Deloitte.

Deloitte Cyber Security Report 2024

Der Einfluss von Artificial Intelligence auf die Cybersicherheit österreichischer Unternehmen: Warum man jetzt auf Zero Trust setzen sollte.

Eine Studie von Deloitte Österreich in Kooperation mit Foresight

MAKING AN IMPACT THAT MATTERS since 1845

Inhalt

01

Vorwort

Laufend wird in den Medien über Cyber-Attacken und die Einführung strengerer Vorschriften im Bereich der Cyber-Sicherheit berichtet. Dadurch hat das Bewusstsein hinsichtlich Cyber Security in Unternehmen deutlich zugenommen. Die strengeren Vorschriften und die neue EU-Gesetzgebung (NIS 2, AI Act, DSGVO, DORA und Cyber Resilience Act) tragen einen beträchtlichen Teil zur gestiegenen Awareness bei. Angesichts der zunehmenden Komplexität und wechselseitigen Abhängigkeiten digitaler Systeme bleiben Unternehmen aber weiterhin vulnerabel für Cyber-Angriffe.

Vor allem die rasante Entwicklung von Artificial Intelligence (AI) bringt neben Chancen auch Risiken im Bereich Cyber Security mit sich. Einerseits bietet die neue Technologie fortschrittliche Analysefähigkeiten, die Unternehmen dabei unterstützen können, potenzielle Bedrohungen frühzeitig zu erkennen und proaktiv darauf zu reagieren. Andererseits können Angriffe durch AI automatisiert und verschleiert werden. Das stellt herkömmliche Sicherheitsmaßnahmen vor völlig neue Herausforderungen.

Doch wie gut sind Österreichs Unternehmen auf die zunehmend professionellen Ransomware-Angriffe vorbereitet? Und wie beeinflussen die Möglichkeiten der AI den Umgang mit dem Thema Cyber-Sicherheit? Diese und weitere Fragen beantworten wir in unserem jährlichen Cyber Security Report. Gemeinsam mit dem Forschungsinstitut Foresight wurden insgesamt 350 österreichische Unternehmen ab 50 Beschäftigten zu ihrer Einschätzung in diesem Bereich befragt.

Wir wünschen eine spannende Lektüre!

Karin Mair | Georg Schwondra | Christoph Hofinger

Karin Mair
Managing Partner |
Risk Advisory & Financial Advisory

Georg Schwondra
Partner | Risk Advisory

Christoph Hofinger
Geschäftsführer | Foresight

02

Key Findings

Awareness und Technik verhindern Datenverschlüsselung

Ransomware-Attacken werden immer effizienter und professioneller. Trotzdem ist die Zahl der Angriffe, die zu Datenverschlüsselungen führen, im Vergleich zu 2022 um mehr als die Hälfte gesunken. Die technischen Infrastrukturmaßnahmen sind für diese Entwicklung nicht alleinig ausschlaggebend: Sie verhindern nur noch in 34 % der Fälle die Ausbreitung der Attacken – im Jahr 2022 waren es noch 76 %. Der Grund für die sinkende Zahl der Verschlüsselungen kann in einer erhöhten Mitarbeiter:innen-Awareness liegen. Regelmäßige Schulungen und Tests für Mitarbeiter:innen stärken die Awareness und tragen dazu bei, dass Angriffe rasch an die richtigen Stellen im Unternehmen gemeldet werden. Diese können frühzeitig Maßnahmen gegen Cyberangriffe setzen und schwerwiegende Folgen, wie Datenverschlüsselungen, verhindern.

AI als Chance und Risiko

Mehr als die Hälfte der befragten österreichischen Unternehmen hat Artificial Intelligence (AI) bereits in ihre Sicherheitssysteme integriert – Tendenz steigend. Somit ist die neue Technologie ein wachsender Bestandteil der Cyber Security der Betriebe. Gleichzeitig wird auch das Risiko von AI in den Händen von Angreifer:innen von mehr als der Hälfte der Unternehmen als ziemlich oder sehr hoch eingestuft.

