KPMG

Cybersecurity in Österreich

Sicherheitsforum
Digitale Wirtschaft
Österreich

Mai 2025

kpmg.at/cyber

10 JAHRE CYBER SECURITY STUDIE

Was haben Schildkröten mit Cybersecurity zu tun?

Die Schildkröte ist bereits seit 2022 unser Wegbegleiter durch die Tiefen der Cybersecurity. Und kaum ist ein besseres Tier für diese Aufgabe vorstellbar, als sie – haben ihre Geschichte und Lebensweise doch zahlreiche Gemeinsamkeiten mit den vielfältigen Facetten der Cybersicherheit.

Schildkröten sind Urgesteine, mit denen Weisheit und Beständigkeit assoziiert werden – zwei Eigenschaften, die es unbedingt braucht, um durch die rauen Gewässer der Cyberwelt zu navigieren. Unsere Schutzmaßnahmen müssen genauso robust und anpassungsfähig sein wie sie.

Der Lebensraum der Schildkröte hat sich stark verändert und ist auch weiterhin im Wandel. Für dieses langlebige Tier wird es immer schwieriger, zu überleben. Sie musste sich abermals auf neue Bedrohungen einstellen. Parallel dazu kommen nahezu täglich neue Cyberbedrohungen auf

Unternehmen zu, angetrieben durch die rasanten Entwicklungen der Digitalisierung. Auch wir müssen dafür Sorge tragen, dass uns die veränderten Bedingungen nicht zum Verhängnis werden. Denn am Ende des Tages bleiben uns zwei Möglichkeiten: abtauchen und uns am Meeresgrund verstecken oder weiterschwimmen. So wie die Schildkröte, die zäh und anpassungsfähig ist und viel Ausdauer beweist. Nehmen wir uns ihre Resilienz zum Vorbild.

Um unserer Inspiration Dank zu verleihen und auf das Artensterben aufmerksam zu machen, übernimmt KPMG die Patenschaft für die Europäischen Sumpfschildkröten im Tiergarten Schönbrunn. Diese Schildkrötenart ist die einzige in Österreich heimische und ist bedroht.[1]

Mit der Patenschaft schließt sich auch unser 10-Jahres-Kreislauf – unsere erste Cyberstudienpräsentation fand 2016 in der ORANG.erie im Tiergarten Schönbrunn statt. Bleiben Sie gespannt, welche Wegbegleiter wir Ihnen auf unseren Reisen in den nächsten Jahren noch vorstellen dürfen.

[1] https://www.zoovienna.at/tiere/reptilien/europaische-sumpfschildkrote/ und https://www.zoovienna.at/natur-und-artenschutz/sumpfschildkroete/, abgerufen am: 02.05.2025.

Um unserer Inspiration Dank zu verleihen und auf das Artensterben aufmerksam zu machen, übernimmt KPMG die Patenschaft für die Europäischen Sumpfschildkröten im Tiergarten Schönbrunn.

Mariana Herrloss, Marlene Zauner, Robert Lamprecht (v. l. n. r.)

Vertrauen im Fadenkreuz

Die Umfrageergebnisse unserer diesjährigen Studie machen eines klar: Geopolitische Konflikte sind in Österreich angekommen. Das lesen wir deutlich aus den Zahlen im Vergleich zum Vorjahr. Die aktuell stattfindenden Umbrüche in puncto Diplomatie und Zusammenarbeit führen zu massiven, weltweiten Unruhen. Doch welche Auswirkungen hat das für heimische Unternehmen? Wie haben sich in diesem Zusammenhang Advanced Persistent Threats verändert? Und welche wirtschaftlichen Implikationen haben staatliche Bedrohungen in Verbindung mit Desinformationskampagnen?

Konflikte erkennen
Geopolitische Auseinandersetzungen werden zunehmend auch auf unternehmerischer Ebene, im Informationsraum sowie im Cyberspace ausgetragen. Während wir konventionelle Formen der Kriegsführung sehen und spüren können, nehmen wir Konflikte im Cyberraum nicht unmittelbar wahr. Ihre Auswirkungen sind allerdings real. Im Cyberraum wird getestet, wie anfällig wir sind. Noch gibt es dabei keine menschlichen Schäden.

Doch nicht nur Unternehmen stehen im Visier dieser neuen Art der Konfliktaustragung. Auch die Zivilgesellschaft wird durch Desinformationskampagnen und Manipulationsversuche auf eine harte Probe gestellt. Dabei spielt Künstliche Intelligenz eine wesentliche Rolle. Durch sie sind immer realistischere und schwer zu erkennende Deepfakes im Umlauf. Gezielte Desinformationskampagnen beeinflussen so unser gesellschaftliches Narrativ und untergraben unser Vertrauen in die Wirklichkeit und ineinander. Vertrauen ist essenziell für eine gute Zusammenarbeit zwischen Unternehmen, öffentlichen Einrichtungen, kritischen Infrastrukturen und der Zivilgesellschaft. Vertrauen wird zum raren Gut.

Bewusstsein schaffen
Um Vertrauen zu sichern, braucht es einen gemeinsamen Dialog. Wir müssen unser aktuelles Cybersecurity-Lagebild kennen. Das schaffen wir nur dann, wenn wir über Cybersicherheit sprechen.

Cyberkonflikte sind unsichtbar, aber ihre Auswirkungen sind real und tiefgreifend.

Resilienz entsteht durch die enge Zusammenarbeit von Unternehmen und Gesellschaft.

Mit dieser Studie möchten wir Jahr für Jahr einen Beitrag leisten, um das Lagebild heimischer Unternehmen an die Oberfläche zu bringen. Denn nur durch den gemeinsamen Austausch können wir Betroffenheit herstellen und Bewusstsein erzeugen. Und nur so können wir Maßnahmen umsetzen, die uns resilienter machen.

Dialog fördern
Zum zehnten Mal in Folge zeichnen wir heuer in Kooperation mit dem Sicherheitsforum Digitale Wirtschaft des Kompetenzzentrum Sicheres Österreich (KSÖ) ein Cybersecurity-Lagebild für Österreich. Ein großer Dank gebührt den 1.391 heimischen Unternehmen, die ihre Erfahrungen mit Cyberkriminalität und -sicherheit mit uns geteilt haben, so wie all den Expert:innen, die uns in Interviews und hinter den Kulissen mit Antworten und Anregungen zur Verfügung gestanden sind. Sie alle helfen uns dabei, Bewusstsein zu schaffen.

Vertrauen in der digitalen Welt erfordert gemeinsame Anstrengungen.

Wir wünschen Ihnen eine spannende Lektüre unserer Jubiläumsausgabe und würden uns freuen, auch mit Ihnen in einen Dialog zur Cybersecurity in Österreich treten zu dürfen. Denn nur gemeinsam sind und bleiben wir resilient!

Robert Lamprecht, Andreas Tomek,
Michael Schirmbrand

Robert Lamprecht
KPMG Partner

Andreas Tomek
KPMG Partner

Michael Schirmbrand
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)

Kompass für die Zukunft

Zehn Jahre gemeinsame Analyse, zehn Jahre intensiver Austausch, zehn Jahre wachsendes Bewusstsein: Die KPMG & KSÖ Studie zur Cybersecurity in Österreich ist längst mehr als ein jährlicher Bericht – sie ist ein verlässlicher Kompass für Politik, Wirtschaft und Gesellschaft geworden.

Was einst als Spezialthema begann, hat sich bis heute zu einem zentralen Faktor für unsere wirtschaftliche Resilienz und staatliche Handlungsfähigkeit entwickelt. Digitalisierung eröffnet große Chancen – bringt jedoch auch neue, komplexe Risiken mit sich. Unsere Jubiläumsausgabe nimmt diese Realität ernst: Sie analysiert aktuelle Bedrohungslagen, blickt auf ein Jahrzehnt der Entwicklung zurück und zeigt klare Handlungserfordernisse für die Zukunft auf.

Technologischer Fortschritt – ob durch Künstliche Intelligenz, globale Vernetzung oder neue digitale Geschäftsmodelle – eröffnet vielfältige Chancen. Gleichzeitig entstehen daraus neue Risiken. Wer Cyberrisiken versteht, wer Entwicklungen einordnet und daraus die richtigen Schlüsse zieht, kann aktiv gestalten – statt nur zu reagieren.

Gerade die Sicherheitslücken in Lieferketten und der verantwortungsvolle Umgang mit neuen Technologien – etwa Künstlicher Intelligenz – stehen im Zentrum der Analyse. Dabei wird deutlich: Technik allein reicht nicht. Es braucht Menschen, die Verantwortung übernehmen, Risiken verstehen und aktiv an Lösungen mitwirken.

Als Kompetenzzentrum Sicheres Österreich ist es unser Anspruch, Plattform und aktiver Mitgestalter zugleich zu sein. Wir bringen Menschen zusammen – aus Behörden, Wirtschaft und Wissenschaft – und gestalten so eine Sicherheitskultur, die auf Kooperation, Transparenz und gemeinsames Handeln baut. Denn wir sind heute mehr denn je davon überzeugt, dass wir durch Kooperation bessere Lösungen für Österreichs Sicherheit erreichen können.

FOTO © EVA_KELETY

Mag.
Michael Höllerer
Präsident des KSÖ

Diese Studie ist Ausdruck dieses Anspruchs – und ein starkes Zeichen dafür, dass Cybersicherheit kein Endzustand ist, sondern ein stetiger Prozess, an dem wir alle gemeinsam arbeiten wollen. Lassen Sie uns diesen Weg gemeinsam weitergehen.

Michael Höllerer
Präsident KSÖ

Inhaltsverzeichnis

Eine neue Realität

Seit einem Jahrzehnt analysieren wir systematisch das Cybersecurity-Lagebild in Österreich. Die nun vorliegende zehnte Ausgabe unserer Studie „Cybersecurity in Österreich“ markiert einen Wendepunkt.

Lagen die Schwerpunkte in den vergangenen Jahren auf den ersten beiden Säulen der Informationssicherheit – Vertraulichkeit (Confidentiality) und Verfügbarkeit (Availability) –, zeigt sich im Jahr 2025 ein neues, drängendes Problem: Die dritte Säule – Integrität (Integrity) von Daten, Systemen und Prozessen – wird zum zentralen Sicherheitsfaktor.

In der zehnten Ausgabe unserer Studie nehmen wir Sie mit auf eine Reise durch diese neue Realität. Wir beleuchten die aktuelle Cybersecurity-Lage in Österreich, die durch die geopolitischen Konflikte immer mehr herausgefordert wird. Wir zeigen die zentrale Rolle des Menschen in der Cyberabwehr auf, analysieren die Ambivalenz von KI und blicken gemeinsam in die Zukunft – mit einem hoffnungsvollen Ausblick, der zeigt, dass wir die Herausforderungen meistern können. Wenn wir sie erkennen und anpacken.

Vertrauen: Die Währung der Cybersicherheit

Wir durchleben in der Cybersecurity gerade eine Zeitenwende: In der Vergangenheit waren Vertraulichkeit und Verfügbarkeit die großen Themen, mit denen wir uns alle beschäftigt haben – jetzt geht es um Integrität. Betrachten wir die Entwicklungen der letzten beiden Jahre, ist das wenig überraschend, sondern eine logische Konsequenz der zunehmenden Komplexität und Vernetzung unserer digitalen Welt. KI hat diese Entwicklung in einer unglaublichen Art und Weise beschleunigt. Die Beschleunigung war so rasant, dass wir noch immer von ihr fasziniert sind, wiewohl wir die Risiken und Gefahren nur sehr langsam begreifen. Während Angriffe auf die Vertraulichkeit und Verfügbarkeit von Informationen und Systemen oftmals schnell erkannt und behoben werden können, sind Angriffe auf die Integrität subtiler – und potenziell verheerender. Befeuert werden diese Angriffe durch Desinformationskampagnen, Deepfakes und Social Engineering sowie KI-Halluzinationen von Ergebnissen und Trainingsdaten.

Vertrauen ist die Währung der Cybersecurity der Zukunft. Hierbei muss man das zwischenmenschliche Vertrauen von gesellschaftlichem Vertrauen unterscheiden, welches auch unser Vertrauen in Systeme beinhaltet. Cyberangriffe sind nicht mehr bloß „einfache“ Einbrüche wie Phishingangriffe oder Denial-of-Service-Attacken. Sie zielen darauf ab, Informationen zu manipulieren, Prozesse zu beeinträchtigen und Vertrauen zu untergraben – mit weitreichenden Konsequenzen für Gesellschaft, Wirtschaft und Staat.

Verschwimmende Grenzen

In der aktuellen Bedrohungslandschaft erleben wir hoch entwickelte Angriffsformen, die sich in einem zunehmend hybriden Konfliktfeld entfalten. Geopolitische Spannungen weiten sich auf den Cyberraum aus und befeuern die Lage zusätzlich. Die Grenzen zwischen konventioneller Kriegsführung und der Auseinandersetzung im digitalen Raum verschwimmen immer mehr. Das stellt die Cybersicherheit vor neue Herausforderungen.

Gleichzeitig verändert sich das Sicherheitsbild grundlegend durch die rasante Entwicklung von Künstlicher Intelligenz. Nicht nur ist KI ein Hilfsmittel in der Cyberabwehr, sondern sie ist auch zu einer mächtigen Waffe der Angreifer:innen geworden. Ihnen eröffnet KI neue Möglichkeiten, insbesondere durch Angriffe auf die Integrität von Trainingsdaten und KI-Modellen. Zusätzlich birgt der zunehmende (und teils unüberlegte) Einsatz von KI-Anwendungen in Unternehmen und kritischen Infrastrukturen Risiken, deren Folgen für uns noch nicht in vollem Ausmaß abschätzbar sind.

Cyberkriminelle nutzen die neuen Technologien für ihre Zwecke und experimentieren mit immer mehr Möglichkeiten und Einsatzgebieten – während wir versuchen, ihnen mit denselben KI-Tools hinterherzukommen. Wir müssen aus der Geschichte lernen (Stichwort Enigma und der Versuch Großbritanniens, in Bletchley Park die Verschlüsselung zu brechen) und uns einmal mehr vor Augen führen, dass wir unsere digitale Zukunft nur sichern können, wenn wir innovativ sind und zusammenarbeiten – denn das nicht zu tun und stehen zu bleiben, ist keine Option.

> **Vertrauen ist die Währung der Cybersicherheit.**

Lagebild 2025

Österreich befindet sich 2025 in einem von den geopolitischen Konflikten geprägten, dynamischen und herausfordernden Umfeld. Digitalisierung und KI durchdringen sämtliche Bereiche – von der Verwaltung über die Industrie und kritische Infrastruktur bis hin zum privaten Raum. Das eröffnet eine noch nie dagewesene Menge an neuen Chancen, erhöht aber auch drastisch die Angriffsfläche für Bedrohungen.

Cyberkriminelle agieren mit einer Genauigkeit und Geschwindigkeit, die an Hochfrequenzhandel an der Börse erinnert: Schwachstellen werden in Echtzeit ausgenutzt, Lieferketten als Einfallstor missbraucht, und gezielte Manipulationen an Daten und Systemen sind zum Alltag geworden.

Denn die Bedrohungen kommen aus zahlreichen und vielfältigen Richtungen: kriminelle Netzwerke, staatliche bzw. staatlich unterstützte Akteur:innen, Hacktivist:innen sowie automatisierte, KI-gestützte Angriffe. Die Cyberattacken von heute sind komplex, zielgerichtet und oft Teil eines hybriden Konflikts, der klassische militärische Auseinandersetzungen mit Cyberangriffen und Desinformationskampagnen verbindet.

Zusätzlich dürfen wir auch nicht den Blick darauf verlieren, was noch auf uns zukommt: die potenziellen Gefahren durch Quantencomputing. Noch glauben wir nicht, dass diese Technologie ein Problem darstellt. Aber wenn jetzt verschlüsselte Daten gestohlen werden, haben wir später ein Problem – von „Harvest now, decrypt later“ hin zu „Collect now, exploit later“.

Geopolitische Konflikte und Cyberkrieg

Die geopolitischen Konflikte unserer Zeit spiegeln sich unmittelbar im Cyberraum wider. Cybercrime ist das neue Mittel der Wahl, um politische, wirtschaftliche und gesellschaftliche Ziele zu verfolgen. Desinformationskampagnen wirken dabei wie ein digitales Gift, das langsam, aber spürbar das Vertrauen in Institutionen, Me-

dien und demokratische Prozesse zersetzt. Die Grenzen zwischen Wahrheit und Manipulation verschwimmen immer mehr.

Angriffe auf Unternehmen haben nicht mehr nur Datendiebstahl oder Erpressung durch Ransomware zum Ziel, sondern ganze Geschäftsprozesse sollen manipuliert werden. Kritische Infrastrukturen werden gezielt attackiert, um Unsicherheit auszulösen und gesellschaftliche Prozesse zu stören. Der Druck steigt, nicht nur die eigenen Systeme, sondern auch die der Partner und Dienstleister abzusichern.

Die Lieferkette als Achillesferse

Die Lieferkette ist ein heikler Punkt geworden. Sie gleicht einer komplexen Abfolge aus Dominosteinen, und ein einziger Fehltritt bringt das gesamte Konstrukt ins Wanken. Eine Cyberattacke auf nur ein einziges Glied in der Kette kann weitreichende und verheerende Konsequenzen für ganze Branchen oder sogar Volkswirtschaften haben.

Die europäische Regulatorik wie NIS-2, DORA, Cyber Resilience Act und RKE-Richtlinie zwingt heimische Unternehmen dazu, die Lieferkettensicherheit nicht länger als Randthematik zu behandeln, sondern als zentralen Bestandteil der eigenen Cyberresilienz. Wer hier versagt, riskiert nicht nur wirtschaftliche Schäden für das eigene Unternehmen, sondern auch Imageschäden sowie Vertrauensverlust.

> **Cybersicherheit ist eine gesellschaftliche Notwendigkeit.**

Mensch sticht Technik

Inmitten all dieser Umbrüche bleibt der Mensch der entscheidende Faktor für die Cyberabwehr. Man könnte es als Ironie bezeichnen, dass ausgerechnet der Mensch, der oft als Einfallstor für Cyberangriffe gilt, es ist, der gleichzeitig eine Barriere gegen die immer ausgeklügelteren Angriffe darstellt. Arbeiten Algorithmen und Sicherheitssysteme mit mathematischer Präzision, sind es am Ende doch Intuition, kritisches Denken und menschliche Erfahrungswerte, die den Unterschied machen.

Gerade auch deshalb sind Security-Awareness-Trainings, die in vielen Unternehmen noch immer als lästige Pflicht betrachtet werden, in Wahrheit das Rückgrat einer funktionierenden Cyberabwehr. Sie fördern ein Bewusstsein der Mitarbeitenden für Risiken, das sich nicht durch Software ersetzen lässt. Denn Realität ist: Kein noch so ausgefeiltes technisches System kann uns davor bewahren, dass ein unachtsamer Klick auf einen manipulierten Link oder eine gut getarnte Phishingmail zum Einfallstor für Cyberkriminelle wird. Aus der Praxis geht hervor, dass es heute nur mehr weniger als 72 Minuten von der Phishingmail bis zum erfolgreichen Zugriff auf die IT-Systeme des Unternehmens benötigt. Das Zusammenspiel zwischen Mitarbeitenden und Technik ist für Unternehmen also entscheidender denn je, um eine resiliente Sicherheitsarchitektur zu entwerfen.

Ambivalenz der KI

Künstliche Intelligenz ist das funkelnde Versprechen der digitalen Zukunft – und zugleich ihre größte Gefahr. KI kann mittlerweile automatisiert Angriffe erkennen, große Datenmengen analysieren und bei der Entscheidungsfindung helfen. Doch das hat seinen Preis. KI kann manipuliert, ausgetrickst und für Zwecke missbraucht werden, die weit über unser Vorstellungsvermögen hinausgehen. Aus aktuellen Erfahrungsberichten sehen wir, dass KI von staatlichen Akteuren mittlerweile großflächig eingesetzt wird: von simplen Hilfsdiensten in der Vorbereitung auf Angriffe über Phishingattacken bis hin zu Social Engineering.

Auch die gesellschaftliche Debatte um KI ist von Ambivalenz geprägt. Der Hoffnung auf eine bessere, effizientere und sicherere Zukunft steht die Sorge vor Kontroll- und Vertrauensverlusten gegenüber. KI-Systeme müssen deshalb transparent, nachvollziehbar und sicher sein. Ohne diese Grundvoraussetzungen spielt KI trojanisches Pferd der Cyberkriminalität und manipuliert nicht nur unsere Systeme, sondern auch unsere Wahrnehmung der Realität.

Umbrüche und Ausblicke

Die Grenzen zwischen der digitalen und unserer analogen Welt verschwimmen immer mehr – und mit ihnen unsere traditionellen Konzepte von (Cyber-)Sicherheit. Die Ausgestaltung von Cybersecurity wird zu einer gesellschaftlichen Mammutaufgabe. Innovation und Sicherheit dürfen keinen Widerspruch darstellen, sondern sind zwei Seiten derselben Medaille. Die Herausforderungen, die in den nächsten Jahren noch auf uns alle zukommen werden, lassen sich nicht durch Technik allein lösen. Es benötigt dafür eine intensive Zusammenarbeit zwischen Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft. Nur so kann Österreich seine digitale Souveränität sicherstellen. Nur so kann Österreich die Chancen der digitalen Zukunft nutzen, ohne dabei die Risiken zu vernachlässigen. Und noch etwas sehen wir ganz klar: In Zeiten geopolitischer Umwälzungen muss Europa autonom werden und darf sich nicht mehr auf andere verlassen. Europa muss ein eigenes Profil im Cyberraum entwickeln.

Und trotz alledem wird es uns nicht erspart bleiben, auch als Gesellschaft zu lernen, mit und in diesen unsicheren Zeiten zu leben. Hundertprozentige Sicherheit ist in unserer vernetzten Welt nicht möglich. Das Beste, was wir tun können, ist Risiken erkennen, bewerten und diese angemessen steuern. Denn Resilienz ist die wichtigste Grundvoraussetzung für die Cybersecurity-Strategien von heimischen Unternehmen.

Der Cybersecurity-Marathon

Unsere Studie widmet sich auch heuer wieder all diesen Herausforderungen im Detail. Sie zeigt auf, wie Österreich im Jahr 2025 aufgestellt ist, welche Rolle der Mensch im Zusammenspiel mit Technik einnimmt, wie KI die Sicherheitslage beeinflusst und welche Weichen für die Zukunft gestellt werden müssen. Wir zeichnen damit erneut ein umfassendes Bild der Cybersecurity-Landschaft in Österreich und zeigen Wege auf, wie Österreich seine digitale Resilienz im Spannungsfeld zwischen Innovation, Sicherheit und gesellschaftlicher Verantwortung stärken kann.

Cybersecurity ist wie ein Marathon – auf einem Laufband, das ständig schneller wird. Wer stehen bleibt, fällt runter. Wer meint, schon am Ziel zu sein, hat den Wettlauf nicht verstanden. Die Zukunft gehört jenen, die bereit sind, sich ständig weiterzuentwickeln, dazuzulernen und zu investieren – in Technologie, Organisation, aber vor allem auch in die Menschen.

Robert Lamprecht
KPMG Partner

> **KI muss liefern, weil das Momentum eindeutig auf der Seite der Angreifer:innen liegt.**

Ein Jahr danach

Im Jahr 2024 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?“***

Haben sich unsere Erwartungen erfüllt? Welche Meinungen äußern unsere Interviewpartner:innen heute?

FOTO © PRIVAT

Stéphane Duguin
CEO CyberPeace Institute

Reflecting on the past year, we have indeed made notable progress on a tactical level. A significant achievement has been the launch of our cyberpeacetracer, which aims to empower and protect civil society by providing accessible tools to trace and understand cyber threats. This initiative has been instrumental in raising awareness and enhancing the capabilities of those at risk of cyberattacks. However, it is with some regret that I must note the geopolitical landscape has not seen much improvement. The accountability of criminal actors in cyberspace remains a major challenge. Despite our continuous efforts, the lack of cooperation and consensus among international stakeholders has hindered substantial progress in holding these actors responsible for their actions.

FOTO © MAG. KERSTIN HEHENBERGER

Ing.in Mag.a Dr.in Sylvia Mayer, MA
Stellvertretende Direktorin DSN (Direktion Staatsschutz und Nachrichtendienst)

Eine unserer wesentlichsten Aufgaben im Verfassungsschutz ist weiterhin die Bekämpfung des islamistischen Extremismus und Terrorismus als schwerwiegende Bedrohung für die öffentliche Sicherheit in Österreich. In meinem Interview im Jahr 2024 hatte ich mir gewünscht, dass wir als Sicherheitsbehörde über die technischen und rechtlichen Befugnisse verfügen, um diese Aufgabe bestmöglich erfüllen zu können. Mittlerweile gab es zu einer ganz wesentlichen dieser Befugnisse, nämlich der Überwachung von verschlüsselter Messenger-Kommunikation im Rahmen der Gefährderüberwachung, einen veröffentlichten Begutachtungsentwurf, ebenso steht die Maßnahme als Vorhaben im aktuellen Regierungsprogramm. Dementsprechend bin ich optimistisch, dass diese bald umgesetzt sein wird.

FOTO © BKA

Carsten Meywirth
Leiter der Abteilung Cybercrime im Bundeskriminalamt in Deutschland

Wir können auf ein erfolgreiches Jahr zurückblicken, mit vielen Ermittlungserfolgen und Fortschritten bei der Bekämpfung von Cybercrime. Gemeinsam mit unseren internationalen Partnern haben wir beispielsweise mit unserer Operation Endgame die Verbreitung von Ransomware zeitweise eingedämmt. Dennoch bleibt die Lage ernst. Unsere Erfolge sind ein Lichtblick, aber mit Sicherheit nicht schon das Ende des Tunnels. Cybercrime entwickelt sich ständig weiter. Damit wir Schritt halten können, brauchen wir bessere Rahmenbedingungen: zum Beispiel Cyberabwehrbefugnisse, längere Speicherfristen für IP-Adressen und mehr Ressourcen für die aufwendigen Ermittlungen.

FOTO © BMLV/D. PHOTO OY

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

Die Entwicklung im letzten Jahr hat gezeigt, dass hybride Bedrohungen vor allem aus dem Cyberraum zugenommen haben. Die Implementierung neuer Technologien, wie etwa KI-gestützte Lösungen, zur frühzeitigen Erkennung und Abwehr von Cyberangriffen oder Drohneneinsätzen muss weiter intensiviert werden. Die Bevölkerung muss weiterhin besser über hybride Bedrohungen aufgeklärt werden, um sie widerstandsfähiger/resilienter gegen Desinformation und Propaganda zu machen. Weiters ist eine stärkere finanzielle und personelle Unterstützung für die Sicherung kritischer Infrastrukturen wie Energieversorgung und Kommunikationsnetze vonnöten.

FOTO © PRIVAT

Florian Schütz
Direktor Bundesamt für Cybersicherheit in der Schweiz

Vor einem Jahr habe ich gesagt, ich würde mir wünschen, mehr Transparenz geschaffen zu haben. Diesem Ziel sind wir mit der Einführung der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen einen großen Schritt näher gekommen. Die Meldepflicht ist am 1. April 2025 in Kraft getreten und wird zu mehr Transparenz führen. Denn unter anderem ermöglicht die Meldepflicht dem Bundesamt für Cybersicherheit (BACS) eine noch bessere Einschätzung der Bedrohungslage. Dies wiederum wird zu einer noch früheren Erkennung von Cybergefahren führen, damit potenzielle Opfer besser informiert und damit geschützt werden können.

Key Findings 2025

sagen, dass Österreich nicht gut darauf vorbereitet ist, auf schwerwiegende Cyberangriffe gegen die **kritische Infrastruktur** zu reagieren.

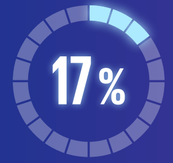
Bei jedem dritten Unternehmen waren **Lieferanten oder Dienstleister Opfer** von Cyberangriffen, die wesentliche Auswirkungen auf das eigene Unternehmen hatten.

würden bevorzugt Security-Lösungen **von österreichischen Unternehmen** einsetzen – eine Zunahme um 23 % gegenüber dem Vorjahr.

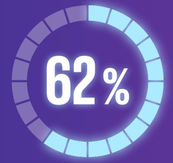
Mehr als jeder 4. Angriff ist auf **staatlich unterstützte Akteur:innen** zurückzuführen.

Jeder 7. Cyberangriff in Österreich ist **erfolgreich.**

Jeder 10. **Social-Engineering-Versuch** nutzt bereits Deepfake für Sprach- und Videonachrichten.



sagen, dass KI die Cybersicherheit verbessert hat. **KI hat also noch nicht die erhofften Fortschritte gebracht.**



konnten Cyberangriffe mithilfe der **eigenen Mitarbeitenden** identifizieren – vor technischen Lösungen und Systemen.

01

10 Jahre im Rückblick

Zu Beginn der zehnjährigen Jubiläumsausgabe unserer Studie blicken wir zurück, bis ins Jahr 2016, wo alles mit einer Idee unter der Federführung von Michael Schirmbrand, Gert Weidinger und Robert Lamprecht begann. Seit Ausgabe zwei unterstützt auch Andreas Tomek das Team tatkräftig.

Begeben Sie sich mit uns auf eine Reise: die Entwicklung der Cybersecurity in Österreich und die unserer Studie.
Eines können wir schon vorweg verraten: Das Umfeld und die Entwicklung sind durchaus volatil gewesen. Genau diese Volatilität bilden wir auch in folgendem Rückblick ab. Diesen haben wir in drei Phasen unterteilt:
Phase eins beschäftigt sich mit den Anfangsjahren 2016 bis 2017, getreu dem Motto „Cybersecurity, das unbekannte Wesen, findet seinen Weg auf die Agenda".
In der zweiten Phase behandeln wir die Jahre 2018 bis 2020. Wir sehen, dass Cybersecurity immer mehr ins Gespräch kommt. Eine stetig wachsende Gruppe beschäftigt sich mit dem Thema. In dieser Phase lernen wir, mit mehr Details umzugehen und die unterschiedlichen Facetten von Cybersicherheit im Allgemeinen und Cyberangriffen im Speziellen einzuordnen.
In Phase drei, den Jahren 2021 bis 2025, erleben wir, dass Cybersicherheit essenziell wird. Wir sind im geopolitischen Spiel der Kräfte angekommen, Cyberangriffe werden zunehmend existenzbedrohender und auch die Reaktionen der Unternehmen werden immer professioneller.

Kommen Sie also mit auf unsere Zeitreise, auf der uns auch das ein oder andere Tier begegnen wird. Denn auch unsere Studiensujets haben sich den Umständen angepasst.

Cybersecurity kommt auf die Agenda (2016–2017)
Im Jahr 2016 haben wir mit unserer Studie erstmals versucht, ein Lagebild für Österreich zu erstellen. Die ersten Flugversuche haben begonnen. Aufgrund der tatkräftigen Unterstützung vieler Personen, die an unserer Umfrage teilgenommen und in Interviews wertvolle Einblicke mit uns geteilt haben, war es möglich, diese Studie für Österreich zu verfassen.

Studie 2016 (die Eule)
Zeitraum: 11–12/2015
94 Teilnehmende

Die Studie aus dem Jahr 2016 macht klar, dass Cyberkriminalität eine ernsthafte Bedrohung darstellt und viele Unternehmen noch nicht ausreichend vorbereitet sind, um sich effektiv vor dieser zu schützen.

Bewusstsein für Cyberkriminalität: 92 Prozent der Unternehmen glauben, dass Cybersecurity kein Hype, sondern Alltag ist. Das Bewusstsein für die Bedrohungen durch Cyberkriminalität ist bereits weit verbreitet. Dennoch besteht erheblicher Handlungsbedarf, um dieses Bewusstsein in konkrete Schutzmaßnahmen umzuwandeln.

Häufigkeit von Cyberangriffen: 49 Prozent der Unternehmen waren bereits Opfer eines Cyberangriffs. Diese Zahl verdeutlicht die Allgegenwärtigkeit von Cyberkriminalität und wie wichtig es für Unternehmen ist, sich proaktiv gegen Angriffe zu wappnen.

Unzureichende Schutzmaßnahmen: 71 Prozent der befragten Unternehmen finden, dass Cyberangriffe kaum bis gar nicht verhindert werden können. Das unterstreicht die Dringlichkeit, effektive Sicherheitsstrategien zu entwickeln, die über reine technische Lösungen hinausgehen und auch organisatorische und menschliche Faktoren berücksichtigen.

Mangel an strategischer Integration: 63 Prozent der Unternehmen haben Cybersecurity in der IT-Abteilung angesiedelt. Cybersecurity wird also noch nicht oft als strategisches Thema auf Führungsebene behandelt. Um langfristig gegen Cyberkriminalität gewappnet zu sein, muss Cybersecurity als Chef:innensache betrachtet und in die Unternehmensstrategie integriert werden.

Fehlende Messinstrumente: 60 Prozent der Unternehmen können die Auswirkungen von Cyberangriffen nicht messen. Ohne geeignete Messinstrumente ist es allerdings schwierig, die Effektivität von Sicherheitsmaßnahmen zu beurteilen und damit auch kontinuierlich zu verbessern.

Studie 2017 (die Qualle)
Zeitraum: 4–5/2017
236 Teilnehmende

Die zweite Studie verdeutlicht die weitverbreitete Bedrohung durch Cyberangriffe auf heimische Unternehmen. Es zeigt sich, dass Industrieunternehmen besonders anfällig sind. Erstmals sehen wir, dass Cybersecurity zunehmend als strategisches Thema auf Führungsebene behandelt wird. Das stellt einen Wandel in der Unternehmenspolitik dar. Auch Awareness-Trainings sind ein zentraler Aspekt, um menschliche Schwachstellen zu adressieren und die Widerstandsfähigkeit gegen Cyberkriminalität zu erhöhen.

Hohe Anzahl von Cyberangriffen: 72 Prozent der befragten Unternehmen waren in den letzten 12 Monaten Opfer von Cyberangriffen.

Industrieunternehmen besonders betroffen: Industrieunternehmen sind ausgesprochen anfällig für Cyberangriffe. 87 Prozent der Unternehmen in dieser Branche wurden Opfer von Cybercrime. Die direkte Auswirkung auf Produktionsabläufe macht sie zu einem lukrativen Ziel für Cyberkriminelle.

Mangel an Cyber Threat Intelligence: 52 Prozent der Unternehmen verfügen über zu wenig Hintergrundwissen, um die Chancen von Cyber Threat Intelligence zu verstehen. Es bedarf besserer Informationsbeschaffung und -nutzung, um Bedrohungen effektiv zu begegnen.

Awareness als Schlüssel zur Sicherheit: 87 Prozent der Unternehmen betonen die Bedeutung von Awareness-Trainings zur internen Bewältigung von Cyberrisiken. Die Sensibilisierung der Mitarbeiter:innen ist entscheidend, denn viele Angriffe zielen auf den Faktor Mensch ab.

Cybersecurity als strategisches Thema: Obwohl 68 Prozent der Führungsebenen Cybersecurity als technische Angelegenheit betrachten, wird das Thema mittlerweile in 74 Prozent der Unternehmen auf oberster Ebene diskutiert. Wir erleben einen Wandel hin zu einer strategischen Betrachtung von Cybersecurity als Teil des Risikomanagements.

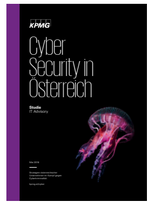
Was wir aus den ersten beiden Studien gelernt haben

Die Cybersicherheitslage in Österreich erfordert sowohl strategische als auch technische Maßnahmen, um die wachsende Bedrohung durch Cyberkriminalität zu bewältigen. Unternehmen stehen vor wirtschaftlichen Risiken, darunter finanzielle Verluste und Reputationsschäden. Diese werden durch mangelhafte Schutzmaßnahmen und fehlende strategische Integration von Cybersecurity in die Unternehmenspolitik verstärkt.

Industrieunternehmen sind besonders gefährdet, denn ihre komplexen Produktionsabläufe sind attraktive Ziele für Angreifer:innen. Die Sicherung dieser Abläufe ist entscheidend, um wirtschaftliche Einbußen zu verhindern bzw. zu verringern. Während Cybersecurity zunehmend als strategisches Thema auf Führungsebene behandelt wird, fehlt oftmals noch die umfassende Einbindung in die Unternehmensstrategie.

Cyber Threat Intelligence und Awareness-Trainings müssen weiter ausgebaut werden. Da viele Angriffe auf menschliche Schwachstellen abzielen, sind eine bessere Informationsbeschaffung sowie Mitarbeiter:innensensibilisierung zwingend nötig. Unternehmen müssen zudem geeignete Messinstrumente implementieren.

Cybersecurity kommt ins Gespräch (2018–2020)



Studie 2018 (die Qualle)
Zeitraum: 4–5/2018
269 Teilnehmende

Die Studie aus dem Jahr 2018 zeigt, dass österreichische Unternehmen zwar zunehmend die strategische Bedeutung von Cybersecurity erkennen, jedoch trotzdem oft noch als rein technisches Thema betrachten. Unternehmen müssen darüber hinaus in die Ausbildung und Sensibilisierung ihrer Mitarbeiter:innen investieren, um deren Cyberkompetenz zu stärken und die Infrastruktur besser zu schützen.

Cyberangriffe sind weit verbreitet: 61 Prozent der österreichischen Unternehmen waren in den letzten 12 Monaten Opfer einer Cyberattacke.

Menschliche Schwachstellen sind ein Hauptziel: 60 Prozent der Angriffe zielen auf die „Schwachstelle Mensch" ab, was die Bedeutung von Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter:innen unterstreicht.

Cybersecurity wird zunehmend als strategisches Thema erkannt: 79 Prozent der Unternehmen diskutieren Cybersecurity-Themen auf oberster Unternehmensebene und sehen diese Themen somit als strategische Priorität. Dennoch betrachten 70 Prozent der Geschäftsführung Cybersecurity immer noch als technische Angelegenheit.

Mangelnde Meldung von Cybervorfällen: Trotz der hohen Anzahl von Angriffen melden 45 Prozent der Unternehmen cyberkriminelle Vorfälle nicht. Wir sehen ein erhebliches Problem in puncto Transparenz und Informationsaustausch. Das behindert auch die Entwicklung effektiver Abwehrstrategien.

Steigende Investitionen in Cybersecurity: 52 Prozent der Unternehmen prognostizieren einen Anstieg des Cybersecurity-Budgets. Diese Investitionen sind entscheidend, um den Schutz vor immer ausgeklügelteren Cyberattacken zu gewährleisten.

Studie 2019 (die Qualle)
Zeitraum: 2–3/2019
342 Teilnehmende

Die Studie 2019 hat gezeigt, dass Cyberkriminalität weiterhin eine bedeutende Bedrohung für Unternehmen darstellt. Die Notwendigkeit von Cyber Resilience, um nicht nur Angriffe abzuwehren, sondern auch die Geschäftskontinuität zu sichern, rückt verstärkt ins Zentrum der Aufmerksamkeit. Auch die Zusammenarbeit mit Drittparteien stellt ein unterschätztes Risiko dar, welches systematisch bewertet und gemindert werden muss. Nur so kann die Sicherheit der gesamten Wertschöpfungskette gewährleistet werden. Die Wichtigkeit von Bewusstseinsbildung und der strategischen Integration von Cybersicherheit in Unternehmensprozesse wird hervorgehoben, um den Herausforderungen von Digitalisierung und Industrie 4.0 effektiv begegnen zu können.

Zunahme von Cyberangriffen: Die Zahl der von Cyberattacken betroffenen österreichischen Unternehmen steigt weiter auf 66 Prozent.

Häufige Angriffsarten: Phishing und Malware sind die häufigsten Angriffsarten, mit denen knapp die Hälfte der befragten Unternehmen konfrontiert wurde (jeweils 47 Prozent). Diese

Angriffsarten nutzen oft die Gutgläubigkeit und Neugierde der Mitarbeiter:innen aus, was die Bedeutung von Schulungen und Bewusstseinsbildung weiter unterstreicht.

Finanzielle Auswirkungen: Rund 41 Prozent der Unternehmen erlitten aufgrund eines Cyberangriffs finanziellen Schaden. Die finanziellen Auswirkungen variieren, wobei bei großen Unternehmen 38 Prozent einen Schaden von mehr als EUR 50.000 erlitten. Mit unzureichender Cybersicherheit sind auch wirtschaftliche Risiken verbunden.

Unterschätztes Risiko durch Drittparteien: Nur 7 Prozent der Unternehmen glauben, dass ihre Lieferanten ausreichende Sicherheitsmaßnahmen treffen. Durch mangelnde Sicherheitsvorkehrungen bei Drittparteien entsteht ein erhebliches Risiko für die Unternehmen. Sie müssen diese Risiken systematisch bewerten und kontrollieren.

Bewusstseinsbildung und strategische Integration: 65 Prozent der Unternehmen haben laut eigener Angabe ausreichendes Cybersecurity-Wissen, jedoch gibt es noch erheblichen Aufholbedarf bei der Integration von Cybersecurity in die Unternehmensprozesse. Das ist entscheidend, um den Herausforderungen der Digitalisierung und der Industrie 4.0 effektiv begegnen zu können.

Studie 2020 (die Qualle)
Zeitraum: 2–3/2020
652 Teilnehmende

Unsere fünfte Studie zeigt, dass Unternehmen ihre digitalen Infrastrukturen gegen immer raffiniertere Cyberangriffe schützen müssen. Trotz der gestiegenen Bedrohungslage herrscht oft ein falsches Sicherheitsgefühl. Aber auch mangelhaftes Vertrauen in die Sicherheitsvorkehrungen von Drittanbietern ist bei den Unternehmen vorhanden. Hervorgehoben wird die Bedeutung von Cyber Resilience – Unternehmen müssen trotz widriger Umstände ihre Leistung kontinuierlich erbringen. Gefordert wird auch eine stärkere Zusammenarbeit zwischen staatlichen und privaten Akteur:innen.

Steigende Bedrohung durch Cyberangriffe: 57 Prozent der österreichischen Unternehmen waren in den letzten zwölf Monaten Opfer einer Cyberattacke, wobei die Hälfte dieser Unternehmen mehrfach angegriffen wurde.

Falsches Sicherheitsgefühl: Ein Drittel der Unternehmen glaubt, dass sie nur ein bis vier Wochen benötigen, um eine:n Angreifer:in aus ihrem Netzwerk zu entfernen. Ein Viertel ist sogar davon überzeugt, es in zwei bis sechs Tagen zu schaffen. Bei den Unternehmen scheint ein falsches Sicherheitsgefühl vorzuliegen.

Mangelndes Vertrauen in Drittanbieter: Nur 8 Prozent der Unternehmen vertrauen den Sicherheitsmaßnahmen ihrer Lieferanten und Dienstleister. Sicherheitsvorkehrungen in der Lieferkette müssen verbessert werden.

Investitionen in Cybersecurity: Das Cybersecurity-Budget ist mittlerweile auf durchschnittlich rund drei bis fünf Prozent des IT-Budgets gestiegen, wobei 27 Prozent der Unternehmen über kein dezidiertes Budget für Cybersecurity verfügen.

Bedeutung von Cyber Resilience: Mehr als die Hälfte der befragten Unternehmen hat technische und organisatorische Maßnahmen in Vorbereitung auf einen Cyberangriff definiert. Das veranschaulicht die Bedeutung von Cyber Resilience.

Was wir aus den Studien 3 bis 5 gelernt haben
Österreichische Unternehmen stehen vor einer zunehmend gefährlichen Cyberlandschaft. Cyberangriffe häufen sich und stellen erhebliche (wirtschaftliche) Risiken dar. Nur durch die Inklusion sowohl technologischer als auch menschlicher Aspekte in die Sicherheitsstrategie kann die Geschäftskontinuität gewährleistet werden.

Phishing und Malware sind häufige Angriffsarten und unterstreichen die Notwendigkeit von Schulungen und Bewusstseinsbildung für die Mitarbeiter:innen.

Obwohl Investitionen in Cybersicherheit steigen, fehlt es vielen Unternehmen an klaren finanziellen Ressourcen. Auch mangelt es am Vertrauen in die Sicherheitsvorkehrungen von Drittanbietern. Die Bedeutung von Cyber Resilience wird zunehmend erkannt.

Cybersecurity muss als strategische Priorität in die Unternehmensprozesse integriert werden, um den Herausforderungen der Digitalisierung und der Industrie 4.0 effektiv zu begegnen.

Cybersecurity ist essenziell (2021–2025)

Studie 2021 (der Taucher)
Zeitraum: 1–2/2021
417 Teilnehmende

Unsere Studie aus dem Jahr 2021 zeigt, dass die Digitalisierung durch die Pandemie beschleunigt wurde. Das hat die Verwundbarkeit von Unternehmen gegenüber Cyberangriffen erhöht. Traditionelle Sicherheitskonzepte werden zunehmend obsolet, ein proaktiver Ansatz ist erforderlich, um Cyberattacken zu verhindern. Die Zusammenarbeit zwischen Unternehmen und staatlichen Institutionen sowie die Ausbildung von Fachkräften sind entscheidend für die Bewältigung der zahlreichen Herausforderungen.

Zunahme von Cyberangriffen während der Pandemie: 60 Prozent der befragten Unternehmen waren in den letzten 12 Monaten Opfer eines Cyberangriffs. Besonders betroffen sind große Unternehmen, von denen 54 Prozent einen Anstieg der Angriffe während der Pandemie registrierten. Durch die verstärkte Nutzung digitaler Technologien und Homeoffice-Lösungen werden Unternehmen verwundbarer.

Bedrohung durch staatlich unterstützte Angriffe: Ein Viertel der großen Unternehmen hat Angriffe durch staatliche oder staatlich unterstützte Akteur:innen erlebt. Diese Angriffe stellen eine ernsthafte Bedrohung dar, da sie oft hochprofessionell und schwer abzuwehren sind. Verstärkte Sicherheitsmaßnahmen und internationale Zusammenarbeit werden dringend benötigt.

Wunsch nach staatlicher Unterstützung: 78 Prozent der befragten Unternehmen wünschen sich eine stärkere Unterstützung durch den Staat beim Thema Cybersecurity. Bei den Unternehmen wächst die Besorgnis über ihre Fähigkeit, sich allein gegen die komplexen Bedrohungen zu verteidigen.

Investitionen in Cybersicherheit: 49 Prozent der Unternehmen wären bereit, in den Schutz vor Cryptolocker und Ransomware zu investieren, würde Geld keine Rolle spielen. Das unterstreicht die Notwendigkeit von Budgeterhöhungen, damit heimische Unternehmen effektive Schutzmaßnahmen implementieren können.

Kommunikation und Transparenz bei Cyberangriffen: Nur 10 Prozent der befragten Unternehmen gehen im Fall einer Cyberattacke proaktiv an die Öffentlichkeit. Bei großen Unternehmen sind es 35 Prozent. Gründe könnten Angst vor Image-

schäden oder auch Vertrauensverlust sein. Eine strategische Kommunikation ist hier entscheidend, um das Vertrauen der Stakeholder:innen zu erhalten.

Studie 2022
(die Schildkröte)
Zeitraum: 1–2/2022
550 Teilnehmende

Die Studie verdeutlicht die zunehmende Bedrohung durch Cyberangriffe, die sowohl von staatlich unterstützten Akteur:innen als auch von kriminellen Gruppen ausgehen. Sie betont die Wichtigkeit einer umfassenden Cyberresilienzstrategie für Unternehmen. Digitalisierung und geopolitische Spannungen erweitern die Angriffsflächen. Unternehmen müssen verstärkt in Managementthemen und die Ausbildung von IT-Expert:innen investieren, um diese neuen Herausforderungen zu meistern. Menschliches Versagen ist oftmals die Ursache für Sicherheitsprobleme, die eigenen Mitarbeiter:innen können aber gleichzeitig auch wertvolle Schutzmechanismen sein – die menschliche Komponente ist beim Thema Cybersecurity essenziell.

Zunahme von Cyberangriffen: 20 Prozent der befragten Unternehmen wurden in den letzten 12 Monaten Opfer eines Cyberangriffs, der zu Schäden führte.

Bedeutung staatlich unterstützter Cyberangriffe: 52 Prozent der Unternehmen berichten, dass Cyberangriffe durch staatlich unterstützte Akteur:innen für sie an Bedeutung gewonnen haben. Das unterstreicht die geopolitischen Spannungen und die Rolle von staatlichen Akteur:innen im Zusammenhang mit Cyberbedrohungen. Es zwingt Unternehmen dazu, ihre Sicherheitsstrategien entsprechend anzupassen.

Herausforderungen bei der Rekrutierung von IT-Expert:innen: 40 Prozent der Unternehmen haben Schwierigkeiten beim Rekrutieren von IT-Expert:innen. Es herrscht Fachkräftemangel im Bereich Cybersicherheit. Für Unternehmen ist es jedoch wesentlich, in die Ausbildung und Rekrutierung von qualifizierten Talenten zu investieren, um den steigenden Cybersecurity-Anforderungen zu begegnen.

Finanzieller Schaden durch Cyberkriminelle: 67 Prozent der Unternehmen erleiden finanziellen Schaden durch Cyberkriminelle. Die wirtschaftlichen Auswirkungen von Cyberangriffen sind real.

Investitionen in Cybersecurity-Budgets: 69 Prozent der Unternehmen haben ihr Cybersecurity-Budget deutlich erhöht.

Studie 2023
(die Schildkröte)
Zeitraum: 2–3/2023
903 Teilnehmende

Cyberangriffe haben in Österreich weiterhin stark zugenommen, insbesondere durch geopolitische Konflikte. Cybersecurity ist nicht nur eine technische Herausforderung, sondern auch eine gesellschaftliche Verantwortung und erfordert eine verstärkte Zusammenarbeit zwischen Unternehmen und öffentlichen Stellen. Um mehr Menschen für den Cybersecurity-Bereich zu begeistern und den Fachkräftemangel in den Griff zu bekommen, sollte die Vielfalt der Berufsfelder stärker kommuniziert werden.

Zunahme von Cyberangriffen: Cyberangriffe haben in den letzten 12 Monaten um 201 Prozent zugenommen. Das ist vor allem auf geopolitische Konflikte zurückzuführen, die eine neue Welle von Angriffen ausgelöst haben.

Finanzieller Schaden durch Cyberangriffe: Etwa 12 Prozent der Unternehmen erlitten einen finanziellen Schaden von mehr als EUR 1 Mio. durch Cyberangriffe.

Bedeutung von Business Continuity Management: Für 44 Prozent der befragten Unternehmen hat Business Continuity Management in den letzten zwölf Monaten an Bedeutung zugenommen. Unternehmen erkennen, wie wichtig es ist, ihre Geschäftstätigkeiten auch nach einem Angriff sicherzustellen.

Fachkräftemangel in der Cybersecurity: 43 Prozent der befragten Unternehmen benötigen durchschnittlich vier bis sechs Monate, um IT-Expert:innen einzustellen. Unternehmen müssen neue Wege finden, um qualifizierte Mitarbeiter:innen für sich zu gewinnen.

Rolle der Unternehmensleitung in der Cybersicherheit: 65 Prozent der Befragten stimmen der Aussage zu, dass die Unternehmensleitung Informationssicherheit nicht als einen möglichen Wettbewerbsvorteil betrachtet. Hier mangelt es also noch an der strategischen Einbindung der Cybersicherheit in die Unternehmensführung. Das kann die Effektivität der Sicherheitsmaßnahmen beeinträchtigen.

Studie 2024
(die Schildkröte)
Zeitraum: 2–3/2024
1158 Teilnehmende

Unternehmen sind mit komplexeren und gezielteren Cyberangriffen konfrontiert, wobei Social Engineering und Desinformationskampagnen in diesem Jahr besonders hervorstechen. Die Unsicherheit der Unternehmen ist groß, denn die Angreifer:innen werden immer raffinierter und die technischen Voraussetzungen für Cyberangriffe verbessern sich kontinuierlich. Ständige Weiterbildung und Anpassung der Sicherheitsstrategien sind unumgänglich, um den digitalen Gefahren effektiv zu begegnen.

Zunahme von Cyberangriffen: Jeder sechste Cyberangriff gegen ein Unternehmen war in den letzten 12 Monaten erfolgreich. Das stellt eine Steigerung gegenüber dem Vorjahr dar, als jeder zehnte Angriff erfolgreich war.

Bedeutung von Social Engineering und Desinformation: Social Engineering und Desinformationskampagnen sind für heimische Unternehmen besonders gefährlich. Sie haben in den letzten 12 Monaten den höchsten Zuwachs erfahren. Desinformation ist sogar um drei Plätze nach oben geklettert. Diese Angriffe zielen direkt auf den Menschen ab und erfordern folglich auch die verstärkte Sensibilisierung und Schulung der Mitarbeiter:innen.

Rückgang von Ransomware-Angriffen: Ransomware-Angriffe sind um 27 Prozent zurückgegangen. Dennoch hat jedes dritte Unternehmen mindestens einmal eine Lösegeldforderung im Zusammenhang mit einem Ransomware-Angriff bezahlt. Die Bedrohung muss also trotz Rückgang weiterhin ernst genommen werden.

Herausforderungen durch Künstliche Intelligenz: Die Nutzung von Künstlicher Intelligenz birgt sowohl Chancen als auch Risiken. 65 Prozent der Unternehmen sehen KI als Chance, während 22 Prozent der Unternehmen den KI-Einsatz als irrelevant betrachten. Klare Regeln sind notwendig, um die Vorteile zu maximieren und die Risiken zu minimieren.

Psychische Belastung durch Cyberangriffe: Die psychischen Auswirkungen von Cybersicherheitsvorfällen sind erheblich. Stress und Angst sind hier die dominanten Folgen für die Betroffenen. 63 Prozent der Befragten haben diese Auswirkungen erlebt. Deshalb ist es wichtig, dass Unternehmen nicht nur technische, sondern auch menschliche Faktoren in ihrer Cybersicherheitsstrategie berücksichtigen.

Was wir aus den Studien 6 bis 9 gelernt haben
In den betrachteten fünf Jahren hat sich die Cybersicherheitslandschaft in Österreich stark verändert. Die Digitalisierung und geopolitische Spannungen haben zu einer Zunahme und Komplexität der Cyberangriffe geführt. Unternehmen sind oftmals gezielten Angriffen ausgesetzt, die sowohl technische als auch menschliche Schwachstellen ausnutzen. Das geschieht insbesondere durch Social Engineering und Desinformationskampagnen.

Die Angriffe haben auch wirtschaftliche Auswirkungen (sowohl direkte finanzielle Verluste als auch indirekte Schäden durch Vertrauensverlust). Unternehmen haben als Antwort darauf ihre Sicherheitsbudgets erhöht. Der Fachkräftemangel bleibt allerdings eine große Herausforderung.

Entscheidend ist auch die Rolle, die die Unternehmensleitung einnimmt. Eine strategische Einbindung von Cybersicherheit als Wettbewerbsvorteil fehlt oftmals noch. Die psychischen Belastungen durch Cyberangriffe, die in diesem Jahr erstmals in unserer Studie untersucht wurden, sind ein wesentlicher Aspekt, der in Sicherheitsstrategien von Unternehmen berücksichtigt werden muss.

Die Zahlen der letzten 9 Jahre im Detail
Unsere Analyse der Cybersecurity-Studien von 2016 bis 2024 zeigt mehrere interessante Trends und Entwicklungen, die für die heimischen Unternehmen von entscheidender Bedeutung sind. Die Daten wurden in zwei Zeiträume unterteilt: 2016 bis 2020 und 2021 bis 2024. So können spezifische Entwicklungen und Veränderungen besser verstanden werden. Diese Unterteilung ermöglicht auch eine detaillierte Betrachtung der Fortschritte und Herausforderungen über die Jahre.

Topthemen 2016 bis 2020

Opfer von Cyberangriffen: In den Jahren 2016 bis 2020 schwankte die Anzahl jener Unternehmen, die Opfer von Cyberangriffen wurden, zwischen 49 Prozent und 66 Prozent. Die hohen Zahlen verdeutlichen, dass Unternehmen sehr anfällig für Cyberbedrohungen waren und möglicherweise nicht über ausreichende Schutzmaßnahmen verfügt haben.

Phishing: Phishingangriffe waren ein konstantes Risiko mit einem Anstieg von 25 Prozent im Jahr 2016 auf 47 Prozent im Jahr 2019. Phishing ist eine von Angreifer:innen bevorzugte Methode, da es relativ einfach durchzuführen ist und oft auf menschliche Schwächen abzielt. Unternehmen müssen verstärkt in Schulungen und Awareness-Programme investieren, um ihre Mitarbeiter:innen dahingehend zu sensibilisieren.

Malware und Ransomware: Die Bedrohung durch Malware und Ransomware blieb hoch, mit einem Anstieg von 26 Prozent im Jahr 2016 auf 29 Prozent im Jahr 2019. Diese Angriffe führten oft zu erheblichen finanziellen Schäden und Betriebsunterbrechungen. Unternehmen müssen in fortschrittliche Erkennungs- und Abwehrmechanismen investieren, um die Auswirkungen solcher Angriffe gering zu halten.

Social Engineering: Social-Engineering-Angriffe stiegen von 15 Prozent im Jahr 2016 auf 16 Prozent im Jahr 2019. Diese Angriffe nutzen menschliche Schwächen aus. Die österreichischen Unternehmen sollten auch hier verstärkt auf die Schulung ihrer Mitarbeiter:innen setzen, um die Risiken zu minimieren.

Denial-of-Service (DDoS)-Attacken: DDoS-Angriffe stiegen von 8 Prozent im Jahr 2016 auf 38 Prozent im Jahr 2019. Diese Angriffe können die Verfügbarkeit von Diensten erheblich beeinträchtigen. Sie erfordern robuste Abwehrmechanismen. Für Unternehmen ist es deshalb entscheidend, in Technologien zu investieren, die eine rasche Erkennung und Abwehr solcher Angriffe ermöglichen.

Topthemen 2021 bis 2024

Opfer von Cyberangriffen: 2022 sank die Zahl der Unternehmen, die Opfer erfolgreicher Angriffe wurden, auf 12 Prozent, stieg jedoch bis 2024 wieder auf 17 Prozent. Dieser Rückgang lag vor allem an der geänderten Befragung. Waren wir zu Beginn primär daran interessiert, ob die Unternehmen Opfer von Cyberangriffen waren, haben wir in weiterer Folge den Fokus auf die Schäden gelegt.

Phishing: Phishingangriffe stiegen bis 2024 auf 87 Prozent. Phishing ist und bleibt eine bevorzugte Angriffsmethode, durch die Unternehmen kontinuierlich gefährdet sind.

Malware und Ransomware: Die Bedrohung durch Malware und Ransomware stieg bis 2024 auf 86 Prozent. Unternehmen müssen weiterhin verstärkt in robuste Abwehrmechanismen investieren.

Social Engineering: Social-Engineering-Angriffe stiegen bis 2024 auf 62 Prozent. Mitarbeiter:innen-Awareness und -Schulungen sind nach wie vor auf der To-do-Liste der Unternehmen.

Denial-of-Service (DDoS)-Attacken: DDoS-Angriffe stiegen bis 2024 auf 41 Prozent. Eine schnelle Erkennung und Abwehr solcher Angriffe sind wichtiger denn je für heimische Unternehmen.

Themen mit den größten Veränderungen im Zeitraum von 2016 bis 2020

Erfolgreiche Abwehr von Angriffen: Die Fähigkeit der Unternehmen, Angriffe erfolgreich abzuwehren, war im Jahr 2016 mit nur 6 Prozent äußerst gering. Wir sehen eine anfängliche Schwäche in der Sicherheitsinfrastruktur.

Erkennung von Angriffen durch eigene Sicherheitsmaßnahmen: Im Jahr 2016 erkannten 37 Prozent der Unternehmen Angriffe intern. Eine anfängliche Investition in die Sicherheitsinfrastruktur ist daraus abzulesen.

Verständnis von Cyberrisiken: Das Verständnis von Cyberrisiken war im Jahr 2016 noch verhältnismäßig gering ausgeprägt. Mitarbeiter:innen-Schulungen und Awareness-Programme müssen auf den Plan rücken.

Investitionen in Sicherheitstools: Im Jahr 2016 investierten nur 18 Prozent der Unternehmen in Sicherheitstools.

Prävention von Angriffen: Im Jahr 2016 hatten 47 Prozent der Unternehmen einen Krisenplan. Die Investition in proaktive Maßnahmen ist für Unternehmen notwendig, um sich auf mögliche Angriffe vorzubereiten.

Themen mit den größten Veränderungen im Zeitraum von 2021 bis 2024

Erfolgreiche Abwehr von Angriffen: Bis 2024 stieg die Fähigkeit der Unternehmen, Angriffe erfolgreich abzuwehren, auf 59 Prozent. Die Sicherheitsinfrastruktur der Unternehmen hat sich merklich verbessert. Diese muss jedoch weiterhin kontinuierlich überprüft und angepasst werden, um mit den sich ständig ändernden Bedrohungen Schritt zu halten.

Erkennung von Angriffen durch eigene Sicherheitsmaßnahmen: Bis 2024 erkannten 74 Prozent der Unternehmen Angriffe intern. Offenbar haben Unternehmen weiter in ihre Sicherheitsinfrastruktur investiert.

Verständnis von Cyberrisiken: Im Jahr 2024 haben 91 Prozent der Unternehmen ein verbessertes Verständnis von Cyberrisiken. Die Schulungen und Awareness-Programme scheinen zu fruchten.

Investitionen in Sicherheitstools: Bis 2024 investierten 65 Prozent der Unternehmen in Sicherheitstools – ein deutlicher Anstieg im Vergleich zu den Vorjahren.

Prävention von Angriffen: Bis 2024 hatten 57 Prozent der Unternehmen einen Krisenplan, was ebenfalls einen Anstieg im Vergleich zu den Vorjahren darstellt.

Themen, die besonders stabil geblieben sind: Zeitraum 2016 bis 2020

Cyberbudget: Bei 74 Prozent stieg das Cyberbudget im Jahr 2016. Das Budget blieb bis 2020 stabil. Unternehmen investieren kontinuierlich in Cybersicherheit, um sich gegen die wachsenden Bedrohungen zu schützen.

Vertrauen in Schutzmaßnahmen: Im Jahr 2016 vertrauten 89 Prozent der Unternehmen ihren Schutzmaßnahmen.

Meldung von Angriffen: 31 Prozent der Unternehmen meldeten 2016 Angriffe an die zuständigen Stellen.

Awareness für Cyberangriffe: Im Jahr 2016 waren sich 92 Prozent der Unternehmen der Gefahr von Cyberangriffen bewusst. Sie nehmen die Bedrohung ernst und informieren sich kontinuierlich.

Bedenken bezüglich Cloud-Nutzung: Im Jahr 2016 hatten 75 Prozent der Unternehmen Bedenken bezüglich der Cloud-Nutzung. Trotz Vorteilen, die sich durch die Cloud-Nutzung ergeben, bestehen Sicherheitsbedenken.

Themen, die besonders stabil geblieben sind: Zeitraum 2021 bis 2024

Cyberbudget: Das Cyberbudget blieb bis 2024 stabil mit einem leichten Anstieg. Die Wichtigkeit des Themas bleibt also in den Köpfen der Verantwortlichen verankert.

Vertrauen in Schutzmaßnahmen: Bis 2024 vertrauten nach wie vor 89 Prozent der Unternehmen ihren Schutzmaßnahmen.

