KPMG

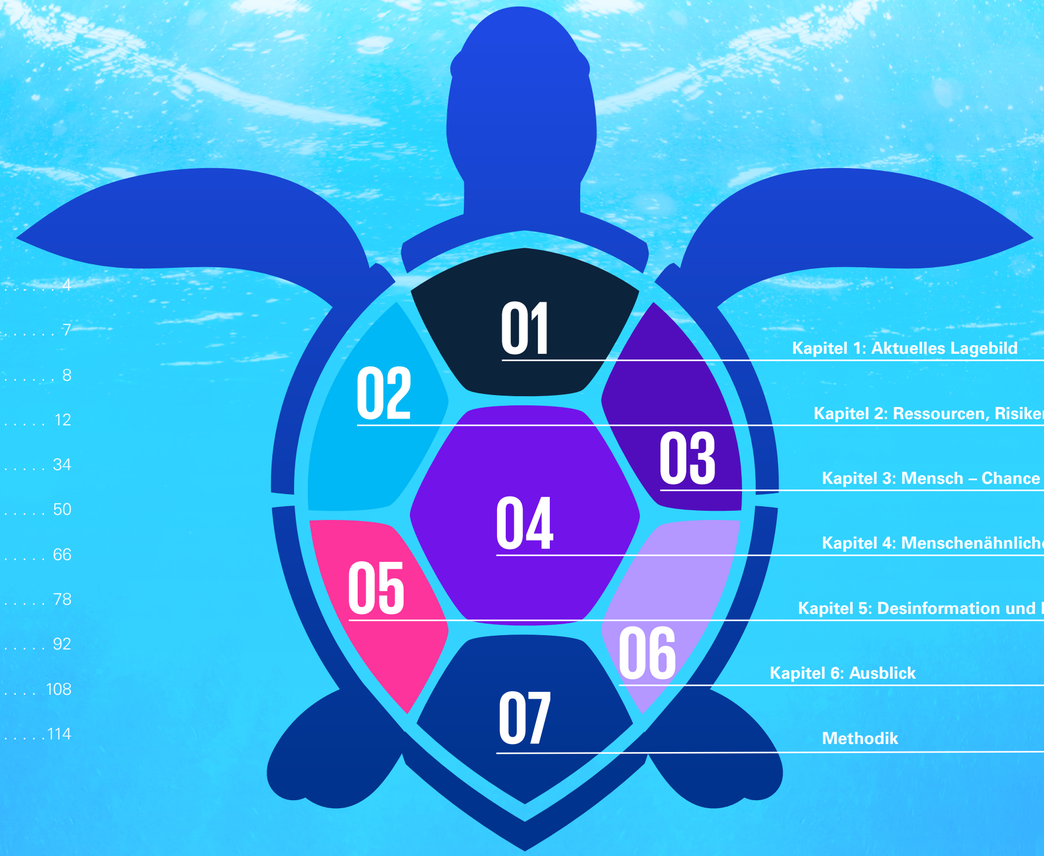
Cybersecurity in Österreich

Sicherheitsforum
Digitale Wirtschaft
Österreich

April 2024

kpmg.at/cyber

Inhaltsverzeichnis



Erfahren Sie mehr in unserem Podcast IMPULSE

Ins Netz gegangen

Mitarbeitende stehen nach wie vor im Fokus von Cyberangriffen. Auch in den letzten 12 Monaten hat sich eine Vielzahl von Angriffen direkt und gezielt gegen sie gerichtet. Social Engineering ist hierbei ein besonders gefährliches Einfallstor in die Systeme der Unternehmen. Am häufigsten haben die Befragten in diesem Kontext Beeinflussungsversuche über E-Mail-Nachrichten erlebt. Aber auch das Phänomen Deepfake in Form von Sprach- und Videonachrichten nimmt Fahrt auf und wird gezielt eingesetzt. Durch die von der Digitalisierung beschleunigten Möglichkeiten, Desinformationen zu verbreiten, steht die Integrität massiv auf dem Prüfstand.

Eine weitere alarmierende Entwicklung, die wir festgestellt haben: Jedes dritte Unternehmen hat zumindest einmal eine Lösegeldforderung in Zusammenhang mit Ransomwareangriffen bezahlt. An dieser Stelle muss klar gesagt werden, dass die Gefahr besteht, durch die Bezahlung für Trittbrettfahrer:innen attraktiv zu werden. Worst-Case-Szenario: Weitere Täter:innen versuchen, Angriffe gegen die betroffenen Unternehmen durchzuführen.

Langer Atem

Die Cybersecurity-Studie 2024 zeigt, dass sich auch die Aufsichtsrät:innen den Herausforderungen bewusst sind und dass Cybersicherheit für sie zu einem wichtigen Teil ihres Lebens geworden ist. Sie haben klar dafür Sorge zu tragen, dass der Unternehmensfortbestand – auch durch die digitalen Cybersecurity-Maßnahmen – gewährleistet wird.

Unternehmen brauchen einen langen Atem, um mit dem Tempo der aktuellen Cyberangriffe mitzuhalten. Dafür müssen sie in Sicherheitsmaßnahmen investieren und auch ihre Mitarbeitenden für den Ernstfall trainieren. So sorgen sie vor allem in Krisenzeiten für enorme Sicherheit.

Woran können wir jetzt aber festmachen, ob sich Investitionen in Cybersecurity auszahlen? Unternehmen, die unter die NIS fallen, müssen sich schon länger mit Cybersecurity beschäftigen und

> **Cyberangriffe zeigen uns ungeschminkt, dass Risiken, die andere für uns eingehen, auch unsere eigenen Risiken sind.**
>
> Robert Lamprecht

> **Unternehmen brauchen einen langen Atem, um mit dem Tempo der aktuellen Cyberangriffe mitzuhalten.**
>
> Michael Schirmbrand

erleben deshalb auch immer weniger kritische Schäden, die sie außer Gefecht setzen. Sie haben damit den Beweis bekommen, dass sich die Investitionen doch lohnen. Durch die NIS2 wird sich die Lage hoffentlich noch weiter verbessern, da sich jetzt noch mehr Unternehmen damit auseinandersetzen müssen.

Mit der Strömung

Wir erleben gerade den Lackmustest für unsere Sicherheitsmaßnahmen. Bestehen können wir nur, wenn wir es gemeinsam machen. Cyberangriffe zeigen uns ungeschminkt, dass Risiken, die andere für uns eingehen, auch unsere eigenen Risiken sind. Die NIS2 und DORA sind hier ein eindringlicher Aufruf der Regulatorik, dass Cybersicherheit nur gemeinsam funktionieren kann.

Bereits zum neunten Mal veröffentlichen wir in bewährter Kooperation mit dem Sicherheitsforum Digitale Wirtschaft des Kompetenzzentrum Sicheres Österreich (KSÖ) die Studie „Cybersecurity in Österreich“. Ein großer Dank geht an dieser Stelle an die zahlreichen Teilnehmenden, die an unserer Umfrage mitgewirkt und unsere Fragen beantwortet haben sowie an alle, die uns im Rahmen von Interviews unterstützt haben. Nur mit Ihrer Hilfe ist es möglich, die Cybersecurity-Studie erneut in diesem Umfang und in dieser Qualität zu veröffentlichen!

> **Cybersicherheit ist für Aufsichtsrät:innen zu einem wichtigen Teil ihres Lebens geworden, denn sie tragen die Verantwortung, den Unternehmensfortbestand durch digitale Sicherheitsmaßnahmen zu gewährleisten.**
>
> Andreas Tomek

Ob sich unsere Anstrengungen im Cyberozean bereits bezahlt gemacht haben und wo wir besser werden können, lesen Sie in unserer Studie. Wir wünschen Ihnen ein spannendes Eintauchen in die Erkenntnisse. Sollten Fragen offenbleiben, melden Sie sich gerne. Wir freuen uns von Ihnen zu hören!

Robert Lamprecht
KPMG Partner

Michael Schirmbrand
KPMG Partner

Andreas Tomek
KPMG Partner

Unsere Kooperationspartner

Vielen Dank an unsere Kooperationspartner für die Zusammenarbeit bei der Studie:

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.

KSÖ Kompetenzzentrum Sicheres Österreich

Sicherheitsforum Digitale Wirtschaft Österreich

Wir bedanken uns auch bei unseren Kooperationspartnern in den Bundesländern:

iv Industriellenvereinigung Kärnten

SILICONALPS

WKO Wirtschaftskammer Wien Information · Consulting

FH Salzburg

JOANNEUM RESEARCH

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

Cybersicherheit im Fokus

FOTO © EVA KELETY

Mag.
Michael Höllerer
Präsident des KSÖ

„Die Welt ist aus den Fugen geraten" – so beschreiben Sicherheitsexpert:innen und Analyst:innen die geopolitische Lage 2024. Zuletzt hat Ende Jänner 2024 das Bundesministerium für Landesverteidigung sein „Risikobild 2024" vorgelegt. Die acht von den Studienautor:innen definierten größten Risiken für Österreich reichen von den Auswirkungen militärischer Konflikte auf Österreich über Störungen der Lieferketten bis hin zu Cyberangriffen und Kämpfen in Computernetzwerken. Cyberangriffe dienen nicht mehr nur rein kriminellen Zwecken, der Erpressung von Lösegeld oder dem Absaugen von Daten. Sie sind vielmehr ein Instrument zur Durchsetzung politischer, wirtschaftlicher, strategischer oder militärischer Ziele geworden. Das kann die Störung von Lieferketten, die Einschränkung der Strategiefähigkeit eines Staates oder die Planung internationaler Desinformationskampagnen betreffen.

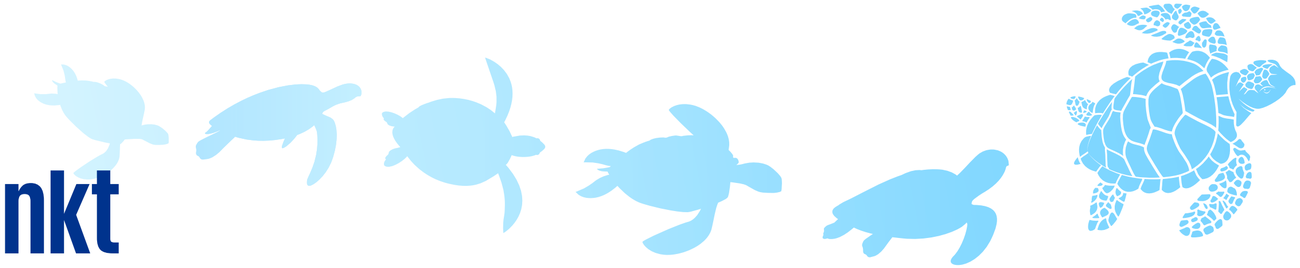
Die Nutzung von Künstlicher Intelligenz und die damit verbundenen neuen Angriffsmethoden und Angriffsvektoren erhöhen die Angriffspotenziale der Cyberkriminellen um ein Vielfaches. Erste Berichte über Opfer von Deepfakes mit Schadenssummen in Millionenhöhe sind bereits bekannt geworden.

Auch die Kriminalstatistik des Bundesministeriums für Inneres, die Ende März 2024 für das Jahr 2023 präsentiert wurde, bestätigt einen sich seit mehreren Jahren entwickelnden Trend: Cyberkriminalität steigt weiter an. Dies betrifft zum einen Cyberangriffe auf Unternehmen, Behörden oder Privatpersonen. Bedenklich sind zudem jene Entwicklungen, wo der Cyberraum zunehmend für „klassische" Kriminalitätsformen wie Betrug, Mobbing oder Erpressung genutzt wird.

Für uns im KSÖ bedeuten diese Entwicklungen, dass wir weiter und noch stärker auf die Zusammenarbeit und den Erfahrungsaustausch der Stakeholder in Österreich setzen. Die Ihnen vorliegende Studie von KPMG und KSÖ ist ein Beispiel dafür, welcher Mehrwert aus einer gemeinsamen Initiative entstehen kann – und das schon seit mittlerweile neun Jahren.

2024 werden wir wieder eine Reihe von Aktivitäten setzen, um gemeinsam mit unseren Partnern in Wirtschaft, Staat, Technologie und Forschung sowie in der Zivilgesellschaft daran zu arbeiten, Österreich ein Stück weit sicherer zu machen. Dazu zählen u. a. der KSÖ-Sicherheitsgipfel am 4. Juni 2024, der sich den Chancen und Risiken der KI widmen wird; ein internationales Cyber-Planspiel, das wir am 6. und 7. November 2024 gemeinsam mit dem AIT durchführen sowie eine Veranstaltung „Tag der Kritischen Infrastruktur", die wir gemeinsam mit dem BMI für die nationalen Unternehmen der Kritischen Infrastruktur im Herbst 2024 organisieren.

Die Integrität am Scheidepunkt



Die Wasseroberfläche wirkt ruhig, der Wellengang flach. Aber der Schein trügt und von Entspannung kann keine Rede sein, denn jeder sechste Cyberangriff ist erfolgreich.

Die Unternehmen sind augenscheinlich sensibilisiert und glauben, Angriffe gut wegstecken zu können. Bedeutet das jetzt, dass wir nichts mehr tun müssen? Ganz im Gegenteil: Tauchen wir tiefer in die Situation bei heimischen Unternehmen ein, so sehen wir, dass alle unsere Sicherheitsmaßnahmen gerade intensiv auf die Probe gestellt werden. Im Vergleich zum Jahr 2023 erleben wir zum einen eine signifikante Zunahme der Angriffe und zum anderen eine wesentliche Verschiebung in den Angriffsarten. Qualitativ hochwertigere Angriffe rücken in den Vordergrund.

Cyberangriffe vereinen aktuell zwei Komponenten: Sie werden erstens direkt gegen den Menschen durchgeführt. Unsere Studienergebnisse belegen, dass Mitarbeitende, die auf einen Cybersicherheitsvorfall reagieren müssen, großen Belastungen sowie psychischen und physischen Folgen wie Stress und Angst, Schlaflosigkeit, Schuldzuweisungen, Auswirkungen auf das soziale Leben / auf Beziehungen sowie Aggression ausgesetzt sind. Das schwächt wiederum das gesamte Unternehmen.

Die Angriffe sind zweitens gepaart mit verbesserten technischen Mitteln und Werkzeugen. Das wird durch den kombinierten Einsatz von Desinformationskampagnen und Deepfakes besonders deutlich. Desinformationskampagnen fungieren als Ablenkungsmanöver und versetzen Unternehmen in einen Ausnahmezustand. Währenddessen wird der eigentliche Cyberangriff unbemerkt ausgeführt. Das kann bis zur wirtschaftlichen Destabilisierung führen.

Ein ständiges Wettschwimmen

Wir befinden uns alle in einem Wettschwimmen. Die Kernfrage ist, ob wir in der vorderen oder in der hinteren Gruppe sind. Werden wir von den Raubtieren gefressen oder entkommen wir ihnen regelmäßig, weil immer jemand langsamer schwimmt und zuerst gefressen wird? Es zahlt sich also aus, in Sicherheitsmaßnahmen zu investieren, um in der vorderen Gruppe mitzuschwimmen. Vor allem bei größeren Unternehmen merken wir, dass es nicht mehr diesen Erklärungsbedarf gibt, warum Geld für Cybersecurity benötigt wird. Sie haben sich darauf eingestellt, dass sie Geld für Cybersicherheitsmaßnahmen ausgeben müssen und auch darauf, dass Cybersecurity ein laufender Prozess ist, der nicht einmal abgehakt und für die nächsten zehn Jahre erledigt werden kann. Wir sehen aber auch, dass kleinere Unternehmen, die sich diese Kosten nicht leisten können, ein Problem haben.

Unter NIS2 werden mehr Unternehmen fallen und dadurch wird sich hoffentlich auch der Security-Standard heben. Das sind aber nur ca. 2 Prozent der Unternehmen in Österreich. Damit wird es immer noch viel zu viele Ziele für die Angreifer:innen geben. Verlagern sich jetzt alle Angriffe auf kleine Unternehmen, die nicht unter NIS2 fallen und die weniger Budget für Cybersecurity haben? Dagegen spricht, dass es bei diesen auch weniger zu holen gibt. Gegen wen sich die Angriffe in Zukunft richten werden, bleibt abzuwarten. Gewiss ist, dass sich die Angreifer:innen andere Ziele suchen werden. Die Kernfrage lautet, ob wir es schaffen, unser Security-Level so weit zu erhöhen, dass sich die Täter:innen Ziele außerhalb Europas suchen.

Kein Gewohnheitsrecht im Cyberozean

Wir dürfen nicht den Fehler machen, uns nur auf die am häufigsten vorkommenden Angriffsarten zu fokussieren, unsere Systeme gegen diese abzusichern und uns dann in falscher Sicherheit zu wiegen. NIS2 und DORA gehen klar einen Schritt weiter. Wir können nicht pauschal sagen, dass, wenn wir gegen bspw. Angriffsart „XYZ" abgesichert sind, wir dann gut unterwegs oder besser als der Durchschnitt sind. Denn schon die Vorschriften um uns herum verlangen wesentlich mehr. Da ist es dann egal, ob wir besser sind als der Durchschnitt.

Es ist gefährlich zu glauben, dass nur weil eine Sache bis dato funktioniert hat, sie auch so gemacht werden sollte. Wenn man regelmäßig150 km/h fährt und niemals aufgehalten wird, beginnt man zu glauben, dass die Geschwindigkeit angemessen ist. Und dann ist man überrascht, wenn eines Tages doch ein Strafzettel kommt. Aber die Sache ist die: Es war immer schon verboten, auch wenn man bis jetzt nicht erwischt worden ist. Es gibt kein Gewohnheitsrecht. Auch Unternehmen haben kein Gewohnheitsrecht auf Cybersecurity-Maßnahmen. Die Maßnahmen müssen immer wieder neu evaluiert und angepasst werden – sonst erwischen uns irgendwann die Täter:innen.

Wohin wir schwimmen

Es ist wesentlich, dass wir mit unseren Maßnahmen in die richtige Richtung arbeiten und den Fokus auf die entscheidenden Themen setzen. Das Schlüsselproblem ist nicht mehr, wodurch wir bedroht werden, sondern was wir dagegen tun sollen. Nicht, dass es nicht auch wichtig ist, zu wissen, was uns bedroht. Aber es muss ein Abgleich stattfinden, ob wir noch am richtigen Weg sind bzw. in den richtigen Bahnen vorwärts schwimmen.

Sich anpassen

Der verstärkte Einsatz von Künstlicher Intelligenz (KI) sowohl auf Unternehmens- als auch auf Täter:innenseite ist ein Beispiel dafür, dass wir unsere Cybermaßnahmen immer wieder neu evaluieren müssen. Viele der befragten Unternehmen glauben, dass KI zwar die Cybersicherheit verbessern kann, aber es herrscht auch Beunruhigung darüber, dass KI von Angreifer:innen genutzt wird. Durch die technologischen Möglichkeiten von z. B. Künstlicher Intelligenz und Deepfakes ist es immer einfacher geworden, unsere bisherigen Sinne und Erfahrungswerte auszutricksen.

Dadurch passiert auch eine Verschiebung in der CIA-Triade: Zwar haben wir immer noch ein Confidentiality (C)-Problem durch Dataleaks etc., aber da wissen wir, wie wir uns verhalten müssen. Wir können es eindämmen. Nach wie vor exis-

tiert ein Availability (A)-Problem dank Ransomware, aber auch hier wissen wir nach und nach, was zu tun ist mit Back-up und vielen anderen Maßnahmen. Aber: Wir haben ein Integrity (I)-Problem und wir wissen nicht, wie wir damit umgehen sollen.

Schillernde Oberfläche

Die Integrität steht am (Wasser-) Scheidepunkt. Was können wir noch glauben und nehmen wir überhaupt noch etwas für bare Münze? Wir sind bereits darauf trainiert, hinter jeder Information eine Verschwörungstheorie zu vermuten. Das ist eine Problematik, die mit der Digitalisierung gekommen ist.

Bis vor ein paar Jahren war das noch kein Thema. Das Risiko, dass Angreifer:innen unsere Daten manipulieren, wirkte unwahrscheinlich und wenig lukrativ. Dass jemand z. B. in eine Bank eindringt und die Kontodaten verändert, schien in neun von zehn Fällen in Spielfilmen zu passieren und einmal in der Realität. Wer schaut sich nach einem Ransomware- oder Cybersicherheitsvorfall auch die Integrität der im System befindlichen Daten vollständig an? Wann rechnet man damit, dass Daten manipuliert werden – und das schon lange bevor Ransomware überhaupt ausgelöst wird?

Mittlerweile sind wir aber durch unsere Abhängigkeit von der Digitalisierung in diesem Bereich deutlich verwundbarer geworden. Das fängt bereits in kleinem Maßstab mit dem Enkeltrick oder dem „Hallo Mama, hallo Papa"-Trick an. Und wir haben bestimmt auch noch nicht den Zenit erreicht. Wie stellen wir in Zukunft sicher, dass wir z. B. tatsächlich mit unseren Kindern am Telefon sprechen? Früher galt der Tipp, wenn man eine verdächtige Nachricht erhalten hat, die Person anzurufen. Aber mittlerweile kann die Stimme durch Deepfakes simuliert werden. Deepfakes haben sich im letzten Jahr mit einer Zunahme um 119 Prozent bei den Unternehmen mehr als verdoppelt und die Sorge über Desinformation ist groß. 54 Prozent waren in den letzten 12 Monaten Opfer von Desinformationskampagnen.

> **Die Schildkröte hat einen Panzer entwickelt, um sich vor Feinden zu schützen. Entwickeln auch wir uns weiter und lernen wir unsere Sinne zu schärfen.**
>
> Robert Lamprecht

Cybersecurity als Anker

Auf technischer Seite haben wir die Integritätskomponente immer schon in der Cybersecurity als Schutzziel mitgedacht. Bis jetzt haben wir sie aber unter „ferner liefen" abgehandelt. Wir haben zwar anerkannt, dass auch sie abgesichert werden muss, haben uns aber auf die größeren Baustellen konzentriert. Momentan wird alles über Zertifikate geregelt, was auch nicht perfekt funktioniert und mühsam ist.

Wir müssen uns jetzt fragen, welchen Beitrag die Cybersecurity-Community leisten kann, um dieses eigentlich stark soziale Thema auch auf technischer Seite zu lösen. Warum ist Phishing bspw. noch immer so eine große Herausforderung und warum lässt sich nicht zuverlässig und einfach prüfen, ob die Person, die mir gerade schreibt, legitim und authentisch ist – Stichwort: Challenge Evil Within Trusted? Wer kann garantieren, dass die Informationen, die ich erhalte oder die Personen, die ich in einer Videokonferenz sehe, echt sind? Müssen wir zuerst die Bestätigung von einer Handvoll Menschen einholen, dass die Person am anderen Ende echt ist? Und wer erklärt sich überhaupt noch dazu bereit, die Echtheit zu bestätigen?

(Un)Geschärfte Sinne

Angetrieben durch die Digitalisierung wird es also erforderlich zu prüfen, welche Informationen tatsächlich wahr sind. Zwar haben wir noch keinen eindeutigen Nachweis dafür, dass sich durch Desinformationskampagnen viel Geld verdienen lässt. 2024 wird aber ein Superwahljahr und damit rücken Falschinformationen und Deepfakes noch einmal mehr ins Zentrum. Ursprünglich echte Informationen können im Laufe der Zeit verändert werden. Auch können absichtlich falsche Informationen produziert werden – siehe Fake News. Die Phänomene Fake News und Rufschädigung wurden auch von unseren Befragten als für sie am herausforderndsten eingestuft. Im Vergleich zum Vorjahr sind sie um drei Plätze nach oben gewandert. Eine dritte Möglichkeit ist die Verbreitung, dass eigentlich wahre Informationen nicht der Wahrheit entsprechen würden, was wir z. B. im Rahmen von Verschwörungstheorien erleben.

Wir wissen folglich nicht mehr, wie weit wir den digitalen Informationen, von denen wir mittlerweile abhängig sind, noch trauen können. Wahrscheinlich konnten wir ihnen noch nie trauen. Nur war das bis jetzt noch nicht so ein großes Problem, weil sich die Angreifer:innen ein anderes, lohnenderes Ziel gesucht haben. Das verschiebt sich gerade.

Wir haben noch kein Sensorium für Falschinformationen im digitalen Bereich entwickelt. Bis jetzt haben wir das in der Menschheitsgeschichte auch nicht gebraucht. Im echten Leben sind wir schon weiter. Wenn ein Mensch vor uns steht und zu schwitzen beginnt, wenn er uns eine Geschichte erzählt, dann wissen wir, dass er lügt. Im digitalen Bereich fehlt uns dieser Hinweis. Wir können nicht wissen, ob am anderen Ende die Temperaturen gerade ansteigen oder ob die Maschine zu vibrieren beginnt. Wir sehen die (digitalen) Schweißperlen auf der Stirn der Angreifer:innen nicht.

Die nächste Stufe der Evolution

Daraus lassen sich jetzt drei wesentliche Erkenntnisse ableiten: Erstens, die Angreifer:innen prüfen aktuell sehr intensiv unsere Sicherheitsmaßnahmen. Zweitens, Angriffe werden diffizil und schwieriger festzustellen. Drittens, der Mensch rückt als Ziel immer stärker in den Mittelpunkt, im Vergleich zum letzten Jahr sogar noch deutlicher.

Im Cyberozean ist nicht immer alles, wie es scheint, und oft unterliegen wir Trugschlüssen. Unsere Sinne sind dahingehend noch nicht ausgeprägt. Die Schildkröte hat einen Panzer entwickelt, um sich vor Feinden zu schützen. Nehmen wir sie zum Vorbild: Entwickeln auch wir uns weiter und lernen wir unsere Sinne zu schärfen. Schützen wir uns gemeinsam vor den digitalen Raubtieren.

Robert Lamprecht
KPMG Partner

Ein Jahr danach

Im Jahr 2023 haben wir unsere Interviewpartner:innen gefragt:

„Wenn wir uns in einem Jahr wieder treffen, was würden wir uns dann wünschen, heute schon getan zu haben?“

Wie hat sich die Lage in den letzten 12 Monaten verändert? Ist das eingetreten und passiert, was wir uns gewünscht haben? Was sagen unsere Interviewpartner:innen heute?

FOTO © SCHREINER

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

Der Status quo ante im Ausbildungsbereich ist unverändert: Es fehlen in den Bildungsdirektionen weiterhin die direkten Ansprechpartner:innen bzw. Verantwortliche für die einzelnen Schultypen sowie ein regelmäßiger, strukturierter Austausch.

Konzertierte Schulentwicklung? Nein! Weiterentwicklung an den individuellen Standorten? Ja!

FOTO © STADT WEIZ

Andreas Lehofer
Abteilungsleiter IT
Stadtgemeinde Weiz

Bei uns entwickeln sich die Dinge aktuell positiv. Wir setzen auf mehrere Säulen in der Cybersecurity. Einerseits bekommen wir aktuell das Budget zur Verfügung gestellt, um uns technisch weiterzuentwickeln und andererseits rückt Cybersecurity immer mehr ins Bewusstsein unserer Dienstnehmer:innen.

Wir führen aktuell gerade eine Phishingkampagne durch und starten zusätzlich noch eine Awareness-Kampagne, um unsere Dienstnehmer:innen noch ein Stück weiter zu sensibilisieren.

FOTO © PRIVAT

DI Christina Schindlauer
Specialist Cyber Threat Intelligence
EC3 - Europol

Ein Jahr nach unserem Gespräch bleibt der notwendige kontinuierliche Fokus auf die Themen IT- und Cybersicherheit unerlässlich. Wir dürfen nicht nachlassen in unseren Bemühungen, da die Bedrohungen und Akteur:innen zunehmend vielfältiger werden. Neben technischen Sicherheitsmaßnahmen ist die Förderung von Cyberkompetenzen nicht nur bei Mitarbeiter:innen, sondern insbesondere im Managementbereich entscheidend, um wesentliche Fortschritte zu erzielen.

In diesem Zusammenhang wird die Bedeutung von Cybersicherheit und Cyberprävention als wesentliche Schwerpunkte noch deutlicher. Nur durch kontinuierliche Aufmerksamkeit und Engagement können wir hoffen, den Herausforderungen einer sich ständig wandelnden und wachsenden digitalen Landschaft effektiv zu begegnen und eine sicherere, informiertere Gesellschaft zu fördern.

FOTO © FOTOSTUDIO HRUBY GMBH ZELTWEG

HR Dir. Mag. Herbert Giegerl
Schulleiter HAK Tamsweg

Das vergangene Jahr war für unseren Ausbildungszweig „Sicherheitsmanagement & Cyber Security“ sehr ereignisreich. Die beiden Ministerien (BM.I und BMBWF) haben ihre Kooperation intensiviert und dadurch positive Impulse gesetzt. Das Bundeskriminalamt koordiniert die Zusammenarbeit mit den verschiedenen Abteilungen des BM.I, die ihr Fachwissen an die Schüler:innen weitergeben. Auch Expert:innen aus der Privatwirtschaft unterstützen die Schüler:innen mit ihrem Know-how.

Im schulischen Bereich gibt es aktuell zwei Handelsakademien, die den Schulversuch durchführen dürfen. Ab dem Schuljahr 2024/25 kommt eine weitere HAK hinzu. Die Qualität der Ausbildung steht bei allen drei Standorten im Vordergrund. Gemeinsam werden langfristige Konzepte für die Fort- und Weiterbildung entwickelt. Die steigende Zahl von Cyberangriffen erfordert eine kontinuierliche Anpassung der Lehrinhalte. Nur so können wir unseren Absolvent:innen weltweit attraktive Jobperspektiven bieten und gegen Cyberkriminalität bestehen.

FOTO © HTL PINKAFELD

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

Die Kommunikationswege mit den diversen Bildungseinrichtungen haben sich in den letzten Monaten wesentlich positiv entwickelt. Es gab auf mehreren Ebenen Personalwechsel bzw. -rochaden, die es (etwas) erleichtern, verschiedenste Dinge in Bezug auf Security zu verbessern.

Das bedeutet, dass das Thema rund um Security zumindest rudimentär angekommen ist und verstärkt durch Berichte in den Medien, die verschiedenste Sicherheitsmängel in den Firmen aufgezeigt haben, auch aufgeschlagen ist. Daher sehe ich eine zumindest teilweise Awareness zum Thema Security in den Köpfen dieser oben genannten Personen: Der Weg ist das Ziel – ein erster wichtiger Schritt ist aus meiner heutigen Sicht getan! Weitere Schritte werden/müssen folgen… ich bin zuversichtlich!

FOTO © PRIVAT

Mag. Elisabeth Huber
Stadtamtsleiterin
Stadtgemeinde Spittal an der Drau

In diesem Jahr ist – Gott sei Dank – nichts passiert! Von einem weiteren Hackerangriff oder -versuch sind wir verschont geblieben! Seitens der Stadtgemeinde wurden keine weiteren Dispositionen und Anschaffungen getätigt.

Derzeit versuchen wir uns mit Sicherheitsmaßnahmen unserer IT-Abteilung zu schützen und es gibt laufend Informationen an die Mitarbeiter:innen über verdächtige Mails oder Anhänge. Über den Abschluss einer Cyberversicherung wird noch diskutiert.

FOTO © PHILIPP MONIHART

Dr. Walter Leiss
Generalsekretär
Österreichischer Gemeindebund

Wenn wir uns in einem kalten Cyberkrieg mit Russland befinden würden, würden wir uns wünschen, dass wir bereits auf Bundes-, Landes- und Gemeindeebene unsere fortschrittlichen Cyberverteidigungssysteme nutzen könnten, über robuste Sicherheitsprotokolle verfügen und auf die starke internationale Zusammenarbeit zur Bewältigung von Cyberbedrohungen setzen könnten.

In den Gemeinden wären wir dankbar, bereits für eine gut etablierte und gesicherte digitale Infrastruktur gesorgt zu haben sowie unsere lokalen Behörden so weit ausgestattet zu haben, dass sie sich mit entsprechenden Ressourcen und dem nötigen Know-how gegen Cyberangriffe verteidigen können, um ihre Bürger:innen zu schützen.

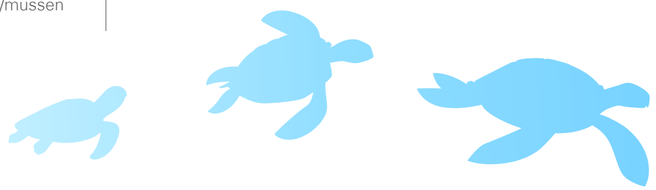


FOTO © KATHARINA SCHIFFL

Mag. Caroline Schmidt M.A., MAS
Programmdirektorin
Bundesministerium für Inneres

Vor einem Jahr habe ich die geringe Zahl an weiblichen Arbeitskräften im Bereich Cybersicherheit adressiert, mich für mehr Frauen in diesem Bereich ausgesprochen und mit Zuversicht in die Zukunft geblickt. Das letzte Jahr hat gezeigt, dass wir noch aktiver werden müssen. Der Anteil von Frauen im Cybersicherheitsbereich ist leicht gestiegen, aber da ist noch Luft nach oben. Wir müssen unsere Bemühungen intensivieren. Ich denke, Cybersicherheit wird nach wie vor mit rein technischen Inhalten assoziiert.

Dabei ist Cybersicherheit ein sehr breiter und abwechslungsreicher Bereich. Dieses Missverständnis muss aktiv angegangen werden, um dem Fachkräftemangel entgegenzuwirken. Was den Frauenanteil in Cybersicherheit betrifft, ist es, denke ich, wichtig aufzuzeigen, dass es bereits, wenn auch leider wenige, Frauen in dem Bereich gibt. Andere Frauen und Mädchen können sich dadurch stärker mit dem Berufsfeld Cybersicherheit identifizieren. Trotz des umfassenden Handlungsbedarfs blicke ich weiterhin optimistisch in die Zukunft und hoffe, dass in 12 Monaten die prognostizierten Fortschritte übertroffen wurden.

FOTO © BMI/GERD PACHAUER

DI Philipp Blauensteiner, MA
Abteilungsleiter Netz- und
Informationssicherheit
Bundesministerium für Inneres

Wir haben gerade einen Gesetzesentwurf für die neue NIS2-Richtlinie in Begutachtung. Im BMI wird eine Gruppe „Nationales Cybersicherheitszentrum“ aufgebaut. Wir konnten uns seit letztem Jahr personell um ein Drittel vergrößern – was allerdings auch nur ein erster Schritt ist.

Wir haben einen großen Beteiligungsprozess initiiert; eine Arbeitsgruppe in der Cyber Sicherheit Plattform (CSP) ins Leben gerufen, um inhaltlich die künftigen Risikomanagement-Maßnahmen zu diskutieren; eine „Österreichrundfahrt“ gestartet, um auch in den Bundesländern präsent zu sein, NIS-2 vorstellen zu können und Fragen zu beantworten. Ich würde also sagen: Es ist viel geschehen. Nun läuft die Begutachtung und wir erwarten den parlamentarischen Prozess. Es gilt nun auch für uns, die zahlreichen Pläne auch tatsächlich umzusetzen. Dies wird die große Herausforderung für das nächste Jahr werden.

FOTO © BMI/GERD PACHAUER

Oberrat Mag. Gernot Goluch
Stv. Abteilungsleiter Netz-
und Informationssicherheit /
Referatsleiter Recht & Audit
Bundesministerium für Inneres

Übersicht Key Findings

Die Top 5 Angriffsarten waren (Spear-)Phishingattacken (87 %), Malware (86 %), Business-E-Mail-Compromise / CEO-/CFO-Fraud (80 %), Social Engineering (62 %) und Denial-of-Service-Attacken (54 %).

6. Jeder sechste Cyberangriff gegen ein Unternehmen war erfolgreich.

54 % der befragten Unternehmen waren in den letzten 12 Monaten Opfer von Desinformationskampagnen, wobei 42 % sogar mehrmals Ziel waren.

33 % Jedes dritte Unternehmen hat zumindest einmal die Lösegeldforderung im Zusammenhang mit einem Ransomwareangriff bezahlt.

66 % haben Bedenken, dass Cyberangriffe gegen ihre Dienstleister Auswirkungen auf sie selbst haben werden.

33 % der Aufsichtsrät:Innen haben angegeben, dass Cybersicherheit für sie zu einem wichtigen Teil ihres Lebens geworden ist.

+119 % Deepfakes haben sich in Österreich mit einer Zunahme um 119 % mehr als verdoppelt.

+11 % Desinformation wird von den Unternehmen als große Herausforderung gesehen. Sie hat in den letzten 12 Monaten den höchsten Zuwachs erfahren und ist um drei Plätze nach oben geklettert.

37 % der Befragten würden bevorzugt Security-Lösungen von österreichischen Unternehmen einsetzen, ein Aufwärtstrend im Vergleich zum Vorjahr.

63 % Die dominantesten psychischen Auswirkungen für diejenigen, die bei einem Cybersicherheitsvorfall involviert waren, waren Stress und Angst.

33 % der Unternehmen haben Bedenken, dass Unternehmensdaten für Dritte durch KI zugänglich werden könnten.

56 % Mehr als die Hälfte hatte bei der Bearbeitung eines Sicherheitsvorfalls Unterstützung durch einen externen Dienstleister in Form eines Retainers.

-27 % Ransomwareangriffe sind um 27 % zurückgegangen.

+119 % Deepfakes haben sich in Österreich mit einer Zunahme um 119 % mehr als verdoppelt.

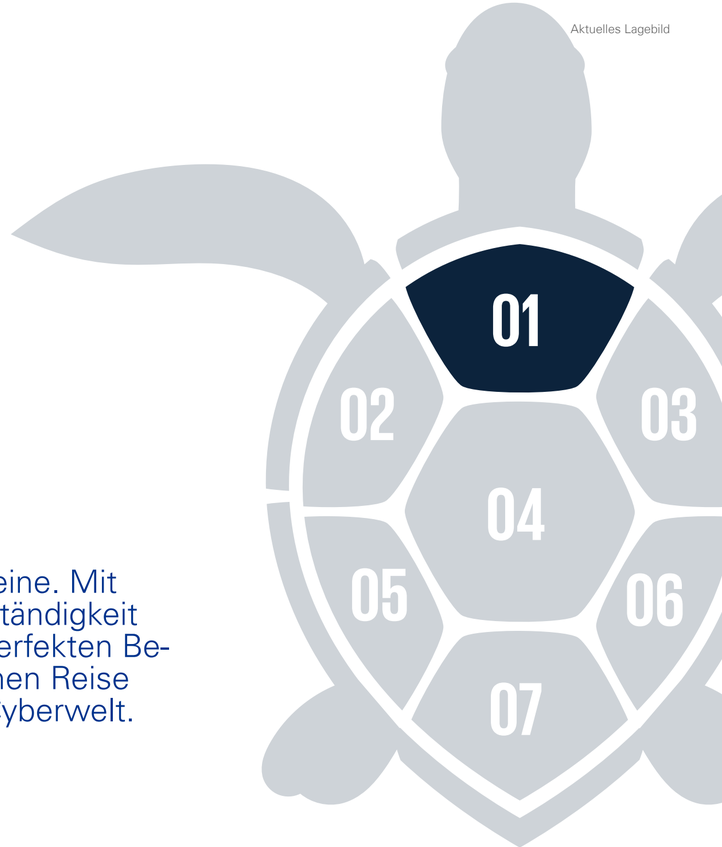
-41 % Denial-of-Service (DoS)-Attacken sind um 41 % zurückgegangen.

33 % Jedes dritte Unternehmen hat zumindest einmal die Lösegeldforderung im Zusammenhang mit einem Ransomwareangriff bezahlt.

01

Aktuelles Lagebild

Schildkröten sind wahre Urgesteine. Mit ihnen werden Weisheit und Beständigkeit assoziiert. Das macht sie zum perfekten Begleiter auf unserer abenteuerlichen Reise durch die rauen Gewässer der Cyberwelt.



Gemeinsam mit unserer Cyberschildkröte werfen wir zunächst einen Blick in die Vergangenheit und schauen, wie es den Unternehmen in den letzten 12 Monaten in puncto Cybersicherheit ergangen ist.

