell noch eher gezielt auf größere Unternehmen statt, um möglichst lukrativ zu sein. Im weltweiten Vergleich wendet sich das Blatt aktuell allerdings zu Gunsten der ganz Großen: Laut COVEWARE lässt sich eine Verschiebung von der „Großwildjagd" hin zur „Mittelwildjagd" erkennen. Cyber-Kriminelle versuchen so, strafrechtliche Konsequenzen zu vermeiden. Grundsätzlich sind die Einfallstore vielfältig. Ransomware kann über drei Wege auf Geräte und Systeme gelangen: Erstens über nach außen verfügbare Anwendungen wie zum Beispiel SharePoint, Exchange oder Citrix, zweitens über Phishingmails und drittens über externe Remote Services (RDP). Die Corona-Pandemie hat hier jedenfalls dazu beigetragen, dass sich die Angriffsfläche dramatisch vergrößert hat.

Technologien im Fokus

Am aufsteigenden Ast: Wechseln wir von der Täterseite zu den Unternehmen: Welche Cyber Security-Bereiche haben in Österreich im letzten Jahr an Bedeutung gewonnen? Auch hier haben wir einen genauen Blick auf die heimischen Unternehmen geworfen. Vulnerability Management, also die Identifikation, Bewertung und Behandlung potenzieller Schwachstellen, Third Party Risk Management, Risiken aus der Zusammenarbeit mit Dritten, und Business Continuity Management (BCM), die Funktionsfähigkeit unternehmenskritischer Geschäftsprozesse und Ressourcen sind am Vormarsch. Sie alle haben in ca jedem zehnten Unternehmen in den letzten zwölf Monaten an Wichtigkeit gewonnen. International ist ein Trend zu Angriffen auf das schwächste Glied und damit eine Infektion der eigentlichen Ziele innerhalb der digitalen Lieferkette (Cyber Supply Chain) festzustellen. Das zeigt auf, wie wichtig es ist, die Sicherheit und Widerstandsfähigkeit aller Partner der Lieferketten im Auge zu behalten – das wissen auch die Angreifer. Dicht gefolgt werden die genannten technologischen Themen von End User Security, Security Information and Event Management (SIEM) und Governance Themen (Security Regulations & Compliance).

Managementthemen am Vormarsch

Klar verdrängt: Vergleicht man die Angaben mit dem Vorjahr, so zeigt sich: Insbesondere BCM wurde in den letzten Jahren systematisch vernachlässigt und hat nun endlich seine ihm zustehende Wichtigkeit gewonnen. War das Thema im Vorjahr noch im zweiten Drittel des Rankings zu finden, so ist es nun zum Spitzenreiter geworden und hat sogar den „Dauerbrenner" End User-Sicherheit auf der Prioritätenliste geschlagen. Auch das gerne vernachlässigte Thema Third Party Risk Management hat stark aufgeholt und arbeitete sich vom drittvorletzten Platz im Vorjahr auf das Prioritäten-Stockerl.

Doch welche Erkenntnis lässt sich hier ablesen? Eines zeigt sich deutlich: Unternehmen geben den Managementthemen den Vortritt vor rein technischen Bereichen. Sie haben einen Reifegrad erreicht, in dem es längst nicht mehr „nur" um die Abdeckung technischer Sicherheitsaspekte zum Schutz vor Cyber-Kriminellen geht. Sie arbeiten intensiv auf einer Governance- und Managementebene, um sich im Bereich Cybersicherheit bestmöglich zu wappnen. Natürlich bedeutet der Gewinn an Wichtigkeit der einzelnen Themen nicht, dass Unternehmen ihren Schutz automatisch optimiert haben. Doch es zeigt klar: Sie erkennen, wo die Reise hingeht.

Offene Baustellen

Vertrauen ist schlecht: Nichtsdestotrotz entsprechen die bisher getroffenen technologischen Maßnahmen oft nicht dem Ernst der Lage. Insbesondere aufgrund des Trends zu hybriden Arbeitswelten kommt etwa dem Identitätsmanagement eine große Rolle zu – Stichwort: Zero Trust. Jeder Nutzer, jede Anwendung, jedes Gerät, das von intern oder extern auf Unternehmensdaten zugreifen will, muss sich gemäß diesem Konzept authentifizieren und wird überprüft. Darüber hinaus braucht es weitere zielgerichtete Investitionen und eine bessere Vorbereitung auf den Krisenfall.

Von Beginn an: Security by Design, also die Berücksichtigung von Security-Elementen bereits während der Produktentwicklung, ist und bleibt ein Stiefkind. Und das, obwohl es schon mit dem Bekanntwerden der Datenschutzgrundverordnung (DSGVO) vor mehr als vier Jahren explizit gefordert wurde – dort unter dem Begriff „Privacy by Design". Seit Jahren wird darauf hingewiesen, dass die eigentliche Ursache für Cyberangriffe oft in Sicherheitslücken bei den Herstellern liegt – betroffen sind sowohl Hardware als auch Software. Vorfälle der jüngeren Vergangenheit – wie etwa Log4j oder Spring4Shell – demonstrieren uns diese Abhängigkeit und Komplexität aufs Neue. Seit Jahren werden klarere Regelungen diskutiert, viele fordern auch, dass der Gesetzgeber die Haftung der Hersteller für Sicherheitsmängel verschärft. Nur so können bessere Systeme auf den Markt kommen und so mancher Cyberangriff im Vorhinein ausgeschlossen werden.

2021 stieg der Betrug beim Internet-Banking im Vereinigten Königreich im Vergleich zu 2020 um 117 Prozent im Volumen und 43 Prozent im Wert an, da die Menschen mehr Zeit mit Onlineinkäufen verbrachten. 2021 gab es in Österreich 46.000 Cybercrime-Anzeigen, um fast ein Drittel mehr als 2020. Laut Kriminalstatistik entfällt der Großteil davon auf Betrugsdelikte, bei Erpressungen ist der Überblick schwierig, weil die Dunkelziffer sehr hoch sein dürfte. «

Zusammenarbeit und Wissensaustausch sind essenziell

Als eines der führenden Technologieunternehmen ist die Infineon Technologies Austria AG mit besonderen Herausforderungen der Cyber Security konfrontiert. Wie das Unternehmen damit umgeht und was in puncto Cybersicherheit noch notwendig ist, darüber sprechen Infineon Vorstandsvorsitzende Sabine Herlitschka und CISO Raphael Otto im Interview.

FOTO © INFINEON AUSTRIA

Sabine Herlitschka
ist seit 2011 Mitglied des Vorstandes der Infineon Technologies Austria AG, wo sie seit Jänner 2012 als Vorstand die Bereiche Technik und Innovation verantwortet. Seit April 2014 ist sie als Nachfolgerin von Monika Kircher Vorstandsvorsitzende der Infineon Technologies Austria AG.

Wie hat sich der Stellenwert von Cyber Security im gesamten Unternehmen im Gegensatz zum letzten Jahr geändert?
Cyber Security hat für Infineon seit jeher einen sehr hohen Stellenwert. Zunehmend verschiebt oder erweitert sich die Bedeutung aber von einer rein technischen Expertenfunktion zu einer strategisch beratenden Enabling-Funktion.

Was sind aus Ihrer Sicht die wesentlichsten Cyberbedrohungen für Infineon?
Durch Cyberangriffe verursachte Produktionsausfälle oder Industriespionage gehören zu den Top-Bedrohungen für unsere Branche.

Wie hat sich das Thema Industriespionage für Infineon in den letzten zwei bis drei Jahren verändert? Gibt es ein neues Gefahrenpotenzial?
Wir beobachten eine konstante Gefährdung durch Cyber-Industriespionage, die sich aber nicht wesentlich verändert. Natürlich gibt es abseits davon ständig neue Angriffsvektoren, vielfältige Akteure und umfangreiche Gegenmaßnahmen. Deren Auswertung und Anwendung gehört für uns jedoch seit vielen Jahren zum Tagesgeschäft.