Meldung von Angriffen: Bis 2024 blieb die Meldung von Angriffen an Behörden konstant. Unternehmen erkennen weiterhin die Notwendigkeit, Vorfälle zu melden, um Unterstützung zu erhalten und andere zu warnen.

Awareness für Cyberangriffe: Bis 2024 blieb das Bewusstsein für Cyberangriffe hoch.

Bedenken bezüglich Cloud-Nutzung: Bis 2024 blieben die Bedenken bezüglich der Cloud-Nutzung konstant.

Was bleibt und wie es weitergeht

In den letzten neun Jahren hat sich das österreichische Cybersecurity-Lagebild von einem kaum beachteten Thema zu einer existenziellen Herausforderung entwickelt. Die Reise war alles andere als geradlinig. Die Jahre 2016 und 2017 waren eine Zeit, in der es Cybersecurity langsam auf die Agenda der Unternehmen geschafft hat. Trotz Erkenntnis, dass Cyberkriminalität ein alltägliches Problem darstellt, waren viele Unternehmen kaum darauf vorbereitet. 2018–2020 wurde Cybersecurity als strategisches Thema ernst genommen. Unternehmen erkannten die Bedrohung durch Phishing und Malware und verstärkten ihre Sicherheitsmaßnahmen. Die Diskussion über Cybersecurity-Themen auf oberster Unternehmensebene nahm zu, doch die Zusammenarbeit mit Drittparteien blieb ein blinder Fleck. Die Pandemie beschleunigte in der Phase ab 2021 die Digitalisierung – und damit auch die Verwundbarkeit der Unternehmen. Plötzlich war Cybersecurity nicht mehr nur ein technisches Problem für Unternehmen, sondern sie wurde zur gesellschaftlichen Verantwortung.

Die Cybersicherheitslandschaft in Österreich hat sich wesentlich seit den Anfängen unserer Studie verändert. Heimische Unternehmen stehen jetzt vor gezielten Angriffen, die sowohl technische als auch menschliche Schwachstellen ausnutzen und enorme wirtschaftliche Auswirkungen nach sich ziehen. Der Fachkräftemangel bleibt eine Herausforderung, die nur durch ein Umdenken im Recruiting und in der Ausbildung von qualifizierten neuen Talenten gelöst werden kann.

Bedrohungen werden immer ausgeklügelter – nicht zuletzt begünstigt durch KI – und machen eine ständige Weiterentwicklung der Abwehrmechanismen für heimische Unternehmen alternativlos. Cybersecurity erfordert auch eine stärkere Zusammenarbeit zwischen allen Beteiligten.

Hoffentlich kommt diese Erkenntnis bei den Unternehmen nicht erst, wenn der Schaden bereits angerichtet ist. Trotzdem: Besser spät als nie. Schließlich ist es nie zu spät, den Sprung ins kalte Wasser zu wagen – solange man schwimmen kann.

Rethinking Cybersecurity: A Proactive Approach

Richard Harknett, Director of the Center for Cyber Strategy and Policy at the University of Cincinnati, shares his insights on the evolution of cybersecurity. He discusses the need for a proactive approach, the role of AI, and the challenges posed by increasing interconnectedness.

Could you tell us more about your role as a cybersecurity expert? What specific experiences and insights did you gain from your research and work at the University of Cincinnati that have shaped your perspectives on cybersecurity?
Richard Harknett: I've been involved in cybersecurity for quite some time, with a significant milestone in 2016 when I served as the first scholar in residence at US Cyber Command. Today, I am speaking in my capacity as a professor at the University of Cincinnati, not as a representative of any U.S. government agency or department. My work supporting the U.S. government began over three decades ago with the Department of Defense on nuclear issues. In the early 90s, I was asked to assess the security implications of browsers, which led to the realization that traditional security approaches didn't fit the networked environment. This insight has guided my work in cybersecurity over the past 30 years, focusing on how interconnected spaces require new security strategies.

Have the changes you've observed over the years been significant in terms of how technology has shaped society and altered our perception of security?
Richard Harknett: Yes, technology has indeed shaped society, but in a way that is distinct from the physical world. Interestingly, my perspective hasn't changed much over the past 30 years, despite significant technological advancements. This is because the fundamental principles underlying these advancements have remained stable. The core architecture of the Internet, for example, has been quite consistent; we've simply built upon it. The key issue I identified in the early 1990s was that network computing is fundamentally about access, which is the opposite of security. Security typically involves segmentation, but the interconnected nature of cyberspace requires us to rethink our approach to security.

> **Cyberspace's interconnected architecture requires us to rethink security.**

What technological and strategic developments have most significantly changed the cybersecurity landscape over the past decade?
Richard Harknett: Over the past decade, significant changes in cybersecurity have been driven by both technical and strategic developments. Technically, the increase in vulnerabilities due to interconnected systems has provided more opportunities for exploitation by criminal and state actors. Strategically, the concept of cyber persistence and persistent engagement has emerged, notably through the „defend forward" strategy adopted by US Cyber Command. This approach emphasizes anticipating vulnerabilities and maintaining initiative to enhance security, as detailed in „Cyber Persistence Theory."

Does defending forward by anticipating threats and vulnerabilities put you in a better position to react quickly and limit the impact of potential exploitations?

FOTO © PRIVAT

Erfahren Sie mehr in unserem Podcast IMPULSE

Dr. Richard Harknett is a Professor of Political Science and Director of the School of Public and International Affairs at the University of Cincinnati. He co-directs the Ohio Cyber Range Institute and chairs the Center for Cyber Strategy and Policy. He also holds positions at UC's School of Information Technology and the Diplomatic Academy Vienna. He was a Fulbright Professor at Oxford University in 2017 and the first Scholar-in-Residence at US Cyber Command in 2016. His research focuses on international relations and cyber strategy.

> **We need a cybersecurity minute, not a cybersecurity month.**

Richard Harknett: I'll emphasize the importance of moving beyond a reactive stance. Anticipation is crucial for resilience. Traditionally, resilience has been viewed as reactive system that can adapt and recover after an incident. However, with a „defend forward" and persistent engagement approach, anticipation must precede reaction. If resilience is purely reactive, adversaries can dictate security conditions within your networks, keeping you on the defensive. You might discover breaches too late, after losing intellectual property or experiencing data disruptions.

This approach moves away from traditional firewall-based cybersecurity, which is ineffective. Governments with legal authority to operate outside their networks need to be more anticipatory and proactive. For example, the British National Cyber Force, the Dutch strategy, and Japan's constitutional amendments for active defense all reflect this shift. South Korea has adopted a similar approach. This trend isn't limited to the United States; cyber powers like Russia and China have long understood the importance of initiative persistence, while the West has been more focused on deterrence, which is inherently reactive. These other cyber powers have been proactive in their operations for quite some time.

Should we consider cyber-physical attacks when discussing the „defend forward" strategy, or are these attacks something we can anticipate occurring later? Is the threshold too high for adversaries to cross into using such tactics now?
Richard Harknett: Cyber-physical attacks can be equivalent to armed attacks, and should be treated as acts of war, whether executed through conventional means or cyber methods. Deterrence strategies should apply equally to both. Despite the capability for such attacks, they are rare outside of war contexts, like Russia's „BlackEnergy" attack in Ukraine. Stuxnet remains a notable example. States leverage cyberspace to shift power – economic, military, social, and political – without direct conflict. North Korea, for instance, uses cyber operations to manipulate financial transactions, bypassing sanctions to support its nuclear program. This strategic engagement allows states to compete without crossing the threshold of armed attack.

> **Cybersecurity requires a mindset shift from reactive to proactive.**

How have cyber operations like Stuxnet and recent hacks, such as North Korea's attack on crypto exchange Bybit, demonstrated the strategic capabilities of cyber warfare, and what implications does this have for global security?
Richard Harknett: Stuxnet and similar operations have shown the world what's possible with advanced cyber capabilities. These actions are strategic behaviors, not just intelligence or crime. North Korea, for example, uses cyber operations to bypass international sanctions and support its national security, demonstrating state strategic behavior. Despite the capability to destroy, organized crime focuses on ransomware, which is digitized extortion. They take data hostage, which is often more valuable and easier to manage than people. This highlights the need to rethink cyber activities and prepare for these real threats with proactive measures.

How can small and medium-sized enterprises in Austria protect their intellectual property from cyber threats and balance cybersecurity budgets for proactive defense?
Richard Harknett: In today's digital age, businesses must integrate cybersecurity into their core business model. Recognizing that reliance on cyberspace comes with inherent vulnerabilities, companies need to find the balance between leveraging digital tools for profit and protecting against potential threats that could undermine their success. This involves developing a robust cybersecurity plan and making strategic investments to safeguard critical assets, particularly intellectual property. By proactively addressing cybersecurity, small and medium-sized enterprises can maintain their competitive edge and ensure long-term viability in the global market.

> **The fundamental principle of network computing was about access, which is the antithesis of security.**

What role do you anticipate artificial intelligence will play in cybersecurity, and what challenges and risks might arise from integrating AI into business strategies?
Richard Harknett: When discussing artificial intelligence, we're referring to algorithmic decision-making. The importance of AI in your organization affects security concerns; minimal roles pose fewer issues, while significant decision-making roles, like in autonomous vehicles, require robust security measures. AI impacts cybersecurity by aiding both vulnerability detection and exploitation, as algorithms lack moral codes. It influences the scale, scope, and speed of activities, enabling rapid data analysis and decision-making. Organizations need a framework to define AI roles that prioritize safety and security, ensuring AI functions correctly and is protected from manipulation.

How can organizations balance the excitement of integrating AI with the need for continuous cybersecurity awareness, ensuring they don't overlook potential risks that may not yet be on their radar?
Richard Harknett: Integrating AI into existing systems doesn't replace the underlying network architecture, which already has vulnerabilities. Instead, it adds another layer to it. This means that while AI offers significant advancements, it also increases our reliance on a space that remains vulnerable. Organizations must therefore maintain continuous cybersecurity awareness and adapt their strategies to address both existing and new risks introduced by AI.

As we look to the future, if you could make one significant change to the cybersecurity landscape, what would it be and why would you choose this particular change?
Richard Harknett: The key change needed in cybersecurity is a shift in mindset from reactive to proactive, focusing on initiative persistence. Technology will do what we ask, but we must anticipate threats and disrupt them before exploitation occurs. Governments play a crucial role in protecting citizens and organizations by limiting what others can do through proactive measures. Cybersecurity is not just a technical issue; it's a political, economic, social, organizational, and behavioral challenge in a technically fluid environment. By integrating these aspects, we can better harness the vitality of cyberspace while mitigating its vulnerabilities.

If we were to meet again in 12 months, what would we wish we had already done today?
Richard Harknett: In 12 months, I hope we have thought more carefully about AI within a framework of roles and responsibilities. My concern is that we might still view AI merely as a tool, rather than considering its impact on decision-making through algorithmic agency. Humans ultimately decide how to deploy AI, and I hope we advance this conversation significantly by then.

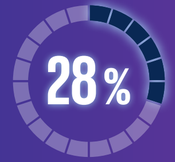
02

Was ist passiert?

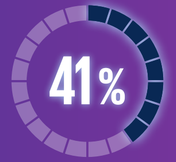
Wie hat sich die Cybersicherheitslage im letzten Jahr entwickelt? Welche Angriffsarten sind häufiger geworden und gab es eine geopolitische Verschiebung der Angriffe? An welchen Stellen waren Unternehmen besonders verwundbar für Cybercrime?
Werfen wir einen Blick darauf, was im letzten Jahr passiert ist. So viel sei vorweggenommen – die Lage ist ernst, die Entwicklungen teils besorgniserregend und noch ist keine Entspannung in Sicht.

Jeder siebte Cyberangriff in Österreich **ist erfolgreich**.

Rund 22 % haben einen **Zusammenhang zwischen globalen geopolitischen Konflikten** und Cyberangriffen auf ihr Unternehmen festgestellt.

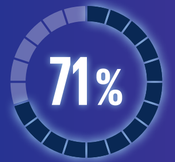


Mehr als jeder 4. Angriff ist auf **staatlich unterstützte Akteur:innen** zurückzuführen.



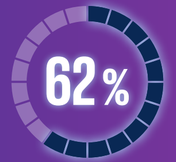
der Angriffe kamen aus dem **asiatischen Raum**.

der Angriffe hatten **europäischen Ursprung**.



fürchten die **Beeinträchtigung des Geschäftsbetriebes** im Zusammenhang mit geopolitischen Konflikten.

Für jedes vierte Unternehmen waren ein **ineffektives und unzureichendes Patchmanagement** und der Schutz vor Schwachstellen Auslöser für erfolgreiche Angriffe.



konnten Cyberangriffe **mithilfe der eigenen Mitarbeitenden** identifizieren – vor technischen Lösungen und Systemen.

Entwicklung der Cyberangriffe im letzten Jahr

Rund ein Viertel der Befragten (22 Prozent) gibt an, dass die Anzahl der Cyberattacken auf ihr Unternehmen in den vergangenen zwölf Monaten stark bzw. eher zugenommen hat. Rund 40 Prozent stellten ein gleich gebliebenes Angriffsniveau zum Vorjahr fest. Einem Drittel der befragten Unternehmen ist allerdings nicht bekannt, ob sich die Angriffe gegen sie in den letzten 12 Monaten verändert haben bzw. auch, in welcher Art und Weise die Veränderungen stattgefunden haben.

Wir sehen also, dass die Angriffe langsam beginnen, sich auf einem sehr hohen Niveau einzupendeln. Es gibt allerdings keine Anzeichen von Entspannung. Die Angriffe werden fokussierter und die Angriffstaktiken ausgeklügelter. Im Jahr 2024 gab rund ein Drittel der Befragten (32 Prozent) an, dass sie eine starke oder eher starke Zunahme der Angriffe festgestellt haben.

Gründe für die Veränderung von Cyberangriffen

Was aus Sicht der Befragten die Gründe für die Veränderung der Cyberangriffe im Vergleich zum Vorjahr waren, lässt sich in die folgenden Kategorien unterteilen:

Die geopolitische Lage spielt eine bedeutende Rolle. Insbesondere der russische Angriffskrieg auf die Ukraine und andere weltweite Krisen und Konflikte, die sich mehr und mehr in den Cyberraum verlagern, führen zu einer erhöhten Bedrohungslage.

Die Digitalisierungsambitionen bringen eine Ausweitung der IT-Infrastruktur mit sich und haben das Angriffspotenzial vergrößert, da mehr Tools und eine größere Attack Surface verfügbar sind.

Die Entwicklung und der Einsatz von Künstlicher Intelligenz haben die Möglichkeiten für Angreifer:innen erheblich vereinfacht. Insbesondere durch die Automatisierung und die Erstellung ausgeklügelter Phishingszenarien entsteht eine neue Dynamik. Autonome, GenAI-basierte Phishingplattformen agieren als One-Stop-Shop für Cyberkriminelle.

Schließlich haben laut Befragten auch die politischen Veränderungen und die allgemeine geopolitische Unsicherheit zu einer Intensivierung der Angriffe beigetragen.

Versuchte Cyberattacken und Schäden

13 Prozent der befragten Unternehmen haben in den letzten 12 Monaten erfolgreiche Cyberangriffe festgestellt, die zu Beeinträchtigungen oder Schäden führten. Jeder siebte Cyberangriff in Österreich ist damit erfolgreich. Im Vergleich dazu war im Jahr 2024 jeder sechste Cyberangriff erfolgreich.

Interessant hierbei ist auch, dass 17 Prozent der befragten Unternehmen nicht wissen, ob sie Opfer einer Cyberattacke waren und ob diese Angriffe zu Schäden geführt haben (15 Prozent im Jahr 2024). Gerade in Zeiten, in denen die Digitalisierung überhandnimmt und die Abhängigkeit von digitalen Technologien und Services von hoher Bedeutung ist – was auch die immer präsenter werdende Regulatorik zeigt – ist es umso bedeutender, dass Unternehmen darüber Bescheid wissen, inwieweit Cyberangriffe auf ihr Unternehmen stattgefunden haben und auch den Schadenswert dieser kennen.

Akteur:innen der Cyberangriffe

Schauen wir uns an, von welchen Akteur:innen die Handlungen in den letzten 12 Monaten ausgingen, so zeigt sich, dass organisierte Kriminalität mit 48 Prozent die dominanteste Quelle ist. Überraschend an zweiter Stelle (mit 28 Prozent) finden sich staatliche oder staatlich unterstützte Akteur:innen. Damit ist klar: Die geopolitischen Konflikte sind in Österreich angekommen. Im Vergleich zum Vorjahr (12 Prozent) sehen wir mehr als eine Verdoppelung der Angriffe durch staatlich unterstützte Akteur:innen. in Österreich. Vor allem in Zeiten geopolitischer Konflikte und der Veränderung

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

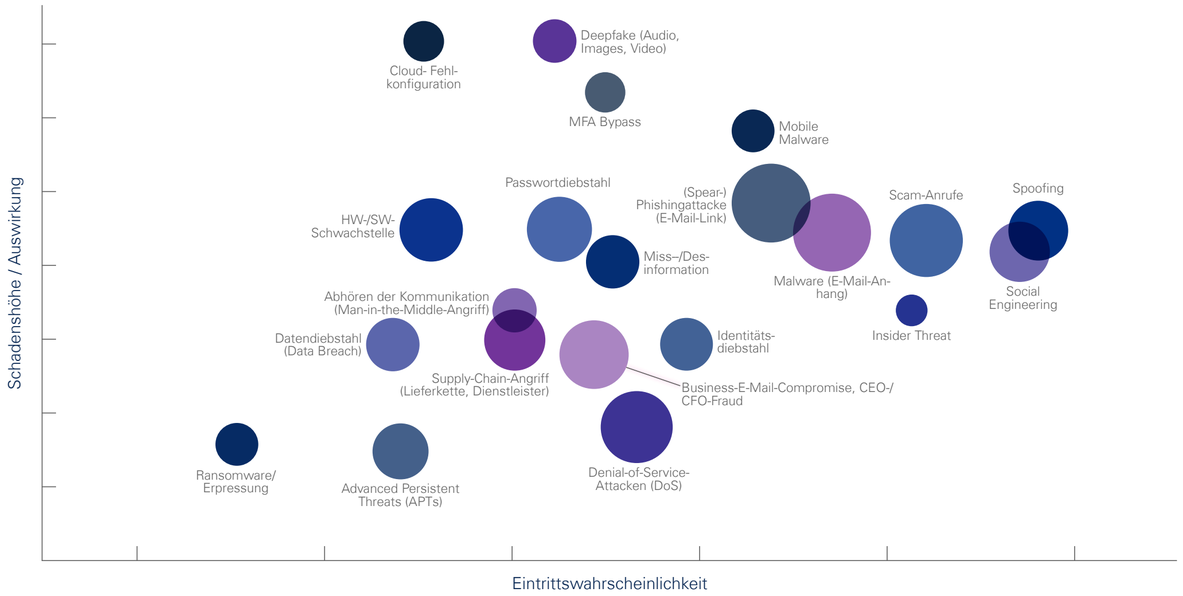
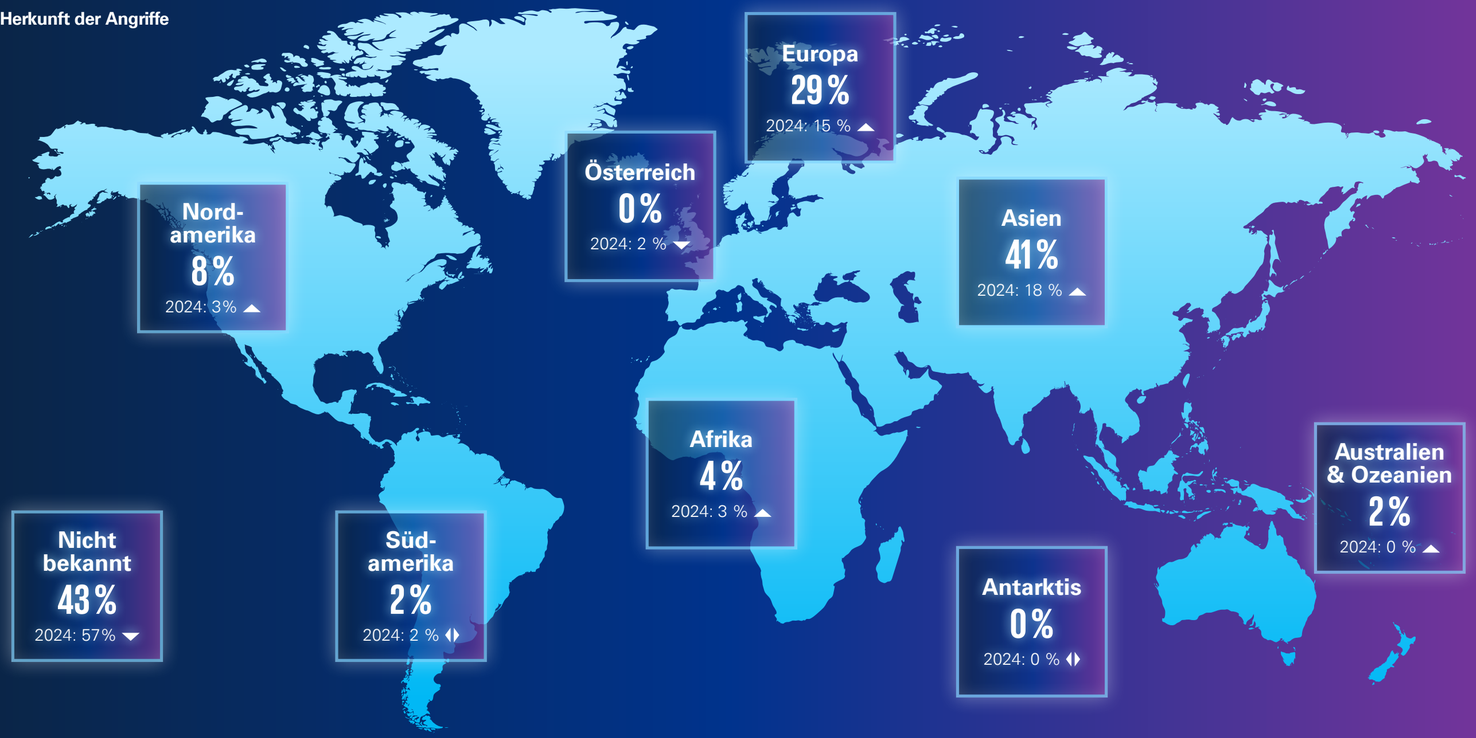


Abb. 2: Herkunft der Angriffe



▲ ▼ ◆ = aktueller Trend / Entwicklung der Angriffe

der globalen Weltordnung kommt es hier zu einer Professionalisierung und Verschiebung der kriminellen Aktivitäten.

Ebenfalls alarmierend: Für rund ein Drittel der befragten Unternehmen (34 Prozent) war es nicht möglich, die Akteur:innen zu identifizieren. Diese Identifikation wird immer schwieriger und damit zu einem großen Problem (25 Prozent im Jahr 2024). Es zeigt sich, dass wir im Wettrennen gegen Cyberkriminelle mehr und mehr ins Hintertreffen geraten und den Anschluss sowie die Kontrolle verlieren.

Herkunft von Cyberangriffen

Fragt man nach der Region, aus der die Cyberangriffe gekommen sind, so zeigt sich, dass der asiatische Raum unangefochten an erster Stelle liegt – mit 41 Prozent der Angriffe. Angriffe aus Asien haben sich 2025 mehr als verdoppelt, von 18 auf 41 Prozent, und Angriffe aus Europa sind von 15 auf 29 Prozent gestiegen. Hier kann natürlich nicht eindeutig belegt werden, ob es sich nicht um Relays oder Proxys handelt und die eigentliche Herkunft der Angriffe verschleiert wird. Auf dem dritten Platz finden wir Angriffe aus Nordamerika (8 Prozent).

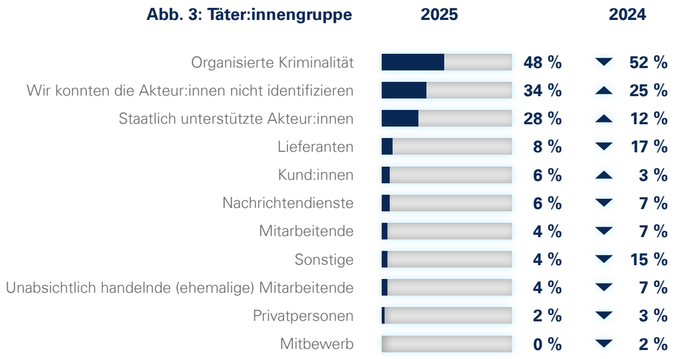
Weniger als die Hälfte der befragten Unternehmen (43 Prozent) weiß allerdings nicht, woher die Cyberattacken gegen sie stammen. Auch wenn wir eine Verbesserung gegenüber dem Vorjahr (2024: 57 Prozent) bemerken, ist diese Zahl nicht weiter verwunderlich. Führt man sich die Professionalisierung des Cybercrime-Ökosystems vor Augen, so sieht man, dass Verschleierungstechnologien immer mehr überhandnehmen bzw. diese auch immer einfacher in der Handhabung werden. Somit ist die Herkunft der Täter:innen nicht mehr eindeutig bestimmbar. Inwieweit es sich dabei um staatliche oder staatlich unterstützte Gruppierungen handelt, die im Auftrag von Nationalstaaten arbeiten, kann nicht eindeutig identifiziert werden. Es bleibt also eine gewisse Unsicherheit bei der Einordnung und Attribuierung der Angreifer:innengruppen.

Geopolitische Konflikte und Cyberangriffe

Mehr als jedes fünfte befragte Unternehmen (22 Prozent) gab an, dass sie einen (z. B. zeitlichen oder inhaltlichen) Zusammenhang zwischen globalen geopolitischen Konflikten und Cyberangriffen auf ihr Unternehmen festgestellt haben. 27 Prozent ist nicht bekannt, ob es hierbei einen Zusammenhang gibt (15 Prozent im Jahr 2024).

Gerade in Zeiten geopolitischer Krisen kann es durchaus vermehrt vorkommen, dass Unternehmen zum Opfer von Cyberangriffen werden – entweder gewollt (hier stehen zum Beispiel Industriespionage und Diebstahl geistigen Eigentums im Mittelpunkt, die vor allem im Auftrag

Abb. 3: Täter:innengruppe



staatlicher Akteur:innen ausgeführt werden) oder aber auch ungewollt (indem z. B. aufgrund von Namensgleichheiten oder ähnlich lautender Firmenbezeichnungen, aber auch einfach nur zufällig ein Angriff auf das Unternehmen stattfindet). Unabhängig der Tatsache, von welchem Zusammenhang wir hier sprechen, ist jedes Unternehmen aufgerufen, Sicherheitsvorkehrungen zu treffen, um gerade in Zeiten geopolitischer Konflikte resilient zu sein und zu bleiben.

Zusammenhang zwischen geopolitischen Konflikten und Cyberangriffen

Die Antworten aus unserer Umfrage deuten auf einen klaren Zusammenhang zwischen geopolitischen Spannungen, insbesondere dem russischen Angriffskrieg auf die Ukraine, und einer Zunahme von Cyberangriffen hin. Die Befragten vermuten, dass Destabilisierungsversuche und gezielte Angriffe, z. B. von pro-russischen Gruppierungen, im Kontext dieses Konflikts stehen. Staatliche Behörden und Infrastrukturen sind dabei besonders gefährdet und vermehrt Angriffen ausgesetzt, wie etwa DDoS-Attacken über Bot-Netze. Zudem scheinen politische Ereignisse wie die Wahlen in Österreich die Angriffsaktivität zu verstärken, möglicherweise als Versuch der Wahlmanipulation. Angriffe auf VPN-Geräte und andere gezielte Cyberattacken aus Russland scheinen ebenfalls für die Befragten Teil dieses Musters zu sein.

Bedenken im Zusammenhang mit geopolitischen Konflikten

Fragt man, vor welchen Cyberrisiken Unternehmen im Zusammenhang mit geopolitischen Konflikten die größten Bedenken haben, so gehen die Top 3 hier ganz eindeutig hervor: Auf Platz eins liegt die Beeinträchtigung des Geschäftsbetriebes (71 Prozent), was natürlich eine unmittelbare Konsequenz auf jedes Unternehmen hat und zu Kollateralschäden führen kann. An zweiter Stelle werden finanzielle Verluste durch Cyberangriffe genannt (62 Prozent). Diese sind eine der Folgen eines beeinträchtigten Geschäftsbetriebes. An dritter Stelle haben Unternehmen Bedenken, sensible Informationen und geistiges Eigentum zu verlieren (61 Prozent). Gerade das geistige Eigentum ist es, was die Grundlage der unternehmerischen Existenz sichert und vor allem auch dazu dient, im globalen Wettbewerb bestehen zu können. Geht dieses geistige Eigentum (z. B. Forschungs- und Entwicklungsdaten, Patente vor

Fortgeschrittene Technologien zur Verschleierung

1. KI und Social Engineering
Angreifer:innen nutzen generative KI-Modelle für hyperrealistische Phishingkampagnen. Durch Deepfake-Technologien wird eine Echtzeitimitation von Stimmen möglich. Die Angriffe finden über Multi-Channel-Strategien (z. B. durch Kombination von E-Mails, SMS, Messengerdiensten und Nachrichten auf Kollaborationsplattformen) statt. So wird die Glaubwürdigkeit erhöht.

2. Anonymisierungsdienste
Durch Netzwerkverschleierungstechnologien können Angriffsherkunft und Identität getarnt werden. Folgende Technologien sind derzeit im Einsatz: Tor „The Onion Router" (Routing über drei verschlüsselte Knoten – Entry, Relay, Exit – zur IP-Verschleierung), VPN (Ende-zu-Ende-Verschlüsselung des gesamten Datenverkehrs über Remote-Server) und Proxies (IP-Maskierung ohne Verschlüsselung).

3. Cloud-basierte Verschleierung und Infrastrukturmissbrauch
Cyberkriminelle verwenden Cloud-Dienste, um kriminelle Aktivitäten als legitimen Traffic zu tarnen. Zusätzlich missbrauchen sie Remote-Management-Tools für Lateral Movement. Diese hinterlassen keine Malware-Signaturen.

4. Professionalisierung von Cyberkriminalität
Durch die Kommerzialisierung von Angriffswerkzeugen wird die Einstiegshürde für Täter:innen gesenkt und das Angriffsvolumen vergrößert. Folgende Angebote finden sich bereits:

- Phishing-as-a-Service: KI-generierte Kampagnen inklusive Zielpersonen-Recherche
- Ransomware-Kits: Automatisierte Exploits scannen Schwachstellen in Echtzeit und passen Verschlüsselungsroutinen an
- Darknet-Märkte: Verkauf gehackter VPN-Zugänge oder kompromittierter Proxies für Angriffsinfrastrukturen

5. Abwehrstrategien und Zero-Trust-Architekturen
Zur Abwehr empfehlen Expert:innen verhaltensbasierte Erkennung (Analyse von Nutzer:innenaktivitäten auf Anomalien), Kernel-Level-Überwachungen (Tools zur Identifizierung von LotL-Techniken), Identity Governance (Zugriffskontrollen und MFA) sowie Threat Intelligence Sharing (branchenübergreifender Austausch).

Einreichung) verloren, ist es für den Mitbewerb in anderen Ländern – hier blicken wir insbesondere nach Asien – ein leichtes Unterfangen, ein Konkurrenzangebot gegenüber heimischen Unternehmen aufzubauen. Der Schutz des geistigen Eigentums muss deshalb unbedingt im Mittelpunkt stehen, um hier wettbewerbs- und konkurrenzfähig zu sein. Dabei geht es nämlich auch im Umkehrschluss darum, die eigene unternehmerische Existenz abzusichern.

Weitere Bedenken im geopolitischen Kontext

Wir haben die Unternehmen gefragt, vor welchen sonstigen Cyberrisiken sie im Zusammenhang mit geopolitischen Konflikten die größten Bedenken haben. Aus den Antworten lesen wir heraus, dass Bedenken dahingehend bestehen, dass Datenschutzverletzungen und Brute-Force-Attacken auf Remote-Zugänge die Performance beeinträchtigen und zu Betriebsstillständen führen könnten. Hybride Kriegsführung und gezielte Sabotage, insbesondere gegen kritische Infrastrukturen wie die Energieversorgung, stellen eine weitere Bedrohung dar. Auch Supply-Chain-Attacken und Cyberattacken bei Lieferanten könnten den operationellen Betrieb erheblich beeinträchtigen.

Weitere Risiken umfassen die Verbreitung von Mal- und Spyware, Ransomware-Angriffe, Phishing, Scam-E-Mails und den Verlust von Daten. Politisch motivierte Angriffe gegen die Wertschöpfungsindustrie europäischer Staaten sowie Desinformation und die Nutzung von KI zur Beeinflussung der Gesellschaft sind ebenfalls für die Befragten besorgniserregend. Zudem gibt es Bedenken hinsichtlich der Abhängigkeit von Anbietern aus Drittstaaten, die zu Kostenerhöhungen oder Leistungseinschränkungen führen könnten. Auch wird befürchtet, dass DDoS-Attacken und Blackouts zu einem kompletten Geschäftsstillstand führen.

Verschiedene Angriffsarten

Werfen wir nun einen Blick darauf, wie häufig verschiedenste Arten von Angriffen innerhalb der letzten 12 Monate bei den befragten Unternehmen vorkamen. Hier lassen sich einige interessante Beobachtungen, gerade auch im Vergleich zum Vorjahr, feststellen.

Auf Platz eins liegt heuer erstmalig Malware ex aequo mit (Spear-)Phishing (81 Prozent). Scam-Anrufe befinden sich heuer mit 65 Prozent auf dem dritten Platz. Unter diesem Phänomen werden auch oftmals der Enkel- bzw. Neffen-Trick verstanden, die im Bereich sozialer Netzwerke oder Messengerdienste auftreten. Hierbei stehen (versuchter) Identitätsdiebstahl, Täuschung, Erpressung oder Diebstahl von Vermögenswerten im Vordergrund. Scam-Anrufe verzeichnen einen dramatischsten Zuwachs. Dieser Trend reflektiert die zunehmende Professionalisierung von Social-Engineering-Angriffen via Voice-Channel, möglicherweise unterstützt durch KI-generierte Stimmen oder gezielte Vorabrecherchen über Opfer.

Auf Platz Nummer vier rangiert Business-E-Mail-Compromise. Mit 59 Prozent sehen wir hier immer noch ein sehr häufiges Auftreten, vor allem wenn es um finanzielle Bereicherung oder die Umleitung von Finanztransaktionen (z. B. falsche Rechnungen oder Share-Seed-Phrase Scam) geht. Bei dieser Art von Angriff steht die Beeinflussung der Identität im Mittelpunkt und der gute Glaube der Opfer, die meinen, mit einer legitimen Person in Kontakt zu stehen. Trotz eines Rückgangs bei Social Engineering von 62 Prozent im Vorjahr auf 41 Prozent im Jahr 2025 sowie von Business-E-Mail-Compromise von 80 Prozent im Vorjahr auf 59 Prozent im Jahr 2025, bleiben diese Vektoren zentrale Risiken. Der Rückgang könnte auf verbesserte Mitarbeiter:innensensibilisierung und den Einsatz von KI-basierten E-Mail-Filtern zurückzuführen sein. Die weiterhin hohen Werte unterstreichen jedoch die anhaltende Attraktivität menschlicher Schwachstellen als Angriffspunkt.

Auf dem fünften Platz mit 55 Prozent finden wir Denial-of-Service (DoS)-Attacken. Gerade diese Entwicklung ist durchaus beachtenswert, denn wir sehen darin eine gewisse Veränderung in der Taktik der Angreifer:innen und merken, dass Schadsoftware momentan dominiert. In Zeiten der politischen Veränderung, vor allem durch Wahlen, nehmen solche Attacken Fahrt auf, da durch sie eine gezielte Beeinflussung initiiert werden kann.

Parallel dazu ist MFA Bypass (17 Prozent Neuauftreten 2025) ein Indikator für die wachsende Fähigkeit von Angreifer:innen, selbst mehrstufige Authentifizierungssysteme zu kompromittieren – etwa durch Session Hijacking oder Phishingtools wie Evilginx.

Auch in diesem Jahr zeigt sich wieder, dass der Faktor Mensch derjenige ist, der im Mittelpunkt der Angriffe steht und dessen Identität beziehungsweise Glaubwürdigkeit aufs Spiel gesetzt wird. Unsere Aufgabe muss es sein, die damit verbundenen Themen Vertrauen und Integrität in den Griff zu bekommen. Es wird eine Mammutaufgabe, hier entgegenzuwirken – es gibt einen Wettlauf zwischen Angreifer:innen und Verteidiger:innen, und es bleibt abzuwarten, wer hier schlussendlich die Oberhand behält.

Auffällig ist die Stabilität bei Denial-of-Service-Angriffen (55 Prozent), die trotz weit verbreiteter DDoS-Schutzlösungen kaum rückläufig sind – ein Hinweis auf die steigende Leistungsfähigkeit botnetbasierter Angriffe, möglicherweise verstärkt durch unsichere IoT-Geräte. Ransomware verharrt auf hohem Niveau (26 Prozent), was die zunehmende Professionalisierung von Ransomware-as-a-Service-Modellen und die Fokussierung auf kritische Infrastrukturen widerspiegelt. Gleichzeitig bleibt Datendiebstahl mit 34 Prozent (2025) ein Problem, was die Notwendigkeit verschlüsselter Datenpipelinekonzepte unterstreicht.

Geopolitische Konflikte sind in Österreich angekommen.

Positiv entwickeln sich Cloud-Fehlkonfigurationen (15 Prozent), was auf verbesserte CSPM-Tools (Cloud Security Posture Management) sowie Cloud-Sicherheitsprozessen hindeutet. Der starke Rückgang bei Insider Threats (8 Prozent) könnte auf verhaltensanalytische Überwachungssysteme oder strengere Zugriffskontrollen zurückzuführen sein.

Die leichte Verschiebung bei Advanced Persistent Threats (33 Prozent) trotz Rückgangs zeigt, dass staatlich unterstützte Akteur:innen weiterhin gezielte Langzeitangriffe auf kritische Sektoren durchführen. Die Veränderung der Bedrohungen im Bereich der Miss-/Desinformation (31 Prozent) verweist auf die Ambivalenz von KI-gestützten Erkennungstools gegen Fake-News-Kampagnen.

Die Daten zeigen einen teilweisen Erfolg defensiver Maßnahmen in Bereichen wie Cloud-Sicherheit und Insider-Bedrohungen, während gleichzeitig neue Angriffsvektoren (Scam-Anrufe, MFA Bypass) entstehen. Die Branche sieht sich einem dynamischen Gegner gegenüber, der Lücken in technologischen und menschlichen Sicherheitskontrollen systematisch ausnutzt.

Ursachen für erfolgreiche Angriffe

Was hat dazu geführt, dass Angriffe bei den Unternehmen erfolgreich waren? Der Blick auf die Zahlen zeigt, dass wir es immer noch mit denjenigen Themen zu tun haben, die im Bereich der Basishygiene bzw. der Basis-Sicherheitsanforderungen liegen. So gibt jedes vierte Unternehmen an, dass ein ineffektives und unzureichendes Patchmanagement und der Schutz vor Schwachstellen Auslöser dafür waren, dass ein Angriff erfolgreich war. An zweiter Stelle finden wir schwache Anmeldedaten beziehungsweise den Diebstahl und Missbrauch von Anmeldedaten (22 Prozent). Auf Platz drei liegt ineffektiver Datenschutz (20 Prozent), der zu Diebstahl oder Manipulation geführt hat.

> **Im Wettrennen gegen die Cyberkriminellen geraten wir immer mehr ins Hintertreffen.**

Wir sehen also, dass wir es immer noch mit Basisanforderungen zu tun haben, deren Mangel in weiterer Folge Auslöser für erfolgreiche Angriffe ist. Auffällig ist allerdings, dass bei jedem fünften Unternehmen nicht klar ist, was zu erfolgreichen Angriffen geführt hat. Hier sind unbedingt noch Verbesserungen der Transparenz beziehungsweise im Monitoring, aber auch Verbesserungen im Bereich der technischen Analyse zur Identifizierung der Schwachstellen und der Eintrittsvektoren notwendig.

Weitere Ursachen für erfolgreiche Angriffe auf heimische Unternehmen

Unsichere Zwei-Faktor-Authentifizierungsmethoden, die anfällig für Phishing sind, und eine mangelnde Awareness bei den Nutzer:innen haben laut den Umfrageteilnehmenden ebenso zu potenziellen Schwachstellen geführt. Gefälschte Log-in-Seiten, die über Suchmaschinen aufgerufen werden, waren ebenfalls ein Risiko. Obwohl Angriffe nicht immer direkt erfolgreich waren, haben neue Arten von DDoS-Attacken dennoch zu Beeinträchtigungen geführt.

Wie man auf Angriffe aufmerksam wurde

Bei der Frage danach, wie Unternehmen auf die Angriffe aufmerksam wurden, zeichnet sich vor allem eines ab: Die eigenen Mitarbeitenden sind der unmittelbare Schlüssel zum Erfolg. 62 Prozent der befragten Unternehmen gaben an, dass sie durch die Meldung der Mitarbeitenden auf die Angriffe aufmerksam wurden (minus 5 Prozent gegenüber 2024). Damit stehen Mitarbeitende ganz besonders im Mittelpunkt und sind für die Identifizierung der Angriffe unabdingbar – sie leisten einen wesentlichen Beitrag für die Cybersicherheit. Auf Platz Nummer zwei finden wir interne Sicherheitssysteme mit 57 Prozent (minus 17 Prozent gegenüber 2024) und auf dem dritten Platz die Analyse von Log-Daten (48 Prozent). Technologie hat also nahezu den gleichen Stellenwert wie die Mitarbeitenden, wenn es um die Erkennung der Angriffe geht.

Interessant ist, dass sich die Rolle der externen Dienstleister gegenüber dem Jahr 2024 wesentlich verändert hat. Diese sind von Platz drei auf Platz sechs zurückgerutscht und liegen nun nur noch bei 24 Prozent (minus 20 Prozent gegenüber 2024). Diese Zahlen unterstreichen, dass Unternehmen selbst in Technologien zur Erkennung von Cyberangriffen investieren und entsprechende Fähigkeiten auf- und ausbauen.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1. Angriffe durch staatlich unterstützte Akteur:innen haben sich in Österreich mehr als verdoppelt. Geopolitische Konflikte sind somit in Österreich angekommen.
2. Angriffe pendeln sich auf einem sehr hohen Niveau ein, werden aber gleichzeitig zielgerichteter. Es ist kein Anzeichen von Entspannung in Sicht.
3. Es wird immer schwieriger, die Akteur:innen zu identifizieren und wir geraten im Wettrennen gegen die Cyberkriminellen immer mehr ins Hintertreffen.

Sicherheit im digitalen Zeitalter: Österreichs Kampf gegen Cybercrime und Desinformation

In einem umfassenden Interview geben **Andreas Holzer**, Direktor des österreichischen Bundeskriminalamtes, und **Hermann Kaponig**, Direktor der Direktion für IKT und Cyber im österreichischen Bundesheer, Einblicke in die aktuellen Herausforderungen und Strategien zur Bekämpfung von Cyberkriminalität und hybriden Bedrohungen.

Da wir es mit verschiedenen Einrichtungen und Abteilungen zu tun haben, wäre es interessant, wenn Sie uns zunächst einen kurzen Überblick geben könnten. Was sind Ihre Aufgaben, welche Funktion haben Sie, welche Rolle spielen Sie und welche Kompetenzen bringen Sie mit?

Andreas Holzer: Ich bin Direktor des österreichischen Bundeskriminalamtes und seit 32 Jahren Polizist. Das Bundeskriminalamt ist die zentrale Stelle der Kriminalpolizei in Österreich, mit etwa 800 Mitarbeitenden in der Zentrale und 5 Außenstellen. Wir leiten und koordinieren die Kriminalpolizei, die aus etwa 5.000 bis 6.000 Kriminalist:innen besteht. Unsere Hauptaufgaben sind die Koordinierung von Ermittlungen in Österreich und die Führung internationaler Ermittlungen, in Zusammenarbeit mit Partnern wie dem FBI, dem deutschen Bundeskriminalamt, Europol und Interpol.

Hermann Kaponig: Ich bin Direktor der Direktion 6 für IKT und Cyber im österreichischen Bundesheer und Kommandant der Cyber- und Informationskräfte. Wir sind verantwortlich für Führungsunterstützung, Cyberabwehr, Informationsoperationen und Weltraumservices für das Bundesheer. Unsere Arbeit ist sowohl national als auch international verankert, und wir entwickeln uns zu einer eigenständigen Truppengattung im Cyber- und Informationsraum.

Internationalität wird immer wichtiger, da Cyberkriminalität keine Grenzen kennt. Cybercrime ist ein wachsendes Problem in Österreich, mit steigenden Fallzahlen und immer komplexeren Angriffen, wie die jährlichen Berichte des Bundeskriminalamtes zeigen. Könnten Sie uns einen Überblick über die aktuelle Lage geben? Welche Arten von Cyberkriminalität treten Ihrer Beobachtung nach besonders häufig auf, und wie unterscheiden sich diese in Bezug auf ihre Komplexität?

Andreas Holzer: Statistiken zu Cyberkriminalität sollten im langfristigen Kontext betrachtet werden. Über die letzten 10 Jahre haben die Fälle dramatisch zugenommen. Im Jahr 2023/24 gab es einen leichten Rückgang, aber wir erwarten in den kommenden Jahren wieder einen Anstieg. Die Statistik spiegelt nicht immer die Realität wider, da es eine hohe Dunkelziffer gibt. Oft erstatten Opfer keine Anzeige, besonders bei geringem Schaden oder aus Scham, wie bei Love Scams oder Sextortion.

Cyberkriminalität wird in zwei Kategorien unterteilt: Im engeren Sinn sind es Angriffe auf Daten, wie Ransomware. Im weiteren Sinn umfasst

FOTO © FOTOSTUDIO SEMRAD

General Mag. Andreas Holzer, MA ist seit Februar 2021 General und Direktor des Bundeskriminalamtes. Zuvor leitete er die Abteilung für Ermittlungen im Bundeskriminalamt. Er besitzt einen Masterabschluss in Strategischem Sicherheitsmanagement und einen Abschluss in Politikwissenschaft. Holzer hat zahlreiche internationale Erfahrungen gesammelt, darunter Vorträge zu Themen wie Doping- und Arzneimittelkriminalität sowie Bekämpfung der Organisierten Kriminalität. Er wurde mehrfach ausgezeichnet, unter anderem als „Kriminalist des Jahres“ und mit dem Goldenen Ehrenzeichen für Verdienste um die Republik Österreich.

FOTO © KULLEC HBF

Generalmajor Hermann Kaponig hat die Offiziersausbildung an der Theresianischen Militärakademie und den Generalstabslehrgang an der Landesverteidigungsakademie absolviert. Er hat darüber hinaus ein universitäres Diplomstudium abgeschlossen. Kaponig hat verschiedene Leitungspositionen als Referats-, Abteilungs- und Gruppenleiter im BMLV innegehabt. Er kann auf zahlreiche Vorträge, Fachpublikationen und Diskussionsforen zu Themen der Cybersicherheit und Cyberverteidigung verweisen. Zudem konnte er auch internationale Erfahrungen bei Einsätzen, Übungen und Ausbildungen sammeln. Führungspositionen waren als Kommandant des „Führungsunterstützungszentrums“, des „Kommandos Führungsunterstützung & Cyber Defence“, des „IKT & Cybersicherheitszentrums“ und aktuell als Leiter der „Direktion 6 - IKT&Cyber“, sowie als Kommandant der Cyber- & Informationskräfte des ÖBH und als CDO und CIO des BMLV.

Erfahren Sie mehr in unserem Podcast IMPULSE

es Delikte, bei denen das Internet als Tatmittel verwendet wird, wie zum Beispiel Internetbetrug oder Erpressung. Zwei Drittel der Fälle sind Betrugsdelikte, die die Polizei stark belasten, da sie viele Phänomene umfassen, wie Phishing. In Österreich gibt es etwa 530.000 Anzeigen pro Jahr, davon rund 62.000 im Bereich Cybercrime, was die Polizei personell und ressourcenmäßig stark fordert. Um darauf zu reagieren, haben wir das C4, Cybercrime Competence Center, im Bundeskriminalamt eingerichtet und eine Kriminaldienstreform durchgeführt, die eine systematische Vorgehensweise von der Polizeiinspektion bis zum Bundeskriminalamt sicherstellt.

Betrachten wir die strukturelle Seite des Bundesheeres, sehen wir die Bedrohung durch hybride Angriffe. Das jährliche Risikobild 2025 des Bundesheeres warnt vor Cyber-Physical-Angriffen auf kritische Infrastrukturen wie Energieversorger. Wie bewertet das Bundesheer diese Bedrohungslage für Österreich, und auf welche Szenarien bereiten Sie sich vor, um koordinierten Angriffen zu widerstehen und vorbereitet zu sein?
Hermann Kaponig: Wir sehen aus den Analysen, dass Angriffe auf die kritischen Infrastrukturen, sowohl im Vorfeld als auch bei einer konkreten Auseinandersetzung, zum Standard geworden sind.

Für uns ist die Bedrohungslage für den Cyber- und Informationsraum bereits über Jahre hinweg

> **Cybercrime-Delikte fordern die Polizei personell und ressourcenmäßig stark.**
>
> Andreas Holzer

sehr hoch und kann als angespannt betrachtet werden.

Das Bundesheer bereitet sich auf diese hybriden Herausforderungen gut vor. Aber um am Ende in der vollen Dimension erfolgreich sein zu können, wird nationale als auch internationale Zusammenarbeit intensiv gepflegt.

Wir schützen unsere Systeme mit gehärteten Systemen und qualifizierten Expert:innen. Im Grunde genommen sind wir da täglich gefordert. Zur Prüfung und Weiterentwicklung unserer Fähigkeiten nehmen wir regelmäßig an nationalen oder internationalen Übungen teil. Wir üben die Abwehr von Angriffen im Cyber-, Informations- und elektromagnetischen Raum im vollen Spektrum möglicher Angriffsvektoren auf militärische Systeme bis hin zu kritischer Infrastruktur.

Die Aufklärung von Cyberkriminalität ist in Österreich eine große Herausforderung. Was sind Ihrer Meinung nach die größten Hindernisse dabei? Liegen sie eher in technischen Hürden oder in rechtlichen Rahmenbedingungen?
Andreas Holzer: Die Polizei in Österreich hat generell eine hohe Aufklärungsquote, aber bei Cyberkriminalität ist sie niedriger wegen Anonymisierungstechniken wie VPNs. Probleme bei der Rückverfolgung von IP-Adressen und fehlende Vorratsdatenspeicherung erschweren die Ermittlungen. Unterschiedliche Gesetze in der EU und Drittstaaten machen grenzüberschreitende Ermittlungen schwierig, besonders bei Verschlüsselung und Kryptowährungen.

Trotzdem liegt Österreich mit einer Aufklärungsquote von etwa 30 Prozent im Cybercrime-Bereich im internationalen Vergleich gut. Wir ermutigen die Bevölkerung, alle Vorfälle vollständig anzuzeigen, da es immer eine Spur gibt, die zu Ermittlungen führen kann. Das Melden von Vorfällen ist entscheidend. Obwohl viele Unternehmen nicht in den Medien erscheinen wollen, ist die Zusammenarbeit mit der Polizei wichtig. Erfolgreiche Ermittlungen, oft mit Unterstützung von Europol oder Interpol, sind möglich, wenn alle Beteiligten, einschließlich Unternehmen und Polizei, zusammenarbeiten. Nur durch diese Zusammenarbeit können Täter:innengruppen effektiv verfolgt und zur Rechenschaft gezogen werden.

Wir wollen wissen, was Täter:innengruppen tun, und gleichzeitig sicherstellen, dass die Kommunikationssysteme des Bundesheeres abhörsicher sind. Verschlüsselungen sollten schwer zu knacken sein, besonders im Hinblick auf Quanten- und quantensichere Kommunikation. Welche Herausforderungen sehen Sie bei der Post-Quanten-Kryptografie für das Bundesheer? Gibt es besondere Aspekte, auf die wir achten müssen?
Hermann Kaponig: Wir haben im Bundesheer gestufte Sicherheitssysteme, die in Abhängigkeit der zu schützenden Information unterschiedliche Sicherheitslevels aufweisen. Diese reichen von der herkömmlichen Mehrfaktorauthentifizierung bis hin zu Hochsicherheitmaßnahmen mit Kryptoverschlüsselung.

Das wird aber für die Zukunft nicht ausreichen. Die aktuelle Herausforderung liegt in der enormen Leistung zukünftiger Quantencomputer, die das gesamte Sicherheitsbild verändern werden. Dies erfordert einen Wechsel von der aktuellen Verschlüsselungstechnologie zu einer neuen Hochsicherheitstechnologie. Daher sind wir in internationale Forschungsprojekte eingebunden. Aktuell testen wir bereits Quantenkommunikation in realen Bedingungen, um hohe Sicherheitsstandards zu gewährleisten. Post-Quanten-Kryptografie (PQC) und Quantum-Key-Distribution (QKD)-Know-how werden in der Organisation aufgebaut.

> **Es ist wichtig, sich ständig weiterzuentwickeln, da sich Bedrohungen schnell ändern.**
>
> Hermann Kaponig

Es gibt einen dringenden Aufruf, gegen Desinformation und Deepfakes vorzugehen, die als hybride Bedrohungen eingesetzt werden. Deepfake-Betrugsfälle haben in den letzten Jahren stark zugenommen. Gibt es rechtliche Lücken, die die Strafverfolgung behindern? Haben wir die Technologie, um solche Fälle zu erkennen, oder fehlt uns diese derzeit?
Andreas Holzer: Deepfake-Technologien, ob Bilder, Videos oder Sprachaufzeichnungen, werden zunehmend für Betrug genutzt. Es gibt viele leicht zugängliche Programme, die solche Manipulationen ermöglichen. Ein Beispiel ist der Internetbetrug, bei dem Prominente wie der Bundespräsident für betrügerische Investmentseiten verwendet werden. Auch Cybermobbing nimmt zu, mit KI-manipulierten Bildern, die ohne Zustimmung verbreitet werden. Es gibt rechtliche Lücken, da Kriminalität und Technologie sich ständig weiterentwickeln. Ermittlungen sind schwierig, da der Vorsatz der Täter:innen nachgewiesen werden muss. Die Polizei arbeitet mit großen Plattformen zusammen, um illegale Inhalte frühzeitig zu verhindern. Der Digital Services Act bietet Möglichkeiten, illegale Inhalte schneller zu melden. Internationale Zusammenarbeit ist entscheidend, da Täter:innen oft grenzüberschreitend agieren. Europol spielt eine zentrale Rolle im Kampf gegen Cyberkriminalität und hybride Bedrohungen. Die Joint Cyber Crime Action Task Force (J-CAT) bei Europol koordiniert länderübergreifende Ermittlungen. Kürzlich wurde unter deutscher Führung die pädophile Plattform „Kit Flix“ zerschlagen, wobei auch Österreich beteiligt war. Internationale Kooperation ist unerlässlich.

Es ist wichtig, das Bewusstsein für Desinformationskampagnen und gezielte Beeinflussung zu schärfen, um sich davor zu schützen. Das Bundesheer arbeitet an Tools zur Erkennung von Propagandanarrativen, die über KI hinausgehen und Destabilisierung verhindern sollen. Können diese Technologien skaliert werden, um besser vor solchen Angriffen zu schützen?
Hermann Kaponig: Wir erleben tagtäglich Desinformationskampagnen und bereiten uns auch

für den Einsatz in militärischen Auseinandersetzungen darauf vor. Das Bundesheer baut dazu neue Fähigkeiten und Strukturen auf, indem es eine „Strategische Kommunikation" auf militärstrategischer Ebene etabliert und die Fähigkeit zu Informationsoperationen auf operativ taktischer Ebene entwickelt. Dabei gewonnene Erfahrungen könnten auf gesamtstaatlicher Ebene genutzt werden.

Österreich ist zudem am Rapid Alert System (RAS) der EU beteiligt, das die Koordinierung gegen Desinformation verbessert und den Austausch über eine verschlüsselte Plattform ermöglicht.

Das Bundeskriminalamt legt im Regierungsprogramm einen Schwerpunkt auf die Erkennung von Desinformationskampagnen. Gibt es Datenquellen aus sozialen Medien, dem Darknet oder Foren, die fusioniert werden können, um Unternehmen zu schützen und Kampagnen frühzeitig zu erkennen?
Andreas Holzer: Wir müssen Betreiber in die Pflicht nehmen und fortschrittliche Analysemethoden wie Natural Language Processing, Machine Learning und Netzwerkanalysen nutzen, um Muster und Anomalien zu erkennen, die auf Desinformationskampagnen hinweisen. Dabei ist es wichtig, die Privatsphäre und Meinungsfreiheit zu respektieren und die Analyse im Einklang

> **Erfolgreiche Ermittlungen sind möglich, wenn alle Beteiligten zusammenarbeiten.**
>
> Andreas Holzer

mit rechtlichen Bestimmungen durchzuführen. Es ist sinnvoll, soziale Medien, Online-IDs, Nachrichtenartikel, Darknet-Foren und Kommentarbereiche zu überwachen, um solche Kampagnen frühzeitig zu erkennen.

Im Kontext geopolitischer Konflikte geraten kritische Infrastrukturen wie Energieeinrichtungen stärker in den Fokus. Übt das österreichische Bundesheer in Kooperation mit Unternehmen und kritischen Einrichtungen, um Angriffsszenarien zu bewältigen und sich vor solchen Angriffen zu schützen?
Hermann Kaponig: Das ÖBH übt regelmäßig den Schutz kritischer Infrastrukturen und profitiert von der hervorragenden Zusammenarbeit innerhalb Österreichs.

Die Zuständigkeiten sind klar. Das Innenministerium ist im Normbetrieb und bei Cyberkrisen federführend zuständig, das Verteidigungsministerium im Rahmen der Militärischen Landesverteidigung.

Um Bedrohungen abzuwehren, führt das Bundesheer einerseits selbst Übungen durch und nimmt andererseits an gesamtstaatlichen Übungen gemeinsam mit österreichischen Stromnetzbetreibern teil.

2024 waren wir z. B. mit unserem „Militärischen Cyberzentrum" in der Schweiz, um gemeinsam mit Expert:innen aus den Bereichen Finanzen und kritischer Infrastruktur an einer großen internationalen Cyber-Übung teilzunehmen. Auch beteiligt sich das ÖBH laufend an internationalen Übungen wie der „Locked Shields". Dabei arbeiten unsere Expert:innen Hand in Hand mit Miliz-Expert:innen und Vertreter:innen der kritischen Infrastruktur zusammen.

Der Cybercrime Report zeigt, dass 58 % der analysierten Angriffe mit staatlich geduldeten oder unterstützten Akteur:innen verbunden sind. Wie kann man diese Unterscheidung praktisch umsetzen? Und was können Unternehmen tun, um die Wahrscheinlichkeit solcher Angriffe zu verringern?
Andreas Holzer: In Österreich funktioniert die Zusammenarbeit zwischen dem Verteidigungs- und Innenministerium sehr gut, was auch der Kleinheit des Landes und dem Zugang der Akteur:innen geschuldet ist. International ist das nicht überall so. Die Unterscheidung zwischen kriminellen und geopolitisch motivierten Angriffen, insbesondere im Bereich Ransomware, ist komplex, da die Grenzen oft verschwimmen. Kriminelle Angriffe sind finanziell motiviert und zielen auf Unternehmen ab, während geopolitische Angriffe kritische Infrastrukturen und strategisch wichtige Einrichtungen betreffen. Staatliche Akteure können kriminelle Gruppen anheuern, was die Unterscheidung weiter erschwert. Das Bundeskriminalamt nutzt verschiedene Methoden, um Angriffe zuzuordnen, wobei die Grenzen oft verschwimmen.

Die EU-Cybersolidaritätsverordnung, die im Dezember verabschiedet wurde, zielt darauf ab, die Resilienz und Reaktionsfähigkeit gegenüber Cyberangriffen zu stärken und das Krisenmanagement in allen Mitgliedstaaten zu fördern. Wie bewerten Sie die Umsetzung dieser Verordnung in Österreich, insbesondere in Bezug auf die Zusammenarbeit zwischen den Behörden und die Rolle der EU-Agentur für Cybersicherheit, ENISA?
Hermann Kaponig: Die Zusammenarbeit auf europäischer Ebene ist hervorragend, mit vielen Aktivitäten und Rahmenbedingungen wie der NIS-Richtlinie, dem Cybersecurity Act und an-

> **In modernen Konflikten beginnen militärische und politische Maßnahmen oft im Cyber- und Informationsraum.**
>
> Hermann Kaponig

deren. Diese zivilen Richtlinien und Absichten werden weitgehend umgesetzt. Im militärischen Bereich entwickelt die EU eine Cyber Defense Coordination Cell, die bis Jahresende eine stehende Struktur für den militärischen Informationsfluss und das Bedrohungsmanagement bilden wird. Diese Maßnahmen sind richtungsweisend und zivilorientiert, was wir sehr begrüßen. Wir planen, dauerhaft Personal in Brüssel abzustellen, da dies der zentrale Informationshub für die militärische Cyberabwehr in Europa wird.

Im Regierungsprogramm wird die Einrichtung einer eigenen Teilstreitkraft für Multidomain-Operationen, die Cyber- und Informationsraum umfasst, erwähnt. Warum ist das aus Ihrer Sicht wichtig und was steckt dahinter? Was soll damit erreicht werden?
Hermann Kaponig: In modernen Konflikten beginnen Maßnahmen oft bereits im Cyber- und Informationsraum, bevor kinetische Mittel eingesetzt werden. Dafür benötigt man entsprechende performante Fähigkeiten.

Das Bundesheer entwickelt im Zuge der Maßnahmen zum Aufbauplan und Zielbild ÖBH2032 mit dem „Cyber Information Domain Component Command" (CyIDCC) eine eigene Teilstreitkraft für den Cyberraum, Informationsraum, Elektromagnetischen Raum und für Services im Weltraum.

Damit wird Cyber und Information als Domäne den anderen Teilstreitkräften wie Land, Luft und Spezialkräfte gleichgesetzt. Eine hybride Auseinandersetzung ist heutzutage nur mehr im engsten Zusammenwirken aller dieser Domänen vorstellbar. Die Cyber- und Informationskräfte sind damit nicht nur Unterstützungstruppe, sondern auch Kampftruppe.

Der Aufbau umfasst die Strukturierung des CyIDCC und gleichzeitig den Aufbau hochmobiler Cybereinheiten für Einsätze im In- und Ausland, um im Rahmen von domänenübergreifenden Operationen einen entscheidenden Beitrag zu leisten.

Diese neue Teilstreitkraft wird dabei voll in den Führungsprozess integriert, um ein gemeinsames Lagebild zu schaffen, die Prozesse massiv zu beschleunigen und damit militärische Ziele zu erreichen.