Hohe Eintrittswahrscheinlichkeit

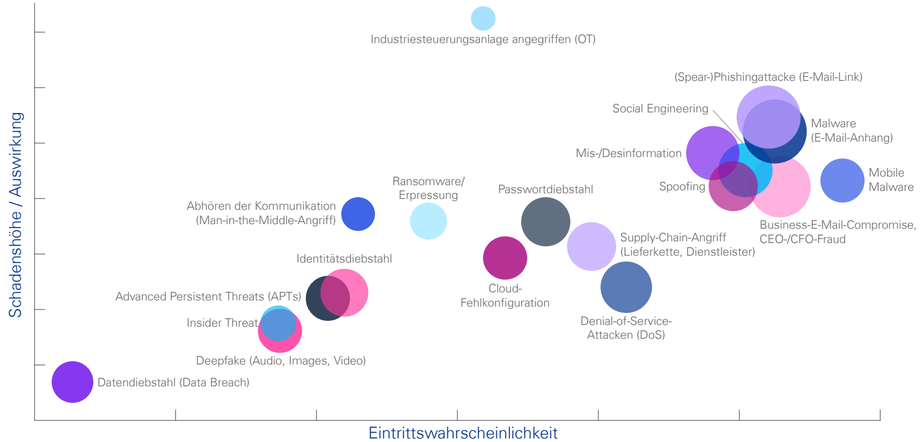
Gerade im Bereich der breitenwirksamen Angriffe erleben wir eine gewisse Konzentration. Damit sind Angriffe gemeint, die eine große Masse an Personen erreichen, wie zum Beispiel Phishing, Malware, Spoofing, Social Engineering, Business-E-Mail-Compromise, Mobile Malware sowie Mis- und Desinformation. Die Eintrittswahrscheinlichkeit dieser Angriffe war in den letzten 12 Monaten sehr hoch. Obwohl ihre Auswirkungen nicht exorbitant waren, haben sie dennoch für wesentliche Schäden bei Unternehmen gesorgt.

Mittlere Eintrittswahrscheinlichkeit

Im Mittelfeld finden wir zielgerichtete, fokussierte und komplexere Angriffe. Besonders auffällig dabei ist, dass Ransomware einen leichten Rückgang verzeichnet. Die Auswirkungen sind dennoch spürbar, Unternehmen haben aber gelernt, mit diesen umzugehen. Im gleichen Bereich befinden sich Cloud-Fehlkonfigurationen – also falsch eingestellte Sicherheitsparameter bei Cloud-Systemen, die zu unerlaubten Zugriffen führen –, Passwortdiebstahl, Angriffe gegen die Lieferkette und Denial-of-Service-Attacken. Besonders überraschend ist, dass verstärkt Angriffe auf die Lieferkette mit einer durchwegs hohen Eintrittswahrscheinlichkeit stattgefunden haben. Die Auswirkungen haben hingegen noch nicht den Zenit erreicht.

Angriffe auf Industriesteuerungsanlagen (OT-Systeme) sind heuer ein Ausreißer. Deren Eintrittswahrscheinlichkeit liegt im mittleren Bereich, die Auswirkungen können jedoch signifikante Schäden und Beeinträchtigungen mit sich bringen. Durch die Konvergenz zwischen IT und OT erleben wir mehr solcher Angriffe mit wesentlich spürbaren Auswirkungen. Aufgrund der Tatsache, dass OT-Systeme für Lebenszyklen von mehr als zehn Jahren ausgelegt sind, ist auch ein Austausch dieser Systeme im Rahmen des Produktlebenszyklus schier undenkbar. Hier sind jedenfalls die Hersteller gefordert (die Europäische Union wirkt bereits u. a. mit dem Cyber Resilience Act entgegen), Sicherheitsupdates bereitzustellen und im Zusammenwirken mit den Unternehmer:innen für hinreichende Sicherheit bei Industriesteuerungsanlagen zu sorgen.

Abb. 1: Eintrittswahrscheinlichkeit und Auswirkungen von Cyberangriffen in den letzten 12 Monaten



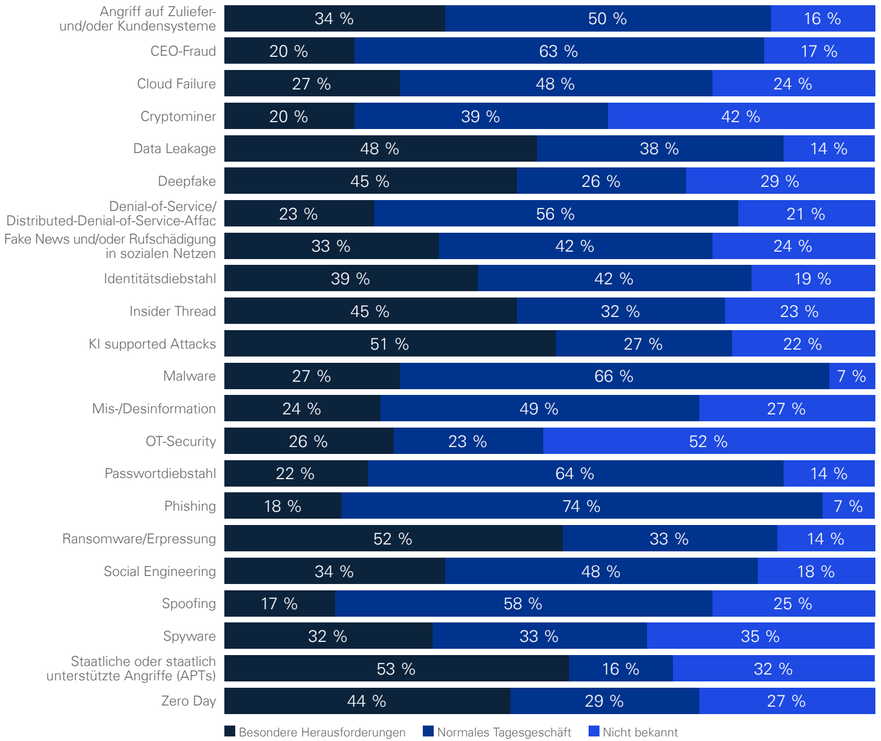
Geringe Eintrittswahrscheinlichkeit

Im unteren Bereich finden wir Angriffe, die besonders zielgerichtet sind und durchaus erhöhten Aufwand erfordern. Das sind unter anderem Advanced Persistent Threads, also Angriffe, die von staatlichen oder staatlich unterstützten Organisationen ausgehen, Insiderbetrug, da hier vor allem Kenntnisse über die internen Abläufe verfügbar sein müssen, Deepfakes, also die Vorspiegelung falscher Tatsachen im Rahmen von künstlich generierten Bildern, Audiodateien und Videos, der Identitätsdiebstahl und als Schlusslicht der Data Breach.

Angriffstaktik Ablenkung

Es zeigt sich jedenfalls, dass wir in den letzten Monaten massive Veränderungen erlebt haben. Sprachen wir in der Vergangenheit noch vorrangig von Ransomware als dem Phänomen, das die heimische Wirtschaft nachhaltig beeinträchtigt, so sehen wir jetzt, dass Angreifer:innen ihre Taktik

Abb. 2: Besondere Herausforderung vs. normales Tagesgeschäft



verändert haben und nun zielgerichtet Informationsbeeinflussung von Staaten betreiben. Diese werden durch Künstliche Intelligenz und weitere technologische Errungenschaften beschleunigt und können so zur Destabilisierung und in weiterer Folge zur Beschädigung unserer Systeme eingesetzt werden.

Wir dürfen allerdings nicht vergessen, dass Desinformationsangriffe in erster Instanz als Ablenkung zu verstehen sind. Sie haben zum Ziel, die Glaubwürdigkeit an die uns dargestellten Informationen zu erschüttern, uns in unseren Grundfesten zu beeinträchtigen und so die Aufmerksamkeit auf ein komplett anderes Thema im Feld zu lenken. Diese pure Ablenkung schafft es, die Kräfte und Ressourcen in Unternehmen zu binden, um so in deren Windschatten einen zielgerichteten Cyberangriff durchzuführen. Welche Konsequenzen damit verbunden sind, werden wir in den nächsten 12 Monaten verstärkt sehen. Vor allem die geopolitischen Ereignisse, die zunehmend schwierigen wirtschaftlichen Bedingungen in den USA, aber auch die veränderten geopolitischen Machtverhältnisse führen dazu, dass dieser Bereich einen besonderen Aufschwung erfährt. Fakt ist auch, dass der Cyberraum im Rahmen der aktuell geführten Konflikte zwischen den unterschiedlichsten Konfliktparteien eine nicht unwesentliche Komponente darstellt. Unternehmen sind gefordert, auch diesen Raum aktiv zu beobachten. Denn es ist durchaus schon mit einfachen Mitteln und ohne viel Aufwand möglich, Unternehmen zu destabilisieren und in weiterer Folge Manipulationen von Unternehmenswerten und Börsenkursen herbeizuführen.

Besondere Herausforderung vs. Normales Tagesgeschäft

Staatliche oder staatlich unterstützte Angriffe (APTs) werden von Unternehmen am stärksten als besondere Herausforderung empfunden (53 Prozent). An zweiter Stelle finden wir Ransomware/Erpressung (52 Prozent) und an dritter Stelle KI-unterstützte Angriffe (51 Prozent). Hier merken wir, dass Deepfakes und KI immer mehr Aufmerksamkeit fordern: APTs sind zwar nach wie vor dominant, aber die neuen Technologien rund um KI und Deepfakes sind bereits inmitten der Unternehmen angekommen.

Hingegen zählt für die Unternehmen Phishing mit 74 Prozent zum ganz normalen Tagesgeschäft. Auf Platz zwei befindet sich Malware mit 66 Prozent, dicht gefolgt von Passwortdiebstahl (64 Prozent). Vergleichen wir das mit den häufigsten Angriffsarten, von denen Unternehmen in den letzten 12 Monaten betroffen waren: (Spear-)Phishingattacken waren auf dem ersten Platz, Malware auf Platz zwei. Es ergibt also Sinn, dass genau diese beiden Angriffsarten von den Unternehmen am stärksten als normales Tagesgeschäft eingeschätzt werden. An dritter Stelle waren Unternehmen im letzten Jahr mit Business-E-Mail-Compromise bzw. CEO-/CFO-Fraud konfrontiert. CEO-Fraud wird mit 63 Prozent ebenfalls hoch als normales Tagesgeschäft eingestuft (siehe Abb. 2).

Abenteuer Cyberspace

Cyberangriffe sind in Österreich bereits auf einem sehr hohen Niveau

Abb. 3: Herkunft der Angriffe

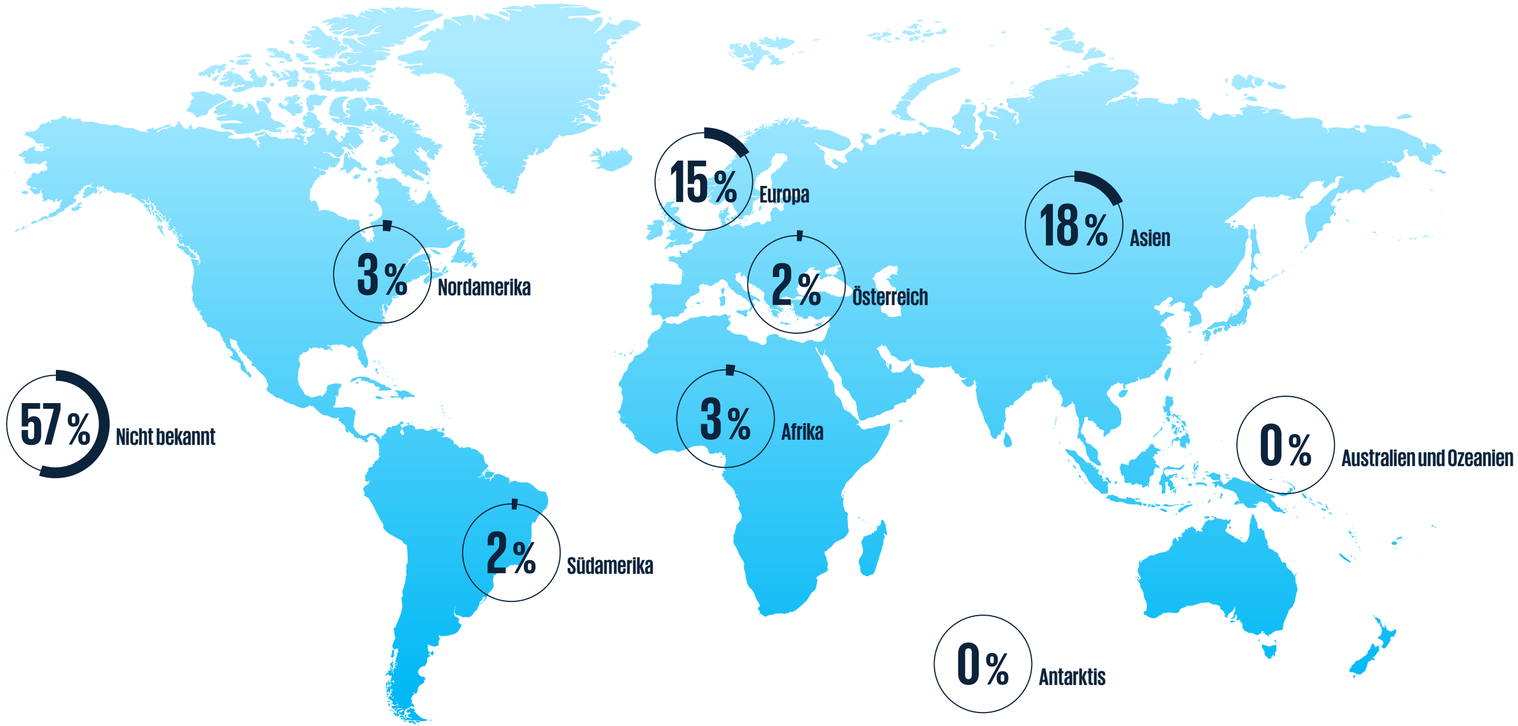
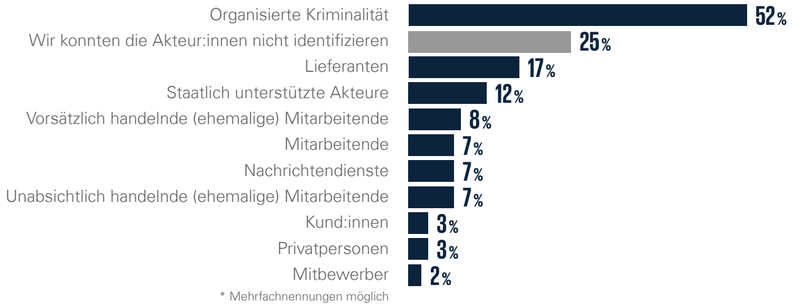


Abb. 4: Täter:innengruppen*



* Mehrfachnennungen möglich

und haben Unternehmen auch im Vorjahr massiv beschäftigt. Ob wir uns auf diesem Niveau einpendeln, bleibt abzuwarten. Vorerst zeichnet sich aber noch keine Entspannung der Lage für heimische Unternehmen ab.

32 Prozent der Befragten haben eine (starke) Zunahme der Anzahl an Cyberattacken gegen ihr Unternehmen festgestellt. Bei 36 Prozent ist die Anzahl gleichgeblieben. Die besorgniserregende Entwicklung: Jeder sechste Cyberangriff gegen ein Unternehmen war in den letzten 12 Monaten erfolgreich. Zum Vergleich war in unserer Studie 2023 noch jeder zehnte Angriff von Erfolg gekrönt. Die Trefferquote hat sich somit für die Angreifer:innen erhöht. 15 Prozent wissen nicht, ob es erfolgreiche Cyberangriffe gegen ihr Unternehmen gab.

Verstreut in allen Weltmeeren

Die organisierte Kriminalität im Cyberraum wird zum größten Problem für Unternehmen. Werfen wir einen Blick darauf, von welchen Akteur:innen die Attacken ausgehen, so sehen wir, dass die meisten Angriffe (52 Prozent) aus dem Umfeld der organisierten Kriminalität kommen. Auf dem zweiten Platz befinden sich die Lieferanten mit 17 Prozent und auf dem dritten Platz staatlich unterstützte Akteur:innen mit 12 Prozent. Einem Viertel der Unternehmen (25 Prozent) ist es nicht gelungen, die Angreifer:innen zu identifizieren.

Es verwundert, dass Lieferanten bereits den zweiten Platz einnehmen und somit genau zwischen der organisierten Kriminalität und staatlich unterstützten Akteur:innen stehen. Wenn Angriffe entlang der Lieferkette – zu der Lieferanten zählen – an Bedeutung gewonnen haben, bedeutet das auch, dass das bisherige Credo, dass Cybersicherheit nur gemeinsam funktionieren kann, auf eine sehr unangenehme Art und Weise torpediert wird. Gerade in diesem Bereich ist die Zusammenarbeit ein wichtiger Punkt und wir müssen uns fragen, ob wir gleichzeitig Freund und Feind im eigenen Haus haben (siehe Abb. 4).

Mehr als die Hälfte der Unternehmen (57 Prozent) konnte nicht feststellen, aus welcher Region die Angriffe gekommen sind. Jene Angriffe, die zurückverfolgt werden konnten, kamen an erster Stelle zu 18 Prozent aus Asien, dicht gefolgt von Europa mit 15 Prozent. Lediglich zwei Prozent der nachverfolgbaren Angriffe kamen aus Österreich selbst. Einmal mehr zeigt sich, dass Cyberangriffe über alle Ländergrenzen hinausgehen und so gut getarnt sind, dass es immer schwieriger wird, ihre Herkunft zu identifizieren (siehe Abb. 3).

Somit ist es umso wichtiger, dass die internationale Zusammenarbeit zwischen den Behörden funktioniert und sie ausreichende Befugnisse haben. Mindestens genauso wichtig ist es, dass Unternehmen die Vorfälle und Angriffe, die sie erleben, melden. Nur durch das Zusammenspiel von Meldung, behördlicher Kooperation und Transparenz schaffen wir es, dass Täter:innengruppen identifiziert und festgenommen werden und sich unser Sicherheitsniveau wieder erhöht.

Anpassung an einen neuen Lebensraum

Im Vorjahresvergleich beobachten wir eine Verschiebung der Angriffsarten. Eine besondere Veränderung gegenüber letztem Jahr ist auch, dass sich die Angriffsarten an das Umfeld angepasst haben. Wir sehen einmal mehr, dass die Täter:innengruppen unsere Maßnahmen genauestens beobachten und sich dahingehend neu ausrichten. Auf die Verschiebung der Angriffsarten und das geänderte Verhalten müssen wir jetzt wiederum passende Antworten finden. Deepfakes haben sich in Österreich verdoppelt. Auch der Insider Threat hat eine große Zunahme erfahren (29 Prozent). Supply-Chain-Angriffe (18 Prozent), APTs (12 Prozent) und Social Engineering (9 Prozent) haben ebenfalls zugenommen.

Die Angriffe finden auf sehr hohem Niveau statt und sind außerordentlich wirksam mit jedem sechsten Angriff, der eine positive Erfolgsbilanz aufweisen kann. Das bedeutet für die Unternehmen am Ende des Tages, wenn jeder sechste Angriff erfolgreich ist, die Angreifer:innen fünf Versuche brauchen, um an ihr Ziel zu kommen. Man könnte also überspitzt formuliert unterstellen, dass sich Interessierte lediglich ein „5 + 1"-Paket im Darknet kaufen brauchen und damit erfolgreich in ein Unternehmen oder Ziel eindringen können.

Bedeutet das jetzt, dass die Unternehmen schlechter in ihren Präventions- und Abwehrmaßnahmen geworden sind? Nein. Die Angreifer:innen gehen dazu über, sich auf das Umfeld einzustellen. Sie haben gelernt, dass wir in der Lage sind, neue Angriffe zu erkennen und abzuwehren. Darum müssen sie wiederum ihr Verhalten ändern. Das merken wir durch den vermehrten Einsatz von Deepfakes und Insider Threats. Auf unserer Seite rücken dadurch wieder verstärkt der Mensch und der kognitive Bereich in den Mittelpunkt.

Wie die Realwirtschaft setzen auch Cyberkriminelle zunehmend auf Arbeitsteilung, einen wachsenden Dienstleistungscharakter und eine enge Vernetzung über Länder- und Branchengrenzen hinweg. Mit dem Konzept des „Cybercrime-as-a-Service" agieren Cyberkriminelle immer professioneller, denn die Spezialisierung auf bestimmte Dienstleistungen ermöglicht es ihnen, ihre „Services" gezielt zu entwickeln und einzusetzen.

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html, abgerufen am 4.3.2024.

Abb. 5: Veränderung der Angriffsarten	Wert	Veränderung gegenüber 2023
Abhören der Kommunikation (Man-in-the-Middle-Angriff)	26 %	0 %
Advanced Persistent Threats (APTs)	38 %	12 %
Business-E-Mail-Compromise, CEO-/CFO-Fraud	80 %	-9 %
Cloud-Fehlkonfiguration	36 %	-10 %
Datendiebstahl (Data Breach)	32 %	-30 %
Deepfake (Audio, Images, Video)	35 %	119 %
Denial-of-Service-Attacken (DoS)	54 %	-41 %
Identitätsdiebstahl	45 %	-24 %
Insider Threat	22 %	29 %
Malware (E-Mail-Anhang)	86 %	-10 %
Mis-/Desinformation	54 %	erstmals 2024 abgefragt
Mobile Malware	34 %	-13 %
OT-Kompromittierung (Industrial Control System)	8 %	-11 %
Passwortdiebstahl	47 %	0 %
Ransomware/Erpressung	24 %	-27 %
Social Engineering	62 %	9 %
(Spear-)Phishingattacke (E-Mail-Link)	87 %	-13 %
Spoofing	52 %	0 %
Supply-Chain-Angriff (Lieferkette)	46 %	18 %

Eine neue Dimension

Die Grafik zeichnet das Bild eines hohen Angriffsaufkommens, das wir bereits im Jahr 2023 erlebt haben. Aus der aktuellen Umfrage ist allerdings klar ersichtlich, dass wir eine Veränderung in der Dimension und den Facetten der Angriffe erleben. Waren es in den letzten Jahren noch vorwiegend Phishing- und Ransomwareattacken, die uns am meisten beschäftigt haben, so sehen wir in der diesjährigen Studie eine klare Veränderung hin zu komplexer werdenden Angriffen. Das wird unterstrichen durch die Tatsache, dass Desinformation am Vormarsch ist. Inwieweit dieses Phänomen den aktuellen geopolitischen Veränderungen zuzuschreiben ist beziehungsweise den Wahlen, die in Europa und auf der ganzen Welt stattfinden, kann nicht eindeutig nachvollzogen werden. Gewiss ist jedoch, dass durch den verstärkten Einsatz von Künstlicher Intelligenz bzw. KI- und LLM-basierten Verfahren immer „perfektere" Angriffe gestaltet werden können. Es ist nicht weiter verwunderlich, dass wir in den letzten 12 Monaten mehr als eine Verdoppelung von Deepfakes festgestellt haben.

Aufholjagd

Der Insider Threat auf Platz zwei mit einer Zunahme von 29 Prozent zeigt, dass wir dem Aspekt von Inlands-Täter:innen immer noch zu wenig Aufmerksamkeit schenken. Gerade jene Personen, die sich mit den internen Kontrollsystemen auseinandersetzen, können diese auch für eigene Zwecke verwenden, missbräuchlich auf Unternehmensressourcen zugreifen und finanzielle Vorteile daraus lukrieren.

Auf Platz drei befinden sich heuer überraschend Angriffe auf die Lieferkette – zwar nur mit einer Zunahme von 18 Prozent, aber auch hier zeigt sich einmal mehr die veränderte Strategie der Angreifer:innengruppen. Die Angriffe werden vom eigentlichen Ziel (Unternehmen) verlagert zum schwächsten Glied in der Kette (Lieferanten). Die aufkommende Regulatorik unterstreicht die Bedeutung dieses Themas, da vor allem die Verwundbarkeit von großen vernetzten Systemen durch schwache Glieder in der Kette sichtbar wird und hier das Kartenhaus bei einem erfolgreichen Cyberangriff in sich zusammenfällt.

Die Absicherung der Lieferkette stellt eine der größten Herausforderungen dar. Einerseits spielt hier das gegenseitige Vertrauen eine große Rolle, andererseits sind natürlich gewachsene Strukturen vorhanden, die von einem Tag auf den anderen Eintrittspunkt für Angreifer:innen werden können. Grundsätzlich erleben wir auch hier, dass das Vertrauen dominiert und Sicherheit eher zweitrangig ist. Für die Unternehmen ist unabhängig von den Forderungen der Regulatorik Aufholbedarf gegeben, denn wenn wir in der Lage sind, Phishingmails zu identifizieren, müssen wir auch Angriffe über Lieferketten identifizieren können, die unmittelbare Verwundbarkeit mit sich bringen.

Oftmals sehen wir, dass gerade bei Transaktionen und Unternehmenskäufen und -verkäufen Angriffe auf die Lieferkette im Mittelpunkt stehen, denn gerade bei dieser Integration kommt es dazu, dass die Sicherheitsmaßnahmen beim Unternehmen, das gekauft wird, noch nicht jenen Stellenwert haben, den der:die kaufende Unternehmer:in gewohnt ist. Das ist ein lukrativer Zeitpunkt für Angreifer:innen. Wie kommen sie auf diese Idee? Weil Unternehmenskäufe und -verkäufe in Medien publiziert werden. Ist die Sprache hier noch ein Thema? Nein, denn durch Künstliche Intelligenz wird es für Angreifer:innen immer leichter, jegliche Informationen in jeglicher Sprache zu verstehen und für ihre eigenen Zwecke zu nutzen.

Insider-Bedrohungen sind Sicherheitsvorfälle, die von Einzelpersonen innerhalb einer Organisation verursacht werden, einschließlich Mitarbeiter:innen, Auftragnehmer:innen und Drittanbieter:innen. Diese Personen haben Zugang zu sensiblen Informationen und Systemen, die sie zu böswilligen Zwecken oder versehentlich ausnutzen können.

Insider-Bedrohungen können erhebliche finanzielle, rufschädigende und betriebliche Auswirkungen auf ein Unternehmen haben. So kann beispielsweise eine von einem böswilligen Insider verursachte Datenpanne zu großen finanziellen Verlusten, einer Schädigung des Rufs des Unternehmens und einer Unterbrechung des Geschäftsbetriebs führen.

Abb. 6: Die Top 5 der Angriffsarten im Jahresvergleich

Ausbalancieren

Wir sehen jedoch auch rückläufige Entwicklungen bei einigen Angriffsarten, die im letzten Jahr das Lagebild noch besonders dominierten. So sind z. B. Business-E-Mail-Compromise und (Spear-)Phishing leicht rückläufig. Auch Ransomwareattacken sind im Vergleich zum Vorjahr um ein Viertel zurückgegangen. Ob dieser Rückgang nun auf die verbesserten Sicherheitsmaßnahmen der Unternehmen zurückzuführen ist oder auf eine Verschiebung der Interessen der Täter:innengruppen ist unklar. Es gilt auf jeden Fall weiterhin dieses Thema im Auge zu behalten, denn so lange sich die Welt weiterdreht, so lange verändern sich auch die Vorgehensweisen der Angreifer:innen und auch die Mutation an Ransomware-Varianten. Hier ist jedenfalls mit Überraschungen zu rechnen. Obschon die Angriffe zurückgegangen sind, so ist in den Analysen unserer Studie allerdings auffallend, dass Ransomware den Unternehmen nach wie vor große Sorgen bereitet. Auch die Angst vor Datendiebstahl ist weiterhin hoch, obwohl dieser im Vergleich zum Vorjahr abgenommen hat.

Inwieweit die Angriffszunahmen auf der einen Seite den rückläufigen Entwicklungen auf der anderen Seite entgegenwirken, beziehungsweise ob die weiteren Schritte im Angriff die gleichen sind, kann nicht weiter analysiert werden. Die Zunahme der Angriffe im letzten Jahr um mehr als 200 Prozent unterstrich nochmals deutlich, dass Cyberangriffe eine gewisse Komplexität mit sich bringen. Im Jahr 2024 manifestieren sich diese Angriffe auf einem sehr hohen Niveau mit nur leichten Rückgängen in einigen Bereichen.

Für uns als Anwender:innen bedeutet das, dass wir uns mit immer zielgerichteteren, professionelleren und authentisch gestalteten Angriffen auseinandersetzen müssen. Neben dem Faktor Schulung und Sensibilisierung spielt auch der Faktor Technologie eine immer wichtigere Rolle für die Abwehrmaßnahmen in einer vernetzten und komplexen digitalen Welt.

Den Feind im Auge behalten

Unternehmen wurden am häufigsten (74 Prozent) über ihre internen Sicherheitssysteme wie Firewall, IDS, xDR oder SIEM auf Cyberangriffe aufmerksam. Hier zeigt sich deutlich, dass ausgereifte Technik notwendig ist, um mit der Komplexität der Angriffe mithalten zu können. An zweiter Stelle wurden Unternehmen durch die eigenen Mitarbeiter:innen auf die Angriffe aufmerksam (67 Prozent), an dritter Stelle durch externe Dienstleister (44 Prozent). Positiv fällt auf, dass fast ein Viertel (23 Prozent) aufgrund von Behördeninformationen auf die Angriffe aufmerksam geworden ist. Im Vorjahr lag diese Zahl noch bei 10 Prozent.

Im Vergleich zur Studie 2023 zeigt sich, dass dem Aspekt der technischen Sicherheitslösungen und Erkennungssysteme immer mehr Aufmerksamkeit geschenkt wird – wohl auch aus Alternativlosigkeit. Sie sind es, die heute die Identifizierung von Angriffen möglich machen. Im Vergleich zum letzten Jahr haben wir hier eine Zunahme um 7 Prozent festgestellt. Auf Platz Nummer zwei folgt allerdings gleich der Mensch. Auch hier gab es eine Zunahme um 7 Prozent. Der Mensch ist es, der in der Lage ist, dubiose Angriffe zu erkennen – gerade im Zusammenhang mit neuen Angriffsmustern wie Desinformation, KI oder zielgerichteten (Spear-)Phishingattacken. Das Rennen um die besten Möglichkeiten zur Erkennung ist also eröffnet.

Auf Tauchstation

40 Prozent der Befragten haben den Vorfall an die Behörden gemeldet, 29 Prozent an ihre Kund:innen und 26 Prozent an CERT.at. 19 Prozent haben allerdings überhaupt keine Meldung getätigt. Auf die Frage, warum nicht gemeldet wurde, gaben jene Unternehmen an, dass keine Daten gestohlen worden wären oder es nicht gesetzlich notwendig gewesen sei. Auch nicht gemeldet wurde, wenn die Angriffe zu keinem Schaden führten und die Abwehrmaßnahmen im Vorfeld gegriffen hatten. Wenngleich Angriffe zu keinen Schäden führen, so ist es aus praktischer Sicht jedenfalls wünschenswert, wenn Sicherheitsvorfälle gemeldet werden. Die aktuelle NIS2-Richtlinie ermöglicht auch freiwillige Meldungen zu tätigen. Meldungen tragen dazu bei, dass wir alle über das aktuelle Geschehen informiert bleiben und ein verbessertes Lagebild entsteht. So wie auch im letzten Jahr gilt heuer umso mehr, dass Risiken, die andere eingehen, Risiken für uns alle sind. Cybersicherheit funktioniert nur dann, wenn wir gemeinsam an einem Strang ziehen und nicht individuell in unseren eigenen Silos arbeiten.

Im Vorjahr gaben allerdings noch 33 Prozent an, keine Meldung getätigt zu haben. Mittlerweile wird immerhin deutlich mehr gemeldet. Das kann darauf zurückzuführen sein, dass die Schäden sowie auch die Komplexität der Angriffe größer geworden sind. Es lässt auch auf ein gestiegenes Bewusstsein der Unternehmen für die Wichtigkeit von Meldungen schließen. Es ist davon auszugehen, dass hier auch die Regulatorik mitschwingt, die die Unternehmen dazu motiviert, Sicherheitsvorfälle zu melden.

Vielfältige Schadensarten

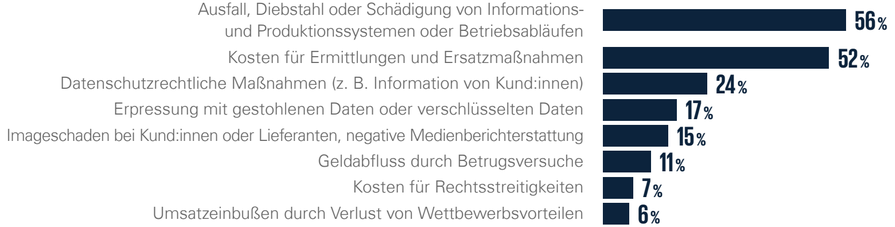
Die häufigsten Konsequenzen, die im Zusammenhang mit Cyberangriffen entstanden sind, waren Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen mit 56 Prozent. Bei 52 Prozent waren es Kosten für Ermittlungen und Ersatzmaßnahmen und bei 24 Prozent datenschutzrechtliche Maßnahmen wie z. B. die Information von Kund:innen. Das stimmt zwar damit überein, dass sich Unternehmen große Sorgen über Datendiebstahl machen, jedoch nicht mit der Tatsache, dass diese Angriffsart im Vergleich zum Vorjahr zurückgegangen ist.

Weitere Schäden, die bei den Unternehmen entstanden sind, waren Erpressung mit gestohlenen oder verschlüsselten Daten (17 Prozent) sowie Imageschäden bei Kund:innen oder Lieferanten bzw. eine negative Medienberichterstattung (15 Prozent) (siehe Abb. 7).

Achtung vor den Raubtieren

Die größte Ursache für Datendiebstähle in Unternehmen war die Software Vulnerability mit 43 Prozent. Die Ursachen für den Datendiebstahl scheitern viel zu oft noch an Basismaßnahmen, über die wir bereits seit der ersten Ausgabe

Abb. 7: Schadensarten*



* Mehrfachnennungen möglich

dieser Studie berichten. In Sachen Softwaresicherheit haben Unternehmen viele Handlungsspielräume und es stellt sich die Frage, wieso nicht aktiv mehr für die Softwaresicherheit getan wird.

33 Prozent machen gezieltes Phishing für die Datendiebstähle verantwortlich. Bei 33 Prozent haben die Daten das Unternehmen durch Diebstahl beim Dienstleister und bei 29 Prozent durch unbedachten E-Mail-Versand verlassen. Hier sollte mehr in die Sensibilisierung der Mitarbeiter:innen investiert werden, damit auch in stressigen Phasen das Bewusstsein vorhanden ist und kurz innegehalten wird, bevor eine E-Mail versandt wird. Unbedachter E-Mail-Versand ist schnell passiert und es gibt (nahezu) kein Zurück mehr.

Beim Datendiebstahl stehen Kund:innendaten im Fokus. Sie wurden am häufigsten gestohlen (52 Prozent), gefolgt von Mitarbeitendendaten und Kommunikationsdaten via E-Mail (jeweils 24 Prozent). 19 Prozent der Befragten wissen nicht, welche Daten gestohlen wurde. Ungefähr jedes fünfte Unternehmen kann folglich auch keine Schlüsse darüber ziehen, was passiert ist, wer zu informieren ist und welche Verstöße begangen wurden.

Abschreckmethoden

Ransomware ist nach wie vor präsent in österreichischen Unternehmen und eines der Schreckgespenster, das Unternehmen großes Kopfzerbrechen bereitet. Bei 59 Prozent hat sich die Erpressung in Form von Verschlüsselung der Daten und Systeme gezeigt. Bei 35 Prozent wurde die Veröffentlichung der Daten angedroht. Zu je 18 Prozent wurden Denial-of-Service-Attacken (DoS) und der Verkauf der Daten an Trittbrettfahrer:innen von den Befragten genannt. 18 Prozent wurden auch mit der Löschung der Daten erpresst.

Angreifer:innen setzten diese mitunter existenzbedrohenden Szenarien als Drohung ein, um Druck auf die Unternehmen aufzubauen und sie zu einer Lösegeldzahlung zu bewegen. Auch hier zeigt sich umso mehr, wie facettenreich das Vorgehen der Angreifer:innen ist. Zieht man alle Möglichkeiten in Betracht, die Angreifer:innen haben und inwieweit sie ihre Kreativität ausnutzen, so sind für diese Methoden keine Grenzen gesetzt.

Lösegeldforderungen

Jedes dritte Unternehmen hat zumindest einmal die Lösegeldforderung im Zusammenhang mit einem Ransomwareangriff bezahlt. Im Vorjahr hat keines der befragten Unternehmen, das von Ransomwareangriffen betroffen war, die damit verbundene Lösegeldforderung bezahlt. Dieser Anstieg ist alarmierend. Warum es hier auf einmal zu einer Trendumkehr kommt und immer mehr Unternehmen die Zahlung in Betracht ziehen, kann aus den Ergebnissen der Studie nicht identifiziert werden. Fakt ist, dass die Lösegeldzahlungen zunehmen. Oft besteht bei Unternehmen der Irrglaube, dass mit dem Begleichen der Lösegeldforderung alle Probleme vom Tisch sind. Jedoch erhöht sich dadurch das Risiko von Trittbrettfahrer:innen.

Die Opfer unterliegen häufig auch der Fehleinschätzung, dass durch die Bezahlung der Lösegeldforderung und der damit verbundenen Übermittlung des Schlüssels zur Entschlüsselung der Daten diese in relativ kurzer Zeit wieder zur Verfügung gestellt werden können. Die Praxis zeigt allerdings, dass die Qualität der Entschlüsselung direkt von der Qualität der Verschlüsselung abhängig ist und Ransomware-Gruppen hier durchaus auf Geschwindigkeit setzen. Ein Test zur Verschlüsselung von Daten durch Ransomware-Schadprogramme hat bspw. ergeben, dass die durchschnittliche Verschlüsselung von 53 GB an Daten nur 42 Minuten und 52 Sekunden braucht. LockBit war hier am schnellsten und hat die Daten sogar in nur 4 Minuten und 9 Sekunden verschlüsselt.[1] Die eingesetzten Verschlüsselungsverfahren sind also nicht in ausreichender Qualität vorhanden. Unternehmen sind dem Risiko einer nicht erfolgreichen vollständigen Entschlüsselung der Daten ausgesetzt, was wiederum bedeutet, dass sich der Wiederherstellungsprozess in die Länge zieht.

Es ist und bleibt die Kombination aus funktionierender Datensicherung und regelmäßigem Üben der Wiederherstellung (Restore), die Unternehmen darauf vorbereiten soll, in Anlassfällen eine möglichst rasche Wiederherstellung ihrer Systeme zu gewährleisten. All das so wie ein funktionierendes Krisenmanagement und ein grundlegender Basisschutz sind die Voraussetzung für einen stabilen und sicheren Betrieb. So gelingt es Unternehmen, ihre Resilienz zu erhöhen.

Schwarmintelligenz

Die Unternehmen wissen, dass sie die Bearbeitung von Cybersicherheitsvorfällen nicht allein bewältigen können. Mehr als die Hälfte (56 Prozent) hatte bei der Bearbeitung eines Sicherheitsvorfalls Hilfe durch einen externen Dienstleister in Form eines Retainers. Unternehmen sichern sich hier schon im Vorfeld externe Unterstützung für einen Cybervorfall, um für den Ernstfall gewappnet zu sein und ein schnelles Reagieren zu ermöglichen.

10 Prozent haben einen externen Dienstleister ohne Retainer hinzugezogen. Insgesamt zwei Drittel der Unternehmen haben sich also Unterstützung geholt. Nur ein Drittel (31 Prozent) hatte keine Unterstützung durch einen externen Dienstleister und nimmt somit die Bearbeitung von Sicherheitsvorfällen immer noch selbst in die Hand.

Generell finden es Unternehmen leicht, einen passenden externen Dienstleister für die Vorfallsbehandlung zu finden. Nur nahezu ein Viertel (24 Prozent) hat hierbei Schwierigkeiten empfunden. Bei den EPUs zeichnet sich allerdings ein völlig anderes Bild: Mehr als der Hälfte (57 Prozent) fällt es schwer, passende externe Dienstleister zu finden.

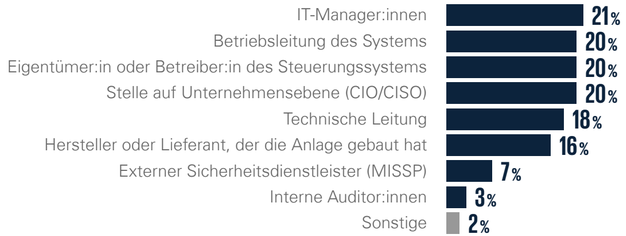
Die Angriffsflächen reduzieren

Bei jenen Maßnahmen, die langfristig nach einem Cyberangriff gesetzt wurden, finden wir am häufigsten (54 Prozent) die Suche nach Schwachstellen in den Systemen. Auch das Krisenmanagement liegt hoch im Kurs und gewinnt an Bedeutung: 49 Prozent haben eine Verbesserung der internen Krisenplanung für Cyberangriffe vorgenommen. 46 Prozent haben zusätzliche Sicherheitstools angeschafft. Erfreulich ist, dass die Anschaffung der Tools nicht dominiert. Die Unternehmen erkennen, dass es für die Bewältigung von Cyberangriffen nicht nur Technologie benötigt, sondern sie darüber hinaus handlungsfähig bleiben und ihre Reaktionsfähigkeit verbessern müssen. Und diese muss auch regelmäßig geübt werden.