Hohe Effizienz bei Datenverschlüsselung

Ransomware Angriffe werden zunehmend professioneller und dynamischer. Technische Maßnahmen können damit häufig nicht entsprechend Schritt halten. Kommt es im Zuge eines Ransomware-Angriffs zur Datenverschlüsselung, können die Daten 2024 nur noch in 17 % der Fälle entschlüsselt werden. Zum Vergleich: 2022 waren es noch 37 %. Ähnlich verhält es sich bei der Wiederherstellung durch Backups. Konnten 2022 noch 59 % der Daten nach einer Verschlüsselung wiederhergestellt werden, sind es aktuell nur noch 28 %. Umso wichtiger ist es, Angriffsversuche frühzeitig zu erkennen und Gegenmaßnahmen einzuleiten.

Optimierungspotenzial beim Zero-Trust-Ansatz

Die technischen Grundsysteme in Unternehmen werden immer vernetzter. Ein traditioneller, statischer Ansatz ist nicht mehr in der Lage, ausreichend für Cyber-Sicherheit zu sorgen. Deshalb gehört Zero Trust mittlerweile zu den führenden Konzepten im Bereich Cyber Security. Mit diesem Ansatz können Unternehmen Cyber-Risiken proaktiv managen. Das Problem dabei: 48 % der befragten Unternehmen haben bislang noch nie von Zero Trust Security gehört.

03

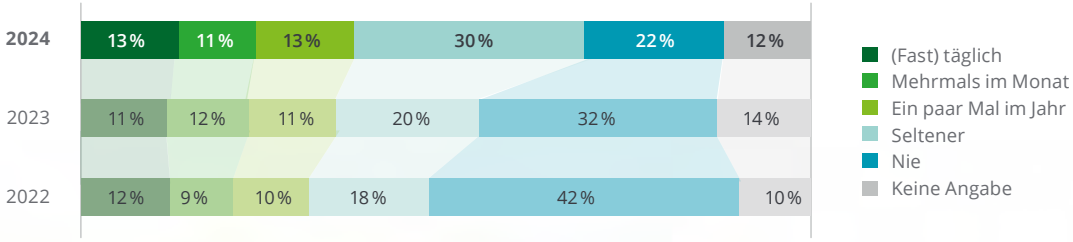
Cyber Awareness und Professionalität der Angriffe steigen

Die Mehrheit der österreichischen Unternehmen fühlt sich hinsichtlich der Sicherheit ihrer Daten und IT-Systeme gut aufgestellt: So geben 65 % der Befragten an, dass ihre Daten und IT-Systeme absolut oder sehr sicher sind.

Der Anteil jener Unternehmen, bei denen es noch nie zu einem Ransomware-Angriff gekommen ist, hat im Vergleich zum Vorjahr um 10 % abgenommen. Bei steigender Häufigkeit und trotz erhöhter Professionalität der Angriffe sind sich immer mehr Unternehmen der Ransomware-Attacken bewusst. Die Einschätzung, gar nicht von Ransomware-Attacken betroffen zu sein, hat sich im Vergleich zu 2022 nahezu halbiert.

Bereits im letzten Jahr hat der Krieg in der Ukraine die Cyber-Sicherheit von mehr als der Hälfte der Unternehmen negativ beeinflusst. Dieses Jahr melden 45 % der Unternehmen, dass die Bedrohungen durch die globalen Konflikte weiter zugenommen haben, für 7 % der Befragten sogar sehr stark.

Häufigkeit von Ransomware-Attacken



Deloitte Cyber Insights

Unsere Beratungspraxis zeigt, dass viele Unternehmen durch bisher getätigte Investitionen über gute Sicherheits-standards verfügen. Aufgrund der stark dynamischen Weiterentwicklung braucht es jedoch laufend weitere Maßnahmen zur Optimierung und Verbesserung der Systeme sowie Absicherung der Daten. Nur so ist es möglich, adäquat auf Cyber-Angriffe vorbereitet zu sein und im Ernstfall schnell und richtig zu reagieren.