Infineon ist sowohl Teil der internationalen Supply Chain für Halbleiterlösungen als auch Kunde von anderen Technologieanbietern. Wie weit ist Infineon anderen Unternehmen in der Erfüllung von Cyber Security-Anforderungen an Supply Chains voraus?
Als global agierendes Unternehmen, welches eine Vielzahl von Märkten bedient, muss Infineon verschiedensten Anforderungen in seiner Forward Supply Chain gerecht werden. Dies tun wir mit hoher Sorgfalt gemeinsam mit unseren Kunden – ganz besonders auch im Bereich Cyber Security. Die zunehmend nationale Regulierung im Bereich Cybersicherheit erhöht die Komplexität in diesem Bereich deutlich. Entsprechende Anforderungen geben wir an unsere eigene Supply Chain weiter, wobei wir hier zusätzliche Anforderungen definieren, die durch unser Cyber Security-Risikomanagement als relevant identifiziert wurden.

Sind Supply Chain-Angriffe die aktuelle Achillesferse der Digitalisierung oder wird die Bedrohung überbewertet?
Mit zunehmender Digitalisierung steigt automatisch die systemische Vernetzung und Integration von Systemlandschaften, aber auch die mit Kunden und Zulieferern. Entsprechend kann sich die Resilienz des Gesamtsystems verschlechtern, wenn einzelne Komponenten des Systems nicht ausreichend geschützt sind. Dadurch können Supply Chain-Angriffe natürlich eine Schwachstelle darstellen – obwohl der Begriff hier zuerst ausreichend differenziert werden müsste. Da Unternehmen oft nur indirekt auf die Sicherheit der Supply Chain einwirken können, ergeben sich daraus nicht zu vernachlässigende Herausforderungen. Ich würde dennoch nicht von einer Achillesferse der Digitalisierung sprechen. Es gab in jüngster Vergangenheit einige prominente Beispiele solcher Angriffe, die auch zum Aufschwung des Begriffes beitragen.

Welche Empfehlungen haben sie hier für andere Unternehmen, die Sie, wenn es um das Thema Sicherheit der Supply Chain geht, teilen können?
Zusammenarbeit und Wissensaustausch sind essenziell: Der Austausch mit anderen Unternehmen der eigenen Branche, aber auch branchenübergreifend, und die Mitarbeit in entsprechenden Gremien und Branchenverbänden hat sich für uns jedenfalls bewährt.

Spielt das Thema der internationalen Vernetzung mit anderen Organisationen und staatlichen Stellen, wie sie bei Infineon durch die internationalen Produktionsstandorte eindeutig vorhanden ist, eine Rolle bei Ihrer Gefahreneinschätzung durch Cyberangriffe?
Vernetzung mit anderen Organisationen und deren Cyber Security-Teams ist ein Kernbestandteil unserer Strategie, unabhängig von der Standortverteilung. Ohne einen solchen Austausch ist moderne Cyber Defense nicht möglich. Denn Angreifer arbeiten ebenfalls zusammen, also müssen wir dies auch in der Verteidigung tun.

Sind wir, was Cybersicherheit anbelangt, in Österreich bereits an dem Punkt angekommen, an dem wir sein sollten?
Zunächst einmal ist Cybersicherheit keine rein nationale Frage. Der Cyberraum kennt keine

»Die Cyberresilienz eines Gesamtsystems kann sich verschlechtern, wenn einzelne Komponenten des Systems nicht ausreichend geschützt sind.«

FOTO © INFINEON AUSTRIA

Raphael Otto
ist Vice President Cyber Security & CISO Infineon Technologies AG, Diplom Informatiker und ehemaliger „Ethical Hacker"

»Vernetzung mit anderen Organisationen und deren Cyber Security-Teams ist ein Kernbestandteil unserer Strategie, unabhängig von der Standortverteilung.«

geografischen Grenzen. Global betrachtet ist Cybersicherheit im stetigen Wandel und wird dies auch bleiben. Angriffs- und Verteidigungsstrategien müssen permanent aufeinander abgestimmt werden, Entscheidungen müssen durch möglichst hohe Risikotransparenz unterstützt und Mitarbeitende, aber auch die Bevölkerung als Ganzes, im sicheren Umgang mit Technologien geschult und unterstützt werden.

Wenn ein Unternehmen seine IT-Security-Strategie ausweiten möchte, was haben Sie an Empfehlungen für Führungskräfte für die nächsten Schritte?
Zu Beginn ist eine Differenzierung zwischen IT-, Cyber- und Informationssicherheit notwendig. Zwar überlappen diese Bereiche, sind aber im Detail unterschiedlich ausgeprägt. Je nach Größe und Sektor des Unternehmens macht es Sinn, unterschiedliche Prioritäten zu setzen. In jedem Fall sollte eine Abwägung zwischen reiner Compliance und echtem Risikomanagement getroffen werden.

Aus meiner Sicht ein zu häufig gemachter Fehler ist folgender: Unternehmen implementieren ein Standardframework und gehen dann davon aus, dass sich die Cybersicherheit dadurch verbessert hat. Dabei ist es viel wichtiger zu verstehen, wer ein Unternehmen angreifen will und wie man sich am besten davor schützt. Erfolgt dies kontinuierlich und nachhaltig, kann man von einer verbesserten Cybersicherheitsstrategie sprechen. In der Regel erzielt man damit gleichzeitig einen Shift von rein präventiven Maßnahmen hin zu Maßnahmen, die sowohl präventive als auch reaktive Komponenten beinhalten und dadurch die Resilienz steigern.

Infineon betreibt ein eigenes Cyber Defense Center und ein PSIRT. Ist das ein Modell für besonders gefährdete Branchen?
Nein, beides ist mittlerweile gängige Praxis und wird von international agierenden Unternehmen häufig so praktiziert.

Soll es eine staatliche Organisation geben, die sich ausschließlich mit Cyber Security auseinandersetzt?
Es gibt staatliche Organisationen, die sich mit Cyber Security beschäftigen. Da Cyber Security aber kein nationales Thema ist, sollten diese vermehrt auf internationaler, insbesondere aber auf europäischer Ebene kooperieren. Europäische Organisationen sollten jedenfalls gestärkt werden. Gleichzeitig sollten die Ziele dieser Organisationen geschärft werden. Zuständigkeiten für Bevölkerungsschutz, Schutz staatlicher Institutionen und Schutz des jeweiligen nationalen Wirtschaftsraums sind oft nicht ausreichend definiert.

In welchem Bereich müsste es einen wesentlichen Fortschritt geben, damit Cyberangriffe reduziert werden?
Eine hohe Zahl erfolgreicher Angriffe geht auf falschen oder unbedarften Umgang mit Technologien und Angeboten im digitalen Raum zurück. Ein oft vernachlässigtes Thema ist die Breitenbildung. Unternehmen investieren sehr viel in die Weiterbildung der Mitarbeitenden – Stichwort Awareness. Diese können die Herausforderung aber nicht allein lösen. Um Bürgerinnen und Bürger zu befähigen, bessere und korrektere Risikoabschätzungen im Umgang mit digitalem Raum zu treffen, müssen Bildungspläne angepasst und neue Bildungsangebote geschaffen werden. Es geht dabei nicht um Fachkräfte, sondern darum, Gesellschaft als Ganzes zu sensibilisieren und zu bilden.

Diese Befähigung sorgt dann für eine insgesamt höhere Hürde, die Angreifer zu überwinden haben und gleichzeitig – hoffentlich – für mehr Akzeptanz und breitere Nutzung gängiger Sicherheitsmaßnahmen wie etwa Multifaktor-Authentifizierung.

