KPMG

Cybersecurity in Österreich

Sicherheitsforum
Digitale Wirtschaft
Österreich

Mai 2023

kpmg.at/cyber

*Erfahren Sie mehr in unserem Podcast IMPULSE

Inhaltsverzeichnis

Hektik in der Cyberwelt

Die Reise durch die Tiefen des Cyberspace ist wahrlich eine faszinierende. Mitunter lauern aber auch große Gefahren und es macht sich eine gewisse Hektik breit. Phishing-Angriffe, Advanced Persistent Threats, Social Engineering und vermehrt aufkommende Deepfake-Angriffe, sie alle sind für heimische Unternehmen mittlerweile nicht mehr wegzudenken.

Cyberangriffe haben im letzten Jahr massiv zugenommen, vor allem auch geschuldet durch die jüngsten geopolitischen Auseinandersetzungen in Europa. Das hat eine neue Welle von Angriffen – ausgeführt von staatlichen oder staatlich unterstützten Akteur:innen – hervorgerufen. Wir erleben Cyberkriminalität der nächsten Generation. Wichtig bei all der Hektik ist es, die Ruhe zu bewahren und unsere wesentliche Infrastruktur so gut wie möglich abzusichern.

Ein schützender Panzer

Unternehmen müssen wie auch die Schildkröte, die uns in diesem Jahr erneut auf unserer Reise begleitet, einen guten Panzer haben, um sich vor den Raubtieren des Cyberozeans zu schützen. Und das haben die Unternehmen durchaus auch im letzten Jahr gemacht, indem sie ihre Abwehrmaßnahmen ausgebaut und ihr Budget für Cybersecurity sowie auch ihre Personalressourcen aufgestockt haben.

Langlebigkeit und Beständigkeit

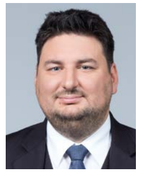
Nicht nur, dass eine verbesserte digitale Sicherheit wichtig für die unternehmerische Existenz ist, es lassen sich dadurch auch Wettbewerbsvorteile generieren. Das möchten wir Ihnen mit unserer Studie mit auf den Weg geben. Lassen Sie uns weiterhin gemeinsam daran arbeiten, die Resilienz für den Wirtschaftsstandort Österreich zu stärken!

Bereits zum achten Mal veröffentlichen wir in Kooperation mit dem Sicherheitsforum Digitale Wirtschaft des Kompetenzzentrum Sicheres Österreich (KSÖ) die Studie „Cybersecurity in Österreich“.

An dieser Stelle bedanken wir uns herzlich bei all jenen, die unseren Fragebogen beantwortet haben. Ohne Sie wäre es nicht möglich gewesen, die Cybersecurity-Studie wieder in diesem Umfang bereitzustellen!

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

Michael Schirmbrand
KPMG Partner



Andreas Tomek
KPMG Partner

Gert Weidinger
KPMG Partner

Vorwort

Ich freue mich sehr, dass ich 2023 erstmals in meiner neuen Rolle als Präsident des Kompetenzzentrum Sicheres Österreich (KSÖ) bei der Präsentation der Ergebnisse dieser Studie dabei sein darf. Die erfolgreiche Fortsetzung der Zusammenarbeit zwischen KPMG und dem Sicherheitsforum Digitale Wirtschaft des KSÖ ist für sich selbst schon Best Practice dafür geworden, wie Zusammenarbeit gut funktionieren und einen Mehrwert für alle schaffen kann.

Die Themen und Ergebnisse der Studie zeigen die Vielfältigkeit der Herausforderungen. Im KSÖ versuchen wir diese in einigen zentralen Themenbereichen direkt aufzugreifen. Ein Beispiel dafür ist der Rechts- und Technologiedialog, den wir gemeinsam mit der Cyber Sicherheit Plattform (CSP) im Bundeskanzleramt und in enger Kooperation mit dem Bundeskanzleramt und dem Innenministerium zum Thema NIS2 durchführen. Wir arbeiten 2023 in insgesamt sechs Workshops die zentralen Themenstellungen – von der Managementschulung über das Thema Meldepflicht bis hin zu Fragen der Baseline-Security für KMUs – durch. Ziel ist es, gemeinsam mit unseren staatlichen Partnern und unter enger Einbindung der Unternehmen der kritischen Infrastruktur, die Grundlagen für eine Umsetzung der EU-Richtlinie in nationales Recht zu erarbeiten, die den Standards höchster Professionalität und bestmöglicher Umsetzbarkeit entsprechen.

In diesem Zusammenhang ist mir eines wichtig: Unternehmen der kritischen Infrastruktur sind regelmäßig Ziel sehr komplexer Cyberangriffe. Sie bereiten sich daher auch gut und umfassend auf solche Risiken vor. Cyberangriffe betreffen alle Unternehmen und daher muss jedes Unternehmen in Österreich cybersicher sein. KMUs sind das Rückgrat der österreichischen Wirtschaft und brauchen daher genauso bestmögliche Cybersicherheitsstandards. Mit unserem gemeinsam mit dem KSV 1870 und der Cyber Trust Austria entwickelten Cyber Risk Rating und dem damit verbundenen Cyber Trust Label haben wir bereits vor mehr als zwei Jahren eine entsprechende Initiative gesetzt. Denn die Rolle und Verantwortung von KMUs als Lieferanten – u. a. für Unternehmen der kritischen Infrastruktur – verlangt auch nach hohen Sicherheitsstandards im Cyberbereich.

Abschließend darf ich schon jetzt den KSÖ Sicherheitsgipfel 2023 ankündigen, der sich am 19. September 2023 mit aktuellen Entwicklungen in der Cyberkriminalität, damit verbundenen neuen technischen Herausforderungen und Angriffsvektoren sowie mit Chancen und Effektivität präventiver Maßnahmen befassen wird. Darüber hinaus verstärken wir unsere Aktivitäten zum Thema Fachkräftemangel im Bereich der Digitalisierung.

FOTO © EVA_KELETY

Mag.
Michael Höllerer
Präsident des KSÖ

Ganz grundsätzlich müssen und werden wir uns – auch im Sicherheitsforum Digitale Wirtschaft – mit der Frage der digitalen Souveränität in Europa auseinandersetzen. Die Chancen für österreichische bzw. europäische Lösungen sind gerade im Thema Cybersicherheit sehr groß. Eine Anstrengung, hier gemeinsam tragfähige Wege und Lösungen zu finden, lohnt sich jedenfalls.

Auf der Welle reiten

Das Pendel schwingt im Vergleich zum letzten Jahr von der Technologie wieder zurück zum Menschen. Er steht im Zentrum, denn er ist der Eintrittspunkt für viele Cyberangriffe. Die Unternehmen haben in den letzten Jahren ihre technische Infrastruktur und ihre Abwehrmaßnahmen ausgebaut. Der Reifegrad und die Definition, wer wofür zuständig ist, müssen noch weiter verbessert werden. Viele Firmen sind bereits am Weg dorthin. Der Rest wird aufpassen müssen, dass er nicht auf der Strecke bleibt. Die Devise lautet: Nicht den Kopf in den Sand stecken, sondern mutig auf die Wellen aufspringen.

Wir haben ein Problem. Der Seegang ist rau und wir werden von einer Krise in die nächste gepeitscht: Die Covid-19-Pandemie, die geopolitischen Konflikte in Europa, die Energie- und Klimakrise sowie die daraus resultierende Inflation – sie alle spielen zusammen und ihre negativen Auswirkungen multiplizieren sich. Das öffnet auch Angreifer:innen Tür und Tor in die Systeme der Unternehmen. Das Erschütternde dabei: Gegenüber letztem Jahr haben wir eine Zunahme der Cyberangriffe um 201 Prozent. Das Ergebnis dieser Entwicklung:

Der Meeresspiegel steigt

Firmen werden angegriffen und das definitiv nicht weniger als zuvor. Cyberangriffe verursachen bei heimischen Unternehmen Schäden in Millionenhöhe. Wir sprechen also nicht von Kavaliersdelikten. Die Technik zieht mit und bietet hier Schutzmöglichkeiten. Sie muss so aufgestellt sein, dass sie den Angreifer:innen standhalten kann. Auch organisatorisch müssen Unternehmen sich so aufstellen, dass sie hier mitziehen können. Die Angriffe verlagern sich mehr und mehr auf die Mitarbeiter:innen. Nicht nur, dass die Mitarbeitenden im Fokus der Angriffe stehen, sondern sie sind es auch, die hauptsächlich auf die Angriffe aufmerksam werden. Einmal mehr zeigt sich, dass Cybersecurity ein People's Business ist.

Der Ozean hat keine Grenzen

Die emotionale Bedeutung von Cybersecurity hat sich durch den russischen Angriffskrieg auf die Ukraine für viele Unternehmen verändert. Das hat schon auch dabei geholfen, dass die Menschen ganz grundsätzlich sicherheitsinteressierter geworden sind. Wir erfreuen uns immer mehr an der Digitalisierung und darüber, welche Influencer:innen gerade dieses oder jenes machen, aber wir lernen auch, wie wir sicherer werden können. Natürlich tun wir uns leichter, wenn die Welt nur aus Freude und Freizeit besteht. Aber es geht nicht immer nur darum, welche Trends gerade „angesagt" sind, sondern auch darum, was über unsere Grenzen hinaus auf der ganzen Welt passiert und wie wir uns besser schützen können. Bei den Unternehmen ist der Wunsch nach einer verstärkten EU-weiten Zusammenarbeit beim Thema Cybersicherheit da. Auch die Zusammenarbeit zwischen Firmen und Lieferanten – Stichwort: NIS2 und Cyber Resilience Act – wird zum Thema.

Abtauchen ist keine Option

Ein Beispiel für diese Zusammenarbeit ist das Thema Operational Technology (OT). Der Hälfte der Befragten war nicht bekannt, ob die OT-Sicherheit eine besondere Herausforderung ist oder zum ganz normalen Tagesgeschäft des eigenen Unternehmens gehört. Das ist ein klares Argument für die Notwendigkeit steigender Professionalisierung in Unternehmen und dass wir hier noch nicht am Ende der Entwicklung sind. Viele Unternehmen sind selbst für die

Robert Lamprecht
KPMG Director

Umsetzung der OT-Sicherheit verantwortlich und nicht etwa der Hersteller oder Lieferant, der die Anlage gebaut hat. Fast die Hälfte empfindet hierbei die Absicherung der Systeme als Herausforderung. Es stellt sich also die spannende Frage, wieso Unternehmen die Umsetzung der Sicherheitsmaßnahmen dann nicht auslagern. Entweder fühlen sich die Hersteller/Lieferanten nicht zuständig oder die Unternehmen wissen nicht, was sie tun sollen – so oder so liegt das Problem ungelöst bei den Unternehmen. Es ist die altbekannte Geschichte, dass OT noch ein Sonderthema ist. In der IT sind wir sehr weit, und obwohl wir über OT schon seit ein paar Jahren sprechen, sind wir dennoch wieder am Anfang. Es ist eine komplexe Frage, die fast schon danach schreit, dass man sie ignoriert. Aber das geht heute nicht mehr.

Die Dämme öffnen

Die Suche nach IT-Expert:innen dauert für Unternehmen durchschnittlich 4–6 Monate. Das ist also eine Herausforderung, die man strategisch und langfristig angehen muss. Erschreckend ist, dass fast die Hälfte der Unternehmen keine einzige Frau im Bereich Cybersecurity beschäftigt. Bei einer durchschnittlichen Größe der Cyberabteilung von 10 Personen beträgt der Frauenanteil 13 Prozent, was 1,3 Personen entspricht. Das ist ein Management-Thema und somit lösbar. Aber: Es wird wehtun und es wird aufwendig. Es braucht viel mehr Beschäftigung mit den Ursachen und man muss die Fühler ausstrecken, um Fachkräfte aus unterschiedlichsten Branchen und mit diversen Backgrounds zu finden. Denn Cybersecurity ist weit mehr als eine MINT-Disziplin!

Mit der Strömung

100 Prozent der von uns befragten Unternehmen wurden in den letzten zwölf Monaten zum Opfer eines Phishing-Angriffs. Auch APTs stellen eine große Bedrohung dar. Geht die Welt davon jetzt unter? Offenbar nicht. Möglicherweise liegt es daran, dass die Schadenssummen so gering sind. Unternehmen können es sich leisten. Das ist vergleichbar mit der Situation am Schulweg regelmäßig ausgeraubt zu werden. Da ist es auch leichter, man schwimmt mit der Strömung, bezahlt 10 Euro und schließt dafür eine Art Abomodell ab, um nicht mehr ausgeraubt zu werden. Wenn jedoch 55 Prozent der Unternehmen sagen, dass Cyberangriffe ihre Existenz bedrohen, dann ist es nicht mehr egal.

Um die Wette schwimmen

65 Prozent stimmten der Aussage zu, dass die Unternehmensleitung Informationssicherheit nicht als einen möglichen Wettbewerbsvorteil betrachtet. Das steht im Kontrast zu den 55 Prozent, die sagen, dass Cyberangriffe ein existenzielles Risiko sind. Die Aussage, dass IT-Sicherheit kein Wettbewerbsvorteil ist, ist auch in der Praxis immer wieder zu hören. Es wäre jedoch einer, wenn man dadurch mehr Kund:innen bekommt. Das ist auch ein Thema der Standortsicherheit: Wir können damit zeigen, dass es besser ist, Geschäftsbeziehungen dort abzuschließen, wo man seinen Partner:innen vertrauen kann und wo die Rechtsprechung funktioniert. Ähnlich wie beim Inflation Act, wo der Wettbewerbsvorteil auch nicht nur primär aus Subventionen besteht.

Unerforschte Gewässer

Jede:r dritte Befragte würde bevorzugt Security-Lösungen von österreichischen Unternehmen einsetzen. Es gibt einen Markt dafür! Dies sei Security-Unternehmen, die sagen, ihnen lassen die großen Unternehmen keine Luft zum Atmen nochmal ans Herz gelegt. Denn unsere Umfrage zeigt, dass es sehr wohl einen Markt für österreichische Produkte gibt. Der Wettlauf der Digitalisierung ist voll im Gange und wir müssen lernen, auf der Welle zu reiten. Bei Quantencomputing & Mikroelektronik haben wir in Österreich z. B. herausragende Kompetenz. Nachholbedarf haben wir hingegen bei der Nutzung selbstgenerierter Daten. Technologien in der Digitalisierung verändern sich immer schneller, das kennen wir alle (Stichwort: ChatGPT von OpenAI). An die Geschwindigkeit haben wir uns bereits gewöhnt, es wird nur immer schwieriger, aufs richtige (See-)Pferd zu setzen, – aber: Wer nicht wagt, der nicht gewinnt! Wer kritisiert, dass die Regulatorik im Bereich der künstlichen Intelligenz nachhinkt, der sollte zumindest eine Lanze für die EU brechen, die sich mit dem AI Act als erste Gesetzgeberin Gedanken zu AI gemacht hat. Es wird spannend sein zu sehen, wie sich die genannten Bereiche künftig entwickeln werden!

Mit voller Kraft voraus

Es geht also zurück von „Wir können das technisch lösen" hin zu „Wir müssen wieder auf den Menschen schauen". Cybersecurity ist wieder viel stärker ein Geschäft für Menschen geworden, weil es die Menschen sind, die angegriffen werden. Wir befinden uns in einem durchaus gefährlichen Umfeld bei der Arbeit mit Digitalisierung. Das Positive daran: Das hat die Menschheit groß gemacht, dass wir uns zusammengetan, uns entwickelt und voneinander gelernt haben. Dabei sind auch viele Erfolgsmodelle entstanden wie der Austrian Trust Circle, CERT.at, die IKT-Sicherheitskonferenz des Österreichischen Bundesheeres und die Austria Cybersecurity Challenge. Jedoch reicht das alleine noch nicht aus, denn das betrifft rein die Expert:innen. Wohin wir müssen: So wie früher alle Aktenzeichen XY geschaut haben, um über Verbrechen Bescheid zu wissen, so müssen wir uns alle informieren, was die gängigen Versuche sind, um unsere Unternehmen anzugreifen.

Alle müssen mit ins Boot

Das Bewusstsein dafür, dass Cybersecurity ein Thema für alle ist, muss wieder steigen. Denn jetzt schlägt das Pendel wieder zurück. Cybersecurity kann daher nicht nur ein IT-Thema sein. Sie betrifft uns alle. Es wäre das Beste, wenn sich alle Mitarbeiter:innen aktiv an der Cyberabwehr beteiligen. So wie es bei der Mülltrennung das Beste ist, wenn alle mitmachen. Und so lässt sich auch wirtschaftlicher arbeiten, wenn alle einen Teil dazu beitragen.

Resilienz als Gebot der Stunde

Wie können wir die Probleme also lösen? Es muss ein Zusammenspiel aus drei Dingen passieren: Der Staat selbst bzw. das Kollektiv muss sich aktiv am Kampf gegen Cyberkriminelle beteiligen. Die Staaten stellen unisono fest, dass sie das Problem mit Regulatorik in den Griff bekommen müssen. Und auch der Staat sagt, dass Cybersecurity überlebensnotwendig ist und nicht ein bloßer Wettbewerbsvorteil. Technische Lösungen müssen ständig weiterentwickelt und verbessert werden. Dazu muss das Budget in Unternehmen aufgestockt und die richtigen Investitionen in IT- und OT-Sicherheit getätigt werden. Und schließlich muss ganz klar der Fokus auf den Menschen gelegt werden, um ihn zu befähigen. Denn nur gemeinsam sind wir stark.

Entweder wir tauchen ab und verstecken uns am Meeresgrund oder wir nehmen uns die Schildkröte als resilientes Tier zum Vorbild, das in der Lage ist mit unterschiedlichsten Umgebungen klar zu kommen. Genau dieses Ziel müssen Unternehmen haben. Das Gebot der Stunde ist Resilienz. Denn wenn die See immer rauer wird, müssen wir resilienter werden.

Übersicht Key-Findings

Cyberangriffe haben in den letzten 12 Monaten um 201 Prozent zugenommen

55% der Befragten sagen, dass Cyberangriffe ihre geschäftliche Existenz bedrohen

33% der Unternehmen berichten von einer Betriebsunterbrechung aufgrund eines Ransomware-Angriffs von rund einer Woche

12% erlitten einen finanziellen Schaden von mehr als EUR 1 Mio. durch Cyberangriffe

Jedes dritte Unternehmen (**33%**) hat Zusammenhänge zwischen dem Krieg in Europa und den Cyberangriffen auf das eigene Unternehmen festgestellt

Bei **25%** der Befragten ist es in privat genutzten sozialen Netzwerken zu Beeinflussungsversuchen gekommen, die auf das berufliche Umfeld abzielten

28% geben sogar an, zwischen sieben und zwölf Monaten zu benötigen, um Fachkräfte zu finden

Jede:r dritte Befragte (**33%**) würde bevorzugt Securitylösungen von österreichischen Unternehmen einsetzen

43% der befragten Unternehmen benötigen durchschnittlich vier bis sechs Monate, um IT-Expert:innen einzustellen

33% der befragten Unternehmen waren Opfer von Ransomware/Erpressung

22% waren in den letzten zwölf Monaten von Deepfakes betroffen

Gehen wir es an!

Cybersicherheit ist ein sehr komplexes und vielschichtiges Thema mit einer Vielzahl an Herausforderungen. Mit KR Ing. Wolfgang Hesoun sprachen wir über die Chancen, Risiken und die Bedeutung von Cybersecurity für den Wirtschaftsstandort Österreich.

Der Begriff Krise hat sich in unserem Vokabular eingeprägt, eine Krise folgt der nächsten. Das World Economic Forum hat in diesem Jahr in Davos den Begriff der „Polycrisis" ins Spiel gebracht. Sind wir an der Schwelle oder bereits mittendrin in einer „Polycrisis"?

Wolfgang Hesoun: Ohne Zweifel hatten wir in den vergangenen Jahren einige Herausforderungen zu bewältigen. Neben der Covid-19-Pandemie und ihren wirtschaftlichen Folgen, hat der Beginn der russischen Invasion in der Ukraine im Februar des vergangenen Jahres zudem auch eine geopolitische Neuordnung initiiert, in der Europa schnellstmöglich neue Strategien für seine Energie-, Wirtschafts- und Sicherheitspolitik formulieren musste. Obwohl diese Herausforderungen ein hohes Maß an Komplexität mitbringen, bin ich dennoch zutiefst überzeugt, dass wir diese auch lösen werden. Ob man diese nun als Polycrisis bezeichnen will, ist meiner Ansicht nach reine Semantik und ändert nichts an der Realität.

Warum können wir aus Ihrer Sicht trotz Polycrisis mit Optimismus in die Zukunft blicken?

Wolfgang Hesoun: Jeder Krise wohnt auch eine Chance inne. Hinzu kommt, dass es meist Druck braucht, um ernsthafte Veränderungen herbeizuführen. Vor einigen Jahren standen saure Flüsse oder das Ozonloch im Zentrum der Diskussionen. Beides steht heute nicht mehr im Fokus. Vielmehr wurden die notwendigen Schritte gesetzt und vielfach in moderne Technologien investiert. Heute prägt der Klimawandel die Endlichkeit von Ressourcen oder aber die Notwendigkeit bzw. die Chancen der Digitalisierung, die Diskussion. Hier gilt es nichts kleinzureden, vielmehr ins Tun zu kommen.

Was machen wir in Österreich besonders gut und worauf können wir stolz sein?

Wolfgang Hesoun: Mit Digitalisierung werden zumeist US- und mittlerweile auch vielfach asiatische Konzerne in Verbindung gebracht. Die Vereinigten Staaten haben zwar einen deutlich höheren Anteil digitaler Unternehmen als die Europäische Union. Doch ist Europa führend bei Unternehmen, die in Maßnahmen investieren, um die Digitalisierung industrieller Prozesse voranzutreiben, sich dem Klimawandel und seinen physischen Auswirkungen zu stellen oder Klimaschutz und Digitalisierung miteinander zu verbinden.

Österreich und Europa nehmen in der Automatisierung und Digitalisierung der Industrieproduktion eine Vorreiterrolle ein. Wir brauchen den internationalen Vergleich mit Innovationsnationen nicht scheuen. Die EU ist mit nur sieben Prozent der Weltbevölkerung für 20 Prozent der globalen F&E-Investitionen verantwortlich. Wir investieren viel in Forschung und Entwicklung und haben eine robuste industrielle Basis, die uns gerade jetzt in der Krise stark geholfen hat. Wir haben hohe Expertise im Bereich künstliche Intelligenz, IoT und Edge Computing in Verbindung mit dem notwendigen industriellen Domain-Know-how, das Microsoft, Google oder andere eben nicht haben.

Wie digital ist die Industrie in Österreich aus Ihrer Sicht? Ist das Thema Cybersicherheit in der OT (Operation Technology – Industriesteuerungsanlagen) schon angekommen? Welchen Stellenwert muss das Thema bekommen?

Wolfgang Hesoun: Corona hat sicherlich dazu beigetragen, dass die österreichische, aber auch die europäische Wirtschaft einen Digitalisierungsschub erfahren hat. Digitalisierung per se ist kein bequemer Prozess. Vielmehr greift sie tief in sämtliche Prozesse des Unternehmens ein, verändert Arbeitsabläufe, Kommunikation oder Kauf- und Kund:innenverhalten – unter Umständen das komplette Geschäftsmodell.

Um den wirtschaftlichen Erfolg und den Wohlstand in Österreich nachhaltig zu sichern, muss es unser Anspruch sein, Österreich zum digitalen Vorreiter zu machen.

Cybersicherheit hat in den letzten Jahren stark an Bedeutung gewonnen. Cyberkriminelle versuchen nicht nur verstärkt in digitale Systeme und Netzwerke einzudringen, sondern entwickeln auch ständig neue Taktiken, um zu sensiblen Daten zu gelangen und daraus Kapital zu schlagen. Österreich ist hier vielfach gut aufgestellt, dennoch gibt es auch noch Entwicklungspotenziale.

Hat der Fachkräftemangel dazu beigetragen, dass diese Entwicklungen, also die Verlagerung in die Länder des Fernen Ostens, beschleunigt wurden? Wie können wir gegensteuern?

Wolfgang Hesoun: Primär muss das Ziel sein, den Arbeitsmarkt entsprechend zu attraktiveren, um dem Fachkräftemangel – aktuell fehlen in Österreich ca. 25.000 IT-Fachkräfte – entgegenzuwirken.

Im Wesentlichen ist dabei an zwei Stellschrauben zu drehen:
Erstens muss der Standort Österreich als attraktiver und lebenswerter Arbeitsort positioniert werden, um auch für einen internationalen Talent Pool attraktiv zu sein. In den vergangenen Jahren war ein Brain-drain hoch qualifizierter Arbeitskräfte in ostasiatische Länder bzw. nach Nordamerika zu erkennen. Hier muss es unbedingt zu einer Trendumkehr kommen, wenn Österreich und Europa langfristig kompetitiv bleiben wollen.
Zweitens gilt es Ausbildungs- und Umschulungsprogramme im MINT-Bereich zu forcieren, um auch eine nationale Talentmobilisierung in Österreich auf den Weg zu bringen und einen Grundstein für die langfristige Verfügbarkeit österreichischer IT-Fachkräfte zu legen.

FOTO © PHOTO SIMONIS

KR Ing. Wolfgang Hesoun
Vorsitzender des Infrastrukturausschusses der Industriellenvereinigung (IV), Vizepräsident der Wirtschaftskammer Österreich (WKÖ), Präsident des Fachverbandes der Elektro- und Elektronikindustrie (FEEI)

Digitalisierung soll zum großen Standortvorteil Europas werden. Wie geht das zusammen mit der fehlenden Offenheit gegenüber disruptiven Technologien? Wie könnte eine Offenheit gegenüber disruptiven Technologien gelingen bzw. erzeugt werden?

Wolfgang Hesoun: Ein zentraler

Treiber eines Paradigmenwechsels in Europa hin zu mehr Technologieoffenheit muss ein Informationsaustausch mit Unternehmen und Staaten sein, die bereits eine Technologieführerschaft in gewissen Branchen aufweisen können. Best Practices und Standards großer Player können richtungsweisend für europäische und besonders österreichische Unternehmen sein. Ein Austausch auf Behördenebene kann ebenso wichtige Einblicke in die Legistik zu bestimmten Technologien geben.

Zudem gilt es zu erkennen, dass disruptive Technologien im IT-Sektor zu einem entscheidenden Wettbewerbsvorteil werden können. Um die internationale Wettbewerbsfähigkeit europäischer Unternehmen langfristig zu sichern, ist es unbedingt notwendig, Offenheit zu beweisen und Innovationen zuzulassen und hinderliche Überregulierungen abzubauen.

Beobachtet man die momentanen Entwicklungen in Europa, so versuchen wir gerade eine Cyberfestung zu werden. Könnte dies für den Standort Österreich negative Auswirkungen haben oder müsste dieses Ziel besser/vorteilhafter kommuniziert werden?
Wolfgang Hesoun: Die Schlüsselattribute der österreichischen IT-Wirtschaft, nämlich die starke Innovationskraft, ein hohes Niveau des Datenschutzes und der Informationssicherheit, könnten in diesem Zusammenhang definitiv vorteilhafter und als Qualitätssiegel kommuniziert werden, das ideale Voraussetzung für die Etablierung einer Cybersicherheits-Zertifizierungsstruktur bietet.

Österreich sollte unbedingt seine starke Innovationskraft nutzen und die Digitalisierung zusammen mit Cybersicherheit – auch mit Fokus auf Internet of Things – als Beschleuniger für Wachstum einsetzen. Die aktuell fehlende Standardisierung sowie Normen könnten durch den Cybersecurity Act sowie eine Zertifizierungsstruktur für Europa und Österreich etabliert werden. Im Sinne der Blockfreiheit könnte Österreich den Neutralitätsbonus beanspruchen und das hohe Niveau des Datenschutzes und der Informationssicherheit als Qualitätssiegel nutzen.

> **Cybersicherheit ist das Zukunftsthema schlechthin.**
>
> Wolfgang Hesoun

Die EU hat mit der NIS2-Richtlinie die Anforderungen für wesentliche und wichtige Unternehmen erhöht und erwartet sich durch die verpflichtende Meldung von Cybersicherheitsvorfällen ein besseres Lagebild. Stärken diese Anforderungen das Vertrauen in den Wirtschaftsstandort oder schreckt es Unternehmen und Investoren ab?
Wolfgang Hesoun: Cyberattacken in Form von Phishingmails, Hacks, Mal- und Ransomware jeglicher Art bergen ein signifikantes und vor allem reales Gefahrenpotenzial für österreichische und europäische Unternehmen und sind bereits heute jährlich für Schäden in Millionenhöhe verantwortlich.

Die NIS1-Richtlinie war bereits ein wichtiger Katalysator, der den Weg für Veränderungen in den institutionellen und regulatorischen Strukturen im Bereich Cybersicherheit geebnet hat. Gleichzeitig wurden aber auch noch nicht identifizierte Problemfelder aufgedeckt, beispielsweise die fehlenden Cybersicherheitsmaßnahmen und das (teilweise) unzureichende Cyber-Resilienz-Niveau der Unternehmen.

Eine gesamtumfängliche Stärkung der Cyber-Resilienz durch NIS2 ist grundsätzlich zu begrüßen, da es uns gelingen muss, Cyberattacken durch proaktiven Austausch und intensivierte Kommunikation zwischen Unternehmen und Behörden vorzubeugen. Ein resilientes und effizientes Cybersicherheitsnetzwerk am Wirtschaftsstandort stärkt dessen Wahrnehmung am internationalen Markt und wirkt sich positiv auf zusätzliche Investitionen im Land aus.

Könnten die Regeln für Anleger aus dem Ausland zu streng sein?
Wolfgang Hesoun: Die steuerlichen Rahmenbedingungen sind ein zentraler Aspekt des Wirtschaftsstandortes Österreich. Aufgrund der Höhe der Abgaben weist der Standort für (IT-) Unternehmen eine geringe Attraktivität auf.

Da der IT-Sektor wie kein anderer durch die Mobilität von Kapital und Arbeitskräften (Remote Work, Homeoffice etc.) geprägt ist, wirkt sich dieser Umstand besonders nachteilig auf den Wirtschaftsstandort Österreich aus und zwingt innovative Unternehmen zur Abwanderung bzw. wird Österreich als potenzieller Standort im Vorhinein ausgeschlossen.

Eine Anpassung des Steuerrechts und Senkung der Abgabenquote sowohl für Unternehmer als auch Anleger – Stichwort Behaltefrist bei der Kapitalertragsteuer – sind hierbei zentrale Hebel, um Anreize für Investitionen und Arbeitsplätze zu schaffen und die Wettbewerbsfähigkeit Österreichs langfristig aufrecht zu erhalten.

Aktuelle Schätzungen gehen davon aus, dass vier- bis fünftausend Unternehmen in Österreich davon betroffen sind. Was wird das für den Wirtschaftsstandort bedeuten?
Wolfgang Hesoun: Derzeit übersteigt die Anzahl der gemeldeten Cyberattacken jene der aufgeklärten Fälle. Um hier chronische Backlogs zu vermeiden und effektive Lösungen zu implementieren, halte ich es für essenziell, die digitalen Kompetenzen in Österreich rasch auszubauen und zu verbessern.

Allein schon das Sammeln und Auswerten von Daten hat eine nicht zu unterschätzende Bedeutung für produzierende Betriebe – hierfür müssen dringend Kompetenzen und Kapazitäten auf europäischer und österreichischer Ebene gesteigert werden.

Auch sollten bestehende Potenziale besser genutzt werden, beispielsweise Cloud-Infrastrukturen, um Unternehmensstrukturen resilienter zu machen und Präventionsmaßnahmen zu forcieren.

Wie relevant ist für den Wirtschaftsstandort das Image Österreichs, ein cybersicheres Land zu sein?
Wolfgang Hesoun: Cybersicherheit ist – neben Digitalisierung und Nachhaltigkeit – für Unternehmen quer über alle Branchen das Zukunftsthema schlechthin. Allein gegenüber dem letzten Jahr können wir in Österreich eine Zunahme der Cyberangriffe um ca. 200 % verzeichnen.

Unternehmen brauchen Planbarkeit und Sicherheit. Das Image eines cybersicheren Wirtschaftsstandorts ist daher essenziell, um heimische Unternehmen im Land zu halten und Unternehmen aus dem Ausland zu signalisieren, dass sie in Österreich auf eine sichere Cyber-Infrastruktur vertrauen können, die Angriffen proaktiv begegnet und sensible Unternehmensdaten schützt.

Mit (Aus)- und Weiterbildung haben wir einen thematischen Schwerpunkt in dieser Studie gesetzt. Berufsbilder und Ausbildungswege haben sich in den letzten Jahren stark verändert. Welchen Bildungsweg würden Sie heute einschlagen, wenn Sie am Anfang Ihrer Karriere stünden?
Wolfgang Hesoun: Ich würde wieder eine technische Ausbildung absolvieren. Die vielfach angesprochenen Herausforderungen von heute und morgen benötigen den Einsatz modernster Technologie. Nur so werden wir die angestrebte Transformation unseres Energiesystems oder aber auch die eben besprochenen Themen rund um Cybersicherheit und Informationstechnologie schaffen.

