Deloitte.

Cyber Security Report 2025

Inhalt

01

Vorwort

Mehr digitalisierte Abläufe in Unternehmen bedeuten auch mehr Angriffsfläche für Cyber-Kriminelle. Diese agieren nicht nur zunehmend professioneller, mit dem Fortschreiten von Artificial Intelligence (AI) stehen ihnen mittlerweile auch immer präzisere Technologien und Tools zur Verfügung, die ein unerkanntes Eindringen in Unternehmenssysteme deutlich einfacher und für die Opfer schadhafter machen.

Auf diese neue Bedrohungslage müssen Unternehmen entsprechend reagieren. Schon in den vergangenen Jahren zeigte unser jährlicher Report, dass das Thema Cyber Security zunehmend in das Bewusstsein der Verantwortlichen gerückt ist – auch weil in der Vergangenheit oft kein Tag vergangen ist, an dem kein Angriff passierte. Die zahlreichen Medienberichte über Cyber-Attacken erledigten ihr übriges in der Wahrnehmung.

Doch haben die Unternehmen dem gesteigerten Bewusstsein auch Taten folgen lassen? Wie gut sind sie auf die neue Bedrohungslage durch AI, aber auch die anhaltenden globale Spannungen vorbereitet? Und wie planen sie künftig mit diesen Themen umzugehen? Gemeinsam mit dem Forschungsinstitut Foresight wurden 350 österreichische Unternehmensvertreter:innen um ihre Einschätzungen dazu gebeten.

Wir wünschen eine interessante Lektüre.

Karin Mair | Georg Schwondra | Christoph Hofinger

Karin Mair
Managing Partner | Consulting

Georg Schwondra
Partner | Risk Advisory

Christoph Hofinger
Geschäftsführer | Foresight

02

Key Findings

Ransomware-Attacken werden aggressiver

Ransomware-Attacken bleiben die häufigste Cyber-Bedrohung für Unternehmen. So hat sich die Zahl der betroffenen Unternehmen von 2022 bis heute beinahe verdoppelt. Zwar konnten 56 % der Unternehmen die Ausbreitung durch technische Maßnahmen verhindern, doch bei einer Verschlüsselung gelingt nur 20 % die (teilweise) Entschlüsselung und 33 % die Wiederherstellung per Backup. Dies zeigt: Die Cyber Security in den befragten Unternehmen verbessert sich, jedoch werden Ransomware-Angriffe gleichzeitig aggressiver und effektiver.

Einschätzung der Sicherheitslage ist ambivalent

Während die Unsicherheit im Hinblick auf die Cyber Security im öffentlichen Bereich hoch ist, wächst das Vertrauen in die eigenen Sicherheits-maßnahmen stetig. Die meisten Unternehmen planen daher in nächster Zeit auch keine Budgeterhöhung für ihre Cyber Security ein. Lediglich ein Drittel will ihre Technik- und nur ein Viertel ihre Personalbudgets aufstocken. Angesichts der neuen Bedrohungslage durch AI besteht allerdings die Gefahr, dass künftig konstant bleibende Budgets nicht ausreichen werden, um eine entsprechende Abwehr zu garantieren – viele Unternehmen wiegen sich hier wohl in einer falschen Sicherheit.

Zero Trust gewinnt an Bekanntheit

Lange Zeit fand der Zero-Trust-Ansatz, der es ermöglicht, Cyber-Risiken proaktiv zu managen, in Unternehmen nur geringe Beachtung. Doch langsam zeichnet sich ein Wandel ab: Der Anteil der Unternehmen, die den Ansatz nicht kennen, sank innerhalb eines Jahres von 48 % auf 41 %. Aufholbedarf gibt es aber hinsichtlich der Implementierung: Zwar ist der Anteil jener Unternehmen, die eine Implementierung planen, im Vergleich zum Vorjahr leicht gestiegen. Allerdings bleibt die Zahl der Betriebe, die Zero Trust im Einsatz haben, mit 24 % aber unverändert gering. Nichtdestotrotz ist es erfreulich, dass die Unternehmen zunehmend die Vorteile erkennen, um sich gegen wachsende Cyber-Bedrohungen zu wappnen. Auch regulatorische Vorgaben wie die NIS-2-Richtlinie, CER-Richtlinie oder DORA, welche Unternehmen dazu verpflichten, ihre Sicherheitsmaßnahmen zu verschärfen, spielen in diesem Zusammenhang eine Rolle.

Unterschiedliche Einstellungen zu AI

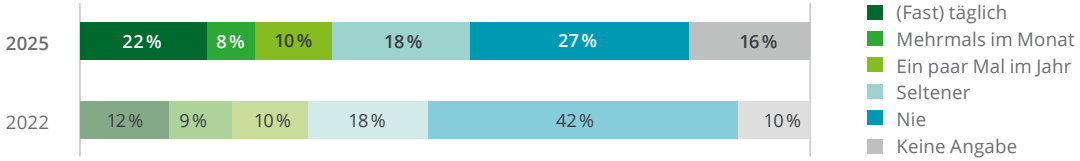
AI-Technologien beschäftigen Unternehmen stark. So nutzt knapp die Hälfte der Unternehmen (45 %) AI für die eigene Cyber Security, etwa bei der Phishing-Erkennung und -Prävention. Gleichzeitig tut sich mit der neuen Technologie aber auch ein neues Bedrohungsfeld auf: Über ein Drittel (37 %) der Unternehmen befürchtet, dass der Einsatz von generativer AI zu Datenleaks führen könnte.