Unterschiedliche Zielgruppen und Altersgruppen erfordern unterschiedliche Maßnahmen. Was brauchen wir, um Menschen auf neue Bedrohungen wie Desinformation, Deepfakes und Cybercrime vorzubereiten und zu sensibilisieren?
Andreas Holzer: Das Regierungsprogramm verweist auf den Digital Services Act und den Digital Market Act, die wir als Kriminalpolizei in Österreich unterstützen. Diese Acts sind wichtig, da wir auf nationaler Ebene nicht in der Lage sind, internationalen Dienstanbietern Verpflichtungen aufzuerlegen. Europäische Lösungen und internationale Zusammenarbeit sind notwendig, um illegale oder kompromittierende Inhalte schnell zu entfernen und den Schaden zu minimieren. Das hat einen präventiven Effekt, indem es Täter:innen die Möglichkeit nimmt, Inhalte zu verbreiten. Das Bundeskriminalamt und die Kriminalpolizei setzen auf Prävention und stärken die Medienkompetenz der Bevölkerung, insbesondere der Jugend. Wir informieren gezielt, um die Menschen zu sensibilisieren und sie vor Täter:innen zu schützen. Dabei kooperieren wir mit verschiedenen Stellen, wie Safer Internet und NGOs,

> **Die Unterscheidung von Ransomwareangriffen ist komplex, da die Grenzen oft verschwimmen.**
>
> Andreas Holzer

sowie mit der Wirtschaftskammer und dem Handelsverband.

Welche Maßnahmen wären angesichts des Fachkräftemangels von über 8.700 Expert:innen im Bereich IT-Sicherheit in Österreich, wie im Regierungsprogramm 2025–2029 beschrieben, notwendig, um diese Lücke bis 2026 zu schließen?
Hermann Kaponig: Diese Herausforderung kurzfristig zu lösen, ist aus meiner Sicht nicht machbar. Hier sind mittel- und langfristige Maßnahmen notwendig, die einer klaren gesamtstaatlichen Strategie folgen sollten.

Dafür wären klare strategische Ziel zu definieren und entsprechende Ressourcen zuzuordnen. Im Bereich der „Digital Awareness“ an den Schulen wären die Aktivitäten für das Lehrpersonal und die Schüler:innen zu intensivieren. Die MINT-Fächer auf Ebene der Fachschulen, HTLs, Fachhochschulen und Technischen Universitäten wären stärker zu bewerben.

Die Ausbildungskapazitäten an den Bildungseinrichtungen und universitären Einrichtungen wären zu erhöhen. Dazu braucht es wohl einerseits mehr Personalressourcen beim Lehrpersonal und andererseits mehr Infrastrukturmaßnahmen für mehr Klassen und Lehrsäle. Die Lehrlingsausbildung sowie Umschulungsprogramme für den Fachbereich wären auszubauen.

Last but not least sollte man auch qualifizierte Zuwanderung von IT-Expert:innen fördern.

Andreas Holzer: Von Seiten der Polizei ist es wichtig, interne Maßnahmen zur IT-Ausbildung zu forcieren. Darüber hinaus müssen wir junge Fachkräfte schon sehr früh motivieren, sich für den Polizeiberuf oder den Verwaltungsdienst im BMI zu begeistern. Derzeit haben wir eine Kooperation mit den sogenannten „CyberHAKs“ in Tamsweg, Horn und an der Vienna Business School in Floridsdorf. Hier werden junge Kräfte auf Cybersecurity und die Bekämpfung von Cybercrime vorbereitet – um sie dann hoffentlich für eine entsprechende Tätigkeit zu rekrutieren.

> **Wir üben regelmäßig den Schutz kritischer Infrastrukturen und profitieren von der guten Zusammenarbeit in Österreich.**
>
> Hermann Kaponig

Wenn wir uns in einem Jahr wieder treffen, was würden wir uns wünschen, bereits heute getan zu haben?
Andreas Holzer: Das ist tatsächlich eine sehr schwierige Frage. Ich habe bereits erwähnt, dass ich ein großer Befürworter des Beamtentums in Österreich bin und auch der zukunftsorientierten Kräfte, die bei uns aktiv sind. Wir denken schon jetzt an die Zukunft, obwohl es Rahmenbedingungen gibt, die uns Herausforderungen bereiten. Dennoch bin ich überzeugt, dass wir in einem Jahr viel erreicht haben werden. Ich habe keine Wünsche, sondern konkrete Pläne, die wir umsetzen. Ein wesentlicher Faktor für mich ist die Bekämpfung von Cyberkriminalität, die hoffentlich in der geplanten Form umgesetzt wird.

Ich bin zuversichtlich, dass wir in Österreich in einem Jahr in diesem Bereich einen Schritt weiter sein werden.

Hermann Kaponig: Wir sind grundsätzlich auf einem sehr guten Weg, der aufbauend auf gediegene Planungen die Zielsetzungen unseres Aufbauplanes ÖBH2032+ verfolgt. Dazu gehört u. a. auch der weitere strukturelle Ausbau unseres „Militärischen Cyberzentrums“ (MilCyZ).

Wenn wir hier die organisatorischen Rahmenbedingungen haben, können wir auch die Aufstellung von eigens strukturierten „Cyber Rapid Response Teams“ (CRRT) sicherstellen. Diese Teams wären eine Art Cyber-Feuerwehr, die jederzeit rasch für Einsätze im In- und Ausland verfügbar wäre.

Eines dieser Teams sollte zudem auch in einer Doppelrolle für militärische und gesamtstaatliche Aufgaben verfügbar sein.

Schutz und Sicherheit im digitalen Zeitalter

Im Gespräch mit **Reinhard Ruckenstuhl** erhalten wir Einblicke in die Strategien des Abwehramtes zum Schutz der Sicherheit des österreichischen Bundesheeres und der Infrastruktur. Er erläutert die proaktiven Maßnahmen und internationalen Kooperationen, die erforderlich sind, um Bedrohungen frühzeitig zu identifizieren und abzuwehren.

Welche Aufgaben und Rollen übernimmt das Abwehramt im Schutz des österreichischen Bundesheeres und in der nationalen Sicherheit?
Reinhard Ruckenstuhl: Das Abwehramt hat die Aufgabe, Bedrohungen für militärische Rechtsgüter wie Personen, Infrastruktur, Waffen, Geräte, Informationen und militärische Geheimnisse zu vermeiden. Dies erfordert proaktives Handeln, um potenzielle Bedrohungen frühzeitig zu erkennen und zu bekämpfen. Das Abwehramt arbeitet in den Phänomenbereichen Extremismus, Terrorismus, Spionage und Cyberbedrohungen, sowohl national als auch international. Es tauscht Informationen mit dem Heeresnachrichtenamt und der Direktion für Staatsschutz und Nachrichtendienst aus, um ein umfassendes Lagebild zu erstellen. Im Bereich Cybersecurity ist das Abwehramt nachrichtendienstlich tätig und zertifiziert alle IT-Systeme im BMLV und entsprechend auch bei Firmen, sofern sie im Verteidigungssektor tätig sind. Sensibilisierung und Bewusstseinsbildung sind ebenfalls wichtige Aufgaben, um Unternehmen auf die Spielregeln der Sicherheit aufmerksam zu machen.

Das Abwehramt ist auch für die Sicherheitsakkreditierung von Informations- und Kommunikationssystemen zuständig. Warum braucht es diese Akkreditierung und wie können Unternehmen im Hinblick auf die Sicherheit ihrer IKT-Systeme davon profitieren?
Reinhard Ruckenstuhl: Wir unterstützen Unternehmen bei der Sicherheitsbetreuung und bei Clearances im internationalen Bereich. Diese Unterstützung ist notwendig, wenn ein Unternehmen überprüft wird, insbesondere wenn es um die IT und die Verarbeitung klassifizierter Daten geht. Firmen profitieren davon, indem sie in unsere Sicherheitsbetreuung aufgenommen werden. Einmal im Jahr werden Bedrohungen und Risiken, auch im IT-Bereich, für alle Firmen über zwei Tage hinweg analysiert und Best Practices geteilt. Unternehmen können daraus wertvolle Erkenntnisse gewinnen. Es gibt einen kontinuierlichen und engen Informations- und Erfahrungsaustausch. Dies ist relevant, wenn ein Unternehmen ein klassifiziertes System betreibt oder im Rüstungsbereich tätig ist.

Laut dem Risikobild 2025 hat sich die Bedrohungslage im Cyberraum erheblich verändert. Welche Entwicklungen beobachten Sie hier, und welche Akteur:innen spielen eine zentrale Rolle?
Reinhard Ruckenstuhl: Wir beobachten eine Zunahme von Angriffen durch staatliche und staatlich unterstützte Akteur:innen, erkennbar an der Professionalität ihrer Vorgehensweise. Der Hauptanteil dieser Angriffe liegt weiterhin auf kriminellen Aktivitäten mit Schädigungsabsicht. Ein weiterer Aspekt ist die gezielte Informationsabschöpfung, die nicht nur den militärischen Bereich betrifft, sondern auch Wissenschaft, Wirtschaft und Forschung. Unternehmen werden gezielt angegriffen, um herauszufinden, ob sie anfällig sind. Die klassischen Angriffsvektoren wie Spear Phishing, Passwort Spraying und der Zugriff über externe Systeme bleiben dabei relevant.

In unserer Studie geben viele der befragten Unternehmen an, dass sie Versuche von Social-Engineering-Angriffen über berufliche oder private

FOTO © PRIVAT

Generalmajor Mag. Reinhard Ruckenstuhl, MAS ist seit Jänner 2020 Leiter des Abwehramtes des österreichischen Bundesheeres. Zuvor war er im Kosovo tätig, wo er als stellvertretender Kommandant der NATO Operation fungierte.

Cyberangriffe sind mittlerweile gesellschaftsfähig und betreffen uns alle.

soziale Netzwerke erfahren haben. Der private Bereich gewinnt immer mehr an Bedeutung. Auch Deepfakes sind auf dem Vormarsch. Welche spezifischen Herausforderungen sehen Sie dadurch für Österreichs Unternehmen?
Reinhard Ruckenstuhl: Die Entwicklungen im Bereich Social Engineering sind nachvollziehbar, da die Grenzen zwischen beruflichen und privaten Bereichen zunehmend verschwimmen. Berufliche Informationen werden häufiger auch im privaten Umfeld ausgetauscht, was Angriffe erleichtert, denn es ist einfach, eine Verbindung zwischen einer Person und ihrer beruflichen Tätigkeit oder ihrem Unternehmenshintergrund herzustellen. Staatliche Akteure sind technisch gut aufgestellt, um hier gezielte Angriffe durchzuführen. Deepfakes zielen auf den:die Nutzer:in ab und werden immer besser, was die Erkennung erschwert. Unternehmen sollten ihre Mitarbeiter:innen sensibilisieren und auf Risiken hinweisen, ohne dabei zu wissenschaftlich zu werden. Es ist wichtig, dass Nachfragen gesellschaftsfähig wird und dass das Thema Cybersicherheit unternehmensweit behandelt wird.

Unternehmen stehen zunehmend im Fokus von Cyberangriffen durch staatliche und staatlich unterstützte Akteur:innen. Welche Strategien aus dem militärischen Bereich könnten Unternehmen helfen, ihre Resilienz gegen solche Angriffe zu stärken?

> **Es reicht nicht aus, sich auf Versicherungen zu verlassen.**

Reinhard Ruckenstuhl: Man sollte Datensicherung als einen wichtigen, wenn auch technisch nicht besonders herausfordernden Bereich betrachten. Trotz der Kosten kann eine zuverlässige Datensicherung innerhalb eines akzeptablen Zeitrahmens viel bewirken und hilft, Herausforderungen gelassener zu begegnen. Zudem ist es wichtig, dass Unternehmen ihre Systeme analysieren, um zwischen Kern-, Ergänzungs- und Peripheriesystemen zu unterscheiden. Auf dieser Grundlage kann der Schutzstatus festgelegt werden, wobei die zentralen Systeme identifiziert werden, die für die Aufrechterhaltung der Kernfunktionalität entscheidend sind. Es geht darum, das „Haus" so zu bauen, dass es sicher ist.

Wie bewerten Sie die aktuellen Entwicklungen und welche Ableitungen gibt es daraus für österreichische Unternehmen in Bezug auf Schwachstellen und Potenziale zur Verbesserung? Sind wir ausreichend auf die Risiken der zunehmenden Digitalisierung vorbereitet, und kommunizieren wir unsere Erfolge im Bereich der Cybersicherheit ausreichend?
Reinhard Ruckenstuhl: Jede:r nimmt die Risiken der Digitalisierung aus seiner:ihrer eigenen Perspektive wahr, was zu unterschiedlichen Einschätzungen führt. In den letzten Jahren wurden viele Initiativen gestartet, um die Zusammenarbeit zu verbessern und die Kräfte zu bündeln. Obwohl wir uns der Risiken bewusst sind und viel Wissen vorhanden ist, bleibt die Frage, ob wir wirklich ausreichend vorbereitet sind, da nicht alle Bedrohungen bekannt sind. Kommunizieren wir unsere Erfolge ausreichend? Wahrscheinlich nicht, und das sollten wir ändern. Die Sicherheitsstruktur muss stärker betont werden, aber das entbindet niemanden von seiner:ihrer persönlichen Verantwortung. In Analogie sollte man auch nicht denken, dass man durch einfache Maßnahmen wie das Tragen eines Helms oder das Überqueren eines Zebrastreifens völlig sicher ist. Es reicht nicht aus, sich auf Versicherungen zu verlassen und nichts weiter zu tun. Das ist der falsche Ansatz.

Wie wichtig ist aus Ihrer Sicht eine verstärkte Public-Private-Partnership im Bereich Cybersicherheit? Welche Maßnahmen könnten dazu beitragen, das Vertrauen zwischen staatlichen Stellen und Unternehmen zu stärken?
Reinhard Ruckenstuhl: Es findet bereits ein reger Austausch mit vielen Organisationen statt, da das Grundinteresse überall gleich ist: Die Organisation soll effektiv funktionieren. Der Austausch ist definitv zielführend, und es geht nicht um firmeninterne Daten, sondern darum, funktionale Abhängigkeiten zu erkennen. Funktionalitäten im Sinne der Digitalisierung können nur gemeinsam geschaffen werden, und das Militär ist hier aufgeschlossener, als man denkt. Vertrauen entsteht durch vertrauensbildende Maßnahmen. Gemeinsame Interessen unter Wettbewerbern zu definieren und eine bessere Kommunikation können hilfreich sein. Cyberangriffe sind mittlerweile gesellschaftsfähig und betreffen jede:n, unabhängig von den getroffenen Sicherheitsmaßnahmen. Man könnte damit offener umgehen.

Die IKT-Sicherheitskonferenz, eine Veranstaltung die federführend vom Abwehramt organisiert und schon seit vielen Jahren durchgeführt wird, hat sich als führende Plattform für den Austausch zum Thema Informations- und Cybersicherheit etabliert. Was macht diese Veranstaltung aus Ihrer Sicht so erfolgreich?
Reinhard Ruckenstuhl: IKT-Sicherheit ist seit Jahrzehnten ein zentrales Thema für das Militär, und der Austausch mit anderen Stellen, wie der FH OÖ und Cyber Security Austria, hat sich als vorteilhaft erwiesen. Das Militär ist nicht nur Anbieter, sondern auch Bedarfsträger geworden. Die Veranstaltung hat sich von einem Seminar zu einer anerkannten Konferenz entwickelt und ist die größte ihrer Art im deutschsprachigen Raum. Der Erfolg der Veranstaltung liegt in ihrem einfachen und offenen Zugang sowie ihrer hohen Qualität und einem breiten Themenspektrum.

Die Austria Cyber Security Challenge ist ein Erfolgsprojekt zur Förderung junger IT-Talente in Österreich, das vom Bundesheer gemeinsam mit Cyber Security Austria initiiert wurde. Wie wichtig ist diese Initiative für die langfristige Cybersicherheit des Landes? Welche Erfolge konnten bisher erzielt werden?
Reinhard Ruckenstuhl: Die Veranstaltung dient als Plattform, um junge Menschen für IT und IT-Sicherheit zu begeistern. Der bekannte Mangel an IT-Fachkräften in Österreich macht solche Initiativen wertvoll, da sie helfen, die Scheu vor einer beruflichen Laufbahn in diesem Bereich zu überwinden. Der große Vorteil der Security Challenge ist, dass sie den Teilnehmer:innen ein breites Spektrum an Kontakten bietet und sie als Multiplikatoren fungieren können. Je mehr Menschen teilnehmen, desto größer wird das Netzwerk. Dieses Erfolgsmodell „Made in Austria" läuft nun schon im internationalen Rahmen und hat bereits auch einmal die „European Challenge" nach Österreich geholt.

Die Cybersicherheit entwickelt sich ständig weiter – sowohl in Bezug auf Bedrohungen als auch auf Technologien zur Abwehr dieser Angriffe. Wie sehen Sie die Entwicklung der Cybersicherheit in Österreich bis 2030? Welche Trends oder Technologien werden besonders wichtig sein?
Reinhard Ruckenstuhl: In den kommenden Jahren wird Künstliche Intelligenz vermehrt sowohl Chancen als auch Risiken mit sich bringen. Selbstlernende Systeme haben großes Potenzial, doch ihre zukünftige Entwicklung ist schwer abzuschätzen. Ein Vergleich: Von den 11.000 Satelliten im Orbit wurden 7.000 in den letzten Jahren gestartet, und niemand weiß, ob die Entwicklung linear bleibt oder neue Möglichkeiten eröffnet. Die Dimensionierung ist komplex, da Ideen und Werkzeuge vorhanden sind, aber ihre konkrete Ausformulierung unklar ist.

KI sollte positiv gesehen werden, da sie großes Entwicklungspotenzial bietet. Die Herausforderung liegt darin, wie sie sich weiterentwickelt und wie wir damit umgehen. Letztlich geht es darum, wie der Mensch mit diesen Veränderungen umgeht.

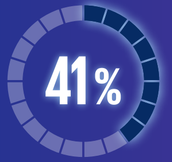
Wenn wir uns in einem Jahr wieder treffen, was würden wir uns dann wünschen, heute schon getan zu haben?
Reinhard Ruckenstuhl: Als Pragmatiker denke ich, dass wir uns nächstes Jahr fragen werden, warum wir einer Organisation nicht rechtzeitig gesagt haben, dass sie ihre Daten sichern oder ihr IT-System richtig aufstellen soll. Warum haben wir es zu spät erkannt? Es wird jemanden treffen.

03

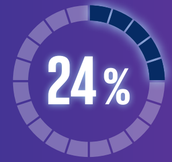
Was waren die Folgen?

Wir haben gelernt, dass nach wie vor keine Entspannung der Lage in Sicht ist. Cyberangriffe haben weitreichende Konsequenzen und können Unternehmen personell, finanziell und zeittechnisch einiges abverlangen. Von hohen Schadenssummen und Betriebsunterbrechungen über Lösegeldforderungen bis hin zu Datendiebstahl und Social Engineering. Richten wir unser Augenmerk nun auf die Folgen von Cyberattacken, mit denen heimische Unternehmen im letzten Jahr zu kämpfen hatten.

der Unternehmen **hatten Schäden durch Cyberangriffe** in Form von Kosten für Ermittlungen und Ersatzmaßnahmen.

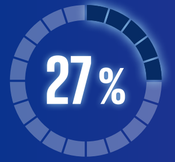


Für 41 % ist die **technische Integration** von veralteten OT-Technologien mit modernen IT-Systemen die größte Herausforderung für die Absicherung der OT-Systeme.



der **Social-Engineering-Versuche** laufen über Bewerbungen auf Stellenanzeigen.

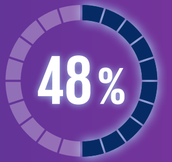
Sabotage ist einer der am wenigsten betrachteten Schäden, die aber dennoch gegenüber dem Vorjahr um 10 % zugenommen haben.



Bei 27 % der Befragten hat die **Dauer der Aufarbeitung** eines Cybersecurity-Vorfalls weniger als 24 Stunden gedauert.

Phishing als Einfallstor für Datendiebstahl hat um 20 % zugenommen.

Jeder 10. **Social-Engineering-Versuch nutzt bereits Deepfake** für Sprach- und Videonachrichten.



Fast jeder zweite **Social-Engineering-Versuch** kommt über Messengerdienste.

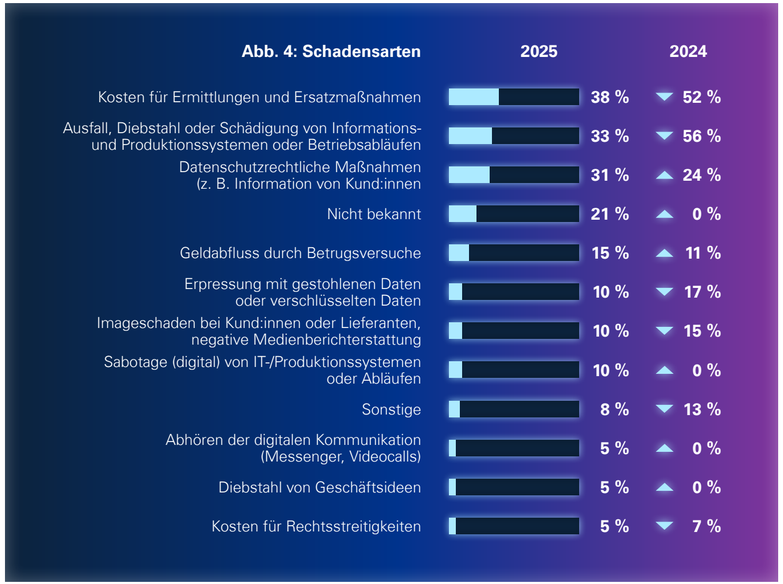
Schadensarten

Blicken wir nun auf die Schäden, die im Zusammenhang mit Cyberangriffen bei heimischen Unternehmen entstanden sind, so sehen wir, dass an erster Stelle die Kosten für die Ermittlungen und Ersatzmaßnahmen mit 38 Prozent dominieren.

Auf Platz zwei liegt mit 33 Prozent der Ausfall und Diebstahl oder die Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen. Gerade hier zeichnet sich umso mehr ab, dass Cyberangriffe kein rein technologisches Thema mehr sind, sondern es sich um ein unternehmensweites Problem handelt. Es kommt zu Beeinträchtigungen der Betriebsabläufe und in weiterer Folge geht es hier um die Existenzbedrohung von Unternehmen, sollten längerfristige Ausfälle die Konsequenz sein.

An dritter Stelle stehen datenschutzrechtliche Maßnahmen, die als Schäden entstanden sind, mit 31 Prozent. In diesem Zusammenhang geht es oftmals darum, dass Informationen von Kund:innen abhandengekommen sind bzw. eine Verletzung von personenbezogenen Daten stattgefunden hat. Ebenfalls interessant zu beobachten: 10 Prozent der befragten Unternehmen haben Sabotage (digital) von IT-/Produktionssystemen oder Abläufen genannt. Diese Schadensart hat im Vergleich zum Vorjahr um 10 Prozent zugenommen. Sabotage ist somit eine der am wenigsten betrachteten Schäden, die aber dennoch stark angewachsen ist.

Abb. 4: Schadensarten



Jedes fünfte Unternehmen kann nicht benennen, welche Schäden im Zusammenhang mit Cyberangriffen entstanden sind. Gerade in Zeiten, in denen die Digitalisierung immer mehr Überhand gewinnt und für die Existenz von Unternehmen von Bedeutung ist, damit sie im internationalen Wettbewerb bestehen können, ist es doch sehr überraschend, dass Schäden nicht benannt werden können. Dies wird umso prekärer, da Unternehmen vor allem durch die Regulatorik gefordert sind, Risiken aus Cyberangriffen zu qualifizieren und zu quantifizieren, um geeignete Maßnahmen ableiten zu können. Die Schäden aus Cyberangriffen müssen im Verhältnis zu den gesetzten Abwehrmaßnahmen stehen und können auch ein Argument dafür bilden, wie viel Unternehmen in den Schutz ihrer digitalen Technologien investieren wollen. Hier gibt es großen Aufholbedarf.

Finanzieller Schaden

Fragt man Unternehmen nach der Höhe des finanziellen Schadens und der Kosten für die Aufarbeitung, die sie durch Cyberangriffe in den letzten 12 Monaten hatten, so erhält man ein differenziertes Bild. Vor allem eine Aufschlüsselung der Verteilung der finanziellen Schäden sowie der Vergleich der Jahre 2024 und 2025 zeigen interessante Veränderungen in der Risikolandschaft.

Geringfügige Schäden (< EUR 1.000): Der Anstieg von 24 Prozent (2024) auf 30 Prozent (2025) deutet auf eine Zunahme kleinerer, möglicherweise automatisierter Angriffe hin, die zwar eine große Anzahl von Unternehmen betreffen, aber einzeln betrachtet geringe Schäden verursachen. Phishingangriffe oder automatisierte Malware-Infektionen könnten dahinterstecken.

Mittlere Schäden (EUR 1.001–50.000): In dieser Kategorie gab es einen Rückgang (z. B. EUR 1.001–5.000 von 14 Prozent auf 8 Prozent und EUR 10.001–50.000 von 12 Prozent auf 8 Prozent). Gründe dafür könnten sein, dass Unternehmen effektivere Schutzmaßnahmen implementiert haben oder aber auch, dass sich die Angreifer:innen auf höherwertige Ziele konzentrieren.

Höhere Schäden (EUR 100.001–1 Mio.): Der Anstieg von 4 Prozent im Vorjahr auf 7 Prozent in diesem Jahr zeigt, dass es also durchaus auch existenzbedrohende Angriffe gab. Unternehmen dürfen das nicht unterschätzen und müssen ihre Cybersecurity-Strategien ausbauen.

Unbekannte Schäden: Der signifikante Anstieg jener Unternehmen, die keine Angaben zu den Schäden machen konnten (von 21 Prozent auf 28 Prozent), ist besorgniserregend. Das könnte auf mangelnde Transparenz bei der Erfassung von Cybersecurity-Vorfällen, unzureichende interne Reportingmechanismen oder eine Unterschätzung der tatsächlichen finanziellen Auswirkungen hindeuten.

Die finanziellen Auswirkungen von Cybersecurity-Vorfällen sind vielfältig und können sich erheblich auf die Rentabilität und den langfristigen Erfolg eines Unternehmens auswirken. Unternehmen müssen nach einem Cyberangriff mit direkten Kosten (Wiederherstellungskosten, Rechtsberatung, Strafzahlungen, Betriebsunterbrechungen und Umsatzeinbußen) sowie indirekten Kosten (Reputationsschäden, Opportunitätskosten aufgrund der Ressourcenbindung für den Cybersicherheitsvorfall und erhöhte Versicherungsprämien) rechnen.

Auch wenn die Anzahl derjenigen Fälle, die sehr hohe Schadenssummen hatten, nicht dominiert, so zeigt sich dennoch, dass Cyberangriffe signifikante Auswirkungen haben können. Eine gezielte Vorbereitung sowie das Treffen finanzieller Vorsorgemaßnahmen sind essenziell, um im Falle eines Falles gewappnet zu sein. Ob diese finanziellen Absicherungen über Cyberversicherung oder finanzielle Rücklagen erfolgen, ist jedem Unternehmen selbst überlassen. Wichtig ist hier

aber jedenfalls, diesen Aspekt in der Planung und den Risikoüberlegungen zu berücksichtigen. Die Analyse der Cybersecurity-Schadensdaten zeigt, dass Cybersecurity-Risiken für österreichische Unternehmen weiterhin bestehen. Eine proaktive und umfassende Cybersecurity-Strategie ist unerlässlich, um finanzielle Schäden zu minimieren und die langfristige Wettbewerbsfähigkeit zu sichern.

Die Folgen von Cyberangriffen sind ein teurer Weckruf für unzureichende Sicherheitsmaßnahmen.

Dauer der Aufarbeitung eines Cybersecurity-Vorfalls

Blickt man auf die Dauer der Aufarbeitung eines Cybersecurity-Vorfalls, so sieht man, dass Unternehmen durchaus besser werden. Bei 27 Prozent der Befragten hat die Aufarbeitung weniger als 24 Stunden Zeit in Anspruch genommen. Auf der anderen Seite gab es aber auch Vorkommnisse, die von längerer Dauer waren. So haben 15 Prozent der befragten Unternehmen zwischen ein und zwei Wochen und 10 Prozent drei bis vier Wochen benötigt, um Cybersicherheitsvorfälle aufzuarbeiten.

Ein signifikanter Anteil der Unternehmen (27 Prozent) konnte Cyberangriffe im Jahr 2025 innerhalb von weniger als 24 Stunden aufarbeiten, während im Jahr 2024 kein einziger Fall in dieser Kategorie verzeichnet wurde. Auch der Anteil der Unternehmen, die 1–2 Tage für die Aufarbeitung benötigten, ist mit 15 Prozent nennenswert.

Die Anteile der Unternehmen, die 3–6 Tage (von 23 Prozent auf 15 Prozent) oder 1–2 Wochen (von 33 Prozent auf 15 Prozent) für die Aufarbeitung benötigten, sind deutlich gesunken. Unternehmen sind möglicherweise besser gerüstet, um Angriffe schneller zu identifizieren und zu beheben. Die Aufarbeitungszeiten scheinen insgesamt kürzer zu werden.

Das ist ein positives Zeichen und könnte darauf zurückzuführen sein, dass Unternehmen möglicherweise effektivere Technologien und Prozesse einsetzen, um Cyberangriffe frühzeitig zu erkennen. Auch ihre Incident-Response-Teams sind möglicherweise besser geschult und verfügen über optimierte Verfahren, um Angriffe schnell einzudämmen und zu beheben. Der Einsatz von Automatisierungslösungen im Bereich der Cyberabwehr könnte dazu beitragen, Routineaufgaben zu beschleunigen und die Reaktionszeiten zu verkürzen.

Allerdings gibt es auch Aspekte, die Anlass zur Sorge geben: 14 Prozent der Unternehmen geben an, die Aufarbeitungsdauer nicht zu kennen. Dies könnte auf mangelnde Transparenz oder unzureichende Nachverfolgungsprozesse hindeuten. Es ist möglich, dass die schnelleren Aufarbeitungszeiten ein Indiz für eine Unterschätzung der tatsächlichen Auswirkungen von Cyberangriffen sind. Unternehmen konzentrieren sich auf die schnelle Wiederherstellung von Systemen, ohne dabei die Angriffsursachen vollständig zu analysieren und zu beheben.

Es traten jedoch auch Vorfälle in Erscheinung, die von längerer Dauer waren, und Unternehmen sieben bis acht Wochen bzw. sogar drei bis vier Monate für die Aufarbeitung gebraucht haben. Es zeigt sich einmal mehr, dass die Aufarbeitung durchaus lange Zeit in Anspruch nehmen kann. Gerade für diese Zeit bedarf es eines resilienten Krisenmanagements, um als Organisation vorbereitet und richtig aufgestellt zu sein. Es gilt die Durchhaltefähigkeit zu gewährleisten.

Herausforderungen der OT-Sicherheit im Kontext der IT-/OT-Konvergenz

Durch die zunehmende Integration von IT- und OT-Systemen kommt es zu hybriden Umgebungen, in denen unterschiedliche Technologielebenszyklen und Sicherheitsparadigmen aufeinanderprallen. Dadurch werden kritische Schwachstellen offenbart, die Unternehmen vor komplexe, teils existenzbedrohende Risiken stellen. Die Absicherung von OT erfordert einen Paradigmenwechsel weg von rein technischen Lösungen hin zu einem ganzheitlichen Ansatz, der technologische, organisatorische und regulatorische Maßnahmen miteinander verbindet.

Berichten zufolge hat eine in Asien ansässige Firma, die Roboterhunde herstellt, offenbar ein Backdoor (Hintertür) in selbigen vorinstalliert. Diese macht eine weltweite Überwachung von Kund:innen möglich. Jeder Person, die auf die öffentlich zugängliche Web-API gelangte, war es möglich, den Standort der Roboterhunde einzusehen.
War ein Roboterhund gerade online, konnten sogar Livecam Feeds abgerufen werden – einloggen war dafür nicht nötig. Wurden die standardmäßigen Raspberry-Pi-Zugangsdaten nicht geändert, war es Cyberkriminellen sogar möglich, den Roboterhund zu kontrollieren.[1]

[1] https://www.axios.com/2025/04/01/threat-spotlight-backdoor-in-chinese-robots-future-of-cybersecurity, abgerufen am: 15.04.2025

Technologische Heterogenität als Kernproblem

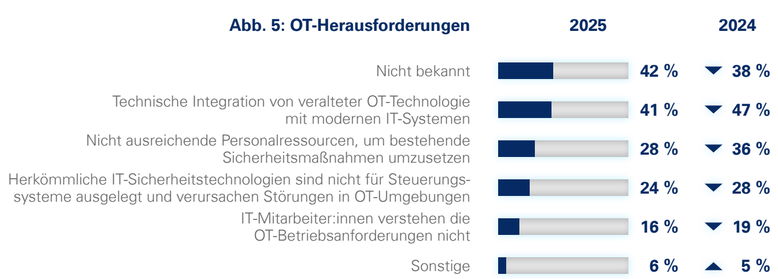
Ein zentraler Schmerzpunkt, den 41 Prozent der Unternehmen identifizieren, liegt in der Integration veralteter OT-Infrastrukturen in moderne IT-Architekturen. Während IT-Systeme durch kurze Innovationszyklen geprägt sind, operieren OT-Komponenten oft über eine Lebensdauer von mehr als 15 Jahren. Diese Systeme nutzen veraltete Protokolle, ungepatchte Betriebssysteme und bieten nur begrenzte Sicherheitsfunktionen. Das führt zu Inkompatibilitäten bei der Implementierung moderner Sicherheitskontrollen wie Endpoint-Detection-Lösungen oder Zero-Trust-Architekturen. Gleichzeitig entstehen unvorhergesehene Angriffsvektoren, denn bis dato isolierte OT-Systeme verlieren jetzt durch die Vernetzung mit IT-Netzen ihre traditionelle Abschottung („Air Gap"). Cyberkriminelle können so gezielt Schwachstellen in alternden OT-Komponenten ausnutzen, um in kritische Produktionsprozesse einzudringen.

Personelle und organisatorische Schwachstellen

28 Prozent der befragten Unternehmen sehen den Mangel an qualifizierten Fachkräften als weiteres Problem. Die Absicherung von OT-Umgebungen erfordert interdisziplinäres Wissen, das über klassische IT-Sicherheitskompetenzen hinausgeht. OT-Spezialist:innen müssen in der Lage sein, IT-Sicherheitskonzepte wie Netzwerksegmentierung oder Multi-Faktor-Authentifizierung auf industrielle Steuerungssysteme zu adaptieren, ohne dabei die Echtzeitanforderungen der Produktion zu gefährden. Gleichzeitig benötigen IT-Teams tiefgehendes OT-spezifisches Know-how, um Störungen kritischer Prozesse durch ungeeignete Sicherheitsmaßnahmen zu vermeiden. Die Schulung von Mitarbeitenden im Umgang mit IIoT (Industrial Internet of Things)-Geräten und der Absicherung von OT-spezifischen Protokollen bleibt eine Daueraufgabe, die aufgrund des Fachkräftemangels und der dynamischen Bedrohungslage kaum bewältigbar scheint.

Systemimmanente Risiken durch Sicherheitsmaßnahmen

Die Anwendung herkömmlicher IT-Sicherheitstools in OT-Umgebungen führt bei 24 Prozent der Unternehmen zu Betriebsunterbrechungen. Dafür verantwortlich sind strikte Echtzeitanforderungen industrieller Steuerungssysteme,



denn diese tolerieren keine Verzögerungszeiten durch Security Scans oder automatische Updates. Auch entstehen Zielkonflikte zwischen Safety- und Security-Anforderungen: Notfallzugriffe auf OT-Komponenten werden durch restriktive Zero Trust Policies oder Multi-Faktor-Authentifizierung behindert, was im Krisenfall lebensbedrohliche Folgen haben kann. Herkömmliche Sicherheitslösungen wie Firewalls oder Intrusion-Detection-Systeme sind zudem oft nicht in der Lage, OT-spezifische Angriffsmuster zu erkennen – etwa Manipulationen an speicherprogrammierbaren Steuerungen (SPS) oder Angriffe auf industrielle Kommunikationsprotokolle.

Regulatorische und lebenszyklusbedingte Schwachstellen

Der langsame Erneuerungszyklus von OT-Systemen erfordert alternative Schutzansätze, da klassische Patchmanagement-Strategien hier nicht anwendbar sind. Ein Ansatz liegt im Retrofitting bestehender Anlagen, bei dem OT-fähige Sicherheitskomponenten wie NAC (Network Access Control)-Lösungen nachgerüstet werden. Parallel bedarf es regulatorischer Innovationen: Analog zur technischen Überwachung physischer Anlagen nach § 57a könnten OT-Systeme verpflichtend auf Cyberresilienz geprüft werden – einschließlich Firmware-Integritätschecks, Protokollanalysen und Penetrationstests. Solche Prüfungen müssten neben mechanischen Komponenten auch digitale Sicherheitsaspekte abdecken, um Safety- und Security-Anforderungen konsistent abzubilden. Die Entwicklung branchenspezifischer OT-Security-Standards wie IEC 62443 muss beschleunigt werden, um eine harmonisierte Grundlage für Zertifizierungen und Audits zu schaffen.

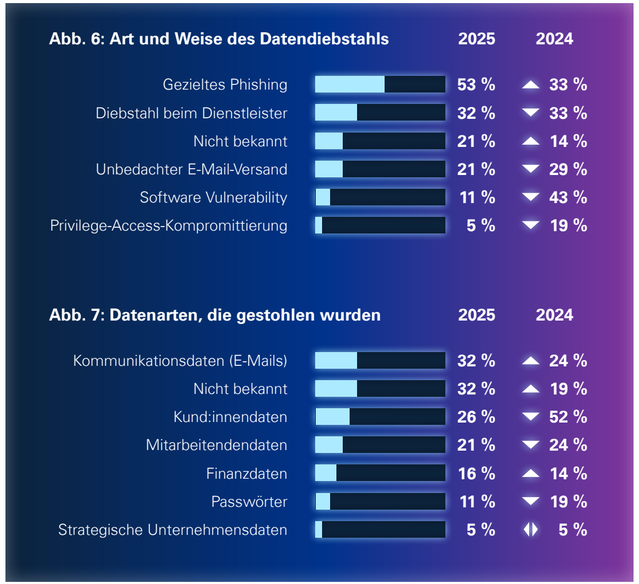
Weitere Herausforderungen bei OT-Systemen

Eine wesentliche weitere Herausforderung besteht für die Befragten darin, die Systeme auf dem neuesten Stand zu halten und eine klare Trennung zwischen IT und OT zu gewährleisten, was zunehmend schwieriger wird. Die Aufteilung der Verantwortung für die Absicherung zwischen IT und OT ist ebenfalls ein kritischer Punkt für die Befragten. Budgetbeschränkungen und mangelnde Unterstützung der Geschäftsleitung erschweren die Implementierung effektiver Sicherheitsmaßnahmen. Zudem fehlt oft der Überblick über alle OT-Umgebungen, und Mitarbeitende in OT-Bereichen sind sich der IT-Sicherheitsanforderungen und -maßnahmen häufig nicht ausreichend bewusst.

Zuständigkeiten im OT-Bereich

Wer ist bei den befragten Unternehmen für die Umsetzung der Sicherheitsmaßnahmen im Bereich der OT-Systeme/Industriesteuerungsanlagen verantwortlich? Aktuell gibt es bei heimischen Unternehmen noch keine eindeutige Tendenz dafür, wer die Verantwortung trägt: Bei 38 Prozent ist diese Zuständigkeit nicht eindeutig geregelt. Diese Verantwortung entsprechend festzumachen ist jedoch eine Notwendigkeit.

12 Prozent der befragten Unternehmen sehen die Verantwortung bei einer Stelle auf Unternehmensebene (CIO/CISO), 11 Prozent bei den Eigentümer:innen oder Betreiber:innen des Steuerungssystems und 10 Prozent bei der technischen Leitung. Durchaus spannend ist, dass immerhin 3 Prozent der Befragten die Verantwortung für das Thema Sicherheit bei den Herstellern oder Lieferanten der Anlage sehen. Es ist zwar grundsätzlich möglich, dass eine Verant-



wortlichkeit bei externen Personen liegen kann, dennoch bleibt die Endverantwortung immer bei den Unternehmern selbst.

Wie die Daten das Unternehmen verlassen haben

Datendiebstähle sind eines der häufigsten auftretenden Phänomene als Konsequenz von Cyberangriffen. Neben gesetzlichen Vorgaben, beim Verlust von Daten entsprechende Meldungen durchzuführen, ist es für Unternehmen von entscheidender Bedeutung, herauszufinden, auf welche Art und Weise die Daten das Unternehmen verlassen haben.

Die Zahlen unserer diesjährigen Studie zeigen, dass bei jedem zweiten Unternehmen gezieltes Phishing das Einfallstor war. Phishing hat um 20 Prozent zugenommen im Vergleich zum Vorjahr. Interessant ist auch, dass bereits an zweiter Stelle bei jedem dritten Unternehmen der Datendiebstahl über einen Dienstleister erfolgte. Das unterstreicht einmal mehr, dass die Lieferkette und in weiterer Folge das Risiko, das von Dritten ausgeht, an Bedeutung gewinnen und in den Fokus rücken müssen. Auffällig ist auch, dass jedes fünfte Unternehmen (21 Prozent) nicht in der Lage war, zu identifizieren, auf welche Art und Weise die Daten das Unternehmen verlassen haben. Ebenfalls 21 Prozent der Befragten geben an, dass ein unbedachter E-Mail-Versand für den Datendiebstahl verantwortlich war.

Abb. 8: Ransomware-Drohungen/Erpressungen

	2025	2024
Veröffentlichung der Daten	57 %	▲ 35 %
Daten und Systeme bleiben verschlüsselt	29 %	▼ 59 %
Nicht bekannt	29 %	▲ 12 %
Verkauf der Daten an Dritte	29 %	▲ 18 %
Löschung der Daten	14 %	▼ 18 %
Denial-of-Service-Attacken (DoS)	7 %	▼ 18 %

Abb. 9: Social Engineering Details

	2025	2024
E-Mail-Nachrichten	86 %	▼ 87 %
Messengerdienste (z. B. Telegram, Signal, WhatsApp)	48 %	▼ 49 %
Soziale Netzwerke (beruflich)	48 %	▲ 36 %
Telefonanrufe	43 %	▼ 58 %
Soziale Netzwerke (privat)	33 %	▲ 20 %
Bewerbung/Antwort auf Stellenanzeigen	24 %	▲ 0 %
Privates Umfeld	19 %	▲ 16 %
Deepfake-Sprach-/Videonachrichten	10 %	▼ 13 %

Der vermehrte Einsatz von Smartphones und Tablets im Arbeitskontext ist ein zweischneidiges Schwert: Auf der einen Seite wird so flexibles Arbeiten möglich, auf der anderen Seite kommt es zu kognitiven Überlastungen und damit steigt auch das Risiko, dass Mitarbeitende Sicherheitsprotokolle umgehen.

Die Mitarbeiter:innen greifen über unsichere Netzwerkverbindungen auf Cloud-basierte E-Mail-Systeme zu, verzichten auf die Aktivierung von Zwei-Faktor-Authentifizierung und öffnen ungeprüft Anhänge. Dieses Risiko erhöht sich zusätzlich durch eine lückenhafte Sicherheitsarchitektur vieler Unternehmen, die mobile Geräte nicht oder nur unzureichend in ihre Zero-Trust-Modelle integrieren.

Um diese Risiken einzudämmen, müssen Unternehmen technologische, organisatorische und menschliche Faktoren miteinbeziehen. So sollten beispielsweise neben einer Transportverschlüsselung und Sicherheitsrichtlinien zur Nutzung mobiler Geräte auch gezielte Schulungen und das Etablieren einer Kultur, in der Sicherheitsvorfälle ohne Angst vor negativen Konsequenzen gemeldet werden können, etabliert werden.

Gestohlene Datenarten

Blicken wir auf die Art der Daten, die gestohlen wurden, stehen an erster Stelle Kommunikationsdaten (E-Mails). Auffällig ist auch, dass jedes dritte Unternehmen (32 Prozent) nicht in der Lage ist, zu identifizieren, welche Daten gestohlen wurden. Das ist insofern bedenklich, weil vor allem durch zielgerichtete Angriffe auf der einen Seite, durch den globalen Wettbewerb auf der anderen Seite wertvolle Informationen und Daten von Unternehmen rasch entwendet werden können.

> **Datendiebstahl stellt die unternehmerische Existenz auf die Probe.**

Bei jedem vierten Unternehmen wurden Kund:innendaten gestohlen. Diese Daten sind es auch, die für Mitbewerber interessant sind – könnte man doch günstigere Lösungen und Produkte anbieten und somit einen Wettbewerbsvorteil erzielen.

Drohungen im Zusammenhang mit Ransomware

Fragen wir danach, welche Drohungen im Zuge von Ransomware-Angriffen ausgesprochen werden, sehen wir, dass die Veröffentlichung der Daten im Mittelpunkt steht. Die überwiegende Mehrheit der betroffenen Unternehmen wurde mit dieser Art der Erpressung konfrontiert. Das ist nicht weiter verwunderlich, stellt es doch die naheliegendste und einfachste Form der Erpressung dar, um die Unternehmer:innen zur Zahlung der Lösegeldforderung zu bewegen.

An zweiter Stelle bleiben die Systeme und Daten weiterhin verschlüsselt oder werden zum Verkauf an Dritte angeboten, denn gerade damit lässt sich weiterhin noch gutes Geld machen. Das ist – vor allem wenn wir an die Strukturen der heimischen Wirtschaft denken – besonders lukrativ, da österreichische Unternehmen Weltmarktführer in ihren Nischenbereichen sind und damit diese Daten von besonderer Bedeutung für sie sind.

Ein weiteres Phänomen, mit dem Unternehmen konfrontiert sind, ist die Löschung der Daten auf dem vierten Platz. Aus diesen Ergebnissen geht klar hervor, dass heimische Unternehmen unterschiedlichsten Repressalien und Drohungen ausgesetzt sind. Die Lage ist ernst.

Demgegenüber stehen aber auch positive Nachrichten: Die von Ransomware betroffenen Unternehmen haben zumindest laut eigenen Angaben nicht die Lösegeldforderungen bezahlt. Das ist ein ermutigendes Signal. Es gilt jedenfalls achtsam und wachsam zu bleiben, denn die Facetten und Methoden der Angriffe ändern sich regelmäßig.

Vor allem getrieben durch die Digitalisierungsinitiativen werden unsere Systeme immer anfälliger. Aus diesem Grund kann das aktuell leicht zurückgehende Phänomen Ransomware in Zukunft wieder einen Höhenflug erleben.

Social Engineering

Einer der einfachsten Wege, um Menschen hinters Licht zu führen, ist Social Engineering. Dabei handelt es sich um ein Verfahren, bei dem das Vertrauen der Menschen aufs Spiel gesetzt und zielgerichtet ausgenutzt wird, um sie zu unüberlegtem Handeln zu bringen. Die Studienzahlen verdeutlichen, dass Social Engineering nach wie vor hauptsächlich über E-Mail-Nachrichten stattfindet. Auch die Entwicklungen der letzten Wochen und Monate zeigen, dass dieses Phänomen weiterhin präsent ist und für hohe Schäden sorgen kann. So wurden beispielsweise in letzter Zeit über gefälschte E-Mails bei heimischen Unternehmen hohe Geldbeträge auf andere Konten überwiesen. In diesem Zusammenhang sprechen wir auch von Business-E-Mail-Compromise oder CEO-Fraud.

Social Engineering verlagert sich immer mehr in die sozialen Netzwerke. Das ist eine niederschwellige Möglichkeit, um zu Informationen zu kommen. Soziale Netzwerke, die beruflich genutzt werden, befinden sich auf Platz zwei jener Wege, über die Versuche der Beeinflussung stattgefunden haben. 48 Prozent der Befragten waren Opfer von Social-Engineering-Attacken, die im beruflichen Umfeld stattfinden. Gerade beruflich genutzte soziale Netzwerke sind für eine gewisse Form der Selbstdarstellung prädestiniert. Dadurch wird aber auch die Anfälligkeit für solche Angriffe immer höher. Auch wenn es für das Eigenmarketing und die eigene Darstellung gut ist, muss doch eine gewisse Skepsis an den Tag gelegt werden. Denn nicht jede Kontaktanfrage hat eine positive Absicht.

Eine große Rolle spielen auch Messengerdienste wie Telegram, Signal oder WhatsApp, die zu Social-Engineering-Zwecken missbraucht werden und sich ex aequo mit den beruflichen sozialen Netzwerken auf dem zweiten Platz wiederfinden. Diese Medien sind in unserer Gesellschaft weit verbreitet und werden von vielen Menschen sowohl beruflich als auch privat genutzt. Gerade durch diese Vermischung von Beruflichem und Privatem ist Social Engineering über Messengerdienste besonders erfolgreich.

Auf Platz vier finden wir Social Engineering über die klassischen Telefonanrufe. Auf Platz 5 liegen soziale Netzwerke, die privat genutzt werden. Es zeigt sich, dass der private Bereich zusehends an Bedeutung gewinnt und soziale Netzwerke immer mehr zum Einfallstor werden. Social Engineering für berufliche Zwecke findet mehr und mehr im privaten Umfeld statt. Jeder vierte Social-Engineering-Versuch läuft bereits über Bewerbungen auf Stellenanzeigen. Jeder zehnte Social-Engineering-Versuch nutzt darüber hinaus Deepfake-Sprach-/Videonachrichten.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1. Jedes fünfte Unternehmen kann nicht benennen, welche Schäden im Zusammenhang mit Cyberangriffen entstanden sind. Unternehmen sind allerdings durch die Regulatorik gefordert, Risiken aus Cyberangriffen zu qualifizieren und zu quantifizieren, um geeignete Maßnahmen ableiten zu können. Hier gibt es noch großen Aufholbedarf.

2. Die überwiegende Mehrheit der von Ransomware betroffenen Unternehmen wurde mit der Veröffentlichung von Daten erpresst. Das ist nicht weiter verwunderlich, stellt es doch die naheliegendste und einfachste Form der Erpressung dar, um die Unternehmer:innen zu Lösegeldzahlungen zu bewegen.

3. Social Engineering, d. h. die persönliche Ansprache zur Informationsgewinnung, verlagert sich in soziale Netzwerke. Hier gewinnt v. a. der private Bereich zusehends an Bedeutung und wird zum Einfallstor, denn auch Social Engineering für berufliche Zwecke findet mehr und mehr im privaten Umfeld statt.

Österreichs Sicherheitsarchitektur: Herausforderungen und Strategien

Sascha Bosezky, Leiter des Heeres-Nachrichtenamtes (HNaA), beleuchtet die Rolle des HNaA in der nationalen Sicherheitsstruktur. Er spricht über die Zusammenarbeit mit anderen Diensten und die Anpassung an komplexe Bedrohungen.

Könnten Sie uns bitte kurz die Aufgaben des Heeres-Nachrichtenamtes in Österreich sowie dessen Zusammenarbeit und Abgrenzung zu anderen zivilen und militärischen Diensten erläutern?
Sascha Bosezky: Das Heeres-Nachrichtenamt ist Österreichs strategischer Auslandsnachrichtendienst mit einer Frühwarnfunktion für Bedrohungen wie militärische Konflikte, hybride Bedrohungen, irreguläre Migration und Terrorismus. Es warnt Entscheidungsträger frühzeitig, um Maßnahmen zu ermöglichen. Da viele Bedrohungen aus dem Ausland kommen, ist die Zusammenarbeit der nationalen Nachrichtendienste entscheidend. Das Heeres-Nachrichtenamt und das Abwehramt gehören zum Verteidigungsministerium, während die Direktion Staatsschutz und Nachrichtendienst im Innenministerium für den Verfassungsschutz zuständig ist. 2021 wurde eine Kooperationsstelle für die strukturierte Zusammenarbeit der drei Dienste geschaffen, wobei ihre Eigenständigkeit und Verantwortungsbereiche erhalten bleiben.

Wie wird sich das sicherheitspolitische Umfeld Europas in den nächsten fünf bis zehn Jahren verändern und welche Rolle spielt Österreich in der europäischen Sicherheitsarchitektur?
Sascha Bosezky: Die geopolitische Konfrontation und multipolare Tendenzen haben zugenommen, verstärkt durch den Isolationismus der USA. Traditionelle sicherheitspolitische Partnerschaften werden infrage gestellt, was Europa vor Herausforderungen stellt. Konflikte in der Nähe Europas werden nicht schnell gelöst, und ihre Auswirkungen sind langanhaltend. Die Hauptbedrohung für Europa ist Russland, das den Ukraine-Konflikt als Teil eines größeren Kampfes gegen den Westen sieht. Der Westbalkan ist ebenfalls von Interesse für Österreich und die EU. Europa muss auf Krisen in seiner Nachbarschaft und darüber hinaus vorbereitet sein, wobei innere Stabilität und Zusammenhalt entscheidend sind.

> **Wir befinden uns im Status einer politisch-gesellschaftlich-wirtschaftlich-militärischen Polykrise.**

Wie hat sich die Rolle des Heeres-Nachrichtenamtes in den letzten Jahren angesichts der zunehmenden Komplexität der Bedrohungslage verändert?
Sascha Bosezky: Die Rolle der Nachrichtendienste in Europa hat sich grundlegend verändert, was einige als „Zeitenwende" bezeichnen. Der US-chinesische Konflikt hat an Schärfe gewonnen, und die Bedrohung durch Spionage ist gestiegen. Vor fünf Jahren waren die Herausforderungen durch Krisen wie bewaffnete Konflikte, islamistischen Terrorismus und Massenmigration geprägt. Heute erleben wir eine Polykrise, die politisch, gesellschaftlich, wirtschaftlich und militärisch ist, verstärkt durch konventionelle Kriege und hybride Bedrohungen. Diese Entwicklungen geschehen vor dem Hintergrund rasanter technologischer Fortschritte, wie im Cyberraum, sozialen Medien, KI und Big Data. Nachrichtendienste müssen mit

FOTO © PAUL KULEC

Seit dem 1. Oktober 2020 ist **Generalmajor Mag. Sascha Bosezky** Leiter des Heeres-Nachrichtenamtes. Das HNaA als strategischer Auslandsnachrichtendienst Österreichs ist im Bundesministerium für Landesverteidigung angesiedelt und spielt eine entscheidende Rolle bei der Frühwarnung vor sicherheitspolitischen Bedrohungen und dem Schutz österreichischer Soldatinnen und Soldaten im Ausland. Bosezky hat sich als erfahrener und verlässlicher Nachrichtendienst-Offizier mit hoher Reputation bei internationalen Partnern etabliert. Sein Werdegang umfasst eine Generalstabsausbildung sowie langjährige militärische Führungs- und Einsatzerfahrung im In- und Ausland, darunter Kommandantenfunktionen als Truppenoffizier und Auslandseinsätze im Kosovo und bei der Deutschen Bundeswehr.

diesen Veränderungen Schritt halten, um Sicherheitsrisiken zu minimieren. Der Cyberraum darf nicht Terroristen und Extremisten überlassen werden, und die Anpassung der Befugnisse der Dienste ist entscheidend. Trotz Digitalisierung bleibt die Informationsbeschaffung durch menschliche Quellen (HUMINT) wichtig. Die Kombination von HUMINT und Cyberaufklärung (CYBINT) bietet wertvolle Synergien.

Welche strategischen Verschiebungen sehen Sie in der internationalen Sicherheitsordnung, insbesondere bei Allianzen wie AUKUS und BRICS+? Welche sicherheits- und wirtschaftspolitischen Folgen hat dies für Europa, und wie sollte Österreich darauf reagieren, insbesondere hinsichtlich seiner nachrichtendienstlichen Kapazitäten?

Sascha Bosezky: Der Ansatz der US-Administration unter Donald Trump stellt die regelbasierte Weltordnung und das globale Engagement der USA infrage. Aussagen zu Kanada und Grönland deuten auf ein Weltbild hin, in dem große Akteure Einflusssphären beanspruchen. Eine geostrategische Dreipoligkeit zwischen USA, China und Russland scheint angestrebt zu sein, wobei die USA China nachhaltig schwächen wollen. Der Konflikt zwischen den USA und China betrifft Sicherheit, Militärpolitik, Geoökonomie und Schlüsseltechnologien. China und Russland fördern BRICS, während die USA

> **Staatlich unterstützte Akteure spielen im aktuellen Bedrohungsbild im Cyberraum eine zunehmende Rolle.**

auf Allianzen mit Südkorea, den Philippinen und Japan setzen, um China im Indopazifik einzudämmen. Trotz der regionalen Bedeutung der BRICS-Länder ist ihre Bedeutung als Staatenbund aufgrund ihrer Heterogenität gering. Österreich, obwohl kein globaler Akteur, ist von den Großmachtrivalitäten sicherheitspolitisch betroffen. Der österreichische Auslandsnachrichtendienst muss globale Entwicklungen beobachten und analysieren. Dafür sind unabhängige Analysefähigkeiten, Experten und zeitgemäße Methoden notwendig, was entsprechende Mittel und Befugnisse erfordert.

Welche strategische Rolle spielt das Heeres-Nachrichtenamt in der nationalen Sicherheitsstruktur angesichts wachsender außenpolitischer Unsicherheiten?

Sascha Bosezky: Das Heeres-Nachrichtenamt hat als strategischer Auslandsnachrichtendienst eine wichtige Frühwarnfunktion für die militärische und politische Führung. Es erstellt einen mittel- bis langfristigen Aufklärungsplan mit thematischen Prioritäten und tritt in Dialog mit Bedarfsträgern im gesamtstaatlichen Kontext. Diese Rolle zeigt die gesamtstaatliche Bedeutung der nachrichtendienstlichen Aufklärung. Das HNaA arbeitet eng mit den politischen und militärischen Führungskräften zusammen, und die positive Resonanz sowie die Nachfrage nach seiner Expertise bestätigen den Erfolg dieses Ansatzes.

Welche hybriden Bedrohungsszenarien sind derzeit besonders relevant für westliche Demokratien? Welche staatlichen und nicht staatlichen Akteure sind dabei besonders aktiv?

Sascha Bosezky: Ein Ziel des hybriden Konflikts gegen Europa ist die Zersetzung des gesellschaftlichen Gefüges und die Unterminierung demokratischer Prinzipien, was die Wehrfähigkeit gegenüber Russland und anderen Akteuren schwächt. Besonders relevant sind die Auswirkungen auf westliche Demokratien durch „Foreign Information Manipulation and Interference" (FIMI)-Operationen, die gesellschaftliche Spaltungen ausnutzen. Seit dem Ukraine-Krieg nehmen gezielte Angriffe auf Europas kritische Infrastruktur zu, wobei russische Geheimdienste Windparks, Gaspipelines, Strom- und Internetkabel kartieren. Die Zerstörung von Unterwasserinfrastruktur im Baltischen Meer durch „Unfälle" begleitet diese Aktivitäten. Auch militärische und wirtschaftliche Einrichtungen an Land, wie LNG-Terminals und Kernkraftwerke, sind von Spionage betroffen. Verschleierungsmaßnahmen erschweren das Erkennen und Zuordnen hybrider Vorfälle. Österreichs zentrale Lage in Europa erhöht die Gefahr von Spionage und Sabotage, da wichtige europäische Infrastrukturen durch das Land verlaufen.

Welche Rolle spielen staatlich unterstützte Akteur:innen im aktuellen Bedrohungspanorama der Cyberwelt? Welche Angriffsmuster sind verstärkt zu beobachten und welche Wirtschaftsbereiche sind besonders betroffen?

Sascha Bosezky: Staatlich unterstützte Akteure spielen im Cyberraum eine zunehmend wichtige Rolle. Es gibt verschiedene Typen: politisch oder ideologisch motivierte Hacktivisten, die mit DDoS-Angriffen Systeme oder Webseiten lahmlegen, um ihre Werte zu verbreiten; „loyale und bezahlte" Akteure, die Bot-Netze und Desinformationen nutzen, um Fakten zu hinterfragen und Personen oder Organisationen zu diffamieren; und ausländische IT-Firmen, die Spionagesoftware einsetzen, um im Auftrag staatlicher Akteure Informationen über politische Ebenen oder den Rüstungs- und Wirtschaftssektor zu sammeln. Besonders betroffen sind kritische Infrastrukturen und Unternehmen, die als lukrative Ziele gelten.

> **Generative KI verstärkt die Gefahren der Desinformation durch realistische, skalierbare Falschinhalte.**

Wie kann Europa in einer multipolaren Welt seine strategische Autonomie bewahren, ohne sich zwischen den USA und China positionieren zu müssen? Welche Rolle spielt Österreich dabei, und wie wird dies im sicherheitspolitischen Lagebild berücksichtigt?

Sascha Bosezky: Die strategische Autonomie Europas ist ursächlich mit der Fähigkeit und den Kapazitäten, die eigenen Interessen zumindest im regionalen Kontext wahren oder durchsetzen zu können, verbunden. In erster Linie geht es um die selbstständige Abschreckung Russlands – im gesamten konventionellen bis hin zum nuklearen Spektrum. Eine deutliche Investition beispielsweise in die Bereiche Frühwarnung, weitreichende Wirkmittel und Flug- sowie Raketenabwehr sind dabei primäre Erfordernisse. Die strategische Kooperation mit außereuropäischen Partnern, wie beispielsweise Kanada, bietet sich ebenso wie verstärkte wirtschaftliche Beziehungen, wie etwa mit MERCOSUR oder Indien, an. Dabei wären eine Fokussierung auf den europäischen Markt und die Reduktion der Abhängigkeit von US-Dienstleistern naheliegend.

Was bedeutet wirtschaftliche Souveränität heute, besonders in Bezug auf kritische Technologien, Halbleiter, Energieträger und seltene Erden? Welche Risiken entstehen durch externe Abhängigkeiten?

Sascha Bosezky: Wirtschaftliche Souveränität bedeutet, Wasser, Nahrungsmittel, kritische Technologien, Energieträger und Rohstoffe unabhängig und sicher zu beschaffen und zu nutzen. Für Europa ist sie entscheidend für die Resilienz gegenüber geopolitischen Spannungen und globalen Lieferkettenstörungen, um strategische Interessen zu wahren und technologische Wettbewerbsfähigkeit zu sichern. Nach einer Phase des freien Handels auf Grundlage der WTO gibt es nun mehr handelshemmende Faktoren, wie protektionistische Maßnahmen, Sanktionen und Konflikte, die die Stabilität der Lieferketten beeinträchtigen und Volatilität verursachen. Die Vorteile der Kosteneffizienz und Stabilität durch enge Handelsverflechtungen stehen Risiken wie der Verwundbarkeit der Lieferketten und Abhängigkeit von Lieferanten gegenüber.

Welche Schlüsseltechnologien sind strategisch entscheidend für Europas Zukunftssicherung aus sicherheitspolitischer und wirtschaftlicher Sicht? Welche davon haben das größte Missbrauchspotenzial?

Sascha Bosezky: Quanten- und Biotechnologie sowie Neuro- und Materialwissenschaften sind strategische Schlüsseltechnologien, die als Multiplikatoren für andere Forschungsfelder, einschließlich militärischer Anwendungen, wichtig sind. Quantenkryptografie zur Verschlüsselung sensibler Informationen hat in Österreich und Europa Priorität, birgt aber langfristig die Gefahr der Entschlüsselung sicherer Kommunikation. Europa muss seine Technologiekompetenz und Implementierungskraft steigern, um global wettbewerbsfähig zu bleiben. Schlüsseltechnologien wie KI, Quantentechnologie und Mikroelektronik haben aber auch Missbrauchspotenzial: KI kann für Manipulation durch Deepfakes oder diskriminierende Entscheidungen genutzt werden, Quantencomputer könnten Verschlüsselungen unwirksam machen, und die Abhängigkeit von importierten Elektronikkomponenten birgt Manipulationsrisiken.