Ein Jahr danach

Im Jahr 2022 haben wir unsere Interviewpartner gefragt:
„Wenn wir uns in einem Jahr wieder treffen, was würden wir uns jetzt wünschen, bereits getan zu haben?“

Wie hat sich die Lage im vergangenen Jahr verändert? Was sagen sie heute?

Im vergangenen Jahr wurden Maßnahmen gesetzt, die kurzfristigen Erfolg versprechen.

Die großen Fragen zu den langfristigen Herausforderungen, wie beispielsweise die Steigerung der nationalen Resilienz, des Wehrwillens und der Steigerung der strategischen Autonomie der Europäischen Union können jedoch nicht mit Ad-hoc-Maßnahmen beantwortet werden.

Es gilt Jahrzehnte der Illusion aufzuholen.

FOTO © MATTHIAS WASINGER PRIVAT

ObstltdG Mag. (FH) Matthias Wasinger MoS Ph.D.
Gründer des Onlinejournals The Defence Horizon Journal

Die Fachkräftethematik hat sich wie erwartet verschärft. Aber es wurde auch einiges getan, beispielsweise hat eine Gruppe von Frauen mit Verena Becker (WKO, Bundessparte Information und Consulting) als Vorsitzende im vergangenen Jahr das Austria Chapter von Women4Cyber gegründet. Women4Cyber ist eine europäische Non-Profit-Organisation mit dem Ziel, Frauen im Bereich der Cybersicherheit zu fördern.

Im Ausbildungsbereich hat die FH Salzburg einen neuen Studiengang „Cybersecurity“ aufgebaut, der ab 2023/24 angeboten wird.

Es setzt sich auch immer mehr das Verständnis durch, dass Cybersecurity-Expert:innen höhere Löhne erwarten und dass dies ein Teil des empfundenen Fachkräftemangels ist. Allerdings geschieht dieser Bewusstseinswandel immer noch zu langsam und währenddessen wandern die Expert:innen zu internationalen Unternehmen ab.

FOTO © WWW.ANNARAUCHENBERGER.COM

Wolfgang Rosenkranz
Teamleiter cert.at

Wir haben zwar viele Fortschritte gemacht und sehen auch, dass die Themen Cybersicherheit und -resilienz nicht nur in den Führungsetagen, sondern auch in der breiten Öffentlichkeit angekommen sind, jedoch gibt es noch immer Aufholbedarf – bei der Umsetzung der notwendigen Maßnahmen sowie bei der Notwendigkeit, schneller auf Veränderungen zu reagieren.

Die Angriffsmöglichkeiten, die sich Kriminellen mit Werkzeugen wie ChatGPT oder Stable Diffusion bieten oder aber auch der kriminelle Missbrauch im Bereich Decentralized Finance sind hier relevante Beispiele. Hier muss noch ein stärkerer Fokus auf vorausschauende Risiko- und Technologiebewertung, aber auch auf bessere Kollaboration und Prinzipien wie Security, Privacy and Safety by Design gelegt werden.

Mit NIS2 und anderen relevanten Regelwerken wie dem Digital Services Act sind hier in der EU aber sehr wichtige Meilensteine erreicht worden, die uns bei der Erreichung unseres gemeinsamen Zieles – einer sicheren, nachhaltigen und menschengerechten digitalen Zukunft für die Unternehmen und Bürger:innen der EU – signifikant unterstützen und auch als Innovationsansporn dienen werden.

FOTO © WWW.ANNARAUCHENBERGER.COM

Dr. Philipp Amann
Head of Strategy
Europol

IT-Sicherheitsmaßnahmen können weiterhin mehr Stärkung vertragen, es gibt leider erste Firmen, die aufgrund von Ransomware-Attacken pleite gegangen sind. Hier können wir von der Ukraine lernen, die durch Diversifizierung und permanente Warnungen ihre IT-Infrastrukturen selbst unter Cyberkriegsbedingungen stabil hält.

Das kritische Auseinandersetzen mit sozialen Medien ist leider noch nicht eingetreten, die Melange aus Desinformation, Influencer:innen kreierten ökonomisch basierten „Wahrheiten" und journalistischem False Balancing hat nicht dazu beigetragen, dass sich die Diskursqualität verbessert hat, sondern im Gegenteil, selbst kleinste Anlässe wie der Fall „Winnetou" entwickeln sich völlig unnötigerweise spontan zu „politisch relevanten" Themen.

FOTO © BUNDESWEHR

Oberst i.G. Dipl.-Ing. Sönke Marahrens
Director COI Strategy and Defense Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats

Cybersecurity und Krisenvorsorge sind ein Begriffspaar in unsicherer Zeit! Tragfähige Lösungen sind daher immer nur eine Antwort für den Moment. Wir dürfen also nicht meinen, dass es den einen Masterplan gibt, der einmal entwickelt für alle Zeiten Gültigkeit behält. Dies hat die im Zuge des Ukraine-Krieges ausgerufene „Zeitenwende" und die damit verbundene Besinnung auf die Landes- und Bündnisverteidigung nachdrücklich in den Fokus gerückt.

Im Duo von Cybersecurity und Krisenvorsorge geht es also darum, Restrisiken zu definieren, geeignete Verfahren zu entwickeln, um mit getrennt gesicherten oder sogar analogen Daten weiterzuarbeiten und Akteur:innen gezielte Anreize zu bieten, selbst in Sicherheit zu investieren. In einer Zeit der Gleichzeitigkeit von Ereignissen und Szenarien wird dabei auch die Anzahl und die Ausrichtung der Akteur:innen mannigfaltiger.

FOTO © NICOLE LEHMANN/PRIVAT

Björn Stahlhut
Bereichsleiter und Projektleiter Notfallversorgung und Gesundheitssicherheit
Deutsches Rotes Kreuz

Die nationale und internationale Zusammenarbeit bei der Bekämpfung von Cyberangriffen ist enorm wichtig.

Ein regelmäßiger Austausch mit Partner:innen aus dem In- und Ausland kann entscheidend sein und muss auch in Zukunft gefördert werden.

FOTO © PASCAL LAMIA PRIVAT

Pascal Lamia
Bundesamt für Cybersicherheit in der Schweiz

Die Zahlen im Jahresvergleich

Veränderung der Angriffe
Werfen wir einen Blick darauf zurück, wie sich die Dinge im Vergleich zum Vorjahr verändert haben. Haben sich unsere Anstrengungen bezahlt gemacht oder haben wir noch nicht all unsere Kraft aufgewendet? Schauen wir uns die Top 5 genauer an:
Das dominanteste Phänomen ist der *Identitätsdiebstahl*. Es ist nicht weiter verwunderlich, dass dieser auf Platz eins ist, obwohl uns die Dominanz durchaus überrascht. Hier können drei verschiedene Ursachen dahinterstecken: Erstens wird zusammenhängend mit der gestiegenen Bedeutung von Social Engineering – welche auch unsere Studie zeigt – immer stärker versucht, Identitäten zu stehlen, um mit vergleichsweise geringem Aufwand direkten Zugriff auf Daten o. Ä. zu erhalten. Die zweite Ursache liegt im Phänomen Ransomware, bei dem es auch zum Diebstahl von Identitäten kommt, wo diese an die Öffentlichkeit gelangen. Das lädt Trittbrettfahrer:innen dazu ein, diese missbräuchlich zu verwenden. Drittens ist hier noch die verstärkte Nutzung von Cloud(SaaS)-Lösungen zu erwähnen, die angegriffen werden und im Zuge dessen Benutzer:innen- bzw. Kund:innendaten gestohlen werden.

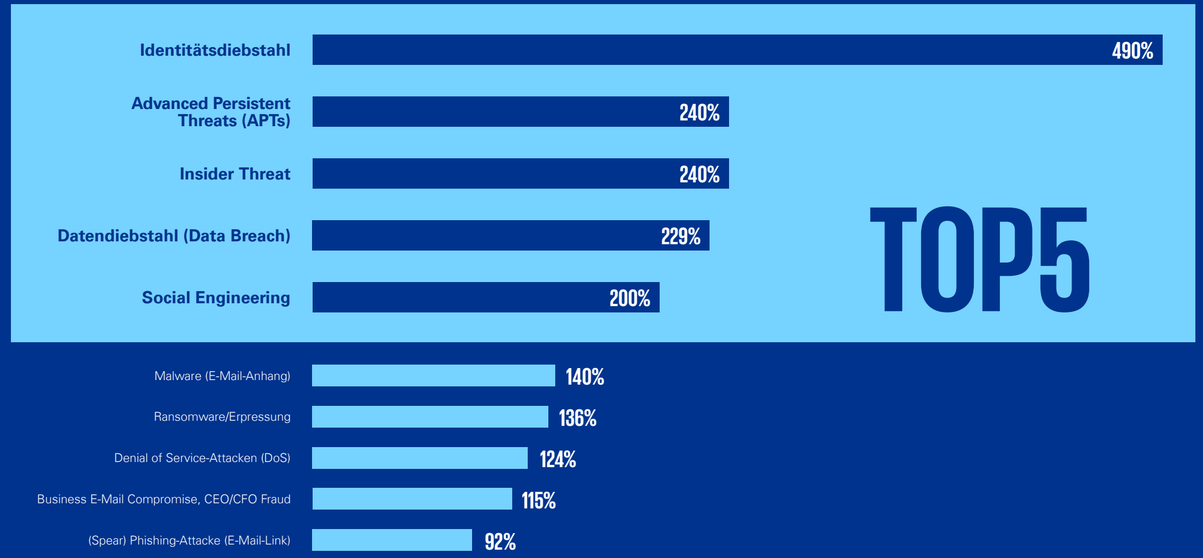
An zweiter Stelle befinden sich *Advanced Persistent Threats (APTs)*. Diese sind auf die Zunahme geopolitischer Spannungen und Konflikte zurückzuführen sowie auf die gezielte Absicht von Nationalstaaten, geistiges Eigentum vom Mitbewerb zu stehlen bzw. Spionage zu betreiben.

Insider Threat ist ein in der Vergangenheit unterschätztes Phänomen, aber in Zeiten wirtschaftlicher Herausforderungen und sozialer Spannungen ist es ein Phänomen, das mehr Aufmerksamkeit bedarf, weil Opportunist:innen hier ihre Chance ergreifen. Unternehmen investieren auch kaum in Tools zur Bekämpfung. Die veränderte Arbeitswelt weg von einem sehr stark kontrollierten Bereich hin zur hybriden Arbeitswelt, in der noch keine passende Security-Antwort gefunden wurde, stellt auch einen Grund für die Veränderung dar. Auch die explosionsartige Zunahme von APIs (Application Programming Interfaces), die oft nachlässig oder unzureichend abgesichert werden und so eine Einladung für Angreifer:innen darstellen, müssen in diesem Zusammenhang erwähnt werden.

Die Zunahme von *Datendiebstahl* (Data Breach) hängt mit den verstärkten Ramsomare-Aktivitäten zusammen, was auch eine Form der Erpressung und des Druckaufbaus darstellt. Es ist also kein Wunder, dass die Zahlen in die Höhe schießen, wobei der derartig hohe Anstieg doch überraschend ist.

Die Zunahme von *Social Engineering* unterstützt erneut die Aussage, dass der Mensch im Mittelpunkt steht, weil es die einfachste Möglichkeit ist, ihn durch Manipulation bzw. Beeinflussung und Desinformation zu attackieren.

Veränderung der Angriffe von 2022–2023



Einordnung der Bedrohungen
Besonders hervorstechend ist, dass staatliche oder ***staatlich unterstützte Angriffe*** auf dem Vormarsch sind. Das Thema der professionellen und zielgerichteten Angriffe wird für Unternehmen allgegenwärtig.

Phishing bleibt weiterhin auf einem sehr hohen Niveau und für Unternehmen gleichzeitig normales Tagesgeschäft. Hier stellt sich die Frage, dass wenn wir wissen, dass jedes Unternehmen Opfer von Phishing wurde, warum es dann weiterhin für die Unternehmen „nur" normales Tagesgeschäft bleibt.

Social Engineering verzeichnet Zunahmen als besondere Herausforderung, da v. a. die gezielte Desinformation hier als Bedrohung immer präsenter wird.

Der Zunahme von ***Insider Threats*** tragen Unternehmen bereits Rechnung und sehen es immer mehr als besondere Herausforderung, diesen zu begegnen.

Im Vergleich zu 2022 ist ***Ransomware/Erpressung*** für viele noch immer eine besondere Herausforderung.

Cybersicherheitsmaßnahmen im Vergleich:
Weiterhin Spitzenreiter ist hier das ***Business Continuity Management***, stellt es doch die Fortsetzung der Geschäftstätigkeiten nach einem Angriff sicher. Das Spannende dabei: Das Thema, mit dem wir uns schon vor 15 Jahren beschäftigt haben, erlebt einen erneuten Höhenflug.

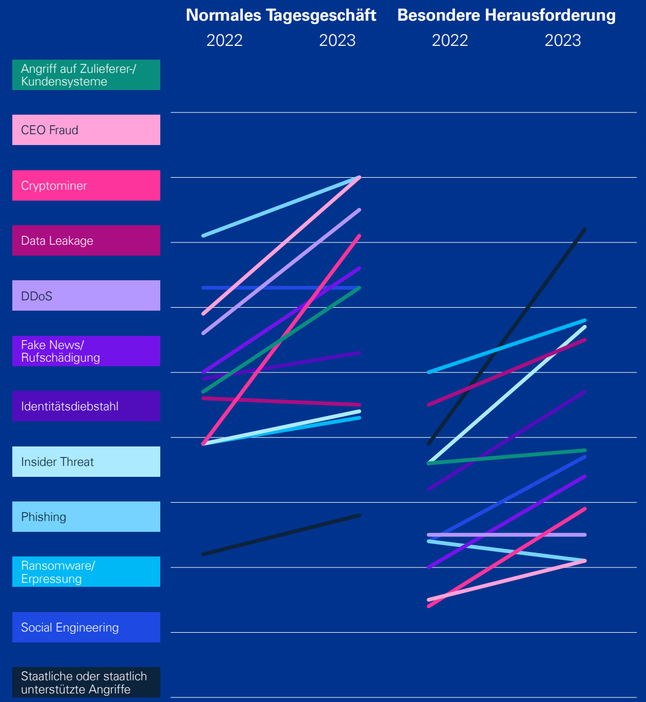
End User Security & Awareness bleibt weiterhin stabil und nicht auf dramatischem Niveau. Unternehmen setzen sich mit dem Thema auseinander, da sie eine gewisse grundlegende Notwendigkeit darin sehen.

Zwei Aspekte, die uns jedoch aufhorchen lassen: Es gibt einen Rückgang im Bereich ***Vulnerability Management*** gegenüber dem Vorjahr. Obwohl Schwachstellen immer noch das Einfallstor Nummer eins sind, ist das Thema generell etwas in den Hintergrund gerückt.

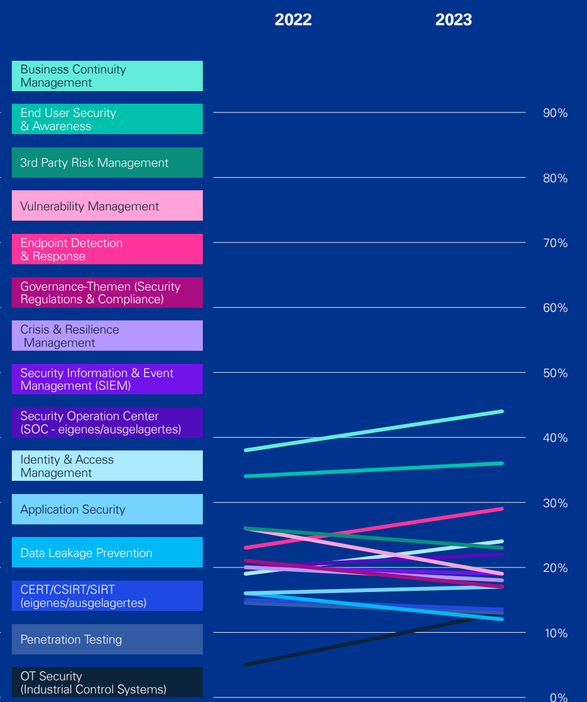
Die zweite Überraschung findet sich im Zusammenhang mit ***Data Leakage Prevention:*** Obwohl bekannt ist, dass Datenabfluss eine wesentliche Zunahme erfahren hat und unter den Top 5 zu finden ist, ist das Thema und dessen Priorität nach hinten gerückt und nimmt hier die niedrigeren Ränge ein.

Zahlen im Jahresvergleich

Einordnung der Bedrohungen: Zwischen normalem Tagesgeschäft und besonderer Herausforderung



Cybersicherheitsmaßnahmen im Vergleich



Rückblick

100 % haben in den letzten zwölf Monaten Phishingattacken erlebt

88 % waren Business E-Mail Compromise und CEO Fraud ausgesetzt

0 % der befragten Unternehmen, die von Ransomware-Angriffen betroffen war, haben die damit verbundene Lösegeldforderung bezahlt

69 % EPUs wurden Opfer von Phishing

42 % haben eine (starke) Zunahme von Cyberangriffen in den vergangenen zwölf Monaten beobachtet

14 % der Befragten wissen nicht, ob erfolgreiche Cyberattacken gegen ihre Unternehmen stattgefunden haben

10 % wurden erst durch Lösegeldforderungen auf einen Angriff auf ihr Unternehmen aufmerksam

60 % wurden über die eigenen Mitarbeiter:innen auf Angriffe aufmerksam

In den letzten zwölf Monaten war jedes der von uns befragten Unternehmen mindestens ein Mal Ziel eines Cyberangriffs.

Das ist mittlerweile tägliche Routine, denn Cyberangriffe finden zu jeder Tages-und Nachtzeit an sieben Tagen die Woche statt. Ob sie erfolgreich sind oder nicht, hängt von den Vorkehrungen ab, die Unternehmen treffen.

42 Prozent unserer Befragten haben eine (starke) Zunahme von Cyberangriffen in den vergangenen zwölf Monaten beobachtet. Im Vergleich zum Vorjahr lag der Wert noch bei 29 Prozent. Damit zeigt sich auch hier die besorgniserregende Entwicklung, dass Cyberangriffe mittlerweile mitten im Unternehmensalltag angekommen sind.

Auch die Aktivitäten im Cyberraum (Cyberdomäne[1]), die während der aktuellen geopolitischen Konflikte besonders stark zugenommen haben, führten zu einer verstärkten Anzahl von Angriffen. Den Unternehmen muss bewusst werden, dass es sich bei staatlichen oder staatlich unterstützten Angriffen (APTs) um reale und existenzbedrohende Angriffe handelt: Sie passieren nicht irgendwo weit weg und gehen uns nichts an, sondern sie werden bewusst von staatlichen Akteur:innen in Auftrag gegeben und haben das Potenzial – und auch das Ziel – heimische Betriebe sowie unsere kritische Infrastruktur lahmzulegen.

Auf Tauchstation

Rund jeder zehnte Angriff (12 Prozent) in den letzten zwölf Monaten war ein erfolgreicher Cyberangriff, der zu Schäden für die Unternehmen führte. Ganze 14 Prozent der Befragten wissen jedoch nicht, ob Cyberattacken festgestellt wurden. Dies lässt darauf schließen, dass es immer noch keine Transparenz bezüglich Cyberattacken in Unternehmen gibt.

Was hier besonders überrascht: Auch 14 Prozent der EPUs wissen nicht, ob es Cyberattacken auf ihr Unternehmen gab, die zu Schäden geführt haben. Diese Ergebnisse stimmen auch mit der Analyse des KSV1870 überein, dass drei von zehn österreichischen Unternehmen es nicht schaffen, IT-Sicherheitsvorfälle zu erkennen[2].

Artenvielfalt

Was die Angriffsarten auf Unternehmen innerhalb der letzten zwölf Monate angeht, berichten 33 Prozent von Ransomware/Erpressung, 57 Prozent von Social Engineering und 39 Prozent von einem Angriff auf die Lieferkette. Auch Deepfakes treten mit 22 Prozent als Phänomen auf. Business E-Mail Compromise und CEO/CFO Fraud erleben Hochkonjunktur mit 88 Prozent. Phishing ist ganz klar gekommen, um zu bleiben: 100 Prozent haben in den letzten zwölf Monaten Attacken dieser Art erlebt. Blickt man im Speziellen auf die EPUs, so zeigt sich, dass 69 Prozent Opfer von Phishing wurden, 79 Prozent von Malware und 59 Prozent von Passwortdiebstahl.

Diese Zahlen verdeutlichen, dass Unternehmen alle Hände voll zu tun haben, um die Vielfalt der gegen sie gerichteten Angriffe abzuwehren bzw. deren negative Auswirkungen möglichst gering zu halten.

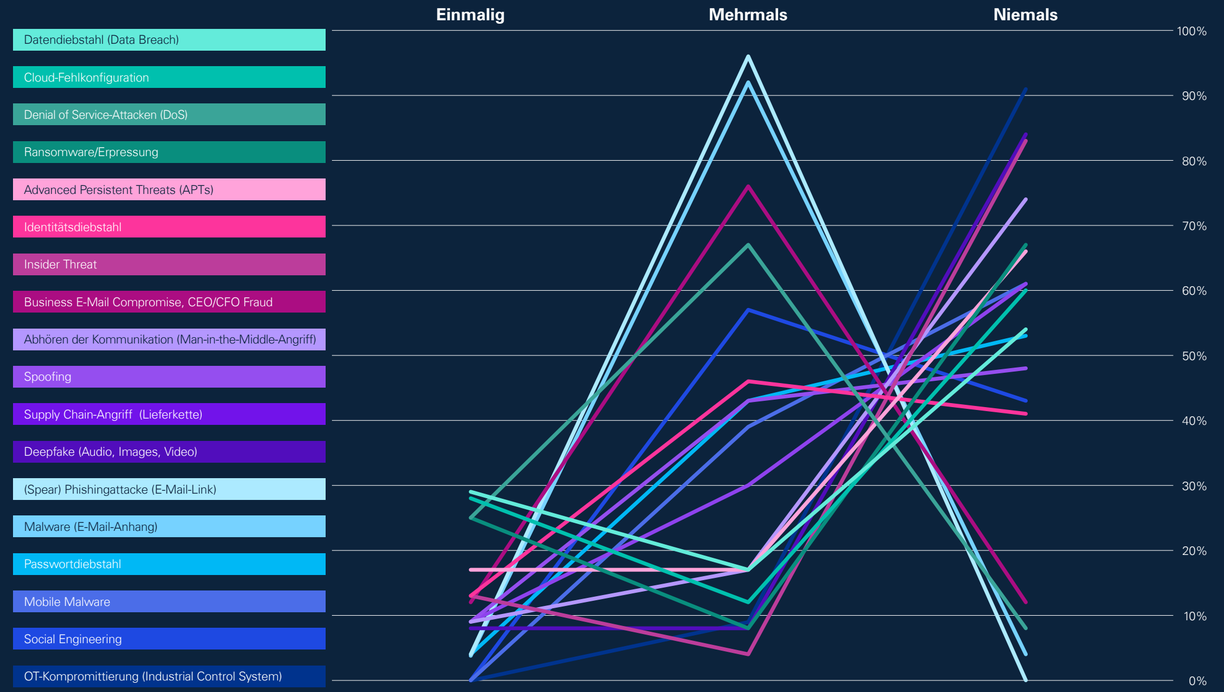
Keine voreiligen Entscheidungen

Bei der Frage, wie die Unternehmen auf die Angriffe aufmerksam wurden, ist auffallend, dass 10 Prozent erst durch Lösegeldforderungen auf einen Angriff auf ihr Unternehmen aufmerksam wurden.

Keines der befragten Unternehmen, das von Ransomware-Angriffen betroffen war, hat die damit verbundene Lösegeldforderung bezahlt.

[1] Geopolitische Konflikte werden in unterschiedlichen Domänen ausgetragen: Land, Wasser, Luft, Weltraum, Information und Cyber. Diese sind auch Bestandteil von hybriden Konflikten.
[2] KSV CyberRisk-Analyse März 2023

Häufigkeit der Angriffsarten in den letzten zwölf Monaten



Ransomware gilt nach wie vor als eine der größten Cyberbedrohungen für Unternehmen im Jahr 2023. Alleine im Jahr 2022 entfiel fast ein Drittel aller bekannten Ransomware-as-a-Service (RaaS)-Angriffe auf eine Gruppe.

Dass die Verhandlungen in Sachen Lösegeldzahlungen nicht immer einfach sind und oft auch nicht den gewünschten Erfolg bringen, zeigen jüngste Beispiele: Nach wochenlangen Verhandlungen hat eine Gruppierung die Aussicht auf Lösegeld aufgegeben und jene Dateien veröffentlicht, die sie beim Ransomware-Angriff gestohlen hat.

14 Prozent wollten sich nicht äußern, ob sie Lösegeld bezahlt haben. Das bestätigt die in Österreich vorherrschende Verschlossenheit bei diesem Thema. Es ist zu vermuten, dass Nationalstaaten in den nächsten Jahren immer mehr Gesetze erlassen werden, die Ransomware-Zahlungen, -Geldstrafen und -Verhandlungen reglementieren.

Die Schildkröte steht als Warnung vor übereilten Entscheidungen. Genauso sollte man auch bei Lösegeldforderungen nicht vorschnell reagieren und erst alle möglichen Auswege abwiegen. Ganz nach dem Vorbild unserer Schildkröte.

Wenn der Betrieb stillsteht

Bei ganzen 14 Prozent dauerte die Betriebsunterbrechung aufgrund eines Ransomware-Angriffs länger als vier Wochen. Jedoch zeichnet sich auch ab, dass die Ereignisse der vergangenen Jahre scheinbar dazu beigetragen haben, die Unternehmen zu sensibilisieren und besser vorzubereiten: 29 Prozent hatten nur eine Unterbrechung von weniger als 48 Stunden. Die Maßnahmen der Unternehmen zeigen also Wirkung.

Dennoch darf man den verhältnismäßig hohen Prozentsatz jener Unternehmen nicht außer Acht lassen, bei denen die Betriebsunterbrechung mehr als vier Wochen anhielt. Ein derartiger Betriebsausfall stellt eine klare Existenzbedrohung für viele Unternehmen dar und ist mit enormen Schäden verbunden.

Unsichtbarer Feind

Behörden, Kund:innen sowie CERT wurden nur teilweise von den Unternehmen über einen Ransomware-Vorfall informiert. Hier gibt es noch viel Aufhol- und Sensibilisierungsbedarf in puncto Vorfallsmeldung: Verschlossenheit dominiert auf diesem Gebiet nach wie vor und es findet kein Austausch zwischen den betroffenen Parteien über derartige Vorfälle statt. Die mangelnde Vernetzung und der mangelnde Austausch spielen den Angreifer:innen in die Hände, denn so können diese nahezu unsichtbar unter der Wasseroberfläche lauern.

Was Sie sich aus diesem Kapitel mitnehmen sollten:

1. **Cyberangriffe sind mittlerweile zur Routine für österreichische Unternehmen geworden: In den letzten zwölf Monaten war jedes der von uns befragten Unternehmen zumindest ein Mal Ziel von einem Cyberangriff.**

2. **Nach wie vor herrscht große Verschlossenheit bei Unternehmen über Cyberattacken und Lösegeldzahlungen.**

3. **Betriebsausfälle und -unterbrechungen nach einem Cyberangriff haben mitunter eine Dauer von über vier Wochen. Damit stellen sie eine klare Existenzbedrohung für viele Unternehmen dar und sind mit enormen Schäden verbunden.**

Erfahren Sie mehr in unserem Podcast IMPULSE

Bereit für NIS2?

Ende 2022 wurde die neue NIS2-Richtlinie veröffentlicht, die im Oktober 2024 offiziell in Kraft tritt. Bis dahin haben die Mitgliedstaaten Zeit, die Richtlinie umzusetzen. Im Interview mit Philipp Blauensteiner und Gernot Goluch sprachen wir über die Chancen und Herausforderungen.

Im Jahr 2016 hat das EU-Parlament die NIS-Richtlinie in Kraft gesetzt. Sechs Jahre später gibt es eine Neuauflage – die NIS2-Richtlinie, die Ende 2022 verabschiedet wurde. Was waren im Rückblick die großen Herausforderungen bei der Umsetzung der NIS1?

Philipp Blauensteiner: Eine der großen Herausforderungen war das Ändern des Mindsets vom reinen „Wir sind Partner der Betreiber kritischer Infrastruktur" hin zu „ Wir haben auch behördliche Aufgaben wahrzunehmen". Im operativen Bereich war natürlich die größte Herausforderung, dass auch wir Personal aufbauen mussten, damit wir diese Behördenaufgaben wahrnehmen konnten und dass wir uns an diese Behördenrolle auch gewöhnen mussten. Aber natürlich haben wir weiterhin beide Hüte auf – nämlich als Ansprechpartner unterstützend tätig zu sein, aber eben als Behörde auch Kontroll- und Aufsichtsaufgaben durchzuführen.

Gernot Goluch: Neben dem Thema, die behördlichen Aufgaben mit Leben zu erfüllen, was eine durchaus spannende Aufgabe war, möchte ich noch anführen, dass es ja vor dem NIS-Gesetz solche gesetzlichen Regelungen nicht gegeben hat und allein diese Tatsache machte das Ganze so interessant, sowohl für uns als Behörde als auch für betroffene Unternehmen.

Hat sich das Bewusstsein für Cybersicherheit und die Umsetzung von diesen Sicherheitsmaßnahmen durch die NIS1 wesentlich verändert?

Gernot Goluch: Für die Sektoren, die im NIS-Gesetz definiert wurden und die Betreiber wesentlicher Dienste sind, gilt das auf jeden Fall. Denn auch wenn diese Unternehmen sich schon vorher mit dem Thema befasst haben, ist es immer ein Unterschied, ob ein:e CISO der Unternehmensleitung Vorschläge unterbreitet oder ob dahinter ein Gesetz steht, dessen Umsetzung auch behördlich kontrolliert und eingefordert wird. Aber ich denke, dass sich in anderen Sektoren auch etwas bewegt hat, einfach weil man genauer hinschaut.

Philipp Blauensteiner: Definitiv. Dadurch, dass es ein Gesetz geworden ist, also weg von einer reinen IT-Materie, für die ein:e CISO verantwortlich ist, hin zu einer Materie, die aufgrund der verschiedensten Vorgaben auch in der obersten Leitungsebene ankommt. Durch diese Verordnung werden die CISOs, die zumeist ohnehin wissen, was getan werden sollte, in ihren Aufgaben massiv unterstützt und finden plötzlich wesentlich mehr Gehör.

Inwieweit waren neben den behördlichen Vorgaben auch die häufiger stattfindenden Cyberangriffe auf Unternehmen, die immer wieder medial aufschienen, ein ausschlaggebendes Kriterium für die umfassenden Maßnahmen der Unternehmen?

Philipp Blauensteiner: Das ist natürlich ein Aspekt, der mit dazu gehört, aber ich habe das Gefühl, dass diese Angriffe – auch wenn sie medial Aufmerksamkeit erregen – dann nur eine relativ kurze Aufmerksamkeitsspanne bei den betroffenen Unternehmen nach sich ziehen. Durch das Gesetz wurde das Thema Cybersicherheit zum permanenten Thema.

Gernot Goluch: Absolut. Allerdings ist es immer ein wenig schwer zu beurteilen, wie die Lage außerhalb der Cyber Community aussieht, denn wir sind natürlich jeden Tag mit Themen wie Ransomware konfrontiert. Aber natürlich ein Gesetz ist ein Gesetz – und da kann man davon ausgehen, dass das auch von außerhalb wahrgenommen wird.

Stichwort Cybersecurity Community: Besteht hier die Gefahr, dass Dinge übersehen werden, weil wir uns ständig mit den Themen auseinandersetzen, über die jeder spricht, wie Ransomware? Haben wir ein zu enges Blickfeld?

Gernot Goluch: Nein, denn rein aus der Gesetzesperspektive müssen wir uns ja um ein ganzes Set von Maßnahmen kümmern und nicht nur um eine spezifische Bedrohung wie Ransomware. Das reicht von Versicherungen über den Umgang mit Lösegeldforderungen bis hin zur Strafverfolgung.

Philipp Blauensteiner: Ransomware ist sicher das mediale Schlagwort. Aber man darf nicht vergessen, dass wir uns in den letzten Jahren auch mit anderen Cybersicherheitsthemen befasst haben, auch medial, diese aber eben nicht diese enorme Aufmerksamkeitsspanne bei den Unternehmen erreicht haben wie Ransomware. Hier gibt es natürlich immer einen Fokus darauf, weil es allgegenwärtig ist – und das Thema Ransomware ist auch allgemein leichter zu adressieren als tiefergreifende Themen wie Supply Chain Security.

> **Bei der Cybersicherheit ist es wie beim Automobil. Sie wird technologisch sukzessive weiterentwickelt und der Gesetzgeber zieht mit Regulativen nach.**

FOTO © BMI / GERD PACHAUER

DI Philipp Blauensteiner, MA
Leiter der Abteilung Netz- und Informationssicherheit im BMI, die die Aufgaben der operativen Behörde nach dem NIS-Gesetz wahrnimmt.