„Wir beobachten die Einstellungen zu Cyber-Risiken schon seit vielen Jahren. Typisch ist, dass es bei Entscheidungsträger:innen einige Jahre braucht, bis bestehende Bedrohungen auch in den Köpfen ankommen."

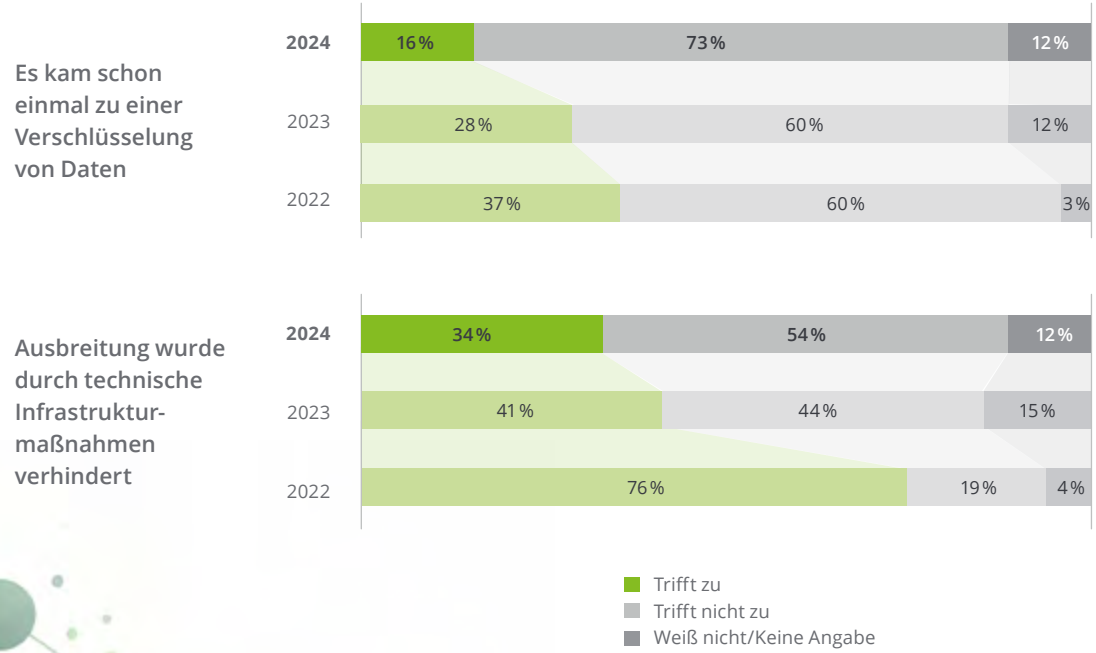
Christoph Hofinger | Geschäftsführer | Foresight

Awareness und Technik verhindern Datenverschlüsselung

Obwohl die Ransomware-Attacken effizienter und zielgerichteter geworden sind, zeigen die Daten der aktuellen Umfrage, dass es bei den Angriffen immer seltener zu einer Datenverschlüsselung kommt: Wurden im Jahr 2022 noch 37 % der Daten verschlüsselt, sind es aktuell 16 %.

Allerdings verhindern technische Infrastrukturmaßnahmen die Ausbreitung von Ransomware-Attacken in nur 34 % der Fälle. Im Vergleich dazu waren es 2022 noch 76 %.

Auswirkungen von Ransomware-Attacken



Deloitte Cyber Insights

Wie hängt die Abnahme von Datenverschlüsselungen und die geringere Wirksamkeit von technischen Infrastrukturmaßnahmen zusammen? Unsere Beratungspraxis zeigt: Das Bewusstsein von Mitarbeiter:innen ist einer der wichtigsten Wege, um Angriffe, die Verschlüsselung von Daten zur Folge haben, zu erkennen. Für Unternehmen ist es daher essenziell, ihre Mitarbeiter:innen regelmäßig zu schulen, Anzahl und Qualität der Schulungen sind für den Erfolg ausschlaggebend. Die Inhalte müssen kontinuierlich weiterentwickelt werden. Das erlernte Wissen muss laufend in der Praxis getestet werden, um die Awareness zu stärken.