Welche sicherheitspolitischen Risiken entstehen durch generative KI, insbesondere bei Meinungsbeeinflussung, Deepfakes und automatisierter Manipulation? Welche gesellschaftlichen Schutzmechanismen sind notwendig?

Stärkung der rechtlichen Rahmenbedingungen ist ein Quantensprung für einen modernen Nachrichtendienst.

Sascha Bosezky: KI hat sich von einer kritischen emergenten Technologie zu einem strategischen Aktivposten entwickelt, der zur globalen Beeinflussung genutzt wird und enorme geo- und sicherheitspolitische Auswirkungen hat. Generative KI birgt Risiken durch die Verstärkung von Desinformation, indem sie realistische und personalisierte Falschinhalte erzeugt und verbreitet. Sie kann schnell Deepfakes erstellen, die schwer von echten Inhalten zu unterscheiden sind, und so gesellschaftlich schädliche Trends durch ausländische Akteure verstärken. Ein Hindernis im Kampf gegen diese Angriffe ist das Recht auf Meinungsfreiheit. Regulierung allein reicht nicht aus; es braucht eine Kombination aus regulativen, organisatorischen, gesellschaftlichen und technischen Maßnahmen.

Welche sicherheitspolitischen Entwicklungen, ob global, regional oder technologisch, sind derzeit besonders kritisch oder unterschätzt? In welchen Bereichen besteht dringender Handlungsbedarf?

Sascha Bosezky: Zwei relevante Trends sind besonders kritisch: Erstens, der Rückzug der USA aus internationalen Organisationen und die Kürzung von Hilfsgeldern könnten Chinas globale Ambitionen fördern, insbesondere in Afrika, und westliche Interessen gefährden. Zweitens, der Vertrauensverlust in den militärischen Schutz durch die USA verstärkt die Bedrohungswahrnehmung bei Staaten ohne Nuklearwaffen, was zu einer Zunahme von Staaten führen könnte, die eigene Nuklearwaffen entwickeln, um den wegfallenden Schutz auszugleichen.

Wie kann Österreich seine Analyse- und Reaktionsfähigkeit in Sicherheitsfragen stärken? Welche Rolle spielen Nachrichtendienste, Wissenschaft und Wirtschaft dabei?

Sascha Bosezky: Sicherheit ist eine komplexe Herausforderung, die bereits in den 1970er Jahren als „Umfassende Landesverteidigung" in der österreichischen Verfassung verankert wurde. Der Angriffskrieg Russlands gegen die Ukraine zeigt die enge Verbindung zwischen der Verteidigungsfähigkeit der Streitkräfte, dem Verteidigungswillen der Bevölkerung, der Resilienz der Gesellschaft und der Wirtschaft. Eine gesamtstaatliche Reaktionsfähigkeit erfordert ein akkurates Lagebild, zu dem Nachrichtendienste durch exklusive Methoden beitragen. Wissenschaft spielt ebenfalls eine wichtige Rolle, insbesondere durch die Zusammenarbeit mit sozial-, wirtschafts- und technologieorientierter Forschung. International kooperieren Nachrichtendienste im „Intelligence College in Europe" mit wissenschaftlichen Einrichtungen, um den Austausch zwischen Intelligence Communities, Universitäten und Entscheidungsträgern zu fördern.

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

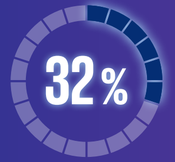
Sascha Bosezky: Als Leiter eines Strategischen Auslandsnachrichtendienstes ist es meine Kernaufgabe sicherzustellen, dass ich diese Frage in einem Jahr für mich mit gutem Gewissen mit „Nichts" beantworten kann. Die Nachrichtendienstliche Aufklärung antizipiert Bedrohungen für die oberste staatliche Führung, damit diese zeitgerechte Maßnahmen zu deren Abwehr beziehungsweise Bewältigung setzen kann. Gleichzeitig ist es meine Aufgabe als Leiter eines Nachrichtendienstes aus dem Ergebnis dieser Antizipation die richtigen Schlussfolgerungen für die Weiterentwicklung meiner eigenen Organisation zu ziehen. Dazu gehören rechtliche, technologische, personelle und infrastrukturelle Aspekte. Natürlich gibt es hier Grenzen in den gesetzlichen und budgetären Rahmenbedingungen, das HNaA ist aber aus meiner Sicht gut aufgestellt und zukunftsfit. Von ganz besonderer Bedeutung ist dabei die jüngste Absichtserklärung im Regierungsprogramm, die rechtlichen Rahmenbedingungen der Befugnisse unserer Arbeit zu stärken. Deren Realisierung ist für uns ein weiterer Quantensprung in Richtung eines modernen Nachrichtendienstes für das 21. Jahrhundert.

04

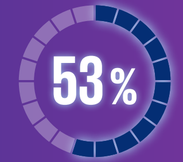
Wie wurde gehandelt?

Wir wissen nun Bescheid über die weitreichenden Folgen, die Unternehmen aufgrund von Cyberangriffen in den letzten 12 Monaten verspürt haben. Doch wie sind sie damit umgegangen? Wurden Meldungen an zuständige Stellen durchgeführt? Welche Maßnahmen haben sie nach einem Angriff gesetzt und wie soll die Wirksamkeit dieser Maßnahmen überprüft werden? Holen sich Unternehmen Unterstützung von externen Dienstleistern oder schließen sie Cyberversicherungen ab?

haben keine Meldung eines **Cybersicherheitsvorfalls** durchgeführt.



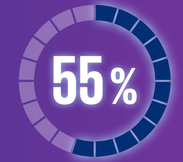
planen **Penetrationstests**, um die Wirksamkeit ihrer Sicherheits-/Resilienzmaßnahmen in den kommenden 12 Monaten zu prüfen.



ziehen keine **externen Dienstleister** bei der Vorfallsbearbeitung und -behandlung heran.

Jedes zehnte Unternehmen hat Schwierigkeiten, einen **passenden externen Dienstleister** zu finden.

Jedes fünfte Unternehmen besitzt eine **Cyberversicherung**.



Knapp 55 % möchten, dass die Cyberversicherung die **Kosten für Lösegeldzahlungen** abdeckt.

Meldung von Cyberangriffen

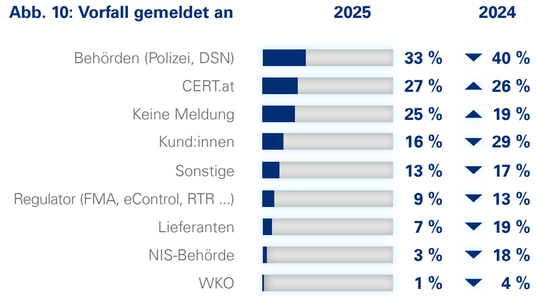
Wenn es um die Meldung von Cyberangriffen geht, so sehen wir, dass Meldungen an Behörden (Polizei sowie Direktion Staatsschutz und Nachrichtendienst) an erster Stelle stehen. Im Jahr 2025 sank der Anteil im Vergleich zu 2024 jedoch um ca. 7 Prozentpunkte. Dies könnte auf eine veränderte Wahrnehmung der Effektivität dieser Stellen oder auf eine stärkere Orientierung hin zu anderen Meldekanälen zurückzuführen sein. An zweiter Stelle liegen mit 27 Prozent Meldungen an CERT (AEC, CERT.at, GovCERT). Das ist ein Anstieg um +1 Prozentpunkte, was darauf hinweist, dass spezialisierte Institutionen für Cybersicherheit zunehmend als vertrauenswürdige Ansprechpartner wahrgenommen werden. Darüber hinaus fanden auch Meldungen an die Datenschutzbehörde statt.

Wir sehen signifikante Rückgänge bei Meldungen an Kund:innen (-13 Prozentpunkte), Lieferanten (-12 Prozentpunkte) und die NIS-Behörde (-15 Prozentpunkte). Das könnte darauf hindeuten, dass Unternehmen zunehmend andere Prioritäten setzen oder alternative Kommunikationswege nutzen.

Die Kategorie „Sonstige" sowie Meldungen an Regulatoren wie FMA, eControl und RTR verzeichneten ebenfalls einen Rückgang (jeweils -4 Prozentpunkte). Gründe hierfür könnten sein, dass spezifische regulatorische Anforderungen oder Zuständigkeiten weniger klar sind oder dass Unternehmen diese Kanäle als weniger relevant empfinden.

Wir beobachten also eine Verschiebung des Meldeverhaltens hin zu spezialisierten Stellen wie CERT.at bei einer gleichzeitigen Zunahme von Nichtmeldungen. Das unterstreicht die Notwendigkeit einer klareren Kommunikation über Meldepflichten und -wege sowie einer stärkeren Sensibilisierung für die Bedeutung von Cybersicherheitsmeldungen.

Abb. 10: Vorfall gemeldet an



Warum keine Meldung erfolgte

Im Vergleich zum letzten Jahr ist allerdings auch eine Trendumkehr dahingehend zu sehen, dass vermehrt überhaupt keine Meldungen mehr stattfinden. Haben im Vorjahr noch 19 Prozent keine Meldung durchgeführt, liegen wir heuer bei 25 Prozent. Durch die zunehmende Regulierung werden Meldungen an die zuständigen Stellen allerdings immer mehr zur Notwendigkeit und sollten daher von den Unternehmen auch in die gelebte Praxis übernommen werden.

Interessanterweise stiegen die Fälle, in denen keine Meldung erfolgte, um etwa 6 Prozentpunkte. Ein Teil der Betroffenen ist möglicherweise unsicher über die richtigen Meldewege oder entscheidet sich bewusst gegen eine Meldung– möglicherweise aus Angst vor Reputationsschäden oder rechtlichen Konsequenzen.

Auf die Frage, warum niemand über den Cybersicherheitsvorfall informiert wurde, gaben die Befragten an, dass die Beeinträchtigung durch die Angriffe nicht groß genug gewesen wäre, um eine Meldung zu rechtfertigen, und keine Verpflichtung zur Meldung bestehe, insbesondere wenn die Angriffe nicht erfolgreich waren. Zudem wurde der Schaden erfolgreich abgewehrt, und die betroffenen Systeme waren keine Produktivsysteme, was die Relevanz einer Meldung weiter reduzierte.

Maßnahmen gegen Cyberattacken

Schauen wir uns an, welche Maßnahmen langfristig von den Unternehmen nach einem Cyberangriff gesetzt wurden.

Die anfängliche Reaktion auf einen Cyberangriff bleibt erwartungsgemäß die Schwachstellensuche in den Systemen (2025: 51 Prozent, 2024: 54 Prozent). Dieser Schritt ist entscheidend, um unmittelbare Schäden zu begrenzen und weitere Angriffe zu verhindern. Es ist jedoch besorgniserregend, dass die Anschaffung zusätzlicher Sicherheitstools (2025: 35 Prozent, 2024: 46 Prozent) weiterhin eine hohe Priorität hat. Das deutet darauf hin, dass viele Unternehmen erst nach einem Vorfall in grundlegende Sicherheitsvorkehrungen investieren. Ein strategischerer Ansatz wäre hier wünschenswert.

Bemerkenswert ist der signifikante Anstieg beim Aufbau von Security-Kompetenzen (2025: 33 Prozent, 2024: 0 Prozent), der Aktualisierung des Identity and Access Managements (2025: 27 Prozent, 2024: 0 Prozent) und dem Austausch / der Modernisierung der SIEM-Tools (2025: 24 Prozent, 2024: 0 Prozent). Diese Entwicklung signalisiert ein wachsendes Verständnis für die Notwendigkeit interner Expertise und fortschrittlicher Technologien, um Cyberbedrohungen effektiv zu begegnen. Unternehmen scheinen zu erkennen, dass eine nachhaltige Sicherheitsstrategie auf internem Know-how und modernster Technologie basieren muss.

Die Verbesserung der internen Krisenplanung für Cyberangriffe ist zurückgegangen (2025: 33 Prozent, 2024: 45 Prozent). Eine Überschätzung der bestehenden Pläne könnte der Grund hierfür sein. Eine regelmäßige Überprüfung und Anpassung der Krisenpläne sind jedoch unerlässlich, um mit der sich ständig verändernden Bedrohungslandschaft Schritt zu halten. Ebenso ist der Rückgang bei der Inanspruchnahme externer IT-Berater (2025: 40 Prozent, 2024: 66 Prozent) und Investitionen in Mitarbeiter:innenschulungen (2025: 24 Prozent, 2024: 28 Prozent) kritisch zu hinterfragen. Externe Expertise und kontinuierliche Weiterbildung spielen eine wichtige Rolle bei der Aufrechterhaltung eines hohen Sicherheitsniveaus.

Die Zunahme der anlassbezogenen Medienarbeit (2025: 14 Prozent, 2024: 6 Prozent) ist ein positives Zeichen für mehr Transparenz und Verantwortungsbewusstsein im Umgang mit Cybervorfällen. Eine offene Kommunikation mit Kund:innen und Stakeholder:innen ist entscheidend, um Vertrauen zu erhalten und die Reputation des Unternehmens zu schützen.

Die rückläufigen Zahlen bei der Prüfung der Sicherheit der Lieferanten (2025: 20 Prozent, 2024: 24 Prozent), der Risikoabdeckung mit einer Cyberversicherung (2025: 19 Prozent, 2024: 22 Prozent), dem Einstellen neuer Mitarbeiter:innen für Security (2025: 10 Prozent, 2024: 20 Prozent) sowie den sonstigen Maßnahmen (2025: 10 Prozent, 2024: 20 Prozent) geben Anlass zur Sorge. Sie alle sind entscheidend für eine umfassende Sicherheitsstrategie.

Die Verlagerung der Security-Verantwortung sowohl an externe Dienstleister (2025: 8 Prozent, 2024: 0 Prozent) als auch nach intern (2025: 8 Prozent, 2024: 0 Prozent) zeigt, dass Unternehmen

unterschiedliche Wege gehen, um ihre Sicherheitslücken zu schließen. Beide Ansätze können effektiv sein, solange sie auf einer klaren Strategie und einer fundierten Risikobewertung basieren.

Insgesamt deuten die Daten auf eine positive Entwicklung zu einer proaktiveren und kompetenzorientierten Cybersecurity-Strategie hin. Es ist jedoch wichtig, dass Unternehmen nicht nachlassen und weiterhin in alle Sicherheitsaspekte investieren. Nur so können sie den sich ständig weiterentwickelnden Bedrohungen wirksam begegnen. Nur so sind sie nachhaltig resilient gegenüber Cyberangriffen.

Wirksamkeitsprüfung

Wie planen Unternehmen, die Wirksamkeit ihrer Sicherheits-/Resilienzmaßnahmen in den kommenden 12 Monaten zu prüfen? Die besten Maßnahmen nach einem Cybersicherheitsvorfall reichen nicht aus, wenn man sich nicht von deren Wirksamkeit überzeugen kann. Unternehmen sind also angehalten, die umgesetzten Aktivitäten, Kontrollen und Sicherheitsvorkehrungen auch auf deren Funktionalität hin zu prüfen. Die Durchführung von Penetrationstests steht dabei für 32 Prozent der befragten Unternehmen an oberster Stelle. Diese Form der Überprüfung kennen wir schon seit langer Zeit und sind es auch gewohnt, diese Art der Tests durchzuführen. Einschränkend muss jedoch gesagt werden, dass Penetrationstests nur eine Momentaufnahme sind und keine regelmäßige und wiederkehrende Statusfeststellung ermöglichen. Oftmals handelt es sich dabei um eine sehr isolierte Betrachtung, wenngleich sie zur Verbesserung der Sicherheit einen guten Beitrag leisten kann.

An zweiter Stelle führen Unternehmen interne (28 Prozent) und an dritter Stelle externe (22 Prozent) Gap-Analysen durch. Hier befinden wir uns im organisatorischen Bereich der Informationssicherheit, da es oft um die Einhaltung von Vorgaben geht. Unternehmen bewegen sich dabei also eher im Bereich der Compliance-Adressierung und weniger im Bereich der Wirksamkeitsprüfung. Die Befragten versuchen auch immer stärker den Umgang mit Ausnahmesituationen zu erlernen. 22 Prozent planen in den nächsten 12 Monaten simulierte Übungen, sogenannte Tabletop Exercises, durchzuführen. Mit diesen Übungen kann man die Herangehensweise an außergewöhnliche Situation simulieren, um Lücken, Handlungsfelder, aber auch Erfolge aufzuzeigen.

Eine fortgeschrittene Form der Wirksamkeitsprüfung sind sogenannte strukturierte Angriffssimulationen. Wir sprechen hier von Threat-Led-Penetrationtests (9 Prozent) sowie von szenariobasierten Tests (13 Prozent), die durchgeführt werden. In diesem Zusammenhang ist jedenfalls zu erwähnen, dass die Durchführung von Threat-Led-Penetrationtests im Banken- und Versicherungsbereich und in der Finanzwirtschaft vor allem durch die Regulatorik immer stärker gefordert wird. Wenngleich Industrieunternehmen noch nicht dieselben regulatorischen Auflagen haben, sind sie jedenfalls dazu angehalten, diese Tests auch in ihre Wirksamkeitsprüfung mit aufzunehmen. Durch die Ende-zu-Ende-Analyse der beiden Tests kann die Wirksamkeit der Abwehrmaßnahmen und der eingesetzten Technologien und Lösungen intensiv auf Herz und Nieren geprüft werden.

Schade ist, dass 46 Prozent der befragten Unternehmen plant, in den nächsten 12 Monaten keine Maßnahmen durchzuführen. Diese Lücken müssen geschlossen werden. Ist es doch genau die Wirksamkeitsprüfung, die entscheidet, ob das richtige Geld auf die richtigen Themen mit dem richtigen Ziel und dem richtigen Fokus gesetzt wurde. Und auch aus der Sorgfaltspflicht der Unternehmen heraus ist es unerlässlich, eine Wirksamkeitsprüfung durchzuführen.

Abb. 11: Dienstleisterunterstützung Vorfall

> **In der Cybersicherheit ist Selbstzufriedenheit keine Option: Aufmerksamkeit ist Pflicht.**

Unterstützung durch einen externen Dienstleister

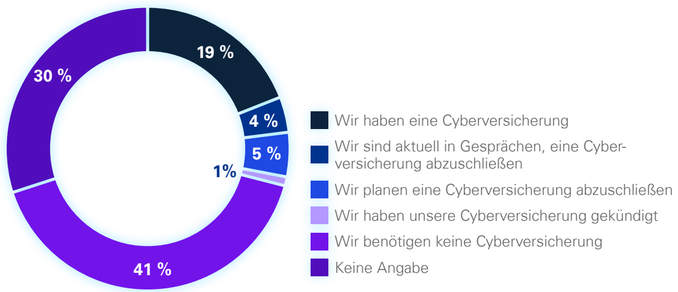
Gerade in der Bewältigung von Sicherheitsvorfällen ist es notwendig, mit der entsprechenden Ressourcenausstattung vorzugehen. Dafür holen sich Unternehmen bei Cybersicherheitsvorfällen mitunter auch externe Unterstützung. 40 Prozent der betroffenen Unternehmen hatte bei der Bearbeitung eines Sicherheitsvorfalls Unterstützung durch einen externen Dienstleister. Interessant ist hier vor allem auch die Veränderung gegenüber dem Vorjahr: Wir sehen, dass die Unterstützung durch externe Dienstleister abgenommen hat und immer mehr Unternehmen Kompetenzen intern aufbauen.

In Ausnahmesituationen ist es essenziell, schnell Hilfe zu erhalten. Hierfür setzen Unternehmen vermehrt auf sogenannte Retainer. Dabei handelt es sich um eine vertragliche Vereinbarung mit einem Dienstleister, die unter Einhaltung von gewissen Reaktionszeiten eine Präsenz vor Ort im Anlassfall sicherstellt und das betroffene Unternehmen bei der Aufarbeitung des Sicherheitsvorfalls unterstützt. Die Zahlen aus unserer aktuellen Studie zeigen, dass rund 31 Prozent der befragten Unternehmen Unterstützung durch externe Dienstleister hatten, die über einen Retainer abgesichert waren. Daraus lässt sich schließen, dass für sie vor allem die Reaktionsfähigkeit von Bedeutung ist.

53 Prozent der Befragten gaben allerdings auch an, keine externe Unterstützung bei der Vorfallsbearbeitung und -behandlung heranzuziehen. Diese Unternehmen investieren in die eigene Vorsorge und Reaktionsfähigkeiten.

> **Die Frage ist nicht, ob ein Sicherheitsvorfall eintritt, sondern wann. Entscheidend ist, wie schnell und effektiv heimische Unternehmen darauf reagieren.**

Abb. 12: Cyberversicherung



Schwierigkeit, den passenden Dienstleister zu finden

Einen Dienstleister für außergewöhnliche Situationen zu finden, bedarf natürlich auch eines gewissen Vertrauens und persönlichen Empfehlungen. Hat jemand bereits gute Erfahrungen mit einem Dienstleister gemacht, spricht sich das herum. Dennoch bleibt die Frage, wie schwierig sich die Suche für heimische Unternehmen gestaltet. Unsere Zahlen aus der Studie zeigen, dass nur noch jedes zehnte Unternehmen Schwierigkeiten hat, einen passenden externen Dienstleister zu finden. Die überwiegende Mehrheit (66 Prozent) gibt an, dass sie keine Probleme damit hatte. Die Befragten teilten uns mit, dass sie über etablierte Kontakte oder persönliche Referenzen den für sie passenden Dienstleister gefunden haben. Neben Vergabeverfahren und Ausschreibungen wurden zusätzlich auch über den Vorschlag von Cyberversicherern passende Dienstleister gefunden.

Interessant ist, dass vorwiegend externe IT-Dienstleister, mit denen bereits bestehende Verträge etabliert sind und die die laufenden Betreuungstätigkeiten durchführen, als Dienstleister im Sicherheitsvorfall herangezogen werden. Wiewohl diesem Argument sehr viel Verständnis abgewonnen werden kann, so ist es gerade bei einem Sicherheitsvorfall von unabdingbarer Notwendigkeit, eine objektive zweite Meinung einzuholen. IT-Dienstleister versuchen möglicherweise stellenweise Unzulänglichkeiten zu kaschieren – was aber niemandem unterstellt werden soll. Es geht nicht darum, die Verlässlichkeit dieser IT-Dienstleister infrage zu stellen. Dennoch ist eine Unterstützung mit einem frischen Blick in solchen Situationen oft viel hilfreicher, um rasch zum Ziel zu kommen bzw. unmittelbare Sofortmaßnahmen zielgerichtet umsetzen zu können. Unabhängig davon, welche Dienstleistungen für die Behebung eingesetzt werden, ist es essenziell, dass Unternehmen schnell wieder in den Urzustand zurückgeführt werden und mit ihrer Geschäftstätigkeit fortfahren können.

Cyberversicherungen

Cyberversicherungen werden intensiv diskutiert und jedes fünfte Unternehmen besitzt eine solche. Das ist ein leichter Rückgang von 22 Prozent auf 19 Prozent und spiegelt eine gewisse Marktdynamik wider. Fast die Hälfte der befragten Unternehmen sieht aktuell keinen Bedarf an einer Cyberversicherung. Das deutet auf ein gestiegenes Vertrauen in die eigenen Sicherheitsvorkehrungen oder eine veränderte Risikobewertung hin. Es bleibt jedoch unklar, inwieweit diese Unternehmen tatsächlich Vorsorge treffen, um im Schadensfall adäquat reagieren zu können. Die in jüngster Vergangenheit aufgetretenen Ransomware-Angriffe und die damit verbundenen Versicherungsstreitigkeiten haben gezeigt, dass die Erwartungen der Unternehmen hinsichtlich der abgedeckten Leistungen von Cyberversicherungen oft nicht mit der Realität übereinstimmen. Dies hat zu Verunsicherung geführt und verdeutlicht die Notwendigkeit einer klaren Kommunikation und Transparenz seitens der Versicherungsanbieter. Die Anpassung der Leistungsangebote der Versicherungen aufgrund der gestiegenen Ransomware-Fälle ist ein positiver Schritt, um den veränderten Bedrohungen gerecht zu werden.

> **Der Mensch bleibt der entscheidende Faktor für die Cyberabwehr.**

Gewünschte Abdeckung durch eine Cyberversicherung

Unternehmen möchten vor allem die Kosten für Datenverlust und Wiederherstellung (66 Prozent im Jahr 2025, 74 Prozent 2024) sowie Computerbetrug, Erpressung und Lösegeldzahlungen (55 Prozent) durch eine Cyberversicherung abgedeckt haben. Auch Betriebsunterbrechungen und entgangene Gewinne (53 Prozent) sowie Rechtsberatung und Instandsetzung/Wiederherstellung (49 Prozent) sind wichtige Aspekte für die Unternehmen. Die Bereiche Kommunikation & Information (19 Prozent), Imageverlust/Imagekampagne (17 Prozent) und Kosten für Audit (15 Prozent) werden als weniger relevant angesehen. Der Anstieg jener Befragten, die dazu keine Angabe gemacht haben (von 11 Prozent auf 19 Prozent), könnte bedeuten, dass diese Unternehmen nicht vollständig über den Umfang ihrer Cyberversicherung informiert sind.

Abb. 13: Abdeckung Cyberversicherung

	2025		2024
Datenverlust/Wiederherstellungskosten	66 %	▼	74 %
Computerbetrug/Erpressung/Lösegeldzahlung	55 %	▲	53 %
Betriebsunterbrechung / Entgangene Gewinne	53 %	◆	53 %
Rechtsberatung	49 %	▼	54 %
Instandsetzung/Wiederherstellung	49 %	▼	53 %
Forensische Unterstützung	40 %	▼	45 %
Drittschäden	38 %	▼	43 %
Strafzahlungen	24 %	▼	25 %
Keine Angabe	19 %	▲	11 %
Kommunikation & Information	19 %	◆	19 %
Imageverlust/Imagekampagne	17 %	▲	15 %
Kosten für Audit	15 %	◆	15 %
Sonstige	2 %	▲	0 %

Cyberversicherungen haben sich im Laufe der Jahre weiterentwickelt und bieten nun eine Vielzahl von Paketen, Modulen und Produkten an. Die Prioritäten der Unternehmen bei der Abdeckung durch Cyberversicherungen liegen klar auf den Kosten für Datenverlust und Wiederherstellung, was mit über 60 Prozent an erster Stelle steht. Die Wiederherstellung gestohlener oder zerstörter Daten ist von enormer Bedeutung für Unternehmen. Eng damit verbunden sind die Betriebsunterbrechung und der entgangene Gewinn. Cyberangriffe führen oft zu Unterbrechungen der Geschäftstätigkeit, die von einigen Tagen bis zu einigen Wochen dauern können. Die Kompensation dieser entgangenen Gewinne ist daher ein wichtiger Aspekt der Cyberversicherung.

Die Instandsetzung und Wiederherstellung des Geschäftsbetriebs sind ebenfalls von großer Relevanz – die Kosten für die Wiederherstellungssysteme nach einem Angriff können schnell steigen. Die zunehmenden regulatorischen Anforderungen und Vertragsbeziehungen erfordern zudem eine rechtliche Unterstützung, was die hohe Bedeutung der Rechtsberatung mit 49 Prozent erklärt. Obwohl die Mehrheit der befragten Unternehmen in unserer Studie keine Lösegeldforderungen bezahlen möchte, besteht dennoch der Wunsch nach einer Abdeckung dieser Kosten durch Cyberversicherungen (55 Prozent). Das lässt einen gewissen Widerspruch erkennen. Ungeachtet dessen ist es ratsam, die Ressourcen für präventive Maßnahmen wie Schwachstellensuchen und die Anschaffung neuer Sicherheitstools einzusetzen, um Sicherheitsvorfälle zu verhindern und die potenziellen Schäden zu minimieren.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1 Im Vergleich zum Vorjahr ist die Anzahl der Vorfallsmeldungen weiter rückläufig. War es 2024 noch jedes fünfte Unternehmen, das keine Meldung durchführte, so meldete im Jahr 2025 bereits jedes vierte Unternehmen den Vorfall an keine Stelle.

2 Erfolgreiche Angriffe fungieren als Treiber für die Unternehmen zur Verbesserung ihrer eigenen Security-Kompetenzen. Erst nach einem Cyberangriff wird häufig in den Aufbau zusätzlicher Security-Kompetenzen und die Ausbildung der Mitarbeitenden investiert.

3 Cyberversicherungen werden intensiv diskutiert und jedes fünfte Unternehmen besitzt eine. Das ist ein leichter Rückgang gegenüber dem letzten Jahr. Oftmals klafft die Erwartungshaltung von Unternehmen im Hinblick auf die abgedeckten Leistungen der Cyberversicherungen und die Realität auseinander. Das sorgt für Verunsicherung.

Sicherheitsstrategien im digitalen Zeitalter: Ein Blick hinter die Kulissen

Das Cybercrime Competence Center (C4) ist Österreichs zentrale Anlaufstelle zur Bekämpfung von Cyberkriminalität. **Klaus Mits**, Leiter des C4, gibt Einblicke in die vielfältigen Aufgaben und die Bedeutung der Arbeit für die Sicherheit von Privatpersonen, Unternehmen und staatlichen Institutionen.

Das C4 wird als nationale Koordinierungsstelle zur Bekämpfung von Cyberkriminalität beschrieben. Welche zentralen Aufgaben übernehmen Sie in diesem Kontext? Welche Bedeutung hat Ihre Arbeit für die Sicherheit von Privatpersonen, Unternehmen und staatlichen Institutionen?

Klaus Mits: Das C4 ist die zentrale Anlaufstelle zur Bekämpfung von Cyberkriminalität und dient als nationale und internationale Ansprechstelle der Kriminalpolizei. Es sichert digitale Beweismittel und unterstützt Landeskriminalämter bei komplexen Ermittlungen. Mit Expert:innen für das Darknet, Ransomware und Kryptowährungen bietet das C4 technische Infrastruktur für Ermittlungen und ist über Europol und Interpol international vernetzt. Eine 24/7-Meldestelle ermöglicht schnelle Reaktionen bei Bedrohungen. Das C4 hat zwei Hauptaufgaben: Aufklärung und Prävention. Bei der Aufklärung werden Straftäter:innen identifiziert und zur Verantwortung gezogen, oft in Zusammenarbeit mit internationalen Ermittler:innen. In der Prävention arbeitet das C4 mit Partnern wie der Watchlist Internet und der Wirtschaftskammer Österreich zusammen, um potenzielle Opfer zu sensibilisieren und zu schützen. Neue Bedrohungen werden schnell erkannt und Informationen sowie Warnungen verbreitet, um die Öffentlichkeit zu informieren und zu schützen.

Wie hat sich das C4 seit seiner Gründung weiterentwickelt? In welcher Weise haben sich die personellen und technischen Ressourcen sowie die strategische Ausrichtung in den letzten Jahren verändert?

Klaus Mits: Mit der Gründung des Bundeskriminalamtes 2003 wurde ein Büro zur Bekämpfung von Cyberkriminalität eingerichtet. Wir starteten mit 12 Kriminalbeamt:innen, die sich auf forensische Beweissicherung konzentrierten. Die rasante Digitalisierung machte es erforderlich, unsere Mitarbeiter:innen gezielt weiterzubilden und zusätzliche Ressourcen bereitzustellen. Dadurch konnten wir spezialisierte Ermittlungsteams einrichten, die eigenständig operieren, österreichweit unterstützen, international vernetzt sind und Schulungen für die Polizei anbieten. Das Cybercrime Competence Center (C4) ist inzwischen auf über 100 Mitarbeiter:innen angewachsen, die sowohl kriminalpolizeiliches als auch wissenschaftliches Know-how einbringen. Um bei den Ermittlungen mit den Täter:innen Schritt zu halten, wurde das C4 technisch aufgerüstet. Die zentrale Beschaffung von Hard- und Software durch die Direktion Digitale Services (DDS) im Bundesministerium für Inneres hat die Effizienz gesteigert und eine Vereinheitlichung der IKT-Beschaffungen ermöglicht. Zudem wird eine technische Infrastruktur zur effizienten Bekämpfung der Cyberkriminalität geschaffen.

> **Cyberkriminalität ist ein globales Problem, das nicht auf einzelne Bereiche beschränkt ist.**

FOTO © PRIVAT

Klaus Mits, B.A., M.A. ist seit dem 10. Februar 2003 Leiter der Abteilung II/BK/5 im Bundeskriminalamt und zuständig für Cyberkriminalität. Seit 2021 leitet er das Projekt SelLE zur Schaffung einer technischen Infrastruktur für kriminalpolizeiliche Ermittlungen in Österreich. Seine Karriere begann am 16. Juli 1984 bei der österreichischen Bundesgendarmerie. Am 1. Jänner 1992 wurde er Oberleutnant und stellvertretender Referatsleiter. Am 1. Oktober 1999 wechselte er in die Verwendungsgruppe A1. Am 26. Jänner 2000 übernahm er die Leitung der Abteilung II/16. 2009 erhielt er den Bachelor of Arts in Police Leadership und 2011 den Master of Arts in Security Management.

Cyberkriminalität ist ein weit verbreitetes Problem, das häufig grenzüberschreitende Lösungen erfordert. Wie erfolgt die Zusammenarbeit mit internationalen Partnern oder nationalen Behörden?
Klaus Mits: Cyberkriminalität ist ein globales Problem, das nicht mehr auf einzelne Kriminalitätsfelder beschränkt werden kann. Deshalb ist eine intensive Zusammenarbeit sowohl national als auch international notwendig. Wir arbeiten eng mit Justizbehörden und internationalen Partnerorganisationen wie Europol und Interpol zusammen, die verlässliche Partner bei der Bekämpfung von Cyberkriminalität sind. Das C4 beteiligt sich regelmäßig an internationalen Ermittlungen und ist gut mit Cybercrime-Einheiten vieler Länder vernetzt, die auch gerne zu Hospitationen nach Österreich kommen.

In Österreich gibt es neben dem C4 auch die Direktion Staatsschutz und Nachrichtendienst (DSN), die sich mit Sicherheitsfragen beschäftigt. Was sind die Unterschiede zwischen dem C4 und der DSN, und wie sind ihre Aufgaben verteilt?
Klaus Mits: Das C4 ist für die Bekämpfung von Cyberkriminalität in kriminalpolizeilichen Bereichen zuständig, während die Direktion Staatsschutz und Nachrichtendienst (DSN) sich auf Straftaten im Zusammenhang mit Extremismus, Terrorismus und den Schutz des Staates konzentriert. Dies umfasst Bedrohungen gegen die Republik Österreich und kritische Infrastruktur, wie Cyberangriffe

> **Online-Betrugsdelikte erhalten durch KI nochmal einen Boost.**

auf Ministerien und Versorgungsunternehmen. Die unterschiedlichen Zuständigkeiten basieren auf der Art der Straftaten und den Täter:innengruppen, was verschiedene internationale Partnerschaften erfordert. Beide Direktionen tauschen regelmäßig Erfahrungen aus, da ihre technische Ermittlungsarbeit oft vor ähnlichen Herausforderungen steht. Besonders bei der Bekämpfung von Ransomware-Angriffen arbeiten das C4 und die DSN eng zusammen

Die digitale Welt entwickelt sich ständig weiter und bringt kontinuierlich neue Bedrohungen mit sich. Welche Herausforderungen sind aktuell besonders relevant, und wie wirken sie sich auf die Sicherheit von Unternehmen und Privatpersonen aus?
Klaus Mits: Unsere Aufgabe ist es, uns auf die Bekämpfung aktueller Bedrohungen vorzubereiten, indem wir die Lage analysieren und schnell auf neue Phänomene im Bereich der Cyberkriminalität reagieren. Die Herausforderungen sind vielfältig. Bei Online-Betrugsdelikten ist die große Anzahl der Fälle eine erhebliche Herausforderung, die durch den Einsatz von Künstlicher Intelligenz verstärkt wird. In anderen Bereichen, wie bei Angriffen auf Multi-Faktor-Authentifizierung, steigt die Qualität der Angriffe. Das C4 muss mit der technischen Entwicklung Schritt halten. Deepfake-Technologie stellt eine erhebliche Gefahr dar, die zu finanziellen Verlusten, Rufschädigung und Verletzungen der Persönlichkeitsrechte führen kann. Die Technologie senkt die Eintrittsbarrieren für Kriminelle und verstärkt das Bedrohungspotenzial. Unternehmen erleiden Verluste durch Betrug mit gefälschten Anrufen, und Privatpersonen werden Opfer von Erpressung und Identitätsdiebstahl.

Welche Trends konnten Sie im letzten Jahr beobachten, insbesondere im Hinblick auf neue Angriffstechnologien oder Täter:innenprofile?
Klaus Mits: Die Studie hebt den MFA Bypass als wichtigen Trend hervor, da Angriffe zur Umgehung der Multi-Faktor-Authentifizierung zunehmen. Dies verdeutlicht die technische Raffinesse der Angreifer:innen, die gezielt Kernsicherheitsmechanismen angreifen. Unternehmen sollten über die bloße Einführung von MFA hinausgehen und robustere Sicherheitsmaßnahmen sowie Monitoring in Betracht ziehen. Ein weiterer Trend ist der Anstieg von Vishing, also Telefonbetrug, was eine Verschiebung von E-Mails zu direkten

> **Unternehmen müssen sich auf eine dynamische Bedrohungslandschaft einstellen.**

Anrufen innerhalb der Social-Engineering-Taktiken darstellt. Die Täter:innenprofile sind vielfältig: Massenangreifer:innen beim Phishing, technisch versierte Gruppen beim MFA Bypass und organisierte Gruppen bei Scam Calls. Ein gemeinsames Merkmal ist ihre Anpassungsfähigkeit an Verteidigungsmaßnahmen. Diese Trends zeigen, dass Unternehmen sich auf eine dynamische Bedrohungslandschaft einstellen müssen, in der Angreifer:innen sowohl bestehende Schwachstellen ausnutzen als auch neue Technologien und Kanäle für Angriffe erschließen.

Cyberkriminelle setzen zunehmend auf fortschrittliche Technologien für ihre Angriffe. Welche aktuellen technologischen Trends bereiten Ihnen die größten Sorgen? Wie kann das C4 sicherstellen, dass es mit diesen Entwicklungen Schritt hält?
Klaus Mits: Der Einsatz von KI-basierten Generatoren in kriminellen Bereichen wie Erpressung und Betrug nimmt zu, was die Erkennung für Opfer erschwert. Die Integration von KI in „Crime-as-a-Service"-Umgebungen erhöht das Schadenspotenzial und die Profite für Täter:innen. Um solche Straftaten aufzuklären, ist es entscheidend, technisch auf dem neuesten Stand zu sein, was leistungsfähige Hardware, geeignete Software und Expert:innen erfordert. Grundlegendes Wissen muss in den Polizeiinspektionen vermittelt werden, damit Beamt:innen „cyberfit" sind. Zahlreiche Ausbildungsmaßnahmen, einschließlich neuer Cybercrime-Trainingscenter, sind wichtig, da fast jeder Fall die Sicherung digitaler Spuren erfordert. Die Aus- und Fortbildung von über 30.000 Polizist:innen ist eine große Herausforderung, die durch organisatorische Maßnahmen angegangen wird.

Wie beeinflussen geopolitische Entwicklungen Ihre Arbeit im Bereich Cybercrime-Bekämpfung?
Klaus Mits: Geopolitische Spannungen führen zu einer Zunahme und Komplexität staatlich unterstützter Cyberangriffe, die auf Spionage, Sabotage und Desinformation abzielen. Dies erfordert eine verstärkte internationale Zusammenarbeit, schnelle Anpassung an neue, oft versteckte Taktiken wie Supply-Chain-Angriffe oder den Einsatz von Ransomware zur Tarnung, sowie erhöhte Wachsamkeit beim Schutz kritischer Infrastrukturen und demokratischer Prozesse. Die Zuordnung von Angriffen wird durch den Einsatz von Proxies und kriminellen Methoden erschwert, was die Ressourcen von Verteidigerorganisationen zusätzlich

> **Fokus der Regulatorik sollte auf Prävention und Aufklärung liegen.**

belastet. Es ist entscheidend, organisatorische und nationale Resilienz sowie effektive Krisenmanagementfähigkeiten zu entwickeln, wie sie etwa durch die NIS-2-Richtlinie gefordert werden.

Cyberkriminelle nutzen immer ausgefeiltere Methoden, um ihre Ziele zu erreichen. Wie beeinflussen neue Technologien und Taktiken die Landschaft der Cyberkriminalität, und welche Strategien sind am effektivsten, um sich gegen diese sich wandelnden Bedrohungen zu verteidigen?
Klaus Mits: Die Cyberkriminalität hat sich durch neue Technologien und Taktiken stark gewandelt. Cyberkriminelle nutzen raffinierte Methoden wie Scam Calls und Ransomware, wobei emotionale Manipulation und Deepfake-Technologie eingesetzt werden, um Opfer zu täuschen. CEO-Fraud nutzt KI und Voice Cloning, um Führungskräfte zu imitieren. Um sich zu schützen, sollten Unternehmen strenge Verifizierungsprozesse und Schulungen für Social Engineering einführen. Technische

Maßnahmen wie Multi-Faktor-Authentifizierung und Anti-Phishing-Lösungen sind wichtig. Ein mehrschichtiger Ansatz gegen Ransomware, einschließlich starker Authentifizierung und Zero-Trust-Architektur, hilft, Risiken zu minimieren und die Widerstandsfähigkeit zu erhöhen.

Reicht die derzeitige Gesetzgebung aus, um moderne Bedrohungen wie KI-basierte Angriffe zu bekämpfen? In welchen Bereichen sind Ihrer Meinung nach Anpassungen oder neue Regelungen erforderlich?
Klaus Mits: Die EU hat die „Verordnung über Künstliche Intelligenz" eingeführt, die KI-Systeme nach ihrem Risikopotenzial in vier Kategorien einteilt: minimal, begrenzt, hoch und unvertretbar. Deepfakes werden als KI-erzeugte oder manipulierte Inhalte definiert, die echten Personen oder Ereignissen ähneln und fälschlicherweise als echt wahrgenommen werden könnten. Hochrisiko-KI-Systeme müssen besondere Anforderungen erfüllen, darunter Qualitätsmanagement, Datenqualität und Cybersicherheit. Betreiber von Systemen, die Deepfakes erzeugen, müssen offenlegen, dass die Inhalte künstlich sind. Ein Schwachpunkt der Regelung ist, dass die Kennzeichnungspflicht bei ausländischen Angriffen, insbesondere im politischen Kontext, an ihre Grenzen stößt. KI und Deepfakes sind nicht per se schlecht, sondern werden als Mittel für bestehende Straftaten wie Betrug genutzt. In Österreich bietet die „Servicestelle für Künstliche Intelligenz" Unterstützung zu KI-Regulierung und -Sicherheit.

> **Zero Trust ist als strategischer Ansatz unerlässlich für die Bewältigung komplexer Bedrohungen.**

Um den Herausforderungen durch KI-basierte Bedrohungen effektiv zu begegnen, ist es wichtig, den rechtlichen Rahmen zu überdenken. Statt neue Straftatbestände zu schaffen, sollte der Fokus auf Prävention und Aufklärung liegen, um Straftaten mit KI oder Deepfakes zu verhindern. Eine rechtliche Anpassung könnte darin bestehen, bei bestehenden Delikten einen Qualifikationstatbestand für das Tatmittel KI/Deepfake einzuführen, der mit strengeren Strafen belegt ist.

Welche Maßnahmen empfehlen Sie Unternehmen, um sich besser vor Cyberangriffen zu schützen?
Klaus Mits: Jede Maßnahme, die es Angreifer:innen erschwert, in Systeme einzudringen oder sich darin zu bewegen, ist hilfreich zur Vorbeugung. Das Zero-Trust-Modell ist für Unternehmen jeder Größe sinnvoll, da es Sicherheitsherausforderungen moderner IT-Umgebungen wie Cloud, Remote-Arbeit und interne/externe Bedrohungen adressiert. Die Prinzipien „Niemals vertrauen, immer überprüfen", geringste Rechtevergabe und die Annahme einer Kompromittierung sind zukunftsweisend.

Allerdings ist die vollständige Umsetzung einer Zero-Trust-Architektur nicht für jedes Unternehmen sofort möglich. Die Umsetzbarkeit hängt von Faktoren wie Unternehmensgröße, verfügbaren Ressourcen, der Komplexität der IT-Infrastruktur und der Unternehmenskultur ab. Für kleine und mittlere Unternehmen (KMU) ist eine vollständige Architektur oft unrealistisch, aber die Einführung von Kernprinzipien wie Multi-Faktor-Authentifizierung und geringste Rechtevergabe ist machbar und empfehlenswert. Cloud-Lösungen oder externe Dienstleister können dabei unterstützen.

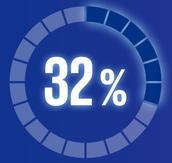
Halten Sie Zero-Trust-Sicherheitsstrategien für entscheidend, um sich gegen zukünftige Angriffe zu schützen?
Klaus Mits: Zero-Trust-Sicherheitsstrategien sind entscheidend für den Schutz vor modernen Cyberangriffen, einschließlich KI-gestützter Bedrohungen. Traditionelle Sicherheitsmodelle reichen nicht mehr aus. Zero Trust erschwert durch „Least Privilege Access" und Mikrosegmentierung die Bewegung von Angreifer:innen im Netzwerk, begrenzt den Schaden bei Angriffen und schützt gegen KI-gestützte Angriffe durch starke Authentifizierung und kontinuierliche Verifizierung. Es ist anpassungsfähig für moderne IT-Umgebungen und erhöht die Widerstandsfähigkeit gegen Cyberangriffe. Als strategischer Ansatz ist Zero Trust unerlässlich für die Bewältigung komplexer Bedrohungen. Ob es auch in Zukunft ausreicht, ist ungewiss, da sich die Technologie schnell entwickelt.

Welche neuen Bedrohungen erwarten Sie in den kommenden Jahren im Bereich Cybercrime und wie plant das C4, auf diese zukünftigen Herausforderungen zu reagieren?
Klaus Mits: Jede neue Technologie, die unser Leben positiv beeinflusst, kann auch von Kriminellen genutzt werden, einschließlich KI. KI senkt die technischen Hürden und ermöglicht es auch weniger erfahrenen Akteur:innen, komplexe Angriffe durchzuführen. Sie beschleunigt den Angriffszyklus und erhöht die Komplexität und Effektivität von Cyberangriffen, wodurch traditionelle Abwehrmaßnahmen zunehmend herausgefordert werden. Neben KI könnte auch die Entschlüsselung von derzeit sicheren Informationen durch Quantencomputing in Zukunft eine große Herausforderung darstellen. Wir planen die Umsetzung der Kriminaldienstreform zur Bekämpfung von Internetkriminalität und werden die Zusammenarbeit mit dem Justizministerium intensivieren. Zudem werden wir Präventionskampagnen ausbauen und die Kooperation zwischen öffentlichen und privaten Einrichtungen verstärken.

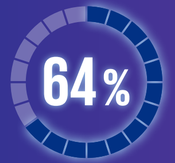
Wenn wir beide uns in 12 Monaten wieder treffen, was würden wir uns dann wünschen, heute schon getan zu haben?
Klaus Mits: Die Bekämpfung der Cyberkriminalität erfordert das gemeinsame Engagement von Staat, Unternehmen, Bürger:innen und der internationalen Gemeinschaft. Der Staat muss Gesetze erlassen und Ressourcen bereitstellen, während Unternehmen ihre Systeme sichern und Mitarbeiter:innen schulen sollten. Bürger:innen müssen sich über Risiken informieren und eigene Schutzmaßnahmen ergreifen. International ist Zusammenarbeit nötig, um globale Standards zu entwickeln. Die Förderung des Cybersicherheitsbewusstseins und die Unterstützung von Forschung und Entwicklung sind ebenfalls wichtig. Unternehmen sollten ein umfassendes Sicherheitskonzept haben, regelmäßige Sicherheitsaudits durchführen, einen Incident-Response-Plan bereitstellen, Mitarbeiter:innen schulen und ihre Systeme auf die neuesten Sicherheitsstandards bringen.

05 Third Party Risk

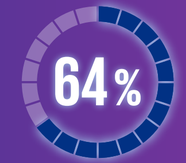
Durch die Vernetzung von Geschäftsprozessen rückt die gegenseitige Abhängigkeit im digitalen Raum immer mehr in den Fokus. Cyberkriminelle wählen als Einfallstor in heimische Unternehmen oftmals Lieferanten oder Dienstleister – sie gelten immer noch als schwächstes Glied in der Kette. Austausch und Zusammenarbeit zwischen Unternehmen und Lieferanten bzw. Dienstleistern ist wichtiger denn je, um Systemsicherheit und Resilienz gegen Cyberangriffe zu garantieren bzw. um hier geeignete Schutzmaßnahmen auszubauen.



bestätigen konkrete Cyberangriffe auf ihre **Lieferkette**.

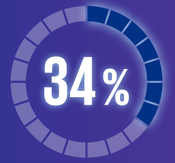


wissen nicht, welche Auswirkungen Angriffe auf die Lieferkette für sie hatten.

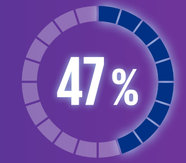


haben Bedenken, dass **Cyberangriffe gegen ihre Dienstleister** Auswirkungen auf sie selbst haben werden.

ist nicht bekannt, **welche Tätigkeiten zur Gewährleistung** der Sicherheit bei ihren Lieferanten oder Dienstleistern durchgeführt werden.



fordern zur Gewährleistung der Sicherheit bei ihren Lieferanten oder Dienstleistern eine **Zertifizierung** an.



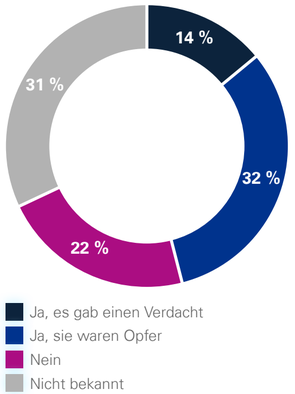
fürchten, dass Zulieferer nicht dieselben **Sicherheitsstandards** einhalten, wie sie selbst, und so zum Einfallstor für Angriffe werden können.

Angriffe auf Dienstleister oder Lieferanten

Unternehmen wissen mittlerweile, dass Cyberangriffe auf ihre eigenen Systeme zu massiven Schäden und Beeinträchtigungen führen können. Aus diesem Grund haben sie ihre Schutzmaßnahmen verbessert, Sicherheitssysteme etabliert und Investitionen in Angriff genommen, um ihre Cybersicherheit auf ein neues Niveau zu heben. Diese Trendwende haben auch Cyberkriminelle erkannt. So sehen wir eine Verlagerung der Angriffe hin zu Kund:innen und Lieferantensystemen, die über die Lieferkette mit dem eigentlichen Unternehmen, das als Ziel ausgekundschaftet wurde, in Verbindung stehen.

Angriffe auf die Lieferkette haben in den letzten Jahren immer mehr an Bedeutung gewonnen, denn sie ist oftmals das schwächste Glied in der gesamten digitalen Supply Chain. Das bestätigen auch unsere Umfrageergebnisse: Die Ergebnisse unserer Umfrage zeigen, dass 32 Prozent der Unternehmen konkrete Cyberangriffe auf ihre Lieferkette bestätigen – ein Wert, der die zunehmende Professionalisierung von Angreifer:innentaktiken widerspiegelt. Cyberangriffe auf Managed Service Provider (MSP), Cloud-Dienstleister oder Logistikpartner ermöglichen es Cyberkriminellen, über Schwachstellen Dritter in hochgesicherte Netzwerke einzudringen (z. B. SolarWinds-Angriff). Die zusätzlichen 14 Prozent Verdachtsfälle deuten auf unzureichende Forensik-Kapazitäten hin: Viele Unternehmen können Incident-Spuren nicht bis zur Quelle zurückverfolgen, insbesondere bei Angriffen über Shared-Service-Plattformen oder Supply-Chain-Softwarebibliotheken (z. B. Compromises via npm-Pakete).[1]

Abb. 14: Waren Ihre Dienstleister/ Lieferanten in den letzten 12 Monaten von Cyberangriffen betroffen?



Die 31 Prozent unbekannter Fälle offenbaren ein strukturelles Problem: Trotz unterschiedlicher regulatorischer Vorgaben fehlen in vielen Verträgen klare SLAs (Service Level Agreements) zur Meldung von Sicherheitsvorfällen. Unternehmen mit veralteten Vendor-Risk-Management-Programmen verlassen sich oft auf jährliche Selbstauskünfte der Lieferanten statt auf Echtzeit-Monitoring via APIs oder Security Rating Services. Verglichen mit dem Jahr 2024, als diese Kennzahlen erstmals erhoben wurden, zeigt die leichte Verschiebung von „Nicht bekannt" zu konkreten Meldungen, dass die Einführung von Third-Party-Risk-Management-Tools erste Wirkung zeigt – jedoch noch nicht flächendeckend.

Auswirkungen von Third-Party-Angriffen

64 Prozent der befragten Unternehmen ist nicht bekannt, welche Auswirkungen Angriffe auf die Lieferkette für sie hatten. Das ist durchwegs verwunderlich und man sieht einmal mehr, dass vor allem die Zusammenarbeit mit Lieferanten und Dienstleistern von besonderer Bedeutung ist. Bei jedem zehnten Unternehmen gab es aufgrund des Angriffs auf die Lieferkette direkte Angriffe auf das eigene Unternehmen. Das veranschaulicht die Vorgehensweise von Cyberkriminellen, die sich über den Dienstleister in die Unternehmen einschleusen. Eine intensive Zusammenarbeit, ein transparenter und offener Austausch zur Verbesserung der Cybersicherheit sind deshalb essenziell.

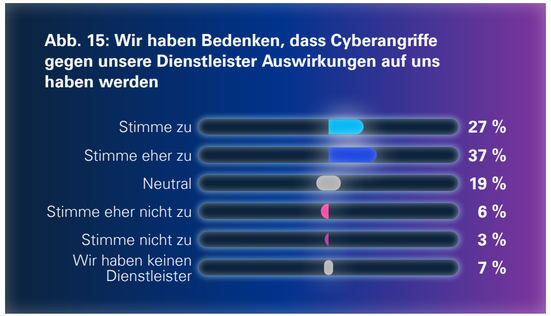
[1]https://www.bleepingcomputer.com/news/security/new-npm-attack-poisons-local-packages-with-backdoors/, abgerufen am: 16.04.2025.

Unternehmen berichten auch darüber, dass sie eingeschränkte Serviceleistungen und Projektverzögerungen, wie etwa einen kurzfristigen Stillstand des Bestellsystems aufgrund einer Denial-of-Service-Attacke auf einen Cloud-Dienstleister, erlebt haben. Angriffe führten zu erhöhten Aufwendungen in den Bereichen Cybersecurity und Business Continuity. Unternehmen mussten zusätzliche Maßnahmen ergreifen, wie das Trennen von Verbindungen und die Überprüfung der Systemintegrität, um ihre Sicherheit zu gewährleisten. Einige Unternehmen wollen ihre Nutzung von Cloud-Diensten überdenken, während andere von der Vielfalt des Marktes profitieren und nicht von einzelnen Lieferanten abhängig sind. Insgesamt zeigen diese Aussagen, dass die Angriffe zwar keine gravierenden Betriebsunterbrechungen verursachten, jedoch einen erhöhten Aufwand für die Absicherung und Anpassung der Sicherheitsprozesse mit sich brachten.

3rd Party Risk

Angriffe auf das eigene Unternehmen über den Dienstleister rücken immer mehr in den Fokus. Damit stellt sich auch die Frage, ob heimische Unternehmen Bedenken haben, dass Cyberangriffe gegen ihre Dienstleister Auswirkungen auf sie selbst haben werden. Knapp zwei Drittel der befragten Unternehmen (64 Prozent) haben Bedenken, dass genau durch diese Art von Angriffen ein Zugriff bzw. damit einhergehende Auswirkungen auf das eigene Unternehmen erfolgen können. 9 Prozent verspüren keine Auswirkungen.

Abb. 15: Wir haben Bedenken, dass Cyberangriffe gegen unsere Dienstleister Auswirkungen auf uns haben werden



Anhand dieser Ergebnisse ist ein eindeutiger Trend erkennbar, dass die Abhängigkeit im digitalen Raum über die Vernetzung von Geschäftsprozessen immer mehr in den Mittelpunkt rückt und unsere digitale Resilienz dadurch beeinflusst wird. Es hat ein Paradigmenwechsel zu erfolgen: Wir müssen weg von gegenseitigen Schuldzuweisungen und Fingerzeigen hin zu einem vernetzten und abgestimmten Miteinander. Sowohl auf Seiten der Auftraggeber und des Unternehmens als auch auf der Seite des Dienstleisters muss es zu einem eng verwobenen Austausch und einer Zusammenarbeit kommen, um die Sicherheit der Systeme und die Widerstandsfähigkeit zu verbessern.

Gewährleistung der Sicherheit

Zusammenarbeit und Transparenz erfordern auch offenen Austausch. Ein offener Austausch impliziert, dass die Gewährleistung der Sicherheit mit den Lieferanten und Dienstleistern regelmäßig zu prüfen ist. Unternehmen ergreifen eine Vielzahl von Maßnahmen, um diese Sicherheit zu gewährleisten.

Interessanterweise geben jedoch auch 38 Prozent der befragten Unternehmen an, dass ihnen nicht bekannt ist, welche Tätigkeiten zur Gewährleistung der Sicherheit bei ihren Lieferanten oder Dienstleistern durchgeführt werden. An zweithäufigsten mit 34 Prozent sagen die Befragten, dass sie eine Zertifizierung anfordern. An dritter Stelle mit 27 Prozent finden wir einen Fragebogen zur Selbstdeklaration. Diese Aktivitäten dienen ausschließlich des schriftlichen Nachweises, geben aber wenig Auskunft darüber, ob tatsächlich wirksame technische und organisatorische Maßnahmen durchgeführt werden. 26 Prozent der befragten Unternehmen haben ein eigenständiges Audit durchgeführt, 19 Prozent haben ein Audit durch Dritte durchführen lassen.

Auch vertragliche Vereinbarungen, die spezifische Sicherheitsmaßnahmen vorschreiben, wie NDAs (Non-Disclosure Agreements), AVVs (Auftragsverarbeitungsverträge), Sonderklauseln und SLAs werden von Unternehmen eingesetzt, um die Sicherheit bei Lieferanten und Dienstleistern zu gewährleisten. Einige Unternehmen setzen auf Eigenentwicklungen, anstatt Lösungen zuzukaufen, um so die Kontrolle über die Sicherheit zu behalten. Sie möchten die Abhängigkeit von Lieferanten und Dienstleistern reduzieren, um einen Vendor Lock-in zu vermeiden. Der Fokus liegt hier auf

Die besorgniserregende Verwundbarkeit der Lieferkette macht den Menschen zum essenziellsten Glied in der Kette.

Open-Source-Software und eigenen Code-Analysen. Außerdem werden Foren, Mailinglisten und Bug-Tracking-Systeme (BTS) verfolgt. Für KMUs ist es allerdings schwieriger, Sicherheitsgarantien von Lieferanten einzufordern, da sie wirtschaftlich weniger Einfluss haben. Dennoch versuchen die von uns befragten Unternehmen durch Besprechungen und Mitigationsstrategien ihre Sicherheitslage zu erhöhen.

Supply-Chain-Software

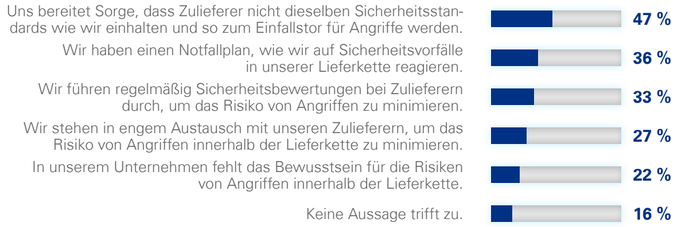
Auf die Frage, ob Angriffe gegen die Development-Pipeline in der Software-Entwicklung (Software Supply Chain Attack) für Unternehmen ein großes Risiko darstellen, geben 55 Prozent an, dass sie in der Tat Risiken sehen. Dieses Ergebnis ist nicht weiter verwunderlich, da vor allem die Manipulation von Codes oder Softwareteilen eine nachhaltige Beeinträchtigung der Funktionalität mit sich bringt. Auch besteht das Risiko, das Backdoors oder Kill Switches in den Code eingeschleust werden, die für unerlaubte Dritte Zugriff auf die Systeme ermöglichen.

Vor allem aber auch die Nutzung von Online Code Repositories, wie sie bei GitHub oder anderen Plattformen zu finden sind, bergen ein inhärentes Risiko, dass nicht qualitätsgesicherter Softwarecode in Umlauf kommt und dadurch Schadcode in die Anwendungen eingebaut wird. Gerade der Komfort, den diese Plattformen bieten, dass schnell und unkompliziert Softwarecodeteile entnommen werden können, erleichtert es Angreifer:innen, Manipulationen in der Software-Entwicklungspipeline durchzuführen. In den letzten Monaten haben vor allem staatliche oder staatlich unterstützte Akteur:innen die Gutgläubigkeit, mit der dieser Code verwendet wird, ausgenutzt. Das potenzielle Risiko, dass dadurch unerlaubter Zugriff auf IT-Systeme, Daten und Anwendungen sowie Cloud-Instanzen und sensible Unternehmensinformationen durch Dritte möglich ist, darf keinesfalls unterschätzt werden.

Risiko Lieferkette

Blicken wir nun auf die Lieferkette und die damit

Abb. 16: Lieferketten-Risiko



verbundenen Risiken, die daraus entstehen, so zeichnet sich ein durchaus differenzierteres Bild. 47 Prozent der Befragten haben Bedenken, dass Zulieferer nicht dieselben Sicherheitsstandards einhalten, wie sie selbst und so zum Einfallstor für Angriffe werden können. Nur 36 Prozent der befragten Unternehmen geben an, dass sie einen Notfallplan haben, wie auf Sicherheitsvorfälle in der Lieferkette reagiert werden muss. In diesem Punkt gibt es also noch enormes Verbesserungspotenzial.

Jedes dritte Unternehmen (33 Prozent) führt regelmäßig Sicherheitsbewertungen bei Zulieferern durch, um das Risiko von Angriffen minimieren zu können. Genau diese Bewertungen fördern auch den Austausch: 27 Prozent der befragten Unternehmen stehen in einem engen Austausch mit den Zulieferern. Bedenklich ist allerdings, dass knapp mehr als jedes fünfte Unternehmen (22 Prozent) angibt, dass im Unternehmen das Bewusstsein für Angriffe innerhalb der Lieferkette fehlt. Gerade unter dem Aspekt der zunehmenden Bedeutung der Angriffe auf die Lieferkette und der Zahlen aus dieser Studie, die eindeutig zeigen, dass eine Verlagerung der Angriffe auf den Dienstleister erfolgt, ist hier definitiv Handlungsbedarf gegeben.

Anhand der Umfrageergebnisse bemerken wir einen Reifungsprozess im Third-Party-Risikomanagement: Im Jahr 2025 priorisieren Unternehmen nicht mehr nur die eigene Perimeter-Sicherheit, sondern analysieren ihre erweiterte Attack Surface durch Cyber Supply Chain Mapping. Die Lücken zwischen Risikowahrnehmung (47 Prozent), Incident-Häufigkeit (46 Prozent) und Schutzmaßnahmen (36 Prozent) verdeutlichen jedoch, dass sich viele Unternehmen noch in der Übergangsphase weg von punktuellen Audits und hin zu integrierten, datengesteuerten Lieferketten-Ökosystemen befinden. Regulatorischer Druck und steigende Cyber-Versicherungsprämien werden diesen Transformationsprozess weiter beschleunigen.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1. Bei jedem zehnten Unternehmen gab es aufgrund des Angriffs auf die Lieferkette direkte Angriffe auf das eigene Unternehmen. Cyberkriminelle schleusen sich über den Dienstleister in die Unternehmen ein. Eine intensive Zusammenarbeit, ein transparenter und offener Austausch zur Verbesserung der Cybersicherheit sind deshalb essenziell.