Je fachlich fundierter und detaillierter unsere Antworten sind, desto mehr Effekt hat das beim Unternehmen.

FOTO © BMI/GERD PACHAUER

Oberrat Mag.
Gernot Goluch
Leiter des Referats Recht & Audit in der Abteilung NIS (Netz- und Informationssystemsicherheit) im Bundesministerium für Inneres und dort mit zentralen Themen bzw. dem Vollzug ebendieser in der operativen NIS-Behörde betraut. Sein beruflicher Werdegang und Betätigungsfeld befindet sich seit seinem Studium an der TU Wien in der Informationssicherheitsbranche.

Supply Chain-Angriffe sind ein spannendes Thema, da wir immer öfter erleben, dass diese von staatlichen Akteur:innen getrieben werden. Inwieweit berücksichtigt die NIS-Richtlinie das Thema staatliche Akteur:innen?

Gernot Goluch: Wenn man sich das aktuelle NIS-Gesetz ansieht, dann sieht man ja, dass die Sicherheitsmaßnahmen nicht auf einen spezifischen Angriffsvektor definiert sind – sprich es beinhaltet schon ein breites Maßnahmenset von Governance über Krisenmanagement, Business Continuity, Supply-Chain bin hin zur Sicherheit von Dritten. All diese Maßnahmen würden aus meiner Sicht auch schon helfen, sich vor staatlichen Akteur:innen zu schützen. Ob das natürlich bei den Unternehmen in all diesen Facetten umgesetzt wird auch im Hinblick speziell auf staatliche Akteur:innen, bleibt offen.

Philipp Blauensteiner: Das möchte ich auch noch einmal betonen. Das Gesetz an sich zielt ja nicht auf bestimmte Phänomene ab, sondern generell auf Sicherheitsmaßnahmen, die zu setzen sind. Aber natürlich, wenn diese ordentlich umgesetzt werden und die richtige Risikoeinschätzung für das eigene Unternehmen vorliegt, können auch für den Bereich staatliche Akteur:innen bessere Maßnahmen gesetzt werden. Aber was es dazu braucht, ist Awareness – und diese zu schaffen, ist auch mit unsere Aufgabe als Behörde.

Ein wichtiger Punkt ist das „voneinander lernen". Ein gegenseitiger Austausch aufseiten der Behörden, aber auch zwischen Unternehmen und den EU-Mitgliedstaaten ist unabdingbar. Wo steht hier Österreich im Vergleich? Was funktioniert gut und wo gibt es Handlungsbedarf?

Gernot Goluch: Natürlich stehen wir mit den anderen EU-Mitgliedstaaten in Austausch. Was die Umsetzung der NIS1-Richtlinie angeht, stehen wir in Österreich denke ich eigentlich recht gut da. Es gibt unter den Mitgliedstaaten unterschiedliche Herangehensweisen, aber ich finde unser Weg einer stärkeren behördlichen Aufsicht – sprich spezifische organisatorische und technische Prüfungen zu verlangen, diese aber auch zu reviewen und wenn notwendig behördliche Maßnahmen zu verhängen – eigentlich positiv. Wie sich das bei NIS2 darstellen wird, bleibt abzuwarten.

Philipp Blauensteiner: Ich glaube auch, dass uns die Umsetzung tatsächlich geglückt ist. Wir schauen wirklich genau hin und hinterfragen auch, was uns vorgelegt wird und dadurch schaffen wir auch eine gewisse Ernsthaftigkeit bei der Umsetzung durch die Unternehmen.

In Bezug auf die Umsetzung geht es natürlich immer auch wieder um das Thema Strafen oder Sanktionen. Sind diese immer das probate Mittel oder können wir es auch mit anderen Mitteln bewerkstelligen?

Philipp Blauensteiner: Sanktionen und Strafen sind immer das letzte Mittel – auch wie wir das NIS-Gesetz vollziehen. Wenn natürlich gegen das Gesetz verstoßen wird, sind uns als Behörde die Hände gebunden, aber wir versuchen ja bereits im Vorfeld zu vermeiden, dass wir diesen Weg gehen müssen. Daher versuchen wir bereits aus den Stellungnahmen, die uns von den Betreibern übermittelt werden, Empfehlungen abzuleiten. Diese haben noch keine Rechtswirksamkeit und sind damit nicht strafbar, wenn sie nicht umgesetzt werden. Aber es ist natürlich eine Unterstützung für die Cybersicherheitsverantwortlichen, um die notwendigen Maßnahmen auch durchsetzen zu können.

Gernot Goluch: Wir sehen, dass eine gewisse Genauigkeit und Fachkompetenz bei unseren Rückmeldungen auch wieder zu einer gewissen Awareness bei den Unternehmen führt. Es sind also nicht immer zwingend Strafen notwendig, um eine Änderung herbeizuführen, aber natürlich schweben im Hintergrund immer potenzielle Sanktionen mit – das ist bei einer behördlichen Arbeit nun mal so.

Stichwort Awareness schaffen: Was können wir tun, damit die Anzahl der Meldungen steigt, um mehr Transparenz zu bekommen?

Gernot Goluch: Grundsätzlich landen die Meldungen ja bei den Computer-Notfallteams und wir verzeichnen seit dem NIS-Gesetz schon ein gestiegenes Meldeaufkommen – aber natürlich kann das immer noch verbessert werden. Ich glaube, es geht um die Frage: Was möchte der:die Melder:in eigentlich nach der Meldung haben? Möchte man nur melden, möchte man Unterstützung? Was ist die Gegenleistung bzw. der Mehrwert für den:die Melder:in abseits des Themas Informationsaustausch – hier herrscht Nachholbedarf.

Philipp Blauensteiner: Ich denke, die Unternehmen müssen noch klarer informiert werden, dass es die Möglichkeit der freiwilligen Meldung gibt, auch wenn man nicht unter die NIS-Richtlinie fällt. Da sollte man wahrscheinlich auch Dienstleister, die Incidence Responses anbieten, mit in die Pflicht nehmen, über diese Möglichkeit zu informieren.

Welche Herausforderungen bringt die NIS2-Richtlinie und deren Umsetzung mit sich und was erwarten Sie sich davon?

Gernot Goluch: NIS2 bringt einfach so viel mit sich, also sowohl für Betroffene als auch für die Behörde und die Computer-Notfallteams. Der legistische Prozess hat gerade begonnen und natürlich haben wir unsere Erfahrungen aus den letzten Jahren, aber es ist doch sehr schwer abzuschätzen, was da wirklich auf uns zukommt. Fix ist, dass es sehr viele Unternehmen treffen wird, die bis jetzt noch gar nicht wissen, dass sie betroffen sind oder in welchem Ausmaß. Und auch der Strafrahmen wird wesentlich ausgedehnt – auch das wird, denke ich, automatisch mehr Bewusstsein schaffen.

Philipp Blauensteiner: Es wird eine große Herausforderung für die gesamte Wirtschaft, aber ich hoffe, dass das Thema Cybersicherheit vielleicht wirklich breitflächig auch bei den mittelständischen Unternehmen ankommt.

Die neue Verordnung sieht ja zwei unterschiedliche Verfahren vor: ex ante und ex post. Somit werden die Unternehmen un-

terschiedlich mit der Richtlinie umgehen müssen. Was ist da zu erwarten?
Gernot Goluch: Es ist gut, dass diese Verordnung eine gewisse Verhältnismäßigkeit vorsieht, denn zu sagen, dass Cybersicherheitsmaßnahmen für alle gleich sind – vom Großkonzern bis zum mittelständischen Unternehmen – ist illusorisch. Und diese Verhältnismäßigkeit betrifft natürlich auch unsere behördliche Arbeit. Auch wir werden überlegen müssen, welche behördlichen Aufsichtsmaßnahmen wir in welcher Intensität wann einsetzen. Und es muss dementsprechend dann auch eine gewisse Rechtssicherheit für die betroffenen Unternehmen geben.

Die NIS2 forderte im Speziellen auch einen risikobasierten Ansatz und Zugang bei der Etablierung von Kontrollen und Maßnahmen. Inwieweit wird das Unternehmen helfen oder ist diese Materie zu komplex, dass Unternehmen den Zugang des risikobasierten Vorgehens verstehen?
Gernot Goluch: Also aus meiner Perspektive ist es sehr positiv für die Unternehmen. Wir sehen bei NIS1 jetzt schon: Der risikobasierte Ansatz ermöglicht den Unternehmen und speziell denen, die dann über die Risikobehandlung entscheiden, gewisse Grenzen zu setzen. Natürlich passiert das im Zusammenspiel mit der Behörde, aber ich glaube, da spielen die Unternehmen und wir gut zusammen. Und ich glaube, es ist sinnvoller, den Unternehmen zu sagen „beschäftigt euch mit Risiko und auf diesem Risiko basierend, setzt dann gewisse Dinge um, die im Regulativ stehen", als die exakt gleich definierte Umsetzung der Maßnahmen für alle Adressaten.
Philipp Blauensteiner: Man muss ja auch bedenken, sich mit Risiken auseinanderzusetzen, ist ja etwas, das ein Unternehmen täglich machen muss und diese Auseinandersetzung wird eben auch auf Cyberrisiken ausgedehnt und hinterfragt werden müssen, was wirklich geschützt werden muss und dann kann man auch zielgerichtet Maßnahmen treffen.

> **Sanktionen und Strafen sind die Ultima Ratio.**
>
> Philipp Blauensteiner

Zukünftig werden mehrere Tausend Unternehmen unter die NIS2-Richtlinie fallen. All diese Unternehmen müssen natürlich unterstützt und überprüft werden und am Ende des Tages macht auch der Fachkräftemangel vor Behörden keinen Halt. Wie geht man damit um?
Philipp Blauensteiner: Ein wesentlicher Punkt ist, dass wir bei der Behörde nun endlich ein IT-Gehaltsschema haben, damit wir auch für bestehende Fachkräfte von Interesse sind – sprich der Gap zwischen den öffentlichen Gehältern und den Gehältern in der Privatwirtschaft hat sich verringert. Ganz geschlossen ist die Lücke nicht, aber wir haben den Vorteil, dass wir wirklich interessante Tätigkeiten anbieten können, die man in der Privatwirtschaft nicht machen kann. Und wir werden als öffentlicher Dienst als fairer Arbeitgeber wahrgenommen, wo manche Dinge wie Väterkarenz, Weiterbildungen etc. einfacher durchzubringen sind. Und ein weiterer Vorteil ist natürlich auch, dass wir nicht den Druck haben, uns selbst oder unsere Dienste verkaufen zu müssen. Wir versuchen stark mit Junior Positionen auch junge Leute zu bekommen, die noch in Ausbildung oder gerade fertig sind, damit wir selbst Fachkräfte entwickeln können und wirklich jedem die Möglichkeit bieten, sich zu spezialisieren in Bereichen, die von Interesse sind. Für NIS1 hat das ganz gut funktioniert – für die NIS2 wird es natürlich eine weitaus größere Herausforderung werden.

Rückblickend betrachtet: Was hat sich in den letzten zehn Jahren in Sachen Cybersicherheit zum Guten verändert und wo gibt es Verbesserungen?
Philipp Blauensteiner: Also ich sehe, dass sich einiges zum Guten verändert hat eben im Hinblick darauf, dass Cybersicherheit in den meisten Unternehmen zumindest nicht mehr als optionales Add-on, das Kosten verursacht, wahrgenommen wird. Dass Cybersicherheit in der Gesellschaft angekommen ist, als etwas Wesentliches, weil ohne Cybersicherheit auch unsere Gesellschaft de facto nicht mehr funktionieren würde. Das Thema ist in der Vorstandsebene angekommen und auch der Gesetzgeber setzt sich immer mehr mit dieser Thematik auseinander. Und durch all das ist es zu einer größeren Awareness gekommen, sodass auch der:die CISO nicht mehr als verhindernd, sondern auch als unterstützend angesehen wird, weil ohne Cybersicherheit einfach nichts geht.

Wenn wir uns in einem Jahr wieder treffen, was sollten wir aus Ihrer Sicht dann erreicht haben?
Gernot Goluch: Mit der NIS-Brille betrachtet, würde ich mir wünschen, dass wir in Bezug auf NIS2 dann schon große Schritte im legistischen Prozess hinter uns gebracht haben und diese Schritte dann auch schon bis zu einem gewissen Grad kommuniziert wurden. Damit die Richtung klar ist und sich die Adressat:innen – oder zumindest ein Teil – bereits vor Inkrafttreten vorbereiten können. Es gibt einen Grund, warum die Richtlinie erlassen wurde, das heißt, ich hoffe, dass man stärker in die Awareness geht, stärker in die Vorbereitung der Unternehmen und das bedingt natürlich, dass man auch behördlicherseits, staatlicherseits einfache Spielregeln, in welche Richtung wir gehen, vorgibt und wie man diese auch kommunizieren kann.
Philipp Blauensteiner: Idealerweise haben wir in einem Jahr einen Gesetzestext zu NIS2, idealerweise wissen in einem Jahr die meisten Unternehmen, die darunter fallen werden, dass sie darunter fallen werden und idealerweise haben wir in einem Jahr schon mit dem Aufbau der Behördenstrukturen für die NIS2-Behörde begonnen und sind schon dabei, auch da wieder Fachkräfte anwerben zu können beziehungsweise auch Kolleg:innen weiterzubilden, damit am 18.10.2024 der Behördenbetrieb auch einen schönen Übergang von NIS1 zu NIS2 geschafft hat.

Wenn die Sicherheit ins Wanken gerät

Erfolgreiche Angriffe von Hacker:innen auf Gemeinden können deren wichtigen Systeme und Dienstleistungen sowie die öffentliche Infrastruktur lahmlegen. Das hat nicht nur negative Auswirkungen auf die Wirtschaft sowie auf die Sicherheit und den Alltag der Bürger:innen, sondern hat auch Potenzial, das Vertrauen in die öffentliche Verwaltung zu schwächen. Wir sprachen mit Vertreter:innen von österreichischen Gebietskörperschaften zum Thema Cybersecurity in der öffentlichen Verwaltung.

Hacker:innen greifen nicht nur Unternehmen, sondern vermehrt auch Verwaltungen an. Was macht Gebietskörperschaften zur Zielscheibe von Hacker:innen?

Elisabeth Huber: Über die Intention, Gebietskörperschaften als Zielscheibe auszuwählen, wurde unsererseits umfassend spekuliert. Ziel von Hacker:innen ist wahrscheinlich eine mögliche Medienpräsenz und natürlich Lösegeld. Die Medienpräsenz ist ihnen auch bei einem Angriff auf die öffentliche Verwaltung sicher. Beim Thema Lösegeldforderung muss man gerade aus dem Bereich der Kommunen sagen, dass die Absicht, hohe Lösegeldforderungen zu erzielen, eher utopisch ist, da Kommunen mit massiven finanziellen Problemen zu kämpfen haben und es unserer Meinung nach eher unwahrscheinlich ist, große Summen an Lösegeld zu erhalten.

Andreas Lehofer: Öffentliche Verwaltungen anzugreifen erregt viel Aufsehen. „Hacktivismus" könnte auch ein Grund sein, um fallweise politische Botschaften zu verbreiten.

Walter Leiss: Gebietskörperschaften verfügen natürlich über eine Vielzahl von IT-Systemen und Datenbanken, die über das Internet miteinander verbunden sind. Wenn diese Systeme nicht angemessen gesichert sind, können sie anfällig für Angriffe sein, bei denen Angreifer:innen versuchen, in das Netzwerk einzudringen und Daten zu stehlen oder Schäden zu verursachen. Darüber hinaus haben Gebietskörperschaften oft Zugang zu sensiblen Informationen wie personenbezogene Daten oder Finanzinformationen, die für Kriminelle von großem Wert sind. Schließlich können Hacker:innenangriffe auch politisch motiviert sein, insbesondere wenn es um Regierungen geht. In diesen Fällen kann das Ziel des Angriffs darin bestehen, politische Instabilität zu schaffen, Propaganda zu verbreiten oder die öffentliche Meinung zu beeinflussen.

Wie ist es um die IT-Sicherheit in kommunalen Behörden, Städten und Gemeinden bestellt? Wird die Gefahr von Angriffen aus dem Internet unterschätzt?

Andreas Lehofer: In der Privatwirtschaft wird möglicherweise mehr in IT-Sicherheit investiert bzw. schneller auf mögliche Bedrohungen reagiert. In der öffentlichen Verwaltung ist die Gefahr erst in den letzten Jahren „sichtbar" geworden.

Walter Leiss: Es ist bekannt, dass sich die Anzahl der Cyberangriffe auf Gebietskörperschaften in den letzten Jahren maßgeblich erhöht hat und dass diese oftmals sehr teuer für die Betroffenen sind. Grundsätzlich ist unseren Gemeinden die Gefahr, die von derartigen Angriffen ausgeht, natürlich bewusst. Insbesondere das Bekanntwerden der tatsächlichen (versuchten) Angriffe in Österreich, beispielsweise jener auf die Kärntner Landesregierung, hat das Bewusstsein jedenfalls nochmals geschärft.

Bei vielen Kommunen und öffentlichen Einrichtungen, insbesondere bei kleineren, mangelt es allerdings an den (finanziellen) Ressourcen, um umfassende Sicherheitsmaßnahmen zu implementieren und zu pflegen. Es wäre wichtig, dass allen Gebietskörperschaften die (finanziellen) Möglichkeiten bereitgestellt werden, um angemessene Sicherheitsmaßnahmen ergreifen zu können.

Elisabeth Huber: Ich kann in diesem Zusammenhang nur für die Stadtgemeinde Spittal an der Drau sprechen. Wir haben eine jahrzehntelang aufgebaute Struktur im IT-Bereich und sehr versierte Mitarbeiter:innen. Die Gefahr von Angriffen aus dem Internet haben wir nie unterschätzt. Dies hat zu einem intensiven Ausbau der IT-Sicherheit geführt. Dennoch muss man realistischerweise sagen, dass man nie davor gefeit ist, Opfer eines – erfolgreichen – Angriffs zu werden. Wie es im Leben so ist, hinkt man der Entwicklung immer hinterher.

Wie haben sich Cyberangriffe aus Ihrer Sicht in den vergangenen Jahren verändert?

Andreas Lehofer: Systeme werden besser geschützt. Hacker:innen entwickeln sich jedoch auch weiter. Angriffe werden besser vorbereitet und die Systeme tiefgehend analysiert. Zugeschlagen wird dann, wenn genügend Information vorhanden ist und größtmöglicher Schaden angerichtet werden kann, sodass Zahlungen getätigt werden. RaaS ist das neue Schlagwort. Ransomware kann als „Service" gebucht werden, die Anbieter:innen sind umsatzbeteiligt. Somit kann jede:r zur:zum Hacker:in werden bzw. ebensolche beauftragen. Mittlerweile hat sich hier ein richtiges Geschäftsmodell entwickelt. Die Frage, ob man angegriffen wird, stellt sich heute gar nicht mehr. Die Frage ist nur WANN der Angriff stattfindet oder schlimmer noch, ob bereits unbemerkt Hacker:innen im System schlummern.

Walter Leiss: Zweifellos haben sich Cyberangriffe über die letzten Jahre stark verändert und weiterentwickelt. Die immer raffinierter werdenden Angriffsmethoden und eine zunehmende Professionalisierung der Angreifer:innen haben zu einer deutlichen Zunahme von Cyberangriffen geführt. Insbesondere ist hier die Zunahme von Ransomware-Angriffen hervorzuheben. Ein weiterer Trend ist die Verbreitung von Phishing-angriffen.

Elisabeth Huber: Die Anzahl der Cyberangriffe ist stark gestiegen. Wie sich diese verändert haben, kann ich nicht beurteilen. Die mediale Zurschaustellung dieser Angriffe ist möglicherweise kontraproduktiv. Unabhängig von möglichen Lösegeldforderungen ist die mediale Präsenz sicherlich ein Motiv für derartige Handlungen.

Blicken wir noch einmal zurück auf einen Cyberangriff, den Sie erlebt haben. Wie bewerten Sie die Krisenbewältigung aus heutiger Sicht? Wie haben Sie die Krise sowohl organisatorisch als auch technisch bewältigt?

Elisabeth Huber: Wir hatten noch keinen Cyberangriff. Die „Erpresser-E-Mail" vom Oktober 2022 mit einer Lösegeldforderung hat sich als Fake herausgestellt.

Andreas Lehofer: Organisatorisch haben wir den Cyberangriff durch die interne Kommunikation mit der Stadtamtsdirektion und dem Bürgermeister, zusätzlich auch mittels Stadtkommunikation bewältigt. Die externe Kommunikation hat mit der DSB und in weiterer Folge auch mit der Polizei stattgefunden. Auf technischer Seite hat unser Back-up-Konzept funktioniert. Es kam zur Abschaltung des Gesamtsystems und dem stufenweisen Wiederhochfahren der einzelnen Server. Wir hatten einen Ausfall von ca. 2 Stunden für die Mitarbeiter:innen. Danach standen die wichtigsten Dienste wieder zur Verfügung und ab Mittag auch das Komplettsystem. Danach erfolgten Hintergrundarbeiten für die nächsten Tage und die zusätzliche Absicherung der Systeme.

Was ist aus Ihrer Sicht gut gelaufen?

Andreas Lehofer: Alles – bis auf den Angriff.

Wie lange hat die Bewältigung des Vorfalls insgesamt gedauert?

Andreas Lehofer: Der Verschlüsselungsvorfall konnte schnell abgehandelt werden. Zusätzlich wurden aber auch Daten gestohlen und die Hacker:innengruppe drohte damit, diese zu veröffentlichen. Hier waren wir dann mit dem LKA in Kontakt und haben nicht gezahlt. Es konnten jedoch nur wenige, mehrere Jahre alte Daten entwendet werden. Diese wurden dann veröffentlicht und nach ca. 1,5 Stunden über eine Abuse-Meldung an den Filehoster durch das LKA vom Netz genommen. Weitere technische Maßnahmen wurden gesetzt und werden nach wie vor gesetzt. Die technische und organisatorische Bewältigung war damit abgeschlossen. Die persönliche Bewältigung wird nie abgeschlossen sein, da seit diesem Vorfall immer die „Angst" vor einem neuen Angriff im Hinterkopf ist.

Was war besonders herausfordernd?

Andreas Lehofer: Die schnellstmögliche Reaktion auf den Vorfall, da es keine Erfahrungswerte gab, – auch nicht von anderen Gemeinden – und dass sofort Entscheidungen zu treffen waren. Im Nachhinein gesehen haben wir richtig gehandelt.

Worauf sollten sich andere Gebietskörperschaften, aber auch Unternehmen besonders vorbereiten?

Andreas Lehofer: Man kann nur versuchen, sich bestmöglich zu schützen. Noch wichtiger ist jedoch ein funktionierendes Back-up- und Recovery-Konzept.

Welche Auswirkungen haben erfolgreiche Hacker:innenangriffe auf die öffentliche IT-Infrastruktur?

Elisabeth Huber: Da muss man unterscheiden zwischen Angriffen, die Schäden und Kosten verursachen, da Daten verschlüsselt werden, und zwischen möglichen Datenleaks, die nicht unbedingt sofort auffallen, da keine Daten verschlüsselt, sondern nur abgesaugt werden, die dann irgendwo im Netz wieder auftauchen. Im ersten Fall entsteht ein massiver Arbeitsaufwand und damit verbunden hohe Kosten. Im zweiten Fall natürlich ein Imageschaden.

Andreas Lehofer: Hacker:innenangriffe auf die öffentliche Infrastruktur

Beim Thema Lösegeldforderung muss man gerade aus dem Bereich der Kommunen sagen, dass die Absicht, hohe Lösegeldforderungen zu erzielen, eher utopisch ist.

FOTO © PRIVAT

Mag. Elisabeth Huber
Stadtamtsleiterin bei der Stadtgemeinde Spittal an der Drau

Die persönliche Bewältigung wird nie abgeschlossen sein, da seit dem Cyberangriff immer die „Angst" vor einem neuen Angriff im Hinterkopf ist.

FOTO © STADT WEIZ

Andreas Lehofer
Abteilungsleiter IT,
Stadtgemeinde Weiz

können massive Auswirkung auf die Bevölkerung haben, z. B. bei der Trinkwasserversorgung oder der Versorgung von Patient:innen in Spitälern.

Walter Leiss: Ein erfolgreicher Hacker:innenangriff kann beispielsweise dazu führen, dass wichtige Systeme und Dienstleistungen einer Stadt oder einer Gemeinde, wie z. B. das öffentliche Verkehrssystem oder die Stromversorgung lahmgelegt werden. Eine Gefahr besteht auch darin, dass sensible Daten gestohlen oder beschädigt werden. Darüber hinaus kann ein erfolgreicher Angriff auch die Funktionsweise der öffentlichen Verwaltung beeinträchtigen, indem er den Betrieb von IT-Systemen und -Diensten stört oder lahmlegt. Erfolgreiche Hacker:innenangriffe auf die öffentliche IT-Infrastruktur können erhebliche Auswirkungen auf die Sicherheit, die Wirtschaft und das tägliche Leben haben, was insbesondere auch das Vertrauen der Bevölkerung in die öffentliche Verwaltung beeinträchtigen kann.

Haben sich weitere Konsequenzen für Ihre tägliche Arbeit ergeben?

Andreas Lehofer: Wir sind alle mehr sensibilisiert und investieren mehr Zeit und Ressourcen in das Thema Sicherheit.

Elisabeth Huber: Wie gesagt, den Hackerangriff im Oktober 2022 hat es nicht gegeben. Unsere Mitarbeiter:innen wurden jedoch in der Vergangenheit und natürlich speziell nach diesem Vorfall angehalten, sorgsam mit E-Mails umzugehen.

Die öffentliche Verwaltung und hier im Speziellen die Gebietskörperschaften (Gemeinden) mit ihren Versorgungseinrichtungen sind wesentlicher Teil für ein funktionierendes gesellschaftliches Zusammenleben.
NIS1 sagt zu den Ländern (und damit auch den Gemeinden):

- *„Einrichtungen der öffentlichen Verwaltung", die Einrichtungen des Bundes und jener Länder, die von der Möglichkeit gemäß § 22 Abs. 5 Gebrauch gemacht haben;*
- *Und: §22 (5) Ein Land kann durch Landesgesetz die Pflichten gemäß Abs. 1 und 2 auch in Hinblick auf die von seinen Einrichtungen erbrachten wichtigen Dienste für anwendbar erklären. Diese Einrichtungen der Länder sind die Ämter der Landesregierungen und weitere Dienststellen der Länder und Gemeinden, die gegebenenfalls von den jeweils in Betracht kommenden Organen des Landes als solche erklärt werden.*

Haben Gemeinden das NIS1-Thema schon für sich erkannt?

Elisabeth Huber: Datenschutz und IT-Sicherheit haben einen hohen Stellenwert in der Stadtgemeinde Spittal an der Drau. Wir sind uns unserer Verantwortung gegenüber den Bürger:innen bewusst und legen sehr viel Wert darauf. Der Anwendungsbereich von NIS1 ist ja äußerst klein umfasst. NIS1 bezieht sich ja mehr oder weniger auf grundlegende IT-Sicherheitsmaßnahmen, die aufgrund der aktuellen Bedrohungslage von jeder IT-Abteilung so umgesetzt werden sollten.

Mit NIS2 soll das anders werden: Wie werden Sie damit umgehen und welche Maßnahmen stehen bei Ihnen an oberster Stelle?

- *„Als gänzlich neu betroffen kommen die Bereiche Abwasser, Weltraum und die öffentliche Verwaltung (jedenfalls der Bundesdienst und die Länder, optional auch Gemeinden) hinzu."*

Elisabeth Huber: Wir gehen davon aus, dass wir vom Geltungsbereich NIS2 umfasst sein werden. Im Endeffekt werden Mindeststandards vorgegeben und es sind diese umzusetzen. Wir werden unsere Prozesse und Abläufe evaluieren und gegebenenfalls bis zum Inkrafttreten des Gesetzes so anpassen, dass wir die Anforderungen von NIS2 erfüllen werden.

Walter Leiss: Bereits jetzt muss ein Bundesland in den Anwendungsbereich optieren, damit seine Einrichtungen (zu denen auch die Gemeinden gezählt werden), den Pflichten des NIS-Gesetzes unterliegen. Dies wird auch bei NIS2 so bleiben. Folglich ergibt sich auf den ersten Blick keine direkte Veränderung, die die Gemeinden betrifft. Eine indirekte Betroffenheit ergibt sich allerdings im Bereich der Unternehmen in Anhang I und II, wo die Gemeinden mittelbar berührt sind (Fernwärme/-Kälte, Trinkwasserversorgung, Abwasserbehandlung, Abfallwirtschaft). Insgesamt sollte bei der Umsetzung der neuen Richtlinie darauf geachtet werden, dass ein zeitgemäßer Standard in Bezug auf Cybersicherheit eingehalten wird, gleichzeitig dürfen die umfassten Verwaltungseinheiten und Unternehmen aber auch nicht durch überschießende Maßnahmen in finanzieller Hinsicht überfordert werden.

Andreas Lehofer: Wir haben uns mit NIS1/2 noch nicht konkret auseinandergesetzt. Daher kann ich hierzu aktuell noch nichts sagen.

Welchen Stellenwert spielt eine Cyberversicherung bei Ihren Maßnahmen?

Walter Leiss: Eine Versicherung kann keinesfalls einen Ersatz für die entsprechenden Schutzmaßnahmen darstellen. Sollte die Kommune trotz Vorkehrungen von einem Angriff betroffen sein, können über eine Cyberversicherung zumindest die finanziellen Nachteile (reine Vermögensschäden) abgefedert werden. Auch im Bereich der Cyberversicherungen gibt es allerdings kein allumfassendes Modell, das jegliche Gefahren abdecken kann. Vielmehr kann aus unterschiedlichen Modellen gewählt werden, für welche Risiken vorgesorgt werden soll.

Andreas Lehofer: Eine Versicherung ist gut, sie kann jedoch maximal das finanzielle Risiko durch einen Cyberangriff abdecken. Vorbeugende und laufende Maßnahmen sowie Back-up-/Recovery-Konzepte sind viel wichtiger.

Elisabeth Huber: Wir haben bereits Angebote im Haus. Ein entsprechender versicherungstechnischer Schutz ist mit Kosten von rund EUR 10.000 pro Jahr verbunden.

Kennen Sie das GovCERT und wissen Sie, was die tun? Würden Sie sich an das GovCERT wenden, wenn Sie einen Vorfall haben?

Walter Leiss: GovCERT Austria ist das nationale Computer Emergency Response Team (CERT) in Österreich und unterstützt die Verwaltung bei der Sicherung und dem Schutz ihrer

IT-Systeme und Daten. Zu den Aufgaben von GovCERT Austria gehört es, Bedrohungen und Schwachstellen im IT-Bereich zu identifizieren, darauf zu reagieren und geeignete Schutzmaßnahmen zu empfehlen. GovCERT Austria bietet auch Schulungen und Beratungsdienste an und unterstützt bei der Umsetzung von Sicherheitsmaßnahmen. Darüber hinaus leistet GovCERT Austria auch Hilfe bei der Untersuchung von Sicherheitsvorfällen und koordiniert gegebenenfalls gemeinsame Maßnahmen zur Bekämpfung von Cyberkriminalität. Das Bewusstsein der Gemeinden hinsichtlich der Leistungen, die GovCERT anbietet, könnte jedenfalls noch weiter gestärkt werden.

Elisabeth Huber: Ehrlicherweise muss ich zugeben, dass wir GovCERT bis dato nicht kannten. Weder im Zusammenhang mit dem Hacker:innenangriff auf das Land Kärnten noch mit anderen öffentlichkeitswirksamen Vorfällen ist uns der Begriff untergekommen. Wir haben die Prüfung des Problems bei dem vermeintlichen Angriff im Herbst 2022 an eine externe Firma ausgelagert. Ursprünglich haben wir uns sogar an die Wirtschaftskammer gewandt, die eine Cybersecurity-Hotline anbietet. Der Service ist leider ausnahmslos nur für Mitglieder verfügbar.

Andreas Lehofer: Mittlerweile ist mir das GovCERT bekannt und ich würde mich auch an das GovCERT wenden.

Wie sehr sind Gemeinden im Bereich IT vom generellen Fachkräftemangel betroffen? Was machen sie dagegen und wie können sie im Wettbewerb um Cybersecurity-Expert:innen dennoch bestehen?

Walter Leiss: Gemeinden sind stark vom Fachkräftemangel betroffen. Dies gilt auch im IT-Bereich. Da der öffentliche Sektor nicht immer in der Lage ist, mit den Gehältern und Vorteilen der privaten Wirtschaft zu konkurrieren, kann es für öffentliche Stellen schwierig sein, qualifizierte IT-Fachkräfte zu finden und zu halten. Wichtig ist, dass sich unsere Gemeinden als attraktiver Arbeitgeber präsentieren und insgesamt attraktive Rahmenbedingungen für ihre Mitarbeiter:innen schaffen können. Leider können Gemeinden in puncto „moderne Arbeitsmodelle“ (Gleitzeit, Homeoffice, Viertagewoche) selten mit der Privatwirtschaft mithalten, da ihre Möglichkeiten rechtlich stark begrenzt sind. Eine Reform des Dienstrechts könnte maßgeblich dazu beitragen, den Gemeinden hierbei mehr Spielraum zu geben und sie für potenzielle Arbeitnehmer:innen attraktiver zu machen.