37 Prozent haben sich externe Hilfe durch spezialisierte IT-Berater:innen oder Dienstleister als langfristige Maßnahme nach einem Cyberangriff geholt. Es ist eine Awareness da, dass Unternehmen nicht alles selbst machen können. 28 Prozent haben in die Ausbildung der Mitarbeiter:innen

[1] https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html, abgerufen am 25.3.2024.

Abb. 8: OT-Zuständigkeiten*



* Mehrfachnennungen möglich

investiert. Digitale Kompetenzen gehören für sie bei den Maßnahmen gegen Cyberattacken mit dazu.

Weitere langfristig gesetzte Maßnahmen waren die Prüfung der Sicherheit der Lieferanten (24 Prozent) sowie der Abschluss einer Cyberversicherung (18 Prozent).

Herausforderung Operational Technology (OT)

Die Absicherung der OT-Systeme gegen Cyberangriffe ist für Unternehmen oftmals herausfordernd. Zunächst müssen die Zuständigkeiten und Verantwortlichkeiten für die OT-Sicherheit im Unternehmen geklärt werden.

21 Prozent der Befragten geben an, dass die IT-Manager:innen für die Umsetzung der Sicherheitsmaßnahmen im Bereich der OT-Systeme/Industriesteuerungsanlagen verantwortlich sind. Je 20 Prozent sehen die Betriebsleitung des Systems, die Eigentümer:in oder Betreiber:in des Steuerungssystems oder den:die CIO/CISO in der Verantwortung. Hier zeigt sich, dass die Konvergenz von IT- und OT-Systemen ein wesentlicher Faktor für die gesamthafte Sicherheit ist. Klare Verantwortlichkeiten sind unerlässlich sowie dass Verantwortliche in den produktions- und steuerungsnahen Bereichen auf die IT- und Sicherheitsverantwortlichen zugehen und gemeinsam zur Cybersicherheit beitragen.

Von altem Ballast lösen

(Spear-)Phishing ist selbst im OT-Bereich ein großes Thema und wurde mit 50 Prozent als einer der initialen Angriffsvektoren bei den Vorfällen im Bereich OT-/Steuersysteme genannt. Jeweils ca. ein Drittel ist über aus dem Internet erreichbare Geräte, externe Remote-Dienste, Kompromittierung der Lieferkette (Supply Chain) sowie Wireless Kompromittierung passiert.

47 Prozent der Befragten nennen als größte Herausforderung für die Absicherung ihrer OT-Systeme und -Prozesse die technische Integration von veralteter OT-Technologie mit modernen IT-Systemen. Das Alter der OT schmerzt uns heute. Aber auch der Faktor Mensch spielt eine Rolle: 36 Prozent empfinden die nicht ausreichenden Personalressourcen, um bestehende Sicherheitsmaßnahmen umzusetzen, als herausfordernd.

28 Prozent geben an, dass herkömmliche IT-Sicherheitstechnologien nicht für Steuerungssysteme ausgelegt sind und Störungen in den OT-Umgebungen verursachen. Hier hat man es mit Integrationsschwierigkeiten zu tun. Diese Integrationsschwierigkeiten bestehen vor allem deshalb, weil die Technologieunterschiede bzw. das Alter der Anlagen eine reibungslose Vernetzung nicht mehr ermöglichen. Hier sind jedenfalls die Hersteller gefordert, dieser Problematik zu begegnen. Auch der Gesetzgeber hat das bereits erkannt: Durch die Einführung des Cyber Resilience Act der Europäischen Union werden Hersteller aufgefordert, genau für diese Komponenten und Systeme hinreichende Sicherheitsmaßnahmen und Vorkehrungen zu etablieren, die auch regelmäßig aktualisiert werden können. Denn genau diese unterschiedliche Lebensdauer der Systeme führt dazu, dass unsere Verwundbarkeit immer größer wird.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1.

Cyberangriffe finden weiterhin auf einem sehr hohen Niveau statt. Wir müssen uns damit auseinandersetzen, dass sich die Angriffsmethoden laufend ändern und wir auch dahingehend unsere Schulungen anpassen müssen.

2.

Deepfakes in Kombination mit Künstlicher Intelligenz erfordern einen neuen Zugang und die Entwicklung von neuen Kompetenzfeldern für Mitarbeiter:innen. Herkömmliche Methoden und Muster genügen hier nicht mehr.

3.

Für die Bewältigung von Krisen ist es unabdingbar, ein hinreichendes Vorfallsmanagement zu etablieren. Das darf nicht nur für das eigene Unternehmen gelten, sondern es müssen auch externe Dienstleister einbezogen werden. Regelmäßiges Üben ist ebenfalls unerlässlich und spielt gerade in Kombination mit Retainern eine immer wichtigere Rolle. Es ist entscheidend, ob mit den vorhandenen Ressourcen wirksam, zielgerichtet und effizient ein Angriff eingedämmt und der Normalbetrieb binnen kurzer Zeit wieder hergestellt werden kann.

Lösegeldzahlungen: ein Investment in das kriminelle Ökosystem

Carsten Meywirth und Robert Lamprecht diskutieren über die Herausforderungen und Strategien im Kampf gegen Cyberkriminalität. Sie beleuchten die Entwicklung von Cybercrime, die Rolle der Anonymität und die zunehmende Professionalisierung der Täter:innen mithilfe Künstlicher Intelligenz.

Sie sind schon lange im Bereich der Cybercrime-Bekämpfung tätig. Gibt es hier eigentlich noch Überraschungen? Was sollten wir wissen, wenn wir unsere Gegner:innen besser verstehen wollen?

Carsten Meywirth: Überrascht hat mich im Laufe der Zeit, dass sich Cybercrime sehr stark gewandelt hat. Das heißt, die Gruppierungen, die in diesem Feld tätig sind, haben sich anders oder besser organisiert und professioneller ausgebildet. Es ist eine Underground Economy entstanden, quasi eine Art kriminelles Ökosystem – wir nennen das Crime-as-a-Service. Ganz genau wie im legalen Bereich, haben sich illegale Servicedienstleister:innen herausgebildet, und diese Personen, die dort tätig sind, kennen sich persönlich gar nicht. Man kennt sich nur unter den Nicknames, die im Internet auf verschiedenen Plattformen verwendet werden. Cyberkriminelle kaufen entsprechende Services ein, um ihre Straftaten begehen zu können.

Also ein florierender Handel, wo am Ende des Tages die Anonymität dominiert und im Vergleich zu den klassischen Täter:innengruppen das Vertrauen eher im Hintergrund steht?

Carsten Meywirth: Ganz genau. Auch der Tatort steht nicht mehr im Vordergrund, weil alles digital ist. Es gibt nur noch eine geringe Schnittstelle zur analogen Welt und das stellt uns natürlich vor ganz große Herausforderungen.

Und genau diese Herausforderungen treffen uns ja auch, wenn wir auf die kritische Infrastruktur schauen, denn die Angriffe gegen die kritische Infrastruktur und Bundesbehörden steigen. Wie geht Ihre Abteilung im BKA damit um?

Carsten Meywirth: 2020 wurde das Thema bei uns auf Abteilungsniveau gehoben, womit eine bessere finanzielle, aber auch personelle Ausstattung einhergeht. Wir haben diesen Bereich aufgewertet und sind nun in der Lage, mit größeren Ressourcen an die Sache heranzugehen. Wir arbeiten auf Bundesebene eng mit den Landeskriminalämtern zusammen. Und wir haben erkannt, dass es sehr schwierig ist, sich bei den Ermittlungen nur auf einen täter:innenbezogenen Ansatz zu konzentrieren, weil es häufig der Fall ist, dass die Täter:innen in sogenannten „Safe Havens“ sitzen, sprich in Staaten, mit denen eine Kooperation schwierig ist und wir daher auch nur schwer an die Täter:innen herankommen. In unserem Bekämpfungsansatz konzentrieren wir uns also auch auf die Infrastrukturen, die die Täter:innen benötigen, um ihre Straftaten im digitalen Raum zu begehen. Wir haben festgestellt, dass das ein sehr effektives Mittel ist, um sie zu stören oder auch ganz wesentlich in ihrem Tun zu beeinträchtigen.

Da sind jetzt einige wichtige Punkte gefallen – ein essenzieller Aspekt ist aber doch, dass das BKA ja eigentlich erst Schritte setzen kann, wenn eine Meldung erfolgt ist.

Carsten Meywirth: Das ist richtig. Wir haben in Deutschland Strafverfolgungszuständigkeiten und wir als BKA sind sehr stark davon abhängig, dass insbesondere Unternehmen, die Opfer von schweren Straftaten werden, dann auch entsprechend Anzeige erstatten – erst dann können wir die Verfolgung aufnehmen. Das ist oftmals ein Problem. Viele Unternehmen scheuen sich vor einer Meldung, weil sie nicht wissen, was das alles für sie im Nachgang bedeutet. Natürlich versuchen wir hier immer wieder Aufklärungsarbeit zu leisten und ich habe auch das Gefühl, dass sich da in den letzten Jahren schon einiges zum Besseren gewandelt hat.

Unternehmen sind oft zögerlich, Anzeige zu erstatten, da sie die Erfolgschancen, die Täter:innen zu erwischen, als gering einschätzen. Dem widersprechen aber etliche Erfolgsgeschichten, bei denen die Behörden aufgrund von Anzeigen tätig werden konnten, um dann die nächsten Schritte zu setzen. Wird über diese Erfolgsgeschichten zu wenig gesprochen, um hier bei den Unternehmen ein Umdenken zu bewirken?

Carsten Meywirth: Diese polizeilichen Erfolge sind sehr wichtig, um einerseits Vertrauen zu schaffen, und andererseits auch einen gewissen Anreiz zu geben, sich an die Polizei zu wenden. Für mich ist das ein wichtiges Ziel bei der Strafverfolgung.

Wie wichtig ist der internationale Austausch bei der Cybercrime-Bekämpfung? Was können wir letztendlich voneinander lernen?

Carsten Meywirth: Das ist ein höchst erfolgskritischer Faktor. Nur im Rahmen von internationalen Allianzen kann man erfolgreich sein. Ich kenne kein Ermittlungsverfahren, kein Beispiel aus den vergangenen Jahren, wo ein Land allein erfolgreich gegen eine global agierende Gruppierung vorgehen konnte. Das hat immer in internationalen Allianzen stattgefunden. Die

FOTO © PRIVAT

Carsten Meywirth
Leiter der Abteilung Cybercrime im Bundeskriminalamt in Deutschland

Nach seiner polizeilichen Ausbildung trat er 1987 in das Bundeskriminalamt ein. Ferner leitete er ab 2005 in der Abteilung Informationstechnik des Bundeskriminalamts unterschiedliche Projekte und war ab 2008 Leiter des Stabes des IT-Direktors. Darüber hinaus leitete er für drei Jahre die Gruppe Cybercrime in der Abteilung Organisierte und Schwere Kriminalität. Im Oktober 2019 wurde er mit der Leitung der Projektgruppe zum Aufbau der Abteilung Cybercrime beauftragt, die zum 1. April 2020 im Bundeskriminalamt eingerichtet wurde.

Täter:innengruppen, insbesondere Akteur:innen, die Ransomware verteilen und sehr viel Geld damit verdienen, sind meist global tätig. Und denen ist es egal, ob das Unternehmen in Japan, Amerika oder Europa sitzt. Für die Ermittlungseinheiten ist es wichtig, die Informationen auf den Tisch zu legen und auch die Aufgaben entsprechend zu verteilen. So ist die eine Einheit vielleicht ein Stückchen weiter, wenn es um die Täter:innen geht, während eine andere Einheit bessere Ergebnisse bei der kriminellen Infrastruktur oder den Kryptoermittlungen verzeichnet. Nur durch eine Zusammenarbeit können wir bessere Ergebnisse erzielen und auch einen Matchplan aufsetzen, wie wir gegen diese Gruppierungen erfolgreich vorgehen. Natürlich ist das keine Sache, die innerhalb von wenigen Tagen oder ein paar Wochen funktioniert. Erfahrungsgemäß dauern diese Verfahren Monate, wenn nicht gar Jahre, in denen man sich austauscht und einen entsprechenden Matchplan verfolgt.

Es geht darum, Informationen auszutauschen, zu sammeln und ein Lagebild zu erstellen. Aus diesem Lagebild heraus: Wie gut sind Unternehmen bei der Abwehr von Ransomwareattacken – momentan eines der dominierenden Phänomene – aufgestellt bzw. was wird es hier noch brauchen?

Carsten Meywirth: Nach unserer Beobachtung sind insbesondere größere Unternehmen besser aufgestellt. Diese verfügen in der Regel über mehr Finanzmittel und haben auch mehr Personal. Kleinere mittelständische Unternehmen sind hier tendenziell nicht so gut aufgestellt, weil sie nicht über diese Ressourcen verfügen. Es ist aber für jedes Unternehmen wesentlich, in Cybersicherheit zu investieren. Man sieht zwar keine direkten Erfolge, aber es ist unwahrscheinlich wichtig, dass man hier die entsprechenden Investitionen tätigt, weil ein Angriff verheerende Folgen haben kann. Nicht zu unterschätzen ist auch die Awareness der Mitarbeitenden, die ein ganz wesentliches Asset in diesem Bereich ist. Angriffe werden nach wie vor sehr häufig über sogenannte Spamming-Phishingattacken gefahren. Es muss daher erheblicher Wert auf die Schulung der Mitarbeitenden gelegt werden.

Schulung ist ein wichtiges Thema – aber kommen wir bei dem Thema nicht irgendwann einmal an ein Limit? Ich meine damit, dass die Dynamik und die Tools, die Täter:innen verwenden, zu kreativ werden, als dass wir sie in unseren konventionellen Awareness-Trainings schulen können?

Carsten Meywirth: Es ist auf jeden Fall wichtig, die Mitarbeitenden zu sensibilisieren, was passieren kann und wie Täter:innen grundsätzlich vorgehen. Wenn man ein Gefahrenradar hat und im Zweifel zum Telefon greift und irgendjemanden anruft und nachfragt, dann zahlt sich das in jedem Fall aus. Genauso wichtig wie die Prävention ist es aber auch, die Mitarbeitenden zu ermutigen, den Servicedesk zu informieren, wenn bereits etwas passiert ist – denn die können dann vielleicht rasch helfen bzw. die richtigen Schritte einleiten.

Das Thema Künstliche Intelligenz wird vor allem im Phishing-bereich immer dominanter. Die Qualität der Phishingnachrichten steigt und alte Merkregeln wie „auf Tippfehler achten" gelten nicht mehr. Inwieweit gibt es hier schon eine gewisse Professionalisierung, bei der auch andere Verfahren oder Methoden eingesetzt werden?

Carsten Meywirth: Wir haben in den vergangenen zwei Jahren gemerkt, dass die Phishing-E-Mails, die versandt werden, erheblich professioneller geworden sind. Die üblichen Fehler sind nicht mehr enthalten und man merkt deutlich, dass die Täter:innen moderne Technik einsetzen und sie verwenden moderne Technik, um Schadcodes zu entwickeln. Was wir noch nicht festgestellt haben, ist eine Art adaptive Schadsoftware, die auf Sicherheitsmaßnahmen reagiert. Aber auch das können wir uns in Zukunft vorstellen.

Wenn man das Thema Künstliche Intelligenz aus einer anderen Sicht betrachtet – welche Potenziale in Richtung Schutzmaßnahmen gibt es für die Zukunft?

Carsten Meywirth: Wo uns KI sicher helfen kann, ist beim Thema Musterkennung – bei Bildern oder auch bei Spurenmustern. Hier kann man KI sehr wertvoll einsetzen, um zu schauen, ob es Hinweise auf die Identität der Täter:innen oder deren Ort gibt.

Laut unserer Studie hat knapp ein Drittel der von Ransomware betroffenen Unternehmen die Lösegeldforderung bezahlt. Gibt es hier eine Handlungsempfehlung?

Carsten Meywirth: Unsere ganz klare Position ist: Nicht zahlen. Denn jede Zahlung ist ein Investment in das kriminelle Ökosystem, das für die Täter:innen weitere Anreize schafft. Und nicht selten wird man aufgrund der Zahlung wieder Ziel einer neuen Attacke. Besser und nachhaltiger ist es, vorher in Prävention zu investieren, als hinterher in die Täter:innen.

Wenn wir beide uns in einem Jahr wieder treffen, was würden wir uns dann wünschen, heute schon getan zu haben?

Carsten Meywirth: Mehr in die Bekämpfung der Cyberkriminalität zu investieren. Da gibt es immer noch Luft nach oben. Es gibt viele Berührungsängste mit der Gesamtthematik, weil diese natürlich sehr komplex und technisch geprägt ist und man daher nicht so richtig weiß, wo das Investment hingeht. Aber es ist ein wichtiger Punkt, denn die Straftaten werden auf einem sehr hohen Niveau bleiben, wenn nicht sogar ansteigen.

Ist es also quasi aus Mangel an Alternativen notwendig, die Investitionen zu steigern, um am Ende nicht auf der Strecke zu bleiben?

Carsten Meywirth: Ja, das glaube ich schon. Die Digitalisierung schreitet voran und die Täter:innen haben große Vorteile aufgrund der Anonymität des Internets, Verschlüsselungstechnologien und Safe Havens. Und die nutzen sie aus, um sehr, sehr hohe illegale Profite zu erzielen. Das wird auch in Zukunft ein boomendes Geschäft bleiben und es wird genügend kriminelle Akteur:innen geben, die uns das Leben schwer machen. Daher wünsche ich mir hier ein größeres Investment in die Sicherheit unserer IT-Systeme und in unsere digitale Sicherheit insgesamt.

> **Wenn man das Bauchgefühl hat, hier stimmt irgendwas nicht, dann besser einmal mehr telefonieren als einmal weniger.**
>
> Carsten Meywirth

Erfahren Sie mehr in unserem Podcast IMPULSE

Was ist die häufigste Frage, die Ihnen gestellt wird bzw. was hat noch nie jemand gefragt, obwohl es eigentlich wichtig wäre, die Antwort zu kennen?

Carsten Meywirth: Die häufigsten Fragen sind sicherlich jene nach Lösegeldzahlungen bzw. der Anzeige – diese Fragen treffen einen Nerv. Zu wenig wird definitiv nach Erfolgen gefragt, die wir ja durchaus vorweisen können. Hier sind Gesprächspartner:innen dann immer wieder überrascht, wie effektiv die Polizei und Sicherheitsbehörden vorgehen und die Täter:innen auch empfindlich treffen können.

66 % haben Bedenken, dass Cyberangriffe gegen ihre Dienstleister Auswirkungen auf sie selbst haben werden.

69 % stimmen der Aussage zu, dass Angriffe gegen die Development-Pipeline in der Softwareentwicklung (Software Supply Chain Attack) für sie ein großes Risiko darstellen.

22 % der Unternehmen haben eine Cyberversicherung.

29 % wünschen sich, dass die Cyberversicherung die Lösegeldzahlung abdeckt.

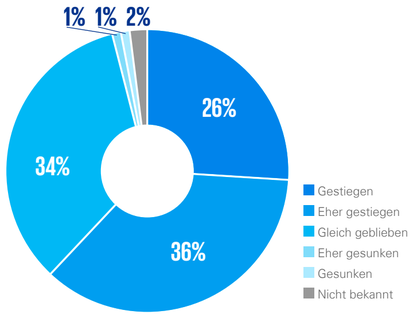
48 % der Unternehmen sagen, dass sie ihr aktuelles Cyberrisiko kennen und es messen können.

02

Ressourcen, Risiken und Regulatorik

Unter Wasser lauern Chancen, aber auch viele Risiken. Wie auch unsere Schildkröte müssen sich Unternehmen dessen bewusst sein und dürfen sich selbst nicht überschätzen.

Abb. 9: Wie hat sich das Budget für Cybersecurity in Ihrem Unternehmen in den letzten zwölf Monaten verändert?



Regularien bieten hier gewisse Leitplanken, aber jedes einzelne Unternehmen muss ein funktionierendes Risikomanagement haben, um die eigenen Risiken zu kennen und in weiterer Folge handlungsfähig bleiben zu können.

Die Ressourcen werden knapper

Beim Schutz vor Cyberrisiken spielt das Budget eine wichtige Rolle. 32 Prozent der befragten Unternehmen haben kein dezidiertes Budget für Cybersecurity. Im Vorjahr waren dies nur 24 Prozent. 12 Prozent (im Vorjahr: ebenfalls 12 Prozent) geben an, dass ihr jährliches Budget für die Umsetzung und Aufrechterhaltung der Cybersecurity 6–10 Prozent des IT-Budgets ausmacht. Bei 62 Prozent der Befragten ist das Cybersecurity-Budget in den letzten zwölf Monaten gestiegen. 2023 gaben allerdings noch 75 Prozent an, dass ihr Budget im Vergleich zu 2022 gestiegen ist. Bei 34 Prozent ist das Budget für Cybersecurity in den letzten zwölf Monaten gleich geblieben.

Kurswechsel

Werfen wir einen Blick auf die Gründe für die Budgetveränderung, so sehen wir, dass neue bzw. veränderte Bedrohungen mit 54 Prozent dominieren. An zweiter Stelle liegt die Unternehmensstrategie mit 43 Prozent. Die (betriebs-)wirtschaftliche Notwendigkeit hat es dieses Jahr in die Top 3 geschafft – von 31 Prozent der Befragten wurde sie als Grund für die Budgetveränderung genannt. Hier hat es eine leichte Zunahme im Vergleich zum Vorjahr (25 Prozent) gegeben.

Im Vorjahr waren die behördlichen Vorgaben noch an dritter Stelle. Dieses Jahr sind sie auf Platz vier gefallen (29 Prozent). Behördliche Vorgaben und Compliance sind zwar nach wie vor wichtige Gründe für eine Budgetveränderung, aber Unternehmen erkennen jetzt auch von sich aus, dass es für sie existenznotwendig ist, ein entsprechendes Cyberbudget bereitzustellen. „Neue Märkte und Expansion" verzeichnet ebenfalls einen starken Anstieg von 4 auf 9 Prozent (siehe Abb. 10).

Verzweigte Nahrungskette

Im Hinblick auf die Lieferkette (Supply Chain) ist die Lage dramatisch: 66 Prozent haben Bedenken, dass Cyberangriffe gegen ihre Dienstleister Auswirkungen auf sie selbst haben werden. Die erhöhte Abhängigkeit von Lieferanten in ihrer Lieferkette schmerzt die Unternehmen zunehmend. Auch im digitalen Bereich wird die Abhängigkeit präsent, wenn es zu Cyberangriffen kommt. Das beeinflusst die Resilienz der Unternehmen. Aktuelle Angriffe verdeutlichen dies einmal mehr.

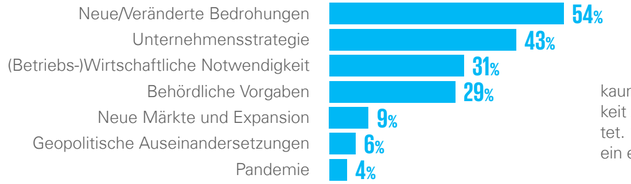
So veranschaulicht ein Angriff auf die Supply Chain eines Softwareunternehmens etwa unsere verstärkte Abhängigkeit von Cloud-Dienstleistern: Die Angreifer:innen nutzten eine Schwachstelle in der Lieferkette aus, um Schadcodes in die Softwarekomponenten des Unternehmens einzuschleusen. Dadurch erlangten die Täter:innen Zugriff auf das Unternehmensnetzwerk und stahlen Quellcodes sowie andere vertrauliche Informationen.[1]

Ein weiteres Beispiel aus der jüngsten Vergangenheit hat die Mitarbeitenden im Fokus: Bei einer Cyberattacke wurde Zugriff auf die Systeme eines Luft- und Raumfahrtkonzerns erlangt. Dies geschah, indem man sich Zugang zu einem Mitarbeitendenkonto eines Kunden des Konzerns verschaffte. Im Zuge dessen wurden tausende persönliche Informationen von Lieferanten kompromittiert.[1]

Auch die kritische Infrastruktur bleibt nicht vor Angriffen auf die Lieferkette verschont, wie ein Lieferkettenangriff auf ein Pipelinesystem belegt: Dabei wurde eine Schwachstelle in einem vom Pipelinesystem verwendeten Softwareprogramm ausgenutzt. Die Angreifer:innen erlangten dadurch Zugriff auf das Netzwerk des Pipelinesystems und verschlüsselten dessen Systeme. Die Pipeline musste für fünf Tage ausgeschaltet werden, was zu einem Benzinmangel führte.[1]

Wir sehen: Lieferanten können ein schwaches Glied in der Kette darstellen und werden somit gerne auch als Eintrittspunkt für Cyberangriffe verwendet. Aus diesem Grund schenken aktuelle Regularien der Lieferkette und der Abhängigkeit von Dritten immer mehr Bedeutung.

Abb 10: Gründe für eine Budgetveränderung*



* Mehrfachnennungen möglich

Schutzmaßnahmen

Bei jenen Aktivitäten, die Unternehmen zur Gewährleistung der Sicherheit bei ihren Lieferanten/Dienstleistern durchführen, dominieren angeforderte Zertifizierungen (31 Prozent), gefolgt von der Durchführung eines eigenständigen Audits (28 Prozent), der Durchführung eines Audits durch Dritte (24 Prozent) und einem Fragebogen zur Selbstdeklaration (22 Prozent). Es muss allerdings gesagt werden, dass ein derartiger Fragebogen zwar ein guter Anfang ist, dieser jedoch nicht immer die größte Aussagekraft hat und in der Praxis kaum Aufschlüsse über die Wirksamkeit der gesetzten Maßnahmen bietet. 14 Prozent der Befragten haben ein externes Rating angefordert.

Jedes vierte Unternehmen (28 Prozent) führt keine Tätigkeiten zur Gewährleistung der Sicherheit bei Lieferanten/Dienstleistern durch. Jedoch haben 34 Prozent der Befragten angegeben, keine Bedenken dabei zu haben, dass Cyberangriffe gegen ihre Dienstleister Auswirkungen auf sie selbst haben werden. Hier klaffen Selbsteinschätzung und Realität auseinander, denn die Zahlen zeichnen ein ganz anderes Bild: Unternehmen, die angeben, keine Maßnahmen zur Gewährleistung der Sicherheit bei ihren Lieferanten und Dienstleistern durchzuführen, haben dennoch große Bedenken (58 Prozent), dass Cyberangriffe gegen ihre Dienstleister eine Auswirkung auf sie haben. Das würde in weiterer Folge bedeuten, dass die Unternehmen ob des latent vorhandenen Risikos dieses dennoch ohne weitere Maßnahmen akzeptieren. Inwieweit sich die Unternehmen dieses Widerspruchs bewusst sind, ist aus den Ergebnissen der Umfrage nicht ableitbar. Es ist aber jedenfalls erkennbar, dass ein Risikobewusstsein vorhanden ist, das nicht zwingend mit der eigenen Wahrnehmung übereinstimmt.

Schwachstellen in der Development-Pipeline

69 Prozent stimmen der Aussage zu, dass Angriffe gegen die Development-Pipeline in der Softwareentwicklung (Software Supply Chain Attack) für sie ein großes Risiko darstellen. Wir sehen somit, dass eine große Abhängigkeit besteht. Die Einbindung von Open-Source-Codes, wie diese z. B. auf GitHub und anderen Portalen abrufbar sind, ist ein verlockendes Angebot. Angreifer:innen können allerdings Schadcodes einschleusen, die dann großflächig verbreitet werden.

Wir erinnern uns in diesem Zusammenhang an die staatliche Ransomwareattacke NotPetya gegen M.E.Doc, ein ukrainisches Programm zur Steuererstellung. Das war einer der ersten Angriffe dieser Art und in dieser Größenordnung und hat zu hohen Schäden geführt. Schwach-

[1] https://www.cloudsek.com/blog/top-5-famous-software-supply-chain-cyber-attacks-in-2023, abgerufen am 25.3.2024.

stellen in der Development-Pipeline begünstigen solche Angriffe. Die Europäische Union hat mit der Verabschiedung des Cyber Resilience Act auch hier eingegriffen und neue Vorgaben zur Verbesserung der Sicherheit veröffentlicht. Dennoch sind Unternehmen angehalten, sich hinreichend um ihre Softwaresicherheit zu kümmern. Gerade im Zusammenhang mit den tosenden Wellen der Digitalisierung – aktuell beschleunigt durch die Fortschritte im Bereich der Künstlichen Intelligenz – spielt die Entwicklung von Software oder Code eine immer wichtigere Rolle. Eine verbindliche Berücksichtigung von Sicherheit in der Entwicklung ist hier unausweichlich.

In der Praxis sehen wir, dass gerade das Zusammenspiel mit den Dienstleistern darüber entscheidet, wie schnell eine Wiederherstellung möglich ist.

Natürlich ist die Wirksamkeit der getroffenen Maßnahmen zum Schutz der Daten, Systeme und anderen Assets eine notwendige Grundvoraussetzung. Aber ohne Üben zeigt sich, dass während der Wiederherstellung ungeplante Verzögerungen stattfinden, die durch regelmäßiges Üben vorab erkannt und behoben hätten werden können.

Versichert ist gleich abgesichert?

Weniger als ein Viertel (22 Prozent) der Unternehmen hat eine Cyberversicherung. 8 Prozent planen eine Cyberversicherung abzuschließen und 5 Prozent sind aktuell in Gesprächen, um eine Cyberversicherung abzuschließen. 39 Prozent sind der Meinung, keine Cyberversicherung zu benötigen. Dieser Anteil hat sich im Vergleich zum Vorjahr (24 Prozent) erhöht. Einige der Befragten haben sogar angegeben, ihre bestehende Cyberversicherung wieder gekündigt zu haben. Bei den EPUs sind sogar 56 Prozent der Meinung, dass sie keine Cyberversicherung benötigen. Eine Entwicklung, die durchaus interessant ist, denn zumindest 10 Prozent der befragten EPUs verzeichneten einen Schaden von mehr als zehntausend Euro durch Cyberangriffe in den letzten 12 Monaten.

Die überwiegende Mehrheit der befragten Unternehmen wünscht sich, dass die Kosten für den Datenverlust und die Wiederherstellung (74 Prozent) sowie für entgangene Gewinne bzw. eine Betriebsunterbrechung (59 Prozent) durch eine Cyberversicherung gedeckt werden. Mehr als jedes vierte Unternehmen (29 Prozent) wünscht sich, dass die Cyberversicherung die Lösegeldzahlung abdeckt. Das ist durchaus verständlich, wenn man bedenkt, dass jedes dritte Unternehmen bereits eine Lösegeldforderung gezahlt hat.

Bei aktuellen Ransomwareangriffen wird das Lösegeld meist in virtuellen Währungen wie Bitcoin gefordert – die Zahlung bietet jedoch keine Garantie für die Freigabe verschlüsselter Daten oder gesperrter Systeme. Stattdessen sollten Betroffene umgehend Anzeige bei der Polizei erstatten. Auch die regelmäßige Erstellung von Back-ups ist eine wirksame Prävention gegen Ransomware. Denn so können im Falle eines Angriffs Datenbestände auch ohne Lösegeldzahlung rekonstruiert werden.

Es ist daher ein Irrtum zu glauben, dass eine Versicherung gegen Lösegeldzahlungen eine akzeptable Möglichkeit der Risikovorsorge darstellt. Wenn überhaupt, dann führt dies zu der unzutreffenden Annahme, dass Unternehmen vor Ransomwareangriffen geschützt sind. Das ist ein großes Problem und kann zu folgendem Worst-Case-Szenario führen: Zuerst zahlen Unternehmen für eine Versicherung, die die Zahlung des Lösegelds übernimmt. In weiterer Folge zahlen sie eine Strafe für die Verletzung von Gesetzen oder Verordnungen, dann eine Strafe für die Nichteinhaltung von Branchen-SLAs, dann Strafen für die Sicherheitsverletzung. Schließlich zahlen sie für die Folgekosten wie Datenverlust, Wiederherstellung inklusive Unterstützung durch Dritte, nachgelagerte Kund:innenauswirkungen und so weiter – die Cyberversicherung deckt höchstens einen Teil dieser Kosten.

Das Schlusslicht bei den Posten, die laut den Befragten durch eine Cyberversicherung abgedeckt sein sollen, stellen Maßnahmen für Imagekampagnen (15 Prozent) dar, wenn durch Cyberangriffe ein Imageverlust für die Unternehmen entstanden ist.

In falscher Sicherheit wiegen

88 Prozent der Unternehmen stimmen zu, dass sie ihre besonders schützenswerten Daten („Kronjuwelen“) kennen. 77 Prozent sagen, dass sie einen vollständigen Überblick über alle ihre schützenswerten Assets haben. Das stimmt nicht damit überein, dass Ransomware den Unternehmen immer noch großes Kopfzerbrechen bereitet und weiterhin als besondere Herausforderung gesehen wird. Auch die Sorge vor Datendiebstahl ist groß bei den Unternehmen und passt nicht in dieses Selbstbild. Denn gerade um wirksame Vorsorgemaßnahmen gegen die Auswirkungen von Ransomware und Datendiebstahl treffen zu können, ist es unabdingbar, einen vollständigen und aktuellen Überblick über die schützenswerten Daten und Assets zu haben. Dieser Überblick ist einerseits für die „Sichtbarkeit“ der Aktivitäten der Angreifer:innen relevant, denn Gegenmaßnahmen können nur dann getroffen werden, wenn bösartige Handlungen erkannt werden. Andererseits ist eine „richtige“ Reaktion im Krisenfall nur dann möglich, wenn hinreichende Transparenz vorhanden sowie die Reihenfolge für die Wiederherstellung der schützenswerten Daten und Assets bekannt ist. In der Praxis gibt es hier noch großen Handlungsbedarf.

62 Prozent geben an zu wissen, welche Daten sich bei Dritten (Dienstleistern) befinden und sicherstellen zu können, dass diese ausreichend geschützt sind. Das stimmt nicht mit jenen 66 Prozent überein, die Bedenken haben, dass Cyberangriffe gegen ihre Dienstleister Auswirkungen auf sie selbst haben werden.

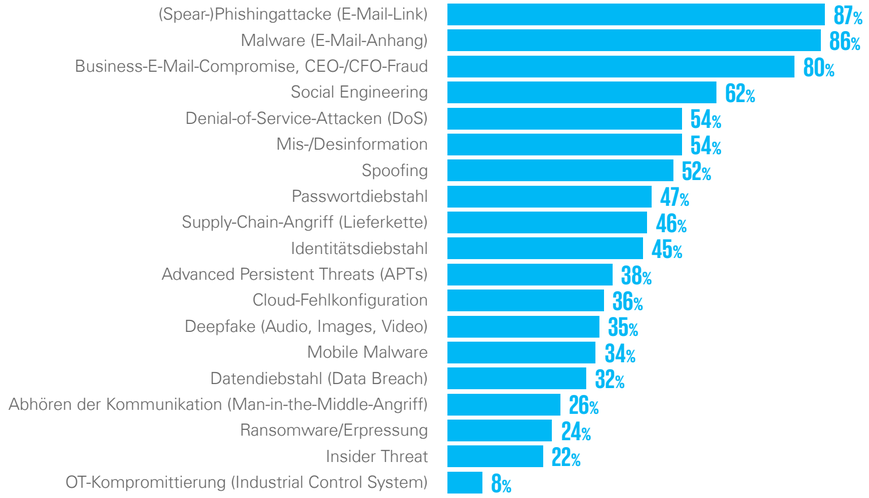
Bei den Unternehmen herrscht ein großes Sicherheitsgefühl. Gerade aber die Fälle in der Praxis zeichnen ein widersprüchliches Bild. Die Aufarbeitung von Sicherheitsvorfällen führt bei Unternehmen zu großen Zeitverzögerungen. Es ist deshalb zu bezweifeln, ob das Bauchgefühl der Unternehmen mit der Realität übereinstimmt.

Kennen ist nicht gleich Quantifizieren

Quantifizierung, Kennen und Messen von Cyberrisiken stellen die Grundlage für viele weitere Maßnahmen dar. 48 Prozent der Unternehmen sagen, dass sie ihr aktuelles Cyberrisiko kennen und es messen können. 22 Prozent verneinen dies allerdings. Jedes fünfte Unternehmen steht demnach noch vor einer Herkulesaufgabe. Bei den EPUs sind die Aussichten noch weniger rosig: Nur 37 Prozent stimmen zu, dass sie ihr aktuelles Cyberrisiko kennen und messen können.

Gerade im Umfeld der Regulatorik (z. B. NIS2, DORA) wird der Quantifizierung eine besondere Bedeutung zugeschrieben, weil sie die Grundlage für alle weiteren Maßnahmen ist. Es ist zu beachten, dass es in puncto Kennen und Messen des Risikos nicht mehr reicht, das Risiko qualitativ zu messen. Die Quantifizierung und Überführung in das weitere Unternehmensrisikomanagement sind uner-

Abb. 11: Die größten Gefahren für Unternehmen (Angriffe der letzten 12 Monate)*



* Mehrfachnennungen möglich

lässlich. Jene 48 Prozent müssen sich hier selbst die kritische Frage stellen, ob sie ihr Risiko auch quantitativ kennen. Die restlichen Unternehmen, die ihr Risiko nicht kennen, haben noch einiges mehr vor sich.

Bedrohungen im Visier?

Die Einschätzung der Befragten bezüglich der Eintrittswahrscheinlichkeit von Cyberangriffen gegen ihr Unternehmen ergibt ein durchwachsenes Bild. Ein Viertel der Unternehmen (24 Prozent) schätzt die Eintrittswahrscheinlichkeit hoch ein. 34 Prozent bewertet diese als durchschnittlich, 4 Prozent ist die Eintrittswahrscheinlichkeit nicht bekannt und über ein Drittel (39 Prozent) bewertet diese als gering.

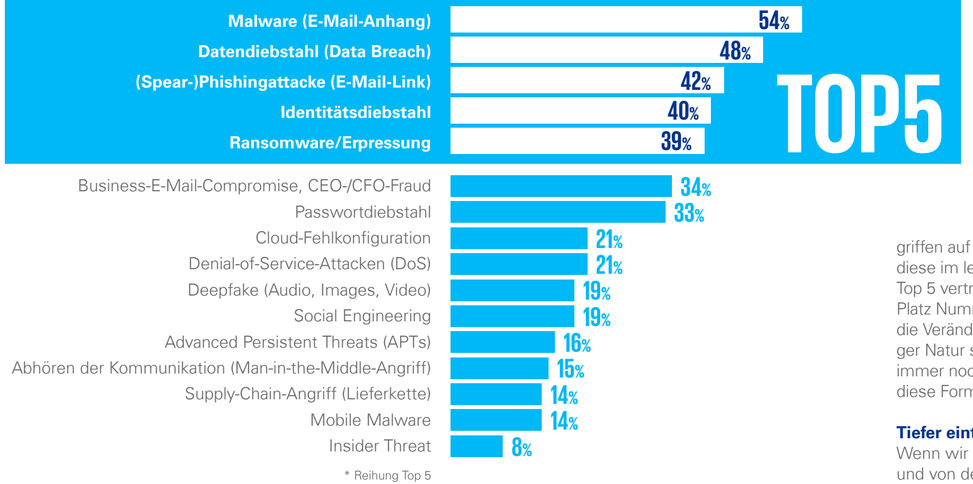
EPUs fühlen sich im Vergleich dazu sicherer: 61 Prozent schätzen die Eintrittswahrscheinlichkeit von Cyberangriffen als gering ein. Hier ist allerdings Vorsicht geboten und EPUs dürfen sich keinesfalls in falscher Sicherheit wiegen.

Die größten Gefahren

Wenn wir einen Blick auf die Angriffe in den letzten 12 Monaten werfen, dann sehen wir, dass im Vergleich zum vergangenen Jahr eine Veränderung stattgefunden hat. (Spear-) Phishingattacken sind zwar immer noch auf dem ersten Platz, dennoch ist hier ein leichter Rückgang erkennbar. Dieser Rückgang ist vor allem der Tatsache geschuldet, dass Unternehmen in der Lage sind, Phishingangriffe zu erkennen. Nichtsdestotrotz befinden wir uns immer noch auf einem sehr hohen Niveau.