Ebenfalls ein bereits erwähntes Problem ist die rein nationale Betrachtung des Cyberraums und möglicher Gefahren. Erfolgreiche Angriffe und Angriffsversuche müssten auf breiter Front international verfolgt und Rückzugsräume entzogen werden. Dadurch würden zumindest die Risiken für Angreifergruppen aus dem Umfeld der organisierten Kriminalität steigen und Angriffe etwas weniger attraktiv. Dass diese Aktion durchaus Wirkung zeigen kann, zeigt das Vorgehen des FBI der USA als Reaktion auf die Angriffe auf die Colonial Pipeline.

1 — 2 — 3 — 4

Der Mensch

Der schützende Panzer

26% rekrutieren IT-Experten leichter im europäischen Ausland als in Österreich.

40% beschäftigen 1-2 Mitarbeiter für Cyber Security.

40% werben aktiv Sicherheitsexperten von anderen Unternehmen ab.

71% werden auf einen Cyberangriff durch eigene Mitarbeiter aufmerksam.

74% haben Schwierigkeiten beim Rekrutieren von IT-Experten.

Cyber Security ist kein IT-Thema. Sie haben richtig gelesen! Denn der Dreh- und Angelpunkt in allen Cybersicherheits-Belangen ist der Mensch. Er ist einerseits die beste und stärkste Firewall, die wir haben und zugleich die größte Schwachstelle. Der Mensch ist das entscheidende Zahnrad.

Es braucht genau seine besonderen Fähigkeiten, um das Unternehmen bestens zu schützen – das ist allerdings nicht immer ganz so einfach, Stichwort: Fachkräftemangel. Und es braucht sein Verständnis und Engagement, um die bereits bekannten, aber auch neu entfaltenden Bedrohungen im Arbeitsalltag unmittelbar zu erkennen – Stichwort: Awareness Building und Sensibilisierung.

Natürlich spielt auch die Technologie eine entscheidende Rolle im Zusammenspiel der einzelnen Teile im Cyber-Puzzle: Sie bildet die solide Basis, um mit weiteren Cyber Security-Lösungen darauf aufbauen zu können und so ein höheres Schutzniveau zu erreichen. Dennoch: Die MitarbeiterIn spielt die Hauptrolle im Cyberkrimi.

Schwachstelle Mensch

Ernüchternde Fakten: Studien gehen davon aus, dass zwischen 88 und 95 Prozent der Cybersicherheitsprobleme auf menschliches Versagen zurückzuführen sind. Unternehmen, die Cyber Security bisher als reines IT-Thema gesehen haben, sollten diese Zahlen wachrütteln.

Denn immer wieder fallen Unternehmen, die viel Geld ausschließlich in moderne Cybersicherheitslösungen investieren, Hackern zum Opfer, die clevere Spear-Phishingmethoden anwenden. Je perfider die Angriffsmethoden, desto entscheidender der Mensch.

Vermutlich weniger überraschend für Unternehmen ist die Erkenntnis, dass hybride Arbeitswelten das Risiko eines erfolgreichen Cyberangriffs deutlich erhöhen. Gründe dafür sind einerseits die schwächeren Sicherheitsstandards der Heim-IT auf der technologischen Seite. Andererseits erhöht das Homeoffice aber auch die Wahrscheinlichkeit, dass Mitarbeiter außerhalb ihrer sozialen Unternehmensstrukturen um einiges leichter zu täuschen sind (zB Deepfakes).

Menschliche Firewall

Die gute Nachricht: Mitarbeiter sind gleichzeitig der beste Schutzmechanismus. 71 Prozent der österreichischen Unternehmen geben in unserer Umfrage an, auf einen Cyberangriff durch eigene Mitarbeiter aufmerksam geworden zu sein. Zum Vergleich: Nur jede zweite Attacke (54 Prozent) wurde aufgrund interner Sicherheitssysteme (NextGen Firewall, XDR etc) sichtbar.

Das Fazit ist eindeutig: Unternehmen müssen ihre Bemühungen im Bereich Human Firewalling definitiv noch weiter verstärken. Sie müssen ihre Mitarbeiter laufend über die neuesten Bedrohungen, Tricks und Kniffe, sowie daraus abzuleitende Vermeidungsstrategien und Handlungsmaßnahmen schulen. Das Ziel: Mitarbeiter sollten sowohl die Grundsätze der Cybersicherheit verstehen als auch ihre Rolle bei der Abwehr unbedingt annehmen. Strategische awareness-building ist der entscheidende Baustein. Bewusstseinsbildende Schulungen für Mitarbeiter sind ein Muss und können Unternehmen vor Cyberangriffen und deren schwerwiegenden Folgen viel besser schützen als pure Technologie. Die Inhalte unterliegen einem wichtigen Wandel: Noch stehen oft technisch geprägte Bereiche im Fokus, der Trend geht aber eindeutig in Richtung vielfältigem Trainingsmaßnahmen-Mix. Und hier gilt es auch einen didaktischen Schwenk vorzunehmen: Nämlich weg vom ausschließlich compliance-motivierten Frontalvortrag hin zum Erkennen von Angriffen und dem bewussten und selbstbestimmten Umgang damit.

Übrigens: Österreichs Mitarbeiter sind kaum selbst die Täter. Der österreichische Bericht Cybersicherheit 2020 zeigt, dass hierzulande primär Außentäter oder technische Gebrechen Vorfallsverursacher sind. Innentäter waren nur bei einer geringen Anzahl von Vorfällen involviert. Diese Statistik zeigt im Vergleich mit den Vorjahren auch: Die Gefährdung durch Außentäter nimmt stark zu, die Gefährdung durch Innentäter bleibt eher gleich.

Heiß begehrt

Klarer Kurswechsel: Um Cyber-Kriminellen Paroli bieten zu können, braucht es entsprechende Strukturen bei Technologie, Organisation und Personal. Wie viele Menschen sich dem Thema im Unternehmen widmen, ist nicht nur eine Frage der Größe, sondern auch der Wertigkeit und Wichtigkeit von Cyber Security. Ein Großteil der österreichischen Unternehmen (40 Prozent) beschäftigt ein bis zwei Mitarbeiter, die dezidiert für Cyber Security zuständig sind, ein Viertel (24 Prozent) drei bis fünf. In jedem zehnten Unternehmen (11 Prozent) sind

» 2019 täuschte eine Deepfake-Audio Mitarbeiter des britischen Tochterunternehmens eines deutschen Energiekonzerns. Die Betrüger riefen mit der gefälschten Stimme eines Vorstandsvorsitzenden den britischen Geschäftsführer an. Sie wiesen ihn an, Geld an einen Lieferanten zu überweisen. Die Mitarbeiter überwiesen 220.000 Euro an die Betrüger. «

sogar mehr als 20 Mitarbeiter für Cybersicherheit im Einsatz. Gerade im Vergleich zum letzten Jahr konnten wir hier eine Zunahme feststellen: Unternehmen suchen verstärkt nach Mitarbeitern für das Thema. Blicken wir fünf Jahre zurück, so waren Stellenausschreibungen für Cyber Security-Experten noch eher selten. Heute erleben wir eine neue Dynamik – die ausgeschriebenen Stellen können nur schwer besetzt werden.

Ein Detail am Rande: Für 42 Prozent der Unternehmen sind Zertifizierungen der Mitarbeiter (zB CISSP, CEH, CISA etc) für den Einstieg in das Unternehmen bzw bei einer Bewerbung nicht relevant. Einschlägige IT-Sicherheitszertifizierungen sind nur für knapp ein Fünftel der Unternehmen (17 Prozent) von Bedeutung. Der Trend geht in eine andere Richtung: Jedes zweite Unternehmen (47 Prozent) ist bereit, die Zertifizierungskosten für die Mitarbeiter zu übernehmen. Anders gesagt: Österreichs Unternehmen sehen es mittlerweile als ihre Aufgabe, selbst dafür zu sorgen, dass ihre Cyber Security-Mitarbeiter Zertifizierungen und Ausbildungen erlangen.