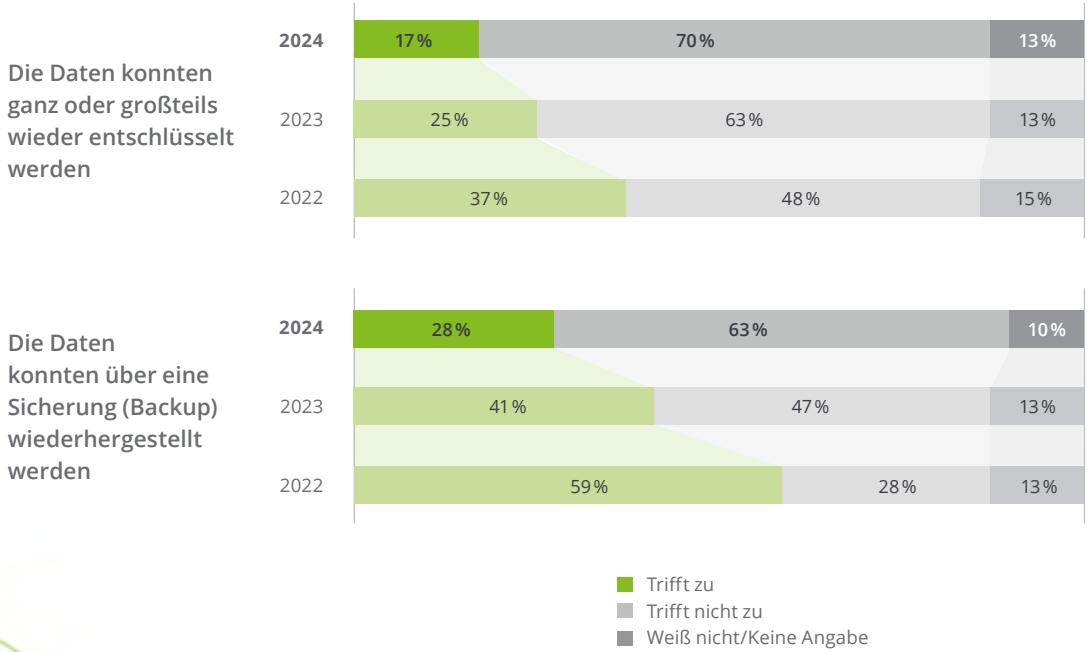
„Neben Cyber-Hygienemaßnahmen können Phishing-Kampagnen, Mitarbeiter:innenschulungen und gut eingestellte Sicherheitssysteme, wie auch E-Mailfilter, die Wahrscheinlichkeit von erfolgreichen Ransomware-Attacken deutlich verringern."

Georg Schwondra | Partner | Risk Advisory

Hohe Effizienz bei Datenverschlüsselung

Unternehmen, deren Daten in Folge eines Angriffs verschlüsselt wurden, können diese aktuell deutlich seltener entschlüsseln beziehungsweise über eine Sicherung wiederherstellen als in den vergangenen zwei Jahren. Wurden 2022 und 2023 noch in 37 % beziehungsweise 25 % der Fälle die Daten entschlüsselt, waren es 2024 nur noch 17 %. Ebenso sind die Fälle, in denen die Daten durch ein Backup wiederhergestellt werden konnten, von 59 % im Jahr 2022 beziehungsweise 41 % im Jahr 2023 auf 28 % in diesem Jahr gesunken.