Die Plätze zwei und drei haben im Vergleich zum Vorjahr getauscht. Auf Platz zwei finden wir heuer erstmals Malware. Hier ist eine deutliche Steigerung im Vergleich zum letzten Jahr zu erkennen. Inwieweit hier eine Abgrenzung zu den sogenannten „Zero Day"-Angriffen vorhanden ist, kann aus den aktuellen Zahlen nicht durchgängig abgeleitet werden. Nichtsdestotrotz wird deutlich, dass der Einsatz von Schadsoftware Unternehmen massiv beschäftigt.

Abb. 12: Die Top 5 der Cyberrisiken (Angriffsarten nach Wichtigkeit für Unternehmen)*



* Reihung Top 5

Auf Platz Nummer drei befindet sich heuer Business-E-Mail-Compromise bzw. CEO-/CFO-Fraud. Platz Nummer vier nimmt Social Engineering ein, womit dem Aspekt des Menschen, der im Fokus steht, auch in diesem Jahr wieder eine besondere Aufmerksamkeit zukommt. Überraschend ist heuer der fünfte Platz, nämlich die Mis- bzw. Desinformation – eine Angriffsart, die es heuer erstmals in die Umfrage und sofort unter die Top 5 geschafft hat.

Aus der Kombination der eingesetzten Angriffsarten erkennen wir klar, dass Angreifer:innengruppen auf den Menschen abzielen. Die Beeinflussung des Menschen rückt aufgrund seiner Gutgläubigkeit immer stärker in den Mittelpunkt. Die Angriffe werden noch dazu mit einer technischen Komponente – Malware – unterstützt. Durch den Einsatz von fortgeschrittenen Beeinflussungsmöglichkeiten und -varianten (Desinformation) entsteht hier nochmals ein zusätzlicher Druck.

Eine Überraschung gegenüber dem letzten Jahr stellen wir noch bei Angriffen auf die Lieferkette fest. Waren diese im letzten Jahr noch unter den Top 5 vertreten, so sind sie heuer auf Platz Nummer neun. Die Gründe für die Veränderungen können vielfältiger Natur sein. Nichtsdestotrotz ist immer noch jeder zweite Angriff auf diese Form zurückzuführen.

Tiefer eintauchen

Wenn wir den Blickwinkel wechseln und von den tatsächlichen Angriffen hin auf die Risikowahrnehmung der Unternehmen gehen, so zeigt sich ein leicht verändertes Bild. Auf dem ersten Platz befindet sich Malware oder Schadsoftware. Das ist natürlich jene Form von Angriffen, die Mitarbeitende unmittelbar spüren, sei es in Form von E-Mails mit kompromittierenden Dateianhängen, in Form von Downloads oder aber auch auf Dateiaustauschplattformen.

Auf dem zweiten Platz überrascht der Datendiebstahl. Hier dominiert durchaus der hohe regulatorische Druck. Auch die Erfahrungen mit Ransomwareangriffen in den letzten Jahren, bei denen Datendiebstahl als Druckmittel eingesetzt wurde, haben hier Spuren bei den Unternehmen hinterlassen. Das Phänomen Ransomware ist folglich in der Risikowahrnehmung der Befragten sehr hoch angesiedelt.

Auf Platz Nummer drei befinden sich (Spear-)Phishingattacken. Bei dieser Angriffsart steht der Mensch im Mittelpunkt. Phishingangriffe sind für Unternehmen mittlerweile Tagesgeschäft, wodurch sie in der Wahrnehmung etwas in den Hintergrund rutschen und nicht diese hohe Aufmerksamkeit genießen. Fakt ist dennoch, dass durch den Einsatz von Künstlicher Intelligenz die Qualität der Phishingangriffe dramatisch zugenommen hat, was wir in den aktuellen Security-Awareness-Trainings noch nicht abgebildet sehen. Hier ist jedenfalls unmittelbarer Handlungsbedarf gegeben, da wir von den herkömmlichen Trainingsinhalten und den Themen der letzten Jahre auf neue Themen umschwenken müssen. Wir müssen die Herausforderungen in der technischen Erkennung – sowohl im Hinblick auf eingesetzte Erkennungssysteme als auch für den Menschen – in den Mittelpunkt rücken.

An vierter Stelle befindet sich der Identitätsdiebstahl. Dieser steht in Zusammenhang mit den Erfahrungen aus den Ransomwareattacken und Phishingangriffen. Identitätsdiebstahl ist ein bekanntes, aber dennoch sehr wirksames Phänomen, da das Identifizieren eines unerlaubten Zugriffs oftmals nicht auf Anhieb passiert und dadurch sämtliches Verhalten zunächst als herkömmliches bzw. gerechtfertigtes Verhalten von Mitarbeitenden ausgelegt wird.

Platz Nummer fünf belegt in diesem Jahr Ransomware. Die aktuellen Entwicklungen zeigen, dass Ransomware in Österreich leicht rückläufig ist, wiewohl die Angriffe immer noch Dominanz und Wirksamkeit aufweisen. Inwieweit das Risikobild mit den tatsächlichen Ereignissen korreliert und wie sich diese Zahlen in den nächsten 12 Monaten verändern werden, bleibt abzuwarten (siehe Abb. 12).

Weite Strecken zurücklegen

Über ein Drittel der befragten Unternehmen (36 Prozent) kann nicht einschätzen, wie hoch der finanzielle Schaden durch Cyberangriffe in den kommenden zwölf Monaten im Durchschnitt sein wird. Mit Hinblick auf NIS2 und die notwendige Quantifizierung der Schäden für das Risikosystem haben diese Unternehmen noch ein sehr großes Defizit aufzuholen.

Im Hinblick auf den maximalen finanziellen Schaden durch Cyberangriffe in den kommenden zwölf Monaten können sogar 41 Prozent keine Einschätzung abgeben. 48 Prozent der Unternehmen sagen zwar, dass sie ihr Cyberrisiko messen können, aber 41 bzw. 36 Prozent sind dennoch nicht in der Lage, die finanziellen Schäden zu quantifizieren. Hier haben wir einen Gap. In Bezug auf die regulatorischen Anforderungen und die damit einhergehende notwendige Quantifizierung von Schäden sehen sich Unternehmen also vor große Herausforderungen gestellt.

Über Wasser halten

Die Maßnahmen von Business Continuity Management (BCM) machen sich bezahlt. Mehr als die Hälfte der Unternehmen (54 Prozent) haben bereits eine Idee, wie sie bei einem größeren Cyberangriff reagieren werden. Unternehmen haben erkannt, dass Cyberangriffe ein Existenzrisiko darstellen und wollen hier handlungsfähig bleiben.

40 Prozent sind der Meinung, dass die Aufwände für Cybersicherheit nicht nur notwendige Kosten sind, die besser woanders eingesetzt werden können, sondern dass diese auch Resultate liefern.

Die Feinde abwehren

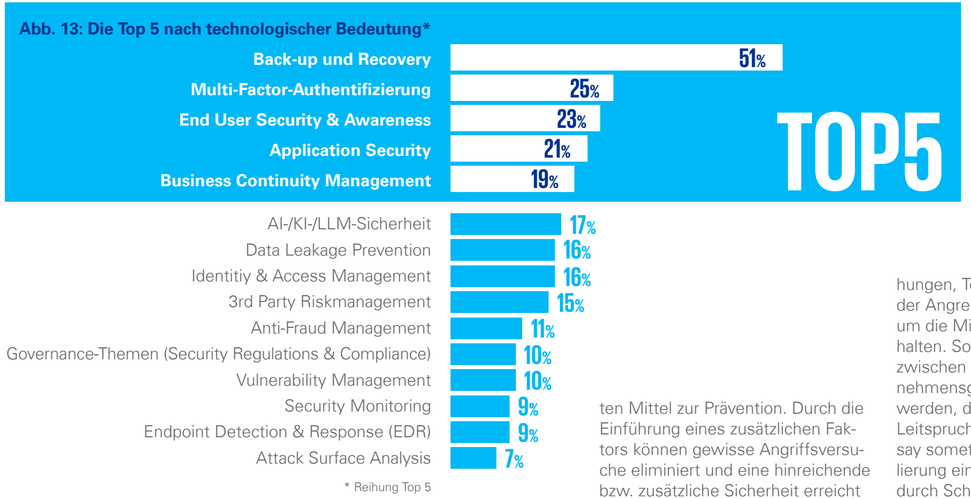
Die Top 5 Themen, mit denen sich Unternehmen aktuell beschäftigen, haben sich in den letzten 12 Monaten ebenfalls verändert. Es überrascht, dass ein zwar sehr wirkungsvolles, aber über die letzten Jahre durchaus in den Hintergrund gerücktes Thema, nämlich die Sicherung und Wiederherstellung der Daten (Back-up und Recovery), heuer den Spitzenplatz einnimmt. Unternehmen haben erkannt, dass es, obwohl es sich um ein traditionelles Thema handelt, das in die Grundzüge eines IT-Betriebs eingreift bzw. darauf aufbaut, alternativlos ist und sie sich damit auseinandersetzen müssen. Gerade Back-up und Recovery sind heute insoweit entscheidend, als dass es Unternehmen eine zeitnahe Wiederherstellung der Betriebsabläufe ermöglicht und so die Ausfallzeiten auf ein absolutes Minimum reduziert. Dies kann nur dann funktionieren, wenn die Wirksamkeit der Datensicherung und die Wiederherstellung regelmäßig geübt werden.

Die Multi-Faktor-Authentifizierung überrascht auf Platz zwei. Gerade bei (Spear-)Phishingattacken und Identitätsdiebstahl ist die Multi-Faktor-Authentifizierung eines der wirksamsten Mittel zur Prävention. Durch die Einführung eines zusätzlichen Faktors können gewisse Angriffsversuche eliminiert und eine hinreichende bzw. zusätzliche Sicherheit erreicht werden.

Auf dem dritten Platz befindet sich End User Security und Awareness. Das Thema ist im letzten Jahr um einen Platz zurückgerutscht, nimmt aber heuer immer noch eine Spitzenposition ein. Es kann nie genügend Sensibilisierung stattfinden, weshalb das Thema auch nie endgültig abgeschlossen werden kann. Laufende Kommunikation über aktuelle Bedrohungen, Techniken und „Maschen" der Angreifer:innen ist unabdingbar, um die Mitarbeitenden informiert zu halten. So kann auch der Austausch zwischen den Personen über Unternehmensgrenzen hinweg gefördert werden, denn es gilt auch hier der Leitspruch „If you see something, say something." Ohne die Etablierung einer Security-Kultur, z. B. durch Schulungen, wird es keinen offenen, transparenten, zeitnahen und raschen Informationsaustausch geben können, damit Angriffe – auch wenn sie erfolgreich gestartet sind – innerhalb kürzester Zeit erkannt und beendet werden.

Heuer erstmals in die Top 5 hat es Application Security auf den vierten Platz geschafft. Hierbei geht es um die Absicherung bzw. laufende Verbesserung der Sicherheit von

Abb. 13: Die Top 5 nach technologischer Bedeutung*



* Reihung Top 5

Anwendungen sowohl innerhalb der Organisation als auch für Webanwendungen. Unternehmen haben erkannt, dass gerade durch die Digitalisierung die Sicherheit von Applikationen an Bedeutung gewinnt und im Zusammenspiel mit Compliance und Regulatorik hier notwendige Schritte erforderlich sind, um die Digitalisierung im Unternehmen erfolgreich voranzutreiben.

Auf Platz Nummer fünf finden wir das Thema Business Continuity Management, das sich im Vergleich zum letzten Jahr um vier Plätze nach unten verschoben hat. Dennoch ist es weiterhin in den Top 5 vertreten und ist besonders im Zusammenspiel mit Back-up und Recovery eines der wesentlichen Komponenten für resiliente Unternehmen. Gerade um die Handlungsfähigkeit unserer Unternehmen in Krisenzeiten sicherstellen zu können, kann BCM die Grundlagen schaffen, damit eine Geschäftstätigkeit (wenn auch eingeschränkt) möglich ist. BCM ist uns schon seit über 20 Jahren bekannt, aber es ist aufgrund der immer komplexer werdenden Angriffe eine der Kernaufgaben der Unternehmen, um auch in turbulenten Zeiten die Kontrolle zu behalten (siehe Abb. 13).

Abb. 14: Übersicht Regularien*

	NIS2	DORA	EBA IKT Risk GL	CRA
Anwendungsbereich	Verschiedene wichtige Sektoren	Finanzmarkt & IKT Dienstleister	Bankinstitute	Hard- & Software Produkthersteller
Rechtlicher Charakter	Richtlinie der Europäischen Union, Nationale Umsetzung sowie Begleitgesetze	Verordnung der Europäischen Kommission. Gilt direkt.	Leitlinien gem. Verordnung (EU)	Leitlinien gem. Verordnung (EU)
Inhaltlicher Schwerpunkt	Kritische IKT Infrastruktur	Alle IKT Risiken (nicht nur Cyber!)	IKT Risiken	IKT Produktsicherheit

*Die Informationen beziehen sich auf den Zeitpunkt der Erstellung der Studie und können sich im Anschluss noch ändern.

Regulierter Cyberozean

Unternehmen haben sich bereits mit den großen, gängigen Regularien auseinandergesetzt. Das vorherrschende Thema ist NIS2: 76 Prozent haben sich schon mit dieser beschäftigt. Aber auch andere Themen kommen auf Unternehmen zu, denen sie sich annehmen müssen. Der Gesetzgeber legt den Fokus auf die Zurverfügungstellung von rechtlichen Rahmenbedingungen, um eine resiliente Infrastruktur und eine resiliente digitale Gesellschaft zu ermöglichen. Diese Resilienz ist unabdingbar, damit ein soziales Zusammenleben für uns als Gesellschaft möglich ist, die Zivilgesellschaft Infrastruktur und Versorgungseinrichtungen nutzen kann und Unternehmen sichere und widerstandsfähige Versorgungseinrichtungen haben und so die Grundlagen für einen resilienten Wirtschaftsraum geschaffen werden.

Wichtig ist dabei vor allem die Auslegung der einzelnen regulatorischen Anforderungen, die immer unter dem Aspekt der Technik und unter Berücksichtigung der Risikogegebenheiten zu etablieren sind. Hier gilt nochmals der Appell, dass gerade ein funktionierendes Risikomanagement, das sowohl qualitativ als auch quantitativ Risiken erfassen kann, in der Lage ist, Bruttorisiken, die Wirksamkeit von Kontrollen und in weiterer Folge die Nettorisiken zu identifizieren, um einen kontrollierten Umgang mit den sich laufend verändernden Bedrohungen zu schaffen.

Mehr zum Thema hören Sie in unserem Podcast mit Florian Schütz.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1.

Die Veränderung der Angriffe in den letzten 12 Monaten hat gezeigt, dass der Mensch weiterhin im Mittelpunkt steht. Jetzt wird der Fokus aber stärker auf eine Kombination aus Angriffen gegen Menschen gepaart mit verbesserten technischen Komponenten gesetzt. Das wird einmal mehr durch den Einsatz von Desinformationskampagnen unterstrichen.

2.

Auch manchmal noch so verstaubte Themen, die unattraktiv scheinen, sind das mit Abstand immer noch wirksamste Mittel, um hinreichende Vorsorge und Sicherheitsmaßnahmen zu treffen und um eine rasche Wiederherstellung zu ermöglichen. Back-up und Recovery ist die Grundlage für einen erfolgreichen Systembetrieb. Deshalb sollten Sie laufend die Funktionsweise testen und auch Ihre Dienstleister inkludieren. Holen Sie auch Nachweise ein, um sichergehen zu können, dass dies auch bei Ihren Dienstleistern funktioniert.

3.

Die Bezahlung von Lösegeldforderungen ist kritisch zu hinterfragen, denn gerade die Bezahlung führt dazu, dass man für Trittbrettfahrer:innen interessant wird und weitere Gruppen Angriffe gegen das Unternehmen versuchen durchzuführen. Investieren Sie in Sicherheits- und Erkennungsmaßnahmen sowie in ein funktionierendes Krisenmanagement. Und allem voran: Üben, üben, üben.

Cybersicherheit hat ein Transparenzproblem

Im Interview sprechen Florian Schütz und Robert Lamprecht über Herausforderungen und Strategien im Bereich Cybersicherheit sowie über die Bedeutung von Transparenz, Prävention und Bildung, um die nationale und internationale Cybersicherheit zu stärken.

Was ist die Aufgabe des Bundesamts für Cybersicherheit in der Schweiz und was ist Ihre Rolle?
Florian Schütz: Wir haben in der Schweiz eine Dreiteilung: Cyber Defense – also militärische nachrichtendienstliche Abwehr –, Strafverfolgung und Design der Sicherheit. Das Bundesamt für Cybersicherheit ist in der letzten Säule tätig. Unsere Aufgabe ist die Umsetzung und Weiterentwicklung der nationalen Cyberstrategie. Wir haben eine Anlaufstelle für Cybervorfälle, ein Computer-Emergency-Response-Team und betreiben eine nationale Plattform für kritische Infrastrukturen, die einen Austausch ermöglicht. Im präventiven Bereich arbeiten wir an Sensibilisierungsprogrammen für die Bevölkerung, Behörden sowie Unternehmen, und haben ein Team, das sich mit Standardisierung und Best Practices beschäftigt. Ein neuer Bereich befasst sich mit Datenanalyse und der Bereitstellung von Daten. Wir haben erkannt, dass es ein Transparenzproblem in der Cybersicherheit gibt und arbeiten daran, dieses zu beheben. Zudem unterstützen wir strategische Initiativen und arbeiten an der Errichtung von Cybersicherheitszentren in verschiedenen Branchen.

Cybersicherheit ist ein vielfältiges Thema. Was hat Sie dazu bewogen, in diesen Bereich zu gehen? Was hat Ihr Interesse geweckt?
Florian Schütz: Das hat schon in meiner Kindheit begonnen, als ich meinen ersten Computer bekommen habe. Ich habe angefangen, mich für das Programmieren zu interessieren und dafür, wie man Programme so manipulieren kann, dass sie nicht mehr das tun, was sie ursprünglich sollten. Mit meiner kindlichen Neugier habe ich begonnen, mich in Themen wie Viren und Betriebssysteme einzulesen. Dieser Forschertrieb hat mich in Folge zur Cybersicherheit geführt.

Sie sind bereits seit vielen Jahren im Bereich der Cybersicherheit tätig. Welche Entwicklungen im Bereich Cyberkriminalität haben Sie am meisten überrascht und was sollten wir wissen, um unsere Gegner:innen besser zu verstehen?
Florian Schütz: Überrascht ist vielleicht ein zu großes Wort, man härtet in diesem Metier leider etwas ab. Durchaus bemerkenswert finde ich aber, dass etwa 95 Prozent aller Vorfälle krimineller Natur sind. Kriminelle haben ein richtiges Geschäftsmodell und optimieren es auch – teils sogar effizienter als legale Firmen.

Es gibt zwei Arten von kriminellen Gruppen: Diejenigen, die breit gefächert agieren, wenig investieren und hoffen, unvorbereitete Opfer zu erwischen. Das ist leider immer noch die Mehrheit. Dann gibt es noch diejenigen, die mehr Zeit und Mühe investieren. Und trotz gestiegener Awareness sind viele Organisationen immer noch schwach aufgestellt und nehmen grundlegende Sicherheitsaufgaben nicht wahr. Das ist eine bemerkenswerte und besorgniserregende Entwicklung.

Sie sagen, dass die Awareness gestiegen ist – sind wir schon dort, wo wir hinmüssen, oder ist es noch ein weiter Weg?
Florian Schütz: Gesamtheitlich betrachtet sind wir noch nicht da, wo wir sein sollten – nicht nur in der Schweiz, sondern auch international. Sicherheit ist ein Prozess und es wird nie ein definitives Ziel geben, aber ich denke, dass wir auf einem guten Weg sind.

Aktuell wird versucht, viel mit Regulatorik zu bewirken. Ist die zunehmende Regulierung eine Reaktion auf das fehlende Bewusstsein der Unternehmen für Cybersicherheit? Glauben Sie, dass regulatorische Maßnahmen notwendig sind, weil Unternehmen und Gesellschaft noch nicht vollständig erkannt haben, wie wichtig Sicherheit ist?
Florian Schütz: In der Schweiz ist die Regulierung in Bezug auf Cybersicherheit nicht so stark ausgeprägt wie in anderen Ländern. Wir sind da eher zurückhaltend. Meiner Meinung nach hat Regulierung zwei Hauptfunktionen: Sie sorgt für fairen Wettbewerb und sie begrenzt

FOTO © PRIVAT

Florian Schütz
Direktor Bundesamt für Cybersicherheit in der Schweiz

Das Bundesamt für Cybersicherheit (BACS) ist das Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. In seiner Funktion als Direktor ist der gelernte Informatiker mit langjähriger Erfahrung in der IT-Sicherheit in der Privatwirtschaft zuständig für die koordinierte Umsetzung der Nationalen Cyberstrategie (NCS) und alle Cyberbelange beim Bund. Seit dem 1. Jänner 2022 hat Florian Schütz zudem den Vorsitz in der OECD-Arbeitsgruppe «Digital Security» (WPDS) inne. Damit kann die Schweiz einen wesentlichen Beitrag zur Erhöhung der Sicherheit im globalen digitalen Raum leisten.

übermäßiges Risiko. In der Schweiz regulieren wir punktuell. Seit 2004 gibt es beispielsweise eine freiwillige Meldepflicht für Cybervorfälle. Allerdings haben wir festgestellt, dass die Meldungen sehr unterschiedlich ausfallen. Einige Firmen melden sehr gewissenhaft, andere kaum oder gar nicht. Um hier für Gleichheit zu sorgen, hat das Parlament nun eine gesetzliche Meldepflicht beschlossen – ähnlich der NIS2-Direktive.

Ich bin der Meinung, dass man manchmal nicht um Regulierung herumkommt. Aber wir haben auch viele andere Mittel zur Verfügung, wie zum Beispiel Anreize, um bestimmte Verhaltensweisen zu fördern und den Markt zu stimulieren. Ein Bereich, in dem wir meiner Meinung nach noch nicht konsequent genug vorgehen, ist der Konsument:innenschutz, insbesondere wenn es um Endgeräte geht, die bei den Verbraucher:innen zu Hause stehen. Es ist heute schwieriger, einen Teddybären mit giftigen Farbstoffen zu kaufen, als einen Router, der voller Sicherheitslücken ist. Hier haben wir noch Möglichkeiten, die weniger reguliert, sondern eher informativ und proaktiv sind, die wir ausschöpfen können.

Also den Präventionsgedanken in den Vordergrund stellen, damit Sicherheit als fixer Bestandteil dazugehört?

Florian Schütz: Ja, Prävention ist ein wichtiger Aspekt, aber sie funktioniert nur, wenn die ökonomischen Mechanismen vorhanden sind. Es wäre wenig sinnvoll, den Markt zu schließen und nur den Verkauf von geprüften Geräten zu erlauben, da dies die Kosten in die Höhe treiben und uns im internationalen Vergleich weniger wettbewerbsfähig machen würde. Den Konsument:innen sollte aber eine informierte Kaufentscheidung ermöglicht werden. Sie sollten wissen, welche Risiken sie eingehen, wenn sie ein bestimmtes Gerät kaufen. Wenn sie wissen, dass sie durch das Ausgeben von etwas mehr Geld eine höhere Sicherheit erlangen können, bin ich überzeugt, dass die Mehrheit der Konsument:innen das auch tun wird.

Warum muss Sicherheit im Bereich der Technologie extra kosten? Warum sind wir hier noch nicht so weit wie z. B. in der Automobilindustrie, wo Sicherheitsmerkmale wie Sicherheitsgurte als Standard gelten?

Florian Schütz: Die Automobilindustrie ist älter und hat im Laufe der Zeit erkannt, dass Sicherheitsmerkmale wie Sicherheitsgurte unerlässlich sind. Anfangs waren diese nicht standardmäßig in Autos enthalten, aber nachdem man erkannt hatte, dass ihre Abwesenheit unverantwortlich war, wurden sie reguliert. Ich schließe Regulation in diesem Zusammenhang nicht aus, die Frage ist nur, wo genau sie angewendet werden sollte. Aus meiner Sicht und in meiner Rolle ist alles, was ein systemisches Risiko darstellt, von Interesse. Es ist provokativ, aber wenn eine Firma in Konkurs geht, ist das aus staatlicher oder systemrelevanter Sicht nicht so problematisch – der Markt regelt das. Es wird jedoch problematisch, wenn viele Firmen sich die notwendigen Sicherheitsmaßnahmen nicht mehr leisten können. Sie haben nach den Mehrkosten gefragt. Ein Auto könnte man billiger produzieren, besonders in Ländern mit niedrigeren Standards. Es gibt verschiedene ökonomische Mechanismen, um hochwertige Produkte günstiger herzustellen, meist über das Volumen. In der IT haben wir das Problem, dass wir oft Produkte auf den Markt bringen, die lediglich zu 80 oder 90 Prozent funktionieren und somit kann die Sicherheit des Produktes nicht hundertprozentig garantiert werden. Das bedeutet, dass Unternehmen Folgekosten einplanen und Prozesse haben müssen, um beispielsweise Schwachstellen zu adressieren. Hier könnte neben der Motivation auch ein gewisser Zwang notwendig sein, sei es durch den Markt oder durch internationale Regulierung.

Also eigentlich genau das, was die Europäische Union mit dem Cyber Resilience Act adressiert: dass digitale Produkte, ob einfache wie ein Teddybär oder komplexere wie Industriesteuerungsanlagen, über ihren Lebenszyklus hinweg mit Updates, Patches und Sicherheitsfunktionen versorgt werden können?

Florian Schütz: Ja, das ist die Grundidee des Cyber Resilience Act. Die Frage ist aber, wie man das umsetzt und wie weit man es ausdehnt, ohne die Innovation zu hemmen. Wir dürfen die Cybersicherheit nicht über alles stellen. Wenn ich z. B. ein kleines Walkie-Talkie zum Spielen habe, ist das Risiko gering. Aber wenn man eine Komponente in einer kritischen Infrastruktur einsetzt, ist das eine ganz andere Sache. Daher muss man in der Diskussion um Regulierung vorsichtig sein und durchaus auch differenzieren. Ich bin persönlich der Meinung, dass der Staat hier zwar eine Rolle hat, aber er versteht auch nicht alle feinen sektorspezifischen Mechanismen im Detail. Daher ist ein Austausch mit der Wirtschaft und der Zivilgesellschaft absolut notwendig. In der Schweiz haben wir als Behörde einen sehr guten Austausch mit der Industrie. Es finden offene Gespräche statt, in denen wir auch Einblicke in die Unternehmen und die Herausforderungen bekommen, mit denen sie konfrontiert sind.

> **Es ist heute schwieriger, einen Teddybären mit giftigen Farbstoffen zu kaufen, als einen Router, der voller Sicherheitslücken ist.**
>
> Florian Schütz

Sie sind vorrangig für die kritische Infrastruktur zuständig. Inwieweit können und dürfen Sie andere Unternehmen bei der Sicherheit und der Bewältigung von Cybervorfällen unterstützen?

Florian Schütz: Ich persönlich halte die Unterscheidung zwischen kritischer und nicht kritischer Infrastruktur für künstlich. Das ist eher szenarioabhängig. Wenn eine einzelne kleine Firma betroffen ist, ist das nicht systemkritisch. Aber wenn viele oder alle betroffen sind, wird es sehr kritisch für unser Wirtschaftssystem. Ich würde mir wünschen, dass wir diese Unterscheidung beiseitelegen und uns erlauben, auch reaktiv zu helfen, wenn wir die Zeit dazu haben – unabhängig davon, ob es sich um eine Schreinerei oder ein Kraftwerk handelt. Natürlich hat das Kraftwerk in einem solchen Fall Priorität, aber das ist eine Diskussion, die politisch geführt werden sollte.

Wie handhaben Sie Situationen, in denen Unternehmen bei Sicherheitsvorfällen eher auf die Identifizierung der Täter:innen fokussiert sind, anstatt sich auf die Krisenbewältigung zu konzentrieren?

Florian Schütz: Hier unterscheiden wir zwischen technischer Attribution, also der Wahrscheinlichkeit, dass eine bestimmte Täter:innengruppe verantwortlich ist, und politischer Attribution, bei der wir ein offizielles Statement abgeben, wer der:die Täter:in war. Bei der politischen Attribution sind wir sehr zurückhaltend, da wir uns immer überlegen müssen, welchen Mehrwert diese Attribution hat. Bei der technischen Attribution hängt es vom Vorfall ab. Bei einem niedrigschwelligen Vorfall macht die Attribution für die Firma oft wenig Sinn, da es wirtschaftlich sinnvoller sein kann, die Systeme einfach neu aufzusetzen. Für die Strafverfolgung ist es natürlich absolut relevant zu wissen, wer der:die Täter:in ist, aber hier muss man die Balance zwischen wirtschaftlicher Sinnhaftigkeit und den Möglichkeiten der Strafverfolgung finden. Bei Ransomwareangriffen und ähnlichen Vorfällen ist die technische Attribution entscheidend, um zu verstehen, wie man vorgehen kann. Kennt man die Täter:innengruppe, kann man vielleicht schon Muster in ihrem Vorgehen erkennen oder Informationen von internationalen Strafverfolgungsbehörden erhalten. Das hilft dann

dabei, die Daten zu schützen und die Situation besser zu handhaben.

Bedeutet das, dass wir eine Attribution auf verschiedenen Ebenen benötigen sowohl auf technischer Ebene für die unmittelbare Vorfallsbehandlung als auch auf politischer Ebene, um bestimmte Täter:innengruppen oder Akteur:innen einzuschränken und diese Einschränkungen über verschiedene Kanäle und Wege zu erreichen?
Florian Schütz: Ja, absolut. Es geht nicht nur um direkte Spionageangriffe, für die der Nachrichtendienst zuständig ist. Es geht auch darum, unsere Infrastrukturen im Land zu schützen. Zum Beispiel, wenn eine Firma Server betreibt oder vermietet und zulässt, dass diese von Kriminellen genutzt werden. Als Land möchten wir nicht, dass unsere eigene Infrastruktur dazu genutzt wird, unsere Firmen anzugreifen. Aber wir können auch nicht einfach sagen, dass wir die Server konfiszieren, weil es nicht die Firma ist, die kriminell ist, sondern ihre Infrastruktur missbraucht wird. Je nachdem, ob es sich um einen Telekommunikationsanbieter oder einen Internet-Serviceprovider handelt, kommen verschiedene Gesetze zur Anwendung. Das sind Themen, die uns sehr stark beschäftigen: Einerseits müssen wir uns auf legislativer Ebene überlegen, ob wir die richtigen Gesetze haben, um solche Situationen einzudämmen. Andererseits kann es auch hilfreich sein, eine abschreckende Wirkung zu erzeugen, indem wir zum Beispiel öffentlich machen, wenn Regeln nicht eingehalten werden, oder andere Wege finden, um gegen solche Firmen vorzugehen. Es gibt verschiedene Instrumente, die weniger invasiv, aber dennoch sehr wirksam sein können, und wir sollten sie entsprechend einsetzen.

In Österreich sehen wir eine klare Tendenz zum Wunsch nach österreichischen Security-Lösungen. Wie sieht es diesbezüglich in der Schweiz aus und welche Herausforderungen und Lösungen gibt es, um strategische Technologien im Land zu behalten?
Florian Schütz: In der Schweiz gibt es verschiedene Technologieunternehmen, die erste Schritte in Richtung Cybersecurity unternehmen. Es gibt einen Markt für große internationale Konzerne, oft amerikanische, und es ist wichtig, dass die Schweiz für diese attraktiv ist. Wir haben Forschungsstandorte großer Firmen in Zürich und Lausanne, was von Vorteil ist, da diese Unternehmen oft internationale Cloud-Lösungen kaufen. Es gibt jedoch auch andere Angebote und es ist gut, eine Auswahl zu haben. In der Schweiz gibt es immer wieder Diskussionen über die Notwendigkeit einer nationalen Cloud. Es gibt Schweizer Cloud-Anbieter, die vielleicht etwas weniger fortschrittlich und teurer sind, aber das Angebot ist vorhanden und meiner Meinung nach regelt der Markt das. Wenn es jedoch keine Anbieter mehr gäbe, müssten wir uns fragen, ob wir das marktwirtschaftlich laufen lassen können oder ob es eine regulative Intervention aus Gründen der Souveränität braucht. Hier kommt die politische Diskussion über Souveränität ins Spiel. Aber es ist nicht unsere Aufgabe zu bestimmen, wie viel Souveränität wir brauchen, sondern zu bewerten, welche Instrumente wir haben und wie die Realität aussieht, um der Politik eine fundierte Diskussion zu ermöglichen.

Infolge der multiplen Krisen der letzten Jahre und der aktuellen geopolitischen Lage erkennt Europa immer mehr die Wichtigkeit, unabhängig zu sein bzw. eigene Kompetenzen aufzubauen – das gilt natürlich auch bei Technologien. Wie stehen Sie zu diesem Thema?
Florian Schütz: Es ist illusorisch zu denken, dass Europa den gesamten Markt allein abdecken könnte. Es geht darum, dass man gemeinsam als Europa überlegt, wie man gewisse Redundanzen schaffen kann, die dann aber auch finanzierbar sein müssen. Es geht also nicht darum, sich vom globalen Markt abzuwenden, was nicht realistisch wäre, sondern darum, Optionen zu schaffen, die es uns ermöglichen, weiterhin an diesem Markt zu partizipieren.

Was ist die häufigste Frage, die man Ihnen gestellt hat, und was hat Sie noch nie jemand gefragt, obwohl es wichtig wäre, die Antwort zu kennen?
Florian Schütz: Unternehmer:innen stellen oft die Frage, wie sie Prioritäten setzen und was sie als nächstes tun sollen. Sie möchten auch wissen, welche Fragen sie der Geschäftsleitung stellen sollten. Diese Fragen sind absolut relevant und es ist oft möglich, dabei zu helfen, sie einzuordnen. Von der Bevölkerung kommen oft Fragen wie: „Ich habe eine Betrugs-E-Mail erhalten" oder „Ich habe eine E-Mail erhalten, die mich bedroht. Ist das echt?".

Eine Frage, die vielleicht noch zu wenig gestellt wird, ist: „Welche Chancen ergeben sich daraus, dass wir uns im Cyberraum schützen?" Es ist immer eine Bilanz von Chancen und Risiken. Länder, die strategisch clever gespielt und sich Chancen aus der Notwendigkeit der Cyberverteidigung geschaffen haben, sind vorne mit dabei. Ich wünsche mir, dass diese Frage öfter gestellt wird, weil sie eine positivere Perspektive in die Diskussion bringt.

Es ist also wichtig, das Positive zu sehen und zu überlegen, wie wir von Cybersicherheit profitieren können?
Florian Schütz: Ganz genau. Anstatt nur auf Verteidigung zu fokussieren, sollten wir in die Konstruktion resilienter IT-Systeme mit hohen Sicherheitsmerkmalen investieren. In den 90er-Jahren haben wir uns auf Firewalls verlassen, aber wenn das System dahinter nur sichere Verbindungen akzeptiert, ist eine Firewall überflüssig. Es sollte attraktiver sein, über den Bau sicherer Systeme zu sprechen. Ein System sicher zu bauen und verifizierbar zu machen ist eine Ingenieurskunst. Wir sollten stolz auf diese Kunst sein und sie entsprechend wertschätzen. Eine Verschiebung weg von dieser Wertschätzung ist nicht gesund für die Entwicklung.

Wie halten Sie die Motivation in Ihrem Team hoch, an diesen Themen weiterzuarbeiten, insbesondere wenn es schwierig ist, ein Ende zu sehen bzw. zu wissen, dass man eigentlich nie fertig wird?
Florian Schütz: Unsere Mitarbeiter:innen in diesem Bereich kommen mit hoher Eigenmotivation. Trotzdem kann es frustrierend sein, wenn man sieht, dass einfache Sicherheitsmaßnahmen nicht umgesetzt wurden und dadurch Probleme entstehen. Ein guter Austausch innerhalb des Teams und über die Hierarchieebenen hinweg hilft dabei, diesen Frust zu bewältigen. Darüber hinaus kompensieren wir die oft frustrierenden Aufgaben im Vorfallsmanagement durch Aufgaben in der Threat Intelligence, Datenanalyse und Prävention. Der Austausch mit der Wirtschaft und Fachpersonen sowie die Nähe zu Fach-Communities sind ebenfalls motivierend. Allerdings müsste man hierzu die Mitarbeiter:innen selbst fragen, weil als Chef:in sieht man das vielleicht auch ein bisschen verklärt.

Wenn wir uns in einem Jahr wieder treffen, was würden wir uns dann wünschen, heute schon getan zu haben?
Florian Schütz: In einem Jahr würde ich mir wünschen, dass wir heute schon mehr Transparenz geschaffen hätten. Ein Jahr ist zwar für strategisches Arbeiten nicht viel Zeit, aber Transparenz ist das Wichtigste, insbesondere weil wir hier auch die Selbstbefähigung in den Vordergrund stellen. Rückblickend könnten wir dann sagen, ob wir genug oder nicht genug getan haben, aber diese Transparenz müssen wir meiner Meinung nach adressieren. Es ist ein Pilotprojekt, in das wir investieren müssen.

Erfahren Sie mehr in unserem Podcast IMPULSE

87 % der Unternehmen, die von Social-Engineering-Angriffen/Erpressungen betroffen waren, haben in den letzten zwölf Monaten Versuche der Beeinflussung durch E-Mail-Nachrichten erlebt.

13 % Fast jedes siebte Unternehmen wurde Opfer von Social Engineering im Kontext von Deepfake.

54 % Der belastendste Aspekt bei einem Cybersicherheitsvorfall ist für die Befragten die Komplexität der Systemumgebung.

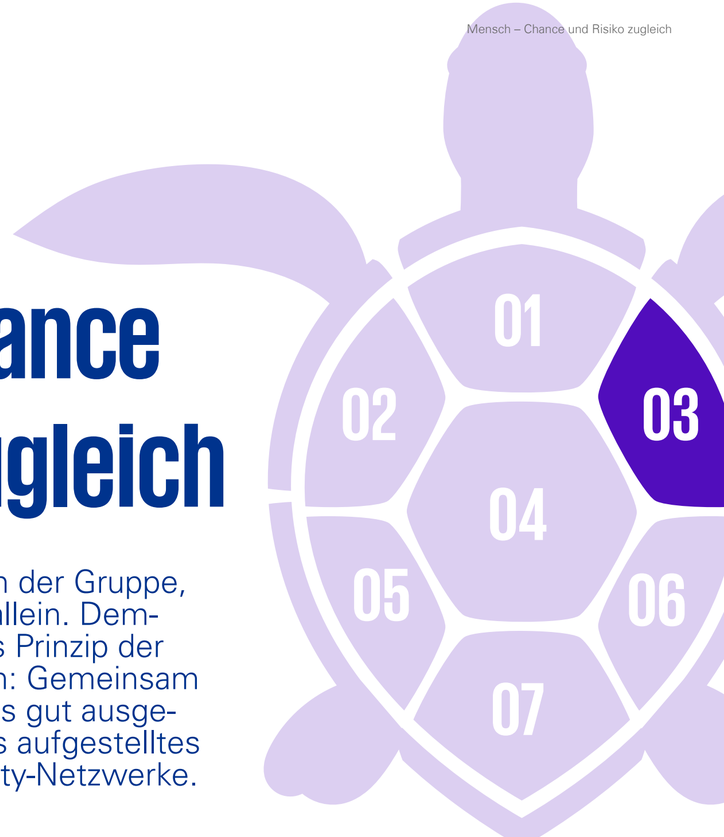
35 % der Befragten, die selbst bei der Aufarbeitung eines Cyberangriffs involviert waren, wollen nicht darüber sprechen, wie häufig sie dabei physische oder psychische Auswirkungen oder Erkrankungen erlebt haben.

63 % Die dominantesten psychischen Auswirkungen für diejenigen, die bei einem Cybersicherheitsvorfall involviert waren, waren Stress und Angst.

27 % der Unternehmen brauchen durchschnittlich 4–6 Monate, um IT-Expert:innen einzustellen.

Mensch – Chance und Risiko zugleich

Schwimmt unsere Schildkröte in der Gruppe, ist sie weniger verwundbar als allein. Demselben Grundgedanken folgt das Prinzip der Cybersicherheit in Unternehmen: Gemeinsam sind wir stärker. Dafür braucht es gut ausgebildete Fachkräfte und ein divers aufgestelltes Team für funktionierende Security-Netzwerke.