Auf der Suche

Doch die Realität zeigt: Wenn Unternehmen Mitarbeiter einstellen wollen, finden sie oft keine. Der Mangel an qualifiziertem Personal bereitet den meisten Cyber Security-Verantwortlichen Kopfzerbrechen. Dreiviertel der Unternehmen (74 Prozent) geben in unserer Umfrage an, Schwierigkeiten beim Rekrutieren von IT- und Security-Experten zu haben. Fast die Hälfte der Unternehmen (43 Prozent) benötigt für die Einstellung (Zeitpunkt bis zur Vertragsunterzeichnung) eines Mitarbeiters durchschnittlich vier bis sechs Monate.

Die Prognose: Fachkräftemangel wird aufgrund der voranschreitenden Digitalisierung zum Dauerbrenner werden. Parallel dazu fahren Unternehmen ihren Bedarf an Sicherheitsexperten wegen zusätzlicher Governance-Themen (zB DSGVO, NIS 2.0, Third Party Risk und andere regulatorische Erfordernisse) sowie neu aufkommender Bedrohungen rasant hoch. Und damit nicht genug: Der österreichische Bericht für Cybersicherheit macht darauf aufmerksam, dass stark steigende Compliance- und Dokumentationsaufwände zunehmend operative Betriebsressourcen binden und dadurch die Effektivität von bestehendem Security-Personal senkt.

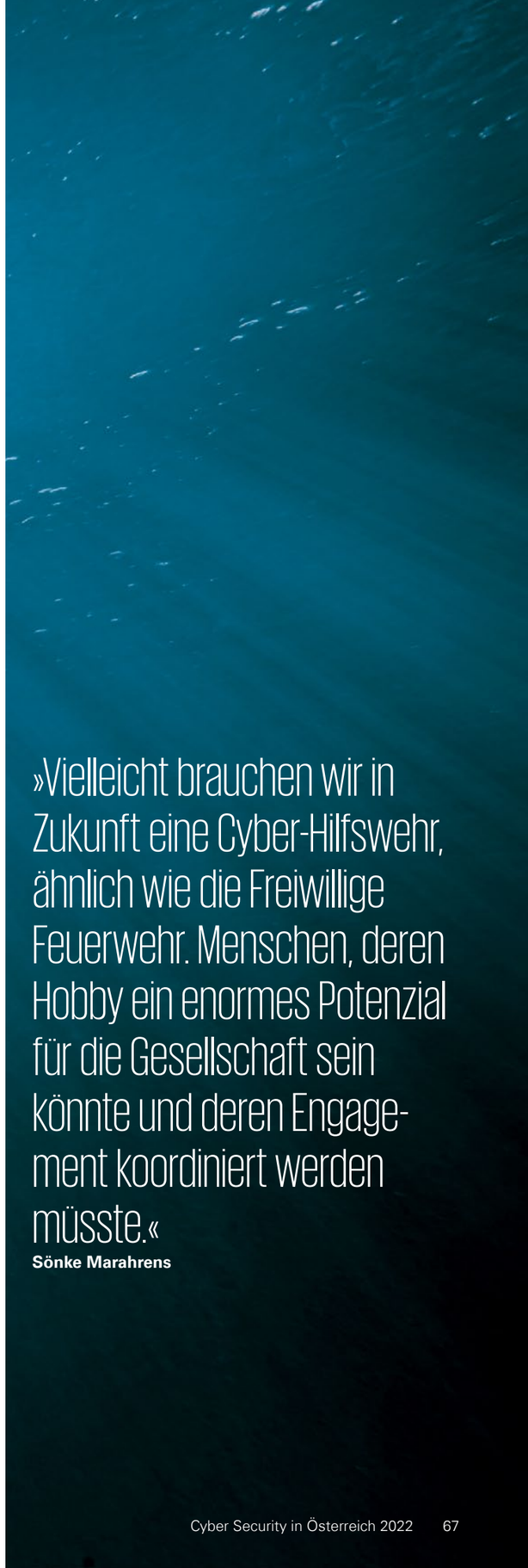
War of Talents

Im Wettkampf-Modus: Das Rennen um die besten Fachkräfte spiegelt sich in einer ganz entscheidenden Zahl unserer Umfrage wider: 40 Prozent der Befragten geben an, aktiv Sicherheitsexperten von anderen Unternehmen abzuwerben. Eine Realität, die die meisten CEOs aufhorchen lassen wird. Es untermauert die Tatsache, dass dem Markt Cyber Security-Experten fehlen und wir uns inmitten eines Verdrängungswettbewerbs von Talenten und Experten befinden.

Für jedes zweite Unternehmen (42 Prozent) ist es mittlerweile üblich, Quereinsteiger anzustellen und diese selbst auszubilden. Cyber Security ist kein rein akademisches Arbeitsfeld mehr, sondern vielfach ein Feld für Quereinsteiger oder Generalisten, die ein großes Interesse an Sicherheitsthemen und eine gewisse IT- und Technik-Affinität mitbringen: 64 bzw 56 Prozent der Unternehmen stellen zwar Bewerber von Fachhochschulen bzw Universitäten ein. Doch Berufsbildende Höhere Schulen wie HTL oder HAK sind stark am Vormarsch (59 Prozent). Um diesen neuen Bewerbern allerdings gerecht zu werden, wird der Ruf nach moderneren Arbeitsmodellen, die diese Entwicklungen berücksichtigen, immer lauter.

In die Ferne schweifen

Eine weitere Zahl, die Österreich wachrütteln sollte: Jedes vierte Unternehmen (26 Prozent) in Österreich berichtet mittlerweile, dass es leichter ist, IT-Experten im europäischen Ausland zu rekrutieren als in Österreich. Nur mehr zwei von drei Unternehmen (65 Prozent) geben zu Protokoll, Experten ausschließlich in Österreich zu suchen. Jedes dritte Unternehmen (34 Prozent) stellt inzwischen Mitarbeiter auch im Ausland an, obwohl es dort keine Niederlassung besitzt. Dies führt jedenfalls zu einem wesentlichen Verlust der Wertschöpfung innerhalb Österreichs.



Konsequenzen-Management ist unerlässlich

Gerald Kortschak, Sprecher der Experts Group IT-Security des Fachverbandes UBIT und Berufsgruppensprecher der IT-Dienstleistungsbetriebe der WK STMK, ist spezialisiert auf strategisches Konsequenzen-Management und spricht mit uns über die Notwendigkeit, den Wirtschaftszweig der Cyber Defense auszubauen, um zukünftig schneller und gezielter gegen Cyberattacken vorgehen zu können.

FOTO © HELMUT LUNGHAMMER

Gerald Kortschak
ist seit 2016 Sprecher der IT-Security Experts Group des Fachverbandes Unternehmensberatung, Buchhaltung und IT der Wirtschaftskammer Österreich (UBIT) und Berufsgruppensprecher der IT-Dienstleistungsbetriebe der WK STMK.

Die Studie hat gezeigt, dass aktuell nur 12 Prozent der befragen Unternehmen angegeben haben, Opfer einer Ransomware-Attacke geworden zu sein. Diese Zahl erscheint im globalen Vergleich doch niedrig. Ist die Zahl aus Ihrer Praxissicht realistisch bzw korrekt oder scheuen Unternehmen davor sich besonders bei diesem Thema zu deklarieren?
Basierend auf unseren Erfahrungen ist die Zahl grundsätzlich realistisch und deckt sich mit den Incident-Meldungen bei der Cyber Security-Hotline, einer gemeinsamen Initiative aller neun Wirtschaftskammern. Jedoch ist die Dunkelziffer sicherlich höher. In den Praxiseinsätzen stellt man hier oft fest, dass die Phasen Angriff-Schadenswirkung-Schadensbehebung vermischt werden. Im Zuge der Schadensbehebung werden oft, verschuldete oder unverschuldete, Mängel in zB der Backup-Struktur erkannt, für die logischerweise niemand die Verantwortung übernehmen möchte bzw es werden generell Rufschädigungen oder Vertrauensverluste befürchtet.