2. Die Abhängigkeit im digitalen Raum über die Vernetzung von Geschäftsprozessen rückt immer mehr in den Mittelpunkt. Es hat ein Paradigmenwechsel zu erfolgen weg von gegenseitigen Schuldzuweisungen hin zu einem vernetzten und abgestimmten Miteinander. Nur durch Austausch und Zusammenarbeit können die Sicherheit der Systeme und die Widerstandsfähigkeit verbessert werden.

3. Unternehmen priorisieren nicht mehr nur die eigene Perimeter-Sicherheit, sondern analysieren ihre erweiterte Attack Surface. Jedoch befinden sich viele noch in einer Übergangsphase und müssen weg von punktuellen Audits hin zu integrierten, datengesteuerten Lieferketten-Ökosystemen. Regulatorischer Druck und steigende Cyber-Versicherungsprämien werden diesen Transformationsprozess weiter beschleunigen.

Building resilience: Lessons from Multinational Collaboration

Jean Nicolas Gauthier, regional security Officer at Siemens AG, emphasizes the importance of conducting risk assessments and raising security awareness among employees. Discover how sharing knowledge across countries can enhance preparedness and resilience in the face of global threats.

How have your military and corporate security experiences shaped your approach to cybersecurity and crisis management, and how can these be applied in your current corporate role?
Jean Nicolas Gauthier: Although I'm not a cybersecurity specialist, my extensive crisis management experience, including leading multinational teams, has shaped my approach to cybersecurity and crisis management. Collaborating with international partners has highlighted the importance of information sharing and collective action against cross-border threats. My military background, particularly in logistics and resource allocation, is valuable in the corporate sector. Lessons from the French Navy, such as the use of checklists and crisis preparedness documentation, are practical tools applicable at all levels. Connecting with partners and sharing information is crucial to avoid isolation and enhance effectiveness.

Are there any principles from military crisis management that you think can be effectively applied in a corporate context?
Jean Nicolas Gauthier: As a commanding officer, decision-making is straightforward with a prepared team. However, my experience in international staff and planning was crucial for handling crises like piracy in the Indian Ocean, revealing broader regional implications. Crisis management pprinciples are consistent: establish facts, set objectives, prepare options, and present them to decision-makers. A clear command structure and situational assessment are vital. To prevent escalation, proactive risk mitigation, preemptive measures, disciplined communication, adaptability, and agility are essential. These principles apply in both military and civilian contexts.

Which significant events or cyber incidents from

FOTO © PRIVAT

Erfahren Sie mehr in unserem Podcast IMPULSE

Jean Nicolas Gauthier has been Siemens AG's Regional Security Officer for Europe, Central Asia, and Israel since January 2022, based in Vienna. A retired Rear Admiral and former helicopter pilot in the French Navy, Gauthier is a naval engineer with a degree in aeronautics. He has ledmulti-disciplinary teams in military and civilian roles across several countries. After his naval career, he joined Siemens France in 2017, gaining insights into industrial transformation and technological innovation. From 2018 to 2021, he was the Regional Security Officer for Western Europe and the Maghreb, based in the UK. In his current role, Gauthier focuses on protecting Siemens' people and assets, supporting security measures, business continuity, and crisis management, including operations in Ukraine and Israel.

It's essential to foster a culture of security and cybersecurity awareness, as well as resilience.

the past decade have most impacted our security landscape, and how have they influenced strategies in Europe and Central Asia?
Jean Nicolas Gauthier: The COVID-19 pandemic, along with cyber incidents like the WannaCry ransomware attack, NotPetya malware outbreak, Log4j vulnerability, and the CrowdStrike incident, have significantly impacted the security landscape over the past decade. These events led to a stronger focus on incident response planning and enhanced collaboration and information sharing among regional organizations and international partners, particularly in Europe and Central Asia. Additionally, there was an increased emphasis on supply chain security and risk assessment in third-party relationships.

In your role at Siemens, you coordinated security measures across various industries. Which strategies have proven to be the most effective in responding to cyber or security threats? Additionally, how has your military experience contributed to these efforts?
Jean Nicolas Gauthier: I've learned a lot from my military experience, as well as from working in the industry, which is well-organized. It's important to establish a centralized and global threat intelligence and incident monitoring system to quickly detect, analyze, and share information. Incident response and crisis management protocols should be developed to align with local regulations. Close collaboration and information sharing with governmental agencies, not just military ones, are crucial to leverage their expertise and influence. We now have a good system coordinating civilian and military efforts with various agencies. It's also essential to foster a culture of security and cybersecurity awareness, as well as resilience. My experiences with crises in Ukraine and Israel have shown me the importance of resilience, and I believe we are not yet fully prepared for such crises. Finally, thorough risk assessments should be conducted, and multilayered security defenses should be implemented.

Establishing a centralized threat intelligence system is crucial for rapid detection and information sharing.

How has leading multinational teams influenced your approach to crisis management, and what challenges and advantages do you see in collaborating across diverse cultures and regions?
Jean Nicolas Gauthier: Leading multinational teams has enhanced my approach to crisis management by emphasizing the importance of considering geopolitical tensions and reallocating resources based on the evolving threat landscape. While challenges such as language barriers and cultural differences exist, the advantages of diverse perspectives and expertise outweigh them. Effective communication and collaboration are crucial for organizing and sharing knowledge. Multinational teams facilitate the sharing of best practices and lessons learned, as demonstrated during COVID-19, and help address globally interconnected crises, strengthening international cooperation and trust.

Given your experience as a naval attaché in your military assignment, how has this influenced the way you approach incidents, crises, and various situations?
Jean Nicolas Gauthier: I learned a lot about diplomatic skills, which are crucial for enhancing cultural awareness and sensitivity in actions. These skills improve communication and collaboration with stakeholders from diverse backgrounds. Negotiating with government authorities in complex regulatory environments is vital in crisis situations. Managing tense situations and maintaining composure under pressure are essential for incident response. As a diplomat, I established valuable networks and relationships that are key in crisis management. I regularly use my diplomatic network to stay informed about situations in different countries and to connect with the right people when needed. Additionally, diplomatic roles enhance conflict resolution and consensus-building skills, which I believe I developed significantly during my time in this position.

In the diplomatic field, you learn that words matter and can either escalate or de-escalate a situation. What is your observation in the corporate and business world? Are we aware of the power of words, or do we tend to escalate situations quickly by using language that may be overly excited or inappropriate?
Jean Nicolas Gauthier: I believe that while companies have strong communication departments focused on recruiting talent and advertising, crisis communication is a specific skill that requires trained individuals. It's crucial to be part of the cri-

sis communication process to improve effectiveness. I agree that sometimes the choice of words can have a greater impact than the actual facts, so we must be careful. Training leadership in handling such situations is important, and at Siemens, this is done. I recommend that leadership teams receive training in this specific skill as part of my advisory role.

Does the level of excitement in communication sometimes accelerate situations prematurely, leading to escalation? Additionally, do people tend to communicate beliefs rather than facts, and how does this affect control over the situation?
Jean Nicolas Gauthier: It's important to stay calm and think twice before speaking. Unfortunately, some businesses have failed because they used the wrong wording or exposed their leadership to the media too early. As part of our training, we emphasize the importance of managing emotions and being cautious in communication. It's crucial to work with experts who can provide the right advice at the right time and to listen to them. You need to prioritize based on your assessment of the situation, which isn't always easy. That's why raising awareness on this topic is important. Siemens excels in this area with a strong cybersecurity organization that offers mandatory training every year, featuring concrete and practical examples. This approach is vital because people need to see real-world examples rather than just theoretical processes

Cultural diversity and varying levels of security maturity are crucial factors to consider.

When dealing with hybrid threats, awareness is crucial. What role does AI play in educating and training security experts, and how can it be used to combat disinformation threats from your perspective?
Jean Nicolas Gauthier: AI plays a significant role in education and training, and I must emphasize that. In Austria, a lot is being done in this area, which I greatly appreciate. We need to educate our people to combat disinformation. AI is an asset because it allows us to develop learning platforms and personalize the educational experience for security professionals, which is quite important. Although I'm not an AI specialist, I see the necessity of using generative AI models to create realistic training data and simulations, helping us better prepare for a wide range of cyber threats, including disinformation campaigns.

I would like to quote French political scientist François Bernoulli, who categorized information warfare into three areas: ‚war on information,' which includes denial of service, ransomware, system disruptions, and data corruption; ‚war by information,' which involves fake news and disinformation; and ‚war for information,' which includes phishing and social engineering. We must face these threats, and AI can help us distinguish between them and effectively educate and prepare our people. But AI should be seen as an advantage because it helps us detect, analyze, and counter threats more quickly than before.

In your role, covering a wide geographical area, do you encounter different challenges in combating disinformation across the regions where you have worked?
Jean Nicolas Gauthier: Yes, linguistic and cultural diversity make it challenging to identify, detect, and counter threats. This is why we need local networks to help us detect weak signals. Additionally, there are varying levels of digital literacy, media awareness, and consumption habits across regions, which means our awareness campaigns may not be suitable for every country. Differences in legal and regulatory frameworks also pose challenges. The rapid spread of disinformation through social media, the dark web, and encrypted messaging apps is a significant challenge, especially when state-sponsored campaigns are involved.

These factors complicate the development of effective counter-strategies.

Based on your experience, what best practices in crisis management should companies implement today to prepare for future threats?
Jean Nicolas Gauthier: To prepare for future threats, companies should implement a comprehensive crisis management framework with clearly defined roles, responsibilities, and decision-making processes. Regular risk assessments, simulation exercises, and scenario-based training are essential. A robust business continuity framework and disaster recovery strategy are crucial, as these are the business's responsibility. Fostering a culture of crisis preparedness and developing resilience among employees is important, though challenging. Leadership commitment is vital, along with strong communication protocols and strategies for effective crisis communication. Plans should be regularly reviewed and updated to adapt to the volatile world, which is why digitalizing crisis plans and introducing AI scenario planning is beneficial.

Which trends and technologies do you think will shape cybersecurity and crisis management in the next 5 to 10 years? What can we expect?
Jean Nicolas Gauthier: It's challenging to predict the future, especially with the rapid changes in the world, but I can highlight several key trends.

Crisis communication is a specific skill that requires trained individuals.

First, integrating geopolitical and threat intelligence into crisis management strategies is crucial. Second, advancements in artificial intelligence and machine learning will enhance threat detection, incident response, and predictive capabilities. Third, there will be increased adoption of cloud-based security solutions, which have both benefits and drawbacks. Cybersecurity must be integrated into broader digital transformation initiatives. Quantum computing is expected to emerge soon, potentially altering cryptography and the security landscape. As Siemens is an industrial company, the expansion of the Internet of Things and its associated security challenges is a significant trend. Lastly, there should be a stronger focus on supply chain security and effective third-party management.

Is there anything else you'd like to share about your global perspective on crisis management or your experience with a multinational team?
Jean Nicolas Gauthier: It's crucial to conduct comprehensive risk assessments and utilize modern technologies to be prepared. Raising security awareness among employees is essential, and every company should have a robust crisis management framework and business continuity plans. Enhancing expertise in cybersecurity is vital, as the threat landscape is growing, necessitating more trained professionals. Additionally, it's important to be aware of global practices, not just those in our own country, and learn from others. Sharing knowledge across countries, especially within the European Union, can improve preparedness.

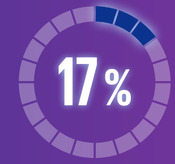
If we were to meet again in 12 months, what would we wish we had done today?
Jean Nicolas Gauthier: We need to accelerate our adoption of emerging technologies like AI and quantum computing to stay ahead of threats. Instead of resorting to protectionism, we should enhance cross-border collaboration and information-sharing mechanisms. Investing in training and developing a highly skilled cybersecurity and crisis management workforce is crucial. As the world becomes tougher, we must strengthen the resilience of our companies, critical infrastructure, supply chains, and people, who may not be as prepared for severe crises. I'm impressed by how our colleagues in Ukraine, Israel, and nearby regions continue working despite various threats, and we can learn a lot from them.

06 Künstliche Intelligenz

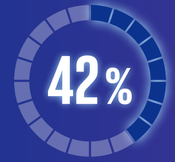
Künstliche Intelligenz erlebt gerade eine Revolution, in der viele Versprechen gemacht und neue Dinge angepriesen werden. Abseits des kreativen Bereichs (Bilder malen, Musik generieren) hilft sie Unternehmen dabei, ihre Effizienz zu verbessern. Auch in der Abwehr von Cyberangriffen erleben wir große Fortschritte durch KI. Doch diese Entwicklungen stehen auch den Cyberkriminellen zur Verfügung, die ihre Angriffstaktiken weiterentwickeln und verfeinern. Mit ihnen befinden wir uns im Wettlauf.

sehen **Künstliche Intelligenz** (eher) als Chance.

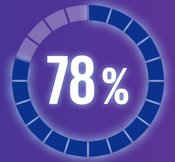
beschäftigen sich bereits mit dem Einsatz von **KI zur Verbesserung der Cybersecurity.**



sagen, dass es **keine Regeln** für den KI-Einsatz für Mitarbeitende benötigt.



Als größtes Hemmnis beim KI-Einsatz werden mit 42 % **Datenschutzanforderungen** gesehen.



sagen, dass sich mit der Einführung neuer Technologien wie KI die **Bedrohungslage verschärft.**

KI – Chance oder Risiko?

Für Unternehmen stellt sich angesichts der rasanten technologischen Entwicklungen die Frage, ob KI Chance oder Risiko ist und wie sie damit umgehen werden. 60 Prozent der Befragten geben an, dass sie KI (eher) als Chance sehen. 31 Prozent ordnen KI neutral ein, knapp jedes zehnte Unternehmen (9 Prozent) befindet KI als Risiko. Somit ist eindeutig der Trend erkennbar, dass die Chancen überwiegen und die Risiken, wenngleich diese zweifelsfrei in der Verwendung der neuen Technologie existieren, eher in den Hintergrund rücken.

Beschäftigung mit KI

Neben Arbeitserleichterung und Effizienzgewinnen in den Unternehmensabläufen bieten KI-Lösungen auch Verbesserungen im Bereich der Cybersicherheit. Viele Hersteller bieten Lösungen an, die scheinbar mit KI ausgestattet sind. Inwieweit es sich dabei um reine Algorithmen handelt, die mit etwas Intelligenz „aufgefettet" sind, oder um tatsächliche KI-Lösungen, ist noch nicht durchgängig erkennbar. Bei den von uns befragten Unternehmen besteht aber durchaus der Wille bzw. der Bedarf, sich mit dem Thema KI zur Verbesserung der Cybersicherheit auseinanderzusetzen. Mehr als jedes vierte Unternehmen (26 Prozent) beschäftigt sich bereits mit dem Einsatz von Künstlicher Intelligenz zur Verbesserung ihrer Cybersecurity. 29 Prozent beschäftigen sich aktuell noch nicht damit, sagen aber, dass das Thema für sie von Bedeutung ist. Ein Drittel der Befragten gibt an, dass sie sich noch nicht damit beschäftigt haben und das Thema für sie auch keine Relevanz hat.

Es ist wichtig, sich beim Einsatz von Künstlicher Intelligenz zur Verbesserung der Cybersicherheit mit den Risiken, die durch den Einsatz der neuen Technologien entstehen, auseinanderzusetzen. Wiewohl Möglichkeiten bestehen, komplexe Sachverhalte interpretieren zu lassen und Verknüpfungen zu machen, die vorher nicht möglich waren, sind diese Werkzeuge auch fehlerbehaftet und die eingesetzten Algorithmen weisen ein gewisses Bias auf. Eine ausgewogene Analyse und Abwägung der Vorteile und Risiken ist für Unternehmen unerlässlich.

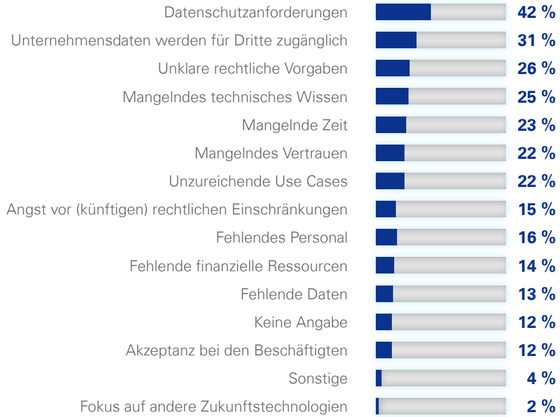
Regeln für den Einsatz von KI

KI ist wie ein Tsunami auf uns zugekommen. Unternehmen waren quasi über Nacht damit konfrontiert, sich mit diesen neuen Entwicklungen und Technologien auseinanderzusetzen und die regelbasierten Ordnungen in Unternehmen wurden komplett ausgehebelt. Auf die Frage, ob Unternehmen Regeln für den Einsatz von Künstlicher Intelligenz für Mitarbeitende haben, gibt mehr als ein Viertel (27 Prozent) an, dass bereits Regeln etabliert wurden. 22 Prozent haben aktuell keine Regeln, planen aber welche einzuführen. 17 Prozent sind der Meinung, dass es keine Regeln benötigt und hierfür auch keine weiteren Aktivitäten durchgeführt werden. Interessant ist, dass, obwohl knapp ein Viertel der Befragten (24 Prozent) sich bereits mit dem Thema beschäftigt hat und KI verwendet, diese sich noch nicht damit auseinandergesetzt haben, ob es Regeln für die Verwendung in der Organisation benötigt. Diese Dynamik sowie der Umgang mit den neuen Technologien, die von Mitarbeiter:innen frei im Internet genutzt werden können, stellt Unternehmen vor besondere Herausforderungen.

Hemmnisse für den Einsatz von KI

Obwohl aktuell die Chancen überwiegen und Unternehmen viel Potenzial in den Einsatzmöglichkeiten von KI sehen, gibt es auch gewisse Vorurteile und Hemmnisse. Als größtes Hemmnis beim KI-Einsatz werden mit 42 Prozent die Datenschutzanforderungen gesehen. Es ist nicht weiter verwunderlich, denn der Schutz der (personenbezogenen) Daten steht an oberster Stelle und es ist nicht immer durchwegs klar, ob bzw. welche dritten Parteien Zugriff auf die Daten erhalten. An zweiter Stelle finden wir mit 31 Prozent die Sorge, dass Unternehmensdaten für Dritte zugänglich gemacht werden. Das steht in direktem Zusammenhang mit den Datenschutzanforderungen. KI erfordert, dass Daten auf Portalen hochgeladen und somit in Rechenzentren verarbeitet und analysiert werden. Dadurch ist es unumgänglich, dass Dritte in den Besitz dieser Daten kommen. Hier ist jedenfalls klar abzuwägen, welche Informationen das eigene Unternehmen verlassen und in weiterer Folge durch die KI analysiert werden dürfen.

Abb. 17: KI-Einsatz Hemmnisse



An dritter Stelle stehen die unklaren rechtlichen Vorgaben. Mehr als jedes vierte Unternehmen (26 Prozent) hat Zweifel, welche rechtlichen Vorgaben für die Verwendung von KI existieren. Denken wir zum Beispiel an den Datentransfer, so ist unklar, in welches Land die Daten übermittelt werden.

Die Qualität der derzeit verfügbaren Tools und Large Language Models (LLMs) ist für die Unternehmen ein weiteres Hindernis, da diese oftmals fehleranfällig sind und nicht immer zufriedenstellende Antworten liefern. Auch die Zuverlässigkeit der Ergebnisse (Gefahr von Halluzinationen) und die Möglichkeit von Industriespionage durch Dritte stimmen die Befragten noch skeptisch. Zudem haben sie ethische Bedenken, insbesondere bei bildgenerierender KI, die fremdes geistiges Eigentum zum Training verwendet. Die potenziellen Auswirkungen auf die Umwelt durch den KI-Einsatz wurden ebenso genannt.

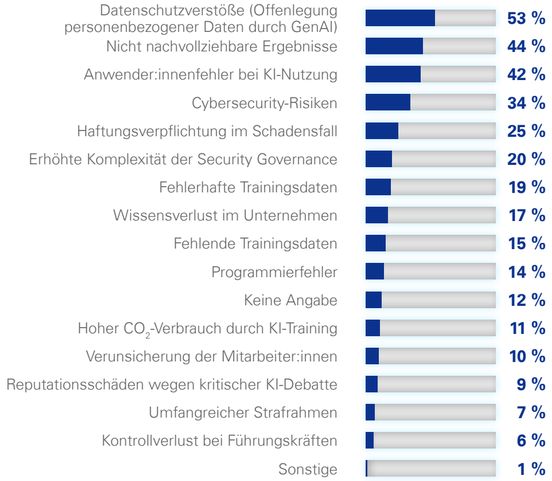
Risiken beim Einsatz von KI

Unsere Umfrageergebnisse zeigen ein vielschichtiges Bild der mit dem Einsatz von KI verbundenen Risiken. Datenschutzverstöße, insbesondere durch die Offenlegung personenbezogener Daten durch generative KI, werden weiterhin als größtes Risiko wahrgenommen – auch wenn ein leichter Rückgang von 55 Prozent im Jahr 2024 auf 53 Prozent im Jahr 2025 zu verzeichnen ist. Das unterstreicht die anhaltende Bedeutung des Themas Datenschutz im Kontext der KI-Nutzung sowie die Notwendigkeit damit einhergehender robuster Schutzmaßnahmen.

Ein weiteres Risiko stellt die mangelnde Nachvollziehbarkeit von KI-Ergebnissen für die Befragten dar. Hier zeigt sich ebenfalls ein leichter Rückgang von 48 Prozent auf 44 Prozent, was auf Fortschritte in der Entwicklung transparenterer KI-Systeme hindeuten könnte. Die Nachvollziehbarkeit bleibt dennoch ein kritischer Aspekt, insbesondere in sicherheitsrelevanten Anwendungen, in denen Entscheidungen nachvollziehbar und überprüfbar sein müssen.

Anwender:innenfehler bei der KI-Nutzung stellen für die befragten Unternehmen ebenfalls ein relevantes Risiko dar, das von 40 Prozent auf 42 Prozent angestiegen ist. Neben technologischen Aspekten spielen auch die Schulung und Sensibilisierung der Anwender:innen eine entscheidende

Abb. 18: KI-Einsatz Risiken



Rolle, um hier Fehlbedienungen und daraus resultierende Sicherheitsrisiken zu reduzieren.

Cybersecurity-Risiken im Zusammenhang mit KI verzeichnen einen Rückgang von 39 Prozent auf 34 Prozent. Ein Grund hierfür könnte sein, dass Unternehmen verstärkt Maßnahmen ergreifen, um ihre KI-Systeme vor Cyberangriffen zu schützen. Dennoch bleibt die KI-Integration in bestehende IT-Infrastrukturen eine Herausforderung, die sorgfältiger Sicherheitsüberlegungen bedarf.

Die Haftungsverpflichtung im Schadensfall ist mit 25 Prozent im Vergleich zum Vorjahr unverändert geblieben. Die rechtlichen Rahmenbedingungen und Verantwortlichkeiten im Zusammenhang mit KI-Schäden sind für die Befragten weiterhin unklar.

Die erhöhte Komplexität der Security Governance als Risiko ist in diesem Jahr angestiegen. Die Integration von KI in Unternehmen bedarf einer umfassenden Überprüfung und Anpassung der bestehenden Sicherheitsrichtlinien und -prozesse.

Weitere Risiken wie fehlerhafte oder fehlende Trainingsdaten, Wissensverlust im Unternehmen und Programmierfehler werden ebenfalls von den befragten Unternehmen als relevant eingestuft, wobei leichte Rückgänge zu verzeichnen sind. Eine verbesserte Datenqualität sowie Entwicklungsprozesse könnten Gründe hierfür sein.

Interessanterweise gibt es auch Risiken, die im Jahr 2025 stärker wahrgenommen werden als im Vorjahr. Dazu zählen der hohe CO_2-Verbrauch durch KI-Training und der umfangreiche Strafrahmen. Neben den unmittelbaren Sicherheitsrisiken sind es also auch ökologische und regulatorische Aspekte, die berücksichtigt werden müssen.

Unternehmen müssen einen ganzheitlichen Ansatz verfolgen, der neben technologischen auch organisatorische und rechtliche Aspekte berücksichtigt. Nur so können die Vorteile von KI vollumfänglich genutzt und gleichzeitig die Risiken gering gehalten werden.

„CISOs need to set realistic expectations and communicate the true potential of AI to senior management and the Board. This involves highlighting the current limitations and having a strategic approach to adoption. By encouraging a culture of experimentation, CISOs can help with the discovery of appropriate use cases that align with the organization's unique needs and priorities. As AI continues to mature and evolve, CISOs must remain vigilant in assessing its capabilities and limitations."[1]

[1] KPMG International (2025): https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2025/03/cyber-considerations-2025.pdf.coredownload.inline.pdf, abgerufen am: 11.04.2025.

Gerade bei den Risiken sehen wir, dass noch ein wesentlicher Handlungsspielraum vorhanden ist und Unternehmen Maßnahmen setzen können, um KI in geordnete Bahnen zu lenken. Kontinuierliche Überwachung und Anpassung der Sicherheitsmaßnahmen sind unumgänglich, um mit den sich ständig weiterentwickelnden Bedrohungen Schritt zu halten.

Fortschritte in der Cybersicherheit durch KI

KI ist für viele Personen ein Rettungsanker, um bisher ungelöste Bedrohungen und Probleme zu lösen und damit auch Verbesserungen in der Organisation herbeizuführen. Auf die Frage, ob die Verbreitung von generativer KI die Cybersicherheit verbessern wird, da sie bei der Abwehr von Angriffen genutzt werden kann, gaben 42 Prozent der befragten Unternehmen an, dass sie hier KI als Schlüssel zum Erfolg sehen. 18 Prozent sind skeptisch und glauben (eher) nicht, dass KI die Cybersicherheit verbessern und Angriffe abwehren kann.

Obwohl die überwiegende Mehrheit große Hoffnungen in KI setzt, bleibt die Nutzung in der Realität ein großes Fragezeichen. Am Ende haben wir es wieder mit einem Katz-und-Maus-Spiel zu tun. KI kann aufgrund ihrer technologischen Fähigkeiten Angriffe korrelieren, Ergebnisse zusammenführen und Informationen in einen Kontext setzen. Aus Daten wird Information, aus Information wird Intelligenz, aus Intelligenz werden kontextualisierte Informationen, die zur Entscheidungsfindung beitragen können. Gerade große Mengen an Informationen können nur mehr mit technischen Lösungen analysiert werden und der Mensch wird zukünftig durch KI unterstützt werden müssen. Denkt man hier beispielsweise an die Menge der Angriffe, die täglich auf Unternehmen zukommen, so können diese nur noch mit technischen Lösungen bzw. entsprechenden KI-Logiken bewältigt werden.

Beeinträchtigung der Cybersicherheit durch KI

Gerade beim Thema KI erleben wir sehr viele Widersprüche. Auf die Frage, ob die Verbreitung von generativer KI die Cybersicherheit beeinträchtigen wird, weil sie von Angreifer:innen genutzt werden kann, antworten 75 Prozent, dass sie (eher) zustimmen. Stellt man diese Antworten jenen der vorherigen Frage gegenüber, so lässt sich eindeutig erkennen, dass es zum einen Hoffnung, aber zum anderen auch Bedenken beim KI-Einsatz gibt.

Fakt ist jedoch, dass die von Menschen geschaffenen Modelle und Algorithmen, die hinter KI stecken, fehleranfällig sind bzw. manipuliert und so zum Vorteil der Angreifer:innen genutzt werden können. Wir versuchen Bedrohungen auf technische Systeme mit technischen Produkten zu lösen. Technik gegen Technik – wo bleibt dabei der Mensch, der diese Systeme richtig steuert?

Verschärfung der Bedrohungslage durch KI

Mit der Einführung neuer Technologien wie

Künstlicher Intelligenz verschärft sich naturgemäß auch die Bedrohungslage. Dem stimmen auch 78 Prozent der befragten Unternehmen zu. Nur 4 Prozent sind der Meinung, dass mit keiner veränderten Bedrohungslage durch den Einsatz von Künstlicher Intelligenz zu rechnen ist.

Erleichterung von Cyberangriffen durch KI

Auf der Schattenseite erleichtert Künstliche Intelligenz Angreifer:innen, Cyberattacken gegen Unternehmen auszuführen. Noch nie war es so einfach wie heute, Angriffe zielgerichtet auf die jeweiligen Personengruppen vorzubereiten bzw. auch Ziele maßgeschneidert zu gestalten – denken wir hier zum Beispiel an Phishingnachrichten, die genau auf den Kontext der jeweiligen Person zugeschnitten werden können. Dementsprechend sind 82 Prozent der Befragten der Meinung, dass KI jedenfalls zur Erleichterung von Cyberangriffen beitragen wird.

Verbesserung der Cybersicherheit in den letzten 12 Monaten

Hat Künstliche Intelligenz jetzt aber die Cybersicherheit der befragten Unternehmen in den letzten 12 Monaten deutlich verbessert? 17 Prozent sind der Meinung, dass KI dazu beigetragen hat, dass wir uns in puncto Cybersicherheit (eher) verbessert haben. 27 Prozent sehen dies skeptisch und geben an, dass KI nicht zur Verbesserung der Cybersicherheit beigetragen hat. In den letzten 12 Monaten hat KI noch nicht jene Verbesserungen gebracht, die sich die Menschen erhofft haben. Große Erwartungshaltungen wurden in KI zur Verbesserung der Sicherheit gesetzt, diese ist allerdings kein Zauberstab, den man nur schwingen muss, um fundamentale Security-Mängel zu kompensieren. Algorithmen können keine Sicherheitslücken schließen, deren Existenz sich Unternehmen nicht bewusst sind – dabei hilft auch keine KI-gestützte Bedrohungserkennung weiter.

Die Daten aus unserer Umfrage zeigen ein Spannungsfeld zwischen technologischem Fortschrittsglauben und tatsächlicher Implementierungskompetenz der Unternehmen. Während sich 17 Prozent der Befragten (eher) positiv zur bisherigen Wirkung von KI äußern, steigt diese Zahl im Hinblick auf die Zukunftserwartung auf 29 Prozent. Dieser Sprung um 12 Prozentpunkte – getragen von der optimistischen Vorstellung, KI werde quasi im Schlafanzug die digitalen Festungen sichern – steht in starkem Kontrast zur Realität: 56 Prozent der Befragten stehen der Frage, ob Künstliche Intelligenz in den letzten 12 Monaten die Cybersicherheit verbessert hat, neutral gegenüber und verharren hier in Passivität. Ihnen sei gesagt, dass Cybersicherheit kein Selbstläufer ist, sondern es aktiven Gestaltungswillen benötigt.

Blick in die Zukunft

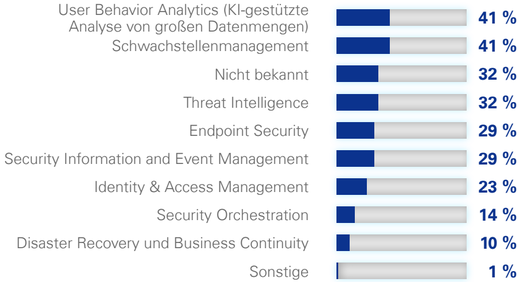
29 Prozent erwarten, dass KI in den kommenden 12 Monaten eine deutliche Verbesserung der Cybersicherheit bewirken wird. Gleichzeitig bemerken wir hier auch eine steigende Ablehnung (von 27 Prozent auf 32 Prozent), was auf ein unausgesprochenes Dilemma hindeutet: Je mehr Künstliche Intelligenz in der Cybersicherheit eingesetzt wird, desto klarer wird, dass sie kein Allheilmittel ist, sondern ein Werkzeug, das nur so gut funktioniert wie die Infrastruktur und Prozesse, in die es eingebettet ist. Viele Unternehmen betrachten KI als Rettungsring für ihre löchrigen Sicherheitsboote, während sie gleichzeitig die grundlegenden Lecks – ungepatchte Systeme, mangelhafte Zugriffskontrollen, ungeschulte Mitarbeiter:innen – ignorieren.

Zwischen Fortschrittsglauben und Realitätsverweigerung

Während KI bei der Erkennung von Anomalien von Vorteil sein und Deepfake-Angriffe effektiver bekämpfen kann, wird kein Algorithmus der Welt jemals ein schwaches Passwort oder einen ungepatchten Exchange-Server ausgleichen. Unsere Umfrageergebnisse lassen vermuten, dass der Cybersicherheitssektor auf die KI als eine Art Deus ex Machina hofft, anstatt die essenziellen Grundlagen zu adressieren. Vielleicht sollte die wichtigste Kennzahl in unserer nächsten Umfrage lauten: „Wie viele Ihrer KI-Security-Tools laufen auf Systemen, die nicht mehr unterstützt werden?“. Möglicherweise wäre das ein Weckruf für diejenigen, die gerade lieber in den KI-Hype investieren als in ein Basic Patchmanagement.

Abb. 19: Verbesserung der Cybersicherheit durch KI

Abb. 20: KI Bereichsverbesserung



Jede:r einzelne von uns sei ermutigt, weiter an den Verbesserungen zu arbeiten, damit wir in den nächsten 12 Monaten einen Fortschritt in diesem Bereich erleben.

Verbesserungsmöglichkeiten durch KI in diversen Bereichen

Unsere Umfrageteilnehmer:innen sehen in den Bereichen User Behavior Analytics (KI-gestützte Analyse von großen Datenmengen) und Schwachstellenmanagement (je 41 Prozent) die größten Möglichkeiten zur KI-Nutzung, um die Cybersicherheit zu verbessern. Unternehmen setzen also vermehrt auf proaktive Analysen und Prävention, anstatt bloß auf Angriffe zu reagieren.

Die Bereiche Endpoint Security sowie Security Information and Event Management wurden nur von jeweils 29 Prozent der Befragten genannt. Wir sehen hier einen Paradigmenwechsel: Traditionelle Perimeter-basierte Ansätze verlieren gegenüber verhaltensbasierten Schutzmechanismen an Relevanz. Diese Entwicklung steht auch im Einklang mit der zunehmenden Verlagerung von Diensten und Services in die Cloud und der Notwendigkeit, verteilte Workloads durch KI-gesteuerte Kontextanalysen zu schützen.

Verhältnismäßig selten wurden die Bereiche Security Orchestration (14 Prozent) sowie Disaster Recovery und Business Continuity (10 Prozent) genannt. Daraus lässt sich schließen, dass sich ein Großteil der Unternehmen noch nicht vollumfänglich mit den Risiken autonomer Entscheidungssysteme auseinandergesetzt hat.

Wir sehen anhand der Ergebnisse, dass KI und deren Einsatzmöglichkeiten breit diskutiert werden. Umso mehr überrascht es, dass knapp ein Drittel der befragten Unternehmen (32 Prozent) aktuell nicht weiß, in welchen Bereichen die KI-Nutzung die Cybersicherheit verbessern kann. Hier bestehen möglicherweise noch Wissenslücken in puncto KI-Einsatz bei den Befragten.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1. KI ist für viele der Schlüssel, um bisher ungelöste Bedrohungen und Probleme zu lösen und Verbesserungen in Unternehmen herbeizuführen. Große Mengen an Informationen können nur mehr mit technischen Lösungen analysiert werden. Auf der Kehrseite erleichtert KI auch den Cyberkriminellen, zielgerichtete Attacken auszuführen. Noch nie war das so einfach wie heute.

2. KI hat in den letzten 12 Monaten noch nicht jene Verbesserungen gebracht, die sich die Menschen erhofft haben. Große Erwartungshaltungen wurden in die KI zur Verbesserung der Sicherheit gesetzt. Diese Versprechen konnten (noch) nicht eingehalten werden.

3. KI kann komplexe Sachverhalte interpretieren und Verknüpfungen machen, die vorher nicht möglich waren. Allerdings ist sie auch fehlerbehaftet und die eingesetzten Algorithmen weisen ein gewisses Bias auf. Eine ausgewogene Analyse und Abwägung der Vorteile und Risiken ist für Unternehmen unerlässlich.

Neue Technologien und globale Sicherheit: Was Unternehmen wissen müssen

Elisabeth Hoffberger-Pippan arbeitet am Leibniz Institut für Friedens- und Konfliktforschung und spricht über die Bedeutung ethischer Standards und die Notwendigkeit, digitale Kompetenz zu stärken, um sich auf zukünftige Herausforderungen vorzubereiten.

Sie forschen am Leibniz Institut für Friedens- und Konfliktforschung zu Themen wie Abrüstung, biologische und chemische Waffen sowie zur Rolle neuer Technologien wie Künstlicher Intelligenz. Könnten Sie uns einen Überblick über Ihre Arbeit geben, und erläutern, warum diese Themen auch für Unternehmen von besonderem Interesse sind?

Elisabeth Hoffberger-Pippan: Meine Forschung konzentriert sich auf drei Hauptbereiche. Erstens untersuche ich die Rolle von Künstlicher Intelligenz und neuen Technologien in der konventionellen Kriegsführung. Dabei analysiere ich den Einsatz autonomer Waffensysteme und Drohnen im Rahmen rechtlicher, ethischer und sicherheitspolitischer Bestimmungen.

Zweitens befasse ich mich mit der Rolle der KI im Bereich des Verbots biologischer und chemischer Waffen. Hierbei geht es um die Möglichkeiten der KI zur Kontrolle und Prävention dieser Bedrohungen.

Der dritte Bereich umfasst völkerrechtliche Fragestellungen, insbesondere die nukleare Abrüstung und die Anwendung neuer Technologien bei Nuklearwaffen.

Für Unternehmen ist meine Forschung relevant, da jetzt einerseits ein höherer Bedarf an Gütern in der Rüstungsindustrie entsteht, gleichzeitig aber zahlreiche (internationale) Regularien existieren, welche die Produktion als auch den Export dieser Güter beeinflussen. Zulieferer, wie Halbleiterhersteller, spielen eine Schlüsselrolle bei der Integration neuer Technologien in Streitkräfte. Unternehmen müssen gewährleisten, dass ihre Produkte den rechtlichen und ethischen Standards entsprechen. Besonders im Bereich der Pharmaindustrie und bei Medizinprodukten ist es wesentlich, den Missbrauch von KI, etwa durch unbefugten Zugriff auf Systeme, zu verhindern. Diese Themen sind komplex und beinhalten sowohl Herausforderungen als auch Chancen für Unternehmen.

FOTO © SEBASTIAN SCHUELER

Erfahren Sie mehr in unserem Podcast IMPULSE

Dr. Elisabeth Hoffberger-Pippan ist Senior Researcher am Programmbereich Internationale Sicherheit und im Forschungsverbund CBWNet. Sie forscht zu Fragen der Verifikation und Einhaltung von Verbotsnormen in Bezug auf biologische und chemische Waffen sowie zur Rolle von Künstlicher Intelligenz im militärischen Bereich.

Angesichts der aktuellen turbulenten Zeiten scheint die völkerrechtliche Perspektive besonders an Bedeutung zu gewinnen. Wie sehen Sie die Rolle des Völkerrechts in dieser Situation?
Elisabeth Hoffberger-Pippan: Das Völkerrecht hat seit jeher das Problem, dass es nicht zwangsweise durchgesetzt werden kann, im Gegensatz zu nationalen Rechtsordnungen. Es ist auf die freiwillige Einhaltung seiner Normen angewiesen, was schwierig wird, wenn Staaten kein Interesse daran haben. Dennoch dienen internationale Normen zumindest teilweise auch den Eigeninteressen von Staaten und letztlich auch Unternehmen. Das kommt natürlich immer auf die jeweilige, in Rede stehende Norm an. Die meisten Staaten haben grundsätzlich ein Interesse an der Einhaltung des Völkerrechts. Dies gilt auch für den verantwortungsvollen Einsatz Künstlicher Intelligenz in der Kriegsführung. Es macht auch aus militärischer Sicht Sinn, Künstliche Intelligenz in einem kontrollierten Rahmen einzusetzen. Die Hoffnung bleibt, dass das Völkerrecht auch in Zukunft eine wichtige Rolle spielen wird, mit einer Rückbesinnung auf staatliche Entscheidungskompetenz.

In Ihrer Publikation „Rethinking Norms in Times of Algorithmic Decision Making" sprechen Sie darüber, wie algorithmische Entscheidungsprozesse bestehende Normen herausfordern. Welche Lehren können Unternehmen aus diesen Entwicklungen ziehen, insbesondere in Bezug auf die Verantwortung bei automatisierten Entscheidungen?
Elisabeth Hoffberger-Pippan: Es gibt eine Trendwende in der Rolle der Künstlichen Intelligenz. Früher lag der Fokus darauf, welche Entscheidungen autonom getroffen werden dürfen, mit Bedenken über ethische Fragen und die Würde des Menschen. Heute wird das Potenzial neuer Technologien genutzt, um Entscheidungen effizienter zu gestalten, während Risiken berücksichtigt werden.

Für Unternehmen und Techniker:innen ist es wichtig zu wissen, dass in den meisten Fällen der Mensch bei der Auslagerung von Entscheidungskompetenz an Maschinen eine gewisse Interventionsmöglichkeit haben muss. Das kommt natürlich immer auf das jeweilige Szenario an. Der Einsatz eines LLM für schulische Zwecke wird wohl keiner Interventionsmöglichkeit bedürfen. Beim Einsatz eines unbemannten Luftfahrzeugs in militärischen Operationen sieht das schon anders aus. Die Rolle des Menschen bleibt entscheidend und wichtig.

> **Die Rolle des Menschen bleibt entscheidend und wichtig.**

Gibt es bei der Kontrolle von Künstlicher Intelligenz ähnliche Herausforderungen wie bei der Regulierung von biologischen und chemischen Waffen?
Elisabeth Hoffberger-Pippan: Das Verbot von biologischen und chemischen Waffen unterscheidet sich, da sich die internationale Gemeinschaft darauf geeinigt hat, dass ihr Einsatz in Konflikten abscheulich und oft militärisch nicht sinnvoll ist. Die unkontrollierbaren Auswirkungen auf Zivilist:innen und Soldat:innen waren der Hauptgrund für das Verbot, das sich durchgesetzt hat. Bei Künstlicher Intelligenz geht es darum, zu prüfen, wie weit wir ihren Einsatz steuern können, insbesondere in militärischen und zivilen Anwendungen. Der Unterschied liegt darin, dass die Auswirkungen der KI bis zu einem gewissen Grad kontrolliert/vorhergesehen werden können. Es geht darum, dass wir KI-Systeme so entwickeln, implementieren und überwachen, dass diese verlässlich, transparent und fair agieren. Entscheidungen müssen nachvollziehbar bleiben (Explainable AI), Schutzmechanismen gegen Fehlfunktionen oder Missbrauch greifen, Diskriminierung muss ausgeschlossen werden und es braucht klare Verantwortlichkeiten (Trustworthy AI). Nur durch diese Kombination aus Transparenz, Robustheit, Datenschutz und ethischer Compliance lässt sich das nötige Vertrauen in KI-Technologien herstellen und langfristig sichern. Mögliche Herausforderungen wie die KI „Black Box" sind durchaus beherrschbar. Im Gegensatz dazu sind biologische und chemische Waffen nicht kontrollierbar, was zu ihrem Verbot führte. Der Gedanke dahinter ist aber ähnlich: Sicherheit und Schutz für den Menschen.

Eine der großen Herausforderungen bei Konflikten, insbesondere im Nahen Osten, ist, dass auch nicht staatliche Akteure bereits Zugang zu chemischen Waffen erlangt haben und diese auch eingesetzt haben. Müssen wir im Bereich der KI ebenfalls damit rechnen, dass schädliche Codes oder autonome Entscheidungssysteme in die Hände solcher Akteure gelangen und unkontrollierbare Kaskadeneffekte verursachen könnten, ähnlich wie in der konventionellen Kriegsführung? Könnte es solche Entwicklungen geben?
Elisabeth Hoffberger-Pippan: Neue Technologien in der Kriegsführung werden zunehmend erschwinglich und damit auch für nicht staatliche Akteur:innen zugänglich. Dies birgt die Gefahr, dass diese Technologien ohne Rücksicht auf Normen oder die Eindämmung von Schäden übernommen werden, was erhebliche Risiken mit sich bringt. Ein zentraler Punkt bei der Regulierung von militärischer KI ist die Verhinderung ihrer Verbreitung an nicht staatliche Akteur:innen. Exportkontrollen könnten dabei hilfreich sein, doch die Umsetzung ist bei digitalen Technologien, die bei-

spielsweise über Cloud-Computing bereitgestellt werden, komplex. Die Herausforderung liegt darin, Software effektiv zu kontrollieren, da sie nicht wie physische Güter exportiert wird.

Bei KI geht es natürlich auch um Geschwindigkeit bei Entscheidungsprozessen. Wie können wir als Gesellschaft und Unternehmen sicherstellen, dass die durch KI beschleunigte Entscheidungsfindung nicht zu voreiligen oder fehlerhaften Entscheidungen führt, die uns möglicherweise schaden?
Elisabeth Hoffberger-Pippan: Die Geschwindigkeit, mit der KI-Entscheidungen trifft, ist eine der größten Herausforderungen. Einerseits kann sie Entscheidungsprozesse effizienter gestalten und Bürokratie abbauen, andererseits besteht die Gefahr voreiliger oder fehlerhafter Entscheidungen. Um dem entgegenzuwirken, sollten wir die Digital Literacy – also das Wissen über KI und digitale Technologien – in der Gesellschaft und Unternehmen erhöhen, etwa durch Bildung und Schulungen.

Ein weiterer Ansatz ist die Investition in Forschung zur Mensch-Maschine-Interaktion, um zu verstehen, wie Menschen mit KI-Systemen effektiv kommunizieren und diese überwachen können. Beispielsweise sollte die Kontrolle von Drohnenschwärmen durch menschliche Operateure noch besser erforscht werden, um sicherzustellen, dass Menschen trotz der Geschwindigkeit der Maschinen die Kontrolle behalten.

> **Der Mensch muss bei der Auslagerung von Entscheidungskompetenzen an Maschinen eine Interventionsmöglichkeit haben.**

Es ist wichtig, Systeme zu entwickeln, die getestet und regelmäßig überprüft werden, um sicherzustellen, dass sie zuverlässig funktionieren. Ein Beispiel ist das israelische Lavender System. Dieses System identifiziert selbstständig Hamas-Kämpfer und unterstützt menschliche Operateure bei der Erkennung und dem Angriff auf legitime militärische Ziele. Laut verschiedenen Medienberichten hat Lavender in sehr kurzer Zeit so viele Kämpfer als legitime Ziele identifiziert, dass die menschlichen Operateure von der Menge an Informationen überwältigt waren.Solche Systeme müssen sorgfältig evaluiert werden, um sicherzustellen, dass sie nicht zu Fehlentscheidungen führen. Es gibt keine einfache Lösung, aber durch kontinuierliche Forschung und Anpassung können wir die Risiken minimieren.

Welche roten Linien sollten beim Einsatz von KI gezogen werden, um sicherzustellen, dass ihre Nutzung verantwortungsvoll und sicher bleibt?
Elisabeth Hoffberger-Pippan: Es ist wichtig, den Zweck von KI im Blick zu behalten und gleichzeitig die damit verbundenen Risiken zu kontrollieren. Eine klare Grenze sollte gezogen werden, wenn KI demokratische Prozesse gefährdet, etwa durch die Verbreitung von Fake News in sozialen Netzwerken. Solche Algorithmen müssen reguliert werden, um Wahlbeeinflussung und gesellschaftspolitische Gefahren zu verhindern. Ein weiteres Risiko besteht in der Diskriminierung durch KI, etwa beim Social Scoring oder in bewaffneten Konflikten. KI-Systeme können Vorurteile verstärken, da sie auf voreingenommenen Daten basieren. Dies kann zu Benachteiligungen für Frauen, Menschen mit dunkler Hautfarbe oder Personen mit Migrationshintergrund führen. Es ist entscheidend, schnell Maßnahmen zu ergreifen, um Diskriminierung durch KI zu verhindern, da dies sowohl demokratische als auch kriegsbezogene Probleme verursachen kann.

Trainingsdaten können Vorurteile in KI-Modellen verstärken und bergen Risiken wie Data Poisoning, bei dem Modelle durch manipulierte Daten unterwandert werden. Welche Maßnahmen können wir ergreifen, um uns vor solchen Angriffen zu schützen? Gibt es überhaupt Möglichkeiten, dies zu verhindern?

Elisabeth Hoffberger-Pippan: Wir haben begrenzte Möglichkeiten, uns gegen Data Poisoning zu schützen, etwa durch Fortschritte in der Verschlüsselungstechnologie. Doch je digitaler wir werden, desto angreifbarer sind wir. Diese Situation ist vergleichbar mit dem Jamming von Drohnen, bei dem Funksignale gestört werden. Verschlüsselung kann Systeme sicherer machen, aber wir müssen uns bewusst sein, dass digitale Technologien immer auch Risiken mit sich bringen. KI kann helfen, Cyberangriffe zu erkennen und darauf zu reagieren, indem sie große Datenmengen analysiert. Sie kann nicht nur für die Entwicklung von autonomen Waffensystemen genutzt werden, sondern auch zum Schutz vor Angriffen.

Ein weiterer wichtiger Punkt ist das Verständnis von Bias und Vorurteilen, die sowohl in KI als auch im menschlichen Denken existieren. Wir neigen dazu, Maschinen zu vertrauen, besonders in Stresssituationen, selbst wenn sie Fehler machen. Es ist entscheidend, zu verstehen, wie das menschliche Gehirn funktioniert und wie wir auf Maschinen reagieren, um eine optimale Interaktion zu gewährleisten.

Wie können wir sicherstellen, dass die Ergebnisse von KI, insbesondere in wissenschaftlichen Publikationen, authentisch und glaubwürdig sind, und wie können wir die Fähigkeit zur kritischen Reflexion bei Menschen stärken, um zwischen echten und von KI generierten Inhalten zu unterscheiden?

> **Die Geschwindigkeit ist eine der größten Herausforderungen, wenn wir über KI sprechen.**

Elisabeth Hoffberger-Pippan: Es ist wichtig, die Fähigkeit zu entwickeln, zwischen Inhalten zu unterscheiden, die von Menschen und von KI verfasst wurden. Ein Problem dabei ist, dass wir uns zunehmend auf KI für alltägliche Aufgaben wie Übersetzungen oder Rezeptvorschläge verlassen. Studien zeigen, dass das menschliche Gehirn dazu neigt, Informationen zu vergessen, wenn es weiß, dass sie leicht nachgeschlagen werden können. Diese Abhängigkeit könnte langfristig dazu führen, dass wir wichtige kognitive Fähigkeiten verlernen, was unsere Fähigkeit zur differenzierten Beurteilung beeinträchtigen könnte.

In vielen Artikeln und Publikationen ist erkennbar, dass sie von KI verfasst wurden, da oft dieselben Wörter verwendet werden. Während KI hilfreich sein kann, um Inspiration zu finden, stellt sich die Frage, wie sich diese Nutzung auf unsere Fähigkeit zur Textverfassung auswirkt. Insgesamt hat die Nutzung von KI sowohl positive als auch negative Seiten, und es ist wichtig, diese abzuwägen.

Wenn wir uns in einem Jahr wieder treffen, was würden wir uns dann wünschen, heute schon getan zu haben?
Elisabeth Hoffberger-Pippan: Ich wünsche mir für das nächste Jahr einen verantwortungsvollen Umgang mit KI und eine größere digitale Kompetenz in der Gesellschaft. Es ist wichtig, dass wir alle, auch diejenigen ohne technischen Hintergrund, ein besseres Verständnis für diese Technologien entwickeln. Die Gesellschaft muss darauf vorbereitet werden, dass KI nicht mehr wegzudenken ist.

Obwohl wir versuchen, KI durch europäische und nationale Gesetze zu regulieren, wird der Druck aus der Privatwirtschaft, insbesondere aus den USA, stark auf uns einwirken. Die USA sind oft Vorreiter bei technologischen Entwicklungen, und wir müssen uns bewusst sein, dass neue Technologien, wie Human-Machine-Interfaces, immer wichtiger werden. Es ist entscheidend, strategisch vorauszuschauen und sich auf kommende Technologien einzustellen, da sie wahrscheinlich unsere wirtschaftliche Landschaft beeinflussen werden. Unternehmen sollten sich darauf vorbereiten, mit diesen Technologien zu arbeiten oder sich zumindest damit auseinanderzusetzen.

07

Des- und Missinformation

Des- und Missinformationen sowie alle anderen Formen der (hybriden) Einflussnahme wirken direkt und ungefiltert auf unsere Gesellschaft – gerade in Zeiten geopolitischer Spannungen. Unsere Weltordnung gerät ins Wanken. Sicherheit ist nicht mehr planbar und längst keine Selbstverständlichkeit mehr, denn alle Bereiche (egal ob Wirtschaft, Technologie, Umwelt oder unsere Gesellschaft) geraten zeitgleich unter Druck. Die Möglichkeiten, die den Täter:innen zur Verfügung stehen, sind vielfältig, die Auswirkungen und Konsequenzen kaum vorhersehbar.

37 %

glauben, dass ihr Unternehmen Opfer eines Cyberangriffs werden kann, durch den **gezielt Einfluss** auf das Unternehmen ausgeübt werden könnte.

35 %

sind **nicht der Meinung,** dass ihr Unternehmen Opfer eines Cyberangriffs werden kann, durch den **gezielt Einfluss** auf das Unternehmen ausgeübt werden könnte.

59 %

sehen ein Risiko durch **politische Hacktivist:innen,** von denen Des- und Missinformationen ausgehen.

56 %

sehen ein Risiko durch **staatliche oder staatlich unterstützte Akteur:innen und Gruppierungen.**

45 %

der befragten Unternehmen sind der Meinung, dass von der **Konkurrenz und vom Wettbewerb** eine Bedrohung ausgeht.

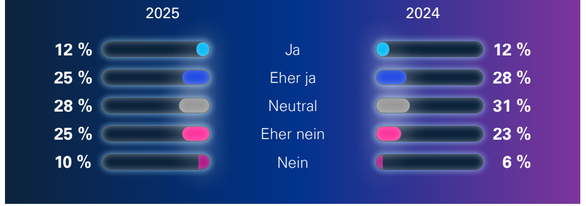
41 %

sehen **staatliche Institutionen als Akteure** im Hinblick auf Desinformationskampagnen.

83 %

sagen, dass Des-/Missinformationskampagnen unsere **gesellschaftliche Resilienz beeinflussen.**

Abb. 21: Glauben Sie, dass Ihr Unternehmen Opfer eines Cyberangriffs werden kann, durch den gezielt Einfluss auf das Unternehmen ausgeübt werden könnte?



Des- und Missinformationen als Bedrohung für Unternehmen

Vor allem geistiges Eigentum, Konstruktionspläne und Unternehmenswerte, aber auch Patente machen Unternehmen erfolgreich und stehen deshalb im Mittelpunkt der Angriffe. Der gezielten Einflussnahme auf die Unternehmen durch die Verbreitung von Miss- und Desinformation kommt hierbei ein immer größerer Stellenwert zu. So ist es nicht weiter verwunderlich, dass im aktuellen Regierungsprogramm auch diesem Umstand Rechnung getragen wird und in den Sicherheitsbereichen entsprechend aufgerüstet wird.

Unsere Umfrageergebnisse zeigen eine komplexe Entwicklung der Risikowahrnehmung von Unternehmen gegenüber Cyberangriffen und Desinformationskampagnen. Die Wahrnehmung, Opfer von gezielten Cyberangriffen zu werden, verschiebt sich. Es herrscht eine paradoxe Stabilität in einer volatilen Bedrohungslage. 37 Prozent der Umfrageteilnehmer:innen glauben, dass ihr Unternehmen Opfer eines Cyberangriffs werden kann, durch den gezielt Einfluss auf das Unternehmen ausgeübt werden könnte. Dieser Wert sank leicht im Vergleich zum Vorjahr um 3 Prozent. Damit steht dieser Befund im diametralen Widerspruch zu internationalen Bedrohungsanalysen. Laut Global Threat Report 2025[1] stiegen staatlich unterstützte Cyberoperationen zur Einflussnahme auf Unternehmen im Vergleich zum Vorjahr um 31 Prozent, wobei besonders Sektoren kritischer Infrastruktur (Energie, Gesundheitswesen) betroffen waren.

35 Prozent der Umfrageteilnehmer:innen glauben hingegen nicht, dass ihr Unternehmen Opfer eines Cyberangriffs werden kann, durch den gezielt Einfluss auf das Unternehmen ausgeübt werden könnte. Im Jahr 2024 verneinten dies nur 29 Prozent. Diese Entwicklung steht im Widerspruch zu globalen Trends: Laut Global Cybersecurity Outlook 2025[2] des Weltwirtschaftsforums haben staatlich unterstützte Angriffe und Hacktivist:innengruppen ihre Aktivitäten in den letzten zwölf Monaten um 22 Prozent intensiviert.

Die Verneinung dieser Frage durch heimische Unternehmen könnte auf psychologische Abwehrmechanismen zurückzuführen sein: Unternehmen, die bereits in defensive Technologien investiert haben (z. B. KI-basierte Intrusion-Detection-Systeme), neigen dazu, Risiken trotz steigender Bedrohungslage subjektiv zu unterschätzen. Dieses Phänomen wird in der Fachliteratur als „Cybersecurity-Complacency-Effekt“ beschrieben – eine trügerische Sicherheit, die durch technologische Fortschritte entsteht.[3]

Die Praxis hat gezeigt, dass vermehrt nicht nur in Übersee, sondern auch in Europa – und auch in Österreich – Einflussnahme auf Unternehmen stattfindet. Österreich als verhältnismäßig kleines Land nimmt zwar keine derartig große geopolitische Rolle ein, wie dies andere Nationen tun, dennoch ist das Risiko von Miss- und Desinformation bei uns latent. Auch in den Risikobildern, z. B. des World Economic Forum[4] oder des österreichischen Bundesheeres[5], wird Des- und Missinformation als eine der wesentlichen Bedrohungen für die nächsten Jahre identifiziert.

Die unterschätzte Gefahr narrativer Kriegsführung

Die grundsätzliche Sorge der Beeinflussbarkeit von Unternehmensaktivitäten durch Desinformation bleibt weiterhin sehr hoch bestehen: 36 Prozent der Befragten halten eine Einflussnahme durch Online-Desinformationskampagnen gegen das Unternehmen für möglich. Die Abweichung zwischen wahrgenommener und tatsächlicher Bedrohung lässt sich durch das „Iceberg-Phänomen der Desinformation“ erklären: Es gibt eine sichtbare Spitze (direkte Angriffe wie Fake-News-Kampagnen werden zunehmend erkannt und abgewehrt). Darunter befindet sich allerdings verdeckte Masse. Indirekte Effekte wie die Untergrabung von Mitarbeiter:innenvertrauen, Manipulation von Investor:innen oder Störung von Lieferketten durch falsche Informationen bleiben oft unerkannt.[6]

Online-Desinformationskampagnen tragen dazu bei, die Meinungsbilder in der Gesellschaft, aber auch bei Unternehmern gezielt zu verändern. Ziel ist es, Druck auszuüben und das von den Angreifer:innen gewünschte Verhalten hervorzurufen.

41 Prozent glauben, dass keine Beeinflussung möglich ist. Während also ein signifikanter Teil der Unternehmen die Bedrohung durch Desinformation ernst nimmt, gibt es auch eine große Gruppe, die sich weniger besorgt zeigt. Dies könnte auf unterschiedliche Erfahrungen, Branchen oder die Effektivität von internen Schutzmaßnahmen gegen Desinformation zurückzuführen sein.

Diese scheinbare Risikominimierung ist trügerisch: Organisationen mit begrenzter Threat-Intelligence-Kapazität überschätzen ihre Abwehrfähigkeiten, während erfahrene Security Operations Center (SOC) gerade durch vertiefte Einblicke in Angriffsmethoden (z. B. Microtargeting mittels LLMs) ihre eigene Verwundbarkeit erkennen.

Besonders kritisch ist die Unterschätzung indirekter Desinformationseffekte: Während direkte Fake-News-Kampagnen gegen Unternehmen und deren Produkte oft erkannt werden, bleiben subtilere Angriffe auf Stakeholder:innen-Beziehungen (Investor:innen, Lieferanten, Mitarbeitende) häufig unentdeckt. Das World Economic Forum identifiziert in seinem Global Risks Report 2025[7] Narrative Supply-Chain-Angriffe als wachsendes Risiko – beispielsweise die gezielte Streuung falscher Informationen über Arbeitsbedingungen, die zu Reputationsverlusten und regulatorischen Sanktionen führen.

Akteur:innen, von denen Desinformation ausgeht

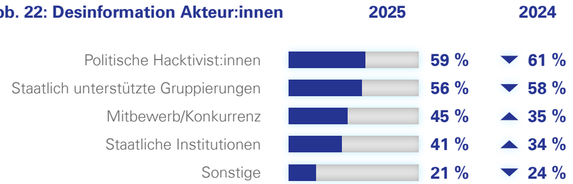
Gerade im Bereich der Desinformationskampagnen gibt es ein vielfältiges Spektrum an Akteur:innen, die sich in diesem Umfeld bewegen.

Politische Hacktivist:innen: Diese sind meist durch politische oder soziale Anliegen motiviert und verbreiten Desinformation, um auf bestimmte Themen aufmerksam zu machen oder um eine Änderung der Geschäftspraktiken bei den angegriffenen Unternehmen herbeizuführen. Die Auswirkungen der Desinformationskampagnen reichen dabei von kurzfristigen Imageschäden bis hin zu langfristigen Veränderungen in der Unternehmenspolitik.

Staatliche oder staatlich unterstützte Akteur:innen: Sie handeln häufig im Rahmen geopolitischer Strategien. Ziel der Desinformationskampagnen ist es, wirtschaftliche Instabilität auszulösen, einen Wettbewerbsvorteil für eigene nationale Unternehmen herbeizuführen oder politische Spannungen zu verschärfen. Unternehmen, die in internationalen Märkten agieren, geraten verstärkt

[1] https://www.securityweek.com/wp-content/uploads/2025/02/CrowdStrikeGlobalThreatReport2025.pdf, abgerufen am: 18.04.2025.
[2] https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf, abgerufen am: 13.04.2025.
[3] https://link.springer.com/article/10.1186/s42400-020-00050-w, abgerufen am: 13.04.2025.
[4] https://www.weforum.org/publications/global-risks-report-2025/, abgerufen am: 06.04.2025.
[5] https://www.bmlv.gv.at/wissen-forschung/publikationen/publikation.php?id=1224, abgerufen am: 06.04.2025.
[6] https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en, abgerufen am: 18.04.2025
[7] https://www.weforum.org/publications/global-risks-report-2025/, abgerufen am: 13.04.2025.

Abb. 22: Desinformation Akteur:innen



ins Visier staatlicher Interessen und sind daher besonders anfällig für Desinformationskampagnen.

Mitbewerber und Konkurrenten: Desinformation wird auch für unlauteren Wettbewerb eingesetzt. Dabei hat sie das Ziel, das Vertrauen der Kund:innen in ein konkurrierendes Unternehmen zu schwächen oder dessen Marktanteil zu verkleinern.