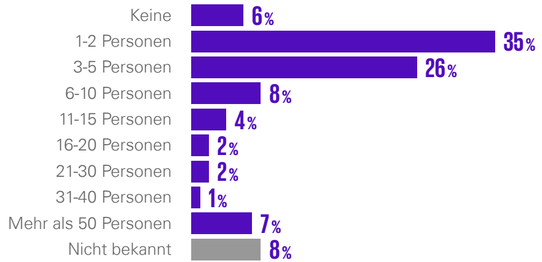
Instabiles Ökosystem

35 Prozent der Befragten beschäftigen 1–2 Mitarbeitende im Bereich Cybersecurity. Bei 26 Prozent sind 3–5 Cybersecurity-Mitarbeiter:innen im Einsatz. Bei immerhin 7 Prozent sind mehr als 50 Personen mit Cybersecurity betraut.

Beim Frauenanteil zeichnet sich ein ähnlich düsteres Bild wie im Vorjahr ab: Knapp jedes zweite Unternehmen (47 Prozent) beschäftigt nach wie vor keine Frau im Bereich Cybersecurity. Dass dieser Wert im Vergleich zum letzten Jahr gleich geblieben ist, zeigt uns, dass wir die Notwendigkeit eines divers aufgestellten Teams mit unterschiedlichen Hintergründen, Problemlösungskompetenzen, Zugangsarten und Sichtweisen zur effektiven Bekämpfung von Cybercrime immer noch nicht verstanden haben. Unternehmen haben hier noch viel Aufholbedarf. Bei einer durchschnittlichen Größe der Cyberabteilung von 7 Personen beträgt der Frauenanteil 6 Prozent. Arbeiten durchschnittlich 9 Personen in der Cyberabteilung, sind davon 14 Prozent Frauen. Umfasst die

> **Technische Bereiche sind für Frauen nach wie vor abschreckend und ich würde behaupten, auch schwerer zugänglich. Ich habe als Frau in der IT selbst damit zu kämpfen, entsprechend „ernst genommen" zu werden.**
>
> Quelle: Studienteilnehmerin

Abb. 15: Mitarbeiter:innen in Cybersecurity-Abteilungen



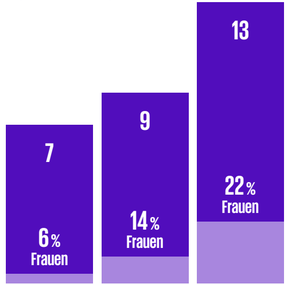
Cyberabteilung durchschnittlich 13 Mitarbeitende, haben wir einen Frauenanteil von 22 Prozent. Wir sehen also, dass Cyber-Mitarbeiterinnen als Pull-Faktor für weitere Mitarbeiterinnen fungieren (siehe Abb. 16).

Gegen den Strom

Erklärungen dafür, dass im Bereich Cybersecurity in Österreich weniger Frauen als Männer tätig sind, gibt es viele. Unsere Befragten folgern, dass Frauen z. B. nach wie vor in den MINT (Mathematik, Informatik, Naturwissenschaft und Technik)-Fächern unterrepräsentiert sind.

Ein Grund könnte der weiterhin bestehende Gender-Bias sein. Ein:e Befragte:r nannte hier als Beispiel einen Chatbot, der Mädchen „weniger technische" Berufe nahegelegt hat. Die Unterrepräsentation von Schülerinnen und Studentinnen an den facheinschlägigen Ausbildungseinrichtungen hat auch weniger Frauen im IT-Bereich zur Konsequenz. Durch veraltete Denkweisen und Rollenbilder in Gesellschaft und Ausbildung werden Kinder in bestimmte Richtungen sozialisiert. Es hält sich der Irrglaube, dass Männer technisch qualifizierter sind. Dadurch

Abb. 16: Frauenanteil in Cybersecurity-Abteilungen



trauen sich viele Frauen den Beruf nicht zu, auch wenn sie Interesse daran haben. Die Ermangelung an Möglichkeiten für einen Quereinstieg oder späteren Umstieg in den Bereich wurde ebenso als mögliche Erklärung von unseren Befragten genannt.

Vorübergehender Rückzug

Auch das Berufsbild an sich kann auf einige Frauen durchaus abschreckend wirken. Assoziationen, die unsere Umfrageteilnehmer:innen mit dem Thema in Verbindung gebracht haben, waren: Männerdomäne und damit verbundene zusätzliche Hürden, unzureichende Kinderbetreuung und fehlende Arbeitszeit-Flexibilität der Unternehmen, teilweise nicht planbare Arbeitszeiten bei einem Sicherheitsvorfall, Gender-Pay-Gap, teilweise fehlende Akzeptanz der männlichen IT-Belegschaft, sexistisches Arbeitsumfeld sowie männlich geprägte Umgangsformen, mit denen sich Frauen nicht wohlfühlen. Vor diesem Hintergrund ist auch unser Ergebnis, dass Frauen in der IT-Abteilung als Pull-Faktoren für weitere Frauen fungieren, einzuordnen und noch einmal mehr nachvollziehbar.

Diversität stärken

Damit wir die Diversität im Cybersecurity-Bereich insgesamt stärken können, finden es Befragte wichtig, bereits früh das Interesse für Technik bei allen Geschlechtern zu wecken und auch aufzuzeigen, welche unterschiedlichen Aufgabengebiete (z. B. die psychologische Komponente bei Phishing und Social Engineering) es gibt. Es braucht eine frühzeitige Bestärkung von Mädchen, die sich für Cybersecurity interessieren, bei gleichzeitiger Aufklärungsarbeit für Buben und Männer, wie sie ein angenehmeres Umfeld schaffen können.

> **Ich denke, wenn eine Frau in diesem Bereich studieren und arbeiten will, hat sie in Österreich durchaus faire und gute Möglichkeiten. Was aber immer noch vorkommt und nicht vorkommen sollte, ist ungleiche Behandlung, ungleiche Bezahlung, Angst vor Ausfallzeiten durch Karenz und die Tatsache, dass Frauen in dem Bereich von vielen Vorgesetzten automatisch weniger zugetraut wird, ohne fundierte Grundlage.**
>
> Quelle: Studienteilnehmer:in

Anreize setzen

In Unternehmen selbst braucht es laut Befragten eine Geschäftsleitung, die für Diversität einsteht, sowie eine Änderung der Denkweisen und

mehr Awareness. Auch Schulungen für Mitarbeitende und Führungskräfte sowie der Bewusstseinsaufbau, dass diverse Teams erfolgreicher sind, wurden hier genannt. Ein wesentlicher Hebel wäre, mehr Frauen in Führungspositionen zu haben. Es ist wichtig, Anreize für Frauen und attraktivere Arbeitsbedingungen sowie Arbeitszeitmodelle zu schaffen und die gleiche Bezahlung für alle Geschlechter sicherzustellen. Relevante Aspekte sind auch Quereinstieg, Training on the Job sowie Möglichkeiten zum Umstieg, speziell auch für ältere Arbeitnehmerinnen, die sich neuorientieren möchten.

Es braucht einen gesellschaftlichen Wandel – angefangen bei Gleichstellung in der Bezahlung bis zur flächendeckenden Bereitstellung von Kinderbetreuung. Bildungsangebote, die schon früh ansetzen – im Kindergarten beginnend – nicht erst auf der Universität. Puppenspielen mit den Buben und Legobauen mit den Mädels und alle Schattierungen dazwischen auch mitnehmen - stereotype Klischees proaktiv aufbrechen!

Quelle: Studienteilnehmer:in

Zusammenspiel

Auf gesellschaftlicher/staatlicher Ebene wurde der Ausbau der Kinderbetreuung in ländlichen Gebieten genannt. Weitere entscheidende Faktoren sind die gerechte Aufteilung der Care-Arbeit auf die Geschlechter und Karenzmöglichkeiten für Männer. Immer wieder wurden auch Quotenregelungen als probates Mittel angeführt.

Guter Orientierungssinn

Die Vorbildwirkung wird als essenziell gesehen. Es braucht neben weiblichen Vorbildern für Mädchen auch explizit auf Mädchen und Frauen ausgerichtete Werbung für den MINT-Bereich. Bei facheinschlägigen Vorträgen, Round Tables und Events sollten vermehrt Frauen sowie nicht binäre Personen eingeladen werden. Auch die Wichtigkeit von weiblichen Vortragenden im Ausbildungsbereich wurde betont.

Volle Kraft voraus

Trotz der vielen noch offenen Hausaufgaben für Unternehmen und die Gesellschaft beobachten die Befragten, dass Cybersecurity zwar bis jetzt eher als Männerdomäne gegolten hat, aber bereits bemerkbar ist, dass bei den jüngeren Generationen der Frauenanteil im IT-Bereich nach und nach steigt.

Gleichzeitig steht aber klar der Appell im Vordergrund: Wir müssen jetzt von der Maßnahmendiskussion in die Umsetzung kommen.

Es geht um Ausdauer

43 Prozent der Unternehmen stehen vor der großen Herausforderung, geeignete IT-Expert:innen zu rekrutieren. Sie empfanden die Rekrutierung in den letzten zwölf Monaten als äußerst schwierig. Bei ca. einem Viertel ist die Herausforderung gleich geblieben. Jedes zehnte Unternehmen hat keine Schwierigkeiten dabei und meint sogar, es sei im Vergleich zum Vorjahr besser geworden. Die Schwierigkeiten beim Thema Rekrutierung von Mitarbeiter:innen hat sich augenscheinlich auf einem sehr hohen Niveau eingependelt. Das Problem ist allerdings weiterhin präsent. Unternehmen können dem mit eigenen Initiativen entgegenwirken und z. B. zusätzliche Weiterbildungen/Qualifizierungen anbieten.

Das Gros der Unternehmen (27 Prozent) braucht durchschnittlich 4–6 Monate, um IT-Expert:innen einzustellen. 14 Prozent benötigen 7–12 Monate, Immerhin 19 Prozent brauchen 1-3 bzw. sogar weniger als einen Monat. 4 Prozent sogar mehr als 12 Monate. Am häufigsten kommen IT-Mitarbeiter:innen durch Bewerbungen in die Unternehmen, am zweithäufigsten über Fachhochschulen. Am dritten Platz befindet sich bereits die aktive Abwerbung von Expert:innen. An vierter Stelle werden Quereinsteiger:innen selbst im Unternehmen ausgebildet und an fünfter Stelle kommen die IT-Mitarbeiter:innen von den (Berufsbildenden) Höheren Schulen, gefolgt von den Universitäten (siehe Abb. 19)

Flexible Tiefseebewohner

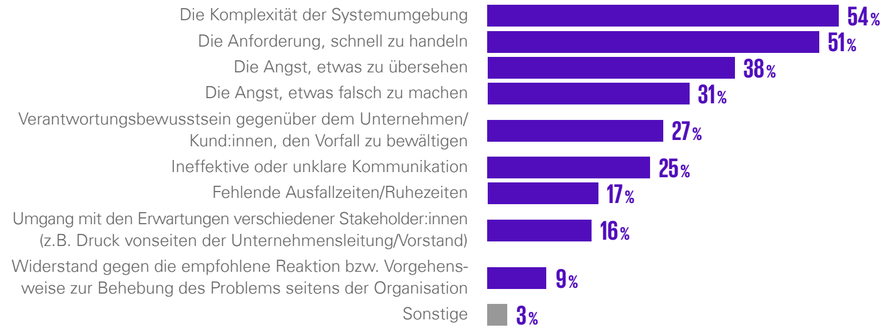
Unternehmen erkennen, dass der Pool an IT-Expert:innen in Österreich ausgeschöpft ist. Nur mehr 39 Prozent sagen, dass sie ihre IT-Expert:innen ausschließlich in Österreich rekrutieren. Im Vorjahr waren das noch 45 Prozent. 22 Prozent finden, dass es leichter ist, IT-Expert:innen im europäischen Ausland zu rekrutieren als in Österreich. Das hat sich auch gegenüber letztem Jahr nicht verändert.

12 Prozent erlauben es ihren IT-Expert:innen im Ausland im Homeoffice zu arbeiten. 14 Prozent stellen auch IT-Expert:innen außerhalb der EU an. Das ist eine der Folgen der

Abb. 17: Herausforderung (HF) vs. Tagesgeschäft (TG) im Jahresvergleich

	HF Rang 2024	HF Veränderung zu 2023	TG Rang 2024	TG Veränderung zu 2023
Angriff auf Zuliefer-/Kundensysteme	10	-1	9	2
CEO-Fraud	17	2	3	-2
Cloud Failure	12	-2	8	1
Cryptominer	13	0	7	0
Data Leakage	5	0	15	0
DDoS	14	1	5	-1
Fake News/Rufschädigung	9	3	11	-3
Identitätsdiebstahl	8	-1	12	1
Insider Threat	4	-1	16	0
Malware	14	1	5	-1
OT-Security	6	2	14	-2
Passwortdiebstahl	16	-2	4	2
Phishing	19	-1	1	1
Ransomware/Erpressung	2	0	18	0
Social Engineering	10	0	9	0
Spoofing	18	-1	2	1
Spyware	7	-1	13	1
Staatliche oder staatlich unterstützte Angriffe	1	0	19	0
Zero Day	3	1	17	0

Abb. 18: Die belastendsten Aspekte bei einem Cybersicherheitsvorfall*



* Top-3-Aspekte je Teilnehmer:in

letzten Jahre. Unternehmen machen sich zielgerichtet auf die Suche nach Fachkräften über Grenzen hinweg, da sie erkannt haben, dass das nicht mehr nur in Österreich allein geht. Das ist eine klare Ansage an den Wirtschaftsstandort Österreich.

Veränderte Angriffslage

Wenn wir nun die Phänomene anhand ihrer Bedeutung für die Unternehmen einordnen, zeigt sich, dass Social Engineering als Bedrohung an sich auf Platz zehn zu finden ist. Allerdings kann Social Engineering heute nicht mehr isoliert betrachtet werden. Auf Platz eins stehen Fake News und Rufschädigung. Genau diese Phänomene stellen eine besondere Herausforderung für die Unternehmen dar und sind im Vergleich zum letzten Jahr um drei Plätze nach oben gewandert. Ein weiteres Phänomen, das um zwei Plätze hinaufgeklettert ist, ist der CEO-Fraud. Auch dabei geht es um die gezielte Beeinflussung des Gegenübers. Es soll eine Machtstellung ausgenutzt werden, um so Finanztransaktionen im Auftrag eines:einer Entscheidungsträger:in durchzuführen (siehe Abb. 17).

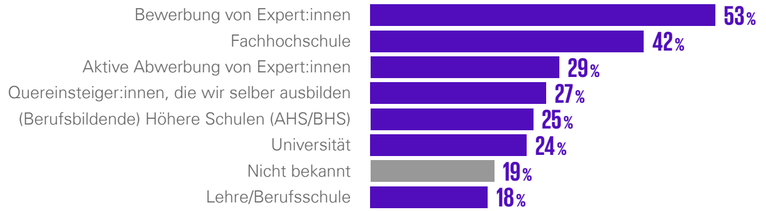
Es ist nicht so, wie es scheint

Mitarbeitende stehen im Fokus von Cyberangriffen, wie unsere letztjährige Studie verdeutlicht hat. Auch dieses Jahr ist eine Vielzahl von Angriffen bemerkbar, die sich direkt und gezielt gegen die Mitarbeiter:innen richtet. Social Engineering ist ein gefährliches Einfallstor in die Systeme der Unternehmen.

Unternehmen, die von Social-Engineering-Angriffen/Erpressungen betroffen waren, haben am häufigsten (87 Prozent) durch E-Mail-Nachrichten in den letzten zwölf Monaten Versuche der Beeinflussung erlebt. Weitere wesentliche Kanäle, über die die Unternehmen angegriffen wurden, waren Telefonanrufe (58 Prozent), Messengerdienste wie WhatsApp oder Telegram (49 Prozent) sowie beruflich genutzte soziale Netzwerke (36 Prozent) und privat genutzte soziale Netzwerke (20 Prozent). Bei den EPUs ist abweichend davon zu beobachten, dass jedes zweite (50 Prozent) über privat genutzte soziale Netzwerke angegriffen wurde und nur 13 Prozent über beruflich genutzte. Hier ist allerdings zu bedenken, dass gerade bei EPUs die Grenze zwischen privat und beruflich genutzten sozialen Netzwerken nicht immer klar gegeben ist.

Das Phänomen Deepfake in Form von Sprach- und Videonachrichten nimmt Fahrt auf: 13 Prozent der Unternehmen wurden in diesem Kontext Opfer von Social Engineering.

Abb.19: Recruiting/Herkunft der IT-Expert:innen*



* Mehrfachnennungen möglich

Belastende Ereignisse

Kommt es zu einem Cybersicherheitsvorfall im Unternehmen, sind diejenigen, die darauf reagieren müssen, großen Belastungen ausgesetzt. Der belastendste Aspekt ist für die Befragten die Komplexität der Systemumgebung. Obwohl diese zwar ein großer Treiber mit 54 Prozent ist, geben auch 51 Prozent die Anforderung an, schnell handeln zu müssen. Weitere belastende Aspekte sind die Angst, etwas zu übersehen (38 Prozent) und die Angst, etwas falsch zu machen (31 Prozent). Schnelles Handeln wird demnach über sorgfältiges Handeln gestellt. Unternehmen müssen aufpassen, dass schnelle Reaktionszeiten nicht Qualitätseinbußen bei der korrekten Bearbeitung des Sicherheitsvorfalls zur Folge haben.

Wenngleich Unternehmen schnelles Handeln in einer Krise oder in einer Ausnahmesituation fordern, so ist hier wesentlich zwischen schnellem und kontrolliertem Handeln und überhastetem Handeln ohne jeglichen Plan zu unterscheiden. Damit Unternehmen ein kontrolliertes, aber auch schnelles Handeln in Ausnahmesituationen schaffen können, ist regelmäßiges Üben unerlässlich. Durch laufendes und wiederkehrendes Praktizieren der Handgriffe und Fertigkeiten – vom Anlernen über die Festigung bis hin zur Perfektionierung – schaffen es Unternehmen, eine Automatisierung ihrer Abläufe und Handgriffe zu erreichen. Vor allem in Krisen geben diese Fertigkeiten enorme Sicherheit.

Mensch – Chance und Risiko zugleich

Je nach Vorfall könnte es sein, dass man nicht weiß, ob die Daten, die nun im System sind, korrekt sind oder verfälscht wurden, falls kein Restore durchgeführt wird bzw. der genaue Zeitpunkt der Attacke(n) unbekannt ist. Außerdem wäre es ein großer Vertrauensbruch gegenüber denen, die uns ihre Daten anvertraut haben und würde unseren Ruf nachhaltig schädigen.

Quelle: Studienteilnehmer:in

Das Verantwortungsbewusstsein gegenüber dem Unternehmen / den Kund:innen, den Vorfall zu bewältigen, ist ebenfalls belastend für die Befragten (27 Prozent). Darüber hinaus hat eine ineffektive oder unklare Kommunikation (25 Prozent) negative Auswirkungen. Fehlende Ausfall- bzw. Ruhezeiten (17 Prozent) werden ebenso als problematisch empfunden. Auch der Umgang mit den Erwartungen verschiedener Stakeholder:innen, wie z. B. der Druck vonseiten der Unternehmensleitung / dem Vorstand, wurde als belastend eingestuft (16 Prozent) (siehe Abb. 18).

Zusätzlich berichten die Befragten von fehlendem Personal/Ressourcen und mangelnder Zeit für Übungen sowie darüber, dass keine klaren Prozesse vorhanden sind. Diese werden meistens erst erstellt, nachdem etwas passiert ist. Die Trägheit bei den Dienstleistern sowie der Vertrauensverlust in die eigenen IT-Systeme sind weitere belastende Faktoren.

Im Netz gefangen

Im Schnitt wollen 35 Prozent derjenigen, die selbst bei der Aufarbeitung eines Cyberangriffs involviert waren, nicht darüber sprechen, wie häufig sie dabei physische oder psychische Auswirkungen oder Erkrankungen erlebt haben.

Bei denjenigen, die darüber Auskunft gegeben haben, waren die dominantesten Auswirkungen des Cybersicherheitsvorfalls Stress und Angst (63 Prozent). Auf dem zweiten Platz findet sich Schlaflosigkeit (47 Prozent), danach Schuldzuweisungen (46 Prozent), gefolgt von Auswirkungen auf das soziale Leben / die Beziehungen (44 Prozent). Aggression befindet sich auf dem fünften Platz (40 Prozent).

Ein weiterer Stressfaktor entsteht durch aufgeschobene Arbeiten, Nacharbeiten und die Implementierung unternehmensweiter Standards. Ebenfalls genannt wurden erhöhte Anspannung und gesteigerter Alkoholkonsum.

Anpassungsfähigkeit

Durch die rasanten Entwicklungen im Bereich Cybersecurity wird es immer schwieriger, Cyberangriffe zu erkennen und abzuwehren. Nicht nur werden wir mehr Expert:innen benötigen, sondern auch jene, die mit diesen Veränderungen Schritt halten können. So ist z. B. noch schwer abschätzbar, welche neuen Bedrohungen durch Künstliche Intelligenz auf uns zukommen. Eines ist jedoch klar: Unternehmen müssen gut aufgestellt sein, um nicht unterzugehen.

Mehr darüber, wie sich Unternehmen schützen können, erfahren Sie in unserem Podcast mit Stéphane Duguin.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1.

Unternehmen erkennen, dass der Pool an IT-Expert:innen in Österreich ausgeschöpft ist. Nur mehr 39 Prozent sagen, dass sie ihre IT-Expert:innen ausschließlich in Österreich rekrutieren. Im Vorjahr waren das noch 45 Prozent. 22 Prozent finden, dass es leichter ist, IT-Expert:innen im europäischen Ausland zu rekrutieren als in Österreich. Das hat sich auch gegenüber letztem Jahr nicht verändert.

2.

12 Prozent erlauben es ihren IT-Expert:innen im Ausland im Homeoffice zu arbeiten. 14 Prozent stellen auch IT-Expert:innen außerhalb der EU an. Das ist eine der Folgen der letzten Jahre. Unternehmen machen sich zielgerichtet auf die Suche nach Fachkräften über Grenzen hinweg, da sie erkannt haben, dass das nicht mehr nur in Österreich allein geht. Das ist eine klare Ansage an den Wirtschaftsstandort Österreich.

3.

Durch die rasanten Entwicklungen im Bereich Cybersecurity wird es immer schwieriger, Cyberangriffe zu erkennen und abzuwehren. Nicht nur werden wir mehr Expert:innen benötigen, sondern auch jene, die mit diesen Veränderungen Schritt halten können. So ist z. B. noch schwer abschätzbar, welche neuen Bedrohungen durch Künstliche Intelligenz auf uns zukommen. Eines ist jedoch klar: Unternehmen müssen gut aufgestellt sein, um nicht unterzugehen.

Lack of trust as the greatest threat

Stéphane Duguin, CEO of the CyberPeace Institute, in conversation with Robert Lamprecht about the challenges of international cooperation in the field of cybersecurity and the impact of artificial intelligence.

Can you tell us what the CyberPeace Institute does – what are its tasks?
Stéphane Duguin: The CyberPeace Institute is a non-profit organization based in Geneva. It was founded in December 2019. We support the most vulnerable in the field of cybersecurity and focus mainly on NGOs. But not only do we provide free support in this area, we also independently analyze the major threats that exist in cyberspace and work with many volunteers from the private sector who support us with their time and knowledge.

And we use this knowledge to inform policy makers. The basic idea is that better laws, better regulation and better enforcement of standards and laws by states should logically lead to systemic change so that vulnerable communities are no longer at risk.

In your opinion, what are the biggest differences between Austria and other countries in dealing with cybercrime and cyberthreats?
Stéphane Duguin: When it comes to building resilience, investigating crimes, identifying perpetrators and bringing them to justice, you need international cooperation. Thanks to its membership of the European Union, Austria has the advantage of having access to many instruments and capacities to combat cybercrime, such as Europol and the Council of Europe. In addition, Austria appointed a cyber ambassador early on to build capacity and have a dedicated representation at the highest and diplomatic level for discussions on cybercrime. That is a pretty good investment. Nevertheless, Austria, like many other countries, suffers from a disconnect between the cybersecurity community and the law enforcement and justice community.

What are the biggest challenges for international cooperation and how could we improve this cooperation?
Stéphane Duguin: The main challenges for international cooperation in the fight against cybercrime lie in the need to build trust between countries and ensure effective cooperation at multiple levels. As cybercrime and cyberattacks are often transnational, cooperation between states is crucial. Sometimes this also requires a multi-stakeholder approach, working with the private sector and civil society in other countries to get a holistic view of an incident.

> **The aim is to instigate systemic change via improved laws, regulation, and state enforcement, safeguarding vulnerable communities at risk.**
>
> Stéphane Duguin

To improve international cooperation, we need to ensure that we know exactly which country the attacks are coming from and that we can rely on that country to take responsibility for them. This requires a high level of trust in cyberspace, which is currently a major challenge.

How can we build this trust? How can this work in a digital world?
Stéphane Duguin: This is a complex task that needs to be tackled both inside and outside the cyberspace. We are currently seeing a loss of trust at an international level, which is also having an impact on cooperation in cyberattacks. The concealment and manipulation of information in connection with cyberattacks make the situation even more difficult.

To build trust, it is important that agreements such as not targeting civilian targets or not spying on critical infrastructure are adhered to. However, this is difficult due to the current low level of trust.

Another important aspect is the rules in cyberspace. Currently, the norms for responsible behavior in cyberspace are not clearly defined and there are no binding rules of conduct. In addition, there is no measurement of whether these standards are implemented or not, which further undermines trust.

To solve this problem, states need to take on a leading or pioneering role. However, the forum in which this should happen, the United Nations, has not been very strong in this regard recently. It is therefore difficult to have this discussion.

You support NGOs and similar organizations and have a good overview of the current threats and challenges. What are currently the most common threats from cyberspace that companies face today?

FOTO © PRIVAT

Stéphane Duguin
CEO CyberPeace Institute

Stéphane Duguin has spent two decades tacking how criminal groups and terrorists weaponize technologies like AI. As senior manager at Europol, he led operations against cybercrime, terrorism and hybrid threats and investigated threat actors deploying cyberattacks, illegal content and disinformation techniques. Today, he leads the CyberPeace Institute, providing free cybersecurity to NGOs who protect the most vulnerable and holding threat actors accountable for the harm that they cause. Duguin is the board member of several initiatives and has published extensively on AI, cybercrime, and disinformation.

Stéphane Duguin: The most common threats are those that could be avoided by simple cyber hygiene. In fact, 80 to 90 percent of attacks could be prevented by basic security measures.

The threats themselves vary depending on the company and its size, but one clear trend is the acceleration of crime through fraud by means of phishing and social engineering. These methods are being used more and more frequently due to increasing digitalization and networking.

Another problem is the increasing use of surveillance and espionage programs. Many states use taxpayers' money to finance private companies to carry out cyberattacks or implement surveillance measures. This undermines security on the internet and leads to a contradiction between the desire for security and the actual practice of states.

How can companies protect themselves as well as their employees and customers?

> **Trust in cyberspace is the biggest problem.**
>
> Stéphane Duguin

Stéphane Duguin: By building a culture of cybersecurity. This includes not only using cybersecurity services, but also being aware of their dependence on the cybersecurity of others. As companies often use third-party software, they are also dependent on the cybersecurity of that software.

An important step in strengthening cybersecurity is working with the private sector. Companies can provide resources and volunteers who have a better understanding of cyber issues. These cyber volunteers can help non-profit, humanitarian organizations that often don't have the money or capacity to protect themselves.

This collaboration is not only good for society, but also opens volunteers' eyes to the reality beyond their own ecosystem. They begin to think about the interconnectivity of resilience and realize that their own cybersecurity doesn't make sense in an interconnected system if they don't also consider the security of others.

Ultimately, a cultural change is required. We need to understand that we are interdependent and that our cybersecurity alone does not make sense. Only by working together and supporting each other can we create a secure digital environment.

One topic that is attracting more and more attention these days is the impact of artificial intelligence. To what extent do you think AI is accelerating misinformation and disinformation? Are we already aware of the consequences?
Stéphane Duguin: Artificial intelligence influences misinformation and disinformation by facilitating the production and dissemination of manipulated content. This is particularly relevant in the context of elections – but this is not a new phenomenon, as information has been manipulated for decades. The methods have not changed significantly – it is still about the falsification of information and its influence.

> **AI is not a new threat, but merely an acceleration of the existing threat.**
>
> Stéphane Duguin

However, with the development of AI and its ability to generate content, the scale and speed at which this manipulated information can be produced and disseminated has increased. In particular, social media platforms and mainstream media taking content from social media have helped to spread this manipulated information in the past.

It is important to emphasize that AI is not the fundamental problem, but rather a tool that exacerbates existing problems.

The European Union is increasingly addressing these new technological threats with new regulations. Do you think we need stricter regulations for AI at an international level?
Stéphane Duguin: I think regulation of AI is inevitable and also necessary – although it is a challenge, as the technology is already developing rapidly. It's like trying to build the track in front of a moving train.

A turning point could be when AI is so advanced that it can independently do things that the user wants it to do, or even things that the user doesn't even know they want it to do. This would be a game changer and a completely new threat.

> **We need to understand that we are interdependent and that our cybersecurity alone makes no sense.**
>
> Stéphane Duguin

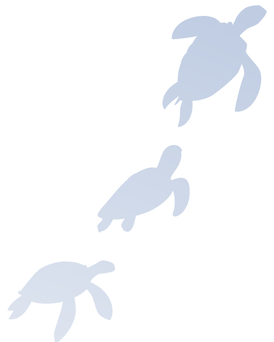
However, the biggest threat doesn't necessarily come from big players like Microsoft, Google or Amazon, but from individuals banding together and abusing existing tools to create things like deepfakes.

If we were to meet again in a year's time, what would we wish we had already done today?
Stéphane Duguin: In one year, we should have made progress in two main areas. First, we should have changed the narrative about the harm caused by cyberattacks and cyber operations. This would give victims a stronger voice and help policy makers, regulators and judges to promote accountability.

Secondly, we should have made enough effort to be able to assess whether we need a new regulation for the cyber area. It is important to check whether the existing regulations are not sufficiently implemented or whether we actually need new regulations.

And as a final point, we should better connect the cybersecurity community to the reality of the regulation in which it lives. It is critical that those who are responsible for cybersecurity take an interest in the entire regulatory space that is happening around them. If we can achieve these goals in one year, it would be a great success.

Erfahren Sie mehr in unserem Podcast IMPULSE



45 % der Unternehmen sehen Datenschutzanforderungen als größtes Hindernis für den Einsatz von KI.

33 % der Unternehmen haben Bedenken, dass Unternehmensdaten für Dritte durch KI zugänglich werden könnten.

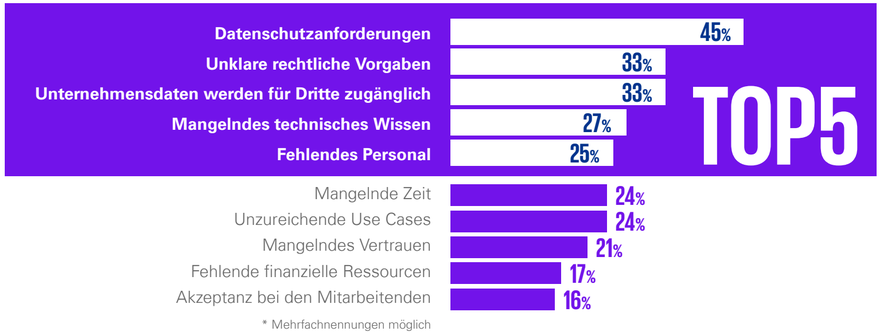
48 % der Unternehmen stimmen zu, dass ein Übermaß an Regulierung der Grund ist, warum KI-gestützte Produkte nicht in der EU entwickelt werden.

Menschenähnliche Verhaltensweisen

Der Lebensraum unserer Schildkröte hat sich in den letzten Jahrzehnten stark verändert und ist auch weiterhin im Wandel. Für dieses langlebige Tier wird es immer schwieriger zu überleben. Dasselbe gilt für unser Überleben im Cyberraum.

Neue Bedrohungen kommen empor, angetrieben von den rapiden Entwicklungen im Bereich Künstlicher Intelligenz (KI). So wie die Schildkröte müssen auch wir schauen, dass uns die neuen Entwicklungen nicht zum Verhängnis werden, sondern wir im Gegenteil die Chancen nutzen.

Abb. 20: Die Top 5 der KI-Einsatz-Hemmnisse*



* Mehrfachnennungen möglich

Von der Welle überrollt

Künstliche Intelligenz (KI) wird von vielen Unternehmen als Allheilmittel gesehen: 65 Prozent betrachten KI als Chance und nur jedes zehnte Unternehmen ordnet sie als Risiko ein. Knapp ein Drittel (31 Prozent) hat sich bereits mit dem Einsatz von KI zur Verbesserung der Cybersicherheit beschäftigt. 36 Prozent haben sich noch nicht damit beschäftigt, sagen aber, dass das Thema für sie von Bedeutung ist. Nur 22 Prozent geben an, dass der Einsatz von KI keine Relevanz für ihr Unternehmen hat.
Fragt man nach den Regeln für die Mitarbeitenden in Bezug auf den Einsatz von generativer KI, wird deutlich, dass Unternehmen von KI überrumpelt wurden: Lediglich 28 Prozent haben bereits Regeln festgelegt. Immerhin 30 Prozent planen, noch Regeln festzulegen. 13 Prozent planen keine Regeln festzulegen, knapp ein Viertel (23 Prozent) hat sich noch nicht damit beschäftigt. Man sieht also, dass KI wie eine Welle über die Unternehmen hereingebrochen ist. Die große Herausforderung besteht jetzt darin, mit den Entwicklungen der Künstlichen Intelligenz mitzuhalten.

Vieles noch unerforscht

Datenschutzanforderungen dominieren bei den größten Hemmnissen für den Einsatz von generativer KI mit 45 Prozent. Auf dem zweiten Platz befinden sich unklare rechtliche Vorgaben sowie Bedenken darüber, dass Unternehmensdaten für Dritte zugänglich werden könnten (je 33 Prozent). Für 27 Prozent stellt mangelndes technisches Wissen ein Hemmnis dar. Schulungen für die Mitarbeiter:innen sind hier von Nöten. 24 Prozent äußern unzureichende Use Cases – KI ist eine große Neuerung, aber es ist noch nicht eindeutig klar, was wir damit eigentlich machen können.

Als weitere Gründe gegen den Einsatz von KI führten die Befragten an, dass das Kosten-Nutzen-Verhältnis nicht bei allen Einsatzgebieten gegeben ist sowie die mangelnde Qualität und Fehleranfälligkeit, Stichwort KI-Halluzinationen. Auch besteht die Sorge, dass die Abhängigkeit von KI- und Cloud-Providern noch größer wird.

KI-Halluzinationen treten auf, wenn große Sprachmodelle (LLMs) falsche Informationen erzeugen. Diese können Abweichungen von Fakten oder Logik sein und erscheinen oft plausibel, da LLMs flüssige, kohärente Texte erzeugen.

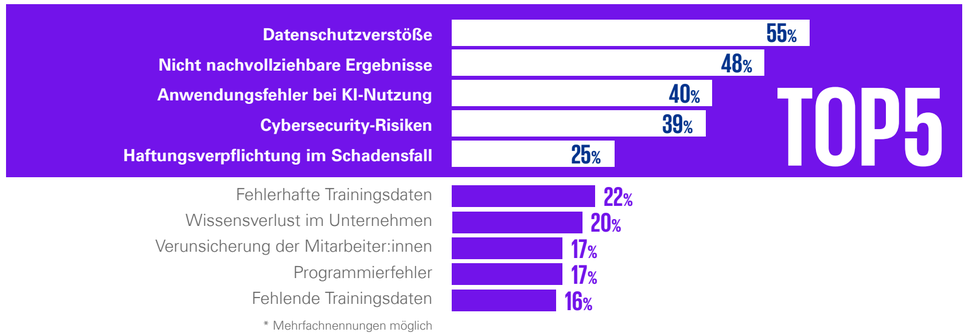
Halluzinationen können jedoch auch unsinnig sein und es gibt keine eindeutige Methode, ihre Ursachen zu bestimmen. Sie können in KI-generierten Videos, Bildern und Audios auftreten und stellen ein Problem dar, da sie das Vertrauen der Benutzer:innen stören können.

Es gibt mehrere Arten von KI-Halluzinationen, darunter Satzwiderspruch, Widerspruch zur Eingabeaufforderung, faktischer Widerspruch und irrelevante oder zufällige Halluzinationen.

Technische Gründe für Halluzinationen können Datenqualität, Generierungsmethoden und Eingabekontext sein.

Es gibt Strategien zur Vermeidung von Halluzinationen, wie klare und spezifische Aufforderungen, Filter- und Rankingstrategien und Multishot-Eingabeaufforderungen.

Abb. 21: Die Top 5 der KI-Einsatz-Risken*



* Mehrfachnennungen möglich

Gefährliche Gewässer

Beim Einsatz von KI im Unternehmen sehen die Befragten Datenschutzverstöße als größtes Risiko. Die Trainingsdaten sind öffentlich zugänglich und Angreifer:innen versuchen hier die Schranken auszuhebeln oder zu umgehen. An zweiter Stelle werden nicht nachvollziehbare Ergebnisse als größtes Risiko gesehen, gefolgt von Anwender:innenfehlern bei der KI-Nutzung, Cybersecurity-Risiken und der Haftungsverpflichtung im Schadensfall.

Es braucht klare Regeln – oder doch nicht?

Die überwiegende Mehrheit (66 Prozent) sagt, dass die Verbreitung von generativer KI die Cybersicherheit verbessern wird, indem sie bei der Abwehr von Angriffen genutzt werden kann. 79 Prozent sind jedoch auch der Meinung, dass die Verbreitung von generativer KI die Cybersicherheit beeinträchtigen wird, weil sie wiederum selbst von Angreifer:innen genutzt werden kann. 56 Prozent finden, dass klare Regeln für die Nutzung von KI europäischen Unternehmen einen Wettbewerbsvorteil verschaffen können. Unternehmen erkennen also, dass es Regeln braucht, um im globalen Wettbewerb bestehen zu können.

20 Prozent halten sich beim Einsatz von KI zurück, weil sie Bedenken haben, gegen Vorschriften zu verstoßen. 42 Prozent sind hier offensiv und nutzen KI, auch wenn sie dabei gegen Vorschriften verstoßen könnten.

48 Prozent stimmen zu, dass ein Übermaß an Regulierung der Grund ist, warum KI-gestützte Produkte (z. B. ChatGPT) nicht in der EU entwickelt werden. Hier sehen wir einen interessanten Konflikt: 56 Prozent sagen, dass klare Regeln wichtig für einen Wettbewerbsvorteil sind, 48 Prozent finden aber, dass die Überregulierung der Grund ist, warum KI-gestützte Produkte nicht in der EU entwickelt werden. Unternehmen wollen beides haben, was aber nicht geht.

> **Wer trägt das Risiko bei Fehleinschätzungen? Wer kann gesichert ein Ergebnis aus einem KI-Ergebnis nachvollziehen?“**
>
> Quelle: Studienteilnehmer:in

Auf die Welle aufspringen

KI ist eine im Grunde alte Technologie – large language models existieren bereits seit 20 Jahren –, die aber jetzt eine breite Aufmerksamkeit erfahren hat. Es gilt zu überlegen, ob, wo KI draufsteht, auch wirklich KI drinnen ist oder einfach nur besseres Routing, das im Algorithmus verpackt ist: Es ist wichtig zu verstehen, dass nicht alles, was als Künstliche Intelligenz bezeichnet wird, auch tatsächlich Künstliche Intelligenz ist. Oftmals handelt es sich dabei um ausgeklügelte Algorithmen, die zwar in der Lage sind, bestimmte Aufgaben effizient zu erledigen, aber nicht die Fähigkeit besitzen, zu lernen oder sich anzupassen – Schlüsselmerkmale echter KI. Diese Algorithmen können Daten analysieren und Muster erkennen, aber sie tun dies auf eine vorher festgelegte Weise und können nicht über ihre ursprüngliche Programmierung hinausgehen. Sie sind nicht in der Lage, aus Erfahrungen zu lernen oder ihre Leistung im Laufe der Zeit zu verbessern. Daher ist es entscheidend, bei der Bewertung von Technologien, die als KI bezeichnet werden, eine genaue Unterscheidung zu treffen. Nur weil KI auf dem Etikett steht, heißt das nicht, dass es sich um echte Künstliche Intelligenz handelt. Es könnte einfach ein guter Algorithmus sein, der für eine bestimmte Aufgabe funktioniert, aber nicht die Fähigkeit hat, über diese Aufgabe hinaus zu lernen oder sich anzupassen. Unternehmen stehen vor der Herausforderung, jene Einsatzmöglichkeiten für KI zu finden, die für ihr Geschäftsmodell am zielführendsten sind. In den nächsten zwölf Monaten erleben wir sicherlich noch weitere rasante Entwicklungen, die nur schwer prognostizierbar sind. Unternehmen können sich insofern vorbereiten, als dass sie bereits jetzt die Rahmenbedingungen schaffen und klare Regeln für Mitarbeitende einführen, rechtliche Aspekte und Datenschutz berücksichtigen, ethische Aspekte des KI-Einsatzes offen und transparent diskutieren und darauf achten, dass ihr geistiges Eigentum nicht für KI-Trainingszwecke verwendet wird und somit einer breiten Öffentlichkeit zugänglich ist.