Wohin muss sich die Zusammenarbeit zwischen Staat und Wirtschaft in der Zukunft verändern?
Wir müssen uns der Tatsache bewusst werden, dass ein Cyber-Incident mit Folgeschäden nie zu 100 Prozent verhindert werden kann, auch wenn das die Präventionsstrategien zu vermeiden versuchen. Der staatliche und wirtschaftliche Fokus lag und liegt auf präventiven Maßnahmen, egal ob es sich hierbei um Förderungs-, Investitions- oder Aufklärungsstrategien handelt. Wir müssen eine lebendige gemeinschaftliche Strategie zur Bewältigung und Minimierung auftretender Schäden nach einem Cyberangriff einführen. Konsequenzen-Management ist hier das Stichwort, damit im Ernstfall ein Plan und realistischer Budgetrahmen für Soforthilfe zur Verfügung steht.

Die WKO bietet heimischen Unternehmen eine Cyber-Security-Hotline an, um im Bedarfsfall Hilfe zu erhalten. Welche Funktion soll diese Hotline erfüllen und mit welcher Unterstützung können Unternehmen hier rechnen? Wie wird sich die Hotline in Zukunft weiterentwickeln?
Die Cyber-Security-Hotline (cys.at) ist ein bundesweites Gemeinschaftsprojekt der Wirtschaftskammern. Den Mitgliedsbetrieben steht unter 0800 888 133 eine 24/7-Hotline für telefonische Erstinformationen zur Verfügung. Kann nicht bereits hier geholfen werden, wird ein Kontakt zu qualifizierten Mitgliedsbetrieben der Experts Group IT-Security des Fachverbandes Unternehmensberatung, Buchhaltung und IT der WKO (UBIT) hergestellt. Diese haben sich bereit erklärt, im Sinne einer nationalen Sicherheitsstrategie, für kostenfreie telefonische Erstgespräche zur Verfügung zu stehen und mussten eine eigene Zertifizierung der UBIT-Akademie incite bestehen. Sind Sofortmaßnahmen – beispielsweise als Vorort-Einsatz – notwendig, so können diese Leistungen separat mit dem Spezialisten vereinbart werden. Ich bin meinen Kolleginnen und Kollegen für ihre pro bono Leistungen sehr dankbar, da ohne dieses Engagement eine derartige Hotline gar nicht möglich gewesen wäre. Dank des Engagements der Wirtschaftskammern konnte der Grundstein einer nationalen „Cyber-Incident-Feuerwehr" gelegt werden.

Für die Zukunft wird an dem Ausbau und einem Monitoring-System gearbeitet, da jeder Anruf wie eine Bodenerschütterung zu verstehen ist, die seismische Wellen aufkommender Cyberbedrohungen darstellen. Unser Ziel ist ein automatisiertes Frühwarnsystem, das, eingebettet in die nationalen Lagebilder, erstmals verkürzte Reaktionsmaßnahmen auf Bedrohungen sicherstellt.

Um Unternehmen in Sachen Cyber Security unterstützen zu können, bedarf es Unternehmen, die spezielle Cyber Security Dienstleistungen anbieten. Wie schätzen Sie die aktuelle Marktlage hier ein? Welchen Handlungsbedarf gibt es hier aus Ihrer Sicht?
Grundsätzlich verfügen wir in Österreich über hochqualifizierte Unternehmen. Traditionell ist der Mensch jedoch nur dann bereit in Sicherheitsstrategien zu investieren, wenn der Schaden bereits eingetreten ist oder eine Zertifizierung zu dokumentierbaren Handlungen zwingt. Dieses Problem kennen wir bereits von anderen Organisationen, für die man zwar dankbar ist, wenn sie im Ernstfall voll ausgerüstet vorhanden sind, die aber in der Zeit bis dorthin im Idealfall nichts kosten dürfen. Würde

»Wir müssen eine lebendige gemeinschaftliche Strategie zur Bewältigung und Minimierung auftretender Schäden nach einem Cyberangriff einführen.«

heute ein Cyber Incident mehrere Unternehmen gleichzeitig treffen, würde man wohl erkennen, dass diese sich um die gleichen Cyber Security Ressourcen streiten müssten. Hier besteht definitiv Handlungsbedarf, denn man kann von der Wirtschaft nicht erwarten, dieses Problem, gerade vor dem Hintergrund der aktuellen Finanzlage, selbst zu lösen. Eine Handlungsfähigkeit im Ernstfall erfordert finanzielle Mittel und Informationen. Auch könnte so dieser Fachbereich für den Nachwuchs interessanter werden, da natürlich auch wir unter einem Fachkräftemangel leiden und leider führen lobenswerte Initiativen wie die „Austria Cyber Security Challenge" nach wie vor ein Schattendasein.

Besonders aufgrund des Fachkräftemangels greifen Unternehmen vermehrt auf Dienstleister zurück. Kann der Markt diesen Bedarf auf längere Zeit abdecken und falls nicht, wie wird es sich aus Ihrer Sicht weiterentwickeln?
Diese Entwicklung ist grundsätzlich positiv, da die Rolle der Dienstleistungsbetriebe hierdurch eine Wertschätzung erfährt und gerade unter den KMU oder EPU es viele hochqualifizierte Spezialistinnen und Spezialisten gibt, die bisher im Schatten von Großbetrieben standen. Jedoch muss generell die Schlagkraft der kleineren Unternehmen und der EPUs gefördert werden. Leider steht zu oft die Quantität an Zertifikaten, MitarbeiterInnen sowie die Bekanntheit im Vordergrund, während praktische Erfahrung sowie Qualität zweitrangig erscheinen. Hier schlummert verborgenes Potenzial und gerade als Experts Group sind wir bestrebt aufzuzeigen, welche Ressourcen hier übersehen werden. Wenn nicht, kommt es bald zu einer Abhängigkeitspyramide der Megakonzerne und man wird erst dann erkennen, welchen Schaden man verursacht hat.

Der Großteil der befragten Unternehmen (46 Prozent) hat angegeben, dass der Schaden eines Sicherheitsvorfalls bis zu EUR 10.000 betrug. Das erscheint jetzt zu dem, was man in den Medien liest,

»Ein Cyber Vorfall mit Folgeschäden kann nie 100 Prozent verhindert werden.«
Gerald Kortschak

auch für kleinere Unternehmen noch verkraftbar. Ist die Bedrohung für Unternehmen durch Cyberangriffe höher als sie durch diese Zahl erscheint?
Jene 87 Prozent der österreichischen Wirtschaft, die als Kleinstbetrieb zu definieren sind, würden 10.000 EUR sicherlich nicht als „leicht verkraftbar" einstufen. Die finanzielle Bedrohung ist, nach meiner praktischen Erfahrung, für Unternehmen deutlich höher als dieser Betrag glauben macht. Schon jeder Spedition kostet 1h Totalausfall wesentlich mehr. Ein Schaden besteht nicht nur aus einer vermeintlichen Summe X. Produktionsausfälle, Lieferverzögerungen, Auftragsverluste, Stehzeiten von MitarbeiterInnen, Kosten der Reparaturdienstleistungen, Austauschinvestitionen und vieles mehr spielen eine Rolle und so kommen rasch 35.000 und mehr Euro zusammen.