03

Cyber-Kriminelle agieren immer professioneller

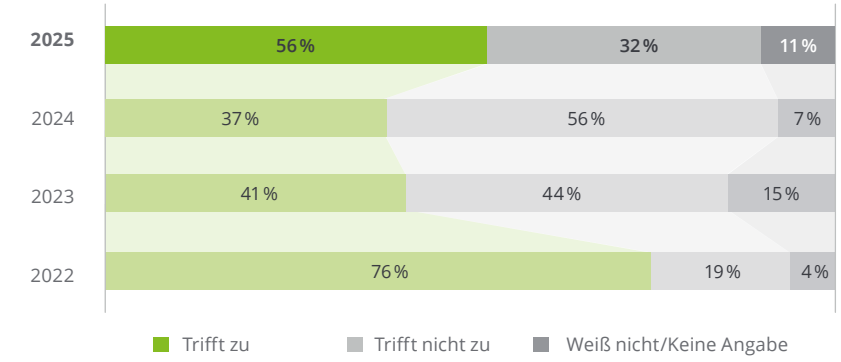
Ransomware-Attacken sind aktuell die größte Bedrohung für Unternehmen im Bereich der Cyber Security. Wie die aktuelle Umfrage belegt, ist die Häufigkeit der Angriffe im vergangenen Jahr stark angestiegen: So hat sich der Anteil jener Unternehmen, welche nahezu täglich Angriffsversuche verzeichnen von 12 % im Jahr 2022 auf 22 % im Jahr 2025 beinahe verdoppelt. Gleichzeitig ist der Anteil der Unternehmen, welche nicht betroffen sind, von 42 % auf 27 % im selben Zeitraum gesunken.

Häufigkeit von Ransomware-Attacken



Trotz der gestiegenen Zahl an Angriffen gelingt es den Unternehmen immer besser, diese effektiv abzuwehren. Während 2024 nur 37 % der Unternehmen von einer erfolgreichen Eindämmung der Ransomware berichteten, stieg dieser Wert im Jahr 2025 auf 56 % an. Zu verdanken ist das vor allem den verbesserten technischen Infrastrukturmaßnahmen, die es Unternehmen ermöglichen, Angriffe frühzeitig zu erkennen und die Verbreitung im Netzwerk zu verhindern.

Auswirkungen von Ransomware-Attacken

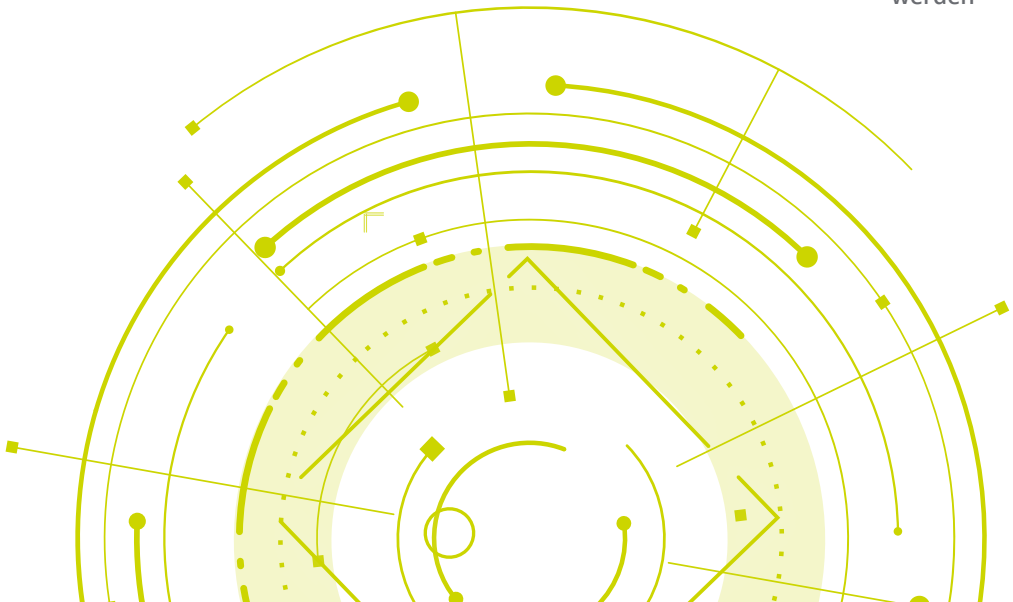


Die Verbindung von AI und einer angespannten geopolitischen Lage bringt bereits jetzt neue Bedrohungssituationen, die sich in den kommenden Jahren noch verschärfen könnten. Wie die jährlichen Befragungen zeigen, braucht die Wirtschaft immer einige Zeit, um sich auf neue Cyber-Gefahren einzustellen – so glauben 2025 nur mehr 27% der Unternehmen, dass sie von erpresserischen Ransom-Angriffen verschont bleiben, vor drei Jahren waren es noch 42%. Umso wichtiger ist, dass den Unternehmen klar wird, mit welchen Risken sie es auf absehbare Zeit zu tun haben werden.

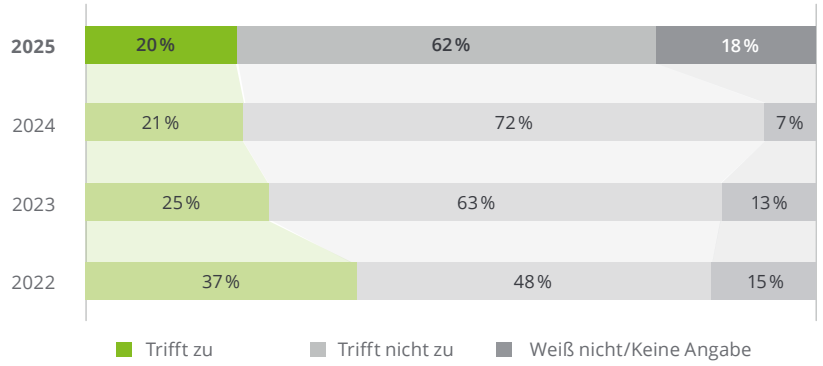
Christoph Hofinger | Geschäftsführer | Foresight

Befinden sich die Cyber-Kriminellen jedoch einmal in den Unternehmenssystemen, wird es immer schwieriger, sie zu bekämpfen. Die vorliegenden Zahlen zeigen, dass der Anteil der Unternehmen, die ihre verschlüsselten Daten vollständig oder größtenteils wiederherstellen konnten, von 37 % im Jahr 2022 auf 20% im Jahr 2025 gesunken ist. Auch die Möglichkeit, Daten über Backups wiederherzustellen, hat sich verringert – von 59 % im Jahr 2022 auf 33 % im Jahr 2025.