Vorwärts schwimmen

Obwohl wir einerseits den Wunsch nach klaren Regeln für KI haben, dominiert andererseits eine Art „wild wild west“-Mentalität bei dieser neuen Technologie, indem Dinge ausprobiert, Grenzen überschritten und Risiken bewusst eingegangen werden. Dieser Widerspruch führt dazu, dass Anwendungsfälle von KI in Unternehmen noch nicht überlegt wurden und der Nutzen für das eigene Geschäft noch nicht abgeleitet wurde. Die große Unschlüssigkeit und die vielen Widersprüche zeigen eine Überforderung mit dem Thema. Jedes noch so erdenkliche Problem soll mittels KI gelöst werden. Wenn wir aber die KI trainieren, damit sie uns unterstützt, herrscht dann nicht eine gewisse Stagnation? Wenn wir bestehendes Wissen nehmen und es einpflegen, inwieweit kann hier noch weitere Entwicklung oder Fortschritt entstehen? Es stellt sich die Frage: „What’s next?“

Praxisbeispiel

Ein weiterer Aspekt ist die Kommerzialisierung von KI. Man denke hier zum Beispiel an den GenAI-Chatbot DarkGemini, der u. a. Malware erstellt oder Personen anhand eines Bildes lokalisiert.[1]

[1] https://www.darkreading.com/cyber-risk/google-gemini-vulnerable-to-content-manipulation-researchers-say, abgerufen am 23.4.2024.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1.

Künstliche Intelligenz (KI) wird von vielen Unternehmen als Chance gesehen, aber es gibt auch Befürchtungen hinsichtlich des Datenschutzes, unklarer rechtlicher Vorgaben und mangelnden technischen Wissens. Unternehmen haben kaum Regeln für den Einsatz von KI festgelegt und nur wenige planen, solche Regeln zu erstellen. Die Sorge vor der Abhängigkeit von KI- und Cloud-Anbietern ist nach wie vor sehr groß und es herrscht Zurückhaltung aufgrund der Qualität und Fehleranfälligkeit von KI.

2.

Die meisten Unternehmen glauben, dass KI die Cybersicherheit verbessern kann, aber sie sind auch darüber beunruhigt, dass KI von Angreifer:innen genutzt werden könnte. Es besteht ein Bedarf an klaren Regeln für die Nutzung von KI, obwohl einige Unternehmen Bedenken haben, gegen Vorschriften zu verstoßen.

3.

Es gibt einen Widerspruch zwischen dem Wunsch nach klaren Regeln für KI und der „wild wild west"-Mentalität, bei der Unternehmen Dinge ausprobieren, Grenzen überschreiten und Risiken eingehen. Dies führt dazu, dass viele Unternehmen noch nicht über den Nutzen von KI für ihr eigenes Geschäft nachgedacht haben.

Den Überblick im Informations-raum behalten

Josef Schroefl und Robert Lamprecht über die zunehmende Bedeutung von Desinformation im Cyberspace und die Herausforderungen, die hybride Bedrohungen für Unternehmen und Gesellschaft darstellen.

Was genau ist das Centre of Excellence for Countering Hybrid Threats? Was ist seine Aufgabe?
Josef Schroefl: Das European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) gibt es seit dem Jahr 2016. Es entstand aus dem Wunsch der EU und der NATO heraus, den zunehmenden hybriden Bedrohungen, die wir zum ersten Mal 2014 bei der völkerrechtswidrigen Annexion der Krim gesehen haben, entgegenwirken zu können. Das Hybrid CoE ist die erste und einzige NATO/EU-Institution.

Die Themen hybride Bedrohungen und Desinformation haben sich im Laufe der Jahre entwickelt bzw. verändert. Was hat Sie in dieser Entwicklung am meisten überrascht in Bezug darauf, wie wir damit umgehen? Was sollten wir wissen, wenn wir unser Gegenüber besser verstehen wollen?
Josef Schroefl: Für mich war die deutlichste Entwicklung in den letzten Jahren, dass der Cyberspace als Domäne immer wichtiger wird. Ohne Cyberspace gäbe es keine neuen Technologien und somit auch keine neuen Formen der Auseinandersetzung: Alle neuen Technologien, egal ob Artificial Intelligence, Cloud-Computing, intelligente Drohnen, intelligente Konfliktführung als solche usw., werden im Cyberspace koordiniert und orchestriert.

Kann man sagen, dass durch die Dynamik, die in den letzten Jahren entstanden ist, dieses Phänomen die Oberhand gewonnen hat und das Potenzial aufseiten der Angreifer:innen höher ist als aufseiten der Betroffenen?
Josef Schroefl: Das ist die große Frage. Nehmen wir folgendes Beispiel: Wir erwarten seit Beginn des russischen Angriffskrieges auf die Ukraine den ultimativen Schlag aus dem Cyberspace auf unsere kritische Infrastruktur, da ja bekannt ist, dass Russland über gewaltige Cyberkapazitäten verfügt. Aber dieser ist bislang ausgeblieben. Jetzt häufen sich die Meldungen über gehackte Quellcodes von Microsoft, Cyberangriffe auf Länder wie Deutschland, Frankreich, Polen und zahlreiche Desinformationskampagnen über X (vormals Twitter) & Co. Also offenbar tut sich etwas – aber diese Riesenattacke hat noch nicht stattgefunden. Dafür gibt es meiner Meinung nach drei Möglichkeiten: Russland konzentriert sich bislang eher auf die konventionelle Kriegsführung, wir waren doch besser vorbereitet als angenommen oder – und diese Möglichkeit finde ich am beunruhigendsten –ein fortschrittlicher Virus oder APT befindet sich bereits in unseren Systemen. Wir wissen es einfach nicht.

Das heißt, die Dimension Cyberangriff muss heute immer parallel mitgedacht werden, wenn wir von hybriden Bedrohungen sprechen.

Wenn wir uns die derzeitigen geopolitischen Spannungen ansehen: Inwiefern befinden wir uns bereits in der nächsten Stufe der Eskalation?
Josef Schroefl: Das ist eine sehr gute Frage. Meine private persönliche Meinung ist, dass wir am Beginn einer Auseinandersetzung – oder teilweise auch schon mittendrin – zwischen Autokratien und Demokratien stehen. Das sieht man im aktuellen Ukraine-Krieg besonders deutlich mit demokratischen Unterstützern aufseiten der Ukraine und autokratischen Unterstützern aufseiten Russlands. Hier sieht man aber auch unterschiedliche Interessen: von Spionage über monetäre Interessen, die über Ransomwareangriffe befriedigt werden, bis hin zu Deepfakes und gezielten Angriffen auf kritische Infrastrukturen.

Wie können diese Angriffstaktiken auf Unternehmen projiziert werden bzw. gibt es hier gewisse Schwergewichte, die gegen Unternehmen eingesetzt werden?
Josef Schroefl: Wenn ein Unternehmen z. B. im Bereich der Ent-

FOTO © BRAND PHOTO OY

Oberst Mag. Dr.
Josef Schroefl,
Stellvertretender Direktor der CoI „Strategy & Defence" am European Center of Excellence for Countering Hybrid Threats (Hybrid CoE).

Josef Schroefl startete seine Karriere 1982 im Österreichischen Bundesheer, bei dem er auch an mehreren UN-Einsätzen beteiligt war. Ab 2006 war er im österreichischen Verteidigungsministerium in den Bereichen „Comprehensive Approach", „Hybrid Threats" und „Cyber Security/Cyber Defence" tätig. Er hat Abschlüsse in Computertechnologie, Internationale Beziehungen und Internationale Politik. Er veröffentlichte mehrere Publikationen zu asymmetrischen/Cyber-/hybriden Bedrohungen und ist Peer-Board-Mitglied verschiedener Zeitschriften. Aktuell ist er stellvertretender Direktor der CoI „Strategy & Defence" am Hybrid CoE in Helsinki, der ersten und einzigen EU/NATO-Einrichtung, dort ist er auch Leiter des Arbeitsgebietes „Cyber".

> **Wir müssen den Cyber- und Informationsraum als Einheit betrachten.**
>
> Josef Schroefl

wicklung von Technologie tätig ist, muss man sicherlich mit den beiden Angriffsvektoren Erpressung und Spionage rechnen und es liegt im Bereich der Unternehmen, vor allem der kritischen Infrastruktur, sich hier auch selbst zu schützen.

Unternehmen müssen sich also darauf einstellen – je nach Geschäftsmodell – nicht nur an einer Front kämpfen zu müssen?
Josef Schroefl: Absolut.

Im Hinblick darauf, dass das heurige Jahr in Österreich ein „Superwahljahr" ist: Wie groß ist die Gefahr, dass Desinformationskampagnen die Wahlergebnisse beeinflussen?
Josef Schroefl: Wir leben sicherlich nicht auf einer Insel der Seligen – da können wir noch so neutral sein. Auch wir sind bereits im Fokus von Des- und Missinformationskampagnen. Und diese Kampagnen sind meist nichts Kurzfristiges. Sie werden oft von langer Hand geplant und über Jahre hinweg ausgeführt, um das Ziel entsprechend zu destabilisieren. Ausschlaggebend hierbei ist der Aufbau eines bestimmten Narrativs, dem Glauben geschenkt wird. Und dieses Narrativ zieht sich dann durch sämtliche Kanäle – zum Teil bis hinein in die Schulbildung. Natürlich ist hier nicht nur die Gesellschaft als solche betroffen, sondern auch Unternehmen. Solche Kampagnen können bisweilen auch zum Ruin eines Unternehmens führen.

Was wären Ihre Empfehlungen für Unternehmen, wie sie sich auf diese Gefahren besser vorbereiten können?
Josef Schroefl: Das ist nicht so leicht zu beantworten. Es ist wichtig, den Cyber- und Informationsraum als Einheit zu sehen und diese Einheit aktiv ins Gefahrenmonitoring miteinzubinden. Das ist vor allem für die Früherkennung ein wichtiger Faktor.

Wenn man von Früherkennung spricht, dann kommt häufig das Thema Künstliche Intelligenz mit ins Spiel. Wenn wir auf die Bedrohungen durch KI schauen: Inwieweit spielen Deepfakes und Co. hier aktuell eine Rolle?
Josef Schroefl: Zum heutigen Zeitpunkt kann ich sagen, dass Deepfakes noch erkennbar sind. Aber die Technologie entwickelt sich unglaublich schnell. Dadurch stehen wir vor dem Problem, dass das Manko an Spezialist:innen, die sich mit diesen Technologien wirklich auskennen und umgehen können, immer größer wird. Wir müssen versuchen, mit einer besseren Ausbildung gegenzusteuern und den Technologievorsprung, den die westliche Welt momentan noch hat, zu halten bzw. auszubauen.

Bei den Themen Desinformation und Vertrauensverlust spielen auch Medien und Politik eine enorme Rolle. Auf welche Weise tragen Desinformationen, die über diese Kanäle kommen, zu gesellschaftlichen Unruhen bei? Oder anders gefragt: Wie resilient sind wir in Europa?
Josef Schroefl: Im Bereich der Awareness haben unsere Medien in den letzten Jahren sehr, sehr viel gelernt – hier sind wir also durchaus resilienter geworden. Wir brauchen vielleicht etwas mehr Zeit, aber dafür machen wir es dann besser.

Resilienz bedeutet auch Kommunikation. Wie schaut es denn mit der internationalen Kommunikation bzw. Zusammenarbeit aus?
Josef Schroefl: Das Wichtigste ist natürlich die Informationsweitergabe. Diese gestaltet sich aber oftmals schwierig, da es in den verschiedenen Ländern unterschiedliche Zuständigkeiten gibt und somit oft auch Informationen auf der Strecke bleiben können.

Könnte hier Ihrer Meinung nach die neue NIS2-Richtlinie helfen, europaweit besser koordinieren zu können?
Josef Schroefl: NIS2 schafft theoretisch alle Voraussetzungen, damit es hier zu einer Informationsweitergabe kommt. Es ist die Frage, inwieweit die Nationalstaaten die Richtlinie umsetzen.

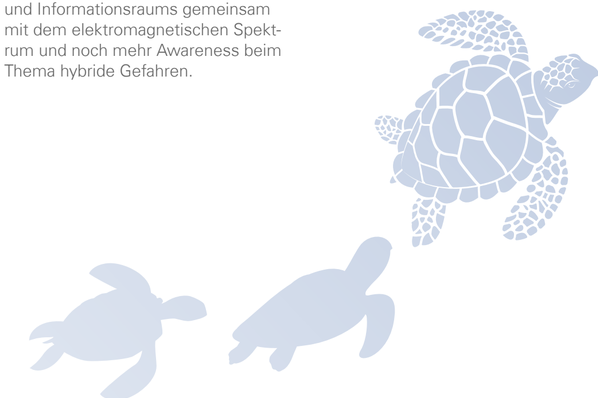
Wie schätzen Sie die hybriden Bedrohungen in der nächsten Zeit ein? Wie wird sich das geopolitisch entwickeln?
Josef Schroefl: Diese Orchestrierung von mehreren Attacken gleichzeitig – wie z. B. Cyberangriffe, juristische Angriffe und Desinformationen – wird zunehmen, fürchte ich.

Stehen wir vor einer gewissen Zeitenwende, wenn es um die Qualität bzw. die Komplexität geht, solche Dinge zu erkennen?
Josef Schroefl: Gerade bei der Erkennung ist Europa auf einem guten Weg. Einer der Parameter dafür ist, dass alle EU- und NATO-Staaten Mitglied bei uns sind und Vertretungen haben, die die Informationen auch weitergeben und bei Ausbildungen unterstützen. Potenzial gibt es innerstaatlich noch in der Regelung der Zuständigkeiten, besonders beim Thema Mis- und Desinformation. Das gleiche gilt heruntergebrochen auch für die Unternehmen: Es braucht klare Zuständigkeiten.

Was ist die häufigste Frage, die man Ihnen schon gestellt hat, und was hat Sie eigentlich noch nie jemand gefragt, obwohl es wichtig wäre, die Antwort zu kennen?
Josef Schroefl: Die häufigste Frage, die in letzter Zeit gestellt wurde, war: „Wohin entwickeln sich die neuen Technologien wie AI etc.?" Was ich noch nie gefragt wurde, obwohl es meines Erachtens gerade in der aktuellen geopolitischen Situation wichtig wäre: „Was können wir beitragen, um den Demokratien zum Sieg zu verhelfen?"

Wenn wir uns in einem Jahr wieder treffen, was würden wir uns wünschen, heute schon getan zu haben?
Josef Schroefl: Eine bessere und komplexere Sichtweise des Cyber- und Informationsraums gemeinsam mit dem elektromagnetischen Spektrum und noch mehr Awareness beim Thema hybride Gefahren.

Erfahren Sie mehr in unserem Podcast IMPULSE



54 % Prozent der befragten Unternehmen waren in den letzten 12 Monaten Opfer von Desinformationskampagnen, wobei 42 Prozent sogar mehrmals zum Ziel wurden.

84 % Prozent der Befragten sagen, dass Desinformationskampagnen unsere gesellschaftliche Resilienz beeinflussen.

+11 % Desinformation hat in den letzten 12 Monaten den höchsten Zuwachs erfahren und ist um drei Plätze nach oben geklettert.

56 % Prozent geben an, dass Desinformation für sie normales Tagesgeschäft ist.

Desinformation und Hybride Bedrohungen

Im Ozean lauern vielen Gefahren und wir können nicht wissen, was sich am Meeresgrund wirklich befindet. Wir haben gelernt, dass Künstliche Intelligenz neue Angriffsarten wie Deepfakes beschleunigt. Das macht uns anfälliger gegenüber Desinformation und beeinflusst unsere gesellschaftliche Resilienz.

Wahlen mit ungewissem Ausgang und unbekannten Auswirkungen stehen uns bevor. Die Welt steht an einer Kreuzung – die Unternehmen ebenso.

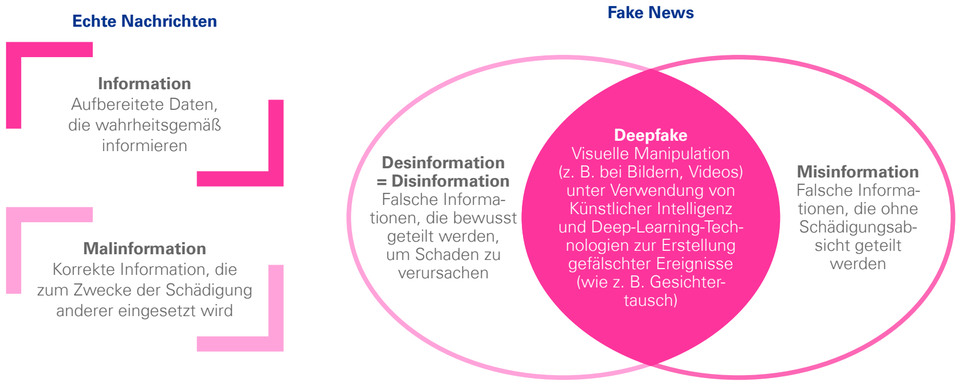
Trugschluss
Bevor wir uns mit den Auswirkungen von Desinformation auseinandersetzen, müssen wir das Themenfeld abstecken und den Bezug zur Cybersecurity herstellen:

Die Begriffe „Misinformation" und „Desinformation" werden oft verwechselt und/oder gleichgesetzt. Wer jedoch den Unterschied zwischen diesen beiden Begriffen kennt, kann passende Maßnahmen zur Abwehr von Onlinerisiken planen und den Ruf des Unternehmens / der Marke schützen.

Misinformation wird definiert als falsche Informationen, die unabhängig von der Absicht der Irreführung verbreitet werden. Es kann sich dabei um Informationen handeln, die sich jemand falsch gemerkt, falsch gelesen oder versehentlich wiederholt hat. Im Allgemeinen liegt bei Misinformation keine böswillige Absicht vor.[1]

Desinformation hingegen ist definiert als absichtlich irreführende

Abb. 22: Echte Nachrichten vs. Fake News



Bildquelle: In Anlehnung an Global disinformation campaigns and legal challenges, October 2020. International Cybersecurity Law Review 1(1-2):125-136.

Leichte Beute

Desinformationen können Unternehmen irreparablen Schaden zufügen. Werfen wir einen Blick darauf, warum Desinformation ein Cybersicherheitsrisiko darstellt und was wir dagegen tun können.

1) Desinformation ist billig
Im Vergleich zu Ransomware ist Desinformation ein kostengünstiger Weg, um ein Unternehmen anzugreifen. Das Aufkommen von Desinformation-as-a-Service (DaaS) zeigt, wie erschwinglich die Verbreitung von Online-Fehlinformationen ist. DaaS-Anbieter:innen berechnen lediglich USD 15 bis 45 pro Artikel mit 1.000 Zeichen, plus weitere USD 65 für die Kontaktaufnahme mit einer Medienquelle, die das Material verbreitet. Das Starten eines Ransomwareangriffes kostet im Durchschnitt USD 1.000.[3]

2) Jede:r kann Desinformationen verbreiten
Eines der größten Risiken von Desinformation ist, dass sie von überall kommen kann. Kriminelle Akteur:innen, wie z. B. staatlich gesponserte Trolle, Mitglieder extremistischer Gruppen, oder unabhängige Anbieter:innen von Desinformationsdiensten, können sich an jeglichen Arten von Kampagnen beteiligen. Die Gründe reichen von einem größeren Bekanntheitsgrad über Gebühren für Dienstleistungen und Werbeeinnahmen bis hin zu sekundärem wirtschaftlichem Gewinn (z. B. Produktverkäufe) und politischen Zielen.[4]

3) Desinformationen verbreiten sich schnell
Wenn eine Desinformationskampagne erst einmal angelaufen ist, lässt sie sich nur schwer wieder aufhalten. Eine Studie des MIT aus dem Jahr 2019 ergab, dass sich Online-Fehlinformationen weiter, schneller und tiefer verbreiten als wahre Fakten. Die Analyse ergab, dass falsche Nachrichten mit 70 Prozent höherer Wahrscheinlichkeit retweetet werden als echte Nachrichten und die ersten 1.500 Personen sechsmal schneller erreichen.[5]

Für Internetnutzer:innen kann es schwierig sein, wahre und falsche Informationen zu erkennen. Die MIT-Studie ergab, dass Bots wahre und falsche Informationen in gleichem Maße verbreiten. Dies deutet darauf hin, dass es echte Personen sind, die Fake News verbreiten und verstärken. Desinformationskampagnen verstecken sich oft unter echten Nachrichten, sodass Einzelpersonen unwissentlich eine Rolle bei der Verbreitung von Fake News spielen[6].

4) Desinformation ist nicht illegal
Es gibt kein Gesetz, das die Verbreitung von Falschinformationen regelt. Suchmaschinen und Social-Media-Plattformen sind nicht gezwungen, ihre Algorithmen so zu konfigurieren, dass sie das Risiko von Desinformationen verringern.

Geringe Konsequenzen wie z. B. der Ausschluss von Personen oder Konten von einer Plattform sind häufig die Folge. In anderen Fällen bleibt für eine Wiedergutmachung nur rechtliche Schritte einzuleiten, wie etwa eine Verleumdungsklage, was Zeit und Geld kostet.[7]

5) Desinformation ist für Unternehmen kostspielig
Einer Schätzung zufolge kostet die Desinformation die Weltwirtschaft jedes Jahr USD 78 Mrd. Da sich Desinformationskampagnen zunehmend gegen den Privatsektor richten, dürften diese Kosten noch steigen: Einige Schätzungen gehen von Kosten in Höhe von USD 100 Mrd. aus. Analysten schätzen, dass ein einfacher Cyberangriff im Vergleich dazu etwa USD 25.000 einbringen könnte.[8]

Unternehmen können sich von Desinformationskampagnen nur schwer erholen. Eine Pizzeria in den USA sieht sich beispielsweise fünf Jahre nach einer Online-Desinformationskampagne, in der (fälschlicherweise) behauptet wurde, das Unternehmen sei in einen Kinderhandelsring verwickelt, immer noch mit Protesten und Streikposten konfrontiert. Über eine US-amerikanische Möbelfirma werden ebenfalls falsche Anschuldigungen bzgl. Kinderhandel verbreitet. Das Unternehmen hat mit zahlreichen Videos zu kämpfen, die Jahr für Jahr veröffentlicht werden und die Desinformation verbreiten. Diese Geschichten schaden kontinuierlich dem Vertrauen in die Marke und behindern das Wachstum von Unternehmen.

6) Desinformation ist mit dem elektronischen Handel verbunden
Die COVID-19-Pandemie hat dazu geführt, dass sich immer mehr Verbraucher:innen auf den elektronischen Handel verlassen. Dadurch haben Täter:innen eine neue Möglichkeit, Online-Fehlinformationen zu verbreiten. Der elektronische Handel hat Desinformation zu einem größeren Cybersecurity-Risiko gemacht, indem er die Käufer:innen dazu verleitet, unwissentlich extremistische Gruppen oder Verschwörungstheorien zu finanzieren.

Websites entfernen zwar offensichtliche Produkte von diesen kriminellen Gruppierungen, Elemente dieser können sich aber durch versteckte Botschaften auf vermeintlich unbedenklichen Produkten wieder einschleichen. Es ist nur schwer durchschaubar, ob ein:e Verkäufer:in mit Verschwörungstheoretiker:innen / kriminellen Gruppierungen zusammenarbeitet oder einfach nur die mutmaßlich harmlose Botschaft auf den Produkten unterstützt.[9]

E-Commerce-Algorithmen können auch dazu missbraucht werden, Produkte zu empfehlen, die eine dunklere Bedeutung haben. Marken müssen ihre Markenerwähnungen sorgfältig überwachen, um Fehl- und Desinformationen, die von Algorithmen oder Influencer:innen verbreitet werden, zu erkennen und zu bekämpfen.

oder voreingenommene bzw. bewusst gestreute Falschmeldungen und Informationen, die manipulierte Erzählungen oder Fakten bzw. Propaganda verbreiten. Desinformation ist die wissentliche Verbreitung von Fehlinformationen; sie wird häufig in hybriden Konflikten eingesetzt, um falsche Informationen zu verbreiten.[2]

Überlebenswichtig

Da Desinformationen so weit verbreitet sind, ist es äußerst schwierig, dieses große Cybersicherheitsrisiko zu bekämpfen. Anstatt zu versuchen, Online-Fehlinformationen vollständig zu eliminieren, sollten Unternehmen versuchen, Erwähnungen über sie zu überwachen und im Vorfeld einen Reaktionsplan erstellen, sollten Desinformationskampagnen auftauchen.

Rauer Wellengang

Fake News können ebenso Auswirkungen auf die Aktienrenditen von Unternehmen haben. Da nicht alle Anleger:innen erkennen können, ob eine Nachricht wahr oder gefälscht ist, kann dies zu Uneinigkeit unter ihnen über den wahren Wert des Unternehmens führen. Das führt unter Umständen dazu, dass die Aktienkurse der betroffenen Unternehmen auf die verbreiteten Fake News reagieren. Untersuchungen haben ergeben, dass negative Fake News negative und signifikante kurzfristige Auswirkungen auf Renditen haben. Bei positiven und neutralen Nachrichten wurde kein eindeutiger Einfluss auf die Aktienrenditen festgestellt. Bemerkenswert ist auch, dass die Studie keinen signifikanten Unterschied zwischen traditionellen Medien und sozialen Medien finden konnte.[10]

Desinformation und Cybersicherheit?

Laut Disinfo.EU[11] gibt es vier Gründe (4Ts), warum Fehl- und Desinformation ein Problem für die Cybersicherheit darstellen:

- **Terrain** (Umfeld), also die Infrastruktur, über die die Fehlinformationen verbreitet werden
- **Tactics** (Taktiken), wie die Desinformation verbreitet wird
- **Targets** (Ziele), sprich die beabsichtigten Opfer der Fehlinformationen, die zu Cyberangriffen führen
- **Temptations** (Verlockungen), also die finanziellen Anreize, die hinter der Verwendung von Fehlinformationen für Cyberangriffe stehen

Cyberkriminelle nutzen die 4Ts seit Jahren als Grundlage für Phishingangriffe, und sie setzen weiterhin auf Fehl- und Desinformation, weil diese so effektiv sind. Denken wir bspw. daran, wie einfach es ist, den:die Empfänger:in einer Phishing-E-Mail zu überzeugen, dass er:sie ein Paket erhält, obwohl er:sie nichts bestellt hat. Empfänger:innen dazu zu bringen, einen Anhang zu öffnen, der von einem:einer Bekannten stammen und daher legitim sein könnte, ist ebenfalls immer noch viel zu leicht möglich.[12]

Phishing im Cyberozean

Die Angriffe sind nicht nur raffinierter geworden, sondern auch häufiger. Laut FBI hat sich die Zahl der Phishingversuche von 2019 auf 2020 verdoppelt. Die Reaktion auf diese Informationsangriffe ist davon abhängig, wie die Cybersicherheitssysteme zum Schutz der Daten und des Unternehmens ausgelegt sind.[13]

Fehlinformationen sind ebenfalls hoch technisiert. Das merken wir an Deepfakes sowie den Möglichkeiten von KI und maschinellem Lernen zur Erstellung falscher Versionen der Realität. Auch wenn KI-generierte Desinformationen noch nicht als Katalysator für Cyberangriffe dienen, werden sie sich in naher Zukunft zu einem ernst zu nehmenden Angriffsvektor entwickeln. Unternehmen müssen darauf vorbereitet sein.[14]

Unsichtbarer Feind

Gerade durch die derzeit stattfindende weltpolitische Neuordnung ist Desinformation sicherlich eines jener Phänomene, denen wir in Zukunft vermehrt Aufmerksamkeit schenken müssen. Waren es in der Vergangenheit Angriffsarten, die durch Nationalstaaten ausgeübt wurden, so wird das Spielfeld durch die Digitalisierung immer größer und immer mehr Akteur:innen nutzen diesen unregulierten Bereich, um ihre Interessen durchzusetzen. Schon unsere Vorjahresstudie hat gezeigt, dass jeder

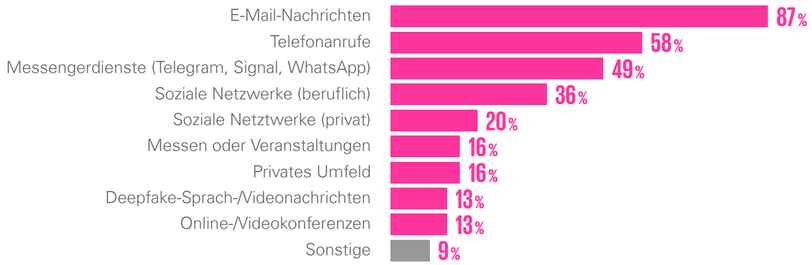
zehnte Angriff auf die Medienberichterstattung eines Unternehmens zurückzuführen war. Die diesjährigen Zahlen unterstreichen umso deutlicher, dass der geschickte Einsatz von Informationen verheerende Auswirkungen mit sich bringen kann. Der Schritt zum Informationskrieg ist dann nur noch ein kleiner.

2024 wird eines der größten Wahljahre der Geschichte sein. In mehr als 50 Ländern werden Wahlen abgehalten. Mehr als 2 Milliarden Menschen werden zur Wahl gehen. Das wird höchstwahrscheinlich die derzeitigen Spannungen in der Welt verschärfen. Weil wir einen wirtschaftlichen Abschwung erleben und unter der Inflation leiden. Weil es einfacher denn je ist, Fehlinformationen zu verbreiten. Weil viele Menschen nach Schwarz-Weiß-Malerei suchen. Weil Politiker:innen und Parteien populistisch sein werden. Weil es ein hohes Maß an Misstrauen gibt. Und vieles mehr. So sehen vernetzte Risiken aus, wie auch der WEF Global Risks Report 2024 bestätigt.[15] Wenn Sie in Ihrem Unternehmen für die Sicherheit zuständig sind, würde ich damit beginnen, dies in Bewertungen zu berücksichtigen.

Desinformationskampagnen sind auf den ersten Blick nicht als solche zu erkennen. Sie haben eine Vorlaufzeit von mehreren Jahren. Desinformationskampagnen folgen einem klaren Drehbuch, sind klar orchestriert und wirken über Messengerdienste wie ein Informations-Tsunami.

Mehr dazu hören Sie in unserer Podcastfolge mit Josef Schroefl.

Abb. 23: Social Engineering*



* Top-3 Aspekte je Teilnehmer:in

Abb. 24: Sind Sie der Meinung, dass Ihre Unternehmensaktivitäten durch Online-Desinformationskampagnen beeinflusst werden können?

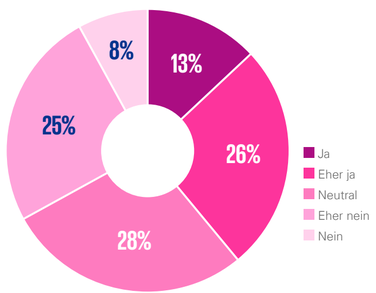


Abb. 25: Desinformations-Akteur:innen*

* Mehrfachnennungen möglich

Mit allen Wassern gewaschen

Gerade in Zeiten großer geopolitischer Spannungen und einer instabilen neuen Weltordnung kennt Desinformation keine Grenzen und geht über bekannte Kanäle hinaus. Wir rechnen damit, dass Desinformationskampagnen in privat genutzten sozialen Netzwerken stattfinden und haben gelernt, dass diese auch bereits in Messengerdiensten Einzug halten. Wir müssen uns aber bewusst sein, dass es keine Grenzen bei Desinformation gibt und diese auch in der beruflichen Meinungsbildung immer präsenter wird – unabhängig davon, um welches Medium oder soziale Netzwerk es sich handelt. Keines von ihnen ist vor Desinformationsangriffen gefeit.

Stürmische See

Desinformation bereitet Unternehmen Sorgen: 40 Prozent glauben, dass ihr Unternehmen Opfer eines Cyberangriffs werden kann, durch den gezielt Einfluss auf das Unternehmen ausgeübt werden könnte. 39 Prozent sind der Meinung, dass ihre Unternehmensaktivitäten durch Online-Desinformationskampagnen beeinflusst werden können. Wir sehen also, dass Desinformation bei den Unternehmen angekommen ist. 54 Prozent der befragten Unternehmen waren in den letzten 12 Monaten Opfer von Desinformationskampagnen, wobei 42 Prozent sogar mehrmals zum Ziel wurden. Dabei wird vor allem die Technologie missbräuchlich gegen uns eingesetzt und das Tag für Tag. So waren 35 Prozent der Befragten Opfer von Deepfake, die für Mis-/und Desinformationszwecke eingesetzt wurden.

In der Einordnung der Unternehmen rückt Desinformation (Fake News/Rufschädigung) vom Tagesgeschäft hin zu einer besonderen Herausforderung. Es ist jene Bedrohung, die in den letzten 12 Monaten den höchsten Zuwachs (+ 11 Prozent) erfahren hat und um drei Plätze nach oben geklettert ist. Damit liegt sie vor Social Engineering (Platz 10). Dennoch verzeichnen Social-Engineering-Attacken in den letzten 12 Monaten eine rasante Zunahme. Gerade weil diese Plattformen und Kanäle keiner Moderation unterliegen, sind die Hürden zur Verbreitung von Desinformationen äußerst niedrig. Bei der E-Mail-Technologie existieren heute bereits gute Möglichkeiten, um Inhalte vor der Zustellung zu filtern. Bei Telefonanrufen ist die Sprache die einzige Chance auf eine begrenzte Beeinflussung. Die volle Bandbreite an Beeinflussungsmöglichkeiten ist vor allem bei Messengerdiensten und sozialen Netzwerken möglich. Hier können alle Deepfake-Register gezogen werden, um Informationen glaubhaft erscheinen zu lassen. Eine kritische Haltung und ein ständiges Hinterfragen der Inhalte ist aktuell das einzige Mittel, um gegen diese Angriffe resilient zu sein.

Von allen Seiten

Desinformation muss aus drei Gesichtspunkten analysiert werden: Erstens wird der politische Kontext betrachtet. Hier geht es um die Beeinflussung demokratischer Strukturen. Zweitens ist der persönliche Kontext hervorzuheben. Die individuelle Meinungsbildung und das Rütteln an gefestigten demokratischen Strukturen sind damit verbunden. Drittens steht der wirtschaftliche Kontext im Fokus, der besonders relevant für Unternehmen ist. Wir berücksichtigen nicht umfassend genug, dass gerade zielgerichtete Desinformationskampagnen dazu führen können, dass Unternehmen in Ausnahmesituationen gebracht werden und sie die volle Aufmerk-

samkeit der Mitarbeiter:innen / des Krisenmanagements fordern. Die Desinformationskampagnen werden als Ablenkung verwendet, um die eigentlichen Cyberangriffe zu verstecken.

Kein sicherer Hafen

Die größten Bedrohungen von Desinformation gegen Unternehmen gehen von politischen Hacktivist:innen aus. An zweiter Stelle wurden staatlich unterstützte Gruppierungen genannt. Diese stehlen im Auftrag der jeweiligen Regierung / des jeweiligen Landes Informationen, um einen Vorsprung für die eigene Wirtschaft zu gewährleisten. An dritter Stelle finden wir Mitbewerb/Konkurrenz. In diesem Zusammenhang darf man auch den Insider Threat nicht vernachlässigen, denn gerade in ökonomisch schwierigen Zeiten suchen Menschen Möglichkeiten, um finanzielle Profite zu erzielen und tragen so dazu bei, dass diese Arten von Angriffen wirksam werden können (siehe Abb. 25).

Unter Berücksichtigung all dieser Faktoren verwundert es kaum, dass 84 Prozent der Befragten sagen, dass Desinformationskampagnen unsere gesellschaftliche Resilienz beeinflussen. Dennoch sind die Auswirkungen für Unternehmen noch nicht hinreichend spürbar: So geben 56 Prozent an, dass dieses Thema für sie normales Tagesgeschäft ist, also eine Bedrohung, die ohne viel Aufwand bewerkstelligt werden kann. Demgegenüber sehen 44 Prozent es als besondere Herausforderung, da sie noch keine wirksamen Mittel haben, um sich davor zu schützen.

Desinformationskampagnen sind abseits der gesellschaftlichen Destabilisierung auch in Österreich ein Mittel, um Unternehmen abzulenken und in deren Verwirbelungen einen Cyberangriff zu starten. Umso wichtiger ist es, sich der Vielfältigkeit von Angriffen bewusst zu sein und nicht jedem einzelnen Ereignis blindlings nachzulaufen.

[1] https://www.apa.org/topics/journalism-facts/misinformation-disinformation, abgerufen am 8.4.2024.
[2] https://www.apa.org/topics/journalism-facts/misinformation-disinformation, abgerufen am 8.4.2024.
https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation,
abgerufen am 8.4.2024.
https://www.onlinesicherheit.gv.at/Services/News/Fake-News-Wie-kann-Desinformation-in-sozialen-Netzwerken-entlarvt-werden.html, abgerufen am 8.4.2024.
Stahl, Bernd Carsten. „On the difference or equality of information, misinformation, and disinformation: A critical research perspective." Informing Science 9 (2006): 83.
[3] https://hackernoon.com/disinformation-as-a-service-content-marketings-evil-twin, abgerufen am 8.4.2024.
[4] Rutgers-Bericht „The Future Of Disinformation Operations and The Coming War On Brands"
[5] https://mitsloan.mit.edu/ideas-made-to-matter/study-false-news-spreads-faster-truth, abgerufen am 31.3.2024
[6] https://mitsloan.mit.edu/ideas-made-to-matter/study-false-news-spreads-faster-truth, abgerufen am 31.3.2024
[7] https://www.axios.com/2023/07/10/ai-misinformation-response-measures, abgerufen am 8.4.2024.
[8] https://cesie.org/en/news/true-cost-of-disinformation-mega/, abgerufen am 8.4.2024.
[9] https://internationalsecurityjournal.com/disinformation-corporate-risk/, abgerufen am 8.4.2024.
[10] https://www.sciencedirect.com/science/article/pii/S0148619523000231, abgerufen am 8.4.2024.
[11] https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat/, abgerufen am 8.4.2024.
[12] https://securityintelligence.com/articles/protecting-data-from-misinformation-cybersecurity/,
abgerufen am 8.4.2024.
[13] https://securityintelligence.com/articles/protecting-data-from-misinformation-cybersecurity/,
abgerufen am 8.4.2024.
[14] https://securityintelligence.com/articles/protecting-data-from-misinformation-cybersecurity/,
abgerufen am 8.4.2024.
[15] https://www.weforum.org/publications/global-risks-report-2024/, abgerufen am 8.4.2024.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1.

Künstliche Intelligenz beschleunigt neue Angriffsarten wie Deepfakes, was zu einer erhöhten Anfälligkeit gegenüber Desinformation führt und die gesellschaftliche Resilienz beeinflusst. Gerade Unternehmen dürfen diese Form der Bedrohung nicht aus den Augen verlieren.

2.

Unternehmen sind zunehmend besorgt über Desinformation. In den letzten 12 Monaten waren viele von ihnen bereits Opfer von Desinformationskampagnen und Deepfake-Angriffen. Diese dienen oftmals als Ablenkung, um den eigentlichen Cyberangriff zu verschleiern.

3.

Desinformation muss aus drei Gesichtspunkten analysiert werden: dem politischen, persönlichen und wirtschaftlichen Kontext. Sie wird schon lange nicht mehr als ausschließlich gesellschaftspolitisches Werkzeug eingesetzt, sondern zunehmend auch zur (wirtschaftlichen) Destabilisierung von Unternehmen.