Staatliche Institutionen: Sie stehen oft in direkter Verbindung mit der Regierung. Mit Desinformationskampagnen soll die Beeinflussung der öffentlichen Meinung oder die Regulierung der Geschäftstätigkeit von Unternehmen erreicht werden. Durch derartige Kampagnen kann die Beziehung zwischen Unternehmen und staatlichen Stellen nachhaltig beeinflusst werden.

Von welchen Akteur:innen heimische Unternehmen betroffen sind

Heimische Unternehmen sehen insbesondere ein Risiko durch politische Hacktivist:innen (59 Prozent), von denen Des- und Missinformationen ausgehen. An zweiter Stelle finden sich staatliche oder staatlich unterstützte Akteur:innen und Gruppierungen (56 Prozent). Nicht außer Acht gelassen werden dürfen Mitbewerber und Konkurrenten. 45 Prozent der befragten Unternehmen sind der Meinung, dass besonders von der Konkurrenz und vom Wettbewerb eine Bedrohung ausgeht. An vierter Stelle finden wir staatliche Institutionen (41 Prozent), die als Akteure im Hinblick auf Desinformationskampagnen gesehen werden.

Die Teilnehmenden unserer Umfrage berichten ebenso, dass Bedrohungen für Des-/Missinformation gegen ihr Unternehmen von ehemaligen Mitarbeitenden ausgehen. Diese können interne Informationen nutzen, um Schaden zu verursachen. Unzufriedene Kund:innen sowie schlechte anonyme Bewertungen können das Unternehmensimage ebenso negativ beeinflussen. Auch Cyberkriminelle, die wahllos Opfer suchen, stellen eine mögliche Bedrohung dar.

Die wahrgenommenen Hauptakteur:innen von Desinformationskampagnen bleiben zwar dominant, verlieren aber im Vergleich zum Vorjahr etwas an Relevanz. Dieser leichte Rückgang könnte durch erfolgreiche Gegenmaßnahmen bedingt sein. Die EU-Kommission berichtet etwa in der Digital Services Act Transparency Database[8], dass die Erkennungsraten von koordinierten Desinformationskampagnen durch KI-gestützte Tools leicht gestiegen sind.

Bemerkenswert in unserer Studie ist jedoch der Anstieg bei Mitbewerbern (+10 Prozent) und staatlichen Institutionen (+7 Prozent). Das lässt sich aus unserer Sicht anhand der folgenden drei Entwicklungen erklären:

Wettbewerbsdynamiken in Krisenmärkten: In Branchen mit sinkenden Margen (z. B. Industrie, Maschinen- und Anlagenbau) gewinnt Industriespionage als strategisches Instrument an Bedeutung. Der Anstieg um 10 Prozent spiegelt hier reale Vorfälle wider, wie die Enthüllung von zielgerichteten Angriffen gegen Hochtechnologieunternehmen. Unter anderem wurden mittelständische Unternehmen gezielt durch getarnte Phishingkampagnen von Konkurrenten ausspioniert.

[8] https://transparency.dsa.ec.europa.eu/?lang=en, abgerufen am: 18.04.2025.

Geopolitische Instrumentalisierung: Staatliche Institutionen setzen Desinformation im Rahmen hybrider Kriegsführung ein. Beispiele wie die „Deepfake-Diplomatie"-Kampagnen im Kontext des russischen Angriffskriegs auf die Ukraine haben gezeigt, wie staatliche Akteure Unternehmen gezielt destabilisieren, um wirtschaftlichen Druck auf sie auszuüben.

Verschwimmende Grenzen: Eine Verschmelzung staatlicher und privater Akteur:innen (z. B. durch Outsourcing von Cyberangriffen an „patriotische" Hacker:innengruppen) erschwert die Zuordnung. Damit entsteht eine neue Form hybrider Bedrohungsakteur:innen.

Desinformation beeinflusst unsere gesellschaftliche Resilienz

83 Prozent der befragten Unternehmen sind der Meinung, dass Des-/Missinformationskampagnen unsere gesellschaftliche Resilienz beeinflussen. Die Übergänge der demokratischen Strukturen, die wir vor allem durch die diplomatischen Veränderungen erleben, stellen uns als Gesellschaft vor große Herausforderungen. Dem müssen wir entgegentreten und Resilienz als nationale Aufgabe sehen. Das größte Momentum für die Resilienz einer Gesellschaft entsteht dadurch, dass alle Personen zusammenhalten. Sicherheit geht uns alle an, und die Einbindung der Gesellschaft ist es auch, die den Zusammenhalt in turbulenten Zeiten ermöglicht. Vor allem skandinavische Länder zeigen, wie die Einbindung ziviler Gesellschaften, Notfallkonzepte und übergreifende Plattformen dabei helfen können, eine Strategie zu entwickeln. Werkzeuge, die uns im Kampf gegen Desinformation zur Seite stehen, reichen allein nicht aus. Es braucht ein klares Narrativ, eine kohärente Strategie und ein gemeinsames Handeln. Die Frage ist nicht, ob Krisen ausgelöst durch Desinformation kommen, sondern ob wir darauf vorbereitet sind. Denn wer heute nicht handelt, wird morgen Zweiter sein.

Strategien zur Abwehr von Desinformationskampagnen

Unternehmen können verschiedene Maßnahmen ergreifen, um sich gegen Desinformation zu schützen:

- Systeme zur Überwachung von Online-Inhalten implementieren und potenzielle Desinformationskampagnen analysieren
- Klare und transparente Kommunikationsstrategien entwickeln zur Widerlegung von Falschinformationen und zur Stärkung des Vertrauens der Stakeholder:innen
- Mit Cybersicherheitsexpert:innen und PR-Spezialist:innen zusammenarbeiten, um Bedrohungen zu erkennen und angemessen auf diese zu reagieren
- Mitarbeitende schulen, damit sie für die Risiken von Desinformation sensibilisiert sind und ihnen Tools zur Erkennung und Reaktion zur Verfügung stehen

Mithilfe dieser Strategien erhöhen Unternehmen ihre Resilienz und schützen ihre Geschäftstätigkeit.

Eskalation strategischer Desinformationskampagnen: Ursachen und Auswirkungen auf Unternehmen.

Die Zunahme von Desinformationskampagnen gegenüber Unternehmen durch den Mitbewerb und staatliche Institutionen ist auf technologische, geopolitische und wirtschaftliche Faktoren zurückzuführen:

Technologische Ermächtigung von Angreifer:innen

Fortschritte in generativer KI (z. B. ChatGPT, Deepfake-Synthesizer) und Automatisierungstools helfen Cyberkriminellen, hyperrealistische Falschinformationen in industriellem Maßstab zu produzieren. KI-gesteuerte Bot-Netzwerke generieren innerhalb weniger Minuten tausende Social-Media-Postings, die gezielt Reputationsschäden verursachen. So werden beispielsweise gefälschte Dokumente zu angeblichen Compliance-Verstößen oder manipulierte Videoaussagen von Führungskräften erzeugt. Ein Beispiel ist die Deepfake-Kampagne gegen einen Energiekonzern

im Jahr 2023, bei der simulierte CEO-Interviews gefälschte Preiserhöhungen ankündigten. Kurzfristige Aktienkursverwerfungen waren die Folge.

Wettbewerbsdynamiken im digitalen Raum
Vor dem Hintergrund globaler Rezessionsängste und verstärkter Marktkonkurrenz nutzen Mitbewerber Desinformationskampagnen, um kostengünstig Wettbewerbsvorteile zu erzielen. Beispielsweise werden manipulierte Bewertungen auf Plattformen wie Trustpilot oder Google Reviews veröffentlicht. Eine weitere Taktik ist die Verbreitung falscher Lieferengpassmeldungen. Damit sollen Partnerunternehmen dazu gebracht werden, Kooperationen zu beenden.

Geopolitische Instrumentalisierung durch Staaten
Staatliche Akteure setzen Desinformationskampagnen ein, um ihre handels- oder sicherheitspolitischen Ziele durchzusetzen, indem etwa gezielt Falschmeldungen in Umlauf gebracht werden. Gleichzeitig nutzen autoritäre Regimes Desinformation, um kritische Infrastrukturen zu destabilisieren. Ein Beispiel hierfür wäre das Streuen von Gerüchten über angebliche Cyberangriffe auf Energieversorger, um dadurch das Vertrauen in deren operative Sicherheit zu untergraben.

Systemische Vulnerabilitäten des Informations-Ökosystems
Eine fragmentierte Medienlandschaft und algorithmengesteuerte Verbreitung von Content auf Plattformen wie X oder Telegram fördern die Verbreitung falscher Narrative. Zusätzlich ermöglichen Werbetools Cyberkriminellen, Desinformation zielgenau bei Investor:innen, Mitarbeiter:innen oder der Lokalbevölkerung zu platzieren.

Ein neues Risikoparadigma

Systematische Hybridangriffe, bei denen ökonomische und geopolitische Motive verschmelzen, werden immer mehr zur Realität. Um nachhaltig resilient zu sein, müssen Unternehmen branchenübergreifende Kooperationen eingehen und in Deepfake-Erkennungstechnologien investieren. Außerdem braucht es internationale Normen gegen den strategischen Missbrauch von Desinformation als Wettbewerbsinstrument.

Strategische Implikationen

Unsere Umfrageergebnisse verdeutlichen, dass traditionelle Cybersecurity-Strategien an ihre Grenzen stoßen. Neben technologischen Abwehrmaßnahmen wie Firewalls und Endpoint Protection müssen Unternehmen auch folgende Aspekte mitbedenken:

1. Analyseteams in Unternehmen, die Cyberbedrohungen im Kontext internationaler Machtdynamiken bewerten
2. Trainingsprogramme zur Erkennung kognitiver Verzerrungen („Prebunking“) zur Immunisierung von Mitarbeiter:innen gegen narrative Manipulation[9]
3. Branchenübergreifende Initiativen zur Stärkung der kollektiven Abwehrfähigkeit gegen hybride Bedrohungen
4. Verstärkte Zusammenarbeit mit Aufsichtsbehörden zur Entwicklung einheitlicher Standards für Desinformationsabwehr
5. Ethische Leitlinien für den Einsatz von generativer KI zur Desinformationserkennung, um Vertrauensverluste durch Überwachungsängste zu verhindern

[9] https://www.klicksafe.eu/en/desinformation-und-meinung/prebunking-schutz-vor-desinformationen, abgerufen am: 13.04.2025.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1. Online-Desinformationskampagnen tragen dazu bei, die Meinungsbilder in der Gesellschaft, aber auch bei Unternehmern gezielt zu verändern. Ziel ist es, Druck auszuüben und das von den Angreifer:innen gewünschte Verhalten hervorzurufen.

2. Unternehmen und unsere Wirtschaft befinden sich im Fadenkreuz von Desinformationskampagnen. Die Möglichkeiten, die den Täter:innengruppierungen zur Verfügung stehen, sind vielfältig, die Auswirkungen und Konsequenzen kaum vorhersehbar.

3. Die Praxis hat gezeigt, dass vermehrt auch in Österreich Einflussnahme auf Unternehmen stattfindet. Österreich als verhältnismäßig kleines Land nimmt zwar keine derartig große geopolitische Rolle ein, wie dies andere Nationen tun, dennoch ist das Risiko von Miss- und Desinformation auch hier bei uns latent.

Tech-Diplomatie: Der Schlüssel zur internationalen Zusammenarbeit

In einer Welt, in der Technologie globale Machtverhältnisse neu ordnet, wird Tech-Diplomatie zum strategischen Hebel für Frieden, Sicherheit und nachhaltige Entwicklung. **Claudia Reinprecht**, Leiterin des Referats für Konnektivitäts-, Tech- und Innovationsdiplomatie im österreichischen Außenministerium, erklärt, warum dieses Feld so zentral für unsere Zukunft ist.

Was ist Tech-Diplomatie und warum ist sie gerade jetzt so wichtig?
Claudia Reinprecht: Tech-Diplomatie ist ein neues außenpolitisches Instrument an der Schnittstelle von Außen-, Wissenschafts-, Technologie- und Innovationspolitik. Tech-Diplomatie bedeutet, neue Technologien außenpolitisch einzuordnen – strategisch, vorausschauend und menschenrechtsbasiert. Unser Ziel ist es, diese Entwicklungen aktiv mitzugestalten und Österreich strategisch zu positionieren – durch Zusammenarbeit mit Forschung, Wirtschaft, Zivilgesellschaft und internationalen Partnern. Denn Technologien wie KI, Quanten- oder Neurotechnologie prägen nicht nur Wirtschaft und Gesellschaft, sondern auch internationale Beziehungen – sie beeinflussen den internationalen Frieden und die Sicherheit, Menschenrechte und nachhaltige Entwicklung. Österreich will zur verantwortungsvollen Gestaltung dieser globalen Transformation beitragen.

Welche strategischen Ziele verfolgt Österreich dabei?
Claudia Reinprecht: Unsere strategischen außenpolitischen Ziele sind der Erhalt des internationalen Friedens und der Sicherheit, die Förderung internationaler Zusammenarbeit, die Stärkung von Demokratie sowie der Schutz von Menschenrechten und Rechtsstaatlichkeit. Dabei handeln wir auf Grundlage des Völkerrechts, insbesondere der Menschenrechte.

Im Bereich digitaler Technologien setzen wir auf den digitalen Humanismus. Dieser menschenrechtsbasierte Ansatz stellt den Menschen und seine Selbstbestimmung sowie und die Nachhaltigkeit unseres Handelns ins Zentrum technologischer Entwicklungen. Er betont die ethische Gestaltung des Verhältnisses zwischen Mensch und Maschine und bietet einen Rahmen für eine breite gesellschaftliche Auseinandersetzung mit den Auswirkungen neuer Technologien auf unsere Gesellschaft, und auch auf internationalen Beziehungen.

Wie können wir völkerrechtliche Grundsätze in Zeiten von Tech-Abhängigkeiten und geopolitischen Spannungen schützen?
Claudia Reinprecht: Vor rund 40 Jahren wurde das Internet bewusst kaum reguliert, um eine offene, globale Informationsgesellschaft zu ermöglichen. Auch heute setzt sich Österreich für ein freies und sicheres Internet sowie für einen inklusiven Multi-Stakeholder-Ansatz zur Gestaltung digitaler Technologien ein.

Tech-Diplomatie ist essenziell, weil Technologie zu einem zentralen Machtfaktor in geopolitischen, wirtschaftlichen und gesellschaftlichen Zusammenhängen geworden ist – während gleichzeitig erhebliche Governance-Lücken bestehen. Die Kehrseiten der Digitalisierung wie Desinformation, Datenmissbrauch und Hassrede zeigen die dringende Notwendigkeit gemeinsamer internationaler Regeln und verantwortungsvoller Zusammenarbeit. Weltweit wächst das Interesse an klaren Politiken und Strukturen – etwa im Rahmen des Global Digital Compact –, um globale Ziele im Bereich der digitalen Kooperation zu erreichen. Tech-Diplomatie spielt dabei eine Schlüsselrolle in der antizipatorischen Governance: Wir müssen Entwicklungen nicht nur beobachten, sondern

FOTO © BMEIA/ MICHAEL GRUBER

Erfahren Sie mehr in unserem Podcast IMPULSE

Dr. Claudia Reinprecht ist seit 2004 im österreichischen Außenministerium tätig. Nach diplomatischen Einsätzen in Wien, Brüssel, Amman, Hongkong und Paris leitet sie das Referat für Verkehrs-, Telekommunikations-, Digital-, Technologie- und Innovationsdiplomatie.Sie diente als Botschafterin Österreichs bei der UNESCO in Paris und als Generalkonsulin in Hongkong und Macao. Vorher beriet sie den österreichischen Vizekanzler und Außenminister Dr. Michael Spindelegger in Fragen des Völkerrechts und der Menschenrechte, der Auslandskultur und Entwicklungspolitik.

Wir sind die Gestalter:innen unserer eigenen Zukunft.

frühzeitig verstehen, in welche Richtung sie sich bewegen könnten. Das bedeutet: Szenarien durchspielen, Risiken erkennen, Chancen nutzen – bevor Technologien breite Wirkung entfalten.

Österreichs Außenpolitik verfolgt das Ziel, Wohlstand, Sicherheit und Lebensqualität zu sichern und einen aktiven Beitrag zur Bewältigung globaler Herausforderungen wie Klimawandel, Digitalisierung und geopolitischen Spannungen zu leisten. Gerade in einer Zeit internationaler Fragmentierung und Vertrauenskrisen kann Tech-Diplomatie helfen, neue Brücken der Zusammenarbeit zu bauen.

Wie verändert sich unser Verständnis vom Informationsraum und was heißt das für Österreichs Diplomatie?
Claudia Reinprecht: Das Thema hat natürlich eine cyber- bzw. sicherheitspolitische Dimension, auf die ich nicht eingehen, sondern die Frage aus der Perspektive Tech-Diplomatie beantworten möchte. Neue Technologien wie Neuro- oder Quantentechnologien beeinflussen unseren Informationsraum, unsere Sicherheit, unsere Wahrnehmung und sogar unsere Entscheidungsfreiheit. Dafür bauen wir Kapazitäten im Außenministerium auf und fördern den Dialog mit anderen Ressorts, Forschung und internationalen Organisationen. Die enge Zusammenarbeit mit den Fachressorts an der Schnittstelle von Sicherheit, Wissenschaft und Technologie ist entscheidend, denn neue Technologien sind ein

Future Literacy, die Fähigkeit, die Zukunft zu antizipieren, ist entscheidend.

strategisches Asset mit weitreichenden Auswirkungen auf Wirtschaft, Sicherheit und Menschenrechte. Während wir bei digitalen Technologien bereits über solides Know-how verfügen, werfen Entwicklungen wie Quanten-, immersive und Neurotechnologien neue Fragen auf.

Gerade Neurotechnologien, die direkt unsere kognitive Autonomie und Sicherheit betreffen, sind besonders vielschichtig. Die Konvergenz von KI-, Neuro- und immersiven Technologien eröffnet neue Möglichkeiten subtiler Manipulation und Überwachung. Diese Entwicklungen betreffen unsere kognitiven Freiheiten – und wir sind gesellschaftlich wie politisch noch nicht ausreichend darauf vorbereitet. Unser Ziel ist es daher, den Kapazitätsaufbau im Außenministerium zu stärken und gemeinsam mit unseren Partnern, wie etwa dem AIT und Ars Electronica Center, einen gesamtgesellschaftlichen Dialog über technologische Zukunftsfragen anzustoßen. Future Literacy – die Fähigkeit, Zukunft aktiv zu gestalten – ist dabei zentral. Denn Technologieunternehmen beeinflussen bereits heute unsere Zukunftsbilder und damit unsere Entscheidungen im Hier und Jetzt.

Wie können wir die Zukunft angesichts der technologischen Entwicklungen effektiv gestalten, und welche Rolle spielt „digitaler Humanismus" dabei?
Claudia Reinprecht: Im digitalen Humanismus geht es darum, das Verhältnis zwischen Mensch und Maschine so zu gestalten, dass unsere Menschlichkeit, Würde und Selbstbestimmung im Zentrum stehen. Neue Technologien haben das Potenzial, unser Bewusstsein vom Menschsein und unserer Menschlichkeit tiefgreifend zu verändern. Umso wichtiger ist es, sie verantwortungsvoll im Einklang mit den Menschenrechten und der Menschenwürde zu gestalten und in eine Richtung zu lenken, die den Menschen dient.
Im Außenministerium greifen wir diese Fragen nicht nur im Rahmen der multilateralen Governance-Prozesse auf, in denen wir die Regeln für die verantwortliche Entwicklung und den Einsatz neuer Technologien verhandeln. Auch im Rahmen der Auslandskulturpolitik sowie des interkulturellen und interreligiösen Dialogs setzen wir uns für einen ethischen Umgang mit neuen Technologien ein – mit dem klaren Ziel, Menschenrechte zu schützen und den Dialog über die Werte zu fördern, die unsere digitale Zukunft prägen sollen.

Wie kann Tech-Diplomatie den Innovationsstandort Österreich unterstützen?
Claudia Reinprecht: Sie öffnet Türen. Das Außenministerium mit seinem weltweiten Netzwerk von ca. 100 Vertretungen vernetzen Start-ups, Forschungseinrichtungen und internationale Organisationen. Wir helfen mit Partnern wie der Austrian Business Agency dabei, Österreich als vertrauenswürdigen Tech-Standort zu positionieren – etwa im Quantenbereich. Dabei geht es auch um technologische Souveränität und darum, Talente im Land zu halten.

Kann Europa seine Position in Schlüsseltechnologien stärken?
Claudia Reinprecht: Europa unternimmt große Anstrengungen, um durch eigene Programme seine strategische Autonomie zu stärken. Die neue Kommission setzt dabei klare Prioritäten: Innovation und Resilienz, insbesondere im Bereich der Stärkung unserer Wettbewerbsfähigkeit und in der europäischen Verteidigung, stehen im Mittelpunkt. Trotz angespannter Haushalte wurde in Europa erkannt, dass es für die Zukunft des Standorts entscheidend ist, gezielt in Forschung und Technologie zu investieren. Auf europäischer Ebene zeichnen sich bereits substanzielle Investitionen in Verteidigung und Schlüsseltechnologien ab. Die aktuelle geopolitische Lage hat ein Umdenken ausgelöst.

Tech-Diplomatie verbindet Außenpolitik und Diplomatie mit Technologie- und Innovationsfragen.

Sie haben betont, dass Europa und Österreich technologisch gestärkt werden müssen. Unsere Studie zeigt, dass die Zustimmung zur Nutzung österreichischer Sicherheitslösungen von 37 Prozent im Jahr 2024 auf 60 Prozent gestiegen ist. Dies ist ein klarer Appell, stärker zu investieren. Was können wir tun, um dies zu erreichen?
Claudia Reinprecht: Technologische Souveränität und digitale Autonomie sind seit Jahren zentrale Themen in Europa. Besonders im Quantenbereich gibt es bereits vielversprechende Ansätze zur Stärkung der industriellen Basis und zur Sicherung unserer wirtschaftlichen Sicherheit.

Österreich spielt dabei eine aktive Rolle – das Austrian Institute of Technology ist führend in Quantenkommunikationsprojekten, und Unternehmen wie Silicon Alpine Labs tragen entscheidend zur technologischen Entwicklung bei.

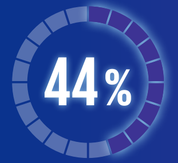
Der Weg nach vorne erfordert klare strategische Ziele und gezielte Investitionen in europäische Projekte. Wir sehen ein stärkeres Engagement der öffentlichen Verwaltung, etwa durch den Einsatz von Quantenlösungen und die Förderung öffentlich-privater Partnerschaften. Das kann nicht nur Innovation beschleunigen, sondern auch helfen, Bürokratie durch effizientere und effektivere Lösungen abzubauen.

Wenn wir uns in einem Jahr wieder treffen, was würden wir uns dann wünschen, heute schon getan zu haben?
Claudia Reinprecht: Mein persönlicher Wunsch: eine starke, koordinierte Plattform für Österreichs Quanten-Ökosystem. Ich weiß, dass daran schon gearbeitet wird. Wir haben viele Initiativen, aber keinen zentralen Ort, an dem wir gemeinsam an strategischen Zielen arbeiten. Quantum Delta Netherlands in den Niederlanden zeigt, wie so etwas funktionieren kann.

Heißt das wir müssen unsere Fähigkeiten bündeln, um gemeinsam und strukturiert ein starkes Ökosystem zu schaffen und dadurch wirkungsvoll zu sein?
Claudia Reinprecht: Ja, das ist doch der Traum Europas, dass wir gemeinsam stärker sind. Wir dürfen nicht darauf warten, dass andere unsere Zukunft gestalten – wir müssen sie selbst in die Hand nehmen.

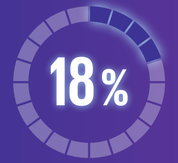
08 Regulatorik

Die regulatorische Landschaft ist derzeit sehr vielfältig und die Entwicklungen der Europäischen Union zu diesem Thema bringen viele neue Vorgaben im Hinblick auf Cybersecurity ans Tageslicht. Die aktuell entstehenden Regularien sind eine Konsequenz daraus, dass Unternehmen und Volkswirtschaften immer stärker unter Druck durch Cyberangriffe geraten. Durch die neuen Regularien soll auch eine Verbesserung der Cybersecurity für den gemeinsamen europäischen Binnenmarkt erreicht werden.

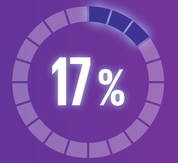


sehen **keine direkte Betroffenheit** durch die Regularien.

stufen die **NIS-2-Richtlinie** als prioritär ein.



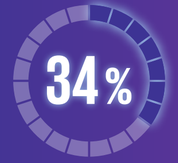
sagen, dass sie von **NIS-1** betroffen sind.



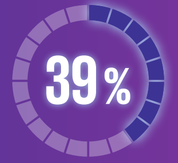
priorisieren **DORA.**

erwarten, vom **AI Act** betroffen zu sein.

gehen davon aus, dass sie von **CRA** betroffen sein werden.



glauben, dass sie bei der Umsetzung der **technischen Risikomanagementmaßnahmen** bereits weit fortgeschritten sind.



sagen, bei der Umsetzung der **organisatorischen Risikomanagementmaßnahmen** weit fortgeschritten zu sein.

Österreich im Spannungsfeld zwischen Regulatorik und KMU-Realität

Die europäische Cyberregulatorik durchdringt im Jahr 2025 zunehmend den österreichischen Wirtschaftsraum. Die Umsetzung gestaltet sich allerdings nicht so geradlinig: Während Großunternehmen und Betreiber der kritischen Infrastruktur wie Energieversorger oder Krankenhausverbünde Compliance-Strukturen etablieren, zeigt sich über alle österreichischen Unternehmen hinweg ein Widerspruch. 44 Prozent der Befragten sehen keine direkte Betroffenheit durch die Regularien, während 36 Prozent die NIS-2-Richtlinie als prioritär einstufen. Diese Zahlen offenbaren ein grundlegendes Missverständnis: Viele Unternehmen erkennen nicht, dass sie als Zulieferer kritischer Infrastrukturen oder durch ihre Rolle in digitalen Ökosystemen indirekt unter die erweiterten Melde- und Sicherheitspflichten fallen. Vor dem Hintergrund, dass laut unserer Studie im Jahr 2025 jeder siebente Cyberangriff auf österreichische Unternehmen erfolgreich war, werden das Befassen mit und die Umsetzung der Regulatorik zur existenziellen Notwendigkeit.

NIS-2-Richtlinie und nationales Umsetzungsgesetz

Die NIS-2-Richtlinie ist eine wesentliche Maßnahme der EU zur Verbesserung der Cybersecurity. Damit werden Anforderungen an die Sicherheit von Netz- und Informationssystemen festgelegt und Unternehmen zur Implementierung geeigneter Risikomanagementmaßnahmen verpflichtet. Im nationalen Umsetzungsgesetz werden diese Vorgaben für heimische Unternehmen konkretisiert. Voraussichtlich wird die Mehrheit aller Unternehmen von der Richtlinie betroffen sein.

Die NIS-2-Richtlinie, die im österreichischen Netz- und Informationssicherheitsgesetz (letztgültiger Gesetzesentwurf per 14. Mai 2025 - NISG 2024) verankert wird, erfasst erstmals mittlere Unternehmen ab 50 Mitarbeitenden und EUR 10 Mio. Jahresumsatz in 18 Sektoren – von der Trinkwasserversorgung bis zum verarbeitenden Gewerbe. Dass 36 Prozent der Befragten die NIS-2 priorisieren, spiegelt zwar die zentrale Rolle der Richtlinie wider, doch jene 44 Prozent, die sich davon nicht betroffen fühlen, unterliegen einer riskanten Fehleinschätzung. Besonders betroffen sind KMUs als Zulieferer kritischer Komponenten: So muss nun bspw. ein Maschinenbauunternehmen als Produzent von Steuerungseinheiten für Windkraftanlagen vertraglich sicherstellen, dass seine Entwicklungsprozesse Secure-by-Design-Prinzipien entsprechen. Die Herausforderung liegt dabei in der Ressourcenknappheit – viele Betriebe verfügen nicht über das Budget für externe Pentests oder die Implementierung von Netzwerksegmentierung in OT-Umgebungen.

18 Prozent sehen sich von NIS-1 betroffen. Das ist ein Indiz dafür, dass einige Unternehmen den Transitionsprozess noch nicht beendet haben.

Dieses Risiko kann durch gezielte Awareness-Kampagnen minimiert werden. Unsere Umfrageergebnisse verdeutlichen jedoch, dass viele Unternehmen die angebotenen Ressourcen nicht nutzen. Gründe dafür könnten mangelnde Bekanntheit oder komplexe Antragsprozesse sein.

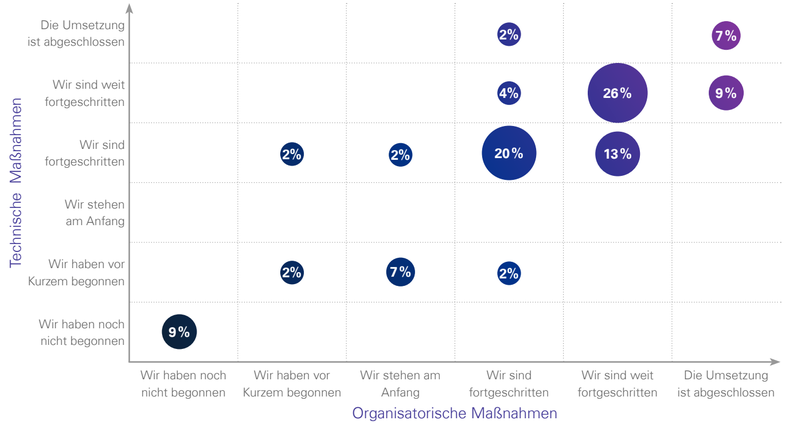
Digital Operational Resilience Act (DORA)

Trotz seiner Verbindlichkeit seit 17. Jänner 2025 priorisieren nur 17 Prozent der Befragten DORA. Das ist ein überraschendes Signal für den Finanzsektor, der besonders stark von Cyberangriffen betroffen ist. Nationale Aufsichtsbehörden wie die FMA fordern von kleinen Fintechs und regionalen Banken die vertragliche Verpflichtung ihrer Cloud-Dienstleister zur Durchführung monatlicher Resilience-Tests. Gründe für die niedrige Priorisierung bei den Umfrageteilnehmenden könnten eine komplexe Revision von Lieferantenverträgen oder unklare Leitfäden sein.

Artificial Intelligence Act (AI Act)

Der AI Act konzentriert sich auf die Nutzung und Entwicklung von Künstlicher Intelligenz. Risiken von KI-Systemen sollen minimiert und deren sichere und ethische Anwendung gewährleistet werden. 30 Prozent der von uns befragten Unternehmen erwarten, vom AI Act betroffen zu sein. Dieser Umstand verdeutlicht auch die wachsende Relevanz von KI in der Unternehmenslandschaft. Dieses Ergebnis steht auch in Zusammenhang

Abb. 23: NIS-2 Umsetzungsstand bei Österreichischen Unternehmen



mit der Tatsache, dass Fintechs, die KI-basierte Betrugserkennung nutzen, zusätzliche Herausforderungen bei der Absicherung gegen Adversarial Attacks zu bewältigen haben.

Cyber Resilience Act (CRA)

Der Cyber Resilience Act hat die Stärkung der Widerstandsfähigkeit von IT-Systemen gegenüber Cyberbedrohungen zum Ziel. Unternehmen müssen ihre Systeme so gestalten, dass sie Cyberangriffen besser standhalten können. 25 Prozent der von uns befragten Unternehmen glauben, dass sie von dieser Regulatorik betroffen sein werden. Das verdeutlicht die wachsende Notwendigkeit robuster Sicherheitsmaßnahmen sowie produktspezifischer Sicherheitsanforderungen, die besonders Hersteller vernetzter Geräte betreffen. Die Umfragezahlen deuten jedoch auf eine zu geringe Priorisierung der Unternehmen hin, die sich möglicherweise auf hohe Zertifizierungskosten und technische Retrofit-Herausforderungen zurückführen lässt. Der Cyber Resilience Act adressiert dies durch akkreditierte Stellen. Innovative KMUs nutzen auch Plattformen für Bug-Bounty-Programme, um so Schwachstellen vor Markteinführung zu identifizieren. Dieser Ansatz ist vor allem für Start-ups mit begrenzten Testkapazitäten von Bedeutung.

Die regulatorische Landschaft in Österreich

Die Grafik 24 zeigt eine Übersicht, von welchen Regularien heimische Unternehmen aktuell betroffen sind bzw. voraussichtlich betroffen sein werden. Die überwiegende Mehrheit der heimischen Unternehmen wird voraussichtlich von der NIS-2-Richtlinie und dem nationalen Umsetzungsgesetz des NISG betroffen sein. Auffällig ist, dass an zweiter Stelle bereits der AI Act steht. 30 Prozent der befragten Unternehmen gehen davon aus, dass sie davon betroffen sein werden. Jedes vierte Unternehmen ist der Meinung, dass es vom Cyber Resilience Act in Österreich betroffen sein wird.

NIS-2 – technische und organisatorische Umsetzung

Wie weit fortgeschritten sind heimische Unternehmen aber bereits bei der Umsetzung der Risikomanagementmaßnahmen? Auch hier scheint die Selbsteinschätzung der Unternehmen von der Realität abzuweichen. 34 Prozent der befragten Unternehmen sind der Meinung, dass sie in puncto technischer Maßnahmen bereits weit fortgeschritten sind. 39 Prozent sagen, bei den organisatorischen Maßnahmen bereits weit fort-

geschritten zu sein. 7 Prozent geben an, sowohl bei den technischen als auch bei den organisatorischen Maßnahmen die Umsetzung bereits abgeschlossen zu haben.

Die Grafik 23 zeigt den Umsetzungsgrad der technischen und organisatorischen NIS-2 Risikomanagementmaßnahmen bei heimischen Unternehmen auf Basis einer Selbsteinschätzung.

Es bleibt abzuwarten, wie die ersten Prüfungen und Einsichtnahmen durch die Behörden aussehen werden und ob der Ist-Stand mit den Erwartungen der unabhängigen Stellen zur Erfüllung der Anforderungen der Risikomanagementmaßnahmen übereinstimmt. NIS-2 ist hier sicherlich ein wesentlicher Baustein, um die Resilienz der Systeme nachhaltig zu verbessern.

Herausforderungen bei der NIS-2-Umsetzung

Unsere Umfrageergebnisse verdeutlichen, dass sich die Unternehmen der Wichtigkeit von Cybersecurity bewusst sind und sie damit begonnen haben, sich auf die neuen Anforderungen, die die Regulatorik mit sich bringt, vorbereiten. Trotzdem geht ihre Selbsteinschätzung nicht immer mit dem tatsächlichen Umsetzungsfortschritt einher und für die Unternehmen gibt es noch einiges zu tun. Die behördlichen Prüfungen werden richtungsweisend sein, um den Ist-Stand zu bewerten. Heimische Unternehmen könnten ihre Sicherheitsstrategien nochmals überarbeiten müssen und ihre Ressourcen aufstocken, um den geänderten Anforderungen und neuen Regularien zu entsprechen sowie um ihre Systeme nachhaltig vor Cyberangriffen zu schützen.

Abb. 24: Regularien

Herausforderungen und Lösungsansätze

Ressourcenknappheit stellt für heimische Unternehmen das größte Hindernis dar: Mittelständische Unternehmen können sich keine eigens für Cybersecurity zuständigen Mitarbeiter:innen leisten und greifen auf Managed Security Service Provider (MSSP) zurück. Eine regulatorische Überlappung – etwa bei Cloud-Anbietern, die NIS-2, DORA und CRA parallel umsetzen müssen – erschwert zusätzlich die Priorisierung. Hier schafft das Compliance Mapping Tool von ENISA durch die Identifizierung von Synergien (z. B. Anrechnung von ISO 27001-Zertifizierungen für multiple Regularien) Abhilfe.

Auch der Fachkräftemangel, besonders in Nischenbereichen wie KI-Sicherheit oder OT-/IT-Konvergenz, kann durch unterschiedliche Initiativen und Förderungen gemildert werden. Die Herausforderung bleibt allerdings bestehen, da viele traditionelle Betriebe wie etwa Familienunternehmen bei der Investition in Schulungen (noch) zurückhaltend sind.

Resilienz als gemeinsame Mission

Die erfolgreiche Implementierung der Cyberregulatorik hängt von der aktiven Beteiligung der Unternehmen ab. Unternehmen, die regulatorische Compliance als Chance begreifen und die diversen Unterstützungsangebote annehmen bzw. auch aktiv einfordern, etablieren sich als vertrauenswürdige Partner und stärken gleichzeitig Österreichs digitale Souveränität im EU-Binnenmarkt.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1 Die aktuell entstehenden Regularien sind eine Konsequenz daraus, dass Unternehmen und Volkswirtschaften durch Cyberangriffe immer stärker unter Druck geraten. Durch die neuen Regularien soll auch eine Verbesserung der Cybersecurity für den gemeinsamen europäischen Binnenmarkt erreicht werden.

2 Durch die NIS-2 werden Anforderungen an die Sicherheit von Netz- und Informationssystemen festgelegt und Unternehmen zur Implementierung geeigneter Risikomanagementmaßnahmen verpflichtet. Im nationalen Umsetzungsgesetz werden diese Vorgaben für heimische Unternehmen konkretisiert. Voraussichtlich wird die Mehrheit aller Unternehmen von der Richtlinie betroffen sein.

3 Österreichische Unternehmen sind sich der Wichtigkeit von Cybersecurity bewusst und haben damit begonnen, sich auf die neuen Anforderungen, die die Regulatorik mit sich bringt, vorzubereiten. Ihre Selbsteinschätzung geht allerdings nicht immer mit dem tatsächlichen Umsetzungsfortschritt einher und es gibt noch einiges zu tun. Die behördlichen Prüfungen werden richtungsweisend sein, um den Ist-Stand zu bewerten.

headline hunter

Beobachtungszeitraum:
1. April 2024 bis 1. April 2025

3.361	Headlines gesammelt
160.409	Wörter analysiert
397	Quellen
33	Sprachen

HeadlineHunter
Es ist oftmals eine Sache der Perspektive, welche Themen in der gegenwärtigen Diskussion an die Oberfläche kommen und wie wir diese wahrnehmen. Betrachten wir das im Kontext von Informationsoperationen und Desinformation, interessiert uns, welche Themen Einfluss auf das Stimmungsbild und die Meinungsbildung haben. Um dieser Frage nachzugehen, wurde vom Kärntner Unternehmen neptun.ai, einem Spin-off der Universität Klagenfurt, eine Analyse der Medienberichterstattung zum Thema Cybersicherheit der letzten 12 Monate durchgeführt. Damit können wir auch einen Vergleich dazu herstellen, wie sich die aktuelle Bedrohungslage in der Berichterstattung widerspiegelt.

Die aktuelle Cybersicherheitslandschaft ist von eskalierenden und immer raffinierteren Bedrohungen geprägt, die Unternehmen und Institutionen weltweit vor große Herausforderungen stellen. Unsere Studienergebnisse unterstreichen die Dringlichkeit robuster Abwehrstrategien angesichts der zunehmenden Professionalisierung von Angreifer:innen und dem Einsatz neuer Technologien wie KI.

Aktuelle Berichte verdeutlichen eine Zunahme kritischer Vorfälle wie Ransomware-Angriffe, die Rekordschäden verursachen, weitverbreitete Phishingkampagnen, die auf sensible Daten abzielen, und politisch motivierte DDoS-Attacken sowie gravierende Datenlecks bei namhaften Organisationen. Diese Entwicklungen werden durch Faktoren wie Ransomware-as-a-Service, KI-gestützte Manipulation und die Ausnutzung menschlicher Schwachstellen sowie technischer Sicherheitslücken weiter verschärft.

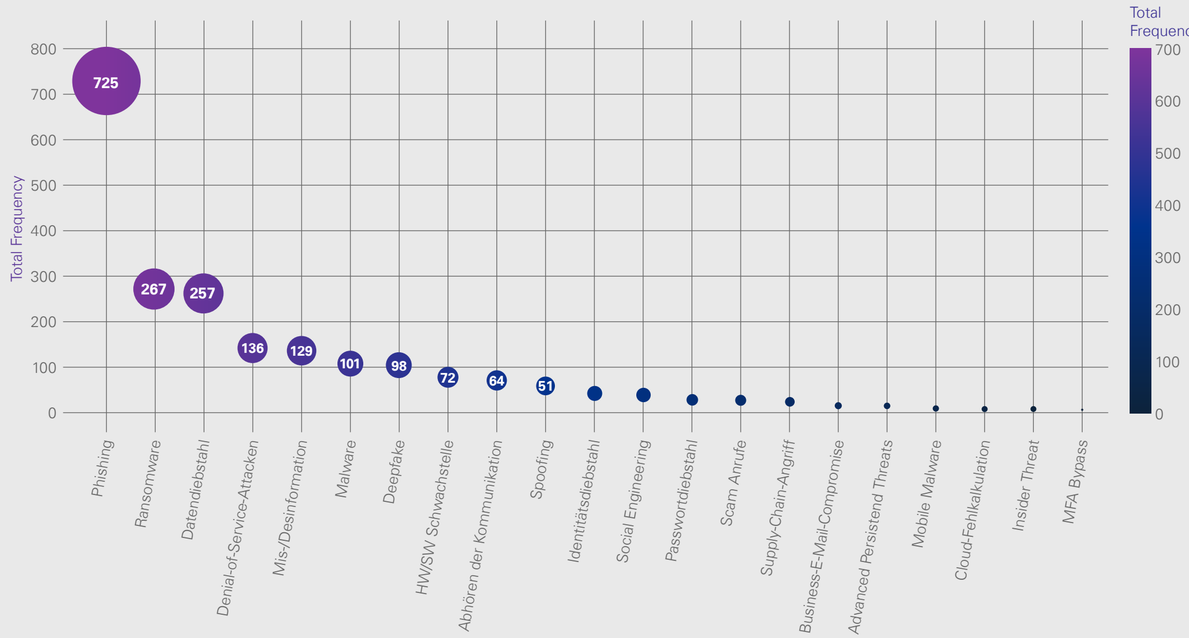
Die Konsequenzen reichen von erheblichen finanziellen Verlusten und Betriebsunterbrechungen bis hin zu Veranstaltungsabsagen aufgrund von Terrorgefahr und öffentlichen Debatten über staatliche Überwachungsmaßnahmen.

Angesichts dieser komplexen Bedrohungslage sind kontinuierliche Investitionen in Sicherheitstechnologien, Mitarbeiter:innenschulungen und proaktive Abwehrmechanismen unerlässlich, um Resilienz aufzubauen.

In der nachfolgenden Grafik ist die Anzahl der Artikel dargestellt, die über die jeweiligen Vorfälle berichten. Blicken wir auf die globalen Top 5 Themen, so zeigt sich folgende Reihenfolge: 1) Phishing, 2) Ransomware 3) Datendiebstahl, 4) Denial-of-Service-Attacken, 5) Malware. Vergleichen wir diese Ergebnisse mit unseren Auswertungen der heimischen Unternehmen, so sehen wir eine Veränderung bei Platz 4, der in Österreich von Miss-/Desinformation besetzt ist.

Nicht außer Acht zu lassen ist dabei natürlich, dass die Berichterstattung immer den aktuellen Entwicklungen geschuldet ist, und mit etwas Verzögerung die Realität abbildet. Unabhängig davon zeigt sich, dass laufende Analysen und ständige Beschäftigung mit diesen Themen unerlässlich sind, um als Unternehmen sowohl gesellschaftlich als auch technologisch resilient und damit cybersicher zu sein.

Abb. 25: Cybersecurity Reporting



Cyberresilienz im Finanzsektor: Strategien und Herausforderungen

Anna Muri, Leiterin des IT-Risiko-Teams der FMA Bankenaufsicht, über die Umsetzung von DORA, die Rolle von IKT-Dienstleistern und die Bedeutung von IT-Governance.

Könnten Sie uns einen kurzen Überblick über die Aufgaben und Schwerpunkte des IT-Risiko-Teams in der Bankenaufsicht geben?
Anna Muri: Unser Fokus liegt auf der Umsetzung der DORA-Aufsicht, die vier Kapitel umfasst: IT-Risikomanagement, Vorfallsmanagement, Resilienz-Tests gegen Cyberrisiken und Drittparteienrisikomanagement. Aktuell konzentrieren wir uns auf IT-Governance, IT-Risikomanagement und Drittparteienrisiko. Wir monitoren einerseits die Mängelbehebung nach OeNB-Prüfungen. Zudem bearbeiten wir Anträge von Kreditinstituten, etwa für Ausnahmen von der starken Kund:innenauthentifizierung im Zahlungsverkehr, und führen Verfahren zu Open Banking. Im Bereich IT-Governance führen wir regelmäßige Einsichtnahmen durch, um die Prozesse und die Einbindung der Geschäftsleitung bspw. in IT-Risiken zu überprüfen.

Ihr Tätigkeitsbereich ist sehr breit mit vielen unterschiedlichen Facetten. Sie haben bereits die Zusammenarbeit mit der OeNB erwähnt. Könnten Sie uns einen Einblick in die Kompetenzverteilung und die Zusammenarbeit geben?
Anna Muri: In Österreich erfolgt die Bankenaufsicht durch die FMA und die OeNB gemeinsam – und diese Zusammenarbeit funktioniert sehr gut. Die FMA trägt die aufsichtsrechtliche Verantwortung: Sie trifft alle behördlichen Entscheidungen und führt diesbezüglich Verfahren, erlässt Bescheide und Verwaltungsstrafen. Die OeNB unterstützt die FMA durch operativ-technische Aufgaben wie die Durchführung von Vor-Ort-Prüfungen bei Banken, die Auswertung von Meldedaten sowie die Erstellung von Analyseberichten und Risikobewertungen. Es gibt einige Ausnahmen, etwa im Geldwäsche- und Conductbereich, aber grundsätzlich übernimmt die OeNB die Vor-Ort-Tätigkeiten und verarbeitet einen Großteil der aufsichtsrechtlichen Meldungen.

Dynamik und Veränderungen im IT-Bereich betreffen auch die Aufsicht. Sie verwenden den Ansatz der Technologieneutralität. Was bedeutet das und wie berücksichtigen Sie es im Arbeitsalltag?
Anna Muri: Der technologieneutrale Ansatz ist wichtig, da sich Technologien ständig ändern. Dies bedeutet, dass aufsichtsrechtliche Vorgaben und Bewertungen unabhängig von der eingesetzten Technologie erfolgen. Wir beurteilen also nicht die eingesetzte Technologie, sondern deren Auswirkungen auf Risiken, Compliance und Stabilität. DORA fordert Unternehmen auf, sich mit aktuellen Technologien auseinanderzusetzen, deren Auswirkungen zu bewerten und mögliche Risiken zu berücksichtigen. Durch den technologieneutralen Ansatz wird klargestellt, dass regulatorische Vorschriften unabhängig von der Verwendung einer bestimmten Technologie einzuhalten sind.

Wenn wir über technologische Entwicklungen sprechen, gibt es zwei wichtige Themen: Künstliche Intelligenz und Quantencomputing, einschließlich Quantenkryptographie und Quantensicherheit. Wie bewerten Sie diese technologischen Veränderungen aus der Risikoperspektive für die Finanzinstitute?
Anna Muri: Technologische Veränderungen wie Künstliche Intelligenz und Quantencomputing haben großen Einfluss auf Finanzinstitute. Jedes Institut muss überlegen, wie es diese Technologien nutzen will und welche Risiken eine Technologie mit sich bringt. Künstliche Intelligenz hat Phishing-Attacken bereits raffinierter gemacht, bspw. mit besserem Wording und weniger Fehlern. Institute müssen KI auch zur Verteidigung nutzen, um Risiken zu managen. DORA verlangt, dass aktuelle technologische Entwicklungen zu beobachten sind und jeweils zu beurteilen ist, inwiefern eine neue Technologie für das eigene Unternehmen in Betracht gezogen werden kann – etwa zur Verbesserung der Cyberresilienz– oder aber zu einer Erhöhung des IT-Risikoprofils beiträgt.

FOTO © PRIVAT

Erfahren Sie mehr in unserem Podcast IMPULSE

Dr. Anna Muri ist Leiterin des IT-Risiko-Teams der FMA Bankenaufsicht und verfügt über mehr als zehn Jahre Erfahrung in der Beaufsichtigung von Banken und Zahlungsinstituten. Sie ist Mitglied in nationalen und europäischen Gremien im Bereich IT-Risiko. Sie absolvierte ein Studium der Rechtswissenschaften in Wien und Dijon und trägt regelmäßig zu IT-Risiken im regulatorischen Kontext vor.

24/7-Erreichbarkeit ist unerlässlich – Angreifer:innen halten sich nicht an Geschäftszeiten.

Die aktuelle technologische Entwicklung ist sowohl beeindruckend als auch beängstigend, da sie mit einer nie dagewesenen Geschwindigkeit voranschreitet. Vergessen wir dabei zu leicht auf den Faktor Mensch und wie er in dieses System passt?
Anna Muri: Der Mensch darf nicht vergessen werden, und Regularien berücksichtigen ihn. Beim Betrug im Zahlungsverkehr ist der Mensch oft der größte Risikofaktor. Für Banken stellt dies eine große Herausforderung dar. EBA-Leitlinien verlangen in diesem Zusammenhang, dass Kund:innen in Bezug auf sicherheitsrelevante Risiken im Zahlungsverkehr zu unterstützen sind. Ansätze wie Geocontrol im Online-Banking helfen, Zahlungen aus bestimmten Ländern zu blockieren. Die gänzliche Vermeidung von Betrug im Zahlungsverkehr ist schwierig, es braucht hier einen ganzheitlichen Ansatz. Sicherheit im Internet wird bspw. zunehmend in Schulen thematisiert, was ein wertvoller Beitrag zur Betrugsprävention ist. Ohne solche Bildung bleibt ein Restrisiko bestehen, das Banken allein nicht ausschalten können.

Regulatorik kann den gesunden Menschenverstand nicht ersetzen. Sollten Awareness-Trainings stärker auf die gesunde Skepsis fokussieren?
Anna Muri: Definitiv. Gerade durch die Fortschritte, die es im Bereich KI in den letzten Jahren gegeben hat, wird es immer schwieriger, Betrugsversuche zu erkennen. Beispiel sind hier simulierte Videokonferenzen, bei denen nichtsahnende Mitarbeitende von vermeintlichen CEOs

> **Mangelnde Kommunikation kann teuer werden.**

angewiesen wurden, hohe Geldbeträge zu überweisen. Gesunde Skepsis ist wichtig. Banken sind hier angehalten, sinnvolle Schulungsprogramme zu entwickeln, die auch an die jeweilige aktuelle Bedrohungslage angepasst werden.

Das Risiko kann also nicht allein durch Regulatorik eingedämmt werden?
Anna Muri: Nein, der Faktor Mensch ist entscheidend. Auf europäischer Ebene gibt es Ansätze wie ein gemeinsames Register für verdächtige IBANs, das aktuell evaluiert wird. Auf nationaler Ebene gibt es sowohl aus der Kreditwirtschaft wie auch von Seiten der Regulatorik Initiativen in diesem Bereich, um die Awareness zu stärken. Das Problem ist, dass sich Technologien wie KI ständig weiterentwickeln und anpassen. Schulungen und Awareness-Trainings sind derzeit der beste Ansatz, um zusammen mit technischen Maßnahmen gegen Betrug und Cyberangriffe vorzugehen.

Könnte es sein, dass die rasante technologische Entwicklung dazu führt, dass wir alleine nicht mehr in der Lage sind, Herausforderungen zu bewältigen? Ist Zusammenarbeit und Kollaboration im Kollektiv der Schlüssel zur Verteidigung?
Anna Muri: Ja, das ist ein wichtiges Thema für uns. Sowohl auf nationaler als auch auf europäischer Ebene ist das momentan ein Schwerpunkt. Die europäischen Finanzaufsichtsbehörden haben erst kürzlich ein Rahmenwerk zum Informationsaustausch und Koordinierung im Fall von systemischen Cyberbedrohungen ins Leben gerufen. Besonders wichtig ist dabei die Geschwindigkeit des Informationsaustauschs – sowohl zwischen Behörden als auch innerhalb des Finanzsektors. Zusammenarbeit ist entscheidend und es gibt noch viel Potenzial für Verbesserungen.

NIS-2 fordert, dass Unternehmen, die als Betreiber wesentlicher Dienste benannt sind, rund um die Uhr erreichbar sein müssen, je nach den angebotenen Services. Wäre es sinnvoll, dies auch für den Finanzsektor zu erwägen?
Anna Muri: Im Finanzsektor ist die 24/7-Verfügbarkeit im Bereich Cybersecurity bereits Standard und absolut notwendig, da sich Angreifer:innen nicht an Geschäftszeiten halten. Unternehmen haben ein Eigeninteresse daran, dies sicherzustellen. Die Frage ist, wie man diesen Standard weiter vorantreibt oder ausweitet. Dies ist letztlich oft eine Ressourcenfrage.

Seit Jänner ist DORA vollständig in Kraft und anwendbar. Warum ist DORA aus Ihrer Sicht gerade jetzt so wichtig für den Finanzmarkt, und welches Ziel wollen wir damit genau erreichen?
Anna Muri: Das Ziel von DORA ist klar: eine höhere Resilienz gegen IT-Risiken und Cyberbedrohungen. Die Notwendigkeit ist offensichtlich, da die Digitalisierung stark voranschreitet und unser Leben zunehmend digital wird. Je mehr wir digitalisieren, desto besser müssen wir uns vor den damit verbundenen Risiken schützen. DORA schafft ein einheitliches Regelwerk, das direkt anwendbar ist, ohne zusätzliche nationale Gesetzgebungen. Dies ist ein wichtiger Schritt, da die Gewährleistung eines Level-Playing Field im Finanzsektor enorm wichtig ist.

Brauchen wir diese Regulatorik, weil Sicherheit und Resilienz bei den betroffenen Einrichtungen und Unternehmen noch nicht die nötige Priorität haben?
Anna Muri: Definitiv. Man könnte naiv denken, dass es im Eigeninteresse eines Unternehmens liegt, sich gut zu schützen. Doch der Schutz gegen Cyberbedrohungen ist komplex und kostenintensiv, weshalb er oft erst dann umgesetzt wird, wenn es klare regulatorische Vorgaben gibt.

Sie haben den Aspekt der Kosten und Ressourcen angesprochen. Welche weiteren Herausforderungen sehen Sie aktuell bei der Umsetzung von DORA in den Instituten? Gibt es Besonderheiten in Bezug auf IT-Risiken oder IT-Sicherheit?
Anna Muri: Oft mangelt es an Kommunikation zwischen technischem und juristischem Personal, was teuer werden kann, wenn Umsetzungen nicht abgestimmt sind. Dies ist oftmals bei großen Projekten im Digitalisierungsbereich der Fall, wenn es konkrete regulatorische Vorgaben gibt. Eine solide Governance-Struktur ist entscheidend. Führungskräfte im Finanzsektor sollten jedenfalls die Risiken verstehen und sich weiterbilden.

Eine weitere Herausforderung, die auch von europäischen Regulatoren nicht vollständig antizipiert wurde, ist die Beteiligung von Drittanbietern im Bereich Informations- und Kommunikationstechnologie (IKT). Diese sind zwar nicht direkt von DORA betroffen, aber indirekt, was bei der Umsetzung viele Schwierigkeiten verursacht.

IKT-Dienstleister gewinnen angesichts der aktuellen weltpolitischen Lage an Bedeutung. Haben wir diese Unternehmen ausreichend im Blick?
Anna Muri: Mit DORA wurde ein Überwachungsrahmen für kritische IKT-Drittdienstleister im europäischen Finanzsektor geschaffen. Das war ein enorm wichtiger Schritt, der die größten Player in diesem Bereich regulatorisch erfasst. Große Unternehmen wie Amazon und Google sind darauf vorbereitet. Die Herausforderung liegt bei kleineren IKT-Dienstleistern, die DORA lange nicht beachtet haben. Als Banken Vertragsanpassungen verlangten, wurden sie mitunter überrascht.

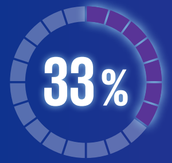
Wenn Sie in drei Jahren einen Artikel oder ein Buch über DORA schreiben müssten, was sollte unbedingt darin enthalten sein?
Anna Muri: Der Fokus auf die IKT-Dienstleister wäre entscheidend. Es wäre wichtig, sie stärker einzubinden und abzuholen. Momentan bedeutet DORA für sie hauptsächlich Mehrarbeit und Mehraufwand.

Ein weiteres zentrales Thema wäre IT-Governance. Ich habe oft gesehen, dass eine starke strukturelle Organisation einen großen Einfluss darauf hat, wie Cybersecurity im Unternehmen umgesetzt wird. Diese beiden Aspekte wären wahrscheinlich die Hauptthemen, die ich in einem Artikel oder Buch über DORA behandeln würde.

Wenn wir uns in einem Jahr wiedertreffen, was würden wir uns dann wünschen, heute schon getan zu haben?
Anna Muri: Ich würde mir wünschen, dass der europäische Fokus stärker auf IKT-Dienstleister gerichtet wird. Aktuell sehen wir Probleme, wenn kleine und mittelständische Unternehmen mit vielen Anfragen regulierter IT-Dienstleister konfrontiert werden, wie es DORA verlangt. Ein europäisches Register, in dem sich Dienstleister einmal registrieren und alle Informationen bereitstellen, könnte sowohl der Dienstleisterbranche als auch der regulierten Branche helfen.

09 Organisation und Ressourcen

Wie gut Unternehmen in puncto Cybersicherheit organisiert sind und welche Ressourcen sie zur Verfügung haben, spielt eine wesentliche Rolle. Wissen die heimischen Unternehmen, was ihre schützenswerten Assets sind, welche ihrer Daten sich bei Dritten befinden oder wie sie bei einem Cyberangriff reagieren werden? Können sie ihr aktuelles Cyberrisiko messen und ihre finanziellen Schäden planen? Auch ihr dezidiertes Cybersecurity-Budget und wie mit diesem umgegangen wird, sind wesentlich. Neben all diesen Themen ist auch der Faktor Mensch entscheidend, sowie die Anzahl jener Personen, die sich mit Cybersecurity in Unternehmen beschäftigen.



Im Schnitt benötigen die Befragten **4 bis 6 Monate,** um IT-Expert:innen für ihr Unternehmen zu rekrutieren.

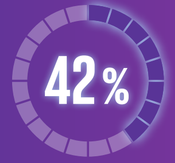
haben einen **vollständigen bzw. sehr guten Überblick** über ihre schützenswerten Assets.

meinen, ihr aktuelles **Cybersecurity-Risiko messen zu können.**

wissen schon heute, wie sie bei einem **großen Cyberangriff** reagieren werden.

Bei fast zwei Drittel ist das **Cybersecurity-Budget** (eher) gestiegen.

Für 4 von 10 Befragten sind **behördliche Vorgaben** ein Treiber für die Budgetveränderung.



können den **durchschnittlichen finanziellen Schaden** durch Cyberangriffe in den kommenden 12 Monaten nicht schätzen.

Mitarbeiter:innen in Cybersecurity-Abteilungen

Große Unternehmen beschäftigen laut eigenen Angaben mehr als 50 Personen im Bereich Cybersecurity, mittlere Unternehmen 3 bis 5 Personen und kleine Unternehmen haben zumindest 1 bis 2 Personen in ihrer Organisation, die sich um Cybersecurity kümmern. Unabhängig von der Größe des Unternehmens ist hier natürlich auch mit Doppelfunktionen zu rechnen oder es existieren gewisse Unschärfen, wenn Security-Themen von Mitarbeitenden bearbeitet werden, ohne dass es dafür eine eigene Stelle im Unternehmen gibt.

Die Entwicklungen zeigen, dass sich Unternehmen der Cyberrisiken bewusst sind. Nichtsdestotrotz besteht noch Aufholbedarf, denn vor allem bei mittelständischen Unternehmen, die Weltmarktführer in ihren Bereichen und Industrien sind, wurden die Bedrohungen noch nicht vollumfänglich erkannt. Schulungs- und Qualifizierungsmaßnahmen sind erste Schritte, um die Mitarbeitenden für Cybersecurity zu qualifizieren. Für mittlere und große Unternehmen ist es empfehlenswert, eine eigene Rolle zu etablieren, die sich ausschließlich mit Informations- und Cybersicherheit beschäftigt und als Vorbild in der Organisation für diese Themen dient. „Vorbild" ist auch das Stichwort, denn gerade in kulturellen Aspekten darf Cybersecurity nicht ein Verhinderer sein, sondern muss dafür sorgen, dass die Unternehmensaktivitäten in einem sicheren Umfeld passieren.

Dieses Mindset ist entscheidend, um die Sicherheitskultur im Unternehmen auszubauen.

Kaum Wachstum bei der Teamgröße

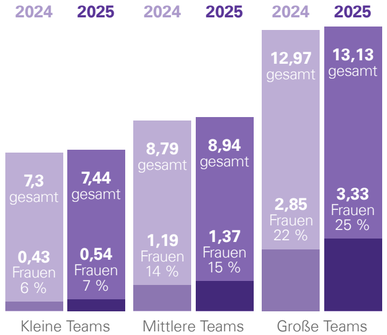
Die minimale Teamgröße von Cyberteams ist von 7,3 Personen im Jahr 2024 auf 7,44 Personen im Jahr 2025 angestiegen. Die durchschnittliche Teamgröße stieg von 8,79 auf 8,94 Personen an. Dieser – wenn auch nur leichte – Anstieg (+0,14 bzw. +0,15) könnte Rückschlüsse auf gestiegene Investitionen in Cybersicherheit zulassen. Bei der maximalen Teamgröße sehen wir einen noch etwas stärkeren Anstieg (+0,16 auf 13,13 Personen). Das könnte ein Indikator dafür sein, dass sich der Abstand zwischen Unternehmen, die Vorreiter sind, und jenen, die hinterherhinken, weiter ausbaut.

Während einige Unternehmen ihre Teams weiter vergrößern – u. a. getrieben durch regulatorische Anforderungen oder ambitionierte Sicherheitsstrategien –, arbeiten andere mit minimalen Teams weiter. Insbesondere kleine Teams stehen vor der Herausforderung, die Cybersicherheit rund um die Uhr zu gewährleisten – Unternehmen müssen aufpassen, dass sie hier nicht an der falschen Stelle sparen.

Luft nach oben beim Frauenanteil

Der gemessene Frauenanteil in unseren Umfrageergebnissen stieg minimal, von 6 Prozent im Jahr 2024 auf 7 Prozent im Jahr 2025. In absoluten

Abb. 26: Frauenanteil Cybersecurity



Zahlen ergibt das einen Anstieg von 0,43 auf 0,54 Frauen. Wir sind hier also nach wie vor weit entfernt von echter Diversität.