Warum ist es für KMUs so schwer, Cyber Security als essenziellen Teil ihres operativen Geschäftsbetriebs zu sehen?
Nach meiner Erfahrung sehen KMUs Cyber Security sehr wohl als eine Bedrohung ihrer lebensnotwendigen digitalen Prozesse, sie bringt im Tagesgeschäft aber keinen direkten Umsatz. Gerade für KMUs sind Investitionen in diesem Bereich eine zusätzliche Belastung, die in etwa so erwünscht ist wie steigende Gas- und Treibstoffpreise. Förderaktionen wie KMU Digital, KMU Cyber Security oder die Aktion Gemeinsam.Sicher sind hier sowohl finanzielle als auch kommunikative Hilfestellungen, die noch deutlich ausgebaut werden müssten. KMUs inkl der Kleinstbetriebe machen 99,6 Prozent der österreichischen Wirtschaft aus!

Die „Gemeinsam.Sicher Cyber-Security Planspiele" der WKO und des BM.I in 2018 haben ganz explizit aufgezeigt, dass diesen Betrieben am meisten mit Hilfe zur Selbsthilfe geholfen werden kann. Während im SKKM-Segment Planspiele an der Tagesordnung stehen, wissen KMUs oft nicht, wie sie im Ernstfall reagieren können und wie sie nur durch Prozesse ihren Eigenschutz bereits erhöhen könnten. Die Ursache ist relativ einfach. Egal ob 10 oder 50 MitarbeiterInnen, jedem Betrieb fällt es schwer, 2 oder 4 Personen für Schulungstage abzustellen. Würde man KMU öfter die Möglichkeit bieten, in einer geschützten Umgebung an einem einzigen Tag zu lernen, wie man die eigenen Ressourcen zu Cyber Security nutzt, könnten viele mehrtätige Ausfälle vermieden werden und Staat und Wirtschaft würden davon profitieren.

Wenn wir uns in einem Jahr wieder über das Thema Cyber Security austauschen, was werden wir uns dann wünschen, heute schon getan zu haben?
Wir müssen den Wirtschaftszweig der Cyber Defense stärken, da uns im Ernstfall sonst die digitale Feuerwehr fehlt. Digitale Grundlagen als Pflichtgegenstand einzuführen war hierfür bereits ein erster wichtiger Schritt. Jetzt besteht noch die Chance, das sensible Netzwerk aus Bildungseinrichtungen und Ausbildungsbetrieben auf die Entwicklung der Cyber Security Bedrohungslage vorzubereiten, indem Lehrpersonal gesondert geschult wird und das Ansehen der IT-Dienstleistungsbetriebe gesteigert wird. Nur so kann eine nachhaltige Resilienz sichergestellt werden. Hierbei ist es wichtig, dass die Maßnahmen für den KMU-Sektor verstärkt werden müssen, denn diese repräsentieren immerhin 99,6 Prozent der österreichischen Wirtschaft. Die heutigen Herausforderungen der KMUs bzw die Schwächung des Mittelstandes werden sonst zum künftigen Problem der gesamten österreichischen Wirtschaft.

Technologie braucht klare Rahmenbedingungen

Die Digitalisierung macht auch vor dem Finanzsektor nicht Halt. Wie es in diesem Bereich mit der Cybersicherheit aussieht bzw was die größten Herausforderungen sind, erzählt Stanislava Saria von der Finanzmarktaufsicht (FMA).

Die FMA führt regelmäßig eine Studie bei Unternehmen durch, die am österreichischen Finanzmarkt vertreten sind. Können Sie unseren Lesern bitte einen Einblick in die Motive, die Ziele und den Umfang Ihrer Studie geben?
Die digitale Transformation am Finanzmarkt macht bei der Digitalisierung interner Prozesse nicht halt. Sie verändert ebenfalls die Produktlandschaft und die Interaktion mit den Kunden, bedingt neue Verflechtungen und begünstigt die Entstehung neuer Geschäftsmodelle. Diese geänderten Rahmenbedingungen bringen für beaufsichtigte Unternehmen abseits der vielen Chancen auch neue Auslegungsschwierigkeiten und Risiken mit sich und stellen zudem die Aufsichtsinstrumente auf den Prüfstand.

Der FMA ist es deshalb wichtig, diesen Transformationsprozess aktiv zu begleiten und Treiber, Trends und mögliche künftige Entwicklungen richtig einzuschätzen. Hierfür haben wir 2021 zum zweiten Mal eine umfassende Analyse zur Digitalisierung am österreichischen Finanzmarkt durchgeführt. Diese hat uns auch dank einer beinahe vollständigen Marktabdeckung in fast allen Sektoren des Finanzmarkts und der großen Beteiligung der beaufsichtigten Unternehmen geholfen, aktuelle Erkenntnisse zum Stand der Digitalisierung und den Einsatzbereichen digitaler Technologien am österreichischen Finanzmarkt zu gewinnen.

Wir wollten bei dieser Gelegenheit zudem eine breitere Diskussion zu den Implikationen der Digitalisierung anstoßen und haben deshalb die Stakeholder (Kunden der beaufsichtigten Unternehmen, ihre Interessensvertretungen, Branchenverbände sowie die interessierte Öffentlichkeit) eingeladen, die im Bericht zur Digitalisierung am österreichischen Finanzmarkt präsentierten Erkenntnisse kritisch zu hinterfragen und um ihre Erfahrungen und Lösungsansätze anzureichern. Die zahlreichen Rückmeldungen, die wir im Q1 2022 im Rahmen dieses Call for Input erhalten haben, sollen nun in die strategische Planung der FMA bzw in die Festlegung der Aufsichtsschwerpunkte entsprechend einfließen.

Die Digitalisierungsstudie 2021 und der Vergleich mit den Ergebnissen im Jahr 2018 bestätigen eine technologiegetriebene Transformation des österreichischen Finanzmarktes. Wo und wodurch hat sich diese Veränderung besonders bemerkbar gemacht?
Die technologiegetriebene Transformation am österreichischen Finanzmarkt schreitet rasant voran, wenngleich das Tempo in den einzelnen Geschäftsbereichen und auch in den einzelnen Häusern durchaus unterschiedlich ist.

Die beaufsichtigten Unternehmen gehen zum einen Kooperationen mit FinTechs/InsurTechs häufiger ein, zum anderen wollen sie aber auch ihre eigenen IT-Kompetenzen noch stärker ausbauen als 2018. Standen 2018 noch die rein technischen Fähigkeiten im Fokus, steigt nun besonders markant der Bedarf an Projektmanagern und Analysten, welche entsprechendes technisches Verständnis haben, um digitale Unterfangen zu leiten und zu unterstützen. Dementsprechend haben wir auch im Hinblick auf den Einsatz digitaler Technologien seit 2018 eine große Dynamik gesehen:
- Ganz klar haben die Cloud Services an Bedeutung gewonnen: 2018 war es die Hälfte des österreichischen Finanzmarkts, jetzt sind es ¾ der beaufsichtigten Unternehmen, die Cloud-Dienstleistungen in ihrem operativen Geschäftsbetrieb nutzen. Somit wurde auch die Erwartungshaltung des Marktes aus 2018 übertroffen.
- Ebenso ist in den letzten drei Jahren die Nutzung von Robotic Process Automation gestiegen, die (mit fast 2/3 der Banken) insbesondere im Bankensektor schon weit verbreitet ist.
- Vorreiter im Einsatz von Machine Learning sind dagegen die Versicherer mit fast 40 Prozent, gefolgt von den Banken mit etwa 30 Prozent.
- Automatisierte Datenschnittstellen, welche die digitale Vernetzung/Zusammenarbeit fördern, werden bereits von 2/3 der Banken und Versicherern genutzt; und auch in den anderen Sektoren werden sie immer häufiger eingesetzt.

In welchen Geschäftsbereichen findet diese technologiegetriebene Transformation des österreichischen Finanzmarktes überwiegend statt?
Neue Informations- und Kommunikationstechnologien werden vor allem an der Schnittstelle zum Kunden immer stärker eingesetzt. Insbesondere im Pre-Sales-Bereich erfolgt der Kundenkontakt zunehmend über digitale Kanäle direkt von den beaufsichtigten Unternehmen aus. Hier ist seit unserer ersten

FOTO © PICCO, WWW.PICCO.AT

Stanislava Saria
leitet seit 2014 die Abteilung Querschnittsthemen der Versicherungsaufsicht und Pensionskassenaufsicht in der FMA. Vor ihrer Tätigkeit für die FMA war sie am Europäischen Gerichtshof in Luxemburg tätig.