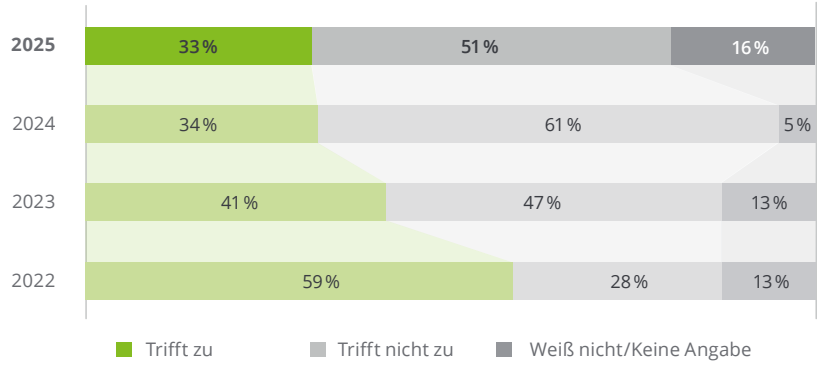
Wir wissen aus unserer täglichen Beratungspraxis, dass präventive Maßnahmen kontinuierlich weiterentwickelt werden müssen, um der wachsenden Komplexität moderner Bedrohungen gerecht zu werden. Das scheinen die Unternehmen in den vergangenen Monaten im Sinne der Abwehr geschafft zu haben. Um der zunehmenden Professionalität der Angreifer entgegenzutreten, müssen sie aber weiter kontinuierlich an ihrer Sicherheitsstrategie arbeiten.



Die Daten konnten ganz oder großteils wieder entschlüsselt werden



Die Daten konnten über eine Sicherung (Backup) wiederhergestellt werden



Deloitte Cyber Insights

Um Ransomware-Attacken heute erfolgreich abwehren zu können, spielen Sicherheitslösungen wie Endpoint Detection und Response (EDR bzw. XDR), Netzwerksegmentierung und Zero-Trust-Architekturen eine entscheidende Rolle. Darüber hinaus ist es aber essenziell, dass Unternehmen ihre Sicherheitsstrategien kontinuierlich an die Bedrohungslandschaft anpassen, um langfristigen Schutz zu gewährleisten.

Zudem erfordern Vorgaben wie etwa die NIS-2- und CER-Richtlinie, die erhöhte Anforderungen an die Cyber-Sicherheit und die Resilienz kritischer Infrastrukturen stellen, eine fortlaufende Anpassung der Schutzmaßnahmen. Unternehmen müssen sicherstellen, dass ihre Sicherheitsstrategien den aktuellen gesetzlichen Anforderungen entsprechen, um nicht nur Compliance zu gewährleisten, sondern auch die Widerstandsfähigkeit gegenüber Cyber-Angriffen zu stärken.

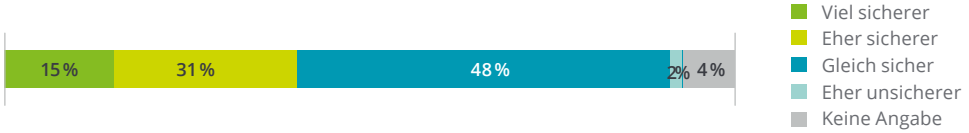
Ein weiterer kritischer Aspekt ist der starke Rückgang der Datenwiederherstellungsrate. Dieser Umstand weist darauf hin, dass moderne Ransomware nicht nur Primärdaten, sondern auch Backups gezielt angreift. Daher ist eine robuste Backup- und Wiederherstellungsstrategie unerlässlich, um im Ernstfall schnell reagieren zu können. Ebenso ist ein umfassendes Business Continuity Management (BCM) notwendig, um wesentliche Geschäftsprozesse auch während eines Cyber-Angriffs aufrechtzuerhalten. Ergänzend dazu empfiehlt sich die Implementierung eines strukturierten Incident-Managements, das eine frühzeitige Erkennung von Sicherheitsvorfällen ermöglicht, koordinierte Gegenmaßnahmen unterstützt und potenzielle Auswirkungen minimiert.

04

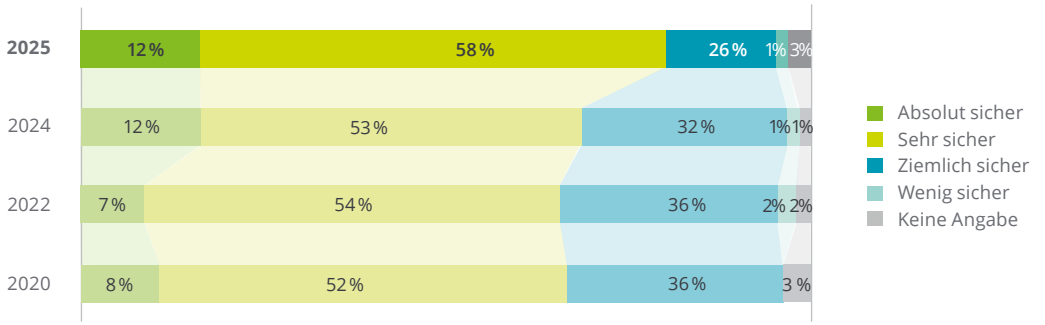
Unternehmen haben ambivalentes Sicherheitsgefühl

Unternehmen vertrauen ihren eigenen Cyber-Security-Sicherheitsmaßnahmen – und das, obwohl die Bedrohungslage derzeit durch AI sowie die sich zuspitzende geopolitische Situation sehr angespannt ist. Beinahe alle Befragten (96 %) schätzen ihre Daten und IT-Systeme als sicher ein und sehen, dass sich die Sicherheitslage seit dem Vorjahr verbessert oder sich zumindest stabilisiert hat.