Andreas Lehofer: In der Privatwirtschaft können Fachkräfte mit (vor allem) finanziellen Mitteln abgeworben werden. Das ist im öffentlichen Sektor nicht möglich. Somit sind die Chancen, gute Arbeitskräfte zu bekommen, sehr gering. Die Arbeitsplatzsicherheit zählt in diesem Bereich nicht. Wir versuchen mit einem guten Umfeld, flexiblen Arbeitszeiten und Homeoffice-Regelungen zu punkten. Meist ist dies jedoch nicht ausreichend.

Elisabeth Huber: Gerade der Wettbewerb um Cybersecurity-Expert:innen ist für Gemeinden mit einem begrenzten Budget und stringenten rechtlichen Rahmenbedingungen sehr hart. Bis dato hatten wir mit unseren Mitarbeiter:innen sehr großes Glück. Wir müssen jedoch in die Zukunft schauen und da sind die Gemeinden wie auch das Land Kärnten, welches die Rahmenbedingungen für Dienstverhältnisse schafft, sehr stark gefordert. Man muss dazu ausführen, dass die Möglichkeiten einer Gemeinde hinsichtlich der Beschäftigung von Mitarbeiter:innen und deren Entlohnung stark von den gesetzlichen Vorgaben des Landes abhängen. Zum anderen natürlich, dass auch ohne rechtliche Vorgaben die angespannte finanzielle Situation es nicht zulassen würde, Gelder wie in der Privatwirtschaft zu bezahlen. Das macht die öffentliche Verwaltung in diesem Bereich nicht konkurrenzfähig.

Wie kann der Öffentliche Sektor bei zunehmender Digitalisierung Cybersicherheit gewährleisten?

Walter Leiss: Für mich müssen die folgenden Dinge sichergestellt sein: Sensibilisierung der Mitarbeiter:innen, eine angemessene Netzwerksicherheit und ein wirksamer Schutz vor Malware und anderen Bedrohungen, Risikomanagement und Notfallpläne, Zusammenarbeit und Austausch von Informationen zwischen den öffentlichen Stellen und eine kontinuierliche Überwachung der IT-Systeme sowie die ständige Verbesserung der IT-Sicherheit.

Andreas Lehofer: Einerseits müssen Ressourcen (HR und finanziell) zur Verfügung gestellt werden, andererseits erachte ich Sensibilisierungsmaßnahmen für sinnvoll.

Elisabeth Huber: Wie so oft ist das eine Frage des Geldes. Es müssten entsprechende Mittel im Budget zur Verfügung stehen, um die entsprechenden Tools anzuschaffen. Mitarbeiter:innenschulungen sind natürlich auch sehr wichtig.

Zum Abschluss würde ich gerne noch einen Blick in die Zukunft mit Ihnen werfen: Wenn wir uns in zwölf Monaten wieder treffen, was würden wir uns dann wünschen, heute schon getan zu haben?

Andreas Lehofer: Hoffentlich NICHTS – hoffentlich haben wir alles getan. Alles andere hätte mit einem weiteren Vorfall zu tun, den sich niemand von uns wünscht!

Elisabeth Huber: Die Beantwortung der Frage hängt von den Vorkommnissen der nächsten zwölf Monate ab. Wenn wir Opfer eines Hacker:innenangriffs werden würden, müssten wir uns die Frage stellen, ob mit einem Mehr an finanziellem und organisatorischem Aufwand der Angriff verhindert hätte werden können. Falls nichts passiert wäre, könnten wir uns gemütlich zurücklehnen und uns in einer möglicherweise trügerischen Sicherheit wähnen und froh darüber sein, nicht so viel Geld und Zeitaufwand investiert zu haben. Ähnlich dem Prinzip einer Versicherung!

Leider können Gemeinden in puncto „moderne Arbeitsmodelle“ (Gleitzeit, Homeoffice, Viertagewoche) selten mit der Privatwirtschaft mithalten, da ihre Möglichkeiten rechtlich stark begrenzt sind.

FOTO © PHILIPP MONIHART

Dr. Walter Leiss
Generalsekretär
Österreichischer Gemeindebund

Cyberangriffe – das existenzbedrohende Damoklesschwert

95 % haben sich nach einem Angriff auf die Suche nach Schwachstellen in ihren Systemen begeben

68 % haben ihre interne Krisenplanung für Cyberangriffe verbessert

50 % haben in die Anschaffung von zusätzlichen Sicherheitstools investiert

45 % investieren als Maßnahme gegen Cyberattacken in die Ausbildung der Mitarbeiter:innen

66 % zählen Fake News und/oder Rufschädigung in sozialen Netzwerken mittlerweile zum ganz normalen Tagesgeschäft

Bei **63 %** sind Angriffe auf Zulieferer- und/oder Kundensysteme normales Tagesgeschäft

12 % erlitten einen finanziellen Schaden von mehr als EUR 1 Mio. durch Cyberangriffe

Cyberkriminelle sind mit allen Wassern gewaschen. Der Schaden, den sie anrichten, ist verheerend und die Angriffe unaufhaltsam. Unternehmen bleibt keine Zeit, Luft zu holen und sich treiben zu lassen. Sie müssen auf die Welle aufspringen und Schutzmaßnahmen sowie Abwehrmethoden zu ihrem Vorteil entwickeln.

Cyberkriminelle sind klar im Vorteil: Die Chancen, sie zu erwischen, sind äußerst gering. Das bedeutet, sie haben geringe bis keine Konsequenzen zu befürchten. Außerdem reicht bereits ein erfolgreich durchgeführter Angriff, um für sie hohe Gewinne abzuwerfen. Für Unternehmen ist ein Cybervorfall auf der anderen Seite wesentlich kostenintensiver: Ressourcen für die Angriffsabwehr oder die Milderung nach einem Angriff müssen bereitgestellt werden. Ebenso können Reputationsverluste, verringertes Vertrauen der Kund:innen nach einem Angriff, betriebliche Stillstände, verschärfte Versicherungsbedingungen, Strafzahlungen und vieles mehr Unternehmen teuer zu stehen kommen.

Die Sache mit dem Geld

Das jährliche Budget für die Umsetzung und Aufrechterhaltung der Cybersecurity macht bei jeweils 19 Prozent der Befragten 3–5 bzw. 6–10 Prozent des IT-Budgets aus.

Das Cybersecurity-Budget ist in den letzten zwölf Monaten bei 75 Prozent gestiegen. Als Gründe für die Budgetveränderung geben 25 Prozent eine (Betriebs-)wirtschaftliche Notwendigkeit an. Unsere Umfrage zeigt, dass hier bei den meisten Unternehmen ein Cyberangriff mit im Spiel war. Für jedes zehnte Unternehmen waren die aktuellen kriegerischen Auseinandersetzungen auf unserem Kontinent ein Auslöser. Auch der Abschluss einer Cyberversicherung und die Erfüllung der damit verbundenen Vorgaben fungieren als Treiber für Compliance.

Als weitere Gründe für die Budgetveränderung wurden Preiserhöhungen durch Lieferanten, erhöhte Compliance-, Vertrags- und Sicherheitsanforderungen, die ISO-27001-Zertifizierung, Sicherheit im Betrieb, ein Cyberangriff im Vorjahr sowie die hohe Inflation genannt.

Auf rauer See

Cyberangriffe können zu existenzbedrohenden Schäden führen, wobei hier die Größe des Unternehmens maßgeblich ist. Entgangener Umsatz, Betriebsunterbrechung, Überstunden der Mitarbeiter:innen, Rechtsberatung, externe Dienstleistung etc. – all das kann den finanziellen Schaden und die Kosten für die Aufarbeitung gewaltig in die Höhe treiben.

Ungefähr jedes zehnte von uns befragte Unternehmen (12 Prozent) hat einen finanziellen Schaden von mehr als EUR 1 Mio. durch Cyberangriffe erlitten. Durchschnittlich liegt der Schaden in der österreichischen Wirtschaft bei EUR 1,2 MIO. In der Industrie ist er sogar noch höher. Bei jedem fünfundzwanzigsten Unternehmen (4 Prozent) lag der Schaden über EUR 500.000. Auf die Größe umgelegt zeigt sich, dass dies vor allem mittelständische und große Unternehmen betrifft. Bei knapp der Hälfte der Unternehmen lag der Schaden bei bis zu EUR 100.000. Dies betrifft vor allem kleine Unternehmen, aber auch Familienunternehmen bleiben nicht verschont.

Es ist zu befürchten, dass sich die Lage in den kommenden Jahren weiter zuspitzt und die Folgekosten von Cyberattacken um ein Vielfaches höher sein werden, als die getätigten Ausgaben für die Gewährleistung von Cybersicherheit.

> **Zeit und Ressourcen für effektive Schulung des Nicht-IT-Personals anstatt standardisierter – mehr oder weniger sinnloser – Webschulungen..**
>
> Quelle: Studienteilnehmer:in

Zusammenarbeit

Mehr als die Hälfte der befragten Unternehmen (53 Prozent) hatte bei der Bearbeitung eines Sicherheitsvorfalls Unterstützung durch einen externen Dienstleister. Allerdings war der Anteil an Retainern mit 46 Prozent hier ziemlich hoch. Dieser Umstand geht einher mit der derzeitigen Lage des Fachkräftemangels und dem Fehlen der notwendigen Skills in den Unternehmen. Gerade bei einem Sicherheitsvorfall ist rasches Reagieren gefragt sowie Durchhaltefähigkeit. Das lässt sich nur mit ausreichend Cybersicherheitspersonal bewerkstelligen.

Unternehmen haben ihre externen Dienstleister auf verschiedene Arten gefunden. Neben bestehenden Kontakten/Partnern/Verträgen wurden externe Dienstleister auch über Vergabeverfahren und durch den bestehenden Rechenzentrumsanbieter gefunden. Externe Expertise hilft vor allem, um ein gewisses Grundmaß an Objektivität zu bekommen und um blinde Flecke, die mögliche Einfallstore für Trittbrettfahrer:innen sein können, nicht zu übersehen.

Ausgeklügelte Taktiken für die Abwehr von Feinden

Welche Maßnahmen haben die Unternehmen langfristig nach einem Cyberangriff gesetzt? 95 Prozent haben sich auf die Suche nach Schwachstellen in ihren Systemen begeben. 68 Prozent haben ihre interne Krisenplanung für Cyberangriffe verbessert. Es gibt aber offensichtlich Aufholbedarf und noch großes Potenzial für Unternehmen zur Verbesserung. Den Unternehmen muss die Wichtigkeit einer internen Krisenplanung für den Fall eines Cyberangriffs bewusst werden. Denn nur, wenn jede:r im Unternehmen genau weiß, wie im Notfall zu reagieren ist, können die Schäden möglichst gering gehalten werden.

Fast jedes dritte Unternehmen (27 Prozent) erachtet es als notwendig, die Sicherheit der Lieferanten zu prüfen. Ca. jedes zehnte Unternehmen (9 Prozent) hat eine neue Cyberversicherung abgeschlossen.

50 Prozent haben in die Anschaffung von zusätzlichen Sicherheitstools investiert. Jedes zweite Unternehmen, das Opfer eines Cyberangriffs war, hat also erst nach einem Angriff zusätzliche Sicherheitstools angeschafft. Das korreliert mit dem bereits erwähnten Budgetanstieg für Cybersecurity.

45 Prozent investieren als Maßnahme gegen Cyberattacken in die Ausbildung der Mitarbeiter:innen. Daran erkennt man, dass die Security Awareness in Unternehmen zwar grundsätzlich vorhanden zu sein scheint, jedoch noch nicht die volle

Aufmerksamkeit bekommt, die sie benötigt.

Gut gepanzert?
Schildkröten haben einen Panzer entwickelt, um sich vor ihren Feinden und den vielfältigen Bedrohungen zu schützen. Genau so können Cyberversicherungen dazu beitragen, Unternehmen zu schützen und entstandene Schäden abzumildern.

Nur jedes dritte Unternehmen (33 Prozent) in unserer Befragung hat jedoch eine Cyberversicherung. Das lässt vermuten, dass sich viele Unternehmen keine Cyberversicherung leisten können. Versicherungsunternehmen achten verstärkt auf das Risikoprofil von Unternehmen, da die Schadenfälle immer kostspieliger und komplexer werden, was mit einer gewissen Zurückhaltung bei Neuabschlüssen einhergeht. Unternehmen sind daher gefordert, die strengen Anforderungen zu erfüllen, um überhaupt versichert werden zu können.

Knapp ein Viertel der Unternehmen (24 Prozent) sagt, dass keine Cyberversicherung benötigt wird. Bei EPUs sind es sogar 63 Prozent, die angeben, keine Cyberversicherung zu benötigen. Auch gibt es Fälle, in denen die bestehende Cyberversicherung gekündigt und keine neue Versicherung abgeschlossen wurde.

> **Das Geld ist da, da die Geschäftsführung sich sehr bewusst ist, was ein Versagen der Sicherheitsmaßnahmen bedeutet.**
>
> Quelle: Studienteilnehmer:in

Bedrohungsszenarien
58 Prozent erachten Ransomware/Erpressung als besondere Herausforderung im Unternehmen. Im Vorjahr waren es 50 Prozent. Data Leakage wird von 55 Prozent als eine besondere Herausforderung gesehen. Dies kann damit zusammenhängen, dass bei Data Leakage und damit einhergehend dem Abfluss von geistigem Eigentum bzw. Intellectual Property eine Vorfallsmeldung zu tätigen ist und die Unternehmen viele Vorgaben nach der DSGVO einzuhalten haben.

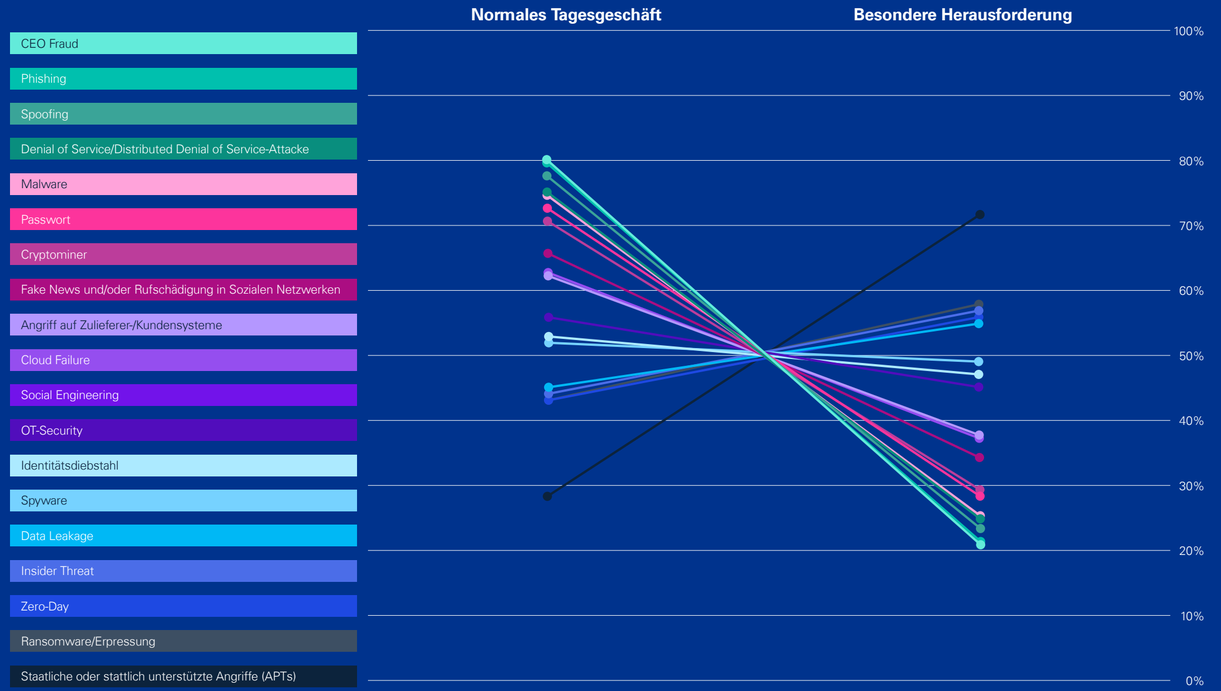
Nicht zu vergessen sind die Insider-Täter:innen: 57 Prozent stufen Insider Threats als besondere Herausforderung für das Unternehmen ein. 56 Prozent finden Zero-Day-Angriffe besonders herausfordernd.

Neben diesen für Unternehmen in besonderem Ausmaß herausfordernden Bedrohungen gibt es allerdings auch jene, die mittlerweile schon so häufig passieren, dass sie für die Unternehmen schon zum ganz normalen Tagesgeschäft geworden sind: Für zwei Drittel (66 Prozent) zählen Fake News und/oder Rufschädigung in sozialen Netzwerken beispielsweise zu solch einem Tagesgeschäft, für 80 Prozent der CEO Fraud.

Bei 63 Prozent sind Angriffe auf Zulieferer- und/oder Kundensysteme normales Tagesgeschäft. Das widerspricht der Tatsache, dass 72 Prozent der Befragten glauben, dass der:die CISO/IT-Sicherheitsverantwortliche:r die Frage, welche kritischen Daten sich bei Dritten befinden und ob sichergestellt werden kann, dass sie in der gesamten Wertschöpfungskette ausreichend geschützt sind, souverän beantworten könnte. Hier liegt eine Fehleinschätzung der Befragten vor.

Beim Thema OT-Security scheiden sich die Geister. Während 56 Prozent es als normales Tagesgeschäft

Einordnung der Bedrohungen: Zwischen normalem Tagesgeschäft und besonderer Herausforderung



sehen, ist es für 45 Prozent eine besondere Herausforderung. Das Thema der OT-Sicherheit scheint für die Befragten nicht wirklich greifbar zu sein und hat sich noch nicht durchgängig im Bewusstsein der betroffenen Unternehmen festgesetzt.

Verbesserungspotenzial

Aus den Antworten der Studienteilnehmer:innen geht hervor, dass diese nicht genügend Ressourcen wie z. B. Personal, Geld oder Zeit haben, um notwendige Sicherheitsmaßnahmen umsetzen zu können. Als Beispiele wurden in diesem Zusammenhang etwa der Wunsch nach mehr Zeit und Ressourcen für effektive Schulungen des Nicht-IT-Personals genannt. Ein weiterer Wunsch, der geäußert wurde, war die Ausweitung von ISMS/NISG auf die komplette IT ungeachtet des gegenwärtigen Scopes. Hier fehlt es laut der befragten Person an Personal und am umfassenden systemischen Bewusstsein, um das zu bewerkstelligen. Obwohl der Mangel an Personal, Zeit oder Geld zweifelsohne eine große Herausforderung für die Unternehmen darstellt, besteht hier klar Handlungsbedarf, um essenzielle Sicherheitsmaßnahmen umzusetzen.

Aber es gibt auch rundum zufriedene Stimmen, wie es eine befragte Person zum Ausdruck bringt: „Das Geld ist da, da die Geschäftsführung sich sehr bewusst ist, was ein Versagen der Sicherheitsmaßnahmen bedeutet."

> **Ausweitung von ISMS/NISG auf die komplette IT ungeachtet des gegenwärtigen Scopes.**
>
> **Es fehlt an Personal und am umfassenden systemischen Bewusstsein für diesen Kulturwandel.**
>
> Quelle: Studienteilnehmer:in

Was Sie sich aus diesem Kapitel mitnehmen sollten:

1. Der finanzielle Schaden durch Cyberangriffe beläuft sich bei rund 12 Prozent der Unternehmen auf über EUR 1 Mio.

2. Bei drei Viertel der Unternehmen ist das Budget für Cybersecurity in den letzten zwölf Monaten gestiegen. Oftmals waren Cyberangriffe ein Mitauslöser dafür.

3. Ein Großteil der Unternehmen hat die interne Krisenplanung für Cyberangriffe erst nach einem Sicherheitsvorfall verbessert. Unternehmen muss die Wichtigkeit einer internen Krisenplanung bewusst werden, um Schäden durch Angriffe möglichst gering zu halten.

Erfahren Sie mehr in unserem Podcast IMPULSE

Hinter den Kulissen

Über die unterschiedlichen Behörden und Abteilungen sowie die Zusammenarbeit sprachen wir mit Christina Schindlauer von der Direktion Staatsschutz und Nachrichtendienst (DSN).

Es gibt in Österreich unterschiedliche Behörden, die sich mit dem Thema Cyberkriminalität bzw. Cybersicherheit auseinandersetzen. Worin unterscheiden sich die Aufgabengebiete des Cyber Crime Competence Center des Bundeskriminalamts und der Direktion Staatsschutz und Nachrichtendienst sowie der Exekutive, also der Polizei?

Christina Schindlauer: Zuerst muss man ganz klar bei den Begrifflichkeiten unterscheiden, weil Cybercrime ist nicht das Gleiche wie Cybersicherheit und Cybersicherheit ist nicht gleichzusetzen mit Cyberprävention. Denn im Cybercrime-Bereich geht es natürlich in erster Linie um die Strafverfolgung der Täterschaft. Im Cybersicherheitsbereich geht es hauptsächlich um die technischen Aspekte und der Präventionsbereich zielt vor allem auf die Awareness, also die Bewusstseinsbildung, ab. Und je nach Bereich gibt es unterschiedliche Institutionen.

Der größte Unterschied ist aber einfach der fachliche Fokus und der jeweilige Zuständigkeitsbereich. Die Direktion Staatsschutz und Nachrichtendienst (DSN) ist im Cybersicherheitsbereich hauptsächlich für kritische Infrastrukturen, internationale Organisationen und verfassungsmäßige Einrichtungen zuständig. Hier gibt es einerseits unsere Ermittler:innen, die Cybercrime bzw. Cybersicherheitsvorfälle bearbeiten und andererseits den Bereich Cybersicherheit, der sich mit den technischen Aspekten eines Vorfalls auseinandersetzt und nicht direkt gegen die Täterschaft ermittelt.

Im Bundeskriminalamt bzw. dem C4 (Cyber Crime Competence Center) liegt der Fokus hauptsächlich auf Cybercrime im engeren Sinn. Also Cyberkriminalität, die gezielt gegen Netzwerke, Server, IT-Infrastrukturen gerichtet ist. Und je nach Umfang des Vorfalles ist entweder das C4 zuständig oder eine der nachgeordneten Dienststellen wie ein Landeskriminalamt oder sogar die Bezirks-IT-Ermittler:innen, die dann diese Fälle koordiniert und strukturiert bearbeiten. Hier geht es aber auch im Besonderen um digitale Forensik, nicht nur bei Cybervorfällen im klassischen Sinn, sondern auch alle möglichen Delikte mitbetrachtet, wo digitale Beweismittel relevant sind, wie z. B. Kinderpornografie.

Sie sind Leiterin der Abteilung technische Infrastruktur und Cybersicherheit? Was kann man sich unter diesem Tätigkeitsbereich vorstellen?

Christina Schindlauer: Bei uns geht es einerseits darum, den Organisationsbereichen technische Möglichkeiten zur Verfügung zu stellen und andererseits, wie der Name schon sagt, um das Thema Cybersicherheit, das ein Wesentliches für unsere ganze Gesellschaft ist. Natürlich ist jede:r Einzelne bzw. jedes Unternehmen selbst für ihre:seine Cybersicherheit verantwortlich, sprich, es gibt keine staatliche Organisation, die einem das abnimmt, aber wir versuchen einen gewissen Gesamtüberblick zu behalten, stehen mit anderen Organisationen im Bund im ständigen Austausch und versuchen, aktiv und innovativ an der Cybersicherheit Österreichs mitzuwirken.

> **Cybercrime ist nicht das gleiche wie Cybersicherheit und Cybersicherheit ist nicht gleichzusetzen mit Cyberprävention.**
>
> Christina Schindlauer

Sie sprechen davon, unsere Gesellschaft sicherer zu machen, – wie steht es aber mit dem Eigenschutz der in diesen Feldern tätigen Personen? Ist es nicht gefährlich, wenn man die Aufmerksamkeit von unterschiedlichen Gruppen auf sich zieht?

Christina Schindlauer: Man muss immer genau wissen, wo man arbeitet und was man macht. Wenn man bestimmte Tätergruppierungen verfolgt, muss man natürlich immer wissen, worauf lasse ich mich ein, welche digitalen Fußabdrücke hinterlasse ich und vor allem wie kann ich mich danach selbst schützen? Natürlich hat man hier als Mitarbeiter:in eine gewisse Sensibilität, aber das gleiche gilt natürlich auch für jede:n Einzelne:n, denn Datenschutz ist ein wesentlicher Punkt, wenn man sich im digitalen Raum bewegt – und hier ist jede:r selbst gefordert, etwas sensibler zu sein im Umgang mit ihren: seinen Daten.

Wie stehen eigentlich die Chancen, einer Tätergruppierung nach einem Vorfall auf die Spur zu kommen, besonders wenn diese vielleicht im Ausland sitzt?

Christina Schindlauer: Also die Chance, die Täterschaft auszuforschen, ist definitiv vorhanden – egal ob im Inland oder Ausland. Denn überall gibt es Gesetze und engagierte Partner. Aber es dauert. Es kommt immer darauf an, wie viele Daten bzw. Beweismittel habe ich und wie viele digitale Spuren kann ich erfassen, um möglichst nahe an die Täterschaft heranzukommen. Das bedeutet viele Daten sammeln, diese Daten möglichst genau anschauen und analysieren, um ggf. auch Fehler der Täterschaft erkennen zu können und weitere Schritte zu setzen. Gerade bei sogenannten Massendelikten – oft auch Crime-as-a-Service – gibt es oft mehrere Spuren, die verfolgt werden können bzw. müssen.

Um das alles bewerkstelligen zu können, braucht es natürlich eine extrem gute internationale Zusammenarbeit, denn oft müssen Daten auch aus dem Ausland angefordert werden. Aber natürlich bedarf es auch immer einer bestimmten Rechtsgrundlage, um an diese Daten zu gelangen und weitere Schritte einleiten zu können. Und es kommt natürlich auch immer stark auf die Art des Delikts an und welcher Strafrahmen dahintersteht, der kann natürlich je nach Land unterschiedlich ausfallen. Je geringer ein Delikt bewertet ist, desto unwahrscheinlicher ist es leider, dass man über die Staatsanwaltschaft Genehmigung für die Anforderung bzw. Auswertung der Daten erhält.

Stichwort Massendelikte: Wie kann man sich das vorstellen? Wie gehen die Tätergruppierungen hier vor? Werden da mehrere Opfer gleichzeitig attackiert?
Christina Schindlauer: Grob gesprochen ist mit Massendelikten alles gemeint, was in die Richtung betrügerische Erpressung im Internet geht – hier sind besonders Ransomware-Attacken weit verbreitet. Aber es ist nicht so, dass diese Delikte auf Knopfdruck bei vielen gleichzeitig passieren, aber einfach laufend und immer wieder – daher werden sie oft als Massendelikte bezeichnet.

Es gibt in der heimischen Wirtschaft unterschiedliche Meinungen, wenn es um die Involvierung von Behörden nach einem Cybersicherheitsvorfall geht. Was raten Sie betroffenen Unternehmen, wenn es um diese Frage geht?
Christina Schindlauer: Grundsätzlich ist es sinnvoll und wichtig, eine Meldung bzw. eine polizeiliche Anzeige zu erstatten, denn der digitale Raum darf kein rechtsfreier Raum sein. Und natürlich haben wir auch nicht die Sichtbarkeit bzw. das Bewusstsein, wenn solche Vorfälle nicht behördlich gemeldet werden. Nur wenn wir einen gesamtstaatlichen Überblick bekommen, können wir sehen, wo die Schwerpunkte der Tätergruppen liegen und welche Schritte oder Maßnahmen wo gesetzt werden müssen. Das gilt auch besonders im kriminalpolizeilichen Bereich, wo Präventivmaßnahmen gesetzt werden sollen – und das können wir schlussendlich nicht, wenn uns die Meldungen nicht vorliegen.

Ich verstehe natürlich die Sicht der Unternehmen, denn so eine Meldung bedeutet natürlich einen gewissen Aufwand, aber dann sollte eine Anzeige ein integrativer Bestandteil der Aufarbeitung eines Cybersicherheitsvorfalls sein, denn nur so können auch andere Unternehmen davon lernen und auch nur dann kann so ein Vorfall strafrechtlich verfolgt werden. Ein weiterer Punkt, warum so eine Meldung wichtig ist, ist die Beweismöglichkeit. Denn oft braucht man eine Bestätigung für die Versicherung oder das Finanzamt, wenn z. B. Daten verschlüsselt wurden und keine Back-ups vorhanden sind. Oder auch als Absicherung vor Schadensanforderungen von Dritten, denn gerade im Ransomware-Bereich kommt es ja oft zu Datenexfiltrationen und wenn diese Daten dann später irgendwo auftauchen, ist es gut, belegen zu können, dass dieser Vorfall passiert ist.

Aber auch für die Geltendmachung von Ansprüchen ist eine Anzeige erforderlich. Wenn z. B. die Täterschaft ausgeforscht wird und große Geldwerte sichergestellt werden, dann hat man als Betroffene:r natürlich die Möglichkeit, sich einer Klage anzuschließen und so einen gewissen Schadenersatz zu bekommen.

Und aus Ermittlersicht ist es natürlich immer hilfreich, wenn mehr Spuren vorhanden sind, denen man nachgehen und die man zusammenführen kann – und eine größere Anzahl an Spuren bringt natürlich größere Chancen, die Täterschaft auszuforschen, weil man dann einfach auch mehr Daten zur Verfügung hat.

Welche Möglichkeiten hat man eigentlich als Betroffener, wenn gestohlene Daten veröffentlicht werden?
Christina Schindlauer: Leider muss man sagen, dass es hier dann nicht viel Handlungsspielraum bzw. Erfolgschancen gibt, daher sollte man natürlich versuchen, schon im Vorfeld durch eine Absicherung der Systeme zu verhindern, dass Daten exfiltriert werden können, denn wenn sie einmal draußen sind, sind sie draußen und das ist eigentlich der Super-GAU für ein Unternehmen.

Aber wenn gestohlene Daten wirklich z. B. über einen Filehoster der Öffentlichkeit zugänglich gemacht werden, dann gibt es die Möglichkeit, über diesen Filehoster die Daten wieder offline nehmen zu lassen. Dafür braucht man auch weder die Behörden noch sogenannte Takedown Services, die anbieten, das zu übernehmen.

Wenn jedoch die Daten über das Tor-Netzwerk zur Verfügung gestellt werden, dann gibt es eigentlich so gut wie keine Chance, diese einfach wieder löschen zu lassen, solange die Infrastruktur der Täterschaft besteht.

Man muss aber leider auch dazu sagen, dass so eine Datenlöschung oft nicht den gewünschten Erfolg bringt. In der Regel haben diese Tätergruppen Kopien der exfiltrierten Daten, um den Druck auf das Opfer aufrecht zu halten und bspw. Lösegeld zu generieren.

Eine berechtigte Sorge von Unternehmen sind auch Trittbrettfahrer:innen. Was raten Sie hier den Unternehmen?
Christina Schindlauer: Leider sehen wir das häufig, dass nach einem Cybersicherheitsvorfall zwar die Systeme wieder bereinigt werden, damit diese wieder online gehen, aber oft nicht nach den Eintrittstüren gesucht wird. Dabei wäre das eine ganz wesentliche und wichtige Frage, die aber eben oft nicht zu-

Cybersicherheit sollte in allen Führungsebenen eine Rolle spielen, weil heutzutage einfach nichts mehr ohne digitale Unterstützung bzw. elektronisches Equipment funktioniert.


FOTO © PRIVAT

DI Christina Schindlauer
ist Abteilungsleiterin für technische Infrastruktur und Cybersicherheit in der Direktion Staatsschutz und Nachrichtendienst (DSN).

reichend beantwortet wird. Natürlich ist es teilweise auch wirklich schwierig, denn oft befindet sich die Täterschaft bereits wochen- oder monatelang im Netzwerk und es sind daher gar keine Logdaten mehr vorhanden. Und wenn ich nicht eindeutig belegen kann, wie die Täter sich Zugriff auf das Netzwerk verschafft haben, dann bleibt hier natürlich immer ein Spielraum für Trittbrettfahrer:innen. Das lässt sich nicht von der Hand weisen.