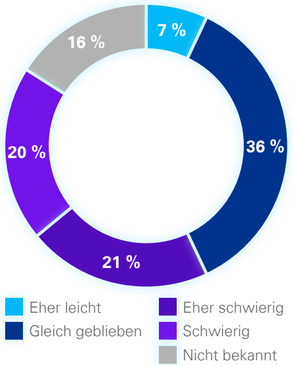
Der durchschnittliche Frauenanteil beträgt 15 Prozent. Vor dem Hintergrund des Fachkräftemangels in der Branche ist das umso unverständlicher. Der maximale Frauenanteil beträgt 25 Prozent, was ein Anstieg von 3 Prozent gegenüber dem Vorjahr ist. Blicken wir auf die absolute Steigerung der Maximalwerte, so sehen wir eine interessante Entwicklung: Teams mit hohem Frauenanteil beschäftigen im Jahr 2025 durchschnittlich 3,33 Frauen (+0,48). Das bestätigt die Annahme, dass Diversität erst ab einer gewissen Masse sichtbar und vor allem auch wirksam wird.

Systemische Barrieren im Arbeitsalltag

Die Umfrageergebnisse decken einige systemische Barrieren auf, die es zu adressieren gilt. Der minimale Frauenanteil von 7 Prozent entspricht in der Realität oft einer einzigen Frau im Team. Führen wir uns nochmals den Unterschied zwischen minimal besetzten Teams (7,44 Personen) und maximal besetzten Teams (13,13 Personen) vor Augen, so erkennen wir zwei unterschiedliche Strömungen in den Unternehmen: Die einen haben Cybersecurity als strategische Priorität erkannt und investieren in den Aufbau ihrer Teams, während es für die anderen eher ein notwendiges Compliance-Übel ist.

Die Maximalwerte (25 Prozent Frauenanteil bei 13,13 Personen) belegen, dass diverse Teams möglich sind. Auch sind sie leistungsfähiger: Sie haben eine Größe erreicht, in der echte Arbeitsteilung und Spezialisierung möglich ist. Diese Unternehmen, die Diversität aktiv leben, sind auch diejenigen, die in anderen Bereichen (Teamgröße, Budget) führen. Das zeigt einmal mehr, dass Inklusion nicht isoliert betrachtet werden darf, sondern als ein wichtiger Teil in einer fortschrittlichen Gesamtstrategie.

Abb. 27: Im Vergleich zum letzten Jahr, wie schwierig oder leicht war es, Cybersecurity-Expert:innen zu rekrutieren?



Eine Branche im Widerspruch

Mit Cybersecurity verbinden wir oftmals Innovation, wirft man jedoch einen Blick auf Diversität, ist davon wenig zu sehen. Der Fortschritt in diesem Bereich ist nur gering, ungleichmäßig verteilt und bleibt oft auf symbolische Gesten beschränkt. Die Komplexität der Bedrohungen nimmt rasant zu und Cyberkriminelle bedienen sich immer moderneren Mitteln. Unternehmen dürfen nicht den Fehler machen, mit ihren Personalstrategien in der Vergangenheit zu verharren.

Die eigentliche Sicherheitslücke, die heimische Unternehmen 2025 schließen müssen, ist nicht technologischer, sondern kultureller Natur: Solange die Cybersecurity-Branche nicht das gesamte Spektrum an Talenten ausschöpft – einschließlich jener 50 Prozent der weiblichen Bevölkerung –, wird sie im Kampf gegen Bedrohungen auf lange Sicht verlieren – sind diese doch agiler, kreativer und diverser als ihre eigenen Teams. Mangelnde Anpassungsfähigkeit darf nicht zum Stolperstein werden, der uns im Wettrennen gegen die Angreifer:innen verlieren lässt.

Rekrutierung von IT-Expert:innen

Cybersicherheit erfordert Expert:innenwissen, um zielgerichtet reagieren zu können. 41 Prozent der befragten Unternehmen gaben in unserer diesjährigen Studie an, dass es ist im Vergleich zum Vorjahr weiterhin (sehr) schwierig ist, Expert:innen für Cybersecurity zu rekrutieren. Mehr als ein Drittel der befragten Unternehmen ist der Meinung, dass sich die Lage gegenüber dem letzten Jahr, die grundsätzlich schon schwierig war, nicht verändert hat und es weiterhin eine Herausforderung bleibt, passende Fachleute einzustellen. Wir sehen also durchwegs eine unverändert angespannte Situation.

Dauer bis zur Einstellung von passenden IT-Expert:innen

So wie im Vorjahr benötigten die Befragten auch heuer wieder im Schnitt 4 bis 6 Monate, um IT-Expert:innen für ihr Unternehmen zu rekrutieren (33 Prozent). Jedes zehnte Unternehmen benötigt zwischen 7 und 12 Monaten (14 Prozent), um die entsprechenden Expert:innen einzustellen.

Ausbildungsinitiativen

Wo wünschen sich die Befragten Initiativen, wenn sie an das Thema Ausbildung im Bereich Cybersecurity denken? Umfassende Schulbildung und universitäre Ausbildung sind für die Umfrageteilnehmenden von enormer Bedeutung, um ein Bewusstsein für Cybersecurity zu schaffen. Dies sollte bereits im Grundschulalter beginnen und sich in den höheren Schulstufen sowie berufsbildenden Schulen und Hochschulen fortsetzen. Auch niederschwellige Angebote für KMU und kostengünstige bzw. geförderte Schulungsprogramme werden als wesentlicher Baustein betrachtet, um mehr Menschen für das Thema zu begeistern.

Neben Aus- und Weiterbildungsinitiativen ist den Befragten aber auch eine praxisorientierte Ausbildung wichtig. Hierzu wurden Training on the Job, praxisnahe Weiterbildungsangebote für IT-Personal und die Integration von Cybersecurity in bestehende Ausbildungsberufe genannt. Auch Cybersecurity als Lehrberuf oder als Zusatzqualifikation zu bestehenden IT-Ausbildungen wurde von den Befragten gewünscht. Als wesentliche Initiative wird auch der Austausch mit anderen Unternehmen und Fachleuten angesehen.

Genannt wurden auch die Sensibilisierung und Schulung von Führungskräften und Mitarbeitenden für Cyberrisiken. Es besteht der Wunsch nach mehr staatlicher Unterstützung und Förderungen, um die Attraktivität und Zugänglichkeit von Cybersecurity-Ausbildungen zu erhöhen.

Verankerung von Cybersicherheit in jeder Generation

Um Cybersicherheit in jeder Generation zu verankern, sind umfassende Aufklärung und Bildung für die befragten Unternehmen von entscheidender Bedeutung. Das sollte bereits in der Schule beginnen, indem Cybersicherheit in das Curriculum inkludiert wird. Social Media und Medien können dabei helfen, die Informationen einem breiten Publikum zugänglich zu machen und die Wichtigkeit von Cybersecurity zu verdeutlichen.

Für die Befragten ist es darüber hinaus wichtig, dass Cybersecurity als zentraler Bestandteil des Alltags und der Unternehmenskultur wahrgenommen wird, und nicht nur als rein technisches Thema. Durch Informationskampagnen sollte darüber hinaus die Sensibilisierung ausgebaut und die Menschen befähigt werden, sich selbst und ihre Daten zu schützen. Eine Zusammenarbeit von öffentlichen und privaten Institutionen und die Einbindung von Expert:innen aus verschiedenen Bereichen kann laut den Befragten dabei helfen, ein umfassendes Verständnis für Cybersecurity zu entwickeln sowie die nötigen Maßnahmen umzusetzen.

Schützenswerte Assets

Einer der wesentlichen Faktoren, um Cybersecurity effizient zu steuern, ist, einen Überblick und die Transparenz über die eigenen schützenswerten Güter zu haben. Unter schützenswerten Gütern verstehen wir zum einen Assets wie Hardware- und Softwarebestände sowie Daten und geistiges Eigentum und zum anderen IP-Adressen und Softwarecodes. Gerade hier ist es entscheidend zu wissen, welche Assets für das Unternehmen besonders wertvoll sind, welchen Beitrag sie in den Geschäftsprozessen spielen und welcher Schutzbedarf dafür notwendig ist. Dafür bedarf es zu Beginn eines guten Überblicks. Dieser Überblick ist vor allem dann entscheidend, wenn es bei einem Cyberangriff darum geht, richtig zu reagieren und Prioritäten abzuleiten.

Auf die Frage, ob sie einen vollständigen Überblick über ihre schützenswerten Assets haben, antworten 65 Prozent der Befragten, dass sie einen vollständigen oder zumindest sehr guten Überblick darüber haben. 16 Prozent der Unternehmen sind der Meinung, dass ihnen dieser Überblick und diese Transparenz noch fehlen. Die Antworten stimmen uns durchwegs positiv, die Praxis zeigt aber ein anderes Bild: Durch die zunehmende Digitalisierung, die Verschmelzung von IT und OT sowie die gestiegene Nutzung von Cloud-Diensten fällt es Unternehmen immer schwerer, genau diesen Überblick zu behalten. Die Antworten aus der Umfrage sind ein Indiz dafür, dass Wunsch und Realität auseinanderklaffen. Aus der Praxis sehen wir, dass gerade Asset-Management-Projekte, also die Inventarisierung von Hard- und Software, Mammutaufgaben für Unternehmen darstellen. Nahezu jedes Unternehmen ist heute damit konfrontiert, genau diese Inventarisierung aktuell zu halten. Das ist kein Projekt, sondern ein Prozess. Aber nur so wird die Aktualität der Daten gewährleistet.

Daten bei Dritten

Die Vernetzung mit Dritten und die Auslagerung der Daten bei Dienstleistern bzw. die Datenverarbeitung durch Dienstleister erhöhen die Abhängigkeit und Komplexität. Gerade deshalb ist es entscheidend zu wissen, wo sich welche Daten befinden. Dieser Überblick ist es auch, der bei einem Sicherheitsvorfall entscheidet, wer wie zu informieren ist und welche Informations- und Berichtspflichten existieren. NIS-2, DORA und alle weiteren Regularien sowie die Datenschutzgrundverordnung legen ein besonderes Augenmerk darauf.

63 Prozent der befragten Unternehmen geben an, dass sie wissen, wo sich ihre Daten befinden und dass sie auch hinreichende Sicherheit darüber haben, dass diese ausreichend geschützt sind. Nur jedes achte Unternehmen ist der Meinung, dass sie keinen hinreichenden Überblick haben. Auch hier klaffen wieder Realität und Wunsch auseinander, denn die überwiegende Mehrheit der Angriffe richtet sich heute gegen Dienstleister. Dienstleister sind für Angreifer:innen besonders lukrativ, da genau sie es sind, die über eine Vielzahl an Systemen, Daten und Kund:innen verfügen und es – da sie das schwächste Glied in der Kette sind – ein leichtes Unterfangen ist, genau auf diese Dienstleister beziehungsweise auf Third Parties zuzugreifen und hier erfolgreiche Angriffe zu erzielen.

Reaktion bei Cyberangriffen

Um Risiken adressieren zu können, ist es notwendig, entsprechende Reaktionsmaßnahmen bei einem Cybersicherheitsvorfall zu etablieren. Das bedeutet, Reaktionspläne parat zu haben, diese zu üben und in der Lage zu sein, diese auch zielgerichtet abzuarbeiten. 52 Prozent der befragten Unternehmen sagen, dass sie heute schon wissen, wie sie bei einem großen Cyberangriff reagieren werden. Dieses Selbstverständnis ist zwar löblich, gerade bei komplexen Cybersicherheitsvorfällen sind es aber die ersten 70 Stunden, die entscheidend dafür sind, inwieweit und ob Cyberangriffe so bearbeitet werden können, dass es zu keinen negativen Konsequenzen für das Unternehmen kommt.

27 Prozent der befragten Unternehmen haben angegeben, dass sie noch nicht wissen, wie sie reagieren werden. Hier besteht definitiv Aufholbedarf. Genau diesen Befragten, die ehrlich ihre Unvollständigkeit in der Bearbeitung der Themen offengelegt haben, sei nahegelegt, dass die erste Reaktion – so wie bei Ersthelfer:innen, die an eine Unfallstelle kommen – entscheidend ist.

Notwendige Kosten

Jedes zweite Unternehmen (49 Prozent) stimmt der Aussage zu, dass die Aufwände für Cybersicherheit notwendige Kosten sind, die besser woanders eingesetzt werden können. Es ist durchwegs überraschend, dass Cybersecurity als notwendiger Kostenfaktor gesehen wird, denn genau sie entscheidet darüber, ob Unternehmen nach digitalen Angriffen weiterhin existenzfähig sind oder nicht.

23 Prozent sagen, dass sie die Aufwände für Cybersicherheit nicht als notwendige Kosten ansehen, die besser woanders eingesetzt werden können. Es ist in unserer digital vernetzten Welt, die von geopolitischen Veränderungen, und der Verlagerung der Bedrohungen in den digitalen und Informationsraum beeinflusst wird, alternativlos, sich mit Cybersecu-

Abb. 28: Veränderung des Cybersecurity-Budgets in den letzten 12 Monaten

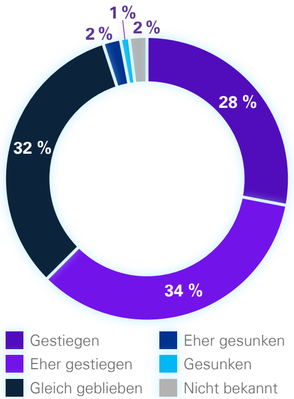
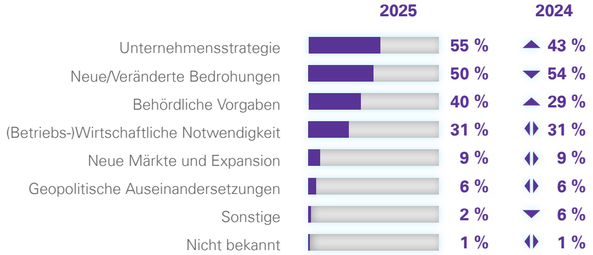


Abb. 29: Cybersecurity-Budget Gründe Veränderung



rity auseinanderzusetzen. Digitalisierung kann nur dann funktionieren, wenn sie auch in der Lage ist, unter widrigen Umständen, das heißt, kontinuierliche Angriffe aus unterschiedlichsten Bereichen, standhaft zu bleiben und die Dienste und Services weiter anzubieten. Als Bürger:in eines Landes möchte man selbst doch auch den Strom nutzen, frisches Trinkwasser konsumieren und auf wichtige Dienste zurückgreifen können, selbst wenn laufend Cyberangriffe auf zentrale Einrichtungen stattfinden.

Budget für Cybersecurity

Wenn wir über Sicherheit und die damit verbundenen Kosten sprechen, müssen wir uns auch dem Cybersecurity-Budget widmen. Bei unserer diesjährigen Umfrage gaben 10 Prozent der befragten Unternehmen an, dass ihr Budget 3 bis 5 Prozent des IT-Budgets beträgt. 9 Prozent gaben an, dass sie 6 bis 10 Prozent des IT-Budgets für Cybersecurity zur Verfügung haben. Bei 10 Prozent der Befragten sind es mehr als 10 Prozent des Budgets, welches sie für Cybersecurity nutzen können. Im Vergleich zum letzten Jahr sehen wir hier eine eindeutige Erhöhung, die uns positiv stimmt. Auf der anderen Seite stehen diese Aussagen im Widerspruch zu den notwendigen Kosten.

Zwei Aspekte stechen besonders ins Auge: 42 Prozent der befragten Unternehmen geben an, dass sie kein dezidiertes Budget für Cybersecurity haben, was im Zeitalter der zunehmenden Angriffe auf digitale Infrastrukturen und Systeme verwunderlich ist. 19 Prozent ist nicht bekannt, ob sie ein Budget zur Aufrechterhaltung für Cybersicherheit haben oder nicht. Zusammengefasst bedeutet das, dass 61 Prozent der befragten Unternehmen entweder über kein dezidiertes Budget verfügen oder keine entsprechende Kenntnis darüber haben. Bedauerlicherweise herrscht im Hinblick auf die budgetäre Dotierung dieses Bereichs wenig Transparenz bzw. kaum Planung.

Obwohl klar ist, dass die Aufwendungen für Cybersecurity nicht immer eindeutig einem Bereich zugeordnet werden können, da sie in anderen Projekten bzw. Betriebsthemen mitverpackt sind, gibt es dennoch Aktivitäten, die eindeutig dem Thema Cybersicherheit zuzuordnen sind und für die ein entsprechendes Budget und Kostentransparenz notwendig sind. Auch die Regulatorik, und hier im Speziellen DORA, verlangt von den Unternehmen eine ausreichende finanzielle Dotierung des Cybersecurity-Bereichs, um dem Thema auch die entsprechende Priorität zu geben. Ohne diese Dotierung können keine risikominimierenden Maßnahmen bzw. keine Behandlung von identifizierten Risiken in ausreichender Qualität erfolgen.

Veränderung des Budgets im Vergleich zum Vorjahr

Im Vergleich zum Vorjahr sehen wir eine Erhöhung des Cybersecurity-Budgets bei den Unternehmen. 62 Prozent gaben an, das das Budget gestiegen oder eher gestiegen ist. Bei einem Drittel der befragten Unternehmen blieb das Budget nahezu gleich. 3 Prozent der befragten Unternehmen geben an, dass es zu leichten Rückgängen in ihrem Cybersecurity-Budget gekommen ist.

Gründe für die Budgetveränderung

Gefragt nach den Gründen für die Veränderung des Budgets steht an erster Stelle (55 Prozent) die Unternehmensstrategie, die als Treiber gewirkt hat. An zweiter Stelle (50 Prozent) gaben die Befragten an, dass neue oder veränderte Bedrohungen hierfür der ausschlaggebende Grund gewesen seien. An dritter Stelle – und heuer durchaus verwunderlich – haben behördliche Vorgaben eine Veränderung des Budgets mit sich gebracht. Die Regulatorik ist aktuell der größte Antrieb für die Veränderung der Security-Budgets im Vergleich zum Jahr 2024. So gaben 40 Prozent der befragten Unternehmen an, dass für sie behördliche Vorgaben ein Treiber für die Veränderung des Budgets gewesen sind. Im Vorjahr waren dies nur 29 Prozent.

Des Weiteren gaben die Befragten in unsere Studie als Gründe für die Budgetveränderung die Investition in die Erneuerung der SOC-Infrastruktur und ein neues Betriebsmodell, die Aufstockung des Personals sowie die Verstärkung der Sicherheitsmechanismen an.

Messung des aktuellen Cyberrisikos

Gerade für die Beurteilung, ob und inwieweit Cyberrisiken existieren bzw. ob Risiken durch die Auslagerung von Tätigkeiten an Dritte bestehen, stellt sich die Frage, ob Unternehmen ihr aktuelles Cyberrisiko kennen und dieses in weiterer Folge messen können. Bei der Messung scheiden sich die Geister, denn zum einen sprechen wir hier von der qualitativen Beurteilung, das bedeutet eine Einordnung auf einer Skala hinsichtlich Eintrittswahrscheinlichkeit und Schadenshöhe und zum anderen von der quantitativen Analyse, bei der finanzielle Beträge hinterlegt sind.

Die aktuell existierende Regulatorik verlangt explizit, dass Unternehmen in der Lage sein müssen, ihre Risiken zu qualifizieren, aber auch dass größere Unternehmen und wesentliche Einrichtungen ihre Risiken zusätzlich zu quantifizieren haben. Auf die Frage, ob Unternehmen in der Lage sind, ihr aktuelles Cybersecurity-Risiko zu messen, gaben 53 Prozent an, dass sie das können. 16 Prozent der Befragten sind der Meinung, dass sie dahingehend noch nicht so weit sind.

Auch hier zeigt sich, dass das Selbstverständnis mit dem, was die praktische Erfahrung widerspiegelt, nicht kongruent ist. Gerade bei der Risikomodellierung und der Identifizierung der Risiken und in weiterer Folge der Beurteilung sehen wir oft noch Verbesserungspotenzial. Aktuell werden Risikobeurteilungsverfahren sehr einfach bzw. oberflächlich gehandhabt und haben noch nicht den Tiefgang, den es benötigt, um Risiken zu steuern. Vor allem vermissen wir oft bei der Risikosteuerung den Bezug zu Assets, also den schützenswerten Gütern. Gerade diese entscheiden erst, ob ein Risiko überhaupt wirksam wird. Sofern kein schützenswertes Gut damit in Zusammenhang steht, ist das Risiko für Unternehmen nämlich auch nur bedingt von Bedeutung. Genau dieses Zusammenspiel ist wesentlich, um eine Priorisierung der Aktivitäten durchführen zu können und in weiterer Folge auch die vorhandenen Ressourcen – personelle als auch finanzielle – zielgerichtet einzusetzen.

Top 5 Angriffsarten

Bittet man die Befragten, die Angriffsarten nach ihrer Wichtigkeit für ihr Unternehmen zu reihen, so ergibt sich ein durchwegs interessantes Bild. Unsere diesjährige Umfrage zeigt eine deutliche Verschiebung der Prioritäten bei der Einschätzung von Cyberrisiken gegenüber dem Vorjahr.

Phishingattacken dominieren mit 70 Prozent der Nennungen als größte Bedrohung, was eine Zunahme von 28 Prozent gegenüber dem Vorjahr darstellt. Diese Entwicklung unterstreicht die anhaltende Effektivität sozialer Manipulationstechniken, die durch Automatisierung und KI-gestützte Personalisierung weiter an Komplexität gewinnen. Der signifikante Anstieg korreliert mit Berichten über ausgeklügelte Phishingkampagnen, die selbst Multi-Faktor-Authentifizierung (MFA) unterlaufen – ein Risiko, das 2025 erstmals mit 24 Prozent in der Wahrnehmung verankert ist.
MFA-Aushebelung etabliert sich als eigenständiges Toprisiko, was auf die zunehmende Verbreitung von Angriffsmethoden wie Echtzeit-Phishing und Session-Hijacking hinweist. Die Tatsache, dass dieses Risiko 2024 noch nicht erfasst wurde, reflektiert sowohl die gestiegene Abhängigkeit von MFA als auch die Adaptionsgeschwindigkeit der Angreifer:innen.
Parallel dazu gewinnen **automatisierte Anrufe** (21 Prozent) als Einfallstor für Social Engineering an Relevanz. Das deutet auf eine Diversifizierung der Angriffsvektoren jenseits rein digitaler Kanäle hin. Während **KI-/ML-basierte Betrugsmethoden** mit 8 Prozent noch vergleichsweise niedrig von den Befragten eingestuft werden, deutet deren erstmalige Erwähnung auf ein wachsendes Problembewusstsein hin – insbesondere im Zusammenhang mit Deepfake-Technologien und automatisierten Angriffssystemen.
Spionage (4 Prozent) komplettiert die Top 5, wobei der vergleichsweise niedrige Wert die Komplexität in der Aufdeckung staatlich geförderter Angriffe und deren Unterrepräsentation in öffentlichen Schadensstatistiken widerspiegeln könnte.

Abb. 30: Veränderung der Angriffsarten

	2025	2024
Abhören der Kommunikation (Man-in-the-Middle-Angriff)	13 %	▼ 15 %
Advanced Persistent Threats (APTs)	11 %	▼ 16 %
Andere Angriffsarten	2 %	▼ 5 %
Aushebeln der Multi-Faktor-Authentifizierung	24 %	▲ 0 %
Business-E-Mail-Compromise, CEO-/CFO-Fraud	26 %	▼ 34 %
Cloud-Fehlkonfiguration	19 %	▲ 21 %
Datendiebstahl (Data Breach)	43 %	▼ 48 %
Deepfake (Audio, Images, Video)	16 %	▼ 19 %
Denial-of-Service-Attacken (DoS)	21 %	◆ 21 %
Identitätsdiebstahl	37 %	▼ 40 %
Industriesteuerungsanlage Kompromittierung (OT)	4 %	▼ 8 %
Insider Threat	5 %	▼ 8 %
KI/ML betrügerisch verwendet	8 %	▲ 0 %
Malware (E-Mail-Anhang)	42 %	▼ 54 %
Mobile Malware	7 %	▼ 14 %
Passwortdiebstahl	31 %	▼ 33 %
Ransomware/Erpressung	30 %	▼ 39 %
Social Engineering	13 %	▼ 19 %
(Spear-)Phishingattacke (E-Mail-Link)	70 %	▲ 42 %
Spionage	4 %	▲ 0 %
Spoofing	3 %	▼ 8 %
Supply-Chain-Angriff (Lieferkette)	10 %	▼ 14 %
Unerwünschte, automatisierte Anrufe (Scam-Anrufe)	21 %	▲ 0 %

Auffällig ist der relative Bedeutungsverlust traditioneller Bedrohungen: **Ransomware** verliert 9 Prozent (auf 30 Prozent), während **Malware via E-Mail-Anhängen** einen Rückgang von 12 Prozent verzeichnet. Diese Entwicklung könnte auf verbesserte Endpoint-Security-Lösungen und erhöhte Mitarbeiter:innensensibilisierung zurückzuführen sein. Dennoch bleibt der **Datendiebstahl** mit 43 Prozent ein Kernrisiko, das eng mit Phishing und MFA-Schwachstellen verknüpft ist.

Anhand der Umfrageergebnisse ist klar, dass Unternehmen die Verwundbarkeit ihrer menschlichen Firewall und technischen Authentifizierungsmechanismen erkannt haben. Parallel dazu verbessert sich die Abwehr klassischer Malware-Angriffe. Das macht eine Neuausrichtung der Cybersecurity-Strategien erforderlich. Unternehmen müssen zunehmend integrierte Lösungen entwickeln, die Verhaltensanalyse, KI-gestützte Bedrohungserkennung und physisch-digitale Sicherheitskonzepte miteinbeziehen.

Einschätzung der Eintrittswahrscheinlichkeit von Cyberrisiken

Neben einem Blick auf die Top 5 Angriffsarten und deren Reihung im Hinblick auf Priorität für die Unternehmen, stellt sich ebenso die Frage, wie Unternehmen die Wahrscheinlichkeit einschätzen, dass die von ihnen genannten Angriffsarten auch tatsächlich Schäden bei ihnen verursachen. Die Lage bei heimischen Unternehmen ist durchaus angespannt, aber das Gefahrenradar ist noch nicht bei allen sensibilisiert. Jedes vierte Unternehmen gibt an, mit einer (eher) hohen Eintrittswahrscheinlichkeit zu rechnen. Mehr als ein Drittel der Unternehmen ist der Meinung, dass die von ihnen genannten Angriffe kaum Schäden verursachen werden.

Blick in die Zukunft: Schätzung und Planung finanzieller Schäden

Auch unsere zehnte Umfrage zeigt, dass es für Unternehmen schwierig ist, die Schäden, die durch Cyberangriffe entstehen können, zu quantifizieren. Wenngleich die Regulatorik von den Unternehmen verlangt, Risiken und Schäden zu

Auch das Bundesministerium für Inneres berichtet im Dezember des Vorjahres von bislang 1.700 Fällen und EUR 4,2 Mio. Schaden für das Jahr 2024 durch den „Tochter-Sohn-Trick".

Dabei wird den Opfern weisgemacht, mit den vermeintlich eigenen Kindern zu sprechen. Diese würden unter einer neuen Telefonnummer anrufen und Hilfe benötigen – verbunden mit dringlichen Geldforderungen, die oftmals im vierstelligen Bereich liegen und auf ausländische Konten überwiesen werden sollen.[1]

[1] https://www.bmi.gv.at/news.aspx?id=2F33526E345939426B69343D, abgerufen am: 18.04.2025.

quantifizieren, so zeigt sich, dass genau dieser Punkt noch immer ein großes Problem für Unternehmen darstellt. Auf die Frage, wie hoch sie den durchschnittlichen finanziellen Schaden für Cyberangriffe in den kommenden 12 Monaten schätzen, gaben 42 Prozent an, dass sie es nicht wüssten. 47 Prozent konnten auch nicht den maximalen Schaden benennen, mit dem sie in den kommenden 12 Monaten rechnen.

Die Umfrageergebnisse zur Einschätzung des maximalen finanziellen Schadens durch Cyberangriffe in den kommenden zwölf Monaten zeigen eine signifikante Verschiebung der Risikowahrnehmung bei Unternehmen im Vergleich zu 2024. Auffällig ist die deutliche Zunahme jener Unternehmen, die ihre potenziellen Schäden nicht quantifizieren können (Anstieg von 36 Prozent auf 47 Prozent). Das deutet auf eine wachsende Unsicherheit in der Risikomodellierung hin, möglicherweise bedingt durch die steigende Komplexität von Cyberbedrohungen.

In allen definierten Schadenskategorien sehen wir einen Rückgang der Einschätzungen – besonders im mittleren Schadensbereich (EUR 5.001–10.000: -4 Prozent; EUR 10.001–50.000: -3 Prozent). Während ein Teil der Unternehmen durch verbesserte Sicherheitsmaßnahmen und Threat-Intelligence-Systeme präzisere Prognosen erstellen kann, kämpft der andere Teil mit einer Untererfassung von Risiken aufgrund unzureichender Exposure-Management-Strategien. Der leichte Rückgang im oberen Schadensbereich (über EUR 1 Mio.: -1 Prozent) steht im Widerspruch zu branchenweiten Prognosen, die für das Jahr 2025 einen globalen Anstieg der Cybercrime-Kosten um USD 1 Billion voraussagen.[2]

Wir sehen auch hier, dass die tatsächliche Bedrohungslage mit dem Risikobewusstsein in Unternehmen auseinanderklafft. Auffällig ist in diesem Zusammenhang auch der Anstieg jener Befragten, denen der finanzielle Schaden nicht bekannt ist. Gründe hierfür könnten unzureichende Penetrationstests, mangelnde Integration von Threat-Intelligence-Daten oder Defizite in der Schwachstellenbewertung sein. Auch könnten hybride Bedrohungsvektoren, die traditionelle Risikobewertungsmodelle überfordern (z. B. Supply-Chain-Angriffe oder Zero-Day-Exploits, deren Schadenspotenzial nur schwer isolierbar ist), etwas mit dem Unwissen der Befragten bezüglich Schadenssummen zu tun haben.

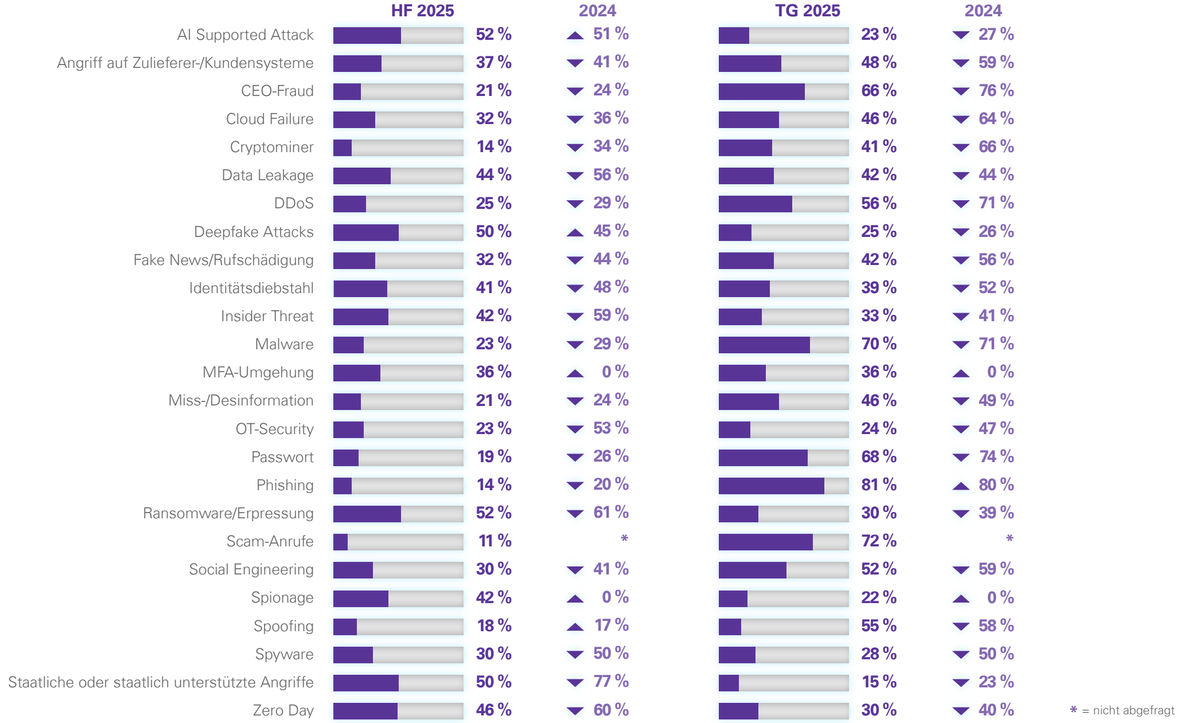
Anstatt sich statischer Schadensprognosen zu bedienen, sollten Unternehmen dynamische Risikoframeworks einsetzen. Diese erlauben ihnen ein kontinuierliches Monitoring, KI-gestützte Bedrohungsmodellierung sowie die Integration von Geschäftsrisiko- und Sicherheitsmetriken. Exposure-Management-Ansätze müssen ganzheitlich im Unternehmen etabliert werden, inklusive Quantifizierung indirekter Schäden wie Imageverlust und operative Ausfallzeiten. Nur so lässt sich die Lücke zwischen erwarteten und realen Cyberrisiken schließen.

Blicken wir jedoch auf die großen Unternehmen, so sehen wir, dass diese mit durchwegs erhöhten Schadenaufkommen rechnen. 18 Prozent der Großunternehmen rechnen mit mehr als EUR 1 Mio. Schaden in den kommenden 12 Monaten. 14 Prozent sind der Meinung, dass sie einen Schaden durch Cyberangriffe in den kommenden 12 Monaten in der Größenordnung von EUR 500.000 bis EUR 1 Mio. haben werden.

Ein Blick auf die mittelständischen Unternehmen zeigt uns, dass diese in den kommenden 12 Monaten mit einem Schaden von EUR 50.000 bis EUR 100.000 rechnen (15 Prozent) bzw. mit EUR 100.000 bis EUR 500.000 (14 Prozent). Auffällig ist, dass 13 Prozent der befragten mittelständischen Unternehmen angeben, dass sie mit maximalen Schäden von mehr als EUR 1 Mio. in den nächsten 12 Monaten planen. 37 Prozent der mittelständischen Unternehmen können keine Aussage diesbezüglich treffen – ihnen ist der finanzielle Schaden, mit dem sie rechnen, nicht bekannt.

[2] https://cybersecurityventures.com/cyberwarfare-report-intrusion/, abgerufen am: 12.04.2025.

Abb. 31: Herausforderung (HF) vs. Tagesgeschäft (TG) im Jahresvergleich



Vergleicht man große mit mittelständischen Unternehmen, zeigt sich, dass die Auswirkungen mit der Größenklasse des Unternehmens korrelieren – ist doch für ein mittelständisches Unternehmen ein Schaden in der Größenordnung von bis zu EUR 500.000 durchwegs existenzbedrohend. Gleiches gilt für große Unternehmen, denn diese rechnen ebenfalls mit Schäden in den oberen Bandbreiten. Vorsorge und Prävention bzw. die entsprechenden Maßnahmen können dabei helfen, den Schaden (zumindest etwas) zu reduzieren.

Tagesgeschäft vs. Besondere Herausforderung

Im Jahr 2025 sehen wir eine Veränderung gegenüber dem Vorjahr darin, welche Cyberrisiken die Befragten als ganz normales Tagesgeschäft und welche sie als besondere Bedrohung einstufen. Neue Technologien, im Speziellen Künstliche Intelligenz, werden für die Unternehmen zu einer besonderen Herausforderung. An erster Stelle finden wir in diesem Jahr AI supported Attacks. 52 Prozent der befragten Unternehmen sehen hierin eine besondere Herausforderung. Ebenfalls auf Platz 1 mit 52 Prozent liegt Ransomware. Ransomware bleibt im Spitzenfeld der besonderen Herausforderungen, ist diese Angriffsart doch besonders vielfältig und oft perfide versteckt.

An zweiter Stelle finden wir ex aequo Deepfake-Attacken sowie staatliche oder staatlich unterstützte Angriffe (jeweils 50 Prozent). Das lässt sich auf geopolitische Veränderungen und die rasante technologische Entwicklung zurückführen. Deepfakes nutzen KI-Technologien, um Sicherheit und Vertrauen vorzutäuschen. Der Zugang zu diesen Tools wird immer niederschwelliger und dadurch stellen sie ein immer größeres Problem dar.

An dritter Stelle befinden sich Zero Days, also Angriffe unter Ausnutzung von Schwachstellen, für die es aktuell noch keine geeigneten Gegenmaßnahmen gibt. Dieses Bild passt gut zu den staatlich oder staatlich unterstützten Angriffen auf Platz 2, stehen diese doch mit Zero Days in Verbindung. Durch die geopolitischen Konflikte kommen vermehrt Zero Days in Umlauf. Nach der erstmaligen Verwendung stehen sie auch Trittbrettfahrern zur Verfügung. Im Bereich der besonderen Herausforderungen erkennen wir eindeutig die Veränderung der geopolitischen Rahmenbedingungen, denn genau die oben genannten Angriffsarten sind es, die in Zeiten zunehmender zwischenstaatlicher Konflikte immer mehr in den Mittelpunkt rücken.

Blicken wir nun auf das normale Tagesgeschäft, also auf Angriffe und Bedrohungen, mit denen wir bereits sehr gut vertraut sind und bereits gelernt haben, mit diesen umzugehen: An erster Stelle liegt Phishing (81 Prozent). Phishingangriffe sind oftmals das Eintrittstor für Täter:innen in die Unternehmen. An zweiter Stelle befinden sich Scam-Anrufe, worunter (versuchte) betrügerische Erpressungen über Telefonie verstanden wird (72 Prozent). Platz 3 belegt Malware, die für Unternehmen immer mehr zum normalen Tagesgeschäft wird. 70 Prozent geben an, dass sie bereits geeignete Mittel haben, um hier zielgerichtet wirksam werden zu können.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1 Diversität in den Cybersecurity-Teams ist auf dem Vormarsch. Diverse Teams sind ein Pull-Faktor und ziehen weitere interessierte Talente an. Damit wird der Anteil an Frauen im Team erhöht.

2 Die Regulatorik verlangt, dass Unternehmen in der Lage sein müssen, ihre Risiken zu qualifizieren. Größere Unternehmen und wesentliche Einrichtungen haben ihre Risiken zusätzlich zu quantifizieren. Aktuell werden Risikobeurteilungsverfahren jedoch sehr oberflächlich gehandhabt und haben noch nicht den Tiefgang, den es benötigt, um Risiken zu steuern. Vor allem der Bezug zu den schützenswerten Gütern fehlt hier oftmals noch.

3 An jenen Angriffen, die für Unternehmen eine besondere Herausforderung darstellen, erkennen wir die veränderten geopolitischen Rahmenbedingungen. Denn genau diese Angriffsarten sind es, die in Zeiten zunehmender zwischenstaatlicher Konflikte immer mehr in den Mittelpunkt rücken.

Nationale und europäische Synergien: Das NCC-AT im Fokus der Cybersicherheit

Hanna Wilhelmer leitet das Aufbauprojekt für das Nationale Koordinierungszentrum für Cybersicherheit (NCC-AT) und spricht über die strategischen Ziele und Herausforderungen bei der Koordination zwischen nationalen und europäischen Akteuren. Erfahren Sie, wie das NCC-AT die Cybersicherheitslandschaft in Österreich stärkt und Innovationen fördert.

Sie leiten den Aufbau des Nationalen Koordinierungszentrums für Cybersicherheit (NCC-AT). Welche Hauptziele verfolgten Sie dabei und welche Herausforderungen, insbesondere bei der Koordination zwischen nationalen und europäischen Akteuren, mussten Sie bewältigen?
Hanna Wilhelmer: Das Nationale Koordinierungszentrum für Cybersicherheit (NCC-AT) fördert die Entwicklung und Nutzung von Forschungsergebnissen und Schlüsseltechnologien im Bereich Cybersicherheit für Wirtschaft, Gesellschaft und öffentliche Einrichtungen. Als Teil eines europäischen Netzwerks von nationalen Koordinierungszentren koordiniert es die Vernetzung der Cybersecurity-Community. Eine Herausforderung war, einen klaren Fokus zu setzen. In Zusammenarbeit mit der Forschungsförderungs GmbH lag der anfängliche Schwerpunkt auf der Unterstützung von Betrieben bei der NIS-2-Richtlinie und EU-Förderungen für Innovation und Deployment.

Das Digital Europe Programm (DEP) ist eines der zentralen EU-Förderprogramme zur Unterstützung von digitalen Technologien und Infrastrukturen. Welche Rolle spielt dieses Programm speziell im Bereich Cybersicherheit?
Hanna Wilhelmer: Das DEP investiert im Bereich Cybersicherheit von 2021 bis 2027 über eine Milliarde Euro in europäische zivile Cybersicherheitslösungen. Dafür wurde eigens das Europäische Kompetenzzentrum für Cybersicherheit, eine neue EU-Agentur in Bukarest, geschaffen, die Expertise und Mittel in der EU dafür bündelt. Das DEP ergänzt damit Schwesterprogramme auf EU-Ebene im Bereich der Forschung durch Horizont Europa und Entwicklung von militärischen Innovationen im EDF. Neben Behörden können damit auch österreichische Unternehmen und Forschungseinrichtungen profitieren und Projektideen kofinanzieren.

> **Cybersicherheit ist ein Teamsport.**

Welche Förderinstrumente bietet das DEP für österreichische Unternehmen und Forschungseinrichtungen im Bereich Cybersicherheit, und wie stärken sie die Innovationskraft und Widerstandsfähigkeit gegen Cyberbedrohungen?
Hanna Wilhelmer: Förderthemen werden in einem mehrjährigen Arbeitsprogramm veröffentlicht, das Inhalte, Förderraten und Ausschreibungszeiten angibt. Im Unterschied zu EU-Forschungsprogrammen werden Projekte meist kofinanziert, da Behörden und Unternehmen im Fokus stehen. Im Arbeitsprogramm 2025–2027 sind 390 Millionen Euro für europäische Cybersicherheitslösungen vorgesehen, darunter neue Technologien wie KI und Post-Quanten-Übergang, das EU-Cybersolidaritätsgesetz, grenzüberschreitende SOC-Infrastruktur, Vorbeugungsmaßnahmen und Unterstützung für KMU, NCCs sowie Dual-Use-Anwendungen. Die Förderung von EU-Einrichtungen signalisiert mehr strategische Autonomie gegenüber nordamerikanischen und asiatischen Märkten.

FOTO © ALEXANDER ZILLBAUER

Mag. Hanna Wilhelmer, BA ist Juristin und leitet das Aufbauprojekt für das Nationale Koordinierungszentrum für Cybersicherheit (NCC-AT) im Bundeskanzleramt Österreich. Sie vertritt Österreich im Verwaltungsrat des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC). Zuvor arbeitete sie in der Ständigen Vertretung Österreichs bei der EU in Brüssel im Bereich Sicherheits- und Außenpolitik. Sie hält Abschlüsse in Rechtswissenschaften und Entwicklungsstudien von der Universität Wien.

Welche Dienstleistungen und Beratungsangebote bietet das NCC-AT, um Unternehmen und Forschungseinrichtungen bei der Beantragung von DEP-Fördermitteln zu unterstützen, und gibt es Schulungen oder Informationsveranstaltungen?
Hanna Wilhelmer: Das NCC-AT-Team berät alle, die sich für eine Bewerbung im Digitales-Europa-Programm interessieren: Neben Webinaren zu den aktuellen Ausschreibungen bieten wir über die Österreichische Forschungsförderungsgesellschaft (FFG) Informationen in individueller Beratung an, ob ein Projektvorhaben zu einer Ausschreibung passen könnte – bis hin zu einem Proposal-Check vor der Einreichung. Darüber hinaus hilft das NCC-AT bei der Partnersuche, auch über die Landesgrenze hinweg.

In unserer Studie gaben 69 Prozent an, dass sie sich eine gezielte politische Förderung heimischer Cybersecurity-Unternehmen wünschen. Wie sehen Sie die Rolle des NCC-AT in diesem Zusammenhang? Welche Maßnahmen könnten ergriffen werden, um diesen Wunsch zu erfüllen?
Hanna Wilhelmer: Heimische Cybersecurity-Unternehmen sind eine wesentliche Zielgruppe des NCC-AT, das als Vermittler zwischen Marktbedürfnissen und Verwaltung fungieren kann. Forschungsergebnisse sollen besser verwertbar werden und die Aus- und Weiterbildung von Fachkräften, insbesondere Frauen, ist wichtig. Diese Maßnahmen können helfen, das EU-Ziel einer

Die aktuelle Förderlandschaft bietet einige Chancen zur Steigerung der Wettbewerbsfähigkeit österreichischer Unternehmen.

stärkeren industriellen Basis im Bereich Cybersicherheit zu erreichen.

Welche strategischen Ziele verfolgt das NCC-AT, um Österreich besser gegen Cyberbedrohungen zu schützen und Innovationen zu fördern?
Hanna Wilhelmer: Mit dem NCC sind zwei Dinge möglich: erstens Förderungen zur Unterstützung der europäischen Cyberindustrie im Gleichklang mit EU-Partnern, zweitens durch Koordination und Community Building, den gesamten Kreislauf von Forschung bis hin zur Anwendung zu unterstützen.

Das NCC-AT arbeitet eng mit dem Europäischen Kompetenzzentrum für Cybersicherheit (ECCC) zusammen. Wie sieht diese Zusammenarbeit konkret aus?
Hanna Wilhelmer: Das ECCC möchte Investitionen in die europäische Cybersicherheit bündeln. Im Bereich Innovation & Uptake entscheiden die 27 EU-Mitgliedstaaten und die Europäische Kommission, zu welchen Teilen z. B. KI in der Cybersicherheit in den kommenden Jahren gefördert wird. In einzelnen Fällen kann das ECCC auch ein Vehikel für gemeinsame Beschaffungen von EU-Staaten sein. Das wird gerade zum ersten Mal im Bereich von grenzüberschreitenden SOC-Infrastrukturen umgesetzt. NCCs können ebenfalls EU-Mittel in nationalen Ausschreibungen verteilen, um die Beteiligung von etwa KMU an den kompetitiven Ausschreibungen zu erhöhen. Insgesamt fließen so bisher rund 100 Millionen EUR in die europäische Wirtschaft. In Österreich wird dieser Mechanismus mit dem Cybersecurity-Scheck der FFG für KMU pilotiert.

Neben der internationalen Zusammenarbeit unterstützt das NCC-AT auch nationale Stakeholder. Können Sie uns genauer erklären, wie diese Unterstützung aussieht?
Hanna Wilhelmer: Ich habe den Anspruch, den Zugang zu Informationen über bestehende Initiativen für nationale Stakeholder zu erhöhen. Das machen wir durch ein breites Informationsangebot inklusive einem eigenen Förderatlas zu Cybersicherheitsförderungen auf der Webseite des NCC-AT, Veranstaltungen für jene, die sich an Kompetenzaufbau rund um das ECCC informieren, sowie Beratungen für EU-Förderprogramme. Wir arbeiten aktuell auch an grenzüberschreitenden Matchmakings für Ausschreibungen im Digital Europe Programme Cybersicherheit.

Das NCC-AT ist Teil eines EU-weiten Netzwerks nationaler Koordinierungszentren. Wie profitieren österreichische Unternehmen und Forschungseinrichtungen von dieser Vernetzung auf europäischer Ebene?
Hanna Wilhelmer: Wir treffen uns regelmäßig als Netzwerk Nationaler Koordinierungszentren – zuletzt in Warschau im April. Aktuell werden die Angebote für die Community, wie etwa Match Makings, auf den Weg gebracht und Best Practices zur Erfahrung der NCCs mit dem Instrument der Kaskadenfinanzierung ausgetauscht. Insgesamt werden auf diesem Weg rund 100 Mio. EUR in Europa für Cybersicherheit für Betriebe ausgeschüttet. Aus dem Netzwerk heraus ist auch ein Projektantrag entstanden, an welchem mehrere NCCs selbst teilnehmen und mit dem Hersteller von Produkten mit digitalen Elementen auf den ab 2027 vollumfänglich geltenden Cyber Resilience Act – mit Informationen, aber auch finanzieller Unterstützung – vorbereitet werden. Für Österreich haben wir die Plattform Industrie 4.0 für das Konsortium SECURE vermitteln können.

Innovation ist ein entscheidender Faktor für den Erfolg im Bereich Cybersicherheit. Wie kann das

EU-Förderungen zielen auf strategische Autonomie gegenüber nordamerikanischen und asiatischen Märkten.

NCC-AT dazu beitragen, innovative Technologien und Ansätze in Österreich zu fördern?
Hanna Wilhelmer: Die momentane Förderlandschaft bietet bereits einige Chancen zur Erhöhung der Wettbewerbsfähigkeit von österreichischen Unternehmen. Für die Zukunft loten wir strategische Möglichkeiten aus und identifizieren Strukturen in Österreich und mögliche Lücken.

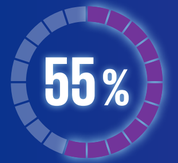
Unsere Studie zeigt außerdem, dass 62 Prozent der befragten Unternehmen besonders auf das Herkunftsland des Anbieters achten, wenn sie Cybersecurity-Lösungen beschaffen. Wie kann Österreich diesen Trend nutzen, um seine Position als vertrauenswürdiger Anbieter von Sicherheitslösungen weiter auszubauen?
Hanna Wilhelmer: Eine verstärkte Vernetzung der heimischen Forschung mit der Industrie in den Stärkefeldern ausbauen – etwa bei der Postquanten-Transition, Hardwaresicherheit, OT-Security, E-Identität und E-Government. Das steht auch in der Österreichischen Strategie für Cybersicherheit 2021. Den schon bestehenden Netzwerken zwischen Universitäten und Unternehmen kommt dabei eine Schlüsselrolle zu.

Was sind Ihrer Meinung nach die wichtigsten Erkenntnisse aus Ihrer Arbeit im Bereich Cybersicherheit?
Hanna Wilhelmer: Cybersicherheit ist ein Teamsport – europäische Zusammenarbeit sowie die Kooperation zwischen öffentlichem und privatem Sektor sind wesentlich.

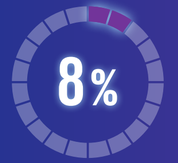
Wenn wir uns in einem Jahr wieder treffen, was würden wir uns dann wünschen, heute schon getan zu haben?
Hanna Wilhelmer: Ziel neun der Österreichischen Strategie für Cybersicherheit umgesetzt: In Österreich gibt es eine koordinierte und vernetzte Forschungs- und Entwicklungslandschaft im Bereich Cybersicherheit!

10 Ausblick

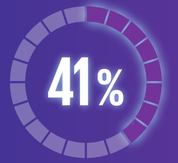
In welche Richtung bewegen sich heimische Unternehmen in der Zukunft und vor welchen technologischen Herausforderungen stehen sie? Was sind die Topthemen, mithilfe derer sie Cybersicherheit in den nächsten 12 Monaten adressieren wollen? Die Top 5 im Jahr 2025 zeigen ein eindeutiges Bild.



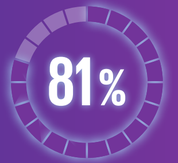
sagen, dass **Österreich nicht gut darauf vorbereitet** ist, auf schwerwiegende Cyberangriffe gegen die kritische Infrastruktur zu reagieren.



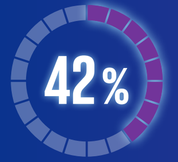
Der Rückgang von **Back-up und Recovery** liegt bei 8 %.



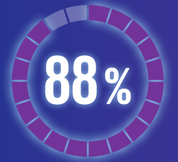
sagen, dass Cyberangriffe ihre **geschäftliche Existenz bedrohen.**



frustriert, dass es bei **Angriffen aus dem Ausland** nur wenig Chancen gibt, die Täter:innen zu identifizieren.

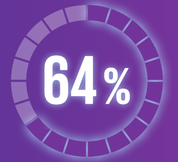


stimmen zu, dass es einer **Erweiterung der Befugnisse** bedarf, um Cyberangriffe aufzuklären.



sagen, dass es eine **verstärkte EU-weite Zusammenarbeit** beim Thema Cybersicherheit benötigt.

würden bevorzugt Security-Lösungen von **österreichischen Unternehmen** einsetzen – eine Zunahme um 23 % gegenüber dem Vorjahr.



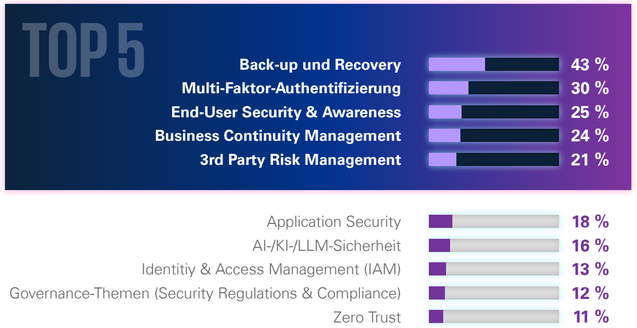
sagen, dass die **heimische Politik** im internationalen Vergleich das Thema Cybersecurity vernachlässigt.

Technologien & Themen – Top 5

Die Analyse der Umfrageergebnisse zu den Top 5 Cybersecurity-Themen des Jahres 2025 und deren Veränderungen im Vergleich zu 2024 zeigt eine interessante Verschiebung in den Prioritäten von Unternehmen. Diese Trends spiegeln die sich wandelnde Bedrohungslandschaft wider und verdeutlichen die strategischen Anpassungen, die nötig sind, um den immer komplexeren Herausforderungen im Cybersecurity-Bereich zu begegnen.

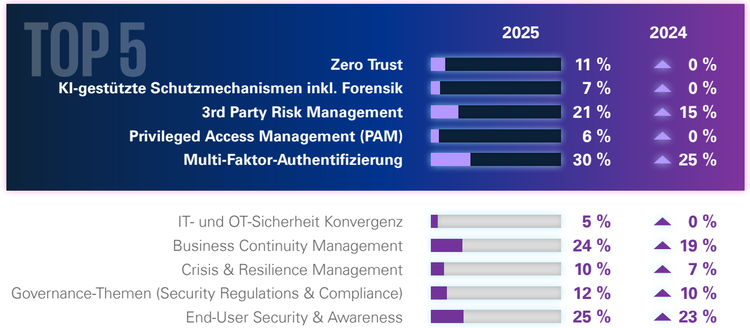
Back-up und Recovery bleibt das wichtigste Thema für Unternehmen, obwohl ein Rückgang um 8 Prozent gegenüber dem Vorjahr zu verzeichnen ist. Dies zeigt, dass Unternehmen weiterhin auf die Sicherung ihrer Daten setzen, insbesondere angesichts der anhaltenden Bedrohung durch Ransomware-Angriffe. Ransomware bleibt eine der lukrativsten Angriffsmethoden für Cyberkriminelle, da sie Unternehmen dazu zwingt, hohe Lösegeldzahlungen zu leisten, um den Zugriff auf ihre Daten wiederherzustellen. Der Rückgang im Vergleich zum Vorjahr könnte darauf hindeuten, dass Unternehmen verstärkt auf fortschrittlichere Technologien wie Immutable Back-ups oder cloudbasierte Disaster-Recovery-Lösungen setzen. Diese bieten eine höhere Widerstandsfähigkeit gegen Angriffe. Auch könnte es darauf hinweisen, dass Unternehmen stärker in präventive Maßnahmen wie Zero Trust oder Incident-Response-Management investieren.

Abb. 32: Die Top 10 nach technologischer Bedeutung



Die Multi-Faktor-Authentifizierung (MFA) hat gegenüber 2024 eine Zunahme von 5 Prozent erfahren und ist nun das zweitwichtigste Thema. Es ist durchaus überraschend, dass sich ein technologisches Thema unter den Top 5 befindet. 30 Prozent der befragten Unternehmen wollen in den nächsten 12 Monaten diesen Aspekt adressieren bzw. finden ihn wichtig. Multi-Faktor-Authentifizierung kann wesentlich zur Verbesserung der Cybersicherheit beitragen. Angriffe auf Identitäten und Benutzer:innenzugänge haben in den letzten 12 Monaten massiv zugenommen. Es ist immer noch das leichteste Einfallstor, über Phishingattacken Informationen zu stehlen und so Datenaccounts bzw. Zugangsinformationen zu kompromittieren. Multifaktor kann hier eine wesentliche Abhilfe schaffen. Die Zunahme von MFA spiegelt eine Bedrohung durch Angriffe auf digitale Identitäten wider, insbesondere durch Credential Stuffing und Phishingkampagnen. MFA bietet eine zusätzliche Sicherheitsebene, die es Angreifer:innen erschwert, Zugang zu sensiblen Systemen zu erhalten, selbst wenn sie Zugangsdaten kompromittieren können. Die steigende Popularität von MFA könnte auch durch regulatorische Anforderungen wie die DSGVO oder NIS-2 bedingt sein, die Unternehmen dazu zwingen, ihre Authentifizierungsmechanismen zu stärken.

Abb. 33 Die Top 10 Zunahmen nach technologischer Bedeutung



End-User Security & Awareness hat ebenfalls einen leichten Anstieg von 2 Prozent verzeichnet. Unternehmen erkennen, dass der Mensch oft das schwächste Glied in der Sicherheitskette ist. Phishingangriffe und Social Engineering bleiben eine der häufigsten Methoden für Angreifer:innen, um Zugang zu Netzwerken zu erhalten. Schulungen zur Sensibilisierung von Mitarbeiter:innen sind daher entscheidend, um diese Bedrohungen zu minimieren. Der Fokus auf End-User Awareness könnte auch durch die zunehmende Verbreitung hybrider Arbeitsmodelle bedingt sein, da diese potenziell anfälliger für Sicherheitsrisiken sind. Die sich ständig verändernden Angriffe durch KI, Desinformationskampagnen oder Deepfakes führen dazu, dass das Bewusstsein der Mitarbeitenden laufend gesteigert werden muss. Allerdings ist mit der Geschwindigkeit, mit der sich das Umfeld verändert, kaum Schritt zu halten, um hier entsprechende Maßnahmen zur Prävention zu treffen.

Business Continuity Management hat mit einem Anstieg von 5 Prozent gegenüber dem Vorjahr (2024: 19 Prozent) an Bedeutung gewonnen. Das Sicherstellen der Geschäftsprozesse wird einerseits über die Regulatorik (DORA, NIS-2) gefordert, um die Resilienz für kritische Einrichtungen zu gewährleisten. Andererseits ist es aber auch alternativlos, sich nicht darum zu kümmern, denn das Funktionieren digitaler Systeme bzw. Infrastrukturen und Dienste ist eine Grundvoraussetzung dafür, dass Unternehmen erfolgreich sein können. Business Continuity Management ist eine der wesentlichen und tragenden Säulen, wenn es bei Sicherheitsvorfällen darum geht, die Kontinuität der Geschäftsprozesse – sei es auch nur eingeschränkt – aufrechtzuerhalten.

Die Zunahme zeigt, dass Unternehmen verstärkt auf die Sicherstellung ihrer Betriebsabläufe im Falle eines Cyberangriffs oder einer anderen Krise setzen. Auch könnte die Zunahme auf die vermehrten Fälle gezielter Angriffe auf kritische Infrastrukturen oder Lieferketten zurückzuführen sein. Angreifer:innen nutzen zunehmend Schwachstellen in IT-Systemen aus, um Betriebsunterbrechungen zu verursachen und Unternehmen unter Druck zu setzen. Business Continuity Management umfasst nicht nur technische Lösungen wie redundante Systeme und Notfallpläne, sondern auch organisatorische Maßnahmen zur schnellen Wiederherstellung des Geschäftsbetriebs.

3rd Party Risk Management ist um 6 Prozent im Vergleich zum Vorjahr angestiegen. Das ist eine direkte Reaktion auf die wachsende Gefahr von Angriffen auf die Lieferkette. Vorfälle wie der SolarWinds-Angriff oder Schwachstellen in Open-Source-Komponenten haben gezeigt, wie verheerend solche

Angriffe sein können. Unternehmen investieren daher verstärkt in Maßnahmen zur Bewertung und Absicherung ihrer Partnernetzwerke sowie in die kontinuierliche Überwachung externer Risiken.

In der aktuellen Cybersecurity-Landschaft gewinnen verschiedene Technologien und Strategien an Bedeutung. Unternehmen setzen verstärkt auf Cyber Security Task Forces, Fraud Intelligence, KI-Sicherheit, SIEM, SOAR oder Schwachstellenmanagement für die kontinuierliche Überwachung. Weitere Themen, mit denen sich Unternehmen beschäftigen, sind unter anderem Zero Trust, Mobile Device Management und Quantum Security, die ebenfalls als wichtige Technologien angeführt werden. Auch die Einführung von SOC-Services und die Verbesserung der OT-Security sind zentrale Maßnahmen. Schulungen und Weiterbildungsprogramme sind entscheidend, um das Sicherheitsbewusstsein der Mitarbeiter:innen zu erhöhen. Weitere relevante Technologien, die im Fokus der Unternehmen stehen, sind Cloud-Access-Security-Broker-Lösungen, Pentests und Red Teaming Exercises. Insgesamt zeigt sich, dass Unternehmen eine breite Palette von Technologien und Strategien einsetzen, um ihre Cybersecurity zu stärken und sich gegen die wachsenden Bedrohungen zu wappnen.

Veränderungen gegenüber 2024 – die größten Zunahmen

Zero Trust hat mit einem Anstieg von 11 Prozent den größten Zuwachs unter allen Themen erfahren. Dieses Sicherheitsmodell stuft jeden Zugriff standardmäßig als potenziell unsicher ein und erteilt erst nach erfolgreicher Authentifizierung und Autorisierung eine Freigabe. Der Anstieg von Zero Trust unter den Umfrageteilnehmer:innen unterstreicht die wachsende Anerkennung dieses Ansatzes als effektive Antwort auf moderne Bedrohungen. Zero Trust ist besonders relevant in hybriden IT-Umgebungen mit Cloud-Diensten und Remote-Arbeitsmodellen.

KI-gestützte Schutzmechanismen haben 7 Prozent hinzugewonnen. KI wird zunehmend eingesetzt, um Angriffsmuster frühzeitig zu erkennen, automatisierte Reaktionen auszulösen und forensische Analysen durchzuführen. Angreifer:innen hingegen nutzen KI für Deepfakes oder zur Automatisierung von Angriffen, was den Bedarf an KI-basierten Verteidigungsmaßnahmen erhöht.

Privileged Access Management (PAM) ist um 6 Prozent im Vergleich zum Vorjahr angestiegen. Kompromittierte privilegierte Konten sind oft Einstiegspunkt für groß angelegte Angriffe. PAM-Lösungen helfen dabei, privilegierte Zugänge besser zu kontrollieren und Missbrauch zu verhindern – ein wichtiger Schritt zur Minimierung des Schadenspotenzials bei Insider-Bedrohungen oder externen Angriffen.

Veränderungen gegenüber 2024 – die größten Rückgänge

Der Rückgang bei Back-up und Recovery um 8 Prozent könnte darauf hindeuten, dass Unternehmen ihre Strategien diversifizieren oder sich stärker auf präventive Ansätze konzentrieren. Neue Technologien wie Immutable Back-ups könnten dazu führen, dass traditionelle Back-up-Methoden weniger priorisiert werden.

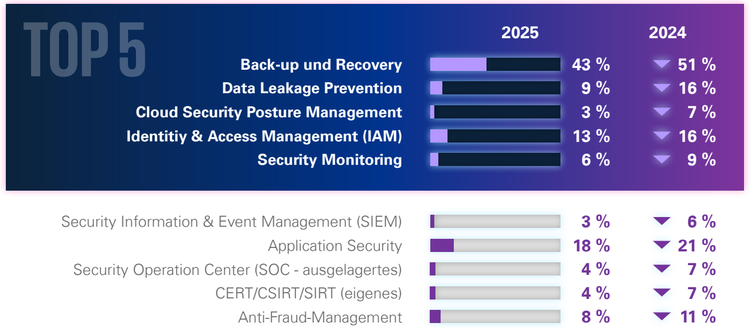
Data Leakage Prevention verzeichnet einen 7-prozentigen Rückgang. Möglicherweise bevorzugen Unternehmen umfassendere Ansätze wie Zero Trust oder sie verlagern ihre Investitionen stärker auf Privileged Access Management.