Sicherheitslage im Vergleich zum Vorjahr



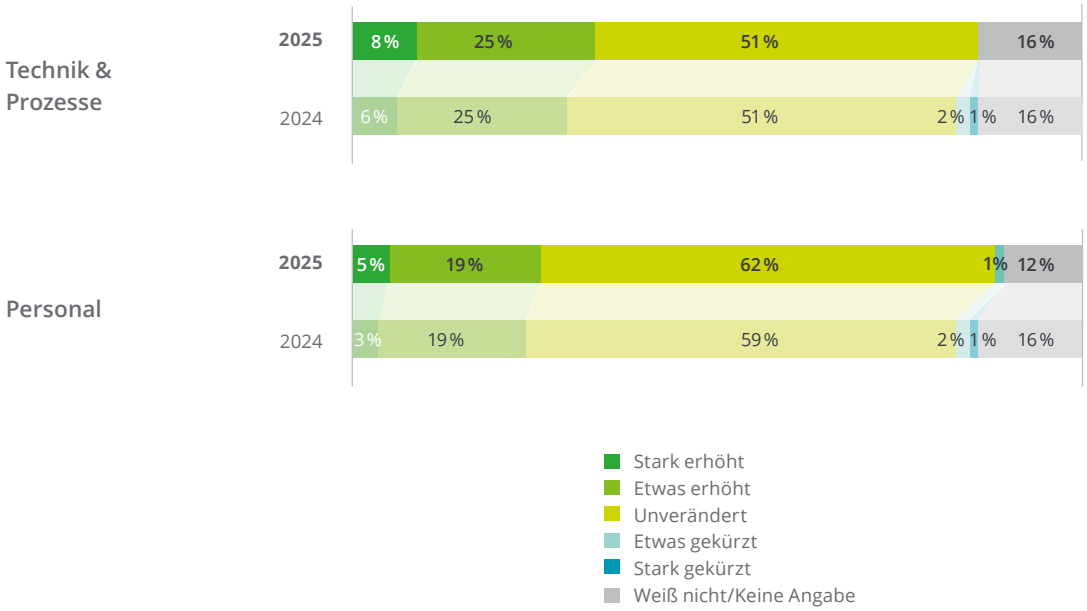
Sicherheit der Daten und IT-Systeme



Dieses gestiegene Selbstbewusstsein wirkt sich auch auf die Budgetpläne der Unternehmen aus. Über die Hälfte möchte in nächster Zeit das Budget nicht verändern, lediglich 24 % möchte die Budgets für Personal und 33 % die Budgets für Technik und Prozesse erhöhen. Starke Kürzungen bei den Sicherheitsbudgets finden sich dieses Jahr ebenfalls nicht.

Es ist erfreulich, dass die Unternehmen trotz der allgemein angespannten wirtschaftlichen Situation derzeit nicht über große Budgetkürzungen im Bereich Cyber Security nachdenken. Gleichzeitig sollten sie sich aber auch nicht in falscher Sicherheit wiegen. Denn Fakt ist auch: Die dynamische Bedrohungslage sowie die neuen Gefahren durch AI verlangen stetige Budgetanpassungen.

Budgetveränderungen



„Unternehmen müssen finanzielle Ressourcen für Cyber Security an die aktuelle Bedrohungslage anpassen. Dabei sollten auch regulatorische Anforderungen, wie zum Beispiel die NIS-2-Richtlinie, CER-Richtlinie, DORA oder der Cyber Resilience Act bedacht werden“

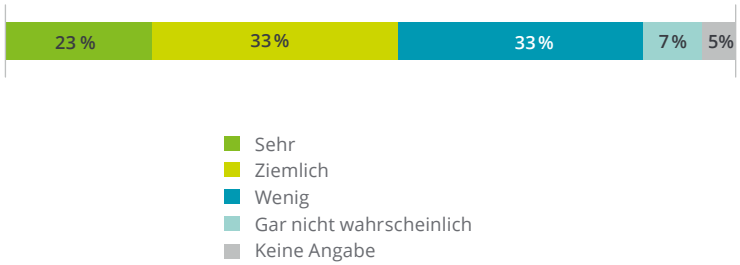
Georg Schwondra | Partner | Risk Advisory

Cyber Resilience Act (CRA)

Der Cyber Resilience Act (CRA) ist eine Verordnung der Europäischen Union, die die Cyber-Sicherheit von Produkten mit digitalen Elementen stärkt. Damit sind Software- oder Hardwareprodukte gemeint, deren bestimmungsgemäßer Zweck oder vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt. Beispiele dafür sind Software, Router bzw. Modems, IoT-Geräte, Bezahlterminals, Laptops oder Smartcards. Betroffen sind Unternehmen, die Hersteller, Importeure und Händler von Produkten mit digitalen Elementen sind. Bei Nichtkonformität erhalten die Produkte ab 11.12.2027 kein CE-Kennzeichen mehr und dürfen am EU-Markt nicht mehr in Verkehr gebracht werden.

Während die Unternehmen ihren eigenen Cyber-Security-Maßnahmen mittlerweile vertrauen, herrscht im Hinblick auf die öffentliche Cyber-Sicherheit große Unsicherheit. Mehr als die Hälfte der Befragten (56 %) hält es für sehr oder ziemlich wahrscheinlich, dass Cyber-Attacken das öffentliche Leben für mehrere Tage zum Stillstand bringen können.
Regulatorische Anforderungen setzen bereits bei der öffentlichen Sicherheit an und fordern strengere Cyber Security Vorgaben von den Unternehmen. Die Etablierung hinkt hinterher. Trotzdem bedarf es einer engen Zusammenarbeit zwischen Regierung, Wirtschaft, Wissenschaft und Zivilgesellschaft, um gesamtgesellschaftlich eine ausreichende Cyber-Sicherheits-Kultur zu etablieren. Zudem sollten robuste Koordinierungsstrukturen etabliert und ausgebaut werden, um schnell und effektiv auf Cyber-Bedrohungen und Incidents reagieren zu können.

Wahrscheinlichkeit, dass Cyber-Attacken das öffentliche Leben zum Stillstand bringen



Deloitte Cyber Insights

Die wahrgenommene Verbesserung der Sicherheitslage durch die Befragten könnte trügerisch sein, da sie möglicherweise auf kurzfristige Maßnahmen, die langfristig nicht ausreichen, zurückzuführen ist. Gleichzeitig ist die Diskrepanz zwischen der wachsenden Bedrohungslage und der positiven Sicherheitswahrnehmung ein Hinweis auf ein mögliches Sicherheitsparadoxon: Während sich Unternehmen sicherer fühlen, wächst die tatsächliche Bedrohung von außen weiter an. Dies birgt die Gefahr von Selbstzufriedenheit und einer unzureichenden Vorbereitung auf potenzielle Angriffe.