Wie ist Ihre Einschätzung in Bezug auf die Verweildauer in Systemen – mit welchem Zeitraum muss man rechnen, dass eine Täterschaft sich im System unentdeckt bewegt?
Christina Schindlauer: Das ist schwer zu beantworten, denn es kommt immer auch auf das Gegenüber an. APT-Gruppierungen z. B. haben natürlich das Ziel, sich möglichst lange unentdeckt in Systemen aufzuhalten und möglichst keine Spuren zu hinterlassen. Dann gibt es Gruppierungen, die versuchen, ihre Spuren durch Ransomware zu verwischen, und es wie einen klassischen

> **Aus Cybersicherheitssicht will man natürlich immer eine größtmögliche Transparenz.**
>
> **Man sollte daher genau vermitteln, was passiert ist – also proaktiv vorgehen, um Interpretationsspielräume so gut als möglich zu vermeiden und den Informationsstrang auch etwas lenken und kontrollieren zu können.**
>
> Christina Schindlauer

Cyberangriff aussehen lassen und daher ist es wirklich schwierig, hier valide Aussagen treffen zu können. Darum ist es wirklich sinnvoll, für die eigene Cybersicherheit zu sorgen und in diesem Bereich aber auch in IT-Sicherheit allgemein ordentlich zu investieren. Diese beiden Aspekte müssen immer getrennt betrachtet werden.

Bei der Frage nach dem Gegenüber spielt natürlich auch immer die Kommunikation eine Rolle. Wie viel soll/kann in der Öffentlichkeit preisgegeben werden?
Christina Schindlauer: Es ist ganz natürlich, dass man wissen möchte, mit wem man es zu tun hat und dieses Wissen ist auch wichtig, um eine Gesamtsicht zu bekommen und die Lage besser einschätzen zu können. Aber gerade im APT-Bereich ist es schon auch eine Frage der Cyberdiplomatie, wie man mit gewissen Fragen umgeht und vor allem, ab welchem Zeitpunkt kann man tatsächlich valide Aussagen treffen und möchte man diese auch kommunizieren. Gerade im internationalen Kontext ist es wesentlich zu definieren, wie man im Cyberraum mit anderen Ländern umgehen bzw. was man transportieren will. Vor allem was man zielgerichtete Angriffe oder Wirtschaftsspionage betrifft, denn hier stehen oft unterschiedliche Interessen im Hintergrund.

Aus Cybersicherheitssicht will man natürlich immer eine größtmögliche Transparenz. Man sollte daher genau vermitteln, was passiert ist, also proaktiv vorgehen, um Interpretationsspielräume so gut als möglich zu vermeiden und den Informationsstrang auch etwas lenken und kontrollieren zu können. Und hier geht es natürlich nicht nur um die Öffentlichkeit, sondern besonders auch um die Mitarbeiter:innen. Leider sehen wir hier oft, dass diese in der Kommunikationsspirale vergessen werden.

Warum ist Transparenz so wichtig?
Christina Schindlauer: Weil jede:r von Transparenz profitiert. Wenn man Opfer eines Cyberangriffs wurde, hat man natürlich ein Riesenproblem und muss versuchen, bestmöglich damit umzugehen. Aber andererseits profitiert man wieder davon, wenn man von ähnlichen Angriffen erfährt und weiß, was getan wurde. Gerade in Zeiten der Pandemie wurden aufgrund der notwendigen schnellen Digitalisierungsmaßnahmen oft Sicherheitsvorkehrungen gröblichst vernachlässigt und genau das können Sicherheitslücken sein, die von den Täterschaften benutzt werden. Wenn diese Informationen dann aber öffentlich sind, können andere Unternehmen davon lernen und ggf. bei ihren Systemen nachbessern, um weitere Angriffe zu vermeiden.

Viele der Digitalisierungsmaßnahmen während der Pandemie waren auch Maßnahmen aus Mangel an Alternativen. Wie lange glauben Sie, werden wir noch die Folgen dieser Digitalisierungsinitiativen in Form von Cyberangriffen spüren?
Christina Schindlauer: Also die „Low Hanging Fruits“ sind jetzt wahrscheinlich schon weitgehend gepflückt worden, aber solange wir unsere Hausübungen nicht machen, werden wir dauerhaft Probleme haben.

Wenn wir uns in 12 Monaten wieder treffen, was würden wir uns dann wünschen, heute schon getan zu haben?
Christina Schindlauer: Das Wesentliche ist, glaube ich, die Sensibilisierung. Es wäre wichtig, wenn sich Unternehmen und Organisationen mehr Zeit nehmen würden, die einzelnen Systeme genau zu prüfen, voneinander lernen und sich besser austauschen. Sicherheitslücken gibt es leider immer und überall, aber es kommt halt immer darauf an, wie gut man damit umgeht bzw. wie man die eigene IT- oder Cybersicherheit entsprechend bewerkstelligt. Und ein weiterer wichtiger Punkt ist die Ausbildung bzw. Weiterbildung, – hier müssen wir unbedingt mehr investieren und auch die Neugier fördern.

Die kritische Infrastruktur im Visier

42 % sehen die größte Herausforderung bei der Absicherung der OT-Systeme und -Prozesse in der technischen Integration veralteter OT-Technologie in moderne IT-Systeme

47 % haben sich bereits mit dem Thema NIS2 beschäftigt

19 % gaben an, dass die technische Leitung für die OT-Security zuständig ist

Bei **17 %** ist der Hersteller oder Lieferant, der die Anlage gebaut hat, für die Umsetzung der Sicherheitsmaßnahmen im Bereich der OT-Systeme/Industriesteuerungsanlagen verantwortlich

31 % sehen die nicht ausreichenden Personalressourcen, um bestehende Sicherheitsmaßnahmen umzusetzen, als größte Herausforderung

12 % finden es herausfordernd, dass die IT-Mitarbeiter:innen die OT-Betriebsanforderungen nicht verstehen

OT (Operational Technology)-Angriffe stehen deutlich stärker im Fokus der Unternehmen. Die Auswirkungen mangelnder Cybersicherheit sind enorm, nicht nur für die kritische Infrastruktur selbst, sondern auch in Bezug auf die gesamte Lieferkette eines Unternehmens.

Bei einem sind sich viele Expert:innen einig: Die Angriffe auf die kritische Infrastruktur werden immer zielgerichteter und komplexer. Es ist nur eine Frage der Zeit, bis OT-Angriffe auch erste menschliche Schäden oder Todesfolgen mit sich bringen und hier neue Dimensionen an Schäden eröffnen. Bei Ransomware-Angriffen ist uns diese Art des zielgerichteten Angriffs bereits bekannt, vor allem im Gesundheitsbereich, wenn wichtige Einrichtungen nicht mehr zur Verfügung stehen.

Klar ist, dass die OT-Sicherheit in Unternehmen einen höheren Stellenwert bekommen muss. Die Herkulesaufgabe, diese besser abzusichern, muss angegangen werden: Es ist alternativlos! Ob die Umsetzung der NIS2 hierzu etwas beitragen und sich die Sicherheitsniveaus und das Bewusstsein der Unternehmen verbessern werden, bleibt abzuwarten.

Veränderter Lebensraum

Die Schildkröte ist zwar ein Urgestein der Tierwelt, jedoch muss auch sie sich immer wieder neu an veränderte Lebensräume anpassen, um zu überleben. Genau das müssen auch Unternehmen tun und sich an die neuen Bedrohungen anpassen – sei es durch die Modernisierung ihrer OT-Technologie oder durch die Aufstockung von Personal.

Als größte Herausforderung für die Absicherung der OT-Systeme und -Prozesse nannten 42 Prozent der Befragten die technische Integration veralteter OT-Technologie in moderne IT-Systeme. 31 Prozent sehen die nicht ausreichenden Personalressourcen, um bestehende Sicherheitsmaßnahmen umzusetzen, als größte Herausforderung.

Auf einer Wellenlänge

Als weitere Herausforderungen wurden die fehlende IT-Standardisierung, das Verständnis der OT-Lieferanten sowie der Umstand, dass OT-Mitarbeiter:innen die IT-Sicherheitsanforderungen nicht verstehen, genannt. Unsere Befragung zeigt auf, dass der Mangel an Verständnis jedoch auch in die andere Richtung geht: 12 Prozent finden es herausfordernd, dass die IT-Mitarbeiter:innen die OT-Betriebsanforderungen nicht verstehen. Eine Lösung für dieses Problem muss der Abbau sprachlicher Barrieren zwischen OT- und IT-Mitarbeiter:innen sein. Darüber hinaus ist das Bewusstsein für die Sicherheit der Industriesteuerungsanlagen und Prozessautomatisierungssysteme zu steigern, denn ohne dieses können eine resiliente digitalisierte Wertschöpfungskette und die resiliente digitalisierte Fabrik kaum Realität werden.

Bei 17 Prozent der Befragten ist der Hersteller oder Lieferant, der die Anlage gebaut hat, für die Umsetzung der Sicherheitsmaßnahmen im Bereich der OT-Systeme/Industriesteuerungsanlagen verantwortlich. Das sollte zu denken geben, da man sich hier für Third Party Risks verwundbar macht. 19 Prozent gaben an, dass die technische Leitung für die OT-Security zuständig ist. Hier scheint also die OT in die IT integriert zu sein. Das wirft aber erneut das Problem der sprachlichen Barrieren zwischen OT- und IT-Mitarbeiter:innen auf. Diese müssen lernen, in dieselbe Richtung zu schwimmen, um sich gemeinsam gegen Angriffe zur Wehr zu setzen.

NIS2: Wohin geht die Reise?

Mit der NIS2 gibt es nun eine Unterscheidung zwischen Unternehmen wesentlicher und wichtiger Kategorien. Das hat zur Auswirkung, dass nun viele weitere Unternehmen davon betroffen sind. Strafzahlungen können sich dabei auf bis zu EUR 10 Mio. oder 2 Prozent des globalen Jahresumsatzes der Unternehmen belaufen.

47 Prozent der Befragten haben sich bereits mit dem Thema NIS2 beschäftigt. Die Erwartungen von NIS2 für das eigene Unternehmen gehen hier klar auseinander: Einerseits erwarten die Studienteilnehmer:innen mehr Compliance-Anforderungen und Dokumentation. Sie empfinden die Vor-

Ransomware-Gruppen machen vor niemandem halt. Sie attackieren kritische Infrastrukturen wie Krankenhäuser, Windparks zur Stromerzeugung, Supermärkte und Handelsketten, aber auch IT-Dienstleister. Die Konsequenz dabei: Wir spüren es unmittelbar und bleiben von den Folgen nicht verschont.

schrift als massive Einschränkung und erwarten auch Änderungen im IT-Umfeld. Auch ist der Wunsch nach mehr Klarheit bezüglich der Einstufung und gezielten Anforderungen für Unternehmen außerhalb der kritischen Infrastruktur vorhanden, da diese noch zu schwammig definiert seien.

Positive Stimmen erwarten mehr Sicherheit und eine Vereinfachung der Prozesse. NIS2 wird als Chance gesehen, Informationssicherheit aufgrund gesetzlicher Anforderungen weiter voranzutreiben. Sie wird als gute Orientierung für die Weiterentwicklung der Informationssicherheitsstrategie gesehen sowie dass sie zur Hebung des generellen Sicherheitsniveaus beiträgt. Es wird zwar mehr Aufwand, aber auch mehr Awareness für das Thema Cybersecurity erwartet.

Speziell beim Thema Aufwand gibt es gemischte Erwartungen seitens der Befragten: Berichtet wird hier von einem Mehr an Aufwand, das aber gerade vom Management nicht

Eine Erleichterung als Betreiber wesentlicher Dienste: Viele unserer Lieferanten müssen dann dem Regelwerk genau so wie wir Genüge tun, ohne dass wir das extra initiieren und verfolgen müssen. Das ist ein Turbo für unser Lieferantenmanagement. Weiters wird es ein Zusammenrücken der Community geben, zugleich aber eine hoffnungslose Ausdünnung des Angebots an Fachkräften und an ermächtigten Prüfstellen.

Quelle: Studienteilnehmer:in

wahrgenommen wird. Ein anderes Unternehmen hingegen, das bereits ein ISMS nach 27001 implementiert hat, schätzt den Mehraufwand als bewältigbar ein. Ein weiteres Unternehmen sieht zunächst keine direkte Auswirkung, will aber im Eigeninteresse daran arbeiten, dem Standard zu entsprechen.

Erleichterungen entlang der Lieferkette

Für Betreiber wesentlicher Dienste wird die NIS2 als Erleichterung gesehen, da sich nun ebenso die Lieferanten an das Regelwerk halten müssen, ohne dass dies seitens der Auftraggeber eigens in die Wege geleitet und kontrolliert werden muss. Auch das Zusammenrücken der Community wird prognostiziert, zugleich aber auch eine Ausdünnung des Angebots an Fachkräften und an ermächtigten Prüfstellen.

Am Meeresgrund

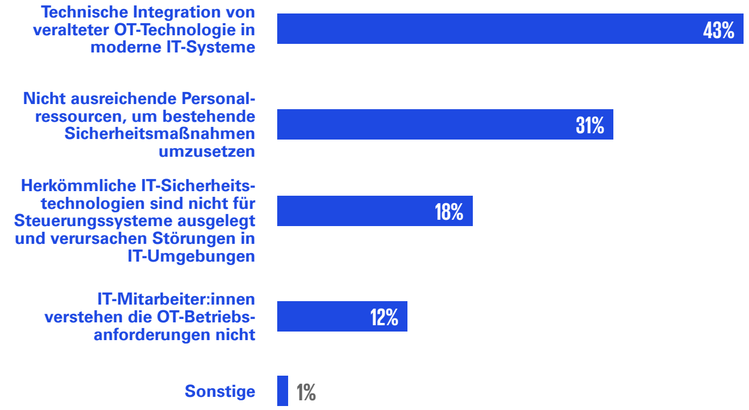
Wie man sieht, gehen die Meinungen und Argumente weit auseinander und die Befragten scheinen sich noch nicht ganz im Klaren darüber zu sein, welche Veränderungen die Umsetzung der NIS2 mit sich bringen wird. Wie es eine befragte Person zum Ausdruck bringt: „Erwarten würde man sich bessere Zusammenarbeit und mehr Transparenz in Sachen Cybervorfällen und Prävention (anonym und von Seiten der Behörde), bekommen wird man mehr Regulatoriken und eine Behörde, die eher ein Aufsichtsorgan ähnlich der Polizei sein wird, als ein Verbündeter im Cybersicherheitsumfeld."

Wir können nicht wissen, was sich wirklich am Meeresgrund befindet, bevor wir hinuntertauchen. Und so wird wohl auch erst die gelebte Praxis der NIS2 zeigen, welche Vor- oder Nachteile sich dadurch für die Unternehmen ergeben.

„Erwarten würde man sich bessere Zusammenarbeit und mehr Transparenz in Sachen Cybervorfällen und Prävention (anonym und von Seiten der Behörde), bekommen wird man mehr Regulatoriken und eine Behörde, die eher ein Aufsichtsorgan ähnlich der Polizei sein wird, als ein Verbündeter im Cybersicherheitsumfeld."

Quelle: Studienteilnehmer:in

Die größten Herausforderungen für die Absicherung von OT-Systemen und -Prozessen*



* Mehfachantworten waren möglich

> **OT-Mitarbeiter:innen verstehen die IT-Sicherheitsanforderungen nicht.**
>
> **Zugleich fehlt es an IT-Standardisierung und am Verständnis der OT-Lieferanten.**
>
> Quelle: Studienteilnehmer:in

Was Sie sich aus diesem Kapitel mitnehmen sollten:

1. Angriffe auf die kritische Infrastruktur werden immer zielgerichteter und komplexer. Unternehmen müssen ihrer OT-Sicherheit einen höheren Stellenwert beimessen.

2. Als größte Herausforderungen werden die technische Integration veralteter OT-Technologie in moderne IT-Systeme sowie Personalmangel gesehen.

3. Unabhängig davon, welche Auswirkungen NIS2 mit sich bringt, ein funktionierendes und wirksames Information Security Management System (ISMS) ist unerlässlich, um im Wettlauf mit den Angreifer:innen nicht ins Hintertreffen zu geraten.

Erfahren Sie mehr in unserem Podcast IMPULSE

Das Ziel muss Resilienz sein

Cybersecurity betrifft uns alle. Es gibt viele Institutionen und Initiativen, die sich mit dem Thema auseinandersetzen. Caroline Schmidt, Program Director im Innenministerium, gibt uns Einblicke in den Behördendschungel und die Aufgaben des BMI in puncto Cybersicherheit.

Cybersecurity ist ein umfassendes Thema, das viele Bereiche betrifft. Welche Rolle bzw. Aufgaben hat das BMI im Bereich Cybersecurity?
Caroline Schmidt: Das BMI ist in puncto Cybersicherheit in verschiedensten Bereichen gefordert. Es gibt einerseits das sogenannte C4, das Cyber Crime Competence Center im Bundeskriminalamt. Die Kolleg:innen dort sind auf Bundesebene zuständig für die Verfolgung von Cyberkriminalität, digitale Forensik und Datensicherung. Auf Landesebene sind die Landeskriminalämter für diesen Bereich zuständig. Auf Bezirksebene soll es sogenannte Bezirks-IT-Ermittler:innen – Cyber Cops – geben. Das ist eine Maßnahme, die das BMI zur österreichischen Strategie für Cybersicherheit eingemeldet hat und die wir sehr ambitioniert verfolgen.

Auf der anderen Seite gibt es das sogenannte CSC, das Cybersecurity Center, welches in der Direktion für Staatsschutz und Nachrichtendienst angesiedelt ist. Das ist die operative Koordinierungsstelle für Meldungen und Angriffe auf die Systeme und Infrastruktur verfassungsmäßiger Einrichtungen.

Und dann gibt es noch die operative NIS-Behörde im Innenministerium. Diese hat die Aufgabe der behördlichen Aufsicht und Umsetzung des NIS-Gesetzes und überwacht somit die Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und öffentliche Einrichtungen.

Und last, but not least gibt es natürlich die Direktion für digitale Services, die für unsere interne Cybersicherheit zuständig ist.
Aktuell gibt es also eine Vielzahl von Stellen, die sich mit dem Thema beschäftigen und eine aktive Rolle einnehmen. Im Regierungsprogramm ist jedoch festgehalten, dass es eine zentrale Stelle für Cybersicherheit geben soll. Ist es sinnvoll, diese Kräfte zu bündeln und eine zentrale Stelle zu haben?
Caroline Schmidt: Ich persönlich glaube, es ist ein vernünftiger Ansatz. Fakt ist, dass Cyberkriminalität ansteigt. Die geopolitischen Veränderungen der letzten Jahre stellen uns vor neue sicherheitspolitische Herausforderungen und natürlich sind wir als Staat und Gesellschaft von IKT abhängig. Hinzu kommt noch, dass nicht nur Österreich, sondern auch viele andere EU-Mitgliedstaaten sehr gefordert sind in der Umsetzung von verschiedenen EU-Vorgaben. Daher wäre es auch die Idee der Europäischen Kommission gewesen, im EU-Cybersicherheitspaket 2020, dass man die NIS2-Richtlinie und die Richtlinie zur Resilienz kritischer Einrichtungen abgestimmt aufeinander umsetzt. Weitere Rechtsakte, die derzeit umzusetzen sind, sind beispielsweise der Cybersecurity Act oder die Einrichtung eines nationalen Koordinierungszentrums, das im Bereich Cybersicherheit EU Fördergelder vergibt. All diese Themen in einem Haus zu vereinen hätte sicher große Vorteile. Ein weiterer Vorteil wäre ein verlässlicher interdisziplinärer Pool an Expert:innen und ein verlässlicher Ansprechpartner, um so das Know-how zu bündeln: Was in Anbetracht der Situation – Know-how und Expert:innen sind weltweit Mangelware – durchaus sinnvoll wäre, um das Land resilienter zu machen.

Stichwort Cyberresilienz: Seit Dezember 2022 gibt es die aktualisierte Version der Richtlinie zum Schutz der Netz- und Informationssicherheitssysteme (NIS2). Welche Auswirkungen können Unternehmen erwarten?
Caroline Schmidt: Die NIS2-Richtlinie betrifft einen weitaus größeren Adressatenkreis. Das bringt sowohl für viele Unternehmen in der Um-

Eine Steigerung des Frauenanteils um 5 Prozent in den nächsten 12 Monaten wäre wünschenswert.

FOTO © KATHARINA SCHIFFL

Mag. Caroline Schmidt M.A., MAS ist als Programmdirektorin für die Umsetzung des EU-Cybersicherheitspakets 2020 im Innenministerium tätig. Sie befasst sich mit rechtlichen und politisch-strategischen Fragen im Zusammenhang mit Cybersicherheit.

setzung, aber auch für die Behörden in der Überwachung einige Herausforderungen. Zukünftig werden große und mittlere Unternehmen aus sehr viel mehr Sektoren als bisher von der NIS2-Richtlinie betroffen sein – da geht es von Energie über Abfallwirtschaft bis hin zur Lebensmittelbranche. Diese werden dann geteilt in sogenannte wesentliche Einrichtungen und wichtige Einrichtungen, die unterschiedlich von der Behörde überwacht werden.

Die wesentlichen Einrichtungen unterliegen einer ex ante Kontrolle. Sie werden also vorab, so wie bisher von den Behörden überprüft. Die wichtigen Einrichtungen unterliegen einer ex post Kontrolle. Das bedeutet, dass die Behörde grundsätzlich jederzeit eine Überprüfung durchführen kann, in der Regel jedoch tätig wird, wenn es zu einem Vorfall kommt.

Kleine Unternehmen mit weniger als 50 Mitarbeitenden und einem max. Jahresumsatz von EUR 10.000.000 unterliegen grundsätzlich nicht der NIS2-Richtlinie. Es gibt allerdings Ausnahmen wie z. B. Anbieter von Vertrauensdiensten. Und natürlich darf man hier auch nicht auf die RKE-Richtlinie vergessen, die auf den physischen Schutz von kritischer Infrastruktur abzielt. Man muss daher die NIS2-Richtlinie immer in Zusammenhang mit der RKE-Richtlinie sehen und daher werden durchaus auch kleine Unternehmen, die als kritische Einrichtung identifiziert werden, automatisch unter die NIS2 fallen.

Und was fordert NIS2 jetzt konkret von den Unternehmen?
Caroline Schmidt: Es wird sicherlich verstärkte Anforderungen an das Risikomanagement geben. Risikoanalyse, Back-up Management, Schulungen sind alles Stichwörter. Dann wird man sich natürlich auch mehr die Lieferketten und Abhängigkeiten von Partnerunternehmen ansehen müssen.

Die Meldepflichten ändern sich: Zukünftig muss man binnen 24 Stunden eine Erstmeldung abgeben. Danach hat man drei Tage Zeit, um eine detaillierte Meldung an die NIS-Behörde abzugeben. Und bei Nichteinhaltung muss man mit Sanktionen bzw. Geldstrafen rechnen.

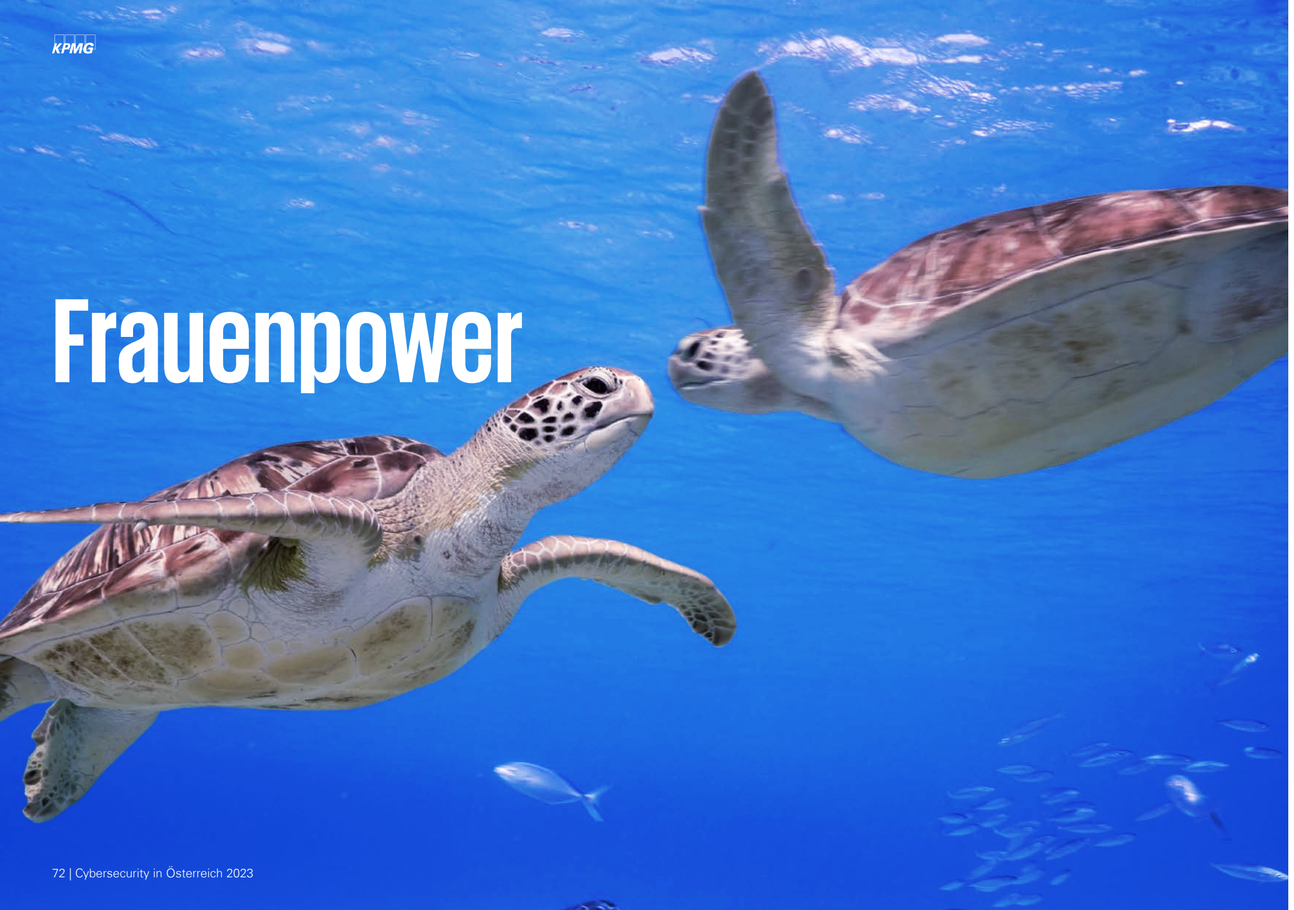
Sie waren bei den Verhandlungen der NIS2-Richtlinie auf EU-Ebene dabei. War es aus Ihrer Sicht eine Herkulesaufgabe oder ein trivialer Weg, um dorthin zu kommen, wo wir jetzt stehen?
Caroline Schmidt: Sehr gute Frage. Verhandlungen auf europäischer Ebene sind immer ein komplexes Thema. Nach dem Vorschlag der EU-Kommission im Dezember 2020 begannen die Verhandlungen im Rat, und natürlich versucht hier jeder Staat seine Interessen so gut wie möglich zu vertreten. Und nachdem die NIS2-Richtlinie schon ein besonders umfangreiches und detailliertes Regelwerk war und man natürlich auch die innerstaatlichen Settings mitberücksichtigen musste, dauerten diese Verhandlungen ungefähr ein Jahr. Nach dem Durchbruch ging es zu den sogenannten Trilog-Verhandlungen zwischen EU-Kommission, EU-Rat und EU-Parlament – diese konnten nach ungefähr sechs Monaten zu einem erfolgreichen Abschluss geführt werden. Anschließend muss der Gesetzestext jedoch noch in mehrere Sprachen übersetzt und jede einzeln abgeglichen werden. Daher dauert es dann noch ein paar Monate, bis die Richtlinie tatsächlich im Amtsblatt steht und in Kraft treten kann. Und dann folgt die nationale Umsetzung. Die Verhandlungen an sich waren eher so wie auch sonst Verhandlungen auf EU-Ebene ablaufen, aber die Umsetzung wird für die meisten Mitgliedstaaten schon eine Herkulesaufgabe werden.

Einer der Punkte, auf den die NIS2-Richtlinie besonders eingeht, ist ein transparentes Lagebild. Im Moment üben sich Unternehmen, die nicht rechtlich verpflichtet sind, noch oft in Zurückhaltung. Was muss aus Ihrer Sicht passieren, damit wir eine bessere Transparenz bekommen bzw. die Unternehmen auch motivieren, Vorfälle freiwillig zu melden?
Caroline Schmidt: Es ist sehr schade, dass die Möglichkeit der freiwilligen Meldung nicht öfters genutzt wird, denn natürlich fließen diese Meldungen in unser Lagebild mit ein und verfeinern bzw. präzisieren es. Aber freiwillig ist freiwillig und man kann niemanden zwingen. Aber es wird zukünftig auch eine andere Situation sein. Momentan fallen rund 100 Unternehmen unter die NIS-Richtlinie. Unter NIS2 werden es dann mehrere Tausend Unternehmen sein. Aber man muss das Thema in die Breite bringen und die Awareness schaffen, dass es gut ist, Cybersicherheitsvorfälle zu melden. Denn abgesehen vom Lagebild - das natürlich wichtig ist, geht es auch um bessere Möglichkeiten der Bearbeitung bzw. der Prävention. Denn mit jeder Meldung gibt es Lessons learned die anderen Unternehmen zur Verfügung gestellt werden können, um resilienter zu werden. Aber eine Meldung kann natürlich auch eine Ausbreitung verhindern – also kann mit einer Meldung verhindert werden, dass ein kleines Waldfeuer zum Waldbrand wird.

Hat es in der Vergangenheit eigentlich schon Maßnahmen und Aktionen ausgelöst, wenn eine gewisse Anzahl von Meldungen überschritten bzw. erreicht wurde?
Caroline Schmidt: Ich glaube, da muss man zwischen Meldungen und Anzeigen unterscheiden. Bei den Anzeigen ist es so, wenn eine gewisse Quantität an Anzeigen da ist – also eine kritische Masse erreicht wird –, geht das Innenministerium, vor allem unser Cyber Crime Competence Center aktiv über Social Media und über Medien raus und warnt die Bevölkerung. Bei den NIS-Unterworfenen ist natürlich auch die Quantität wichtig, aber da geht es vor allem um die Qualität der Meldungen. Da kann auch ein einziger qualitativ hochwertiger Vorfall dazu führen, dass noch andere gewarnt werden.

Wie sehen Sie das Thema Cybersicherheit als Juristin? Vor zehn Jahren bei NIS1 war das Thema für viele noch völliges Neuland. Wie hat es sich in den letzten Jahren aus Ihrer Sicht verändert?
Caroline Schmidt: Ich glaube, dass es schon viel mehr Kolleg:innen gibt, die sich für das Thema interessieren. Das Thema ist auch medial stark vertreten und natürlich auch aus rechtlicher Sicht von großem Interesse. Ich denke nicht, dass es für Jurist:innen jetzt noch völliges Neuland ist, sondern dass man viel motivierter und interessierter ist, auch weil man sieht, dass sich sehr viel entwickelt hat in den letzten Jahren. Ich bin der Ansicht, dass es aus rechtlicher Perspektive in eine gute Richtung geht.

Blick in die Zukunft: Wenn wir uns in zwölf Monaten wieder treffen und wieder über das Thema Cybersicherheit sprechen, was würden wir uns dann wünschen, heute schon getan zu haben?
Caroline Schmidt: Für mich persönlich ist es das Thema Fachkräfte bzw. Frauenanteil. Ein Bericht des WEF von 2021 zeigt auf, dass im Bereich Cybersicherheit weltweit rund 3.5 Mio. Arbeitskräfte fehlen und wir haben bisher nur einen Frauenanteil von 25 Prozent. Das ist wirklich sehr schade – eine missed chance – da meiner Meinung nach Frauen gerade in so interdisziplinären Teams sehr wichtig sind und auch wichtige Aspekte mit hineinbringen. Da frage ich mich, ob wir es uns wirklich leisten können/sollen, dass man nur ein Viertel von einem Geschlecht repräsentiert hat. Es wäre wichtig, dass wir mehr Frauen in diesen Bereich bringen. Und ich hoffe wirklich, dass sich da in den nächsten zwölf Monaten einiges tun wird – sowohl in Österreich als auch weltweit.



Frauenpower

Erfahren Sie mehr in unserem Podcast IMPULSE

Cybersicherheit wird häufig noch immer als Männerdomäne wahrgenommen. Ein guter Grund, um das Thema auch einmal aus Frauensicht zu beleuchten. Wir sprachen mit Christina Bäck, Verena Becker, Madita Führer und Constanze Roedig über ihr Verständnis von Cybersecurity, den Chancen und Herausforderungen in diesem Beruf sowie die notwendigen Entwicklungen in diesem Bereich.

Cybersecurity ist ein breit gefächertes Spektrum. Was ist das Besondere an diesem Thema?

Madita Führer: Das Spannendste ist, dass Cybersecurity nicht nur die IT-Branche betrifft, sondern eigentlich alle Branchen und alle Unternehmen unterschiedlichster Größen. Das heißt, kein Tag ist gleich und man hat es mit unterschiedlichen Anforderungen an die Informationssicherheit zu tun, je nachdem, um welches Unternehmen es geht. Außerdem mag ich, dass die Szene noch relativ klein und übersichtlich ist und daher auch extrem gut vernetzt ist und ein extrem effizienter Austausch stattfinden kann.