Die Absichten der Gegner:innen verstehen

In diesem Interview gibt Sylvia Mayer spannende Einblicke in die Herausforderungen und Strategien der DSN im Bereich Cybersecurity. Sie spricht mit Robert Lamprecht über die Bedeutung von Diversität in der Cybersicherheit und die Notwendigkeit, technische und rechtliche Befugnisse der Behörden zu erweitern.

Welche Aufgaben hat die DSN und wie ist die Abgrenzung zu den anderen Nachrichtendiensten? Und was ist eigentlich der Unterschied zwischen Nachrichtendienst und Geheimdienst?
Sylvia Mayer: Die Direktion Staatsschutz und Nachrichtendienst wurde 2021 als Nachfolgeorganisation des BVT gegründet. Das Hauptziel ist der Schutz der Prinzipien unserer Verfassung, des liberalen demokratischen Rechtsstaats. Unsere Aufgabe ist es, diese Prinzipien vor Personen, Gruppierungen und Bestrebungen zu schützen, die sie unterwandern und umstürzen wollen. Wir bekämpfen religiös, weltanschaulich und ideologisch motivierte Kriminalität und schützen vor Spionageaktivitäten anderer Staaten und vor Gefahren für kritische Infrastrukturen und verfassungsmäßige Einrichtungen. Die DSN besteht aus zwei Bereichen: Staatsschutz und Nachrichtendienst. Der Staatsschutz ist der polizeiliche Bereich, der konkrete Gefahren abwehrt und strafprozessuale Ermittlungen bei entsprechenden Straftaten durchführt. Der Nachrichtendienst dient als Frühwarnsystem. Er erkennt Gefahren frühzeitig und trägt zur Abwehr und Bekämpfung dieser Gefahren bei. Im Gegensatz zu Geheimdiensten, die aktive Maßnahmen setzen, hat ein Nachrichtendienst die Aufgabe, Informationen zu sammeln, auszuwerten, zu analysieren und Lagebilder zu erstellen.

Die DSN unterscheidet sich von anderen Nachrichtendiensten in Österreich durch ihren Fokus auf innere Gefahren und die Aufrechterhaltung der öffentlichen Grundordnung und Sicherheit. Die beiden militärischen Nachrichtendienste des Bundesheeres sind das Abwehramt (AbwA) und das Heeresnachrichtenamt (HNA). Das Abwehramt ist ein militärischer Inlandsnachrichtendienst, der Gefahren gegen das Österreichische Bundesheer abwehrt. Das Heeresnachrichtenamt ist der militärische Auslandsnachrichtendienst, der Entwicklungen im Ausland beobachtet, die eine Relevanz für das Inland haben könnten. Zusammengefasst ist die DSN ein ziviler Inlandsnachrichtendienst, das Abwehramt ein militärischer Inlandsnachrichtendienst und das HNA ein militärischer Auslandsnachrichtendienst.

Welche Rolle hat die DSN im Bereich Cybersicherheit?
Sylvia Mayer: In Österreich gibt es unterschiedliche Akteure innerhalb der Bundesverwaltung, die sich mit Cyberkriminalität, Cybersicherheit und auch Cyberabwehr beschäftigen. Unsere Hauptaufgabe im Bereich Cybersicherheit ist der Schutz verfassungsmäßiger Einrichtungen, internationaler Organisationen und kritischer Infrastrukturen vor Cyberangriffen. Wir sind verantwortlich für den Schutz von Einrichtungen wie dem Bundeskanzleramt, den Bundesministerien, den obersten Gerichtshöfen und dem Parlament. Im Rahmen des Verfassungsschutzes sind wir auch zuständig, wenn fremde Nachrichtendienste durch Cyberoperationen in Österreich spionieren. Wir schützen auch vor Wirtschaftsspionage durch Cyberangriffe, um die österreichische Wirtschaft vor massiven Angriffen anderer staatlicher Akteur:innen zu bewahren. Für herkömmliche Cyberkriminalität, wie Angriffe gegen KMUs, ist das Bundeskriminalamt zuständig. Zusammengefasst ist unser Ziel der Schutz des Staates, seiner Einrichtungen und wesentlicher Teile der Wirtschaft.

Wie geht der Nachrichtendienst mit den Herausforderungen im Cyberraum um bzw. welchen Herausforderungen sehen Sie sich gegenüber?
Sylvia Mayer: Der Fokus des Staats-

FOTO © MAG. KERSTIN HEHENBERGER

Sylvia Mayer
Stellvertretende Direktorin DSN (Direktion Staatsschutz und Nachrichtendienst)

Ing.in Mag.a Dr.in Sylvia Mayer, MA begann ihre Berufslaufbahn nach Abschluss der HTL für EDV und Organisation bei der Polizei in Linz und wechselte im Jahr 2012 in das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT), wo sie das Referat Schutz kritischer Infrastruktur sowie später die Abteilung Sicherheit und Schutz leitete.

In der BVT-Nachfolgeorganisation Direktion Staatsschutz und Nachrichtendienst (DSN) leitete sie die Abteilung Strategie, Grundsatz- und Stabsangelegenheiten. Am 1. Oktober 2023 wurde Sylvia Mayer in der DSN mit der Funktion der stellvertretenden Direktorin und Leiterin des Nachrichtendienstes betraut.

schutzes oder Nachrichtendiensts hat bisher immer sehr stark auf der Extremismus- und Terrorismusbekämpfung gelegen. Extremismus und Terrorismus stellen unmittelbare Gefahren für Leib, Leben und Gesundheit dar und sind daher die unmittelbare Gefahr für den Staat und die Bevölkerung.

Gleichzeitig sehen wir aber, dass Cyberangriffe in den letzten zehn Jahren sehr stark zugenommen haben und ebenso zur Gefahr für den Staat und für seine wichtigsten Einrichtungen werden. Dementsprechend müssen wir uns als Nachrichtendienst auch ausrichten. Das heißt, wir müssen – und wir machen dies auch seit vielen Jahren – den Aufgabenbereich der Cybersicherheit oder der Bekämpfung von Cyberangriffen auf mehreren Ebenen stärker in den Mittelpunkt stellen.

Erstens müssen wir diesen Bereich auch in der Organisation zentral verankern. Nämlich prominent als Abteilung auf erster Ebene mit einer entsprechenden Bedeutung in der Organisation – also auf gleicher Ebene mit der Terrorismus- und Extremismusbekämpfung.

Wir müssen uns zweitens auch rechtlich weiterentwickeln. Wir haben zwar sehr viele Befugnisse im Sicherheitspolizeigesetz, in der Strafprozessordnung, im Staatsschutz- und Nachrichtendienstgesetz, was diese herkömmlichen Gefahren betrifft, also die Sicherstellung von Gegenständen, Hausdurchsuchungen, Betreten von Grundstücken usw. Aber wir haben noch kaum technische Befugnisse, um den technischen Gefahren zu begegnen. Nur so können wir als Nachrichtendienst auch im Vorfeld besser agieren.

Die dritte Ebene betrifft das Budget und die Ressourcen – diese müssen in der öffentlichen Verwaltung noch stärker auf den Bereich Cybersicherheit fokussiert werden. Wir müssen im Nachrichtendienst die Systeme und die Infrastruktur schaffen, um mit den Gefahren umgehen zu können. Wir müssen am Puls der Zeit sein, was die aktuellen Anwendungen und Tools betrifft, um beispielsweise Desinformation zu erkennen, Malware-Analysen durchzuführen, Verschlüsselungen von sichergestellten Telefonen aufbrechen zu können etc. Es braucht mehr budgetäre Mittel für die Beschaffung von IT-Komponenten und Infrastruktur, damit wir mithalten können. Aber wir müssen uns natürlich auch personell entsprechend darauf ausrichten, dass dieser Bereich immer größer wird, indem wir ihn in der öffentlichen Verwaltung und auch bei uns attraktivieren.

Sie haben fehlende Befugnisse im Überwachungsbereich erwähnt. Warum glauben Sie, haben wir mehr Sorge davor, dass der Staat zu viel über uns weiß und weniger davor, welche Daten über unsere Smartphones, Social-Media-Accounts etc. für andere, wie z. B. Technologieunternehmen verfügbar sind?

Sylvia Mayer: Ich glaube, dass die Menschen oft gar nicht so im Blick haben, dass die Daten und die Informationen, die sie auf ihrem Mobiltelefon haben, für viele private Anbieter zugänglich sind. Zusätzlich sind diese Anbieter in den USA oder anderen Ländern gedanklich so weit entfernt, dass sie für die Menschen nicht wirklich relevant sind. Ich gebe Recht, dass die Bedenken vor staatlichen Eingriffen sehr hoch sind. Es ist wichtig, einen guten Mittelweg zwischen Freiheit und Sicherheit zu finden – diese Waage muss man unbedingt immer halten. Aber als Vertreterin einer Sicherheitsbehörde sehe ich schon gewisse Gefahren, wo wir unbedingt mehr polizeiliche Befugnisse brauchen, natürlich unter eingeschränktesten Voraussetzungen, und mit einem umfangreichen Rechtsschutz. Ich denke auch, dass es wichtig ist, die Bevölkerung darüber zu informieren, welche Voraussetzungen das sind und wie der Rechtsschutz aussieht, um diese Angst vielleicht zu nehmen. Grundsätzlich braucht es mehr Sachlichkeit und weniger Verunsicherung, um das Vertrauen in der Bevölkerung zu steigern.

Das heuer vorgestellte Risikobild hat für großes Echo gesorgt und ist weitab von Optimismus. Welche Herausforderungen kommen aus Sicht der DSN auf uns zu und welche Empfehlungen können Sie Unternehmen mitgeben?

Sylvia Mayer: Wir sehen zahlreiche Trends und Entwicklungen, die uns in Bezug auf Sicherheit als Behörde, aber auch als Gesellschaft die nächsten drei bis zehn Jahre sehr stark beschäftigen werden. Einer dieser Trends sind die geopolitischen Entwicklungen, die wir bereits in den letzten Jahren verfolgen konnten und die sich seit dem Angriffskrieg Russlands gegen die Ukraine oder auch mit dem Nahostkonflikt wieder verschärft haben und in den Mittelpunkt der Beobachtungen gerückt sind. Diese geopolitischen Entwicklungen haben nicht nur Auswirkungen auf die Konfliktgebiete, wo sie stattfinden, sondern auch auf die Sicherheitslage in Österreich – sei es Spionage, Desinformation oder Hacktivismus. Das alles spielt bei geopolitischen Entwicklungen immer eine Rolle und dementsprechend wirken sie sich aus.

Der zweite Trend sind die Digitalisierung in der Gesellschaft und die schnelle Entwicklung von Kommunikationstechnologien. Kriminelle und staatliche Akteur:innen kommunizieren fast ausschließlich mit verschlüsselten Technologien, was es für Sicherheitsbehörden schwer macht, diese zu überwachen, weil uns die rechtlichen Befugnisse fehlen. Die Digitalisierung der Gesellschaft führt auch zu mehr Angriffsflächen für Unternehmen, wenn man z. B. an Remote-Zugänge denkt.

Der dritte Trend sind die verstärkte Polarisierung und Ideologisierung in der Gesellschaft. Gewisse Themen werden sehr polarisierend, sehr emotional und sehr ideologisierend diskutiert, wo sich die Ränder häufig sehr stark radikalisieren, was dann letztendlich in Extremismus endet.

Der letzte Trend, den ich erwähnen möchte, ist das sinkende Vertrauen in den Staat, in politische, staatliche Institutionen und Entscheidungsträger:innen. Das beobachten wir seit mehreren Jahren, insbesondere seit der COVID-19-Pandemie, wo sich die Szene der Coronamaßnahmen-Gegner:innen entwickelt hat und sich dann weiterentwickelt hat zu einer Gruppierung, die nicht mehr klar dem ursprünglichen Links-/Rechtsextremismus zuzuordnen ist, sondern die wirklich klar gegen die Demokratie ist.

> **Unsere Motivation liegt in der Herausforderung, als Verteidiger:innen alles schützen zu müssen, während ein:e Angreifer:in nur eine Schwachstelle finden muss.**
>
> Sylvia Mayer

Die konkreten drei Gefährdungen, die durch diese Trends entstehen, sind jedenfalls der islamistische Extremismus und Terrorismus, der Rechtsextremismus und auch die Cyberspionage.

Sie sagen, die Kommunikation findet im Internet statt – also eigentlich völlig unkontrolliert. Können wir es Ihrer Meinung nach irgendwie schaffen, die Diskussionskultur wieder zurückzuholen?

Sylvia Mayer: Öffentliche Diskussionen sind mittlerweile sehr emotionalisiert. Es wäre daher wichtig, die Diskussionskultur wieder mehr auf eine sachliche Ebene zu bringen. Natürlich findet Kommunikation mittlerweile in sozialen Medien statt und das wird man auch nicht mehr ändern können. Was wir dazu beitragen können als Sicherheitsbehörden, ist konsequent gegen

> **Die Aufgabe der Direktion Staatsschutz und Nachrichtendienst ist es, die Prinzipien der Demokratie zu schützen. Also unsere gesellschaftliche Ordnung, wie wir sie leben, aufrechtzuhalten.**
>
> Sylvia Mayer

Hass im Netz und gegen Straftaten vorzugehen und diese zu unterbinden. Selbstverständlich ist die Meinungsäußerungsfreiheit ein wichtiges und hohes Gut in einem demokratischen Rechtsstaat und Eingriffe in diese Freiheit sind daher nur begrenzt möglich. Aber man hat oft den Eindruck, dass User:innen nicht bewusst ist, dass sie auch im Internet oder auf Social Media nicht einfach alles sagen können, was sie wollen. Da muss man dann schon sicherheitsbehördlich vorgehen und das konsequent verfolgen. Aber natürlich muss man auch die sozialen Plattformanbieter in die Pflicht nehmen, Desinformationen oder radikale extremistische Inhalte etc. von ihrer Plattform zu entfernen und entsprechend darauf hinzuweisen. Hier gibt es bereits einige EU-Rechtsakte, die national umgesetzt werden.

Zum Thema Desinformation: Warum sind die anderen so gut im Streuen solcher Informationen und warum können wir nichts dagegen tun?
Sylvia Mayer: Das liegt immer am Interesse des jeweiligen Staates. Russland hat geopolitisch ein großes Interesse daran, Desinformationskampagnen zu streuen. Einerseits aufgrund des Angriffskrieges gegen die Ukraine und den Konsequenzen, die dadurch herbeigeführt wurden, wie die Sanktionen. Russland muss hier dagegenwirken und tut dies unter anderem mit Desinformationskampagnen. Andererseits ist es auch im Interesse Russlands, den Westen und somit demokratische Systeme zu schwächen. Das machen sie bereits seit Jahren und investieren hier auch viele Ressourcen in Desinformationskampagnen.

Wir haben kein Interesse an Desinformation, darum betreiben wir dies natürlich in dem Sinne auch nicht. Wir betreiben auch keine Social-Bot-Farmen oder Trollfabriken, weshalb es schwierig ist, hier technisch etwas entgegenzusetzen. Wir können daher nur gesellschaftlich reagieren, also die Gesellschaft insgesamt resilienter gegen Desinformationen machen.

Wie ordnen Sie das aktuelle Risiko ein, dass uns Desinformationskampagnen beeinflussen bzw. in unseren Grundfesten erschüttern?
Sylvia Mayer: Sie beeinflussen uns definitiv. Nehmen wir das Thema Wahlen als Beispiel. Desinformation beeinflusst Wähler:innen in ihrer Entscheidung oder in ihrer Einstellung zu politischen Entscheidungsträger:innen etc. Sie beeinflusst die Bevölkerung allgemein in ihrem Zugang zur Demokratie. Hier können wir von Desinformation zu unterschiedlichen Zeitpunkten betroffen sein.

Vor der Wahl gibt es das Szenario, dass es Cyberangriffe auf Parteien gibt. Bei diesen Cyberangriffen auf die IT-Systeme werden Daten gestohlen, die dann missbräuchlich oder manipulierend veröffentlicht werden, um jemanden besserzustellen oder zu denunzieren.

Während der Wahl kann es zu einer Beeinflussung von Wähler:innen kommen. Das heißt, dass durch Desinformationskampagnen, die bereits im Vorfeld gestreut werden, Narrative verbreitet werden, die die Wähler:innen zu Gunsten oder Lasten einer bestimmten Partei oder Person beeinflussen sollen. Ein weiteres Szenario während der Wahl wäre ein Cyberangriff gegen Systeme der Wahlbehörden. Dazu muss man sagen, dass Österreich hier sehr resilient aufgestellt ist, weil die Stimmzettel zusätzlich nochmals händisch ausgezählt werden. Eine solche Manipulation würde daher erkannt werden. Nichtsdestotrotz würde ein Angriff für Verunsicherung sorgen und somit bestimmten staatlichen Akteur:innen in die Hände spielen.

Die dritte Phase ist nach der Wahl, wo Desinformation z. B. so platziert werden kann, dass Misstrauen in das Wahlsystem gesät wird und dann auch später die Wahlergebnisse nicht akzeptiert werden, wie wir es auch im letzten US-Wahlkampf gesehen haben.

> **Die Digitalisierung und Technologisierung der Gesellschaft führt natürlich auch zu mehr Angriffsflächen und Verwundbarkeiten.**
>
> Sylvia Mayer

Damit in Zusammenhang stehen Deepfakes: Inwieweit können wir den Dingen, die wir sehen, noch glauben? Was können wir tun, um dagegen anzukommen?
Sylvia Mayer: Grundsätzlich ist es nichts Neues, dass wir nicht alles glauben sollen, was wir hören, bzw. dass man Dinge hinterfragen sollte. Beim Sehen ist es, glaube ich, etwas anders. Wir sind es gewohnt, das zu glauben, was wir wahrnehmen bzw. selbst mit eigenen Augen sehen. Darauf konnten wir uns bisher verlassen – durch Deepfakes ist das allerdings anders geworden und wir müssen uns erst daran gewöhnen, jetzt wirklich alles kritisch zu hinterfragen. Die eigene Recherche und ein eigener Faktencheck unter anderen Quellen sind z. B. Maßnahmen, die man selbst treffen kann.

Ein großes Thema derzeit ist die Künstliche Intelligenz – ist diese neue Technologie Fluch oder Segen?
Sylvia Mayer: Wir sehen KI als Chance und als Risiko, so wie viele Trends, die es gibt. Wir gehen davon aus, dass Künstliche Intelligenz kurz- bis mittelfristig nur eine automatisierte Unterstützung von manuellen Prozessen bei Cyberangriffen sein wird, das heißt, dass z. B. Phishing-E-Mails schneller vorbereitet werden können. Wir gehen nicht davon aus, dass kurz- und mittelfristig Cyberangriffe voll automatisiert durch Künstliche Intelligenz durchgeführt werden. Dasselbe gilt für die Abwehr von Cyberangriffen. Künstliche Intelligenz kann dabei helfen, die Cybersicherheit zu stärken, indem man zum Beispiel gewisse Lock-Analyse-Maßnahmen setzt und so die Abwehr verbessert. Aber eher als unterstützende Maßnahme und nicht voll automatisiert.

Phänomen Cybercrime: Was ist die größte Überraschung, wenn es um das Vorgehen organisierter Gruppen geht? Was müssen wir wissen, damit wir unser Gegenüber besser verstehen können?
Sylvia Mayer: Das Auffälligste im Bereich Cybercrime ist sicherlich die differenzierte Vorgehensweise von staatlichen Akteur:innen und rein kriminellen Organisationen. Staatliche Akteur:innen richten ihre Cyberoperationen nach den Interessen ihres Staates aus. Beispielsweise zielen die Geheimdienste Nordkoreas darauf ab, Krypto-Plattformen und digitale Banken anzugreifen, um ihr Nuklearprogramm zu finanzieren. China hingegen hat das Ziel, bis 2049 die

weltweite Wirtschaftsmacht Nummer eins zu werden. Daher zielen ihre Cyberoperationen darauf ab, Informationen von Hochtechnologieunternehmen auszuspionieren und zu erbeuten, um die eigene Wirtschaft zu stärken. Unternehmen müssen daher wissen, ob sie aufgrund ihres Standorts oder Sektors ein mögliches Ziel sein könnten. Sie müssen wissen, wer die Gegner:innen sind und auch die eigenen „Juwelen" kennen, also jene Bereiche, die für fremde Akteur:innen interessant sein könnten. Im Gegensatz dazu haben kriminelle Gruppen eine rein monetäre Motivation und zielen nicht spezifisch auf bestimmte Unternehmen ab. Sie folgen einer Kosten-Nutzen-Überlegung, um möglichst viel Geld zu erwirtschaften. In dem Fall sind Unternehmen gut geschützt, wenn sie ihre IT-Sicherheit standardmäßig gut implementiert haben.

Es geht bei Ihnen auch um Wirtschaftsschutz – auf welche Bedrohungen aus dem Cyberraum sind unsere Unternehmen Ihrer Ansicht nach schon recht gut vorbereitet und wo können wir noch besser werden?

> **Wir können nur gesellschaftlich reagieren, also die Gesellschaft insgesamt resilienter gegen Desinformationen machen.**
>
> Sylvia Mayer

Sylvia Mayer: Ganz gut vorbereitet sind Unternehmen in Bezug auf Hacktivismus. Hier haben sie es mit aktivistischen Hacker:innen zu tun, die sich für bestimmte Themen einsetzen und meist mit Low-Level-Angriffen wie DDoS, Datenleaks etc. vorgehen. Wo Unternehmen schon gut, aber nicht ausreichend gesichert sind, ist die Gefahr der Ransomware. Da sehen wir eine starke Professionalisierung von Ransomwaregruppierungen, die mittlerweile wie Klein- und Mittelunternehmen agieren und ihre Services auch für andere anbieten. Also Ransomware-as-a-Service. Hier müssen Unternehmen teilweise die Sicherheitsmaßnahmen noch erhöhen. Wo Unternehmen noch nicht ausreichend gesichert sind, sind sogenannte APTs, also Advanced-Persistent-Threat-Angriffe. APT-Akteur:innen greifen zielgerichtet einzelne Unternehmen an – zu Spionagezwecken zum Beispiel – und stecken sehr viel Zeit und Ressourcen in diesen Angriff. Das macht es für die Unternehmen schwer, sich ausreichend dagegen zu schützen.

Wie motivieren Sie Ihr Team, ständig an der Weiterentwicklung und Verbesserung der Cybersecurity zu arbeiten – vor allem, da es in diesem Bereich keine Ziellinie gibt, die man überschreiten kann?
Sylvia Mayer: Unser Team steht vor dem klassischen Defenders-Dilemma: Während ein:e Angreifer:in nur eine Schwachstelle finden muss, um ins System zu gelangen, müssen wir als Verteidiger:innen alles schützen. Diese Herausforderung ist gleichzeitig unsere Motivation. Das Wissen, dass wir den Staat ständig schützen müssen und ständig neue Bedrohungen auftauchen, macht unsere Aufgabe spannend. Bei uns erhält das Team umfassende Informationen von ausländischen Sicherheitsbehörden über aktuelle Angriffe von staatlichen Akteuren wie Russland, Iran, Nordkorea und China. Sie haben die Möglichkeit, aktuelle Angriffsmuster zu analysieren und Cyberoperationen gegen Einrichtungen in Österreich auszuwerten. Die ständige Konfrontation mit den aktuellen Angriffen und der umfassende Überblick sind sehr motivierend.

Wie gehen Sie und Ihr Team mit der psychologischen Belastung um, die durch die Arbeit im Cybersicherheitsbereich entsteht, insbesondere angesichts der Tatsache, dass Sie über Ihre Arbeit nicht mit Außenstehenden sprechen können?
Sylvia Mayer: Das ist natürlich eine Herausforderung. In einem so spannenden Aufgabenbereich wie dem unseren besteht oft das Bedürfnis, über die täglichen Aktivitäten und Herausforderungen zu sprechen. Wir sensibilisieren unser Team jedoch stark dazu, dies nicht zu tun. Innerhalb unserer Teams ist der Austausch wichtig, aber nach außen hin sollte man nicht einmal preisgeben, dass man in unserer Organisation tätig ist, um unerwünschte Nachfragen zu vermeiden.

Mit Blick auf den derzeitigen Fachkräftemangel: Wie können wir diesem vorbeugen und was braucht es ausbildungsmäßig, um auch zukünftig gut aufgestellt zu sein?
Sylvia Mayer: Um dem Fachkräftemangel entgegenzuwirken, setzen wir auf zwei Elemente: Rekrutierung und Weiterentwicklung bestehender Mitarbeiter:innen. Bei der Rekrutierung ist es wichtig, die Attraktivität unseres Aufgabengebiets nach außen darzustellen, was wir beispielsweise über LinkedIn und unsere Website tun. Wir versuchen, potenzielle Bewerber:innen auf uns aufmerksam zu machen und ihnen zu zeigen, was wir tun. Gleichzeitig ist es wichtig, bestehende Mitarbeiter:innen im öffentlichen Dienst und in unserer Organisation weiterzuentwickeln und umzuschulen. Eine unserer Maßnahmen ist die Förderung von IT-Studien, die nebenberuflich absolviert werden können. Auf diese Weise versuchen wir, Mitarbeiter:innen, die in anderen Bereichen tätig waren, in das Feld der Cybersicherheit zu holen. Ausbildungsmäßig sind eine technische Ausbildung und ein Verständnis für die Analyse von Angriffen und die Umsetzung von Gegenmaßnahmen erforderlich. Aber auch Kenntnisse in Data Science sind wichtig, um Erkenntnisse aus großen Datenmengen gewinnen zu können. Das Wichtigste ist jedoch das Grundverständnis der Führungskräfte, dass das Thema Cybersicherheit wesentlich ist und in den nächsten Jahren immer wichtiger werden wird. Dieses Bewusstsein muss sowohl im BMI als auch in unserer Organisation verankert sein.

Was ist die häufigste Frage, die Ihnen bislang gestellt wurde, und welche Frage hat man noch nicht gestellt, obwohl es wichtig wäre, die Antwort zu kennen?
Sylvia Mayer: Die häufigste Frage, die mir gestellt wird, ist wahrscheinlich: „Was sind die größten aktuellen Bedrohungen?" Eine Frage, die mir noch nicht gestellt wurde, die ich aber für sehr wichtig halte, ist: „Gibt es genug Frauen im Bereich der Cybersicherheit und der IT-Ermittlung?" Meine Antwort darauf lautet nein. Es ist äußerst wichtig, diese Antwort zu kennen, denn Diversität unter den Mitarbeiter:innen, insbesondere im Bereich der IT-Ermittlung und Cybersicherheit, ist von großer Bedeutung. Jedes Team profitiert von Diversität in Bezug auf Geschlecht, Alter, Ausbildung usw., und unsere IT- und Cybersicherheitsteams müssen unbedingt weiblicher werden. Das ist ein sehr wichtiges Thema für mich.

Wenn wir uns in einem Jahr wieder treffen, was würden wir uns dann wünschen, heute schon getan zu haben?
Sylvia Mayer: Wir würden uns wünschen, dass wir unsere technischen und rechtlichen Befugnisse erweitert haben, damit wir uns an internationale Standards von Sicherheitsbehörden annähern und dass wir auch rechtlich dort ankommen, wo die Kriminellen längst sind.

32 % der Vorständ:innen und Geschäftsführer:innen hoffen, dass sie sich im kommenden Jahr nicht mehr so viel mit Cybersicherheit beschäftigen müssen.

33 % der Aufsichtsrät:innen haben angegeben, dass Cybersicherheit für sie zu einem wichtigen Teil ihres Lebens geworden ist. 67 % sagen, dass Cyberangriffe in den kommenden 12 Monaten zunehmen werden.

37 % der Befragten würden bevorzugt Security-Lösungen von österreichischen Unternehmen einsetzen, ein Aufwärtstrend im Vergleich zum Vorjahr.

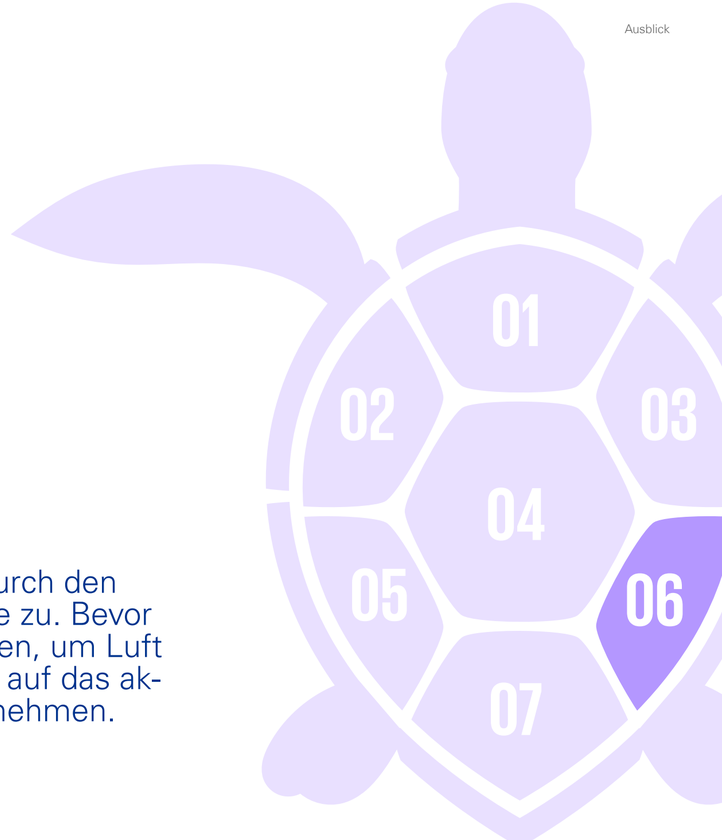
39 % der Befragten glauben, dass eine Erweiterung der Ermittlungsbefugnisse notwendig ist, um Cyberangriffe aufzuklären, eine Steigerung im Vergleich zum Vorjahr (28%).

20 % der Befragten finden, dass ein Cybersicherheitsvorfall einfach und ohne viel Aufwand gemeldet werden kann, ein Rückgang im Vergleich zum Vorjahr (22%).

06

Ausblick

Die Reise unserer Schildkröte durch den Cyberozean neigt sich dem Ende zu. Bevor wir gemeinsam mit ihr auftauchen, um Luft zu holen, werfen wir einen Blick auf das aktuelle Stimmungsbild der Unternehmen.



> **Es ist nicht die Frage, OB ein Unternehmen mit den Auswirkungen eines Cyberangriffs umgehen muss, sondern WANN. Noch blieben wir verschont.**
>
> Quelle: Studienteilnehmer:in

Schauen wir uns an, wie sie die derzeitige Cybersicherheitslage beurteilen und ob auch sie glauben, im nächsten Jahr Luft holen zu können.

Sich treiben lassen

50 Prozent der Unternehmen sagen, dass Cyberangriffe ihre geschäftliche Existenz bedrohen. Hier ist ein leichter Rückgang zum Vorjahr (55 Prozent) zu verzeichnen. Ein Viertel meint sogar, dass Cyberangriffe nicht ihre geschäftliche Existenz bedrohen würden.

Für 40 Prozent der Befragten hat sich die emotionale Bedeutung von Cybersecurity durch aktuelle geopolitische Konflikte verändert. Im Vorjahr haben dieser Aussage noch 47 Prozent zugestimmt. Über Beeinflussungsversuche, Desinformationskampagnen und Spionage staatlicher Akteur:innen aus anderen Ländern wird nahezu täglich medial berichtet und auch heimische Unternehmen haben Hackingangriffe ausländischer Täter:innengruppen bereits zu Genüge verspürt. In Anbetracht des Rückgangs der emotionalen Bedeutung für die Umfrageteilnehmenden stellt sich die Frage: Sind wir nüchterner geworden und werden diese Vorfälle für uns zu einer Art Normalzustand?

Kopf in den Sand

39 Prozent sind der Ansicht, dass es einer Erweiterung der Ermittlungsbefugnisse bedarf, um Cyberangriffe aufzuklären. Hier beobachten wir eine Steigerung im Vergleich zu letztem Jahr (28 Prozent). Täter:innengruppen verwenden moderne Technologien, wo keine Möglichkeit besteht, sie abzuhören, zu identifizieren oder abzufangen. Die Unternehmen merken, dass die Aufklärung mit den momentan zur Verfügung stehenden Befugnissen nicht mehr durchführbar bzw. bewältigbar ist.

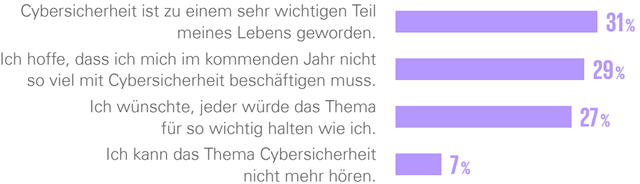
74 Prozent sind der Meinung, dass es bei Angriffen aus dem Ausland nur wenig Chancen gibt, die Täter:innen zu identifizieren. Im Vorjahr stimmten dieser Aussage nur 61 Prozent zu. Der Leidensdruck dürfte hier gewachsen sein. 63 Prozent sagen, dass es eine verstärkte EU-weite Zusammenarbeit beim Thema Cybersicherheit benötigt. Im Vorjahr sahen diesen Bedarf allerdings noch 74 Prozent. Es scheint sich eine gewisse Ohnmacht oder Hoffnungslosigkeit bei den Unternehmen einzuschleichen.

Mehr über die Wichtigkeit internationaler Kooperationen, wie z. B. bei der Zerschlagung von LockBit hören Sie in unserer Podcastfolge mit Carsten Meywirth.

Wissen, wohin es geht

Die Meldung eines Cybersicherheitsvorfalls ist nach wie vor eine Hürde für die Unternehmen: Nur 20 Prozent finden, dass ein Cybersicherheitsvorfall einfach und ohne viel Aufwand gemeldet werden kann. Dieser Wert ist im Vorjahresvergleich (22 Prozent) sogar noch weiter gesunken. Nur 28 Prozent (Vorjahr: 38 Prozent) wissen, bei welchen öffentlichen Stellen sie einen Cybersicherheitsvorfall melden können. Aufklärungsarbeit und Bewusstseinsbildung sind dringend notwendig.

Abb. 26: Cyberstimmung



Zurück nach Hause

37 Prozent würden bevorzugt Security-Lösungen von österreichischen Unternehmen einsetzen. Schön ist zu sehen, dass hier im Vergleich zum Vorjahr sogar ein Aufwärtstrend erkennbar ist. Es gibt somit eine wachsende Präferenz für österreichische Anbieter von Sicherheitslösungen. Dies könnte auf eine starke lokale Expertise, schnellerer und direkterer Unterstützung und strengere Datenschutzstandards zurückzuführen sein. Es unterstreicht auch die Chance für österreichische Unternehmen, ihre Security-Lösungen weiterzuentwickeln und zu vermarkten, da offensichtlich eine erhöhte Nachfrage besteht. Aus volkswirtschaftlicher Sicht entsteht dadurch ein Potenzial für zukünftiges Wachstum und Innovation in der heimischen Cybersicherheitsbranche, wodurch weitere Arbeitsplätze geschaffen werden können und eine Stärkung des Wirtschaftsstandorts erfolgt.

Aber auch in Bezug auf die Aus- und Weiterbildung deutet dies auf einen wachsenden Bedarf an Fachleuten im Bereich Cybersicherheit hin und somit die Bereitstellung von zusätzlichen Bildungsangeboten, um den Bedarf der Industrie zu decken und die wachsende Nachfrage nach lokalen Sicherheitslösungen zu erfüllen. Es ist weiters ein Appell für mehr Investitionen und Ressourcen im Bereich der Forschung und Entwicklung von Cybersicherheitstechnologien.

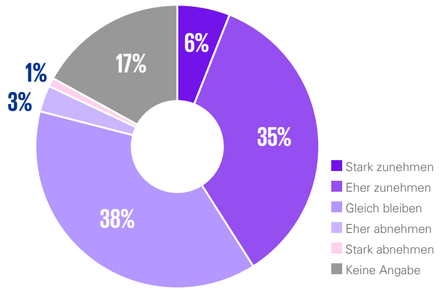
Die eigene Umgebung gut einprägen

31 Prozent der Befragten geben an, dass Cybersicherheit zu einem sehr wichtigen Teil ihres Lebens geworden ist. Im Vorjahr waren das noch 47 Prozent. 27 Prozent (Vorjahr 31) wünschen sich, dass jeder das Thema für so wichtig halten würde wie sie selbst. 29 Prozent hoffen, dass sie sich im kommenden Jahr nicht mehr so viel mit Cybersicherheit beschäftigen müssen, 7 Prozent können das Thema nicht mehr hören (siehe Abb. 26).

32 Prozent der Vorständ:innen und Geschäftsführer:innen hoffen, dass sie sich im kommenden Jahr nicht mehr so viel mit Cybersicherheit beschäftigen müssen. Das ist insofern auch spannend, weil zumindest 49 Prozent zustimmen, dass Cyberangriffe die geschäftliche Existenz bedrohen. 39 Prozent sind der Meinung, dass Cyberangriffe in den nächsten 12 Monaten gegen ihr Unternehmen zunehmen werden.

Bei den Aufsichtsrät:innen haben 33 Prozent angegeben, dass Cybersicherheit für sie zu einem wichtigen Teil ihres Lebens geworden ist. 67 Prozent sagen, dass Cyberangriffe in den kommenden 12 Monaten zunehmen werden. Sie sehen, dass v. a. die technologischen Möglichkeiten, mit denen heute Unternehmen ange-

Abb. 27: Wie werden sich Ihrer Meinung nach die Cyberangriffe gegen Ihr Unternehmen in den nächsten zwölf Monaten entwickeln?



griffen werden können, exponentiell zunehmen. Das ist den sich rasant entwickelnden technologischen Veränderungen und der damit verbundenen Vergrößerung der Angriffsfläche geschuldet.

Bei der Frage, wie sich Cyberangriffe gegen das eigene Unternehmen in den nächsten zwölf Monaten entwickeln werden, sind 41 Prozent der Unternehmen überzeugt, dass diese zunehmen werden. 38 Prozent sagen, dass die Cyberangriffe gleich bleiben werden. Im Vorjahr hatten noch 63 Prozent eine Zunahme prognostiziert, während 27 Prozent der Meinung waren, dass diese gleich bleiben werden. Man merkt: Wir sind bereits auf einem hohen Niveau angelangt. Ob wir uns hier einpendeln, bleibt abzuwarten.

Unberechenbare Reise

Was haben wir auf unserer Reise durch die rauen Gewässer der Cyberwelt gelernt? Und wie wird es weitergehen? Durch die zunehmende Digitalisierung und weltweite Vernetzung sind Unternehmen verwundbarer für Cyberangriffe geworden. Sich dieser Bedrohung bewusst, blicken sie mit gemischten Gefühlen auf die kommenden zwölf Monate. Insbesondere bewegen sie dabei die folgenden Themen:

Für die Unternehmen stellen geopolitische Spannungen und Täter:innengruppen aus nicht kooperierenden Ländern eine zunehmende Bedrohung dar. Die politische Instabilität in bestimmten Regionen könnte zur Intensivierung krimineller Cyberaktivitäten führen. Unternehmen müssen ihre Sicherheitsmaßnahmen verstärken und ihre Mitarbeitenden für diese Bedrohungen sensibilisieren.

Viele der Befragten gehen davon aus, dass kein Unternehmen vor Cyberangriffen sicher ist und dass sich die Angriffswerkzeuge weiterentwickeln. Diese Entwicklung könnte dazu führen, dass Cyberangriffe

> **Technische Voraussetzungen der Angreifer werden immer besser und es ist immer einfacher. Kriminelle arbeiten wie globale Industriebetriebe (arbeitsteilig)!**
>
> Quelle: Studienteilnehmer:in

immer ausgefeilter werden und es schwieriger wird, sie zu erkennen und abzuwehren.

Die Unternehmen sehen den Einsatz von KI sowohl als Chance als auch als Risiko. Einerseits könnte uns KI dabei helfen, Cyberangriffe zu bemerken und abzufangen. Sie befürchten andererseits, dass KI die Angriffe komplexer machen und die Möglichkeiten für Angreifer:innen erweitern könnte. KI könnte es Cyberkriminellen ermöglichen, Angriffe zu automatisieren und auf eine Weise durchzuführen, die für herkömmliche Sicherheitssysteme schwer erkennbar ist. Das führt zu einem Paradigmenwechsel, der das volle Spektrum der Angriffe gegen eine Einzelperson (Informationsbeschaffung, Social Engineering, (Spear-)Phishing, Malware, Data Leakage, Ransomware, Lösegeldabwicklung) automatisiert und mit wenig menschlicher Interaktion auf Seite der Angreifer:innen durchführen lässt.