Angesichts der aktuellen Bedrohungslage ist es unerlässlich, dass Unternehmen ihre Sicherheitsstrategie kontinuierlich anpassen und von einer reaktiven zu einer proaktiven Sicherheitsstrategie übergehen. Dabei sollte auch die Budgetplanung die steigende Bedrohungslage widerspiegeln, um sicherzustellen, dass notwendige Investitionen in Sicherheitsmaßnahmen rechtzeitig erfolgen.

Festzuhalten ist in diesem Zusammenhang auch, das Mitarbeiterawareness ein zentraler Baustein ist, um Cyber-Sicherheit zu gewährleisten. Wir wissen aus unserer Beratungspraxis, dass die Unternehmen in den vergangenen Jahren in diesem Bereich sehr viel investiert haben. Eine hohe Awareness der Mitarbeitenden gegenüber dem Thema ist mittlerweile erfreulicherweise Standard. Das heißt aber nicht, dass künftig nicht weiter in Schulungen und Trainings investiert werden sollte.

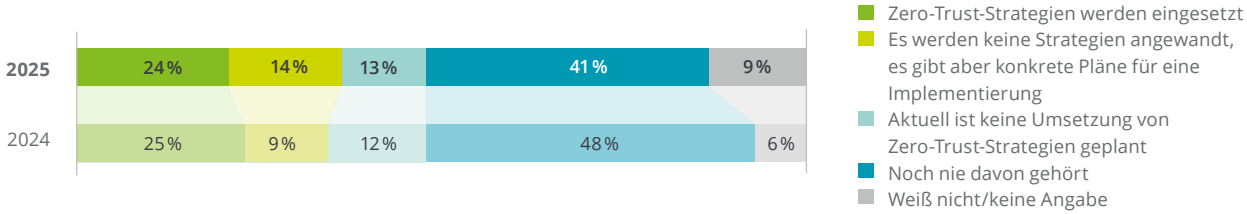
05

Zero Trust Security als effektiver Sicherheitsansatz gewinnt an Bedeutung

Das Sicherheitskonzept Zero Trust, bei dem niemandem automatisch vertraut, sondern jeder einzelne Datenzugriff verifiziert wird, gewinnt in der österreichischen Unternehmenslandschaft an Bekanntheit. Hatten im Vorjahr rund die Hälfte der Befragten noch nie von Zero Trust gehört, ist dieser Anteil in diesem Jahr um sieben Prozentpunkte gesunken. Das ist ein wichtiger Schritt in die richtige Richtung, dennoch müssen Unternehmen ihr Wissen im Bereich Zero Trust weiter ausbauen und ihre Sicherheitsstrategie anpassen um dem dynamischen Bedrohungsfeld standhalten zu können.

Erfreulich ist in diesem Zusammenhang auch, dass die Anzahl der Unternehmen, die konkrete Pläne für eine Implementierung von Zero Trust haben, von 9 % im Vorjahr auf 14 % angestiegen ist. Handlungsbedarf gibt es jedoch weiterhin: Denn der Anteil jener Unternehmen, die Zero Trust bereits einsetzen, bleibt mit einem Viertel (24 %) unverändert gering.

Zero Trust Security



Was ist Zero Trust?

Never trust, always verify: Diesem Motto folgt der Sicherheitsansatz Zero Trust. Traditionelle Strategien gehen davon aus, dass User innerhalb des Netzwerks sicher sind. Bei Zero Trust wird niemandem automatisch vertraut, sondern jeder einzelne Datenzugriff verifiziert. Die Verifizierung ist unabhängig davon, ob der Zugriff intern oder extern erfolgt.
Mit dem Konzept kann Cyber-Sicherheit auch in einem modernen, dynamischen Umfeld sichergestellt werden. Damit wird der optimale Einsatz der bestehenden Personalressourcen gewährleistet, trotz der steigenden Komplexität der Angriffe.

Deloitte Cyber Insights

In unserer Beratungspraxis konnten wir sehen, dass die Unternehmen mit konkreten Plänen im Vorjahr an der Implementierung von Zero Trust auf Herausforderungen gestoßen sind.

Die Umstellung auf Zero Trust ist für viele Unternehmen eine Herausforderung. Es braucht dafür nicht nur technische Anpassungen, sondern auch ein Umdenken in der Unternehmenskultur. Sollten Unternehmen noch nicht auf den Zero-Trust-Ansatz setzen, lautet die klare Empfehlung, sich Experteninput zu holen und das Bewusstsein sowie Verständnis für diese Sicherheitsstrategie zu fördern und umzusetzen. Auch kleinere Betriebe mit weniger Ressourcen können von diesem Ansatz profitieren.

"In einer dynamischen Bedrohungslandschaft, können wir es uns nicht mehr leisten, blind zu vertrauen. Der Zero-Trust-Ansatz ist nicht nur eine Sicherheitsstrategie, sondern eine Denkweise für das digitale Zeitalter. Indem wir niemals vertrauen, sondern immer verifizieren, schaffen wir eine robuste Verteidigung gegen die sich ständig weiterentwickelnden Bedrohungen."

Georg Schwondra | Partner | Risk Advisory

06

Hype um AI als Cyber Security Tool geht zurück

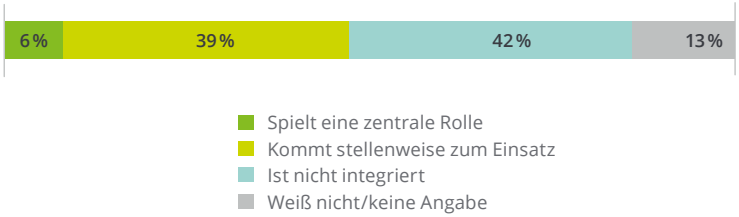
Grundsätzlich ist das Bild, das Unternehmen von Artificial Intelligence als Cyber Security Tool haben, ambivalent: Während die Hälfte der Unternehmen die neue Technologie in der Cyber Security bereits einsetzt, verzichtet die andere Hälfte noch vollständig darauf.