Christina Bäck: Für mich ist das Spannendste an diesem Bereich, dass man einen Purpose hat – also wirklich sagen kann, warum tut man etwas. Wir können dazu beitragen, dass das digitale Space, in dem wir und unsere Kinder sich täglich bewegen, zu einem sichereren Platz wird. Man kann hier in einem digitalen, innovativen Umfeld arbeiten und dabei etwas Gutes tun.

Constanze Roedig: Was ich besonders spannend finde, ist der Wissenstransfer – wie bekomme ich ein mentales Modell meines Verständnisses in die breitere Masse, um auch die Awareness zu schaffen. Und diese Verbindung von Mensch und Maschine, – denn im Cyberbereich geht es eigentlich immer um ein komplexes Konstrukt aus Menschen und Systemen – finde ich wahnsinnig faszinierend.

Verena Becker: Wie schon gesagt wurde, es geht darum, die Gesellschaft zum Positiven zu verändern. Wir haben in den letzten Jahren einen ganz starken Wandel durch die Digitalisierung durchgemacht und wir müssen versuchen, da Schritt zu halten, um auch alle Vorteile nutzen zu können. Es geht darum, nicht Opfer der eigenen Digitalisierung zu werden und daher ist Cybersecurity wirklich ein gesellschaftspolitisches Anliegen, das uns alle als Nation aber auch auf europäischer Ebene betrifft. Wir müssen an einem Strang ziehen, um unsere Gesellschaft voranzubringen.

An einem Strang ziehen bedeutet ja auch, voneinander zu lernen und Erfahrungen auszutauschen.

Was sind Ihrer Ansicht nach hier die wichtigsten Lektionen, die Sie in Ihren Jobs gelernt haben und anderen gerne mitgeben würden?
Verena Becker: Dass Cybersecurity auch für Quereinsteigerinnen sehr attraktiv ist. Wichtig ist, dass man keine Scheu hat, sich mit der Materie zu beschäftigen und bereit ist, täglich dazu zu lernen. Natürlich arbeiten in der Cybersecurity Expert:innen in hochspezialisierten technischen Bereichen, aber es ist auch ein breites Feld, wo es Wissen auf allen Ebenen braucht und Know-how aus unterschiedlichsten Bereichen, z.B. Kommunikation ein großer Vorteil ist.

Madita Führer: Da kann ich nur zustimmen. Keine Scheu haben und eine gewisse Portion Sturheit sind mit Sicherheit ein gutes Rezept, um in dieser Branche weiterzukommen. Aber in meinem Fall hat auch einfach der Zufall mitgespielt, denn vor meinem Job als Beraterin wusste ich nicht, dass es so viele verschiedene Bereiche der Cybersecurity gibt.

Christina Bäck: Wir hören oft, dass viele Kolleg:innen eher aus Zufall in diesen Bereich gekommen sind. Ich glaube, es ist ein bisschen unser Auftrag, das zu ändern, damit die Cybersecuritybranche schon frühzeitig visible wird und ein möglicher Karriereweg sein kann. Es ist wichtig, keine Angst vor Herausforderungen zu haben und auch vor Dingen, die vielleicht als nerdy abgestempelt werden, nicht zurückzuschrecken.

Constanze Roedig: Was mir auffällt, ist, dass die unterschiedlichen Berufsbilder in der Branche noch sehr unklar sind. Security Architect, Vulnerability Manager, das sind alles neue Berufe, die es noch nicht so lange gibt und daher braucht es unbedingt mehr Awareness, dass es diese spannenden Jobs gibt, die nicht einem elitären Kreis vorbehalten sind. Gebraucht wird Neugierde, Sturheit und eine gewisse Sorgfalt.

Diese unterschiedlichen Berufsbilder sind immer wieder ein Thema. Außerhalb der Community wird der Bereich Cybersicherheit immer noch sehr techniklastig gesehen.

Was müssen wir also tun, um besser darstellen zu können, wie breit dieses Thema aufgestellt ist und mehr Menschen für das Thema zu begeistern?
Verena Becker: Ich glaube, Digitalisierung spielt mittlerweile wirklich in allen Bereichen unseres Lebens eine Rolle, – sei es im privaten oder beruflichen Umfeld – es ist das neue Normal. Und Cybersecurity ist die Voraussetzung für diese Digitalisierung, der wir uns alle nicht entziehen können. Ich denke, es braucht dieses viel zitierte Storytelling, denn nur wenn ich emotional einen Zugang zu einem Thema habe, dann weckt das auch Interesse – und das fängt schon bei der Sprache in Stellenausschreibungen an. Ganz banal muss wirklich gesagt werden: Das sind die Guten, die schützen uns vor realen Gefahren aus der virtuellen Welt, die sich ganz direkt auf unseren Alltag auswirken und hier brauchen wir wirklich Menschen, die gemeinsam versuchen, hier den Feind aufzuhalten. Der emotionale Zugang ist ein ganz wichtiger Punkt, um die Menschen mitzunehmen und für das Thema zu begeistern.

Christina Bäck: Ich denke, wir müssen hier Role models in den Vordergrund stellen. Unterschiedliche Berufsgruppen, unterschiedliche Charaktere in unterschiedlichen Rollen vor den Vorhang zu holen und zu zeigen, dass es ein vielfältiges Aufgabengebiet ist, wo neben Mathematik und Programmieren noch weitere Fähigkeiten zum Tragen kommen. Im Endeffekt geht es auch im Cybersecuritybereich immer um den Umgang mit Menschen und hier sind zukünftig gerade Empathie, Einfühlungsvermögen, Kommunikation und Teamarbeit ganz besonders gefragte Skills. Und genau das müssen wir mehr nach draußen transportieren.

Constanze Roedig: In der Cybersecurity dreht es sich eigentlich auch viel darum, ein Problem erst einmal zu verstehen und darzustellen – und dazu muss man kein Hacker, Informatiker oder Developer sein. Es geht wirklich darum, ein Problem von möglichst vielen Seiten zu beleuchten, immer wieder neue Perspektiven zu finden, um das wirklich abbilden zu können. Und gerade diese Vielfalt der unterschiedlichen Zugänge ist es, die wir brauchen, um jene neue Normalität zu erschaffen, wo jede:r ihren:seinen Beitrag leisten kann.

Es geht also viel um Storytelling, aber auch um die Verlagerung des Themas in Richtung einer gesellschaftlichen oder gesellschaftspolitischen Verantwortung?
Verena Becker: Das ist genau auf den Punkt gebracht. Stichwort Fachkräftemangel: Wir haben im ganzen IT-Bereich einen enormen Mangel an qualifiziertem Personal, im Bereich Cybersecurity spitzt sich diese Problematik noch mehr zu. Wenn wir in den Unternehmen, auf Behördenseite und im Bildungsbereich keine Leute dafür haben, dann haben wir als Gesellschaft aber ein echtes Sicherheitsproblem. Aber man muss auch ganz klar sagen: Cybersecurity ist manchmal sehr unbequem und von Unternehmensseite fordert das personelle und finanzielle Ressourcen. Die Unternehmen müssen Personal abstellen und Geld in die Hand nehmen, um ihre Security zu verbessern, und da stellt sich natürlich die Frage: Wer zahlt das und wie zahlt sich diese Investition aus? Und letztendlich ist es natürlich auch eine gesellschaftspolitische Frage: Ist man bereit für ein sicheres Produkt mehr zu zahlen? Für viele Bereiche unseres Lebens z. B. Sicherheit im Straßenverkehr, stellt sich diese Frage nicht mehr, aber wir müssen erst begreifen, dass Investitionen in Cybersecurity notwendig und nicht nur ein „nice to have“ sind.

Madita Führer: Das Problem ist, dass es eine unsichtbare Gefahr ist und hier gibt es dann oft große Diskussionen, warum, weshalb, wieso, wo ist mein Return on Invest? Ich meine, jeder hat eine Haustüre, die man zusperrt, damit niemand in die Wohnung eindringen kann, wenn es aber um den Schutz der Daten geht, ist dieses Verständnis noch nicht überall in den Köpfen angekommen.

Wie bringen wir die gesellschaftliche Verantwortung und das Story-

Perfektion ist eine gefährliche Illusion. Verständnis einer realen Komplexität bringt Sicherheit.

FOTO © BTHOMASHART PHOTOGRAPHY

Dr. Constanze Roedig
leitet an der TUWien die Austrian Open Cloud Community gefördert unter der BMBWF-Ausschreibung „Digitale und soziale Transformation der Hochschule“.

De facto, wir brauchen hier einfach jede und jeden und wir können auf kein einziges Talent verzichten.

FOTO © WWW.FOTOWENINURM.AT

Mag. Verena Becker BSc
ist in der Wirtschaftskammer Österreich in der Bundessparte Information und Consulting tätig. 2022 gründete sie gemeinsam mit anderen Expertinnen das Netzwerk Women4Cyber Austria und fungiert auch als Vorsitzende.

telling in den universitären Sektor, wohl wissend, dass wir natürlich hier stark an den Fakten orientiert sind?

Constanze Roedig: Storytelling ist natürlich eine der wichtigsten Methoden, um überhaupt in das Gehirn einer anderen Person reinzukommen. Weil um etwas lernen zu können, müssen wir ein gewisses emotionales Interesse anregen. Und dementsprechend sehe ich auch hier einen ganz klaren Auftrag an die Lehre bzw. die Pädagogik, diese wichtigen narrativen oder neuen pädagogischen Methoden anzuwenden.

Stichwort Storytelling: Wir hören sehr oft über die negativen Vorfälle, aber selten über erfreuliche. Warum spricht man so wenig über Erfolge und wie schaffen wir es, diese Zurückhaltung wegzubekommen?

Christina Bäck: Fakt ist leider, niemand spricht gerne über Sicherheit oder den Schutz der „Kronjuwelen", denn sobald man darüber spricht, ist es gar nicht mehr so sicher. Aber natürlich wäre es extrem hilfreich, wenn auch über Erfolge gesprochen wird, um zu zeigen, dass man den Bedrohungen nicht machtlos ausgesetzt ist.

Verena Becker: Ich denke, es ist auch eine Frage der Fehlerkultur. Wir sehen oft, dass Unternehmen extrem zurückhaltend sind, weil sie Angst haben, dass es in der Öffentlichkeit eher negativ wahrgenommen wird, obwohl in der Realität eigentlich das Gegenteil der Fall ist. Denn Unternehmen, die einmal Opfer einer Cyberattacke waren und diese gut gemeistert haben, sind im Nachhinein viel besser aufgestellt, aber leider wird das gesellschaftlich überhaupt nicht gewürdigt. Und da braucht es einen gewissen Kulturwandel, um mehr Offenheit zu gewinnen.

Madita Führer: Es ist ein extrem schwieriges Terrain. Man muss immer gut abwägen, wie viel kann ich kommunizieren und wie viel kann ich nicht kommunizieren. Denn im schlimmsten Fall wird man dann vielleicht noch mal zum Opfer und das treibt einfach viele dazu, sich lieber zurückzuhalten. Aber ich glaube auch, dass jene Unternehmen, die betroffen waren und auch darüber gesprochen und Geld in die Hand genommen haben, sich im Endeffekt viel leichter tun.

Constanze Roedig: Ausbildung und Continuous Education sind definitiv notwendig, vor allem, um die Sprache zu ändern und auch das Bild, die Wahrnehmung zu verändern, denn wir müssen lernen, dass es auch Lob geben muss. Und zwar für diejenigen, die ihre Hausaufgaben gemacht haben und hier ist auch der Gesetzgeber gefragt. Aber es muss auch gesagt werden, dass es nie perfekt sein wird.

Regularien legen gewisse Grenzen fest, innerhalb derer wir uns bewegen dürfen. Sind diese Grenzen bei unseren Digitalisierungsbemühungen zu eng oder brauchen wir diese, um die Dynamik in etwas geordnete Bahnen lenken zu können?

Verena Becker: Meine Erfahrung ist, dass wir durch Gesetze alleine gar nichts lösen können. Natürlich braucht man ganz klare Regelungen, damit es keine Interpretationsspielräume gibt, das ist Grundvoraussetzung, aber dann muss man die Unternehmen auch dabei unterstützen, diese Vorgaben auch erfüllen zu können. Das kann durch gute Regelungen, durch Förderungen sein, durch Beratungsmaßnahmen oder durch Aufklären statt Strafen durch die Behörden. Und gerade in einem kleinen Land wie Österreich müssen wir aufpassen, dass wir die Regelungen nicht zu straff anziehen. Unser Rückgrat sind die kleinen und mittleren Unternehmen und man muss wirklich versuchen, die Brücke zu finden, damit auch diese Unternehmen durch die regulatorischen Vorgaben nicht vom Markt gedrängt werden. Denn dann besteht die Gefahr, dass wir uns wieder in eine gewisse Abhängigkeit von großen internationalen Konzernen begeben, die sich in Wahrheit unseren rechtlichen Regelungen ja dann oft entziehen.

Wir müssen von dieser Hardcore Techniksprache wegkommen und das ganze Gebiet ein bisschen sympathischer machen.

FOTO © MELANIE EICHENAUER

DI(FH) Christina Bäck
ist Head of Channel Management für Fortinet Österreich – einem der weltweit führenden Hersteller von Cybersecuritylösungen – und Mitbegründerin des Netzwerks Women4Cyber.

Wir müssen in Österreich oder Europa anfangen, uns wirklich mit eigenen Produkten und eigener Forschung besser aufzustellen und unabhängiger zu werden - das sind einfach Versäumnisse aus der Vergangenheit.

Constanze Roedig: Das kann ich nur unterschreiben. Ich denke, es scheitert hier aber oft auch an der mangelnden Gründungskultur. In Österreich ist es manchmal schon recht aufwendig, wenn man etwas gründen will und hier die Bürokratisierung etwas „zu entrümpeln", wäre sicher ein guter Anfang.

Christina Bäck: Meiner Ansicht nach liegt die Lösung nicht nur in Start-ups – mit einzelnen Projekten wird man das Problem wahrscheinlich nur minimal lösen. Dieses Thema gehört auf EU-Ebene viel weiter aufgegriffen als breit angelegtes System und mit einer langfristigen Strategie. Denn im Bereich Digitalisierung ist Europa im Vergleich zu anderen Kontinenten wirklich ein wenig ins Hintertreffen geraten.

Müssen wir also wieder stärker europäisch denken, um im Bereich der Cybersecurity eine digitale Souveränität zu erreichen?
Constanze Roedig: Meiner Meinung nach auf jeden Fall. Nehmen wir z. B. die Cloud-Branche – hier ist der US-Markt ganz stark oder auch China, aber in Europa haben wir eigentlich nichts anzubieten. Gaia X ist seit Langem wieder ein Projekt, mit dem man versucht, digitale Souveränität zu erlangen, aber das Problem ist, dass wir in Europa von der Gesetzgebung her keinen zentralen Ort haben, um Mandate oder Vergaben schnell und unkompliziert umsetzen zu können. Aber ich denke, es ist notwendig, das Wissen wieder in die Länder reinzuholen.

Verena Becker: Das stimmt grundsätzlich. Aber man muss leider auch sagen, dass es für österreichische Unternehmen ganz schwer ist, sich am Markt zu etablieren und eine Kostenstruktur zu machen oder Services anzubieten, die wettbewerbsfähig sind. Einerseits ist es natürlich eine echte Ressourcenproblematik und

Habe ich mir jemals eine Haustüre gekauft und gefragt, wo ist mein Return on Invest? Ich glaube nicht!

Madita Führer MSc
ist als Managerin bei KPMG Österreich im IT Advisory tätig und hier speziell für den Bereich Cybersecurity und im Rahmen dessen auch für das EMEA Cyber Program.

andererseits fehlt auch die staatliche Unterstützung, die es in anderen Ländern wie z. B. Israel durchaus gibt. Dort bekommen heimische Unternehmen – eben auch aus Sicherheitsgründen – viele behördliche Aufträge, was bei uns in Österreich vergaberechtlich oft sehr schwierig ist und das ist dann aber auch der Grund, warum es letztendlich nicht funktioniert.

Stichwort Fachkräfte: Was können wir tun, um Frauen und Mädchen für das Thema Cybersicherheit zu begeistern, um so auch wieder dem allgemeinen Fachkräftemangel entgegenzuwirken?
Christina Bäck: Ich denke, man muss einfach wirklich laut sein und die frauenspezifischen Vorteile dieses Bereichs hervorstreichen, von denen es wirklich viele gibt. Ein Beispiel dafür ist die perfekte Vereinbarkeit von Beruf und Familie, aber auch die Entlohnung. Wir haben in diesem Bereich überdurchschnittliche Gehälter und somit wäre dieses Berufsfeld vielleicht auch für Alleinerzieherinnen besser geeignet als die typischen Frauenberufe, um den Alltag bestreiten zu können.

Verena Becker: Da kann ich mich nur anschließen, auch wenn ich es persönlich sehr traurig finde, dass wir hier in Österreich immer noch über das Thema Kinderbetreuung reden müssen bzw. es bei uns immer noch mehr ein Frauenthema ist. Aber wir sehen häufig, dass es oft Quereinsteigerinnen nach der Karenz sind, die das Thema Cybersicherheit für sich entdecken. Man braucht einen guten, sicheren Job mit absoluter Flexibilität und aus diesem Grund ist Cybersecurity auch für Frauen mit Betreuungspflichten ein sehr spannendes Berufsfeld

Constanze Roedig: Ich finde, es ist wichtig, das Image des Berufs immer wieder hervorzuheben. Er ist kreativ, er ist flexibel, man ist nicht ortsgebunden und es geht viel um Kommunikation und Austausch – und das ist ja eigentlich auch ein eher klassisch weibliches Thema. Wenn wir es also schaffen, diese positiven Themen in den Vordergrund zu stellen, dann können wir auch mehr Mädchen und Frauen ansprechen und somit vielleicht auch dem allgemeinen Fachkräftemangel Paroli bieten.

Madita Führer: Wie schon erwähnt gibt es in der Cybersecurity viele verschiedene Berufsfelder, die aber niemand kennt und für die man keine MINT-Ausbildung braucht. Das müssen wir definitiv mehr kommunizieren. Ich denke, wir müssen in Österreich oder in Europa grundsätzlich kommunikativer werden, was das Thema angeht, da sind uns andere Länder weit voraus.

Hybride Bedrohungen

74 % finden, dass es eine verstärkte EU-weite Zusammenarbeit beim Thema Cybersicherheit benötigt

22 % finden, dass ein Cybersicherheitsvorfall einfach und ohne viel Aufwand gemeldet werden kann

72 % sehen staatliche oder staatlich unterstützte Angriffe als besondere Herausforderung

38 % wissen genau, bei welchen öffentlichen Stellen sie einen Cybersicherheitsvorfall melden können

Jedes dritte Unternehmen (**33 %**) hat Zusammenhänge zwischen dem Krieg in Europa und den Cyberangriffen auf das eigene Unternehmen festgestellt

80 % sehen CEO Fraud als normales Tagesgeschäft

Für knapp die Hälfte (**47 %**) hat sich die emotionale Bedeutung von Cybersecurity durch den russischen Angriffskrieg auf die Ukraine verändert

61 % stimmten der Aussage zu, dass es bei Angriffen aus dem Ausland nur wenig Chancen gibt, die Täter:innen zu identifizieren

Hybride Bedrohungen werden immer mehr zur Realität für heimische Unternehmen. Diese müssen wie auch unsere Schildkröte besonders zäh und anpassungsfähig sein sowie viel Ausdauer beweisen, um weite Strecken im Kampf gegen die Angreifer:innen zurücklegen zu können.

Damit zusammenhängend halten die momentanen kriegerischen Auseinandersetzungen in Europa sowie Social Engineering, aber auch Ransomware-Angriffe die heimischen Unternehmen verstärkt auf Trab.

Der Krieg vor der Haustür
Die Auswirkungen des russischen Angriffskriegs auf die Ukraine sind in Österreich täglich zu spüren – nicht nur in puncto Teuerung, sondern auch bei Cyberangriffen: Jedes dritte Unternehmen hat bereits einen Zusammenhang zwischen dem russischen Angriffskrieg auf die Ukraine und Cyberangriffen auf das eigene Unternehmen festgestellt. Neben verstärkten Angriffen auf die Unternehmen selbst können diese auch zu Kollateralschäden bei Cyberangriffen auf andere Unternehmen führen. Das Interesse der Angreifer:innen an kritischen Systemen sowie zunehmende Spionage und Angriffe auf die kritische Infrastruktur sind besorgniserregend.

Immer mehr Informationen zum Cyberkrieg Russlands, der schon lange in Vorbereitung zu sein scheint, – Stichwort: Vulkan Files – werden an die Oberfläche gespült. Eines muss uns allen dabei klar sein: Die Zeiten klischeehafter Bilder von warm in Hoodies eingepackten Hacker:innen, die im dunklen Kämmerchen (womöglich sogar im ehemaligen Kinderzimmer?) sitzen, sind längst vorbei. Es handelt sich dabei um professionelle Strukturen mit geregelten Arbeitszeiten, ähnlich einem herkömmlichen Büroalltag. Die Unterscheidung liegt ausschließlich in der kriminellen Absicht bzw. dem Motiv. Wie oft dies von staatlicher Seite in Auftrag gegeben wird, bleibt unklar. Jedoch konnten etliche groß angelegte Operationen mit gewaltigem Zerstörungspotenzial Staaten eindeutig zugewiesen werden.

Staatliche oder staatlich unterstützte Angriffe (APTs) werden auch in unserer Umfrage von 72 Prozent als besondere Herausforderung gesehen. Etwas weniger als die Hälfte der Unternehmen (47 Prozent) berichtet auch, dass sich die emotionale Bedeutung von Cybersecurity durch den russischen Angriffskrieg auf die Ukraine für sie verändert hat.

Wurden Sie schon einmal beeinflusst?
Social Engineering wird von 63 Prozent mittlerweile als normales Tagesgeschäft eingestuft. 22 Prozent der Studienteilnehmer:innen waren auch bereits mit Deepfake-Angriffen konfrontiert.

Auch Forbes sagt für 2023 einen Anstieg an Social Engineering voraus. (Staatlich unterstützte) Angreifer:innen nutzen Social Engineering als ersten Zugriffspunkt um in Systeme einzudringen, Ransomware zu verbreiten oder vertrauliche Informationen zu stehlen. In sozialen Medien verlassen sich die Menschen immer mehr auf bestimmte Indikatoren für ihr Vertrauen, wie z. B. Follower:innenanzahl, Verifizierungen

Hybride Bedrohungen zeichnen sich durch den koordinierten Einsatz verschiedener Methoden der illegitimen Einflussnahme (diplomatische, militärische, wirtschaftliche oder technologische) vonseiten staatlicher und nichtstaatlicher Akteur:innen aus, ohne dass die Schwelle eines offiziell erklärten Krieges erreicht wird.

Beispiele hierfür sind die Behinderung demokratischer Entscheidungsprozesse durch massive Desinformationskampagnen, die Nutzung sozialer Medien zur Kontrolle des politischen Narrativs oder zur Radikalisierung, Rekrutierung und Steuerung von stellvertretenden Akteur:innen.

Quelle: BMEIA

oder wie lange die Accounts schon aktiv sind. So können sie leicht Opfer von Betrug oder Cyberattacken werden.

Auffällig an unseren Ergebnissen ist auch, dass es bei jedem:r Vierten in privat genutzten sozialen Netzwerken schon zu Beeinflussungsversuchen gekommen ist. Bei jedem:r Dritten sogar wurden soziale Netzwerke, die beruflich genutzt werden, bereits angegriffen. Hier muss klar das Bewusstsein geschärft werden, dass wir auch über diese Kanäle angreifbar sind. Das Phänomen der sozialen Netzwerke und die Gefahren, die diese für Unternehmen bergen, sind keinesfalls zu unterschätzen.

Somit scheint es auch kein Zufall zu sein, dass unsere Studienteilnehmer:innen kurz vor Kriegsbeginn bzw. im weiteren Verlauf des Kriegs gezielte Angriffe gegen ihre Unternehmen und auch deren kritische Infrastruktur festgestellt haben.

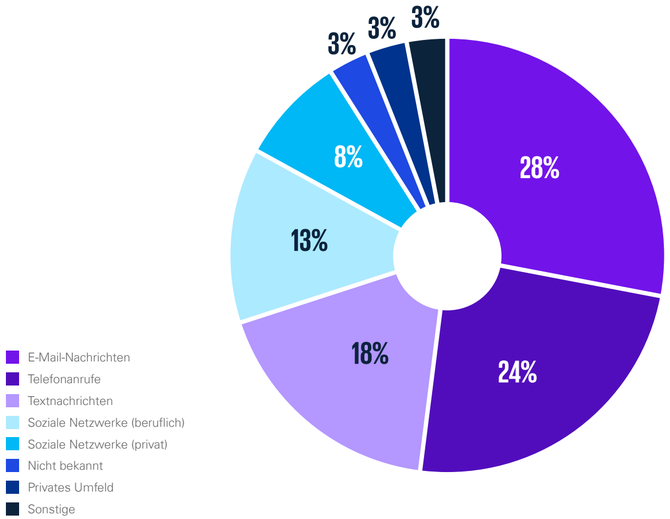
Public-private Partnership
74 Prozent der Befragten finden, dass es eine verstärkte EU-weite Zusammenarbeit beim Thema Cybersicherheit benötigt. Diese Aussage ist damit auf Platz eins der Statements, denen unsere Studienteilnehmer:innen zugestimmt haben. Hier ist die Politik gefordert, diesem Appell nachzukommen.

An zweiter Stelle mit 61 Prozent stimmten die Befragten der Aussage zu, dass es bei Angriffen aus dem Ausland nur wenig Chancen gibt, die Täter:innen zu identifizieren. Diese Aussage steht im klaren Widerspruch dazu, dass nur 28 Prozent finden, dass es eine Erweiterung der Ermittlungsbefugnisse braucht, um Cyberangriffe aufklären zu können.

Ins kalte Wasser geworfen
Nur 38 Prozent wissen genau, bei welchen öffentlichen Stellen sie einen Cybersicherheitsvorfall melden können. Damit übereinstimmend findet nur rund ein Viertel (22 Prozent) der Befragten, dass ein Cybersicherheitsvorfall einfach und ohne viel Aufwand gemeldet werden kann.

> **Im Verlauf des Krieges haben wir verstärkte Angriffe auf breiter Front gegen unser Unternehmen festgestellt.**
>
> **Die Anzahl der Phishing-E-Mails nahm dramatisch zu und es kam zu vermehrter Fake-Werbung. Social Engineering über Scam-Calls (Fake-Telefonanrufe) war an der Tagesordnung.**
>
> Quelle: Studienteilnehmer:in

In welchem Kontext gab es in den letzten zwölf Monaten Versuche der Beeinflussung?



> **Wir waren mit zunehmenden Spionage-Aktivitäten und Angriffen gegen unsere kritische Infrastruktur konfrontiert.**
>
> Quelle: Studienteilnehmer:in

> **Wir haben ca. drei Wochen vor Beginn des Krieges vermehrte Angriffe, die besonders zielgerichtet und professionell waren, von einer Konfliktpartei gegen unser Unternehmen festgestellt.**
>
> Quelle: Studienteilnehmer:in

Der zu betreibende Aufwand, um einen Cybervorfall zu melden, scheint vielen Unternehmen einfach zu hoch zu sein – auch da wir in Österreich nicht eine zentrale Stelle haben, die mit Cybersecurity betraut ist, sondern mehrere dafür zuständige Ministerien und Institutionen.

Somit ist es kaum überraschend, dass immer noch verhältnismäßig wenige Cybersicherheitsvorfälle gemeldet werden. Die Zusammenarbeit zwischen Unternehmen und öffentlichen Stellen muss im Sinne einer Public-private Partnership gestärkt werden, damit diese voneinander lernen und profitieren können.

Auf stürmischer See

Die Aufklärung und Meldung eines Cybersicherheitsvorfalls sind Themen, bei denen noch ganz klar Aufholbedarf besteht und derer sich die Politik annehmen muss. Das ist umso wichtiger, damit Unternehmen und die öffentliche Verwaltung voneinander lernen können. Gerade auch unter dem Aspekt des russischen Angriffskriegs muss allen Verantwortlichen bewusst werden, dass hier richtig viel auf dem Spiel steht und es Zeit ist, die Bedrohungen ernst zu nehmen.

Denn Unternehmen stehen auch selbst unter Zugzwang – sie müssen dringend die Wirksamkeit ihrer Sicherheitsmaßnahmen und Abwehrmöglichkeiten schärfen, um so den Vorsprung der Angreifer:innen minimieren zu können. Die Zeit zu handeln ist jetzt und die Uhr tickt.

Was Sie sich aus diesem Kapitel mitnehmen sollten:

1. Staatliche oder staatlich unterstützte Angriffe sind zur besonderen Herausforderung für österreichische Unternehmen geworden. Der Krieg in Europa hat diese weiter vorangetrieben.
2. Social Engineering ist mittlerweile zum Alltag geworden, mit Beeinflussungsversuchen sowohl in privaten als auch beruflich genutzten sozialen Netzwerken.
3. Bei der Aufklärung von Cybersicherheitsvorfällen braucht es eine stärkere Zusammenarbeit zwischen Unternehmen und öffentlichen Stellen.

Hybride Bedrohungen: Verschleierung der Wirklichkeit

Hybride Bedrohungen werden immer mehr auch für heimische Unternehmen zur Realität. Mit Oberst Georg Kunovjanek von der Theresianischen Militärakademie sprachen wir über die Risiken solcher Bedrohungen sowie über die Wichtigkeit einer militärischen Ausbildung im Bereich Cybersicherheit.

Was ist die Rolle des BMLV und im Speziellen der Theresianischen Militärakademie im Bereich der Cybersicherheit?
Georg Kunovjanek: Verfassungsrechtlich sind die Aufgaben des Bundesheeres klar umrissen und normiert. Neben der militärischen Landesverteidigung und der Assistenzleistung sind Auslandseinsätze zu nennen. Daraus lassen sich nun auch die Aufgaben des BMLV bzw. des Österreichischen Bundesheeres (ÖBH) im Bereich der Cybersicherheit ableiten. Es sind drei Szenarien denkbar. Zunächst vor allem die Aufgabe, die eigenen Systeme und Netzwerke vor Cyberangriffen zu schützen, sowohl im Inland wie auch in einem Auslandseinsatz. Sind Sicherheitsvorfälle dazu geeignet, die Souveränität Österreichs auszuschalten (auch nur teilweise) wird das ÖBH zur militärischen Landesverteidigung im Cyberraum herangezogen sein. Und schließlich kann das ÖBH auch im Rahmen der Assistenzleistung durch andere staatliche Bedarfsträger zum Einsatz gelangen. Die Militärakademie bietet mit dem Fachhochschul-Bachelorstudiengang „Militärische informations- und kommunikationstechnologische Führung" eine akademische Offiziersgrundausbildung mit einem ausgeprägten IKT-Schwerpunkt an, um die Basis für eine spätere Spezialisierung in den drei Teilbereichen elektronische Kampfführung, Informations- und Kommunikationstechnologie oder Cyber zu ermöglichen.

Seit Kurzem gibt es die Ausbildung zum IKT-Offizier. Was waren die Beweggründe und Motive, einen eigenen Studiengang zu schaffen?
Georg Kunovjanek: Die fortschreitende Digitalisierung der Streitkräfte, vor allem im Bereich der Führung und Führungsunterstützung hat einen Bedarf an spezifisch ausgebildeten Führungskräften generiert. Diese Offiziere fungieren als Übersetzer zwischen den militärischen Entscheidungsträgern bzw. Kommandanten und den technischen Leistungserbringern bzw. Providern. Der IKT-Offizier soll sich in beiden Welten – der militärischen wie der technischen Domäne gleichermaßen – zurechtfinden und deren spezifische Sprache verstehen. Er ist somit als technischer Experte das Scharnier zwischen der militärischen Führungskraft als technischem Generalisten und dem IKT-Techniker als technischem Spezialisten. Dieser steigenden Bedeutung eines Dolmetschers zwischen Bedarfsträger und Bedarfsdecker in einer zunehmenden Digitalisierung soll durch diese Ausbildung Rechnung getragen werden.

Mit welchen digitalen Fähigkeiten und Kompetenzen muss heute ein angehender Offizier ausgestattet ein?
Georg Kunovjanek: Sämtliche Tätigkeiten in Frieden und Einsatz sind von der Digitalisierung durchdrungen. Ist es die Verwaltungstätigkeit im Friedensbetrieb, die sich moderner Technik und entsprechender Applikationen bedient, so setzt sich das in der Planungs- und Führungstätigkeit weiter fort. Digitale Planungstools, auch unter Einbindung von künstlicher Intelligenz (KI), werden teilweise schon in der Ausbildung zum Einsatz gebracht und entwickeln sich in absehbarer Zeit zum Standard in der Einsatzplanung. Die Verwendung von Software Defined Radios und anderen digitalen Kommunikationsmitteln sind zum Teil schon „State of the Art" in der Einsatzdurchführung. Der Offizier muss in diesen Bereichen eine digitale Grundkompetenz entwickeln und bereit sein, sich den neuen technologischen Entwicklungen zu stellen, mehr noch diese auch nutzen zu können. Für den IKT-Offizier muss diese Grundkompetenz allerdings noch ein Stück tiefer greifen, soll er doch die anderen Offiziere in ihrer Führungsaufgabe unterstützen können.