»Die technologiegetriebene Transformation am österreichischen Finanzmarkt schreitet rasant voran, wenngleich das Tempo in den einzelnen Geschäftsbereichen und auch in den einzelnen Häusern durchaus unterschiedlich ist.«

Studie im Jahr 2018 die Rolle von sozialen Medien und Videokonferenzen stark gestiegen; ersteres wurde unter anderem durch Konkurrenzdruck in der Neukundenakquise verstärkt und letzteres durch die COVID-19-Pandemie intensiviert. Konventionelle Wege des Vertriebs verlieren außerdem durch den Einsatz von digitalen Vertriebsplattformen, Vergleichsportalen und Robo advice zunehmend an Bedeutung.

Anders gestaltet sich hingegen die Nutzung der Digitalisierung bei der Entwicklung neuer Produkte bzw neuer Geschäftsmodelle: Die Produktlandschaft passt sich an die neuen digitalen Möglichkeiten nur sukzessive an. Im Vordergrund stehen technologiegetriebene Innovationen, bei denen die herkömmlichen Produkte und Dienstleistungen auf die neuen Technologien umgestellt werden. Neue Produktarten werden seit 2018 zwar in einem stärkeren Ausmaß, aber in der Regel noch immer nur partiell bzw experimentell lanciert.

Auch die Blockchaintechnologie hat sich bislang im Hinblick auf die offenen regulatorischen Fragen noch nicht als Basis für neue Produkte bzw Geschäftsmodelle etablieren können. Dies könnte sich aber in naher Zukunft durch die kommenden Regularien wie die MICA ändern.

In unserer Studie im Jahr 2021 haben 20 Prozent der befragten Unternehmen angegeben, die Digitalisierung zumindest teilweise wieder rückgängig machen zu wollen. Welche Hindernisse waren für eine erfolgreiche Digitalisierung bei den Instituten aus Ihrer Sicht besonders einprägsam?
Im Allgemeinen werden die größten Hindernisse in der Regulierung gesehen. Dies ist wohl auf die oft starke Fokussierung der Digitalisierungsbestrebungen auf den Vertrieb bzw die Kundenschnittstelle zurückzuführen und hängt mit den Vorgaben zu eigenhändigen Unterschriften und dem in einigen Sektoren noch postulierten Vorrang der Papierform zusammen.

»Ich bin davon überzeugt, dass die digitale Transformation auf Dauer nicht ohne robuste Begleitmaßnahmen im Bereich der IKT-Sicherheit funktionieren kann.«

Stanislava Saria

Wichtige Hürden der Digitalisierung stellen aber noch immer die Unternehmenskultur (denn die Transformation muss durch Changemanagement und Kulturmanagement begleitet werden) und die Organisation eines Unternehmens (eine erfolgreiche Transformation setzt eine adäquate Expertise und Priorisierung auf Vorstandsebene voraus) dar.

Inadäquate digitale Kompetenz und eine eher abwartende Haltung von Kunden können aber ebenso ein Hemmnis für digitale Lösungen darstellen.
Eine größere Bedeutung als den Hindernissen in der Unternehmenskultur und im Kundenverhalten wird vor allem im Bankensektor den Hindernissen in Bezug auf eine stark fragmentierte und veraltete IT-Landschaft und unzureichende finanzielle Mittel für Forschung und Entwicklung beigemessen.

Ich bin davon überzeugt, dass die digitale Transformation auf Dauer nicht ohne robuste Begleitmaßnahmen im Bereich der IKT-Sicherheit funktionieren kann. Je innovativer die Ideen bei der Weiterentwicklung der Prozesse und des eigenen Geschäftsmodells sind, desto professioneller / sophistizierter und zielgerichteter muss das Fundament sein, das den Einsatz dieser Technologien ermöglicht.

Gerade auch durch die besonders hohe Vernetzung und die neu auftretenden Risiken ist der Finanzmarktsektor für Akteure immer ein interessantes Ziel. Welchen Stellenwert trägt dabei das Supply-Chain-Risiko (Third-Party-Risiko) und wie wird sich dieses in Zukunft entwickeln?
Wie wir auch in unserer letzten Studie gesehen haben, steigt der Grad der Vernetzung des Finanzsektors mit IKT-Dienstleistern durch die Digitalisierung. Am österreichischen Finanzmarkt bestehen rund 1.000 kritische Vernetzungen mit IKT-Dienstleistern. Diese Verflechtungen mit externen (derzeit noch aufsichtsrechtlich unregulierten) Dienstleistern bergen nicht nur operationale Risiken, sondern auch Konzentrationsrisiken. Ein Vorfall oder gar ein Ausfall bei einem Dienstleister kann gleichzeitig zahlreiche beaufsichtigte Unternehmen treffen.

Dies hat aber auch zur Folge, dass sich das IKT-Risiko beaufsichtigter Unternehmen zunehmend an die Schnittstelle zu Dritten (Kooperationspartner, IT-Dienstleister) verlagert.

Gerade deshalb arbeiten wir auch auf europäischer Ebene an harmonisierten Rahmenbedingungen, die digitalisierungsbezogene Risiken erstmalig umfassend adressieren sollen. Dazu bringt der Vorschlag der Europäischen Kommission für eine Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA) entscheidende Neuerungen:
- Zum einen sollen Technologiedienstleister, die entscheidend zum Funktionieren des Finanzsektors beitragen und somit als „kritische IKT-Drittanbieter" eingestuft werden, einer Aufsicht auf europäischer Ebene unterworfen werden.
- Zum anderen sollen die beaufsichtigten Unternehmen angemessene Vorkehrungen treffen, um die Abhängigkeiten von derartigen Anbietern abzumildern. Dies umfasst etwa, dass sie sich entsprechende Zugangs-, Inspektions- und Prüfrechte sichern und bereits im Vorfeld geeignete Ausstiegsstrategien beim Ausfall des IKT-Drittanbieters oder einer Verschlechterung der Qualität der bereitgestellten Funktionen überlegen.

Gerade in diesem Bereich haben wir aber in Österreich schon eine gute Arbeit geleistet und uns im Rahmen der Digitalisierungsstudie einen ersten Überblick über die relevanten Verflechtungen verschafft. Dies hilft uns, die für den österreichischen Finanzmarkt relevanten kritischen IKT-Drittanbieter zeitnah zu identifizieren und die betroffenen beaufsichtigten Unternehmen hinsichtlich dieser neuen regulatorischen Vorgaben zu sensibilisieren.

Der durchschnittliche Reifegrad über alle 13 Themen und den fünf Sektoren liegt laut Ihrer Umfrage bei 3,2. Welche Felder sind hier besonders positiv in Erscheinung getreten und wo gibt es Ihrer Meinung noch Handlungsbedarf?
Nicht nur der Grad der Vernetzung des Finanzsektors mit den IKT-Dienstleistern, sondern auch die Qualität der eigenen IKT-Sicherheitsmaßnahmen der beaufsichtigten Unternehmen steigen. Dies zeigen auch die von der FMA entwickelten Cyber und Cloud Maturity Level Assessments, die der FMA erstmalig einen Einblick in die Cyberresilienz des österreichischen Finanzmarktes erlauben.