Doch der Hype rund um die neue Technologie im Cyber-Security-Management scheint mittlerweile wieder etwas abzuflachen. So ist die Nutzung im Vergleich zum Vorjahr in allen Bereichen zurückgegangen. Verwendeten 2024 beispielsweise noch 54 % AI bei der Phishing-Erkennung und -Prävention, ist dieser Wert mittlerweile auf 41 % gesunken. Ähnlich sieht es bei der Mitarbeiterschulung und -sensibilisierung aus: Hier hat sich der Anteil jener Unternehmen, die AI dafür nutzen, von 55 % auf 33 % verringert.

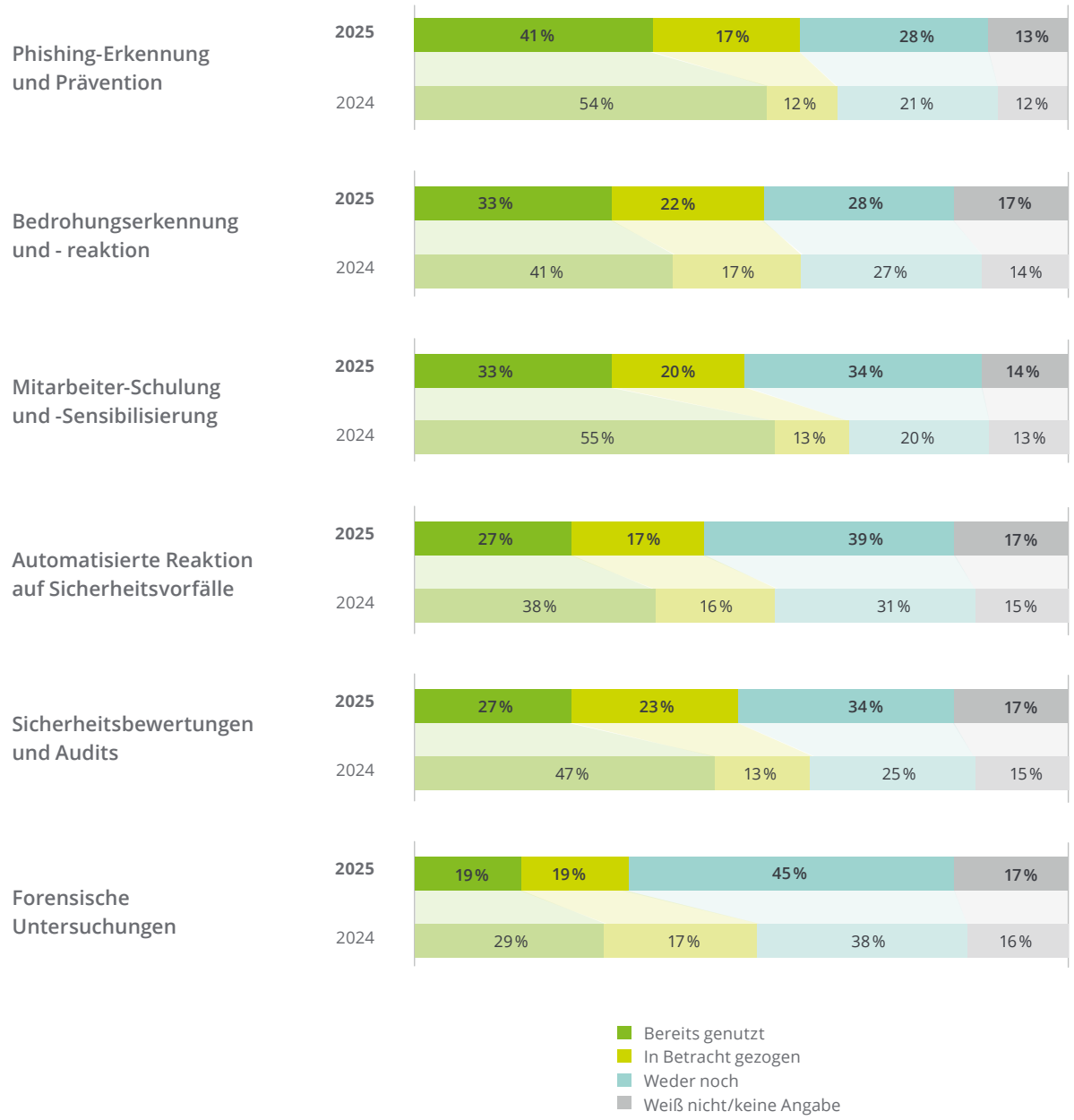
Dennoch zeigt sich, dass die Unternehmen die Potenziale von AI durchaus erkennen, aber bei der praktischen Umsetzung noch auf Hürden stoßen. Besonders auffällig ist der Rückgang im Bereich der Mitarbeiterschulung und -sensibilisierung, was darauf hindeuten könnte, dass Unternehmen wieder auf traditionelle Schulungsmethoden zurückgreifen oder AI-gestützte Lösungen als nicht ausreichend wirksam empfinden.

Zudem haben die befragten Unternehmen auch Sicherheitsbedenken – insbesondere im Zusammenhang mit generativer AI (GenAI). 37 % sind derzeit sehr oder ziemlich besorgt, dass durch den Einsatz von GenAI und damit Tools wie ChatGPT sensible Unternehmensdaten an die Öffentlichkeit kommen. Nur 16 % fühlen sich aktuell beim Einsatz von AI sicher.

Artificial Intelligence in der Cyber Security



Nutzung von AI im Cyber-Security-Management

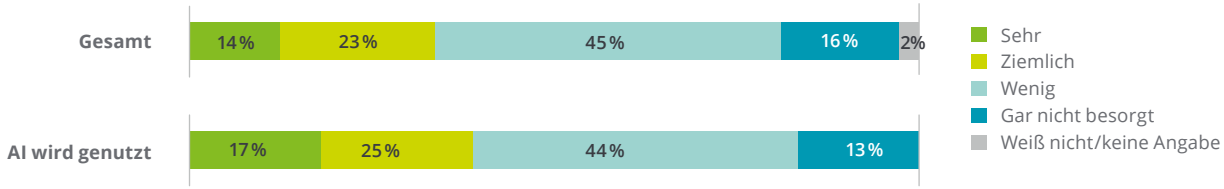


Zudem haben die befragten Unternehmen auch Sicherheitsbedenken – insbesondere im Zusammenhang mit generative AI (GenAI). 37 % sind derzeit sehr oder ziemlich besorgt, dass durch den Einsatz von GenAI und damit Tools wie ChatGPT sensible Unternehmensdaten an die Öffentlichkeit kommen. Nur 16 % fühlen sich aktuell beim Einsatz von AI sicher.