Hybride Bedrohungen sind ein häufig diskutiertes Thema im Bereich der Sicherheitspolitik. Sind diese Bedrohungen weiterhin relevant oder hat sich die Lage durch die aktuellen geopolitischen Konflikte auch in diesem Bereich verändert?
Georg Kunovjanek: Hybride Bedrohungen haben das Ziel der „Verschlei-

> **Hybride Akteure agieren in der Regel unterhalb der Schwelle zum bewaffneten Konflikt. Da ihre Mittel nicht klassischer militärischer Natur sind, ist zwar oft das Ziel erkennbar, jedoch nicht der dahinterliegende Zweck.**

FOTO © THERESIANISCHE MILITÄRAKADEMIE

Oberst des Generalstabsdienstes **Prof. (FH) Ing. Mag. (FH) Georg Kunovjanek, MSD PhD** ist Leiter des Fachhochschul-Bachelorstudiengangs Militärische informations- und kommunikationstechnologische Führung und stellvertretender Institutsleiter des Instituts für Offiziersausbildung an der Theresianischen Militärakademie – Fachhochschule für angewandte Militärwissenschaften in Wiener Neustadt.

> **Hybride Bedrohungen haben das Ziel der Verschleierung der Wirklichkeit.**
>
> Georg Kunovjanek

erung der Wirklichkeit“ mit dem Zweck, einen Gegner in eine Situation zu manövrieren, in der er wehrlos ist. Die aktuellen Konflikte, hier vor allem die Situation zwischen den Vereinigten Staaten von Amerika und Europa auf der einen Seite und der Russischen Föderation (RF) auf der anderen Seite, sind gekennzeichnet von unterschiedlichen Maßnahmen und Aktionen hybriden Charakters. Im Gegensatz dazu ist die Situation zwischen der Ukraine und der RF hauptsächlich durch eine klassische konventionelle Konfliktaustragung charakterisiert, allerdings unter Begleitung einzelner hybrider Schritte. Hybridität war, ist und wird in Zukunft auch weiter Begleiter in der Austragung von Konflikten – unterschiedlicher Ausprägung – sein.

Was versteht man unter hybriden Akteuren genau, haben Sie Beispiele?
Georg Kunovjanek: Hybride Akteure können sehr unterschiedlich beschaffen sein. Beim Handeln dieser Akteure ist aber stets von einem übergeordneten, „staatlichen“ Zweck auszugehen. Der Einzelakteur, welcher zum Beispiel in der Cyberdomäne souveränitätsgefährdende Handlungen setzt, ist vom Akteursbegriff im hybriden Umfeld genauso umfasst wie der Einsatz von Wirtschaftsmaßnahmen (z. B. Sanktionen) durch einen Staat. Um hier nicht als Einzelmaßnahme qualifiziert zu werden, ist die Einbindung der Handlungen in eine übergeordnete Strategie eines der Wesensmerkmale hybrider Akteur:innen.

Ist ein hybrider Konflikt immer gleich als solcher erkennbar?
Georg Kunovjanek: Hybride Akteure agieren in der Regel unterhalb der Schwelle zum bewaffneten Konflikt. Da ihre Mittel nicht klassischer militärischer Natur sind, ist zwar oft das Ziel erkennbar, jedoch nicht der dahinterliegende Zweck. Ein unmittelbarer Ursache-Wirkung-Zusammenhang lässt sich sehr selten auf den ersten Blick feststellen. Oftmals ist auch nicht das Militär primärer Akteur, sondern die Konfliktaustragung erfolgt in anderen Bereichen. Ein sehr häufig auftretendes Phänomen stellt dabei etwa der viel zitierte Wirtschaftskrieg dar. Diese Komplexität, die entsteht, wenn der Ursache-Wirkung-Zusammenhang nicht offensichtlich ist, erschwert die staatliche Reaktion auf die hybriden Bedrohungen und Angriffe.

Inwieweit sind hybride Bedrohungen auch ein Thema für Unternehmen und was können Sie Unternehmen hier mitgeben?
Georg Kunovjanek: Durch eine Verflechtung aller Bereiche einer Gesellschaft sind natürlich neben staatlichen Einrichtungen auch Unternehmen von essenzieller Bedeutung für die Funktionalität der Gesellschaft und letztlich auch des gesamten Staates. Damit werden Unternehmen in einer hybriden Konfliktsituation auch zu potenziellen Angriffsvektoren der Gesellschaft. Hier ist die erste Maßnahme zur Steigerung der Resilienz, die Förderung eines Bewusstseins für die Vielfalt der Bedrohungen. Die Implementierung von technischen und prozessualen Schutzmaßnahmen ist ein weiterer Punkt. Schließlich ist die Zusammenarbeit mit staatlichen Akteuren zum Schutz der Unternehmen nicht erst nach einem Vorfall, sondern schon im Vorfeld anzustreben.

Könnte Österreich in einem Cyberkonflikt zweier anderer Staaten zwischen die Fronten geraten oder ist das nur bei konventionellen Konflikten möglich?
Georg Kunovjanek: Aufgrund der erwähnten Verflechtung und Vernetzung – im Zuge einer voranschreitenden Digitalisierung und Globalisierung – aller Bereiche einer Gesellschaft, die ja über diese hinaus geht, haben Konflikte in der Cyberdomäne das Potenzial sich auch auf Akteuren außerhalb des Konfliktes auszudehnen. So gesehen hat ein Cyberkonflikt zwischen Staaten die Möglichkeit, sich auch auf Österreich auszuwirken.

Welche Rolle spielt die Diplomatie in aktuellen Cyberkonflikten? Welche Rolle sollte sie spielen?
Georg Kunovjanek: Diplomatie ist vor allem in der Phase der Ursachenforschung von großer Bedeutung. Es gilt auf den diplomatischen Kanälen abzuklären, wer denn nun die Akteure im Konflikt sind. Dies hat begleitend zu den anderen Bemühungen eines Staates zur Aufklärung des Konfliktes zu erfolgen. Auch in der Phase der Reaktion auf einen Cyberkonflikt spielt die Diplomatie eine unterstützende Rolle. Die die Reaktion begleitende Kommunikation ist hier beispielhaft zu nennen. Diese wird auf unterschiedlichen Ebenen durchzuführen sein. Von der verdeckten, der Öffentlichkeit verborgenen Ebene bis hin zum offenen diplomatischen Dialog in verschiedenen Organisationen und Gremien. Zusammenfassend ist die Rolle der Diplomatie in aktuellen Cyberkonflikten als sehr hoch einzustufen.

Welche Lektionen hat Ihre Organisation gelernt, die für heimische Unternehmen relevant sein könnten? Gibt es spezielle Ratschläge für Unternehmen, die international tätig sind?
Georg Kunovjanek: Die Einhaltung der Schutzziele – Vertraulichkeit, Verfügbarkeit und Integrität – sind im militärischen wie auch im zivilen Umfeld essenziell. Um diese zu gewährleisten, ist ein aktuelles Lagebild in der Cyberdomäne notwendig. Vor allem in Hinblick auf die Faktoren Kraft, Raum und Zeit spielt die Information eine wesentliche Rolle. Um Wirkung im Cyberraum zu erzielen, sind nur wenige Spezialisten nötig. Die Faktoren Raum und Zeit sind durch die globale Vernetzung zusehends geschrumpft. Somit ist die Information über die konkrete Lage in der Cyberdomäne der Faktor, welcher für Handlungen im Cyberraum Voraussetzung ist. Der Erstellung eines Lagebildes für die relevanten Systeme eines Unternehmens ist ein Schlüssel zur Erreichung der Schutzziele.

Worin sehen Sie im Bereich der Ausbildung von Experten Handlungsbedarf und wie sollte die Ausbildung in Zukunft aussehen?
Georg Kunovjanek: Grundsätzlich sollte eine digitale Grundkompetenz vermittelt werden. Hier geht es aber nicht ausschließlich um die Handhabung digitaler Geräte, sondern vielmehr darum, was man mit diesen bewirkt bzw. bewirken kann. Um dies zu ermöglichen, braucht es Experten, die sowohl die Sichtweise der Techniker als auch die der User kennen und die Bedürfnisse für beide Seiten gesichert sicherstellen. Es braucht Menschen, welche in der Lage sind, den Bedarf der User so für den Techniker aufzubereiten. Es soll dabei nicht „nur“ das technisch Machbare realisiert, sondern dies auf den:die Anwender:in abgestimmt werden. Umgekehrt haben diese Experten auch die Aufgabe, die technischen Möglichkeiten an die User zu kommunizieren. Dies ist umso mehr notwendig, als die technischen Funktionsweisen moderner Geräte immer mehr in den Hintergrund treten und sich für Anwender nicht mehr vollends erschließen.

05

Jagd auf die Expert:innen

60% geben an, dass es in den letzten zwölf Monaten nicht leichter war, IT-Expert:innen zu rekrutieren

43% suchen durchschnittlich 4–6 Monate

10% beschäftigen mehr als 20 Mitarbeiter:innen für Cybersecurity

45% rekrutieren ausschließlich in Österreich

21% fällt es leichter, im europäischen Ausland zu rekrutieren

47% haben keine Frauen im Bereich Cybersecurity

Ca. jedes 10. Unternehmen (**12%**) lässt Mitarbeiter:innen im Ausland im Homeoffice arbeiten

Der durchschnittliche Frauenanteil in einem Cybersecurity Team beträgt **13%**

Das Rekrutieren sowie Halten von Cyberfachkräften bleibt auch 2023 laut WEF eine Herausforderung. Sowohl die Unternehmensleitung als auch Vorgesetzte im Cyberbereich berichten im Vergleich zum Vorjahr vermehrt über kritische Lücken bei ihren Fachkräften. Dieser Anstieg im Vergleich zu 2022 lässt sich aber laut WEF eher auf das gesteigerte Bewusstsein gegenüber der Thematik anstatt auf eine Verschlechterung der Fachkräfte-Situation zurückführen.[1]

Die Situation des Fachkräftemangels ist auch in Österreich im Vergleich zum Vorjahr nicht besser geworden. Wir laufen Gefahr, von einem Fachkräftemangel hin zu einem Arbeitskräftemangel zu kommen. Die momentan schwierige Situation zeigt auch unsere Umfrage: 60 Prozent der Befragten hatten in den letzten zwölf Monaten große Herausforderungen bei der Rekrutierung von IT-Expert:innen.

43 Prozent der von uns befragten Unternehmen benötigen durchschnittlich 4–6 Monate, um IT-Expert:innen einzustellen. Bei unserer Umfrage 2022 waren es ebenfalls 43 Prozent – die Situation bleibt also weiterhin sehr angespannt. Jedes vierte Unternehmen (28 Prozent) gibt sogar an, zwischen 7 und 12 Monaten zu benötigen. Die Unternehmen stehen hier vor der großen Herausforderung, ausreichend Fachkräfte für die Bewältigung der bestehenden und neuen Bedrohungen zu bekommen.

Leer gefischt? – Der Arbeitsmarkt im Umbruch

Bereits ein Drittel (35 Prozent) der von uns befragten Unternehmen hat einen Incident Response Retainer-Vertrag abgeschlossen. Hier sichern sich Unternehmen externe Unterstützung im Falle eines Cyberangriffs bzw. -vorfalls, um im Ernstfall rasch reagieren zu können. Auch das zeigt, wie präsent der Fachkräftemangel für die Unternehmen ist: Nicht jedes Unternehmen ist in der Lage, diese Cybersecurityexpertise im eigenen Haus aufzubauen oder vorzuhalten. Deshalb wird externe Unterstützung in Form von Retainern benötigt – ein Thema, dem wir in Zukunft noch mehr Aufmerksamkeit schenken müssen. Aber Achtung, auch die Qualität und der Umfang der Unterstützungsleistungen sind dabei wichtige Auswahlkriterien.

Unsere Umfrage lässt auch eine deutliche Verschiebung und Öffnung des Arbeitsmarktes über die Grenzen Österreichs hinweg erkennen: Weniger als die Hälfte (45 Prozent) rekrutieren ihre IT-Expert:innen ausschließlich in Österreich. 21 Prozent sagen sogar, dass es leichter ist, IT-Expert:innen im europäischen Ausland anzuwerben. Rund jedes zehnte Unternehmen (12 Prozent) gibt an, dass IT-Expert:innen im Ausland im Homeoffice arbeiten dürfen. Diese Situation zeigt deutlich: Das Becken ist leer. Wir verdrängen uns selbst. Unternehmen begeben sich zunehmend auf die Suche nach alternativen Möglichkeiten und neuen Modellen, um als Arbeitgeber attraktiver zu wirken und so dem Fachkräftemangel entgegenzuwirken.

Die Jagd hat begonnen

32 Prozent der Befragten werben aktiv Expert:innen von anderen Unternehmen ab. Im Jahr 2022 waren es 40 Prozent. Wenngleich ein leichter Rückgang zu verzeichnen ist, bleibt die Situation auf diesem Gebiet weiterhin angespannt.

Momentan betreiben Unternehmen einen Wettlauf auf die Expert:innen, indem sie der gleichen kleinen Gruppe immer mehr Gehalt anbieten. Das verschlimmert allerdings die Situation noch weiter, da eine hohe Fluktuation von Expert:innen erzeugt wird, die von Unternehmen zu Unternehmen wechseln.

An die Oberfläche kommen

Schaut man sich allerdings den Ist-Stand österreichischer IT-Abteilungen an, lässt sich die leicht positive Entwicklung erkennen, dass die Unternehmen es im Vergleich zum Vorjahr geschafft haben, mehr Mitarbeitende zu finden und zu halten. Das gibt ihnen auch die Gelegenheit, zwischenzeitlich aufzutauchen und Luft zu holen.

> **IT und Security werden viel zu sehr als Technikdisziplinen dargestellt, die MINT-Einordnung schadet und schreckt viele ab.**
>
> Quelle: Studienteilnehmer:in

Knapp ein Drittel der Unternehmen (31 Prozent) beschäftigt zwar nur 1–2 Mitarbeiter:innen in der IT-Abteilung. Im Vergleich zum letzten Jahr waren es aber noch 39 Prozent. Die Entwicklung zum Vorjahr zeigt, dass die Unternehmen ihre IT-Abteilungen aufstocken: 29 Prozent haben bereits 3–5 Mitarbeiter:innen für Cybersecurity. 2022 waren es erst 24 Prozent.

8 Prozent der befragten Unternehmen beschäftigen sogar mehr als 50 Mitarbeiter:innen für Cybersecurity. Dies lässt vorsichtig darauf schließen, dass die Wichtigkeit des Themas immer mehr bei den Unternehmen ankommt. Jedes zehnte Unternehmen (10 Prozent) hat mehr als 20 Mitarbeiter:innen. Heraus stechen hier besonders große Unternehmen sowie Unternehmen der kritischen Infrastruktur. Aber auch der Mittelstand ist auf der Überholspur.

Luft nach oben

Beim Frauenanteil in der IT ist allerdings immer noch viel Luft nach oben, was auch unsere Umfrage bestätigt: Denn fast jedes zweite Unternehmen (47 Prozent) gibt an, dass überhaupt keine Frauen im Bereich Cybersecurity zu finden sind. Etwa jedes vierte Unternehmen (27 Prozent) verzeichnet aber 1–20 Prozent Frauenanteil. Diese Tendenz stimmt positiv, dass es hier langsam in die richtige Richtung geht.

Weit mehr als Technik

Die Gründe für den immer noch vorherrschenden niedrigen Frauenanteil dürfen nicht nur eindimensional betrachtet werden, sondern sind multidimensional zu sehen: Einerseits ist die Ausbildung in Österreich für Mädchen zu wenig auf die MINT-Fächer (Mathematik, Informatik, Naturwissenschaft, Technik) fokussiert. Andererseits kann die Zuordnung zu einem MINT-Fach aber auch für viele abschreckend sein. Aus unserer Befragung geht der Appell hervor, die Disziplinen IT und Security nicht nur als reine Technikdisziplinen darzustellen. Die Vielfalt des Berufsfeldes muss stärker in den Fokus gerückt werden: Cybersicherheit hat viele Facetten und ist ein Betätigungsfeld für zahlreiche unterschiedliche Berufsgruppen und Expert:innen. Es braucht neben technischen Expert:innen auch Expert:innen für Kommunikation, Prozessautomatisie-

[1] World Economic Forum: Global Cybersecurity Outlook 2023, S. 23.

rung bei Steuerungsanlagen, Marketing, Training, sowie Psycholog:innen – um nur einige zu nennen.

Geheimnisvoller Ozean

Ein weiterer Punkt, der von unseren Studienteilnehmer:innen angesprochen wird, ist die niedrige Bewerber:innenzahl für IT-Berufe. Gründe hierfür können die bereits genannten Schwächen in der Gestaltung der Ausbildung sein. Generell ist noch zu wenig darüber bekannt, welche Aufgabenfelder abseits der technikastigen Aspekte in diesem Berufszweig existieren.

Laut den qualitativen Rückmeldungen der Studienteilnehmer:innen fehlt vielen das Bewusstsein dafür, dass sich die Fähigkeiten und Ausbildungen im Bereich Cybersecurity nicht allein auf Computerwissenschaften und Technik beschränken. Benötigt werden auch Soft Skills, die durchaus auch aus den Bereichen Wirtschaft, Recht, Psychologie, Soziologie, Kommunikation und Medienwissenschaften kommen können.

Die faszinierende Welt der IT

Geht man einen Moment weg von den möglichen Ursachen, warum sich Frauen nicht aktiv auf IT-Positionen bewerben, und wendet sich der Frage zu, was Unternehmen tun können, um mehr Frauen ins Boot zu holen, stößt man auf ein Problem, dem Arbeitgeber:innen schon mit kleinen Anpassungen entgegenwirken können: die Formulierungen in Jobannoncen. Diese müssen so gestaltet sein, dass es Unternehmen schaffen, auch Frauen damit anzusprechen und für sich zu gewinnen. Laut den Stimmen aus unserer Befragung braucht es mehr Wertschätzung von Frauen in diesen Berufsfeldern, bessere/flexiblere Arbeitszeitmodelle sowie attraktivere Rahmenbedingungen wie Bezahlung, Möglichkeiten der Kinderbetreuung etc.

Generell scheint noch Aufholbedarf in der Kommunikation und Repräsentation gegeben zu sein: IT-Berufen eilt oftmals der Ruf als Männerdomäne voraus, welcher die Arbeit in diesem Feld für manche Frauen unattraktiv macht.

> **Es braucht mehr Informationen darüber, wie breit das Aufgabengebiet der IT- und Informationssicherheit ist und dass es sich nicht nur um technische Aspekte handelt.**
>
> Quelle: Studienteilnehmer:in

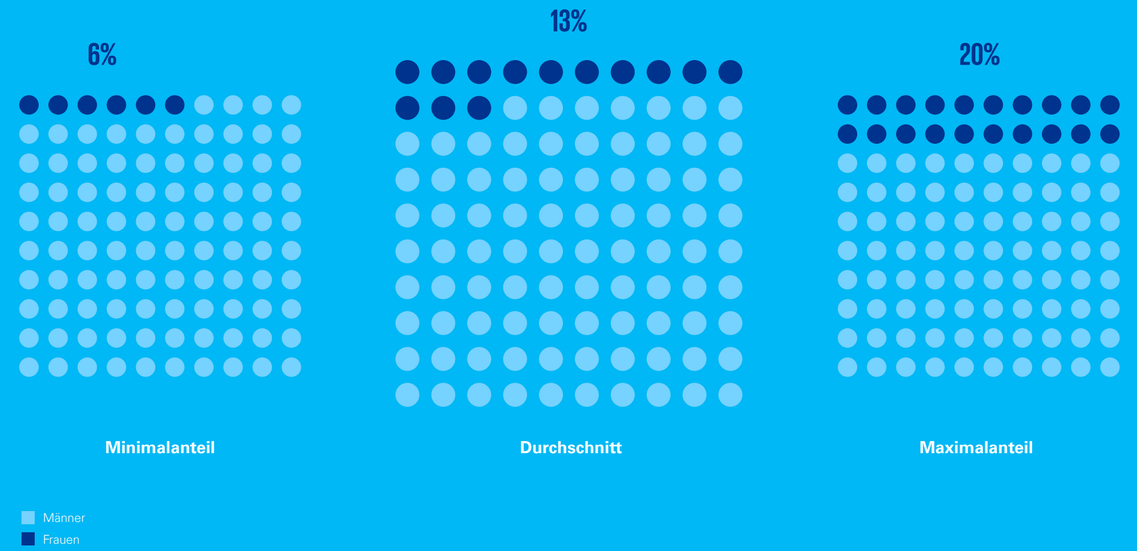
Bereits zu spät?

Für einige der Befragten müssen die Maßnahmen klar viel früher ansetzen, und zwar schon ab dem Eintritt in das Schulsystem. Aus den Antworten auf die Frage, wie man den Frauenanteil in der IT steigern könnte, geht die Wichtigkeit hervor, dass Mädchen schon ab dem frühen Schulalter verschiedenste Berufsbilder kennenlernen. Denn bereits dort werden Mädchen zu wenig in Technik und IT gefördert und bestärkt, hier eine Rolle einzunehmen. Das kann mitunter auch ein Grund dafür sein, warum der Frauenanteil in der IT erst langsam zu steigen beginnt; als Resultat des Umdenkens, das hier in den letzten Jahren begonnen hat.

Die Gesellschaft in der Verantwortung

Klar geht auch hervor, dass es sich hierbei nicht nur um ein in-

Wie hoch ist der Frauenanteil im Bereich Cybersecurity?



dividuelles, sondern auch um ein gesellschaftliches Thema handelt, welches gesamtgesellschaftlichen Handlungsbedarf erfordert, anstatt auf individuelle Präferenzen abzustellen. Mädchen und Frauen müssen alle Wege aufgezeigt werden, die sich ihnen bieten, denn wenn sie keine weiblichen Vorreiterinnen in einem bestimmten Feld sehen, sind sie weniger dazu geneigt, diesen Weg selbst einzuschlagen. Peering ist enorm wichtig, um ihnen alle Wege aufzuzeigen, die sie gehen können. Will man es mit den Worten von Christopher Columbus ausdrücken: „Man kann den Ozean nicht überqueren, solange man nicht den Mut hat, das Ufer aus den Augen zu verlieren."

> **Frühzeitiges Wecken von Interesse an dem Thema, Anpassung des Lehrplans – bereits in der Volksschule sollte das Thema Cybersecurity behandelt werden.**
>
> Quelle: Studienteilnehmer:in

Frauen fördern – Fachkräftemangel entgegenwirken

Eine Lösung für den Fachkräftemangel könnte sein, Inklusion und Diversität im Rekrutierungsprozess zu fördern. Unterrepräsentierte Gruppen wie z. B. Frauen, farbige Menschen oder jene mit informellem Bildungshintergrund wurden in der Vergangenheit häufig entmutigt, technische Karrieren anzustreben, sei es durch gesellschaftliche Erwartungen oder durch das vorherrschende Bild der Arbeitskultur im Cybersecuritybereich.

Wenn man die Ausbildung und Arbeitsangebote für Frauen und weitere unterrepräsentierte Gruppen attraktiver gestaltet, erweitert das auch den Pool an möglichen topqualifizierten Fachkräften in Österreich, deren Talente ansonsten verloren gehen.

Eine weitere Möglichkeit für die Öffnung des Bewerbungsprozesses ist der Fokus auf Fähigkeiten und Erfahrungen, anstatt einzig die Ausbildung als Maßstab heranzuziehen.

Das kann auch dazu beitragen, der mangelnden Identifikation und den Berührungsängsten von Mädchen und Frauen mit den techniklastigen Aspekten des Berufsfeldes entgegenzuwirken.

Optimistisch in die Zukunft

Was uns positiv stimmt und optimistisch in die Zukunft blicken lässt: Gerade auch aus den Antworten der Befragten geht eine klare Ermutigung hervor, diesen Berufsweg mit einer Vielfalt an Möglichkeiten einzuschlagen.

Was Sie sich aus diesem Kapitel mitnehmen sollten:

1. Die Situation des Fachkräftemangels bleibt weiterhin angespannt und Unternehmen fällt es schwer, passende Expert:innen zu rekrutieren.

2. Unternehmen suchen nach neuen Wegen, um Expert:innen für ihr Unternehmen zu gewinnen. Dabei öffnen sie auch den Arbeitsmarkt über die Grenzen Österreichs hinaus.

3. Beim Frauenanteil im Bereich Cybersecurity ist noch deutlich Luft nach oben. Die Vielfalt des Berufsfeldes muss aufgezeigt und die Arbeitsangebote für Frauen attraktiver gestaltet werden.

Erfahren Sie mehr in unserem Podcast IMPULSE

Es ist nie zu früh!

Cybersecurity ist ein Bereich, der immer mehr an Bedeutung gewinnt. Diesem Umstand muss auch bereits in der Ausbildung Rechnung getragen werden. Bislang fanden sich entsprechende Ausbildungsschwerpunkte lediglich an Universitäten und Fachhochschulen – allerdings gibt es auch vereinzelt Initiativen in Berufsbildenden Höheren Schulen. Bei einem Round Table sprachen wir mit Vertreter:innen von österreichischen Bildungseinrichtungen über das Thema Cybersecurity im Bildungssektor.

Warum haben Sie an Ihren Bildungseinrichtungen, also im BHS-Sektor, einen Schwerpunkt im Bereich Cybersecurity gesetzt? Was waren Ihre Motive dafür?

Herbert Gieger: Es hat mehrere Gründe gegeben. Ein Grund war die rückläufige demografische Entwicklung bei unserem Kerneinzugsgebiet. Das heißt, wir suchen daher immer nach Ausbildungsschwerpunkten, mit denen wir neue Schüler:innen akquirieren können. Und ein weiterer Punkt war eine persönliche negative Erfahrung mit Cyber Hacking. Ich habe mir die Bildungslandschaft in Österreich angesehen und erkannt, dass es in diesem Bereich eigentlich keine offizielle Ausbildung gibt. Daraufhin haben wir den Ausbildungszweig „Sicherheitsmanagement und Cybersecurity“ installiert. Und unser Vorteil ist, dass wir bereits jetzt, obwohl wir erst im zweiten Ausbildungsjahr sind, schon Kooperationen mit einigen Unternehmen oder Behörden haben, die jetzt bereits mit ihren zukünftigen Arbeitskräften in Kontakt treten wollen. Heißt, sie ermöglichen uns Praktikumsplätze, aber schicken auch Expert:innen, die bei uns Unterrichtseinheiten übernehmen.

Thomas Gabriel: Ich komme ursprünglich aus der Privatwirtschaft und da habe ich gemerkt, wie locker eigentlich mit Daten umgegangen wird und kein Bewusstsein dafür vorhanden ist. Das war für mich dann auch ausschlaggebend, in den Ausbildungsbereich zu wechseln, um die Möglichkeit zu haben, mehr Awareness für das Thema Datensicherheit zu schaffen. Seit dem heurigen Schuljahr gibt es bei uns auch eine Klasse mit dem Schwerpunkt Informationstechnologie, in der es im Unterschied zu den Informatiklassen weniger ums Programmieren geht. Denn das Programmieren steht häufig im Zusammenhang mit einer hohen Drop-out-Rate, da es nicht jedermanns Sache ist. Und natürlich war für uns auch die rückläufige Schüler:innenzahl mit ein Grund für ein erweitertes Angebot.

Martina Mikovits: Wien ist anders, das ist bekannt – auch in diesem Fall stimmt diese Einschätzung. Wir haben unsere Schwerpunkte nicht aus demografischen Gründen angepasst, wir haben weit mehr Anmeldungen, als wir aufnehmen können, sondern wir haben einfach formal nachgezogen. Sprich, wir haben in den Lehrplan das mit aufgenommen, was unsere Lehrer:innen teilweise schon unterrichtet haben. Denn eines ist klar: Digitalisierung geht nicht ohne Cybersecurity und wir müssen den Schüler:innen nicht nur den Umgang mit neuen Technologien beibringen, sondern auch, wie sie sich schützen können.

Welche Personengruppen möchten Sie mit Ihrem Ausbildungsangebot im Speziellen ansprechen? Welche Inhalte sollen es sein, die die zukünftigen Schüler:innen interessieren sollen?

Thomas Gabriel: Zunächst muss man sagen, dass die Schüler:innen, wenn sie zu uns kommen – also mit 14 Jahren – oft eigentlich noch nicht so richtig wissen, wohin die Reise gehen soll. Daher war es mir ein Anliegen, mit dem neuen Zweig Informationstechnologie auch alle jene anzusprechen, die nicht unbedingt Software Engineer werden möchten. Hier stellen wir also wirklich die IT-Sicherheit in den Vordergrund, aber natürlich braucht man auch hier die Grundlagen des Programmierens, denn ohne die Basis – wie lese ich Codes, wie entschlüssele ich Codes usw. – scheitert man kläglich. Also ein gewisses Grundinteresse muss schon vorhanden sein.

Martina Mikovits: Da stimme ich völlig zu. Viele Schüler:innen werden von dem Begriff Informationstechnologie angezogen, weil sie das einfach mit Computer und Spielen verbinden und wissen eigentlich gar nicht so wirklich, was dahintersteckt. Es klingt oft leichter und interessanter, als es dann manchmal wirklich ist. Umfassende Kenntnisse z. B. in Mathematik,

> **Es braucht Allgemeinwissen, es braucht Fachwissen, es braucht Leistung und man muss geeignet sein.**

FOTO © FOTO SCHREINER

HR Mag. Dr. Martina Mikovits
Direktorin Schulzentrum HTL/HAK/HAS Ungargasse

Naturwissenschaften und Englisch, sind die Voraussetzung, bevor es in die Tiefe zum Programmieren, zur Softwareentwicklung usw. geht und das ist teilweise auch knochentrocken und anstrengend. Und daher ist es wichtig, dass die Schüler:innen das wirklich machen wollen und motiviert sind.

Herbert Gieger: Wir sind hier etwas breiter aufgestellt, sprich, wir beschäftigen uns intensiv mit dem Thema Sicherheitsmanagement. Wir wollen unseren Schüler:innen beibringen, wie sie mit Krisen umgehen. Wie erkenne ich eine Krise, wie manage ich sie – und dazu gehören natürlich auch Cyberangriffe, deshalb haben wir hier einen eigenen Gegenstand. Ein weiteres Standbein ist der:die Information Security Manager:in – hier geht es um die kritische Infrastruktur.

Es dreht sich also viel um Motivation: Wie bringt man Menschen dazu, sich für das Thema Cybersecurity zu interessieren? Was braucht es, um das Feuer zu entfachen?

Martina Mikovits: Das Problem ist nicht das Feuer, das ist jedenfalls da. Cybersecurity klingt spannend, interessant, ein bisschen nach Kriminalität – das zieht immer. Es ist den Interessent:innen bewusst zu machen, dass viel mehr dazu gehört. Es braucht sowohl eine gute Allgemeinbildung als auch technische Fachkompetenz.

Herbert Gieger: Also wir gehen auf den Bildungsmessen oder beim Tag der Offenen Tür den Weg, dass wir keine Show abziehen, sondern wirklich versuchen, so klar wie möglich darzustellen, was auf die Schüler:innen zukommt. Es gibt auch Schnuppertage, wo man einen Tag lang den Unterricht besuchen kann, und da wird nichts abgeändert, damit man wirklich einen Einblick bekommt.

Thomas Gabriel: Das sehe ich auch so. Man muss sich als Schule authentisch präsentieren – das haben wir und das können wir. Und dafür eignen sich natürlich so Schnuppertage sehr gut. Und was ich in der heutigen Zeit natürlich auch als Motivationskraft anführen muss: Auf jede:n Absolvent:in kommen zwei fixe Arbeitsplatzangebote .

Woher bekommen Sie Ihre Lehrkräfte? Können Sie den Bedarf intern abdecken oder braucht es Unterstützung von außen?

Herbert Gieger: Grundsätzlich ist es so, dass das gesamte Team, angefangen von der Direktion bis hinunter dafür brennen und für diese Sache eintreten muss, dann sieht man auch, dass sich was bewegt. Aber da sich dieser Bereich ständig weiterentwickelt, ist es eigentlich notwendig, die Expert:innen auch aus der Praxis zu bekommen, sonst hinkt man ständig hinterher. Und nur die Aussicht, später unsere Absolvent:innen übernehmen zu können, ermöglichen uns eben die vorhin genannten Kooperationen, denn finanziell können wir natürlich nicht mithalten.

Thomas Gabriel: Da kann ich nur zustimmen. In der Lehramtsausbildung auf diesem Gebiet besteht Aufholbedarf. So wie der Ausbildungsplan jetzt ist, braucht es zusätzlich zum Lehramtsstudium Informatik noch weiterführende Kurse – besonders im Programmieren – damit die Kolleg:innen auch in den höheren Klassen eingesetzt werden können. Und jene, die eine adäquate Ausbildung gemacht haben, gehen dann eben sehr oft in die Privatwirtschaft – auch wegen finanzieller Anreize.