Die Verlagerung von Daten und Diensten in die Cloud könnte es Cyberkriminellen erleichtern, Zugang zu sensiblen Informationen zu erhalten. Unternehmen müssen dafür sorgen, dass ihre Cloud-Dienste sicher sind und dass sie über wirksame Maßnahmen zur Erkennung und Abwehr von Cyberangriffen verfügen. Kleinere Unternehmen sehen sich als weniger attraktive Ziele für Cyberangriffe. Das könnte dazu führen, dass sie weniger in Sicherheitsmaßnahmen investieren. Eines steht jedoch fest: Cyberangriffe können uns alle treffen.

> **Geringe Einstiegshürde; vermehrte geopolitische Konflikte mit direkten oder Spillover-Effekten; hohe Chance auf Erfolg bei gleichzeitig geringer Gefahr auf Strafverfolgung.**
>
> Quelle: Studienteilnehmer:in

Einige Unternehmen sehen die derzeitige wirtschaftliche Instabilität und Unsicherheit als potenzielle Treiber für Angriffe. Dadurch könnten Unternehmen, insbesondere solche mit wertvollem geistigen Eigentum, zunehmend ins Visier von Cyberkriminellen geraten, die sich finanzielle Gewinne durch die Angriffe erhoffen.

Die Befragten sind sich bewusst, dass die technischen Voraussetzungen der Angreifer:innen immer besser werden und es immer einfacher wird, Cyberangriffe durchzuführen. Sie sehen kriminelle Aktivitäten zunehmend als globale Industrie.

An die Oberfläche kommen

Unternehmen haben die steigende Bedrohung durch Cyberattacken erkannt und stellen sich auf zunehmend komplexe Angriffe ein. Sie sind sich der Schwierigkeiten bewusst und investieren in Maßnahmen zur Verbesserung ihrer Cybersicherheit. Die Unsicherheit bleibt dennoch groß, da die Dynamik und Komplexität der Bedrohungen auf einem hohem Niveau sind. Es bleibt abzuwarten, wie sich die Situation im kommenden Jahr entwickeln wird und welche neuen Herausforderungen, aber vielleicht auch Chancen sich für heimische Unternehmen ergeben werden.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1.

Trotz der erkannten Bedrohung und getroffenen Maßnahmen gibt es noch Herausforderungen, insbesondere in Bezug auf die Meldung von Cybersicherheitsvorfällen und das Wissen, an welche öffentlichen Stellen sie gemeldet werden können. Es besteht ein Bedarf an weiterer Aufklärungsarbeit und Bewusstseinsbildung.

2.

Es gibt eine wachsende Präferenz für österreichische Anbieter von Cybersecurity-Lösungen, was Chancen für die österreichische Wirtschaft und den Arbeitsmarkt bietet. Es ist ein Appell für die Stärkung der technologischen Kompetenzen und eine Erweiterung der Aus- und Weiterbildungsmöglichkeiten im Bereich Cybersicherheit.

3.

Das volatile Umfeld, das uns umgibt, macht eine Prognose der Angriffsentwicklungen immer unberechenbarer. Wenngleich Unternehmen hohe Auswirkungen von Cyberangriffen gegen ihr Unternehmen erwarten, stellt sich auch eine gewisse Resignation ein, da sie vermehrt hoffen, sich in den kommenden 12 Monaten nicht mehr mit den Themen beschäftigen zu müssen. Allerdings ist Cybersecurity gekommen, um zu bleiben, denn neben der Regulatorik (NIS2, DORA etc.) sind es auch die Täter:innengruppen, die ihr Glück versuchen, um (finanziell) erfolgreich zu sein.

> **Die Unsicherheit überwiegt – es wird immer schwieriger, im Cyberraum wahr von falsch zu unterscheiden.**
>
> **Wir müssen die Fähigkeit entwickeln, die digitalen Schweißperlen auf der Stirn der Angreifer:innen zu erkennen.**
>
> **Nur so können wir sicher in der digitalen Welt navigieren.**
>
> Robert Lamprecht

Cyberfitness ist zukünftig unerlässlich

Ulrike Domany-Funtan und Simon Tjoa diskutieren über die Bedeutung von und die Herausforderungen bei der Cybersecurity-Ausbildung. Sie betonen die Notwendigkeit der kontinuierlichen Weiterbildung und die Rolle von Initiativen wie fit4internet und Hochschulen bei der Förderung der digitalen Kompetenz.

Warum ist Ihrer Meinung nach eine Ausbildung im Bereich Cybersecurity in der heutigen digitalen Welt so wichtig und welche Rolle spielt die kontinuierliche Weiterbildung?
Ulrike Domany-Funtan: Nicht jeder Mensch muss ausgebildeter Cybersecurity-Profi sein, aber wir alle müssen uns mit dem Thema auseinandersetzen. Dabei geht es vor allem ums Erkennen der Auswirkungen des eigenen Digitalverhaltens „Digital Skills Barometer“ sowie der damit verbundenen Gefahren und Risiken. Digitalisierung – und damit Cybersecurity – ist nichts Statisches. Infrastruktur und geltende Sicherheitsstandards entwickeln sich laufend weiter. Und genau deshalb ist es wichtig, „dran“ zu bleiben und sich über Entwicklungen am Laufenden zu halten. Wichtig dabei: Jede Generation muss „cyberfit“ werden. Unsere österreichweite Erhebung, der „Digital Skills Barometer“ , zeigt, dass ältere Menschen seltener in Weiterbildungsmaßnahmen investieren als jüngere. Mit Blick darauf, wie zügig die digitale Transformation voranschreitet und wie wichtig dabei lebenslanges Lernen ist, muss sichergestellt werden, dass jede Generation, die sich in der digitalen Welt bewegt oder bewegen will, Schritt halten kann.

Simon Tjoa: Für mich gibt es zwei Hauptgründe, warum Cybersicherheit zunehmend an Bedeutung gewonnen hat und damit auch die Ausbildung in diesem Bereich. Zum einen sind digitale Technologien aus unserem Alltag nicht mehr wegzudenken. Unabhängig von Branche oder Bereich hat der Einsatz digitaler Technologien deutlich zugenommen, was zu einer hohen Abhängigkeit in Wirtschaft und Gesellschaft führt. Zum anderen nehmen Cyberangriffe und Cybervorfälle branchen- und größenunabhängig zu.

Welche spezifischen Fähigkeiten oder Kenntnisse sollten in einer Cybersecurity-Ausbildung vermittelt werden?
Ulrike Domany-Funtan: Es gibt Angebote in unterschiedlichen Abstufungen, bei denen Fähigkeiten und Kenntnisse in ihrer Ausprägung stark variieren. Aus Sicht von f4i ist es wichtig, dass quer über alle Generationen, Branchen und Bildungshintergründe hinweg ein gezielter Wissensaufbau zu den Grundbegriffen der Digitalisierung stattfindet. Dazu gehört auch Cybersecurity. Ziel muss es sein, dass sich Menschen so viel Wissen aneignen, dass sie sich selbstbestimmt und sicher durch die Onlinewelt bewegen können. Für uns geht es bei der digitalen Fitness im Bereich Cybersecurity um vier konkrete Kompetenzen: Geräte schützen, personenbezogene und vertrauliche Daten sowie Privatsphäre schützen, Gesundheit und Wohlbefinden schützen, sich vor Betrug und Konsument:innenrechtsmissbrauch schützen.

Simon Tjoa: Cybersicherheit hat sich mittlerweile zu einem sehr breiten Feld entwickelt, weshalb die Ausbildungsziele stark von den spezifischen Anforderungen und den daraus abgeleiteten Ausbildungsprofilen abhängen. Ein entscheidender Faktor für Cybersicherheitsexpert:innen ist eine umfassende Ausbildung, die technische und organisatorische Fähigkeiten vereint. Zu den Schlüsselkompetenzen der Expert:innen der Zukunft zählen auf organisatorischer Ebene Governance, Risikomanagement und Compliance sowie auf technischer Ebene sicherer Betrieb von IT-Infrastruktur, Ethical Hacking zur Erkennung von Schwachstellen und Incident Response.

Wie können Unternehmen ihre Mitarbeiter:innen effektiv in Cybersecurity schulen und sensibilisieren?
Ulrike Domany-Funtan: Der aktuelle „Digital Skills Barometer“ zeigt, dass die Faktoren Zeit und Geld wesentliche Aspekte für die Weiterbildung der Österreicher:innen sind. Steht beides zur Verfügung – zum Beispiel durch den Arbeitgeber – steigt auch die Bereitschaft, sich digitales Wissen anzueignen. Das betrifft nicht nur Cybersecurity, sondern sämtliche digitale Wissensbereiche. Mehr als die Hälfte der Österreicher:innen gibt an, bereit zu sein, in die eigene digitale Bildung zu investieren, sofern Staat oder Arbeitgeber finanziell dafür aufkommen. Die Bereitschaft zur Weiterbildung ist demnach - zumindest neuerdings - vorhanden, denn in der Vergangenheit hatten 42 Prozent der Österreicher:innen noch nie eine Schulung oder Weiterbildung in Anspruch genommen, die von Dritten (z. B. dem Arbeitgeber) bezahlt wurde. Aus unserer Sicht ist es daher essenziell, dass Unternehmen eine gute Lernkultur etablieren, entsprechende Angebote schaffen und finanzielle Anreize oder Unterstützung für Betriebe und die:den Einzelne:n zur Verfügung stellen, um digitale Fitness aufzubauen.

Simon Tjoa: Es stellt eine Mammutaufgabe dar, Mitarbeiter:innen regelmäßig für Cybersicherheit zu sensibilisieren und ihnen die Wichtigkeit

FOTO © SABINE KLIMPT

Mag. Ulrike Domany-Funtan, MBA
ist seit 2018 Generalsekretärin des unabhängigen, gemeinnützigen Vereins fit4internet (f4i). Die Standardisierung, Evaluierung, Qualifizierung und Zertifizierung digitaler Skills stehen im Mittelpunkt der Tätigkeiten der Organisation.

dieses Themas nahezubringen. Die Herausforderung besteht darin, Schulungen an die verschiedenen Zielgruppen und die spezifischen Bedürfnisse der Mitarbeiter:innen anzupassen sowie das Interesse am Thema langfristig aufrechtzuerhalten. Besonders wirkungsvoll sind nach meiner Erfahrung Schulungen, die man auch im privaten Umfeld beachten sollte, z. B. Sicherheitsaspekte, die man als Elternteil berücksichtigen sollte.

Welche Zertifizierungen oder Qualifikationen halten Sie für besonders wertvoll im Bereich Cybersecurity?
Ulrike Domany-Funtan: Das lässt sich so pauschal nicht beantworten und hängt immer davon ab, wofür und in welcher Tiefe Cybersecurity-Wissen benötigt wird. Es gibt tolle Angebote, zum Teil auch kostenfrei, die von jeder:jedem in Anspruch genommen werden können. Darüber hinaus gibt es unzählige Angebote auf verschiedenen Levels, die unterschiedliche Zielgruppen bedienen und alle ihre Berechtigung haben.

Simon Tjoa: Es gibt mittlerweile eine Vielzahl von Zertifizierungen in allen Bereichen der Cybersicherheit. Ich persönlich finde, dass viele dieser Zertifizierungen einen wichtigen Beitrag zum lebenslangen Lernen leisten. Ich würde sagen, dass gerade Zertifizierungen und Ausbildungen im GRC-Bereich, der technischen Sicherheitsanalyse z. B. Penetration Testing, digitale Forensik sowie Cyber Defense derzeit stark benötigt werden.

> **Jede Generation muss „cyberfit" sein.**
>
> Ulrike Domany-Funtan

Wie sehen Sie die Zukunft der Aus- und Weiterbildung in Cybersecurity und welche Herausforderungen sehen Sie für die Ausbildung von Cybersecurity-Fachleuten. Welche spezifischen Herausforderungen sehen Sie in Bezug auf die digitale Kompetenz in Österreich?
Ulrike Domany-Funtan: Wir wissen, dass der Bedarf an Weiterbildung im digitalen Bereich auch in den kommenden Jahren steigen wird. Aktuell werden digitale Kompetenzen vor allem informell, also durch Ausprobieren, Learning on the Job, Hilfe von Dritten, YouTube-Videos etc., erworben. Die Analyse der Daten des „Digital Skills Barometer" hat ergeben, dass die formale Bildung ein wichtiger Hebel und Grundlage für die digitale Fitness ist. Aber der Aufbau digitaler Kompetenzen erfolgt dort oft nicht zielgerichtet und strukturiert genug. Cybersecurity, auch in Kombination mit dem Einsatz neuer Technologien (Stichwort KI), bedarf einer fokussierten Aus- und Weiterbildungsstrategie. Und das unabhängig von Alter, Geschlecht, Bildungshintergrund oder Berufsbild.

Aus unserer Sicht kann man auch insbesondere bei der Lehre stärker ansetzen. Lehrberufe ermöglichen eine sehr praxisnahe Auseinandersetzung mit digitalen Werkzeugen und Technologien. Eindeutig ist aber auch, dass wir mehr Cybersecurity-Spezialist:innen in Österreich benötigen, um unsere Betriebe und Infrastrukturen zu schützen. Einschlägige HAKs und HTLs sind hier sicherlich auch ein Schlüssel.

Simon Tjoa: In Zukunft werden wir einer Vielzahl von Herausforderungen gegenüberstehen. Zum einen stellte die rasante Entwicklung neuer Technologien, wie beispielsweise Large Language Models in jüngster Vergangenheit, eine große Herausforderung dar. Darüber hinaus werden die zunehmende Vernetzung und Abhängigkeit von Wirtschaft und Gesellschaft sicherlich schwierig zu meistern sein. Ausbildungen müssen sich daher in der Zukunft wahrscheinlich noch häufiger anpassen, und ich denke, dass die Spezialisierungen zunehmen werden. Eine weitere Herausforderung sehe ich darin, mehr junge Menschen für dieses Thema zu begeistern. Das Interesse für Cybersecurity sollte schon früh geweckt werden. Es ist unabdinglich, Cybersicherheit verstärkt in den Lehrplänen der niedrigeren Schulstufen zu verankern. Digitale Grundbildung ist ein guter erster Schritt, doch setzt diese oft schon zu spät an. Cybersicherheit sollte thematisiert werden, sobald Kinder zum ersten Mal mit der digitalen Welt in Berührung kommen. Danach muss die solide Basis regelmäßig und über verschiedenste (auch spielerische) Ansätze erweitert werden. Kurz gesagt: Die kontinuierliche Weiterbildung muss sich von der Rolle des seltenen Gastes zum stetigen Begleiter wandeln.

Wie trägt fit4internet dazu bei, die digitale Kompetenz in Österreich zu verbessern und wie sehen Sie die Rolle von Hochschulen wie der FH St. Pölten bei der Förderung der Cybersecurity-Ausbildung?
Ulrike Domany-Funtan: fit4internet hat es sich zur Aufgabe gemacht, Interessierten eine kompetente Nutzung digitaler Technologien zu ermöglichen. Wir standardisieren, evaluieren, qualifizieren und zertifizieren auf Basis von EU-Standards. Das ist in Europa einzigartig und wird als Best-Practice-Approach zur Umsetzung des von der Europäischen Kommission empfohlenen Digital Competence Framework umgesetzt. Wir haben Tools entwickelt, die es ermöglichen, die eigenen digitalen Kompetenzen einzuschätzen und Wissenslücken zu identifizieren. Mit dem Dig-CERT haben wir ein Zertifikat für digitales Wissen in Alltag und Beruf etabliert. Wir bieten Unternehmen die Möglichkeit, digitale Kompetenzlücken zu erkennen und geeignete Aus- und Weiterbildungsmaßnahmen abzuleiten. Mit dem „Digital Skills Barometer" werfen wir einen ganzheitlichen Blick auf die digitalen Kompetenzen der Österreicher:innen. Die Etablierung von Spezialausbildungen wie an der FH St. Pölten im Bereich Cybersecurity ist ein weiterer wichtiger Schritt, denn diese vermitteln nicht nur das theoretische Rüstzeug für Studierende, sondern schaffen mit ihrer Praxisnähe und -relevanz unmittelbare Anwendungsmöglichkeiten. Denn bei Kompetenzaufbau geht es um Wissen und konkrete Anwendung. Fachhochschulen in Österreich leisten hier großartige Arbeit.

Simon Tjoa: Initiativen wie fit4internet, welche die digitalen Kompetenzen in Österreich steigern und breite Unterstützung besitzen, sind unerlässlich, um auch in Zukunft wettbewerbsfähig zu bleiben. Die Rolle der Hochschulen in der Cybersecurity-Ausbildung sehe ich als zentral an. Durch spezialisierte Studiengänge bilden Hochschulen neue Fachkräfte in der Cybersicherheit aus, die über breit gefächerte Kompetenzen verfügen, um auch auf neue Herausforderungen reagieren zu können. Weiterbildungsangebote fördern zudem das lebenslange Lernen und vermitteln zusätzliche Fähigkeiten, die am Arbeitsmarkt besonders gefragt sind. Darüber hinaus engagieren sich Hochschulen in der Forschung, um neue Technologien und Methoden zu entwickeln, die die Sicherheit kontinuierlich verbessern.

Warum ist es Ihrer Meinung nach notwendig, zusätzlich zu universitä-

FOTO © PRIVAT

FH-Prof. Mag. Dr. Simon Tjoa leitet das Department Informatik und Sicherheit an der Fachhochschule St. Pölten. Sein Hauptforschungsschwerpunkt liegt auf dem Management der Informationssicherheit, der Cyberresilienz und der Sicherheit Künstlicher Intelligenz.

ren Angeboten spezielle Aus- und Weiterbildungen im Bereich Cybersecurity anzubieten?
Ulrike Domany-Funtan: Der Bedarf an Wissen im Bereich Cybersecurity endet nicht an der (Hoch)Schultüre. Jede:r von uns benötigt ein gewisses Maß an Cybersecurity-Basiswissen, um sich selbstbestimmt und vor allem sicher in der Onlinewelt bewegen zu können. Darüber hinaus geht es dann je nach Berufsweg oder Jobprofil um den Aufbau spezifischer Cybersecurity-Kompetenzen. Es ist wichtig, Aus- und Weiterbildungen auf unterschiedlichen Niveaus für unterschiedliche Bedarfe anzubieten, damit möglichst viele über (zumindest Basis-)Kompetenzen im Bereich Cybersecurity verfügen.

Simon Tjoa: Lebenslanges Lernen ist zentral, um den Herausforderungen der Cybersicherheit begegnen zu können. Obwohl die Hochschulen durch die Studiengänge und Weiterbildungen einen wichtigen Beitrag leisten, ist es nicht möglich, alle Bereiche abzudecken. Daher sind spezielle Aus- und Weiterbildungen neben den universitären Angeboten wichtig.

> **Kontinuierliche Weiterbildung muss sich von der Rolle des seltenen Gastes zum stetigen Begleiter wandeln.**
>
> Simon Tjoa

Welche spezifischen Fähigkeiten und Kenntnisse sollten in einer Cybersecurity-Ausbildung vermittelt werden und wie unterscheiden sich diese zwischen akademischer und nicht-akademischer Ausbildung?
Ulrike Domany-Funtan: Wichtig ist festzuhalten, dass akademische und nicht-akademische Ausbildungen ihren Platz haben. Die eine ist also nicht wichtiger oder besser als die andere. Gerade in der österreichischen Bildungslandschaft sind formale und non-formale Bildungswege wichtige Säulen der Aus- und Weiterbildung und die Vielfalt ist beeindruckend. Was nicht passieren darf ist, dass Bildung auf einem hohen Qualifikationsniveau nur noch in Hochschulen stattfindet. Dann fehlen uns nämlich rasch ausgebildete, qualifizierte Fachkräfte in Bereichen, in denen wir sie dringend und v. a. rasch brauchen. Der „Digital Skills Barometer" zeigt aktuell, dass das digitale Wissen leider abnimmt, je geringer der formale Bildungsabschluss ist. Es ist daher wichtig, auch Angebote für eine gute Aus- und Weiterbildung in der Digitalisierung zu schaffen, die im nicht-akademischen Bereich liegen und in der Breite zugänglich sind – auch zeitlich und örtlich unabhängig, Stichwort Microlearning. Ich denke, dass gerade die praxisorientierte Anwendung, Use Cases, Szenarien/Planspiele etc. in der Cybersecurity-Ausbildung einen hohen Stellenwert haben (müssen).

Simon Tjoa: Es gibt viele Kompetenzmodelle, welche spezielle Fähigkeiten und Kenntnisse aus dem Bereich Cybersicherheit abdecken. Es ist wichtig, auf diesen aufzubauen. Zentral sehe ich hier vor allem organisatorische Aspekte wie Risikomanagement bzw. Sicherheitsmanagement und technische Fähigkeiten rund um das Härten und Testen von Systemen sowie die Bereiche Cyber Defense und Incident Response. Grundsätzlich können und sollten die meisten Disziplinen der IT um wertvolle Sicherheitsaspekte erweitert werden – sei es in der Softwareentwicklung, in der Netzwerktechnik oder in rechtlichen Fragen.

Vom Bodensee zum Neusiedler See

Neun Länder, ein Ziel – wir haben neun Expert:innen aus den den Bundesländern folgende fünf Fragen zum Thema gestellt:

Frage 1: Rückblickend wünschte(n) ich/wir mir/uns, ich/wir hätte(n) in puncto Cybersicherheit viel früher damit begonnen, …

Frage 2: Momentan sehe(n) ich/wir die größte Gefahr durch Cybercrime …

Frage 3: In Zukunft wird Cybersicherheit nicht mehr möglich sein ohne …

Frage 4: Haben Sie ein Vorbild – eine Person, eine Organisation oder ein Land – für den richtigen Umgang mit Cyberbedrohungen?

Frage 5: Wie sind Sie in das Thema Cybersecurity hineingekommen? War es Zufall, Notwendigkeit oder Passion?

FOTO © CAROLA EUGSTER

Dr. Bettina Thurnher
Director Information Security, Zumtobel Group

1: Abhängig von der Branche ist der Entwicklungsstand zur Informationssicherheit unterschiedlich. Dienstleistungsunternehmen und Telekommunikationsunternehmen haben tendenziell einen hohen Reifegrad.

2: Unzureichende IT-Ressourcen, mangelnde Mitarbeiter-Awareness, Angriffe auf Drittparteien und fehlende Security-Architektur sind wesentliche Herausforderungen in der Cybersecurity.

3: … ein umfassendes Partner- und Know-how-Netzwerk für Verteidigung und Abwehr sowie den maßvollen Einsatz von KI zur Stärkung der Defense.

4: Kirsten Davies - Global CISO von Unilever. Sie ist eine versierte und anerkannte Vordenkerin bei der Entwicklung und Umsetzung von Digital-Trust-Programmen.

5: Zufall. Früher dachte ich, dass es bei Informationssicherheit nur um Richtlinien geht. Dann aber erkannte ich, dass Cybersecurity aus den Faktoren Mensch, Technik und Prozessen besteht und somit ein unglaublich spannender Bereich ist.

FOTO © PRIVAT

Mattia Salamanca Orrego
Koordinator für Datenschutz und IT-Sicherheit in der Gruppe IT, Plansee Group Functions

1: Eine dedizierte Abteilung für Informationssicherheit, getrennt von der IT einzurichten. Dies hätte eine Kostenreduktion, eine Verbesserung der IT-Ressourcennutzung und eine frühere Verankerung in der Unternehmenskultur mit sich gebracht.

2: … in Ransomwareangriffen, die mit Künstlicher Intelligenz betrieben werden, in der Bewältigung von Schwachstellen in der Lieferkette sowie im zunehmenden Risiko von Datenverstößen aufgrund von Remote-Arbeit und IoT-Geräten.

3: … fortschrittliche Künstliche Intelligenz und maschinelles Lernen, um Cyberangriffe in Echtzeit zu erkennen und zu verhindern. Außerdem sind gemeinsame Anstrengungen (präventiv und reaktiv) aller relevanten Stakeholder notwendig sowie eine verstärkte nationale und europäische Zusammenarbeit.

4: Alyssa Miller - bekannt für ihre Expertise im Bereich Cybersicherheit, ihr Engagement für Vielfalt und Inklusion in der Branche sowie ihre Bemühungen, andere in diesem Bereich zu bilden und zu stärken.

5: Ich wurde von der einzigartigen Position der Cybersicherheit an der Schnittstelle von Recht, Wirtschaft, Informationsmanagement und Informationstechnologie angezogen. Dank meines vielfältigen Hintergrunds konnte ich einen Mehrwert schaffen, indem ich die Lücke zwischen Gesetzgebern, Geschäftsleiter:innen und technischem Personal schließe.

FOTO © PRIVAT

Mag. Jimmy Heschl
Global Head of Digital Security, Red Bull

1: ... mich nicht auf Good-Practice oder Compliance-Themen zu konzentrieren, sondern auf die Governance. Sie ist nachhaltiger als ein ISMS oder operative, technische Themen. Also als erstes die Verantwortung des Unternehmens zu sehen und diese dann herunterzubrechen.

2: ... im Mangel an echten Expert:innen. Viele fokussieren auf Buzzwords und unwichtige (Compliance-)Aufgaben. Die Basishygiene wie aktuellste Systeme, „g'scheite" Kennwörter bzw. MFA und Back-ups und fehlen dann.

3: ... Qualität über den gesamten Lebenszyklus von IT-Services. Security muss intrinsischer Bestandteil und erwartbarer Qualitätsanspruch an jeden IT-Dienst sein und eine selbstverständliche Leistung – nie ein aufpreispflichtiger Premiumdienst.

4: Ja, Ghandi. Da schwebt der Geist von Sinn, Nachhaltigkeit und Resilienz mit und keine Angst oder Stress. Ich denke lieber an Cyberpeace als an Cybercrime und möchte genau jene Maßnahmen priorisieren, die den Frieden erhalten.

5: Durch Fragen meiner ehemaligen Kunden. Alle hatten die gleichen Fragen und gemeinsam haben wir die Antworten und Ansätze erarbeitet. Über die Zeit wurde Security zu meinem Fokusthema und ist eine echte Passion.

FOTO © HELGE BAUER

LAbg. Herbert Gaggl
Bürgermeister, Marktgemeinde Moosburg

1: Das Bewusstsein für die Notwendigkeit von Maßnahmen zur Stärkung der Cybersicherheit von Gemeinden in Kärnten und in ganz Österreich ist schon lange da. Es fehlt manchmal an den Mitteln und am Know-how zur richtigen Umsetzung der notwendigen Schritte.

2: ... in Angriffen auf die digitalen Services, die innovative Gemeinden für ihre Bevölkerung bereitstellen.

3: ... die Menschen, die die Technologien und IT-Systeme beherrschen und ein hohes Maß an Bewusstsein für Risiken und Potenziale dieser Technologien haben.

4: In unserem Verein „Zukunftsorte Österreich" befassen wir uns als Zusammenschluss innovativer Gemeinden in ganz Österreich mit den Chancen und Risiken der Digitalisierung. Da ist Cybersicherheit ein Fundament, auf dem wir unsere Digitalisierungszukunft aufbauen.
Ich denke, dass der Polizei- und Militärapparat hier sehr gut aufgestellt sind. Und natürlich auch die Rechenzentren des Bundes und der Bundesländer.

5: Es war und ist jedenfalls eine Notwendigkeit. Diese wurde durch die Erfahrungen aus der Corona-Zeit und die damit verbundenen Änderungen für Gemeinden, Behörden und die arbeitende Bevölkerung wesentlich verstärkt.
Cybersecurity ist in ein Thema, seitdem ohne Internet nichts mehr geht. Es war immer eine Notwendigkeit, seine Systeme zu schützen. Aber natürlich hat sich das Bewusstsein in dieser Zeit der Cyberkriminalität noch einmal verstärkt.

FOTO © BERNHARD RAAB

Dr. Markus Gratzer
Generalsekretär, Österreichische Hoteliervereinigung

1: Als Pionier im Bereiche IT & Tourismus haben wir uns schon früh mit den Gefahren beschäftigt und mittlerweile ein umfangreiches Netzwerk und Know-how aufgebaut, welches wir an unsere Mitglieder weitergeben. Diese Weitsicht hat unsere Position noch weiter gestärkt.

2: ... in den immer raffinierteren Formen von Angriffen sowie in der Abhängigkeit von externen Infrastrukturen, wie Online-Buchungsplattformen, auf die man als Hotelier keinen Einfluss hat. Da setzen wir mit gezielten Maßnahmen und Aufklärung bzw. auch mit Schulungen an.

3: ... stetiger Weiterbildung und dem Einsatz modernster Sicherheitstools. Unser Ziel ist es, ein Bewusstsein für die Wichtigkeit dieser Instrumente bei unseren Mitgliedern zu schaffen und ihnen mit Partnern die entsprechenden Tools zur Verfügung zu stellen.

4: Viele Betriebe setzen Cybersicherheit bereits vorbildlich um. Ein Trend, dem wir in der Steiermark natürlich auch folgen und dem wir auf unseren Plattformen eine Bühne in Form von Best Practices, Schulungen und konkreten Lösungen bieten.

5: Unser Engagement für Cybersecurity entstand aus der Notwendigkeit, die steirische Hotellerie zukunftssicher zu machen. Das persönliche Interesse an IT-Themen innerhalb unseres Teams verstärkt unser Bestreben.

FOTO © PRIVAT

DI Hubert Wetschnig
CEO, HABAU Group

1: Wir sind überzeugt, dass wir zeitgerecht begonnen haben und uns im Sinne einer Kosten-Nutzen-Betrachtung auf einem guten technischen Stand befinden.

2: ... E-Mail-Verkehr.

3: ... Unterstützung durch KI.

4: -

5: Nicht zuletzt im Zuge des Ausbruches der Corona-Epidemie und damit des großen Wachstums im Bereich des digitalen Arbeitens, aber auch durch das Bekanntwerden von Cyberangriffen auf andere Unternehmen haben wir die Notwendigkeit erkannt, hier wesentlich mehr zu investieren.

FOTO © ANNA RAUCHENBERGER

Mag. Dr. Claudia Süssenbacher M.B.L.
Geschäftsleitung, Raiffeisen-Holding NÖ-Wien / Mitglied des Vorstandes, RLB NÖ-Wien

1: … das Thema als einen Ausbildungsschwerpunkt in Bildungseinrichtungen zu integrieren. Eine frühzeitige Aufklärung bereitet Kinder auf Risiken vor und schafft Bewusstsein für Datensicherheit. Dies kann das Interesse an IT-Berufen wecken und die Verfügbarkeit von IT-Fachkräften sichern.

2: … in Ransomwareangriffen jeglicher Art. Aufgrund der potenziell schwerwiegenden Auswirkungen ist es von großer Bedeutung, für die eigene Cybersicherheit zu sorgen und umfassende Sicherheitsmaßnahmen zu implementieren.

3: … kontinuierliche Innovation und Weiterentwicklung von Sicherheitstechnologien in Kombination mit achtsamem Handeln jedes Einzelnen im Unternehmen.

4: Skandinavische Länder haben einen umfassenden Ansatz im Bereich Cybersicherheit. Sie verfügen über robuste digitale Infrastrukturen, die kontinuierlich verbessert und gesichert werden. Außerdem gibt es eine enge Zusammenarbeit zwischen Regierung, Industrie und Bildungseinrichtungen, um umfassende Strategien zu entwickeln.

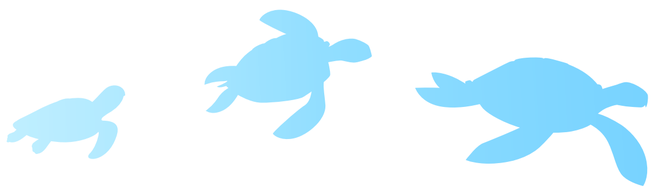
5: Um die Trennung zwischen operativer Durchführung und Kontrollfunktion zu verbessern, wurde der Bereich „Information Security & Resilience“ dem Risikomanagement zugeordnet. Durch die Notwendigkeit dieser organisatorischen Weiterentwicklung habe auch ich mich intensiver mit dem Thema beschäftigt.

FOTO © PRIVAT

Heidelinde Rameder
CISO, Borealis

1: Es ist notwendig Informationssicherheit nicht mehr auf rein technischer, sondern auf strategischer und persönlicher Ebene zu betrachten, und aufgrund unseres zunehmend digitalisierten Lebens unerlässlich für unseren Schutz.

2: Generell sehe ich die größten Bedrohungen für Unternehmen in den Bereichen Ransomware und staatlich gestützten Angriffen zur Sabotage von Infrastruktur und Wirtschaftsspionage. Die Etablierung und breite Nutzung von KI im Mainstream und die unglaublich schnellen technologischen Entwicklungsschritte stellen uns vor Herausforderungen.



3: Cybersicherheit muss Priorität haben, mit Unterstützung des Topmanagements. Zukünftig sind Verifizierungsmaßnahmen und Verschlüsselungstechnologien unerlässlich, um Fälschungen zu erkennen. Jeder trägt Verantwortung und muss IT-Sicherheit verstehen, da Menschen oft die erste Verteidigung gegen Cyberangriffe sind.

4: Ich bin überzeugt, dass es vielfältige Perspektiven und Lösungsansätze braucht, um die Herausforderungen in der Informationssicherheit zu meistern. Daher sind all die unterschiedlichsten Typen von Menschen, die zusammenkommen & sich engagieren, um gemeinsam Lösungen zu entwickeln und bereitwillig andere fördern und ihr Wissen teilen, meine Vorbilder.

5: Meine Neugier und mein Wirtschaftsinformatikstudium führten mich in das Feld der IT und Informationssicherheit. Ich begann meine Karriere als klassische „White-Hat Hackerin“ mit IT-Sicherheitsüberprüfungen – ein unheimlich spannender Bereich. Das vielfältige Karrierepotenzial, verbunden mit meinem Wunsch nach finanzieller Unabhängigkeit, motivierten mich zusätzlich.

FOTO © PRIVAT

Johannes Schmidt, MSc
CISO, Burgenland Energie

1: … einen systematischen Ansatz zur nachhaltigen Implementierung der Cybersecurity über den gesamten Lebenszyklus unserer gesellschaftlichen und geschäftlichen Aktivitäten umzusetzen und dabei das Management stärker einzubinden.

2: … in der unterschätzten Abhängigkeit unseres täglichen Lebens von digitalen Infrastrukturen und in der unzureichenden Anpassung von Sicherheitsmaßnahmen. Angreifer:innen werden raffinierter und verfügen über immer mehr Mittel, die Vorsorge bleibt leider oft auf der Strecke.

3: … eine ganzheitliche und integrative Herangehensweise, die auch den erhöhten Einsatz von Automatisierung im Schwachstellenmanagement, Verschlüsselung und Datenschutz, sowie Cyberhygiene und Bewusstseinsbildung bereits in der schulischen Ausbildung umfasst.

4: Ich bewundere Personen bzw. Organisationen, die Ihre Cybersecurity-Aufwände und -Aktivitäten nicht mehr nur in den Aufbau entsprechender Abwehrmaßnahmen, sondern verstärkt in ihre Resilienz zur Absicherung des Fortbestands ihrer persönlichen Existenz bzw. Ihres Geschäftsmodells investieren. Die Bedeutung der nachhaltigen Fähigkeit zur Rückkehr in den Ursprungszustand hat, wie in der Zunahme der erfolgreichen Cyberangriffe ersichtlich wird, entsprechend zugenommen.

5: Die Interaktion von Menschen und Maschinen hat mich stets beeindruckt und die rasche Notwendigkeit zur Anpassung unserer Gesellschaft aufgrund neuer Technologien hat meine Leidenschaft geweckt, diese Veränderungen cybersicher zu gestalten.

Umfragemethodik

Die vorliegende KPMG Studie „Cybersecurity in Österreich“ beschäftigt sich mit der Frage, wie österreichische Unternehmen den neuen Herausforderungen der Cyberkriminalität im Jahr 2024 begegnen und welche Cybersecurity-Maßnahmen getroffen werden.

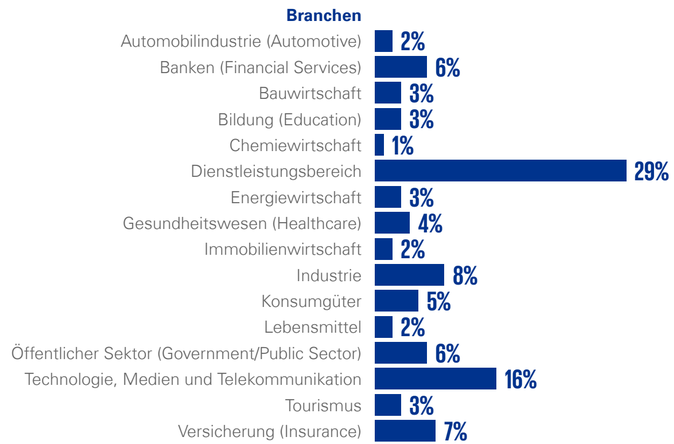
Die Umfrage: Cybersecurity im Überblick
Die Umfrage zur Studie wurde im Februar und März 2024 von KPMG unter 1.158 österreichischen Unternehmen durchgeführt. Die Teilnehmer:innen setzten sich aus Vertreter:innen kleiner und mittlerer Unternehmen sowie Großunternehmen aus den Branchen Automobilindustrie, Banken, Bauwirtschaft, Bildung, Chemiewirtschaft, Dienstleistungsbereich, Energiewirtschaft, Gesundheitswesen, Immobilienwirtschaft, Industrie, Konsumgüter, Lebensmittel, Öffentlicher Sektor, Technologie, Telekommunikation, Tourismus, und Versicherungswirtschaft zusammen.

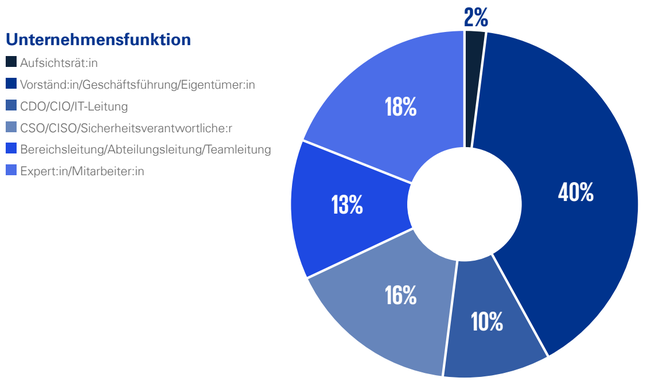
Die Auswertung: Stimmungsbild in Österreich
Jede:r Teilnehmer:in erhielt, ihrer:seiner Funktion im Unternehmen entsprechend, einen Online-Fragebogen mit spezifischen Fragen. Darüber hinaus wurden die quantitativen Fragen (Likert-Skala) um qualitative Aspekte erweitert, um den Teilnehmer:innen die Möglichkeit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

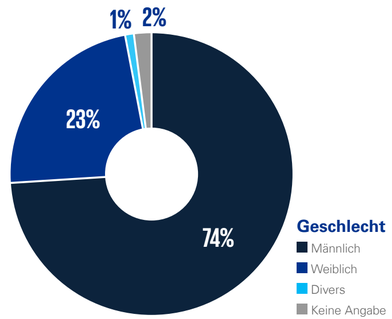
Für die Auswertung wurde zwischen Innensicht/Leitungsebene (Expert:innen, Bereichsleiter:innen, CSO etc.) und Außensicht/Steuerungsebene (Vorständ:innen, Eigentümer:innen, Aufsichtsrät:innen) unterschieden. Die Ergebnisse wurden von einem KPMG Cybersecurity-Expert:innenteam aus dem Bereich IT Advisory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

Die Vertiefung: Im Gespräch mit Expert:innen
In persönlichen Interviews standen außerdem 25 Wirtschaftsvertreter:innen, Vertreter:innen der öffentlichen Verwaltung und Cybersecurity-Expert:innen zum Thema Rede und Antwort. Sie sprachen mit uns 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

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

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

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

Druck:
Ferdinand Berger & Söhne GmbH

ESGeht um unsere Verantwortung: Wir setzen im gesamten Produktionsprozess unserer Publikationen auf Nachhaltigkeit, Umweltschonung und Energieeffizienz.

Die Antworten in den Interviews spiegeln die persönliche Sichtweise der Interviewpartner:innen wider und können durchaus von der jeweiligen Ressortmeinung zu den Fragen abweichend sein. Sind Unternehmen und keine Einzelpersonen gemeint, wird kein Gender-Doppelpunkt gesetzt, beispielsweise beim Begriff Kunde.


KPMG