Umgang mit Ransomware-Attacken



Deloitte Cyber Insights

Insgesamt erholen sich Unternehmen schwerer von Datenverschlüsselungen oder -verlusten. Ursache dafür ist besonders die steigende Professionalität der Ransomware-Angriffe. Der Schlüssel zur Vermeidung von Ransomware-Angriffen liegt dabei in einer professionellen Angriffsprävention. Dazu gehört ein geschärftes Sicherheitsbewusstsein bei Mitarbeiter:innen, damit diese verdächtige E-Mails, Links oder Anhänge frühzeitig erkennen. Ebenso können Risiko-Assessments mögliche technische Schwachstellen im Unternehmen aufzeigen, welche unverzüglich geschlossen werden sollten. Softwaregestützte Angriffsdetektion vermittelt ein Bild von potenziellen Attacken und ermöglicht somit eine rasche Reaktion. Eine robuste Datensicherung ist essenziell, um im Ernstfall jederzeit auf unternehmensrelevante Daten zugreifen zu können und so Datenverluste zu minimieren.

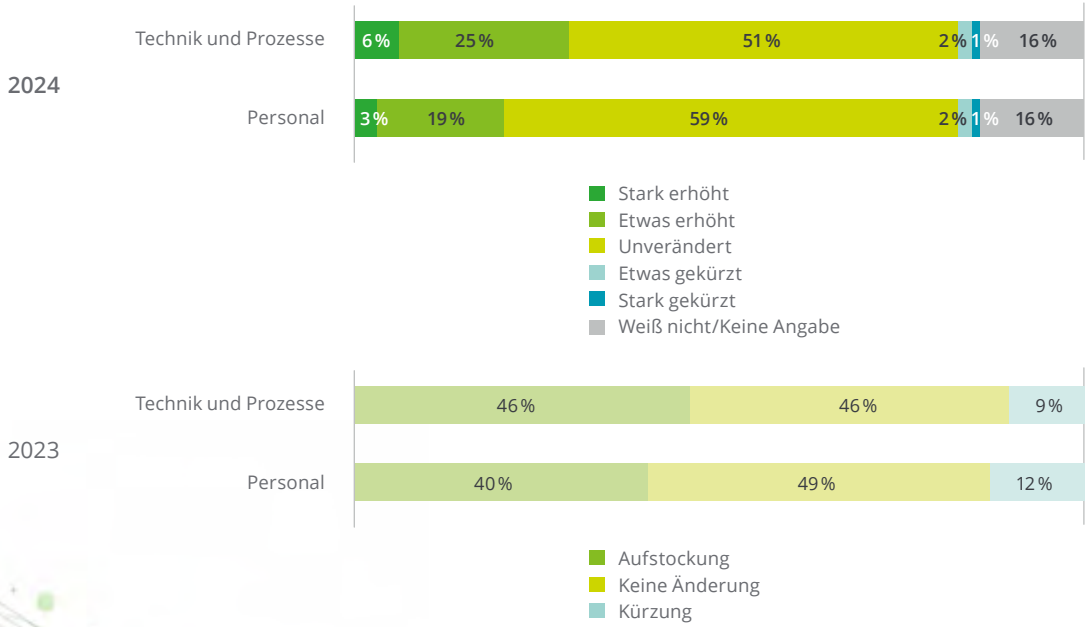
„Ein proaktives Business Continuity Management (BCM) mit getesteten Krisen- und Notfallplänen ist entscheidend, um im Cyber-Ernstfall entsprechend reagieren zu können. Ähnlich wie bei Brandschutzübungen sollte auch für einen Cyber-Angriff regelmäßig mit allen relevanten Stakeholdern trainiert werden."

Karin Mair | Managing Partner | Financial Advisory & Risk Advisory

Budgetäre Anpassungen an neue Bedrohungslage bleiben aus

2023 haben die Unternehmen verstärkt in Cyber Security investiert. Bei der diesjährigen Umfrage gibt mehr als die Hälfte der Befragten an, keine Änderungen des Security Budgets für 2024 geplant zu haben. Es gibt aber auch kaum Unternehmen, die beim Security Budget sparen wollen. 31 % der Befragten haben das Budget für Technik und Prozesse (stark) erhöht, 22 % investieren vermehrt in personelle Ressourcen. Angesichts der steigenden Bedrohungen gibt es hier dennoch Investitionsbedarf.