Diese erfreuliche Entwicklung ist insbesondere im Versicherungssektor gut sichtbar, wo wir die beiden Assessments zum ersten Mal bereits 2019 durchgeführt haben. Der durchschnittliche Maturitätsgrad hat sich in den letzten zwei Jahren von 3,1 auf aktuell 3,7 erhöht.
Bereiche, deren Cyberreifegrad insgesamt über dem Gesamtreifegraddurchschnitt liegt:
- Berechtigungskonzept (Übersichten zu Benutzerberechtigungen liegen grundsätzlich vor, Vergabe nach dem Need-to-know-Prinzip),
- IT-Assets (Inventar der genutzten Hardware, Bestandsverzeichnisse zu Softwareassets, die die Basis für die weiteren Sicherheitsmaßnahmen darstellen, werden teilweise teilautomatisiert geführt),
- Konfigurationen und Sicherheitseinstellungen (So sind etwa Virenscanner grundsätzlich installiert und deren Ergebnismeldungen werden meist zentral erfasst und nach einem vorgegebenen

Prozess dokumentiert und behandelt. Auch Software-Whitelisting, durch welches User nur vordefinierte Applikationen ausführen können, ist weit verbreitet).

Entwicklungsfelder, in denen noch Aufholbedarf, und das vor allem im Hinblick auf die zukünftigen DORA-Vorgaben, besteht:

- Protokollierung & Überwachung (die Sammlung sowie die Überwachung von Logdaten kann insgesamt noch optimiert werden),
- Notfallmanagement (vor allem die Auswahl und die Umsetzung von Tests und komplexere Übungen zum Notfallmanagement sind ausbaufähig),
- Testmethoden & Praktiken (Red Team Tests/ Threat Led Penetration Testing, bei denen ein gezielter Angriff auf die „Kronjuwelen" des Unternehmens erfolgt, drückt den Reifegrad dieser Kategorie nach unten. Allerdings erwartet die FMA die Durchführung solcher ressourcenintensiven Red Team Tests lediglich von signifikanten Unternehmen mit ausreichender Cybermaturität.)

Abschließend hat zwar der österreichische Finanzmarkt im Aggregat die wesentlichsten Vorkehrungen zur Sicherstellung einer angemessenen IKT-Sicherheit getroffen. Hier muss ich allerdings betonen, dass wir uns hier nicht zurücklehnen dürfen, da die IKT-Sicherheit im Hinblick auf die sich ständig weiterentwickelnden Cyberbedrohungen und die steigenden digitalen Kundenansprüche laufende Anpassungen der Sicherheitsmaßnahmen erfordert.

Brauchen wir in Zukunft mehr Regulatorik und Compliance-Vorschriften, um cybersicherer zu werden, oder ist das Verständnis hierfür schon ausreichend vorhanden? Wo sehen Sie in der Zukunft den größten Handlungsbedarf?

Die Technologie an sich bedarf meines Erachtens keiner Regulierung, sehr wohl aber klare Rahmenbedingungen dort, wo die Gefahr besteht, dass durch ihre Nutzung neue Risiken entstehen oder das Vertrauen der Kunden in den Finanzmarkt beeinträchtigt wird. So beaufsichtigt auch die FMA keine Technologien, sondern hat primär Risiken im Blick.

Durch die zunehmende Digitalisierung des österreichischen Finanzmarktes sind dementsprechend auch die Cyberrisiken verstärkt in den Fokus der FMA geraten und sollen strukturiert in unser Risiko-Scoring einfließen. Wie diese zu behandeln sind, darauf gibt im Wesentlichen bereits der Stand der Technik die Antwort.

Deshalb haben wir uns auch bei unseren Cyber und Cloud Maturity Level Assessments in den letzten Jahren an den internationalen Standards im Bereich der IKT-Sicherheit orientiert. Jeder Standard hat dabei bekanntlich einen anderen Fokus, daher haben wir jene Vorgaben herausgefiltert, die für unsere Beaufsichtigten am relevantesten sind.

Insofern verstehe ich auch die regulatorischen Entwicklungen im Bereich der IKT-Sicherheit auf europäischer Ebene als einen logischen Schritt in Richtung Vereinheitlichung / Level playing field und mehr Standardisierung, ohne an den inhaltlichen Prinzipien rütteln zu wollen.

Wichtig ist, dass die österreichischen Finanzmarktteilnehmer hier nicht unvorbereitet sind, sondern diesen Prozess nutzen, um die Maßnahmen zur Stärkung ihrer eigenen Cyberresilienz weiterzuentwickeln, und das, was bereits Teil ihrer Good Governance ist, als ein Gütesiegel zur Stärkung des Vertrauens ihrer Kunden verstehen!

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: Cyber Security im Überblick

Die Umfrage zur Studie wurde im Jänner und Februar 2022 von KPMG unter rund 550 österreichischen Unternehmen 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 und Education zusammen.

Die Auswertung: Stimmungsbild in Österreich

Jeder Teilnehmer erhielt, seiner Funktion im Unternehmen entsprechend, einen Online-Fragebogen mit spezifischen Fragen. Darüber hinaus wurden die quantitativen Fragen (Likert-Skala) um qualitative Aspekte erweitert, um den Teilnehmern die Möglichkeit zu geben, weitere Eindrücke und Beobachtungen zu teilen oder um Antworten auch entsprechend zu kommentieren.

Die Vertiefung: Im Gespräch mit Experten

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 neun Wirtschaftsvertreter und Cyber Security-Experten zum Thema Rede und Antwort.

Bei einem Round Table diskutierten Vertreter von KPMG, Europol und CERT.at über die Frage, was die Wirtschaft von den aktuellen Beobachtungen der ermittelnden Behörden und Cyber Response Teams auf nationaler und internationaler Ebene lernen kann, um den Herausforderungen zum Thema Cyber gewachsen zu sein.

Funktion der Teilnehmer innerhalb des Unternehmens

- Aufsichtsrat 2%
- Vorstand, Geschäftsführer 23%
- CDO/CIO/IT-Leitung 16%
- CSO, CISO, Sicherheitsverantwortlicher 20%
- Bereichsleiter, Abteilungsleiter, Teamleiter 17%
- Experte, Mitarbeiter 22%

Teilnehmer nach Branchen

- Automotive 4%
- Banken 16%
- Bauwirtschaft & Immobilien 3%
- Dienstleistungen 13%
- Education 3%
- Energiewirtschaft 6%
- Industrie 15%
- Insurance 8%
- Öffentlicher Sektor 17%
- Retail, Food &Drink 4%
- Technologie, Medien, Telekommunikation 10%
- Tourismus 1%

Bildung als Chance

Bildung ist ein essenzieller Faktor für eine Gesellschaft und eine wesentliche Voraussetzung für deren Zukunft. Im Sinne der Nachhaltigkeit sehen auch wir es als unsere Aufgabe, Nachwuchs zu fördern – mit unserem KITE Programm.

Das Traineeprogramm KITE (KPMG Information Technology Education) vermittelt über 9 Monate praxisnahe Einblicke in die Themen, die die Techwelt treiben. Zu 50 Prozent nehmen die Studentinnen und Studenten an Schulungen teil, zu 50 Prozent sind sie in Praxisprojekte eingebunden.

Abgerundet wird das Programm durch ein Mentoring Programm mit (internationalen) Experten. Am Ende des Traineeships besteht die Möglichkeit zur Festanstellung mit langfristigen Jobperspektiven.

Alle weiteren Details und Informationen rund um unser KITE Programm gibt es unter https://www.kpmg.at/kite

Gemeinsam Zukunft schreiben

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

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

Koordination:
Mariana Herrloss
T +43 1 313 32-3955
mherrloss@kpmg.at

Grafik und Satz:
Martin Morauf-Schmidl
T +43 1 313 32-3275
mmorauf-schmidl@kpmg.at

Druck:
Ferdinand Berger & Söhne GmbH

KSÖ Kompetenzzentrum Sicheres Österreich

Sicherheitsforum Digitale Wirtschaft Österreich

Die Studie wurde in Kooperation mit dem Sicherheitsforum Digitale Wirtschaft des Kompetenzzentrum 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.