Der Rückgang bei Cloud Security Posture Management (-4 Prozent) ist möglicherweise ein Zeichen dafür, dass Unternehmen ihre Cloud-Sicherheitsstrategien konsolidieren oder neue Ansätze implementieren.

Die Rückgänge bei Security Monitoring sowie Application Security (jeweils -3 Prozent) könnten eine Verschiebung hin zu automatisierten Lösungen wie KI-gestützten Mechanismen oder eine verstärkte Integration von Sicherheitsmaßnahmen direkt in Entwicklungsprozesse bedeuten.

Die Ergebnisse der Umfrage zeigen eine klare Verschiebung hin zu Themen wie Zero Trust und KI-gestützten Schutzmechanismen sowie einen stärkeren Fokus auf Resilienzstrategien wie Business Continuity Management und 3rd Party Risk Management. Das spiegelt auch aktuelle Bedrohungstrends wider und verdeutlicht die Notwendigkeit innovativer Ansätze zur Abwehr moderner Cyberangriffe. Gleichzeitig deuten einige Rückgänge darauf hin, dass traditionelle Sicherheitsmaßnahmen durch spezialisierte oder automatisierte Lösungen ergänzt bzw. ersetzt werden. Die Entwicklungen bestätigen den zunehmenden Druck auf Unternehmen, ihre Sicherheitsstrategien kontinuierlich anzupassen und weiterzuentwickeln.

Abb. 34: Die Top 10 Abnahmen nach technologischer Bedeutung



Mangelnde Ressourcen

Welche Sicherheitsmaßnahmen halten die Befragten in ihrem Unternehmen für notwendig, haben aber keine Ressourcen (Personal, Geld, Zeit) dafür? Als Antwort auf diese Frage wurden u. a. eine Cybersecurity-Taskforce, die kontinuierliche Überwachung durch Systeme wie Security Information and Event Management (SIEM) und die Einrichtung eines Security Operations Center (SOC) genannt. Auch die Einführung von Security Orchestration, Automation, and Response (SOAR) und die Verbesserung der OT-Security werden als wichtige Sicherheitsmaßnahmen angesehen, für die allerdings mehr Ressourcen benötigt werden würden. Auch wünschen sich die Befragten Schulungen zur Sensibilisierung der Mitarbeiter:innen, insbesondere im Umgang mit Phishing, Malware und KI. Notfallübungen, um die Reaktionsfähigkeit bei Sicherheitsvorfällen zu verbessern, sind ebenso gewünscht.

Vulnerability Management, Datenklassifizierung und Verschlüsselung sowie die Einführung von Data Loss Prevention (DLP) und Cloud-Security-Lösungen werden ebenfalls als notwendig erachtet. Weiters wurde die Einführung von Zero-Trust-Architekturen, die Verbesserung des Risiko-Managements und der Business-Impact-Analysen genannt. Die Modernisierung der IT-Infrastruktur und das Ersetzen von End-of-Life-Systemen werden zusätzlich als wichtige Sicherheitsmaßnahmen angesehen, für die es allerdings an Ressourcen mangelt.

Emotionale Bedeutung von Cybersecurity durch geopolitische Konflikte

In einem geopolitisch angespannten Umfeld wirken sich internationale Konflikte auch auf die Unternehmen aus und bewirken eine Veränderung der Wahrnehmung von Cybersecurity. So hat sich für die Hälfte der befragten Unternehmen (50 Prozent) die Bedeutung von Cybersicherheit durch aktuelle geopolitische Konflikte besonders stark verändert. Vor allem im internationalen Wettbewerb kennen Bedrohungen im Cyberumfeld, die

durch geopolitische Konflikte ausgelöst werden, keine Grenzen. Diese Zustimmung verdeutlicht, dass bei der Hälfte der befragten Unternehmen Cyberbedrohungen 2025 emotional stärker wahrgenommen werden als in früheren Jahren. Das geht einher mit dem Anstieg staatlich geförderter Cyberoperationen.

Die vergleichsweise geringe Ablehnung (16 Prozent) verdeutlicht einen Widerspruch: Während auf Führungsebenen Cyberrisiken zunehmend als strategisches Problem eingestuft werden, mangelt es in der operativen Umsetzung oft an Ressourcen, um diese Einschätzung in konkrete Schutzmaßnahmen zu übersetzen.

Nur 5 Prozent haben angegeben, dass ihnen nicht bekannt ist, ob sich die Bedeutung von Cybersicherheit durch aktuelle geopolitische Konflikte verändert hat. Diese Thematik scheint demnach flächendeckend in der Realität der Unternehmen angekommen zu sein.

Cyberangriffe als Bedrohung für die geschäftliche Existenz

41 Prozent der Befragten erkennen die existenzielle Dimension von Cyberangriffen – sie sind der Meinung, dass Cyberangriffe ihre geschäftliche Existenz bedrohen. Das verdeutlicht einmal mehr die zunehmende Professionalisierung der Angreifer:innen.

> **Weitsicht, Innovation und Entschlossenheit gestalten die Cybersicherheit der Zukunft.**

30 Prozent sehen hingegen keine Auswirkungen auf ihre unternehmerische Existenz. Gerade kleinere Unternehmen unterschätzen hier ihre Verwundbarkeit.

Nur 3 Prozent der Umfrageteilnehmer:innen wissen nicht, ob Cyberangriffe ihre geschäftliche Existenz bedrohen. Somit ist das Thema bei nahezu allen Unternehmen präsent – unabhängig von ihrer tatsächlichen Risikobewältigungskompetenz. Die existenziellen Auswirkungen von Cyberangriffen werden uns auch durch die mediale Berichterstattung und aktuelle Anlassfälle immer mehr vor Augen geführt. Die Zahlen unterstreichen, dass das Bewusstsein für die Bedeutung von Cyberangriffen für Unternehmen einen immer wichtigeren Stellenwert in ihrer Risikobeurteilung einnimmt.

Mangelnde Identifizierbarkeit ausländischer Angreifer:innen

Gerade wenn es um das Auffinden der Täter:innen geht – um vor allem auch ein Exempel statuieren und weitere Angriffe eindämmen zu können – herrscht gewisser Unmut und Ernüchterung bei heimischen Unternehmen.

Die große Zustimmung (81 Prozent) jener Befragten, die es frustrierend finden, dass es bei Angriffen aus dem Ausland nur wenig Chancen gibt, die Täter:innen zu identifizieren, unterstreicht ein Kernproblem der modernen Cybersicherheit: Trotz Fortschritten in der KI-gestützten Bedrohungsjagd gelingt die Zuordnung von Angriffen nur selten. Es herrscht eine grundlegende Frustration bei heimischen Unternehmen. Gründe hierfür sind insbesondere Taktiken wie die Nutzung von TOR-Netzwerken, die Verschleierung der Herkunft durch Proxyserver in Drittstaaten oder die Imitation bekannter Angreifer-Tools.

Bemerkenswert ist auch, dass nur 3 Prozent der Befragten dieser Frage nicht zustimmen. Selbst ansonsten skeptische Unternehmen scheinen die Komplexität der Identifizierung anzuerkennen. 13 Prozent stehen der Frage neutral gegenüber. Eventuell halten diese Befragten die Identifizierung der Täter:innen für strategisch nachrangig. Hier sei jedoch festgehalten, dass gezielte Gegenmaßnahmen wie die Ausübung von diplomatischem Druck oder die Verhängung von Sanktionen ohne eine Identifikation der Angreifer:innen nicht möglich sind.

Zusammengefasst kann festgehalten werden, dass es hier einen klaren Appell an die zuständigen Stellen und Behörden gibt, auf internationaler Ebene Handlungen zu setzen, um die Täter:innengruppen zu identifizieren und hier auch im Zuge der Ermittlungstätigkeiten und des Strafvollzugs einen wirksamen Beitrag leisten zu können.

Erweiterung der Ermittlungsbefugnisse der Behörden

Damit aber genau das passieren kann und Chancen bestehen, die Täter:innengruppen zu identifizieren, benötigt es entsprechende Ermittlungsbefugnisse bzw. Möglichkeiten für die Behörden. Es herrscht eine gewisse Ambivalenz, wenn es darum geht, wie viele Einblickmöglichkeiten durch die ermittelnden Behörden gegeben sein sollten.

42 Prozent stimmen zu, dass es einer Erweiterung der (technischen) Möglichkeiten und Befugnisse (z. B. Staatstrojaner) bedarf, damit Cyberangriffe aufgeklärt werden können. Gründe hierfür könnten z. B. Ransomware-Attacken auf Krankenhäuser oder Energieversorger sein, die proaktive Ermittlungsinstrumente für die Zustimmenden legitimieren.

Rund ein Drittel der befragten Unternehmen ist der Meinung, dass keine Erweiterung der Befugnisse nötig ist. Bedenken diesbezüglich könnten eine schleichende Ausweitung staatlicher Überwachung oder auch die Schwächung von Verschlüsselungsstandards sein. Interessant ist hierbei, dass jene Personen, die angegeben haben, dass es keine Erweiterung der Befugnisse benötigt, überwiegend zustimmen, dass es frustrierend ist, dass es keine Chancen gibt, Täter:innengruppen aus dem Ausland zu identifizieren. Das ist ein klarer Aufruf dazu, noch mehr Transparenz bzgl. der Befugnisse und der damit verbundenen Funktionen des Rechtsstaates herzustellen. Auch die Rolle des Rechtsschutzbeauftragten, der über die Angemessenheit der Maßnahmen in der Durchführung dieser Tätigkeiten entscheidet, muss klarer kommuniziert und transparenter gemacht werden. Gerade im digitalen Raum ist es unerlässlich, wirksame Mittel zur Verfügung zu haben, die bei Gefahr im Verzug die Möglichkeit bieten, die Zivilgesellschaft vor Angreifer:innen zu schützen.

Diese Ambivalenz aus 42 Prozent Zustimmung und 32 Prozent Ablehnung bildet die grundlegende Hürde zwischen Sicherheitserfordernissen auf der einen Seite und Datenschutzprinzipien auf der anderen Seite ab.

23 Prozent der Befragten stehen dieser Thematik neutral gegenüber. Es könnte sein, dass sie sich nicht in diesem Spannungsfeld positionieren wollen.

EU-weite Zusammenarbeit bei Cybersicherheit

Neben den technischen Maßnahmen und Möglichkeiten, um Cyberangriffe aufzuklären, ist ein Informationsfluss innerhalb der EU-Mitgliedstaaten essenziell. Der Konsens von 88 Prozent der Befragten, die der Meinung sind, dass es eine verstärkte EU-weite Zusammenarbeit beim Thema Cybersicherheit benötigt, gleicht einem Paradigmenwechsel: Alleingänge von Nationalstaaten verlieren vor dem Hintergrund transnationaler Bedrohungen wie Ransomware-as-a-Service oder staatlich geförderten APT-Gruppen zunehmend an Relevanz. Das sehen wir auch an der Unterstützung für den EU Cyber Resilience Act.

Die geringe Ablehnung von 2 Prozent ist ein klares Signal: Selbst eher EU-skeptische Unternehmen befürworten gemeinsame Cybersicherheitsstandards.

Gerade im Bereich der Regulatorik zur Verbesserung der Cybersicherheit sind entsprechende Schritte schon gesetzt. Allerdings benötigt es speziell für Unternehmen und für betroffene Einrichtungen, die z. B. für die kritische Infrastruktur verantwortlich sind, einen verbesserten Austausch und schnelleren Informationsfluss. Das kann nur dann passieren, wenn innerhalb der Europäischen

Union die Daten auf raschem Weg zwischen den Betroffenen ausgetauscht werden. NIS-2 sieht hier entsprechende Gremien für ein europaweites Krisenmanagement vor – wiewohl Krisenmanagement an sich aber nur die letzte Ausbaustufe der Eskalation sein kann.

Präferenz für österreichische Security-Lösungen

Neben der Möglichkeit der Überwachung der Kommunikation von Cyberkriminellen durch den Staat sind auch die Überwachung des eigenen Netzwerks und der Schutz der eigenen Infrastruktur durch die Unternehmen selbst wesentliche Bausteine. Aktuell existiert eine sehr hohe Abhängigkeit von Herstellern außerhalb der Europäischen Union. Genau diese Abhängigkeit gilt es einzudämmen, um technologisch wieder Souveränität im Bereich der Cybersicherheitsmaßnahmen und -lösungen zu erlangen. So ist es durchaus begrüßenswert, dass 60 Prozent der befragten Unternehmen (im Vergleich zum Vorjahr: 37 Prozent) bevorzugt Security-Lösungen von österreichischen Unternehmen einsetzen würden.

Diese klare Zustimmung ist auch darauf zurückzuführen, dass geopolitische Risiken und regulatorische Anforderungen (z. B. DSGVO, NIS-2) lokale Anbieter begünstigen. Unternehmen versprechen sich von „Made in Austria"-Lösungen schnellere Reaktionszeiten bei Incidents, verbesserte Compliance-Sicherheit und geringere Abhängigkeiten von US-amerikanischen Cloud-Diensten oder Cloud-Diensten aus China.

An dieser Stelle ist – wie auch in den Jahren zuvor – ein eindringlicher Appell angebracht, dass es einen Markt für Sicherheitslösungen aus Österreich braucht und diese mit zielgerichteten Maßnahmen unterstützt werden müssen. Im Sinne der Autarkie ist das wesentlich, damit die technologische Souveränität und der Schutz der kritischen Einrichtungen unabhängig von internationalen Herstellern gewährleistet sind. Natürlich ist es ein Irrglaube, dass man ausschließlich österreichische Lösungen einsetzen kann, denn die Vernetzung und die Abhängigkeiten untereinander sind durch die Entwicklungen der letzten Jahre schlichtweg nicht auflösbar. Dennoch besteht jetzt die Chance, in Zeiten geopolitischer Veränderungen und einer Verschiebung der Werte, dieses Momentum aufzugreifen und mit eigenen Maßnahmen und Initiativen als Vorbild voranzugehen.

Förderung durch die Politik

Diese Vorbildfunktion kann vor allem dann erreicht werden, wenn Unternehmen auch seitens der Entscheidungsträger, der Politik und anderer Interessenvertreter gezielt unterstützt werden. Diese Unterstützungen können mannigfaltig sein. Mit 69 Prozent Zustimmung, dass heimische Cybersecurity-Unternehmen von der Politik gezielt gefördert werden sollten, wird auch der Wunsch nach staatlicher Unterstützung für lokale Anbieter deutlich. Cybersicherheit wird als strategische Schlüsselindustrie wahrgenommen. Unternehmen erwarten sich Förderungen bei Post-Quanten-Kryptografie, KI-gestützter Angriffserkennung und Talententwicklung, um den Fachkräftemangel zu bekämpfen.

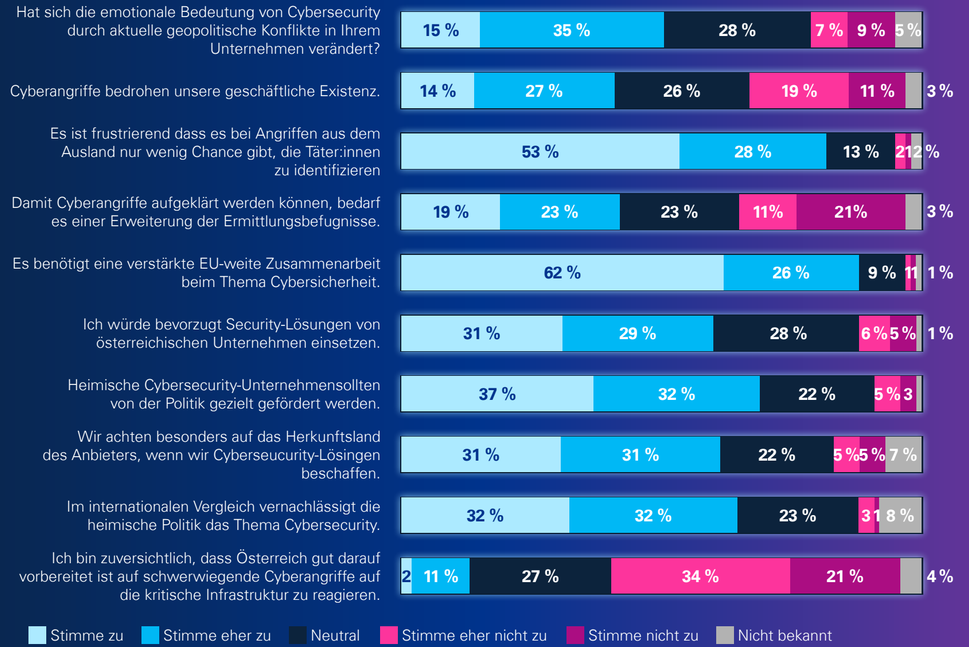
Herkunftsland als Beschaffungskriterium

Die Beschaffung von Cybersecurity-Lösungen fordert eine gewisse Verbundenheit mit dem jeweiligen Wirtschaftsraum und Staat. Andererseits gibt es technologische Abhängigkeiten, die mit dem Kauf diverser Security-Lösungen einhergehen. Dabei entstehen auch Risiken, wenn bspw. Hersteller aus Drittländern Security-Lösungen mit zusätzlichen Funktionen versehen, von denen niemand Kenntnis hat (man denke dabei z. B. an Überwachung). 62 Prozent der befragten Unternehmen achten bereits jetzt besonders darauf, aus welchem Herkunftsland die Anbieter kommen, wenn sie Cybersecurity-Lösungen beschaffen. Das unterstreicht einmal mehr die wachsende Bedeutung geopolitischer Risikobewertung in der Supply-Chain-Sicherheit. Inländische oder EU-basierte Anbieter werden bevorzugt, um so Abhängigkeiten von Ländern mit umstrittenen Überwachungsgesetzen zu minimieren.

Wahrgenommene politische Vernachlässigung von Cybersecurity

Einerseits besteht bei Unternehmen der explizite

Abb. 35: Stimmungsbild zur Cybersecurity-Lage



Wunsch, dass die Politik heimische Cybersecurity-Unternehmen stärker fördert, auf der anderen Seite herrscht eine gewisse Form der Ernüchterung. 64 Prozent meinen, dass die heimische Politik im internationalen Vergleich das Thema Cybersecurity vernachlässigt.

Im aktuellen Regierungsprogramm finden wir im Vergleich zum vorherigen Regierungsprogramm viel mehr Punkte, die das Thema Cybersecurity berücksichtigen. Diese Ankündigungen sind zumindest ein positiver Schritt dahingehend, dass dem Thema mehr Bedeutung zukommt. Im Vergleich zum Regierungsprogramm 2020 bis 2024 wurden neue wesentliche Aspekte mitaufgegriffen. Diese sind auch eine Reaktion auf die sich verändernden Bedrohungen und Herausforderungen im Rahmen einer veränderten geopolitischen Weltordnung. Die entsprechenden Stellen innerhalb der öffentlichen Verwaltung, insbesondere die Landesverteidigung und das Innenministerium, sind hier besonders gefordert. Allerdings muss auch, wenn es um die Steigerung der Bedeutung des Themas für die Unternehmen und für die Zivilgesellschaft geht, viel mehr Bewusstsein durch die öffentliche Verwaltung und die Politik in Form von gezielter Kommunikation geschaffen werden. Vergleichen wir dazu die Themen Desinformation und Fake News, so haben es diese Themen relativ schnell in die Medien geschafft.

Zuversicht in Österreichs Krisenresilienz
Diese Wahrnehmung ist eine logische Konsequenz daraus, dass es mit dem Schutz der kritischen Infrastruktur nicht immer so gut bestellt zu sein scheint.

Wir stehen vor einer Vertrauenskrise in die österreichische Cyberabwehr: 55 Prozent der befragten Unternehmen sind nicht zuversichtlich, dass Österreich gut darauf vorbereitet ist, auf schwerwiegende Cyberangriffe gegen kritische Infrastrukturen zu reagieren. Nur 13 Prozent zeigen sich (sehr) zuversichtlich, dass hier ein hinreichender Schutz gegeben ist.

Es gilt also, Vertrauen bei der Bevölkerung zu etablieren. Die Zahlen sind ein klarer Aufruf zur Verbesserung der Cybersicherheit unserer kritischen Infrastruktur.

Cybersecurity-Arbeitsgruppen
Wichtige Aspekte, die dazu beitragen können, den Schutz zu verbessern, sind der regelmäßige Austausch und regelmäßige Veranstaltungen, die das Bewusstsein auf allen Ebenen – sei es bei Verwaltung, Politik oder Unternehmen – stärken. So geben 38 Prozent der Befragten an, dass Arbeitsgruppen, wie jene zu den NIS-2-Risikomanagementmaßnahmen der Cyber Sicherheit Plattform (CSP) oder des Rechts- und Technologiedialogs (RTD) des Kompetenzzentrum Sicheres Österreich (KSÖ), den aktiven Dialog zwischen öffentlicher Verwaltung und Unternehmen fördern.

Zusammenführung der strategischen Herausforderungen
Die Studienergebnisse offenbaren mehrere Konfliktherde in der heimischen Cybersecuritylandschaft: Wir sehen, dass Unternehmen nationale Souveränität und lokale Lösungen befürworten. Gleichzeitig gehen Cyberangriffe zunehmend über Ländergrenzen hinaus, was eine vertiefte EU-weite und globale Zusammenarbeit notwendig macht. Bemerkbar macht sich das beispielsweise im Wunsch nach politischer Förderung heimischer Anbieter (69 Prozent) auf der einen Seite sowie der gleichzeitigen Forderung einer EU-weiten Zusammenarbeit (88 Prozent) auf der anderen Seite.

Parallel dazu finden wir auch Widersprüchlichkeiten beim hohen Problembewusstsein heimischer Unternehmen (z. B. sind 81 Prozent frustriert über die mangelnde Identifizierung der Täter:innen) und einer gleichzeitig geringen Zuversicht in die nationale Resilienz (13 Prozent). Lösen lassen sich diese Herausforderungen nur mithilfe eines ganzheitlichen Ansatzes, der sowohl technologische als auch regulatorische sowie länderübergreifende Aspekte berücksichtigt.

Was Sie sich aus diesem Kapitel mitnehmen sollten

1. Die Prioritäten der Unternehmen haben sich verschoben, wie ein Vorjahresvergleich der Top 5 Cybersecurity-Themen zeigt. Diese Trends spiegeln die sich wandelnde Bedrohungslandschaft wider und verdeutlichen die strategischen Anpassungen, die nötig sind, um den immer komplexeren Herausforderungen im Cybersecurity-Bereich zu begegnen.

2. Vor allem im internationalen Wettbewerb kennen Bedrohungen im Cyberumfeld, die durch geopolitische Konflikte ausgelöst werden, keine Grenzen. Die Hälfte der befragten Unternehmen nimmt Cyberbedrohungen 2025 emotional stärker wahr als in früheren Jahren.

3. Aktuell existiert eine sehr hohe Abhängigkeit von Herstellern außerhalb der Europäischen Union. Genau diese Abhängigkeit gilt es einzudämmen, um technologisch wieder Souveränität im Bereich der Cybersicherheitsmaßnahmen und -lösungen zu erlangen. Jetzt besteht die Chance, in Zeiten geopolitischer Veränderungen und einer Verschiebung der Werte, dieses Momentum aufzugreifen und mit eigenen Maßnahmen und Initiativen als Vorbild voranzugehen.

Quantenfit: Wie wir uns auf die Zukunft der Technologie vorbereiten

Quantencomputing verspricht, die Cybersicherheit, Finanzwelt und Gesellschaft zu revolutionieren. **Christoph Striecks** vom AIT Austrian Institute of Technology beleuchtet die Chancen und Herausforderungen dieser Technologie. Er erläutert, wie wir uns auf eine quantensichere Zukunft vorbereiten können und welche Schritte erforderlich sind, um die Vorteile dieser Technologie zu nutzen.

Könnten Sie uns mehr über Ihre Arbeit im Bereich Kommunikation und Kryptographie erzählen? Was ist Ihr akademischer Werdegang und welche Rolle spielt die quantensichere Kommunikation in Ihrer aktuellen Forschung am AIT?
Christoph Striecks: Meine Schwerpunkte liegen in der sicheren Kommunikation und Kryptographie. In letzter Zeit konzentriere ich mich besonders auf hybride Schlüsselaustauschverfahren und langfristige Sicherheit. Vor meinem Eintritt beim AIT im Jahr 2016 war ich Postdoc am Karlsruher Institute of Technology in Deutschland, wo ich 2015 meinen Doktor in Kryptographie erhielt. Mein Informatik-Diplom mit den Schwerpunkten Kryptographie und Software-Engineering habe ich 2010 an der TU Braunschweig gemacht. Ich beschäftige mich schon lange mit Kryptographie und sicherer Kommunikation und veröffentliche regelmäßig auf renommierten Konferenzen wie CRYPTO und EUROCRYPT. Aktuell arbeiten wir in der Kryptographie-Gruppe am AIT intensiv an quantensicherer Kommunikation.

Quantencomputing und Quantentechnologie rücken zunehmend in den Fokus der Öffentlichkeit und beeinflussen unseren Alltag. Aber was steckt eigentlich hinter dieser Technologie, die oft als revolutionär beschrieben wird und das Potenzial hat, viele Bereiche zu verändern? Könnten Sie uns eine kurze Einführung in die Grundlagen von Quantencomputern geben und erklären, wie sie sich vom klassischen Computing unterscheiden?
Christoph Striecks: Quantencomputer basieren auf den Prinzipien der Quantenmechanik, um Informationen zu verarbeiten, im Gegensatz zu klassischen Computern. Sie nutzen die Eigenschaft der Superposition, wodurch sie bestimmte Probleme viel schneller lösen können. Quantencomputer haben das Potenzial, viele Bereiche zu revolutionieren, da sie Probleme bewältigen, die für klassische Computer schwer oder ineffizient zu lösen sind. Allerdings gibt es noch bedeutende technologische Herausforderungen, insbesondere hinsichtlich der Fehleranfälligkeit und Skalierbarkeit von Quantensystemen.

> **Unternehmen sollten sofort mit quantensicherer Kryptographie und einem Migrationsplan ihre Daten schützen.**

Könnten Sie uns näher erläutern, was Superposition und Qubits sind und welche Rolle sie in Quantencomputern spielen? Gibt es eine einfache Art, diese Konzepte zu veranschaulichen?
Christoph Striecks: Im Gegensatz zu klassischen Computern, die mit Bits arbeiten, die entweder den Wert 0 oder 1 haben (Strom aus oder Strom an), nutzen Quantencomputer sogenannte Qubits. Diese Qubits können gleichzeitig den Wert 0 und 1 annehmen, dank der Eigenschaft der Superposition. Dadurch können Quantencomputer viele Berechnungen gleichzeitig durchführen, was zu einer

FOTO © AITZINNER

Erfahren Sie mehr in unserem Podcast IMPULSE

Dr. Christoph Striecks ist Senior Scientist am AIT Austrian Institute of Technology, spezialisiert auf sichere Kommunikation und Kryptographie, insbesondere hybride Schlüsselaustauschverfahren und langfristige Sicherheit. Vor seinem Eintritt beim AIT im Jahr 2016 war er Postdoc am Karlsruher Institute of Technology (KIT), wo er 2015 seinen PhD in Kryptographie erhielt. Sein Diplom in Informatik erlangte er 2010 an der Technischen Universität Braunschweig mit den Schwerpunkten Kryptographie und Software-Engineering. Christoph Striecks hat zahlreiche Publikationen im Rahmen von renommierten Konferenzen wie CRYPTO und EUROCRYPT veröffentlicht.

erheblichen Steigerung der Rechenleistung führt. Bildlich gesprochen, kann man sich ein Bit wie eine Münze vorstellen, die entweder Kopf (0) oder Zahl (1) zeigt. Ein Qubit hingegen ist wie eine sich drehende Münze, die gleichzeitig alle Zustände zwischen 0 und 1 annehmen kann. Diese „überlagerten" Zustände ermöglichen es Quantencomputern, viel effizienter zu arbeiten

Im Bereich der Quantentechnologie, insbesondere beim Quantencomputing, hören wir oft vom „Q Day". Warum wird dieser Tag als bedeutende Bedrohung für die Cybersicherheit angesehen, und welche Auswirkungen könnte er auf die digitale Sicherheit haben?
Christoph Striecks: Der Begriff „Q Day" stammt aus der Cybersicherheit und bezeichnet den Zeitpunkt, an dem Quantencomputer in der Lage sein werden, die derzeit verwendeten Verschlüsselungsmethoden zu knacken. Dies stellt eine erhebliche Bedrohung dar, da viele aktuelle Verschlüsselungsverfahren auf mathematischen Problemen basieren, die für Quantencomputer leicht lösbar sind, während sie für klassische Computer schwer zu bewältigen sind. Kryptographie ist essenziell für die digitale Sicherheit und wird täglich für Internetaktivitäten, E-Mails und finanzielle Transaktionen genutzt. Diese Verfahren beruhen auf der Annahme, dass bestimmte mathematische Probleme, wie das Faktorisierungsproblem, schwer lösbar sind. Große Zahlen, die unsere

> **Wir brauchen eine gemeinsame Sprache und einheitliche Regeln, um uns zu verständigen.**

Kryptographie sichern, sind für klassische Computer schwer zu zerlegen, aber für Quantencomputer wäre dies einfach. Obwohl es derzeit keinen kryptographisch relevanten Quantencomputer gibt, bleibt die potenzielle Entwicklung eine große Bedrohung für die Cybersicherheit.

Welche Arten von Daten und Systemen sind Ihrer Meinung nach am stärksten gefährdet durch Quantencomputing, insbesondere im Hinblick auf die derzeitige Verschlüsselung? Warum sind diese Systeme besonders anfällig für das Knacken durch Quantencomputer?
Christoph Striecks: Besonders gefährdet sind Systeme, die herkömmliche Kryptographie benutzen und sensible Daten beinhalten, wie Finanzinformationen, persönliche Daten und staatliche Geheimnisse. Auch Systeme, die auf kryptographischen Verfahren basieren, wie Blockchains und Kryptowährungen, könnten betroffen sein. Daher ist es wichtig, dass Organisationen und Regierungen jetzt Maßnahmen ergreifen, um ihre Systeme quantensicher zu machen. Ein Beispiel dafür ist die Europäische Union, die derzeit die europäische Quantenkommunikationsinfrastruktur (EuroQCI) aufbaut. Diese Initiative zielt darauf ab, ein hochsicheres Kommunikationsnetzwerk innerhalb der EU zu schaffen, das kritische Infrastrukturen über terrestrische und Satellitensegmente schützt. Dieses Netzwerk soll im Zeitalter des Quantencomputers besonders sicher sein und könnte in Zukunft weitere Anwendungsgebiete umfassen.

Man hört häufig das Schlagwort „Postquantenkryptographie" Könnten Sie dieses Konzept erläutern und erklären, wie es uns helfen kann, die Bedrohung durch Quantencomputer zu mindern?
Christoph Striecks: Postquantenkryptographie oder allgemeiner auch die quantensichere Kryptographie umfasst Algorithmen, die gegen Quanten- und klassische Computerangriffe resistent sind. Die zwei Haupttechnologien sind Quantum Key Distribution (QKD), die auf Quantenphysik basiert und spezielle Hardware benötigt, und Postquantenkryptographie (PQC), die auf sicheren Annahmen gegen Quantencomputer beruht und in Software integriert werden kann. Eine Hybridform kombiniert QKD und PQC, um ihre Stärken zu nutzen. Beide Technologien entwickeln sich weiter und werden voraussichtlich neben bestehenden Verschlüsselungsmethoden koexistieren.

Welche spezifischen Fortschritte wurden in den letzten Jahren bei der Entwicklung von Quantencomputern erzielt, und welche Herausforderungen bestehen Ihrer Meinung nach weiterhin?
Christoph Striecks: In den letzten Jahren hat die Entwicklung von Quantencomputern bemerkenswerte Fortschritte gemacht, insbesondere in der Hardwareentwicklung, bei der mehr Qubits und bessere Fehlerkorrektur erreicht wurden. Diese Fortschritte sind das Ergebnis erheblicher Investitionen in Forschung und Entwicklung, und es wird erwartet, dass die Investitionen in die Quantentechnologie weiter steigen. Trotz dieser Fortschritte gibt es immer noch erhebliche technologische und praktische Herausforderungen, die bewältigt werden müssen. Kontinuierliche Forschung und Investitionen sind entscheidend, um die Skalierbarkeit und kommerzielle Nutzung der Technologie zu erreichen und ihr volles Potenzial auszuschöpfen.

Wie weit sind wir Ihrer Meinung nach von der Entwicklung eines funktionierenden Quantencomputers entfernt, der in der Lage ist, aktuelle Verschlüsselungen zu knacken?
Christoph Striecks: Die Antworten, wann ein funktionierender Quantencomputer in der Lage sein wird, aktuelle Verschlüsselungen zu knacken, variieren stark unter Expert:innen. Aus kryptographischer Sicht müssen wir mittelfristig mit ersten Ergebnissen rechnen. Es wird erwartet, dass Quantencomputer zunächst wirtschaftlich interessante Anwendungen haben, bevor sie kryptographisch relevant werden. Ein wichtiger Grund, warum wir uns heute schon mit dem Problem beschäftigen müssen, ist der „Store Now, Decrypt Later"-Angriff. Dabei kann ein Angreifer bereits jetzt verschlüsselte Daten sammeln und speichern, um sie später mit einem Quantencomputer zu entschlüsseln, sobald dieser verfügbar ist. Deshalb ist es wichtig, jetzt auf quantensichere Kommunikation umzustellen, wie es auch in den Empfehlungen und Regulierungen der EU reflektiert wird.

Wie wichtig ist Ihrer Meinung nach die internationale Zusammenarbeit bei der Quantencomputing Forschung, und welche Rollen spielen große Technologieunternehmen und Regierungen dabei? Welche Herausforderungen sehen Sie in der Zusammenarbeit im Bereich Quantencomputing, und wie können diese überwunden werden?
Christoph Striecks: Internationale Zusammenarbeit ist entscheidend für die Entwicklung und sichere Nutzung von Quantencomputern. Große Technologieunternehmen und Regierungen spielen dabei eine zentrale Rolle. Ein Beispiel ist die EuroQCI-Initiative, an der das AIT beteiligt ist, mit nationalen und internationalen Projekten im Bereich der Quantentechnologie. In diesem Zusammenhang arbeitet das AIT auch auf nationaler Ebene an Projekten zur quantensicheren Kryptographie für die Übertragung vertraulicher Informationen zwischen Behörden im Rahmen des nationalen KIRAS-Förderprogramms für Sicherheitsforschung, das vom österreichischen Bundesministerium für Finanzen (BMF) finanziert wird. Unterschiedliche Ansätze weltweit machen die Entwicklung spannend.

Essenziell bei der internationalen Zusammenarbeit ist aber eine gemeinsame Sprache und einheitliche Regeln, um sich zu verständigen z. B. durch die Einführung von gewissen Standards. In Europa spielt die ETSI eine wichtige Rolle, während weltweit das NIST im Bereich der Postquantenkryptographie (PQC) viel zur Standardisierung beiträgt. Welche spezifischen Herausforderungen sehen Sie für Unternehmen in Österreich durch die potenziellen Risiken von Quantencomputern, und wie können sich diese Unternehmen darauf vorbereiten?
Christoph Striecks: Unternehmen in Österreich sollten sich auf die potenziellen Risiken durch Quantencomputer vorbereiten, indem sie ihre Sicherheitsprotokolle überprüfen und in quantensichere Kryptographie investieren. Eine konkrete Maßnahme ist die Erstellung eines Migrationsplans, wie ihn Standardisierungsorganisationen und Industrieakteure bereits erarbeiten. Dieser

besteht aus drei wesentlichen Schritten. Zunächst erfolgt die Inventory Compilation, bei der ermittelt wird, welche Unternehmenswerte von Quantencomputern beeinflusst werden könnten und ob ein Migrationsinventar-Manager sowie Budget vorhanden sind. Anschließend wird der Migration Plan vorbereitet, indem ein Migrationsplan erstellt wird, der mögliche Probleme, Hardware, Schlüsselmanagement, Vertrauensmanagement und die dahinterliegenden Geschäftsprozesse berücksichtigt. Schließlich wird die Migration ausgeführt, wobei der Fokus auf Migrationsmanagement und Anpassung der Geschäftsprozesse liegt. Zusätzlich sind Schulungen und Bewusstseinskampagnen wichtig, um Unternehmen auf die Bedrohungen durch Quantencomputer vorzubereiten und ihre Systeme sicher zu gestalten.

Welche langfristigen Auswirkungen auf die Cybersicherheit und die Gesellschaft sehen Sie im Zusammenhang mit Quantencomputing, und wie sollten wir uns darauf vorbereiten?
Christoph Striecks: Quantencomputing hat das Potenzial, die Cybersicherheit grundlegend zu verändern, insbesondere durch die Umstellung auf quantensichere kryptographische Systeme. Diese Migration wird eine enorme Herausforderung in den kommenden Jahren sein, da es so etwas in der Kryptographie bisher nicht gab. Gleichzeitig eröffnet Quantencomputing viele neue Möglichkeiten in verschiedenen Bereichen. Unternehmen und Gesellschaften können sich darauf vorbereiten, indem sie in Bildung, Forschung und Entwicklung investieren.

> **Wichtig ist, die Technologie verantwortungsbewusst zu nutzen.**

Wie sehen Sie die Zukunft der Finanzwelt im Hinblick auf Quantencomputing? Gibt es spezielle Maßnahmen, die ergriffen werden sollten, oder bleibt alles davon unberührt?
Christoph Striecks: Zunächst sollten Kommunikationsnetzwerke, z. B. zwischen Banken, quantensicher gemacht werden, um die Kommunikation abzusichern. Eine wichtige Maßnahme ist die Implementierung von quantensicherer Kryptographie, um diese Bedrohung zu mindern. Weiters könnte im Bereich der Kryptowährungen tatsächlich eine erhebliche Beeinflussung stattfinden. Die Algorithmen, die in Kryptowährungen verwendet werden, sind nicht direkt von Angriffen wie „Store Now, Decrypt Later" betroffen, was einen gewissen Zeitpuffer bietet. Der Fokus sollte zunächst auf der sicheren Kommunikation in den Netzwerken liegen, aber es ist ratsam, bereits jetzt schon über die Umstellung von nicht-quantensicheren auf quantensichere Blockchains und Kryptowährungen nachzudenken.

Glauben Sie, dass die Vorteile von Quantencomputing die Risiken überwiegen? Wenn ja, warum?
Christoph Striecks: Die Vorteile von Quantencomputing, wie schnelle Berechnungen und neue wissenschaftliche Entdeckungen, könnten die Risiken überwiegen. Wichtig ist, dass wir die Technologie verantwortungsbewusst nutzen. Heißt, bei der Entwicklung und Anwendung von Quantencomputern sollten ethische Überlegungen wie Datenschutz und Sicherheit berücksichtigt werden. Eine verantwortungsvolle Nutzung kann durch klare Richtlinien und regelmäßige Überprüfungen sichergestellt werden. Insgesamt sehe ich das positiv und bin gespannt auf die zukünftigen Entwicklungen im Bereich Quantencomputing.

Wenn wir uns in 12 Monaten wieder treffen, was würden wir uns dann wünschen, heute schon getan zu haben?
Christoph Striecks: In 12 Monaten sollten Maßnahmen ergriffen worden sein, um unsere Daten zu schützen und uns auf die Quantenzukunft vorzubereiten. Zudem wäre es wünschenswert, dass mehr in quantensichere Kryptographie sowie in Bildung und Forschung investiert wird, damit wir eine sichere und vielversprechende Zukunft haben.

Vom Bodensee zum Neusiedler See

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

Frage 1: Rückblickend wünschte ich mir, wir hätten in puncto Cybersicherheit viel früher damit begonnen, …

Frage 2: Momentan sehe ich 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?

Frage 6: Die größte Veränderung in Bezug auf Cybersecurity in den letzten 10 Jahren war für mich/uns …

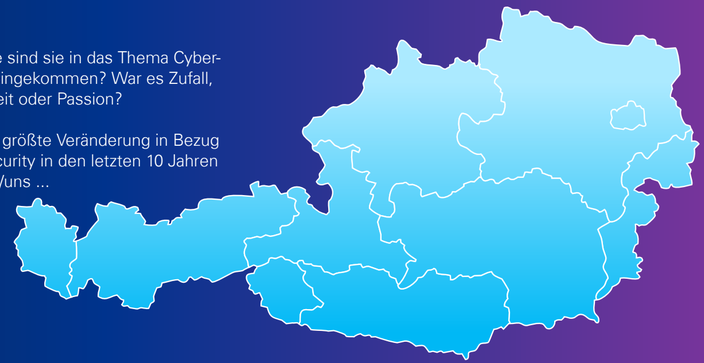


FOTO © PRIVAT

Mag.(FH) Rudolf Ivancsits, MBA
CISO / Land Burgenland

1: ... das Thema zu adressieren, weil dann die Bewusstseinsbildung auf allen Ebenen leichter wäre. Gesetzliche Entwicklungen rund um NIS-2, RKE, CRA etc. sehe ich als Treiber für die Informationssicherheit und sage klar: Digitalisierung und Innovationen ohne Cybersicherheit – das geht sich nicht aus!.

2: ... in den Möglichkeiten der KI. Dennoch bleibt die Prämisse des Risikomanagements der Klassiker: Das jeweils schwächste Glied in der Kette stellt das größte Gefährdungspotenzial dar. Meist ist das noch immer die fehlende Awareness.

3: ... ein ISMS und somit angemessenes Management, Commitment zu Zeit, Budget, Personal und damit klare Rollen- und Entscheidungsdefinitionen – einerseits für den kontinuierlichen Prozess, andererseits, um bei Vor- oder Notfällen schnellstmöglich handlungsfähig zu sein.

4: Nicht Vorbild, aber Wertschätzung für alle Organisationen, welche Informationssicherheit nicht als einmaliges Projekt, sondern kontinuierlichen Verbesserungsprozess „leben“ und notwendige Ressourcen bereitstellen sowie Expert:innen, welche neue Bedrohungen aufzeigen.

5: Nach über 20 Jahren in der IT habe ich die Chance ergriffen vom CIO zum CISO zu werden und mich somit ganzheitlich der Informationssicherheit als Bindeglied vom Top-Level-Management bis zur operativen Ebene zu widmen.

6: ... dass Informationssicherheit langsam, aber sicher sowohl in allen Management-Ebenen als auch bei den Endanwender:innen ankommt und ich den Satz immer weniger höre: „Info-Sicherheit – das ist doch nur Sache der IT ...“.

FOTO © PRIVAT

Dipl.-Ing. Werner Hörner
Geschäftsführer / Humanomed

1: Aus unserer Sicht haben wir rechtzeitig mit dem Thema Cybersicherheit begonnen. Seit 2020 sind wir nach DIN 27001 zertifiziert, d. h. wir haben uns schon im Jahr davor intensiv mit den Fragestellungen zur Informationssicherheit im Unternehmen beschäftigt. Seitdem liegt im Unternehmen ein wichtiger Fokus auf dem Thema.

2: ... in Phishing-Mails in Kombination mit AI-Anwendungen. Es wird immer schwieriger, Bedrohungen zu erkennen. Die technische Umsetzung und Aktualisierung ist die eine Seite, bei unseren 1400 Mitarbeitenden haben wir viele Anwender:innen und damit bieten wir eine breite Angriffsfläche. Schulungen und Awareness sind eine große Herausforderung.

3: ... die Unterstützung der obersten Unternehmensführung, damit die erforderlichen personellen und technischen Ressourcen für das Thema zur Verfügung gestellt werden und ein Unternehmen in diesem Bereich am Stand der Technik gehalten werden kann. Und dann natürlich IT-Expert:innen im Unternehmen, die das umsetzen können und wollen.

4: Nein, eigentlich nicht. Wir halten uns an die Standards international anerkannter Normen als Vorgabe für unser Handeln. Diese Vorgaben kommen auch jetzt aktuell aus der kommenden NIS-2-Verordnung, deren Umsetzung alle unsere Krankenhäuser und Reha-Zentren betrifft und eigentlich alle notwendigen Maßnahmen zur Reduktion des Risikos von Daten- und Informationsverlusten vorgibt.

5: Als Softwarehersteller und IT-Dienstleister für die eigene Unternehmensgruppe Humanomed haben wir es als Verpflichtung gesehen, den maximal möglichen Schutz unserer sensiblen Daten im Gesundheitswesen zu gewährleisten und damit auch weiterhin wettbewerbsfähig zu bleiben.

6: ... die Veränderung der Wahrnehmung zu dem Thema, auch in der Öffentlichkeit. Die möglichen Schäden und negativen Auswirkungen sind gestiegen, die Angreifer:innen sind besser geworden, und natürlich auch die Verteidiger:innen!

FOTO © WWW.POV.AT

DI Markus Kohlheimer, BSc
IKT-Sicherheitsbeauftragter / CISO / NÖ Landesgesundheitsagentur

1: ... umfassender zu denken. Ein ganzheitlicher Resilienzansatz, der vom Personal verinnerlicht ist, stärkt das Vertrauen in die eigene Handlungsfähigkeit und schafft die Grundlage für einen stabilen Betrieb, trotz unvorhersehbarer Cybergefahren.

2: ... dass mit verhältnismäßig geringem Aufwand und Risiko das Vertrauen der Bevölkerung in die Zuverlässigkeit und Leistungen der österreichischen kritischen Infrastruktur - im Kontext der aktuellen geopolitischen Spannungen - geschwächt wird, was zu Instabilitäten führen kann.

3: ... einen ganzheitlichen Sicherheitsansatz, der moderne Technologien, klare Prozesse, Sensibilisierung und Ausfallkonzepte vereint. KI-gestützte Angriffe erfordern schnelle Reaktionen und das Stärken etablierter Notfallprozesse.

4: Nein, wir müssen verstärkt von denen lernen, die direkte Erfahrungen mit Sicherheitsvorfällen gemacht haben oder es unter schwierigen Betriebsbedingungen geschafft haben, den Betrieb erfolgreich aufrechtzuerhalten.

5: Mein Interesse an IT-Sicherheitsmanagement wurde durch meinen HTL-Lehrer geweckt und gefördert. Persönlich fasziniert mich das Spannungsfeld zwischen IT-Sicherheit und Klinikbetrieb, mit dem Ziel, die Patient:innenversorgung zu gewährleisten.

6: ... dass Angriffe immer schneller und spezialisierter wurden, während die Digitalisierung in Kliniken wächst und Abläufe transformiert. Gleichzeitig stiegen die gesetzlichen Dokumentationsanforderungen.

FOTO © STEFAN MAYERHOFER

Sofie Grill, MSc MBA
Stabsstellenleitung Konzern-Informationssicherheit und Datenschutz / Linz AG

1: Eine starke Verankerung der Informationssicherheit in der Unternehmenskultur, die zielgerichtete Nutzung bestehender Strukturen und Abläufe für Informationssicherheitsthemen und die damit verbundene Nutzung von Synergien sind essenziell für starke Informationssicherheitsmaßnahmen.

2: ...bei Angriffsversuchen gegen den Faktor „Mensch“ sowie den Eintrittsvektoren aufgrund Optimierungsbedarf bei den „Basis-Hygiene“-

Maßnahmen (Multi-Faktor-Authentifizierung, Patch-Management etc.).

3: ... eine erfolgreiche Integration in alle Unternehmensprozesse – Informationssicherheit ist grundlegender Bestandteil aller Aktivitäten im Unternehmen und benötigt den Einsatz jeder:s Einzelnen.

4: Informationssicherheit geht nur gemeinsam und persönlich schätze ich den unternehmens- und branchenübergreifenden Austausch der Informationssicherheitsexpert:innen. Zusammenhalt und voneinander Lernen bringen uns alle weiter.

5: Über meine Ausbildung an der FH OÖ Campus Hagenberg und spannenden Einblicken in unterschiedlichen Unternehmen im Umfeld kritischer Infrastrukturen – und ich bin stolz, dass meine Arbeit im weitesten Sinn einen wesentlichen Nutzen für meine Mitmenschen bringt.

6: ... das steigende Informationssicherheits-Bewusstsein in allen Lebensbereichen – sowohl im beruflichen als auch im privaten Umfeld – sowie die entstandenen Treiber der gesetzlichen Anforderungen.

FOTO © PRIVAT

Medina Aganovic, BSc
Leitung des Security Operations Center /
SPAR Gruppe

1: ... geopolitische Einflüsse auf Cybersicherheitsstrategien besser zu verstehen, Frameworks wie MITRE ATT&CK konsequent zu nutzen und zusätzlich zur Technik auch auf Governance und Compliance zu fokussieren, da diese heute untrennbar miteinander verbunden sind, um Bedrohungen effektiv zu begegnen.

2: ... in der angespannten geopolitischen Lage zwischen großen Akteuren wie China, Russland, Iran und den USA, der hohen Abhängigkeit von Tech-Unternehmen außerhalb Europas sowie den rasanten Fortschritten in KI und Quantencomputing.

3: ... den gezielten Einsatz von KI und Automatisierung für schnellere Anomalie-Erkennung, automatisierte Reaktionen und verhaltensbasierte Analysen. Das SOC wird dabei noch mehr an Bedeutung gewinnen und eine zentrale Rolle bei der schnellen, risikobasierten Response spielen.

4: Estland fällt mir besonders im Umgang mit Cyberbedrohungen auf. Während meines Besuchs 2022 beeindruckte mich die digitale Infrastruktur und Cybersicherheit. Estland setzte früh auf digitale Identitäten und starke Kooperation zwischen Staat und Privatwirtschaft zum Schutz vor Cyberbedrohungen.

5: Ich war immer an Security interessiert, ursprünglich aus der Netzwerk-Security-Perspektive. Nach einem Ausflug in Data Science zog mich die Cybersicherheit zurück. Der Weg ins SOC war zunächst zufällig, wurde jedoch schnell Teil meiner Passion.

6: ... automatisierte Tools und AI viele Aufgaben übernehmen, was Fortschritt bedeutet. Doch bei jüngeren Fachkräften fehlt immer mehr das tiefgehende IT-Wissen. Ohne dieses Basis-Know-how, das nicht mehr ausreichend weitergegeben wird, könnten wir in Zukunft vor großen Herausforderungen stehen.

FOTO © PRIVAT

Dr. Rupert Schindler, MBA
Bereichsleiter IT & Digitalisierung /
Energie Steiermark AG

1: ... internes Personal aufzustocken. Schlussendlich ist die Kapazität an ausgebildetem IT-Personal entscheidend für die Cybersecurity, wir haben hier sehr gute Erfahrungen mit internen Ausbildungsprogrammen. Aber im Bereich Sicherheitssysteme hat man permanent den Bedarf nach zusätzlichen Händen.

2: ... in Systemkomplexität und Zero-Day-Themen. Wir haben notwendigerweise eine Systemvielfalt, was zu potenziellen Eingangsszenarien über die Supply Chain führt. Zusätzlich werden die verfügbaren Reaktionszeiten für die IT-Mannschaft immer kürzer.

3: ... spezifische Strukturen und Teams in der IT. Es darf keine Nebenaufgabe des IT-Stammpersonals mehr sein. Entsprechende Ausbildungen bzw. spezielles Recruiting von Profilen ist hier sehr wichtig, z. B. für ein Security Operation Center.

4: Ich glaube, niemand macht hier alles perfekt – wir versuchen im Dialog in der Branche, mit Vendoren und Expert:innenforen für uns das Beste zu definieren. Persönlich bin ich sehr reserviert, wenn vor allem Hersteller bestimmte Lösungen als umfassend anpreisen, die Realität ist meist anders.

5: Aus der Notwendigkeit als IT-Leiter – ich bin über die Jahre immer mehr in das Thema hineingewachsen und es ist eine spannende Aufgabe. Allerdings kommt gerade bei Cybersecurity rasch der Punkt, wo die Themen in hohes Spezialistenwissen abdriften – da ist es für mich wichtig, meinen Team vertrauen zu können und die eigenen Know-how-Grenzen zu kennen.

6: ... dass das Thema komplett im Mainstream angekommen ist und nicht mehr als reines Spezialthema für die IT gesehen wird. Auch die entsprechende Gesetzgebung mit NIS verstärkt diesen Trend, Cybersecurity wird im Management viel intensiver diskutiert als noch vor einigen Jahren.

FOTO © MCI

Prof. Dr. Peter Mirski
CIO / Management Center Innsbruck (MCI)

1: ... die Gesellschaft auf die kommenden Herausforderungen vorzubereiten - ganz im Sinne einer informierten Selbstbestimmung.

2: ... im unabgestimmten Einfluss von Politik, Wirtschaft und Gesellschaft auf notwendige Standards - das schafft riskante und schlecht regulierte Bereiche.

3: ... die Kombination von fortschrittlichen Technologien wie KI und Machine Learning einerseits und andererseits mit der Bildung unserer Gesellschaft für einen bewussten Umgang mit IT.

5: Als CIO sehe ich es als meine Aufgabe unsere Hochschule bestmöglich zu schützen und unsere IT- Abteilung bestmöglich auszustatten sowie in strategische Entscheidungen direkt einzubinden.

6: ... der Umstand, dass Arbeiten und Studieren so stark online wurden und damit die Verfüg-

barkeit und Gefährdung der IT-Systeme massiv zugenommen hat. Auch die Tatsache, dass Fake Content immer schneller und professioneller generiert werden kann, hat eine große Auswirkung auf unsere Gesellschaft.

FOTO © PRIVAT

Dipl.-Inf. (univ.) Thomas Schneider
Informationssicherheitsbeauftragter /
CISO illwerke vkw AG

1: ... ein Security Operations Center mit effizienten und effektiven Prozessen zur Erkennung und Bewältigung von Vorfällen aufzubauen. Dies, gepaart mit frühzeitig eingestelltem, qualifiziertem Personal, das alle Prozesse und Systeme zur Stärkung der Cybersicherheit weiterentwickelt und deren Umsetzung steuert und überwacht.

2: ... in der steigenden Häufigkeit und Komplexität von Angriffen, die sowohl Unternehmen als auch Privatpersonen betreffen. Ein Schutz von Mitarbeitenden und Privatpersonen wird immer aufwändiger und gleichzeitig lassen sich die Täter:innen immer weniger zurückverfolgen und zur Rechenschaft ziehen.

3: ... umfangreiche Qualifikation jedes Mitarbeitenden, ein funktionierendes Informationssicherheits-Managementsystem, effektive Cybersecurity-Prozesse und deren Automatisierung zur Überwachung und zum Schutz der Menschen, Betriebsprozesse und Technologie.

4: Nein, für mich gibt es im Bereich Cybersicherheit kein einzelnes Vorbild. Cyberbedrohungen zu begegnen ist eine Aufgabe, der wir nur gemeinsam begegnen können.

5: Bereits im Studium war die Absicherung von Systemen gegenüber schädigendem Einfluss mein Start in das Themenfeld Cybersecurity, spätestens seit der Übernahme eines Universitäts-Webservers zur Verbreitung von illegalen Inhalten wurde daraus eine Passion, die mich über viele Jahre der technischen bzw. operativen Security begleitet und ins Informationssicherheitsmanagement geführt hat.

6: ... die Bestellung zum Informationssicherheitsbeauftragten eines der größten Energieversorgers Österreichs und für uns als illwerke vkw die Zertifizierung der OT Bereiche nach ISO 27001 und im Folgenden die Erfüllung der geltenden gesetzlichen Anforderungen.

FOTO © PRIVAT

Mag. iur. Victoria Cygne Lara Toriser
Leiterin des Referats Cybergrundlagen & Innovation / Militärisches Cyberzentrum des Österreichischen Bundesheers

1: ... Cybersicherheit bzw. Cyberverteidigung als integralen Bestandteil aller Digitalisierungsvorhaben zu verankern – nicht als nachgelagertes Thema, sondern als Innovationstreiber und Enabler für gesamtheitliche und gesamtstaatliche zukunftssichere IT-Systeme und Prozesse.

2: ... in der zunehmenden Professionalisierung krimineller Gruppen, derer sich natürlich auch staatliche Akteure bedienen – kombiniert mit KI-gestützten Angriffen, die schneller, gezielter und schwerer zu erkennen sind als je zuvor. Außerdem besteht eine besondere Herausforderung in der Verschmelzung klassischer Cyberangriffe mit Desinformationsoperationen und hybrider Kriegsführung – zunehmend automatisiert, skalierbar und gezielt auf militärische Schwachstellen ausgerichtet.

3: ... die konsequente Verzahnung von Mensch, Technik und KI – nur wer adaptive, resiliente Systeme mit kontinuierlicher Aus- und Weiterbildung kombiniert, wird im digitalen Raum dauerhaft handlungsfähig bleiben. Dafür brauchen wir vor allem ein Mindset, das über den Tellerrand hinweg sieht, und Offenheit und Motivation für Innovation zulässt. Daher hat mein Referat im Militärischen Cyberzentrum die Initiative „InnoVision" zur Förderung von Innovation im Bereich Cybersicherheit und -Verteidigung gestartet. Die neue Veranstaltungsreihe „InnoVision" hat das Ziel, einen Raum zu schaffen, in dem Wissen aus verschiedenen Aspekten der Cybersicherheit und -Verteidigung geteilt, Ideen geboren und bahnbrechende Technologien in Österreich für Österreich vorangetrieben.

4: Mich beeindrucken besonders Estland und Finnland. Estland – als Land, das Cybersicherheit holistisch denkt, früh digitale Resilienz aufgebaut hat und Innovation mit einem starken sicherheitspolitischen Mindset verknüpft. Ein echtes Vorbild in Sachen Cyberresilienz. Finnland – als Land, das gesamtstaatliche Sicherheit (Comprehensive Security) aktiv lebt und für Österreich als Vorbild für die Gestaltung und Umsetzung der umfassenden Landesverteidigung herangezogen werden sollte.

5: Es war eine Mischung aus Notwendigkeit und Passion – die Rolle bzw. Bedeutung von Sicherheit und Verteidigung hat mich früh fasziniert, insbesondere in Bezug auf hybride Bedrohungen, wo der Cyber- und Informationsraum natürlich eine bedeutende Rolle spielt. Daraus entstand der Wille, mich aktiv zu beteiligen, diese Dimension mitzugestalten und Innovationen im sicherheitsrelevanten Umfeld voranzutreiben.

6: ... das Aufkommen disruptiver Technologien wie KI, Quantencomputing und autonomer Systeme – sie verändern das Bedrohungsspektrum und eröffnen neue Angriffsflächen. Dies erfordert ein Umdenken in den Bereichen Cyberresilienz und Schutz kritischer Infrastrukturen. Gleichzeitig können diese Emerging Disruptive Technologies (EDTs) auch für die Sicherheit und Verteidigung genutzt werden, weshalb gezielte Innovation und Forschung in diesem Bereich so wichtig ist.
Wir dürfen nicht länger warten – andere globale Akteure warten auch nicht.

Umfragemethodik

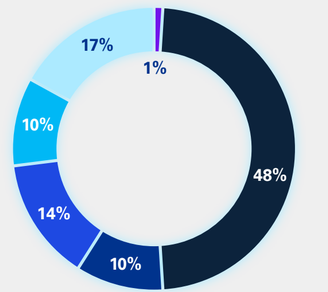
Die zehnte Ausgabe der jährlich erscheinenden KPMG & KSÖ Studie „Cybersecurity in Österreich“ untersucht, wie Unternehmen in Österreich auf die wachsenden Bedrohungen durch Cyberkriminalität reagieren und welche Sicherheitsmaßnahmen sie ergreifen.

Überblick
Im Jänner und Februar 2025 führte KPMG eine Umfrage unter 1.391 österreichischen Unternehmen durch. Die Befragten kamen aus kleinen, mittleren und großen Unternehmen verschiedener Branchen, darunter Automobilindustrie, Banken, Bauwesen, Bildung, Chemie, Dienstleistungen, Energie, Gesundheitswesen, Immobilien, Industrie, Konsumgüter, Medien, öffentlicher Sektor, Technologie, Telekommunikation, Tourismus und Versicherungen.

Analyse
Jede:r Teilnehmer:in erhielt einen Online-Fragebogen, der auf ihre:seine Rolle im Unternehmen abgestimmt war. Neben den quantitativen Fragen, die auf einer Likert-Skala basierten, wurden auch qualitative Aspekte berücksichtigt, um den Befragten die Möglichkeit zu geben, zusätzliche Eindrücke und Kommentare zu teilen. Die Auswertung unterschied zwischen der internen Sicht (Expert:innen, Bereichsleiter:innen, CSO etc.) und der externen Sicht (Vorständ:innen, Eigentümer:innen, Aufsichtsrät:innen). Ein Team von KPMG-Expert:innen aus dem Bereich Cybersecurity-Consulting analysierte die Ergebnisse.

Vertiefung
Zusätzlich führten wir persönliche Interviews mit 26 Vertreter:innen aus der Wirtschaft, der öffentlichen Verwaltung und internationalen Cybersecurity-Expert:innen. Sie sprachen mit uns über Herausforderungen, aktuelle Entwicklungen sowie zukünftige gesellschaftliche und inhaltliche Handlungsfelder.

Unternehmensfunktion



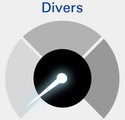
- Aufsichtsrät:in
- Vorständ:in/Geschäftsführung/Eigentümer:in
- CDO/CIO/IT-Leitung
- CSO/CISO/Sicherheitsverantwortliche:r
- Bereichsleitung/Abteilungsleitung/Teamleitung
- Expert:in/Mitarbeiter:in

Geschlecht

71 % (987)
Männlich

27 % (375)
Weiblich

0 % (1)
Divers



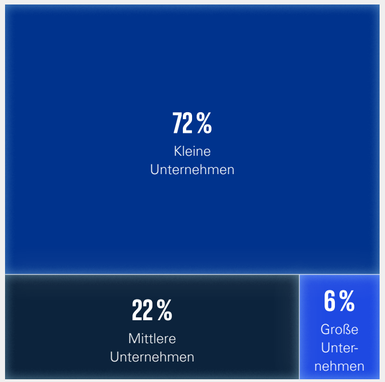
2 % (28)
Keine Angabe

Branche

Automobilindustrie (Automotive)	1 %
Banken (Financial Services)	3 %
Bauwirtschaft	3 %
Bildung (Education)	2 %
Chemiewirtschaft	1 %
Dienstleistungsbereich	45 %
Energiewirtschaft	2 %
Gesundheitswesen (Healthcare)	5 %
Immobilienwirtschaft	2 %
Industrie	4 %
Konsumgüter	3 %
Lebensmittel	1 %
Öffentlicher Sektor (Government and Public Sector)	6 %
Technologie, Medien und Telekommunikation	15 %
Tourismus	2 %
Versicherung (Insurance)	4 %

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

Unternehmensgröße



23 %
Familienunternehmen

9 %
Start-up

25 %
Kritische Infrastruktur

Impressum

Herausgeber
KPMG Security Services GmbH

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

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

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

David Kindermann
M +43 664 816 11 76
dkindermann@kpmg.at

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

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

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

Druck:
Ferdinand Berger & Söhne GmbH

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

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.

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


10
JAHRE
CYBER
SECURITY
STUDIE