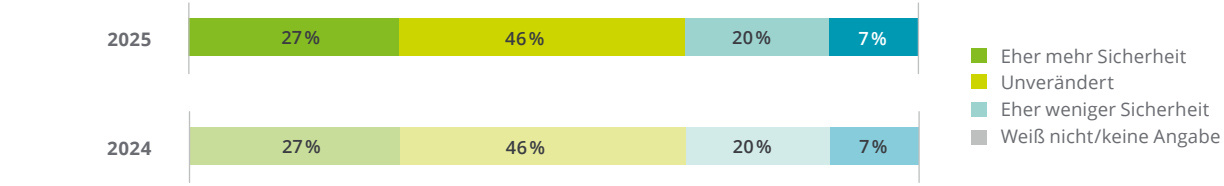
Insbesondere bei Unternehmen, die bereits auf AI setzen, besteht die Befürchtung von Datenleaks. Unternehmen, die AI noch nicht nutzen, schätzen die damit verbundenen Risiken tendenziell geringer ein. Hier besteht die Notwendigkeit, das Bewusstsein für die Sicherheitsaspekte der AI-Nutzung weiter zu schärfen und mögliche Risiken zu erkennen und aktiv zu behandeln.

Die wahrgenommenen Sicherheitslage im Hinblick auf AI bleibt konstant. Laut eigener Einschätzung gehen 27 % der Unternehmen davon aus, dass die Nutzung von Artificial Intelligence im Bereich der Cyber Security zu einer höheren Sicherheit beiträgt. 46 % der Unternehmen sind der Meinung, dass sich die Bedrohungslage durch den Einsatz von AI nicht verändert, während 20 % befürchten, dass die Bedrohungen dadurch sogar zunehmen könnten.

Sorge vor Datenleaks durch den Einsatz von generativer AI (nach Nutzung von AI in der Cyber Security)



Möglichkeiten von AI in der Cyber Security



Deloitte Cyber Insights

Obwohl die Verwendung von AI derzeit noch mit viel Unsicherheit einhergeht, kommt man um die Nutzung mittel- und langfristig nicht vorbei, um kompetitiv zu bleiben. Deshalb ist es wichtig technische Schutzmaßnahmen auszubauen und unternehmensweite Vorgaben zu definieren, um AI sicher zu nutzen und Datenleaks zu verhindern. Cyber-Kriminelle setzen selbst verstärkt auf AI, um Angriffe zu automatisieren und Sicherheitsmaßnahmen zu umgehen. Diese Entwicklung verdeutlicht, dass Unternehmen AI sowohl als Schutzmechanismus einsetzen, als auch ihre Sicherheitsstrategien an die neuen Bedrohungen durch AI-basierte Angriffe anpassen müssen.

„Unsere praktischen Erfahrungen zeigen: AI hat das Potenzial zu einem Kernelement einer dynamischen und adaptiven Cyber-Sicherheitsstrategie zu werden, die es uns ermöglicht, auf die ständig wachsende Komplexität und Geschwindigkeit von Cyber-Angriffen entsprechend zu reagieren.“

Karin Mair | Managing Partner | Consulting

07

Handlungsempfehlungen

Business Continuity Management (BCM) stetig anpassen

Im Sinne einer umfassenden und effizienten Cyber-Security-Strategie sollten Unternehmen auf die regelmäßige Überprüfung und Anpassung der BCM-Pläne achten. Nur so können sie sich für die ständig verändernde Bedrohungslandschaft wappnen und kritische Geschäftsprozesse auch im Notfall aufrechterhalten. Dadurch wird die Resilienz des Unternehmens erhöht und potenzielle Ausfallzeiten werden reduziert.

Vorfallsmanagement implementieren

Ein gut durchdachtes und koordiniertes Vorfallsmanagement stellt sicher, dass Sicherheitsvorfälle schnell erkannt, analysiert und effektiv gehandhabt werden können. Ein solcher Prozess umfasst die sofortige Identifizierung und Isolierung der betroffenen Systeme, die Benachrichtigung der relevanten Stakeholder und die Anwendung vordefinierter Maßnahmen zur Eindämmung und Behebung des Vorfalls.
Um im Ernstfall einen koordinierten und effektiven Einsatz zu ermöglichen, empfehlen wir zudem die Zusammenstellung eines spezialisierten Incident-Response-Teams, das definierte Rollen sowie Verantwortlichkeiten hat und regelmäßig geschult wird.

Notfallübungen und Tests durchführen

Um die Reaktionsfähigkeit im Falle eines Angriffs zu überprüfen und zu verbessern, ist die Durchführung regelmäßiger Notfallübungen ratsam. Solche Übungen fördern das Vertrauen in die Krisenmanagementfähigkeiten des Unternehmens – sowohl seitens externer Stakeholder als auch seitens der Mitarbeitenden.
Sinnvoll in diesem Zusammenhang sind vor allem Simulationen verschiedener Angriffsszenarien – von ausschließlich physischen bis hin zu rein digitalen Angriffen – um die Effizienz der Reaktionspläne zu testen. Damit werden Schwachstellen in den bestehenden Plänen frühzeitig identifiziert und können entsprechend behoben werden.

Backups und Wiederherstellungspläne testen

Die regelmäßige Prüfung von Backups und Backup-Prozessen zur Sicherstellung der Integrität und Verfügbarkeit von Daten ist unerlässlich. Dabei wird garantiert, dass die Daten im Ernstfall nicht nur vorhanden, sondern auch aktuell und vollständig sind und die Wiederherstellung reibungslos verläuft.
Gleichzeitig müssen auch die Wiederherstellungsprozesse kontinuierlich überprüft werden, sodass im Notfall die Datenwiederherstellung schnell und vollständig funktioniert. Effiziente Wiederherstellungsprozesse sind entscheidend, um betriebliche Kontinuität zu gewährleisten.