Martina Mikovits: Ja, das ist ein altbekanntes Problem – Angebot und Nachfrage. Wir bekommen im Augenblick nicht die Leute, die wir brauchen würden, da sie einfach in der Wirtschaft so nachgefragt sind. Wir sind im Schulsystem unflexibel – nicht nur in finanzieller Hinsicht. Es geht auch um die Lehrpläne, die ja immer ein paar Jahre im Voraus festgeschrieben werden und dann in dem Bereich Informationstechnologie vielleicht gar nicht mehr aktuell sind, wenn sie zum Einsatz kommen, da dieses Feld sehr dynamisch ist. Das ist nicht wie Englisch oder Deutsch, wo sich im Grunde nicht viel ändert. Unsere Kolleg:innen bräuchten eine permanente Weiterbildung, was sich aber auch zeittechnisch häufig nicht mit ihrer Lehrverpflichtung vereinbaren lässt. Wenn man natürlich das Glück hat, Lehrer:innen zu haben, die für dieses Thema brennen und bereit sind, auch Extrameilen mit ihren Schüler:innen zu machen, dann kann man hier schon tolle Sachen auf die Beine stellen – weiterführende Freigegenstände oder Sommerkurse zum Beispiel.

Es gibt also einen eklatanten Mangel an Lehrpersonal für diesen Bereich. Müssen wir wieder mehr in die Mobilität der Schüler:innen investieren, weil man einfach nicht an jeder Bildungseinrichtung Cybersicherheit lehren kann?

Thomas Gabriel: Ich finde, man sollte österreichweit fixe Standorte machen, die auch verkehrstechnisch gut erreichbar sind. An diesen Standorten wird dann Cybersecurity unterrichtet. Das Problem dabei ist aber auch, dass es derzeit Jahre dauert, solche Anträge durchzubringen.

Herbert Gieger: Das sehe ich ähnlich, aber man muss aufpassen, dass es nicht inflationär wird, denn dann leidet die Qualität. Und das Wichtigste ist, dass ein hoher Qualitätsstandard gesichert wird – eben auch mit Expert:innen.

Martina Mikovits: Grundsätzlich ja, aber die Standorte allein lösen noch nicht das Problem, dass wir gar nicht die notwendige Anzahl an Lehrer:innen dafür hätten. Das muss man auch bedenken.

Sie erwähnen immer wieder die Notwendigkeit der Allgemeinbildung und der Bereitschaft zu harter Arbeit. Stichwort künstliche Intelligenz: Inwiefern wird mit Tools wie ChatGPT ein ganz anderes Bild vermittelt und der leichte Weg aufgezeigt?

Martina Mikovits: Das ist ein großes Thema. Die Entwicklungen überholen sich und die Schüler:innen haben noch nicht das Wissen, wie mit diesen Entwicklungen umzugehen ist: Sprich, auf der einen Seite ganz wenig Wissen, auf der anderen Seite

Österreich hat die letzten 20 Jahre in der Cybersecurity verschlafen.

FOTO © HTL PINKAFELD

AV Prof. Mag. Thomas Gabriel BSc
Abteilungsvorstand Informatik und Informationstechnologie, HTL Pinkafeld

Im Cyberbereich gibt es eine 100-prozentige Jobgarantie.

FOTO © FOTOSTUDIO HRUBY

HR Dir. Mag.
Herbert Giegerl
Schulleiter HAK Tamsweg

aber unglaublich viele Möglichkeiten. Fakt ist aber, wenn ich kein Allgemeinwissen und kein technisches Wissen habe, kann ich letztlich auch mit der KI nicht umgehen. Denn KI kann mir alles schreiben, aber wenn ich nicht überprüfen kann, ob das halbwegs stimmt, dann funktioniert das langfristig nicht und auch das müssen wir unseren Schüler:innen vermitteln.

Herbert Giegerl: Das unterstreiche ich. Wenn ich keine Basis habe, dann hilft mir die beste KI nichts, weil ich es nicht werten oder kritisch hinterfragen kann. Aber KI wird bleiben und wir werden damit lernen müssen umzugehen.

Wenn wir uns in 12 Monaten wieder treffen, was würden wir uns dann wünschen, heute schon getan zu haben?
Martina Mikovits: Was ich mir für die Zukunft definitiv wünschen würde, ist eine bessere Kommunikationsstruktur mit den Bildungsdirektionen und dem Bildungsministerium, damit wir alle zukünftig flexibler und autonomer agieren können und somit es auch einfacher wird, neue Projekte, Ausbildungszweige wie z. B. Kollegs zu etablieren.

Herbert Giegerl: Das kann ich nur unterstützen. Es geht um gemeinsame Kommunikation und es geht ums unvoreingenommene Reflektieren. Das beinhaltet auch ein gemeinsames Konzept, wo welche Ausbildungen angeboten werden und damit diesem Wildwuchs, wie er derzeit manchmal stattfindet, ein Ende gemacht wird.

Thomas Gabriel: Ich kann mich dem nur anschließen: Die Kommunikation innerhalb des Schulsystems muss verbessert werden.

HTL Pinkafeld: Die Abteilung Informationstechnologie legt verstärkt den Schwerpunkt auf Netzwerktechnik und IT-Sicherheit. Die Schüler:innen erhalten eine breite Ausbildung in Systemtechnik, Medientechnik, Informationssysteme, Softwareentwicklung und Betriebswirtschaft.

Weitere Informationen:
https://www.htlpinkafeld.at/informationstechnologie/

Schulzentrum HTL/HAK/HAS Ungargasse: Die HTL für Informationstechnologie – Netzwerktechnik und IT-Sicherheit bietet eine spezialisierte, praxisbezogene Ausbildung für gesuchte IT-Fachkräfte (System Engineer, Softwareentwickler:in, IT-Systemadministrator:in, IT Security Architect).

Weitere Informationen:
https://www.szu-home.at/ausbildung/htl-informations-technologie-netzwerktechnik/

HAK Tamsweg: Ausbildungszweig „Sicherheitsmanagement und Cybersecurity". Die Cybersecurity-HAK bietet Schüler:innen in integrierter Form kaufmännische Bildung, fundierte IT-Kenntnisse sowie eine Ausbildung in Sicherheitsmanagement und Cybersecurity. Sie kooperiert eng mit Sicherheitsbehörden (sowohl Bund als auch Länder) und mit international agierenden Unternehmen aus der Wirtschaft.

Weitere Informationen:
https://info.haktamsweg.at/management-cyber-security.html

Ausblick

55% der Befragten sagen, dass Cyberangriffe ihre geschäftliche Existenz bedrohen

63% der Unternehmen sind der Ansicht, dass die Cyberangriffe gegen ihr Unternehmen in den nächsten zwölf Monaten zunehmen werden

31% der Unternehmen wünschen sich, dass auch andere das Thema Cybersicherheit für so wichtig halten wie sie selbst

33% Jede:r dritte Befragte würde bevorzugt Security-Lösungen von österreichischen Unternehmen einsetzen

65% stimmen der Aussage zu, dass die Unternehmensleitung Informationssicherheit nicht als einen möglichen Wettbewerbsvorteil betrachtet

Für **44%** hat Business Continuity Management in den letzten zwölf Monaten an Bedeutung gewonnen

33% ist die Funktion des:der CISO im Zusammenhang mit ESG nicht bekannt

Die Unternehmen blicken pessimistisch in die Zukunft. 55 Prozent der Befragten sagen, dass Cyberangriffe ihre geschäftliche Existenz bedrohen. Cybersicherheit ist mittlerweile zu einer wahren Existenzbedrohung für heimische Unternehmen geworden mit Schäden in Millionenhöhe.

Für die meisten der Befragten (44 Prozent) hat Business Continuity Management – also die Widerstandsfähigkeit der Geschäfts- und Unternehmenstätigkeiten nach einem Cyberangriff oder anderen Auslösern – in den letzten zwölf Monaten an Bedeutung gewonnen. Und auch im Jahr 2022 war Business Continuity Management (38 Prozent) bereits Spitzenreiter. Durch die zunehmende Abhängigkeit von Lieferanten und Dienstleistern rückt auch das Thema 3rd Party Risk Management in den Mittelpunkt. Für nahezu jedes vierte Unternehmen (23 Prozent) ist es ebenfalls zu einem großen Thema geworden.

Eine gesunde Portion Pragmatismus

"You can't stop the waves, but you can learn to surf." (Jon Kabat-Zinn)

14 Prozent der Befragten hoffen, dass sie sich im kommenden Jahr nicht mehr so viel mit Cybersicherheit beschäftigen müssen. Was die aktuelle Stimmungslage in Bezug auf Cybersecurity angeht, gehen die Umfrageteilnehmer:innen pragmatisch an die Situation heran: Cybersicherheit wird als untrennbarer Teil der digitalen Gesellschaft gesehen, der zum Alltagsgeschäft in den Unternehmen werden muss.

Wunsch nach Schutz und Stabilität

Unternehmen vermissen deutlich die Unterstützung durch den Staat. Der Schutz vor Cyberkriminalität wird laut den Befragten im Gegensatz zu anderen Formen von Kriminalität vom Staat eher stiefmütterlich behandelt. Dass sich Unternehmen selbst schützen sollen, wird als ineffizient und auch nur begrenzt möglich angesehen. Vielen Unternehmen fehlt es auch einfach an Ressourcen, um sich bestmöglich vor Cyberkriminalität zu schützen. Die mangelnde staatliche Unterstützung eröffnet auch einen Markt für unseriöse Cybersecurityfirmen.

31 Prozent der Unternehmen wünschen sich, dass auch andere das Thema Cybersicherheit für so wichtig halten wie sie selbst. Für 47 Prozent ist Cybersecurity zu einem sehr wichtigen Teil ihres Lebens geworden. Daran erkennt man, dass Cybersicherheit für Unternehmen zu einem dringenden Anliegen geworden ist, bei dem mehr Schutz benötigt wird. 63 Prozent der Unternehmen sind der Ansicht, dass die Cyberangriffe gegen ihr Unternehmen in den nächsten zwölf Monaten zunehmen werden – rund ein Viertel (27 Prozent) ist der Meinung, dass die Anzahl der Angriffe gleich bleiben wird.

Die Tiefen des Cyberspace

Wir haben die Befragten auch um eine Einschätzung der Gründe für die Entwicklung von Cyberangriffen gegen ihr Unternehmen gebeten. Die Antworten waren wie zu erwarten vielfältig:

Einige sehen eine allgemeine Zunahme von Cyberangriffen, was natürlich auch die Wahrscheinlichkeit, individuell betroffen zu sein, erhöht. Cyberangriffe gehören mittlerweile schon zum Tagesgeschäft und das Bewusstsein darüber, zum Ziel von Angriffen werden zu können, muss in das Selbstverständnis eingehen. Befürchtet wird auch, dass immer mehr kleine Unternehmen zum Ziel werden und es wird besonders hervorgehoben, durch Angriffe auf andere Unternehmen Kollateralschäden zu erleiden.

KI-Entwicklungen und die immer stärker werdende Verlagerung von Applikationen in die Cloud werden ebenfalls als Gründe gesehen. Auch durch die Vielzahl an Digitalisierungsinitiativen der Unternehmen und den verstärkten Datenaustausch entlang der Produktions- und Lieferketten werden Angriffe wahrscheinlicher.

Ein Ozean voller Raubtiere

Andere wiederum finden, dass der militärische Bereich von besonderem Interesse ist. Ein Grund für die Entwicklung von Cyberangriffen ist demnach die instabile politische Lage und dass der Cyberraum mittlerweile zum Schauplatz von Kriegen geworden ist. Es wird beobachtet, dass es mehr Akteur:innen am Markt gibt und immer mehr Staaten Cyberangriffe als billiges und legitimes Mittel sehen, um ihre Interessen durchzusetzen. Neben Systemrisiken und der Gefährlichkeit der geopolitischen Lage wurde aber auch der wachsende internationale Bekanntheitsgrad eines Unternehmens angeführt. Auch die Sichtbarkeit und Präsenz in den Medien wird als Grund genannt, zum Angriffsziel zu werden oder zu bleiben.

> **Aus meiner Sicht geht der Trend in Richtung mehr Cyberangriffe, ob jetzt gezielt auf die Unternehmen oder auch unbeabsichtigt z. B. Kollateralschäden bei APT-Angriffen.**
>
> **Daher denke ich, steigt das Risiko auch für unser Unternehmen.**
>
> Quelle: Studienteilnehmer:in

Angreifer:innen haben einen langen Atem

Zusätzlich wird ein Vorteil hervorgehoben, den im Besonderen die Angreifer:innen haben: Es gibt immer mehr Möglichkeiten, einen Cyberangriff durchzuführen – der Erfindungsgabe der Angreifer:innen sind hier keine Grenzen gesetzt. Sie können über lange Zeit unentdeckt in den IT-Systemen der Unternehmen bleiben. Unternehmen hingegen können bei ihrer Abwehr immer nur auf die Angriffe reagieren. Betont wird auch, dass Cyberangriffe leider immer lukrativer werden und Unternehmen durch Lösegeldzahlungen die nächsten Angriffe mitfinanzieren. Hier zeigt sich noch mal deutlich: Zahlen ist keine Option.

Dennoch machen sich unsere gemeinsamen Anstrengungen bezahlt: Konnten Angreifer:innen früher mehrere hundert Tage unentdeckt in den IT-Systemen agieren (dwell time), so haben sie heute nur noch ein kürzeres Zeitfenster von schätzungsweise 30–70 Tagen zur Verfügung.

Kurswechsel

Aber auch eine Verbesserung der Sensibilisierung im Unternehmen aufgrund von vergangenen Cyberangriffen war Thema. Es wurde angemerkt, dass die Personen im Unternehmen

das Thema nicht ernst genug nähmen und erst im Falle eines Ereignisses die Ernsthaftigkeit diesbezüglich größer werden würde. Das unterstreicht unser Ergebnis, dass erst in Cybersicherheit investiert wird, wenn bereits etwas passiert ist.

Chef:innensache?

Cybersicherheit ist Chef:innensache. Doch immer wieder ist zu beobachten, dass sich Vorstände und Geschäftsführer:innen hier zurückhaltend zeigen und die Verantwortung an die IT-Leitung oder den:die CISO (Chief Information Security Officer) abgeben. Eine Praxis, die wohl kaum zukunftsfähig ist.

In Zukunft werden Unternehmen auch im Vorstand einen eigenen Ausschuss für Cybersecurity benötigen. Diese Rolle könnten beispielsweise ehemalige CISOs einnehmen, die Cyberrisiken und den Umgang damit beaufsichtigen und kontrollieren. So soll mehr Transparenz bei Cyberrisiken entstehen. Auch die Kommunikation in den Unternehmen muss sich in Zukunft verbessern.

> **Cyberangriffsversuche (Phishing, Ausnutzung von Schwachstellen, DDoS-Versuche …) gehören zum täglichen Geschäft, an dem wird sich auch in den nächsten zwölf Monaten nichts ändern.**
>
> Quelle: Studienteilnehmer:in

Eine Frage des Vertrauens

Wir wollten von unseren Studienteilnehmer:innen wissen, wie souverän ihr:e CISO/IT-Sicherheitsverantwortliche:r auf bestimmte Fragen des Vorstands antworten würde. Auffällig ist, dass gerade auf die Frage, welche kritischen Daten sich bei Dritten befinden und ob sichergestellt werden kann, dass diese in der gesamten Wertschöpfungskette ausreichend geschützt sind, 28 Prozent der Befragten hier keine souveräne Antwort seitens des:der CISO vermuten.

30 Prozent schätzen die Antwort auf die Frage nach der Größe des aktuellen Cyberrisikos und dessen Messung als nicht souverän ein. Das Wissen darüber, wie bei einem größeren Cyberangriff zu reagieren ist, wird hingegen von 76 Prozent der Befragten als souverän eingeschätzt.

Auch die Beantwortung der Frage nach Wettbewerbsvorteilen durch die eigene Cybersicherheit schätzen 37 Prozent als nicht souverän ein. Das korreliert mit der Aussage, dass die Unternehmensleitung Informationssicherheit nicht als einen möglichen Wettbewerbsvorteil betrachtet. Dieser Aussage haben 65 Prozent zugestimmt. Ebenfalls passt das mit der Tatsache zusammen, dass 78 Prozent finden, dass ihre Führungskräfte nicht verstehen, welche Wettbewerbsvorteile ein größeres Vertrauen durch mehr Cybersicherheit mit sich bringt.

Allerdings ergibt dies einen Widerspruch zur Aussage von 53 Prozent, die sagen, dass das Budget für Cybersecurity aufgrund der Unternehmensstrategie steigen muss. Hier scheinen die Aussagen der Befragten in sich nicht kongruent zu sein oder mit zweierlei Maß gemessen zu werden.

Das letzte Wort

Es braucht eine Trennung und Spezialisierung bei den Aufgaben betreffend IT und Sicherheit. Dann kann der:die CISO als unabhängiges Kontrollorgan zum:zur CIO (Chief Information Officer) fungieren. CISOs sind oftmals das Bindeglied zwischen der IT-Abteilung, Fachbereichen und dem Management und brauchen das Vertrauen aller Beteiligten.

69 Prozent der Befragten sagen, dass die Unternehmensleitung der Meinung ist, dass der:die CISO/IT-Sicherheitsverantwortliche letztendlich für die Cybersicherheit des Unternehmens verantwortlich ist. Die Ansicht, dass Cybersicherheit in der IT angesiedelt sein sollte, scheint in den Unternehmen demnach immer noch weit verbreitet zu sein. An dieser Stelle muss gesagt werden, dass Cybersicherheit letztendlich Chef:innensache ist und diese hier Verantwortung übernehmen müssen. In Unternehmen braucht es eine klare Trennung zwischen der Rolle des:der CISO und der IT-Abteilung.

> **Es wird leider immer lukrativer Cyberangriffe durchzuführen, da leider viele gehackte Firmen mit ihren Lösegeldzahlungen die nächsten Angriffe mitfinanzieren und sich die Angreifer:innen immer potenter aufstellen.**
>
> Quelle: Studienteilnehmer:in

Cybersecurity sollte nicht in der IT angesiedelt sein, sondern der:die CISO sollte direkt dem:der CEO Bericht erstatten. Wenn CISOs direkt an CEOs Bericht erstatten, könnten auch Budgetkonflikte zwischen Sicherheitsinitiativen und Technologieinvestitionen vermieden werden[1].

Ohne Einfluss

Jedes zehnte Unternehmen ist sich unklar darüber, ob der:die CISO genügend Einfluss hat, um die Organisation und ihre Daten zu schützen. Nur 32 Prozent finden, dass er:sie genügend Einfluss hat.

61 Prozent sind der Ansicht, dass die Unternehmensleitung den:die CISO als leitende Führungskraft ansieht. Dies lässt jedoch die Frage zu, warum der Einfluss des:der CISO dann immer noch so gering eingeschätzt wird.

Alles eine Frage der Kommunikation

Eine gemeinsame Sprache wird benötigt, die auf Kennzahlen basiert, mit denen Vorstandsmitglieder etwas anfangen können[2].

Die Hälfte der Befragten ist der Ansicht, dass die Unternehmensleitung technische Einzelheiten nicht nachvollziehen kann. Dies lässt Rückschlüsse auf sprachliche Barrieren zwischen Vorstand und CISO zu. Auch der Global Cybersecurity Outlook 2023 vom WEF berichtet über Schwierigkeiten von Cyber-Führungskräften in der Kommunikation mit der Geschäftsleitung, was eine Verständnislücke zwischen Sicherheitsthemen und den Auswirkungen auf das Unternehmen demonstriert[3].

[1] World Economic Forum: Global Cybersecurity Outlook 2023, S. 28., [2] World Economic Forum: Global Cybersecurity Outlook 2023, S. 4., [3] World Economic Forum: Global Cybersecurity Outlook 2023, S. 22.

> **Durch den dzt. KI-Hype erwarte ich auch eine Nutzung durch Cyberkriminelle, Herabsetzung der notwendigen Skills für Angriffe, und daher eine Zunahme der Angriffe.**
>
> Quelle: Studienteilnehmer:in

83 Prozent finden, dass die Beziehung zwischen der Unternehmensleitung und den CISOs/IT-Sicherheitsverantwortlichen von großem Vertrauen geprägt ist. Diese Aussage sendet eine positive Botschaft, dass ein großes Grundvertrauen in den:die CISO vorhanden ist. Somit besteht allerdings auch die Gefahr, dass sich Vorstände in puncto Cybersicherheit eher zurückhalten und ihre Verantwortung auf den:die CISO abwälzen. Denn auch wenn sie großes Vertrauen in ihre CISOs haben, ist und bleibt Cybersicherheit letztendlich Chef:innensache.

Führungskräfte im Cyberbereich müssen Sicherheitsthemen so präsentieren, dass sie der Vorstand versteht und dementsprechend handeln kann. Die Geschäftsführung muss mehr Verantwortung für operative Cyberanforderungen übernehmen, um die Cyberfähigkeiten des Unternehmens zu verbessern[4].

Mit voller Kraft voraus

80 Prozent der Befragten stimmen der Aussage zu, dass sich die Cybersecuritystrategie an der Strategie und den Zielen des Unternehmens ausrichtet. Das lässt sich auch klar an der Budgetsteigerung für Cybersecurity sowie an der Veränderung der Unternehmensstrategie als Grund für den Budgetanstieg ablesen.

Für 68 Prozent wird Informationssicherheit von Compliance-Anforderungen bestimmt. Für nur 27 Prozent stehen langfristige wirtschaftliche Ambitionen im Vordergrund. 48 Prozent finden, dass die Rolle des:der CISO/IT-Sicherheitsverantwortlichen nicht so strategisch ist, wie sie sein sollte. In diesem Zusammenhang soll noch mal die notwendige klare Trennung von CISO und IT-Security unterstrichen werden, die eine strategischere Ausrichtung der Rolle zulassen würde.

ESG

19 Prozent sind der Ansicht, dass der:die CISO/das Cybersecurity-Team aktuell keinen Auftrag für ESG (Environment, Social, Governance) hat. 33 Prozent ist die Funktion des:der CISO im Zusammenhang mit ESG nicht bekannt.

16 Prozent sind der Meinung, dass der:die CISO/das Cybersecurity-Team ein integraler Bestandteil des ESG-Teams ist, das eine Vielzahl von ESG-bezogenen Aktivitäten vorantreibt.

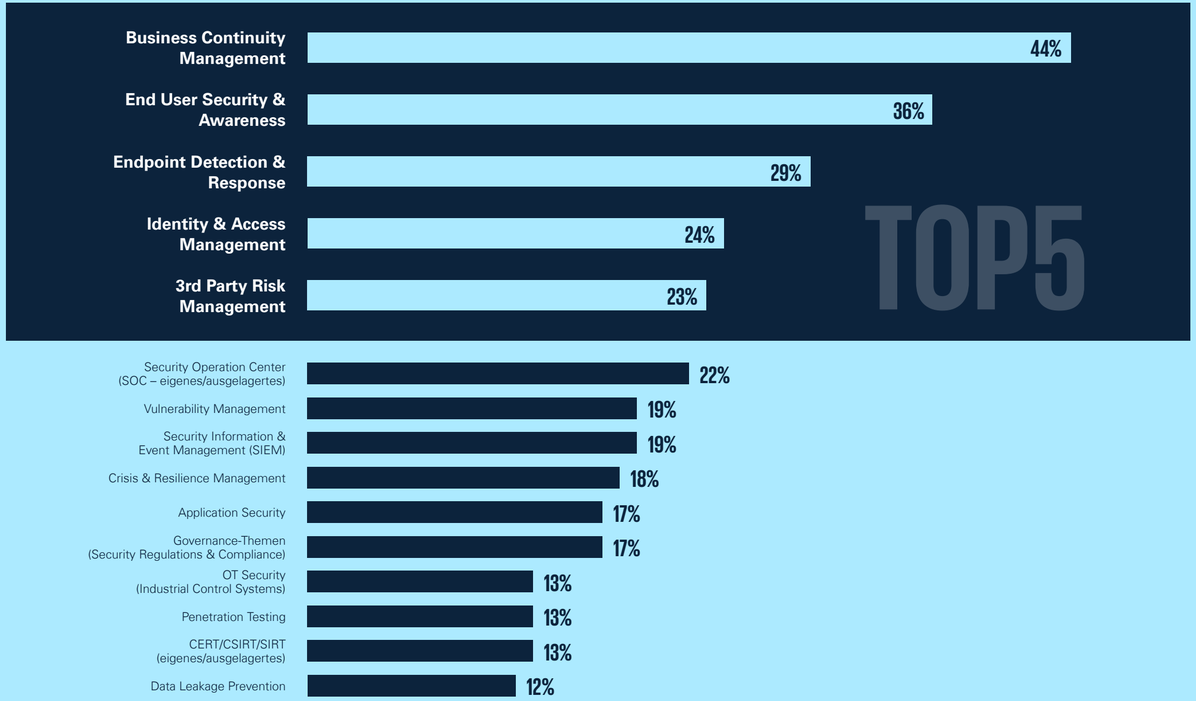
Made in Austria

„Je höher die Wellen, desto wichtiger der Anker." (KarlHeinz Karius)

Jede:r dritte Befragte würde bevorzugt Securitylösungen von österreichischen Unternehmen einsetzen. Daraus geht hervor, dass es einen österreichischen Wirtschaftsstandort für Securitylösungen braucht. Zwar gibt es vereinzelt Leuchttürme in Österreich auf diesem Gebiet, aber international ist man hier noch zu schwach aufgestellt. Von der Förderung von Start-ups bis hin zur Stärkung unserer Technologiekompetenz muss hier noch so einiges in Angriff genommen werden. Die Politik hat hier einen klaren Auftrag und ist gefordert, die Appelle an sie zu hören und diese auch ernst zu nehmen.

[4] World Economic Forum: Global Cybersecurity Outlook 2023, S. 4.

Womit wollen sich Unternehmen in den kommenden zwölf Monaten beschäftigen?



Was Sie sich aus diesem Kapitel mitnehmen sollten:

1. Unternehmen wünschen sich mehr Unterstützung durch den Staat beim Schutz vor Cyberkriminalität. Vielen mangelt es an Ressourcen und Expertise, um sich selbst bestmöglich schützen zu können.

2. Es braucht eine klare Trennung zwischen der Rolle des:der CISO und der IT-Abteilung. Das erlaubt auch eine strategischere Ausrichtung der Rolle.

3. Vorstände dürfen sich beim Thema Cybersicherheit nicht zurücknehmen und ihre Verantwortung auf den:die CISO abwälzen. Cybersicherheit ist und bleibt letztendlich Chef:innensache.

Unsere Kooperationspartner

Wir bedanken uns bei unseren Kooperationspartnern für die Zusammenarbeit bei der Studie

iv INDUSTRIELLEN VEREINIGUNG

KSÖ Kompetenzzentrum Sicheres Österreich

Sicherheitsforum Digitale Wirtschaft Österreich

WKO WIRTSCHAFTSKAMMER WIEN INFORMATION·CONSULTING

FH Salzburg

JOANNEUM RESEARCH

universität innsbruck
Netzwerk Banking, Accounting Auditing, Finance & IT (BAFIT)

Umfragemethodik

Die vorliegende KPMG Studie „Cybersecurity in Österreich“ beschäftigt sich mit der Frage, wie österreichische Unternehmen den neuen Herausforderungen der Cyberkriminalität im Jahr 2023 begegnen und welche Cybersecurity-Maßnahmen getroffen werden.

Die Umfrage: Cybersecurity im Überblick

Die Umfrage zur Studie wurde im Februar und März 2023 von KPMG unter 903 österreichischen Unternehmen durchgeführt. Die Teilnehmer:innen setzten sich aus Vertreter:innen kleiner und mittlerer Unternehmen sowie Großunternehmen aus den Branchen Automobilindustrie, Banken, Bauwirtschaft, Bildung, Chemiewirtschaft, Dienstleistungsbereich, Energiewirtschaft, Gesundheitswesen, Immobilienwirtschaft, Industrie, Konsumgüter, Medien, Öffentlicher Sektor, Technologie, Telekommunikation, Tourismus und Versicherungswirtschaft zusammen.

Die Auswertung: Stimmungsbild in Österreich

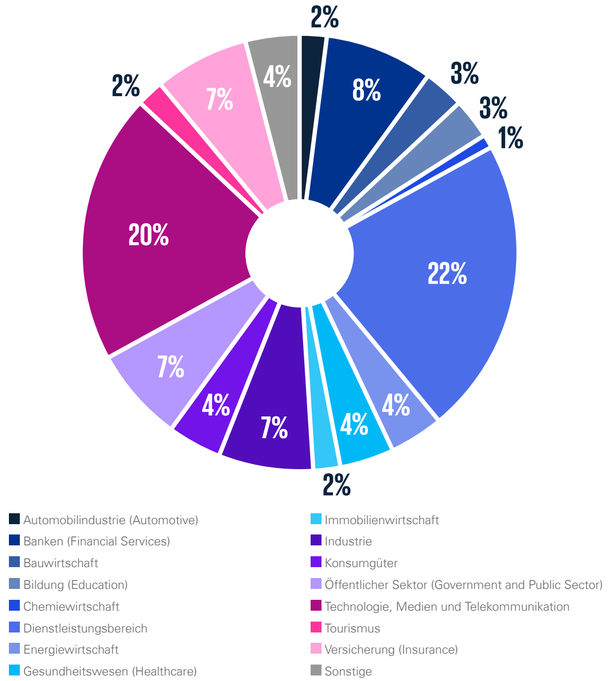
Jede:r Teilnehmer:in erhielt ihrer:seiner Funktion im Unternehmen entsprechend einen Online-Fragebogen mit spezifischen Fragen. Darüber hinaus wurden die quantitativen Fragen (Likert-Skala) um qualitative Aspekte erweitert, um den Teilnehmer:innen die Möglichkeit zu geben, weitere Eindrücke und Beobachtungen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

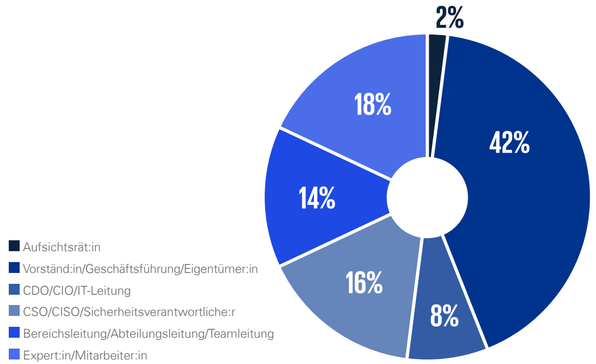
Für die Auswertung wurde zwischen Innensicht/Leitungsebene (Expert:innen, Bereichsleiter:innen, CSO etc.) und Außensicht/Steuerungsebene (Vorständ:innen, Eigentümer:innen, Aufsichtsrät:innen) unterschieden. Die Ergebnisse wurden von einem KPMG Cybersecurity-Expert:innenteam aus dem Bereich IT Advisory ausgewertet.

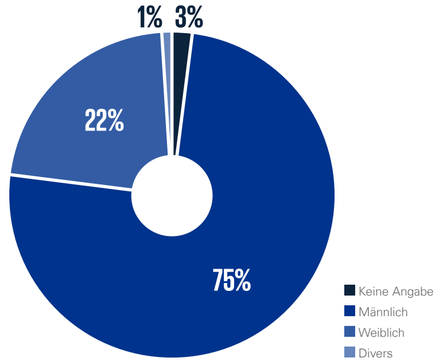
Die Vertiefung: Im Gespräch mit Expert:innen

In persönlichen Interviews standen außerdem 22 Wirtschaftsvertreter:innen, Vertreter:innen der öffentlichen Verwaltung und Cybersecurity-Expert:innen zum Thema Rede und Antwort. Bei unseren Round Tables diskutierten Expert:innen von KPMG gemeinsam mit Direktor:innen und Abteilungsvorständ:innen von Berufsbildenden Höheren Schulen, Vertreter:innen von Women4Cyber Österreich, der Technischen Universität Wien sowie österreichischen Gebietskörperschaften über Herausforderungen, aktuelle Entwicklungen und zukünftige gesellschaftliche und inhaltliche Handlungsfelder.

Hinweis: Etwaige Abweichungen von 100 Prozent sind auf Rundungsdifferenzen zurückzuführen.







Impressum

Cybersecurity 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

Data Scientist
Moritz Löw
M +43 664 821 37 06
mloew@kpmg.at

Koordination:
Mariana Herrloss
M +43 664 816 12 28
mherrloss@kpmg.at

Marlene Zauner
M +43 664 888 290 19
marlenezauner@kpmg.at

Grafik und Satz:
Martin Morauf-Schmidl
M +43 664 883 087 87
mmorauf-schmidl@kpmg.at

Druck:
Ferdinand Berger & Söhne GmbH

Die Antworten in den Interviews spiegeln die persönliche Sichtweise der Interviewpartner:innen wider und können durchaus von der Ressortmeinung zu den Fragen abweichend sein.

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.


KPMG