Sicherheitsbudgets an steigenden Bedrohungen ausrichten

Cyber-Sicherheit ist ein fortlaufender Prozess. Die laufende Beobachtung der sich wandelnden Bedrohungslandschaft und die regelmäßige Anpassung der Sicherheitsstrategien und -budgets sind daher das A und O. Zudem braucht es Investitionen in fortschrittliche Sicherheitslösungen und die Ausbildung von Fachkräften, um aktuellen Bedrohungen entgegenzuwirken. Vor allem qualifiziertes Personal ist ein entscheidender Faktor für die Umsetzung und Wirksamkeit von Sicherheitsmaßnahmen.

Sicherheitsaspekte der AI-Nutzung erkennen

Um AI auch im Bereich der Cyber Security sicher und effizient einsetzen zu können, ist die Entwicklung und Implementierung einer eigenen Richtlinie notwendig, die den sicheren Einsatz und die Verwendung der neuen Technologie regelt. Sie hilft dabei, Missbrauch, Sicherheitslücken und Missverständnisse zu reduzieren. Darunter fällt beispielsweise die Bereitstellung eigener, eventuell selbst gehosteter AI-Tools. Das beugt eventuellen Datenleaks vor und verhindert, dass Mitarbeitende unbewusst die zuvor definierte Richtlinie verletzen. Die Erstellung einer solchen Richtlinie erfordert jedoch nicht nur die entsprechenden Ressourcen seitens der Unternehmen, auch die Politik ist gefragt, um die passenden Rahmenbedingungen vorzugeben.
Um eine sicherheitsbewusste Unternehmenskultur zu ermöglichen, sollten außerdem regelmäßige Awareness-Maßnahmen für Mitarbeitende in Bezug auf Risiken und Sicherheitsaspekte der AI-Nutzung durchgeführt werden.

08 Fazit

Österreichs Unternehmen haben die Bedeutung von Cyber Security mittlerweile nicht nur erkannt, sondern auch ihre Maßnahmen entsprechend implementiert und ausgerichtet. Mit dem Aufkommen von AI tut sich derzeit aber ein neues Bedrohungsfeld auf, auf das die Verantwortlichen mit einer entsprechenden Sicherheitsstrategie reagieren müssen. Vor allem der Einsatz des Zero-Trust-Ansatzes ist in diesem Zusammenhang ein wichtiger Schlüssel zu einer effizienteren Cyber Security, der von den Unternehmen stetig mehr Anerkennung erfährt.

Auch der stetigen Anpassung der Security-Budgets sowie der regelmäßigen Durchführung von Notfallübungen und Tests kommt eine zentrale Bedeutung zu, um Cyber-Angriffe nicht nur zu erkennen und abzuwehren, sondern im Fall des Falles auch rasch und vor allem zielgerichtet darauf reagieren zu können. Unternehmen sollten sich jedenfalls bewusst sein, dass Cyber Security kein abgeschlossener Prozess ist, sondern die stetige Beobachtung der Bedrohungslage und eine flexible Reaktion darauf verlangt.

Unternehmen müssen den aktuellen Herausforderungen entschlossen gegenübertreten, um die Cyber-Risiken zu managen und um langfristig wettbewerbsfähig zu bleiben.

Methode & Sample

Zielpopulation:
Mittel- und Großunternehmen in Österreich
(ab 50 Beschäftigte)

Erhebungsmethode:
Standardisierte Telefonbefragung (CATI)

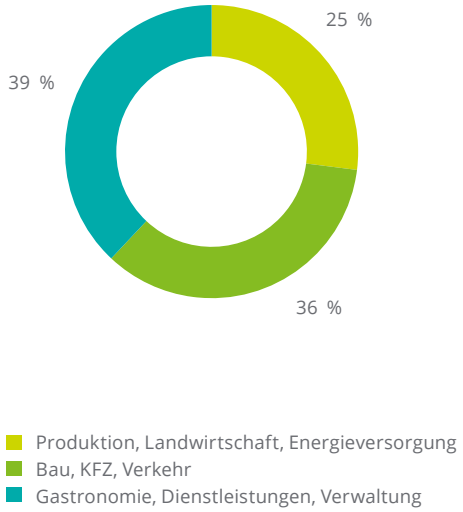
Befragungszeitraum:
Jänner und Februar 2025

Stichprobe:
350 Unternehmen

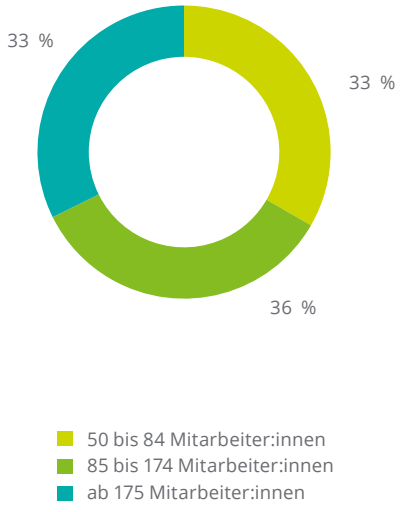
Gewichtung:
Nach Anzahl der Mitarbeiter:innen und Region

Hinweis:
Geringfügige Abweichungen von Sollwerten (z.B. 99 % oder 101 % statt 100 %) sind auf Rundungseffekte zurückzuführen.

Branche



Unternehmensgröße



Kontakt

Karin Mair
Managing Partner | Consulting

+43 1 537 00-4840
kmair@deloitte.at

Georg Schwondra
Partner | Risk Advisory

+43 1 537 00-3760
gschwondra@deloitte.at

Impressum

Herausgegeben von:
Deloitte Consulting GmbH

Autor:innen:
Karin Mair / Deloitte, Georg Schwondra / Deloitte, Christoph Hofinger / Foresight

Unter redaktioneller Mitarbeit von:
Maria Hofer, Armin Nowshad und Theresa Kopper

Grafik und Layout:
Silja Andrej, Claudia Hussovits

Deloitte.

Gesellschaftssitz Wien | Handelsgericht Wien | FN 212552 b