Budgetveränderungen



Deloitte Cyber Insights

Unserer Einschätzung nach bilden die geplanten Investitionen das nötige Budget für die Bedrohung durch Ransomware-Attacken nicht entsprechend ab. Was Unternehmen aktuell noch nicht ausreichend in ihren Budgets berücksichtigen, sind die steigenden regulatorischen Anforderungen und die Herausforderungen durch AI.

Unsere Empfehlung

Prüfen Sie, ob und wie Ihr Unternehmen von aktueller/ neuer EU-Gesetzgebung (NIS 2, AI Act, DSGVO, DORA und Cyber Resilience Act) betroffen ist und bereiten Sie sich auf die Umsetzung und Einhaltung vor. Teamübergreifendes Zusammenwirken (ausreichende sowie richtige Ressourcen im Unternehmen) sowie entsprechende budgetäre Vorkehrungen sind das Fundament für eine professionelle Implementierung. Cyber Security ist stets holistisch zu betrachten. Neben der Prävention, Detektion und Abwehr von Ransomware-Attacken und dem Umgang mit den neuen Sicherheitsrisiken aufgrund von AI sollte die Umsetzung neuer Regularien in ein umfassendes Cyber-Konzept integriert sein.

„Viele Unternehmen haben noch keine ausreichenden Maßnahmen zur NIS 2 Implementierung getroffen und sind damit nicht entsprechend vorbereitet. Dies ist insofern kritisch, da die NIS 2-Richtlinie bereits am 17. Oktober 2024 in Kraft tritt."

Karin Mair | Managing Partner | Financial Advisory & Risk Advisory

04

Verifizieren statt Vertrauen: Zero Trust noch wenig bekannt

Traditionelle Sicherheitskonzepte können mit den steigenden Herausforderungen im Bereich Cyber-Sicherheit nur mehr schwer Schritt halten. Ein Viertel der Unternehmen setzt dementsprechend schon auf eine Zero-Trust-Strategie, bei der jeder einzelne Datenzugriff verifiziert wird. Weitere 9 % haben zudem konkrete Pläne zur Implementierung des Sicherheitskonzepts.

Gleichzeitig zeigen die Zahlen aber auch, dass der neue Ansatz noch nicht flächendeckend in der Unternehmenslandschaft etabliert ist. Fast die Hälfte aller Befragten hat noch gar nicht von Zero Trust Security gehört. 12 % planen derzeit auch keine Umsetzung.

Zero Trust Security

- Zero-Trust-Strategien werden eingesetzt
- Es werden keine Strategien angewandt, es gibt aber konkrete Pläne für eine Implementierung
- Aktuell ist keine Umsetzung von Zero-Trust-Strategien geplant
- Noch nie davon gehört
- Weiß nicht/keine Angabe

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 steigender Komplexität der Angriffe.

„Zero Trust gehört zu den zukunftsweisenden Konzepten im Cyber-Security-Bereich. Prüfen Sie für Ihr Unternehmen, wie Sie Zero Trust anwenden können, um bestmöglich gegen Cyber-Angriffe geschützt zu sein. Auch kleinere Betriebe mit weniger Ressourcen können von diesem Ansatz profitieren."

Georg Schwondra | Partner | Risk Advisory

Zero Trust | The Evolution of Cyber

1980 — 1990 — Today — Tomorrow

Perimeter Security

Information assets protected by perimeters and physical security controls

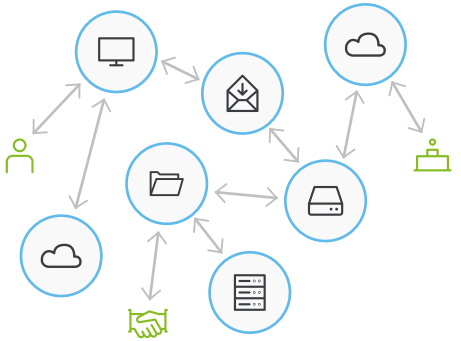
Defense in Depth

Breakouts created for internet access and communication, control by layered logical security controls. More perimeters – North/South protection

Hybrid Cyber

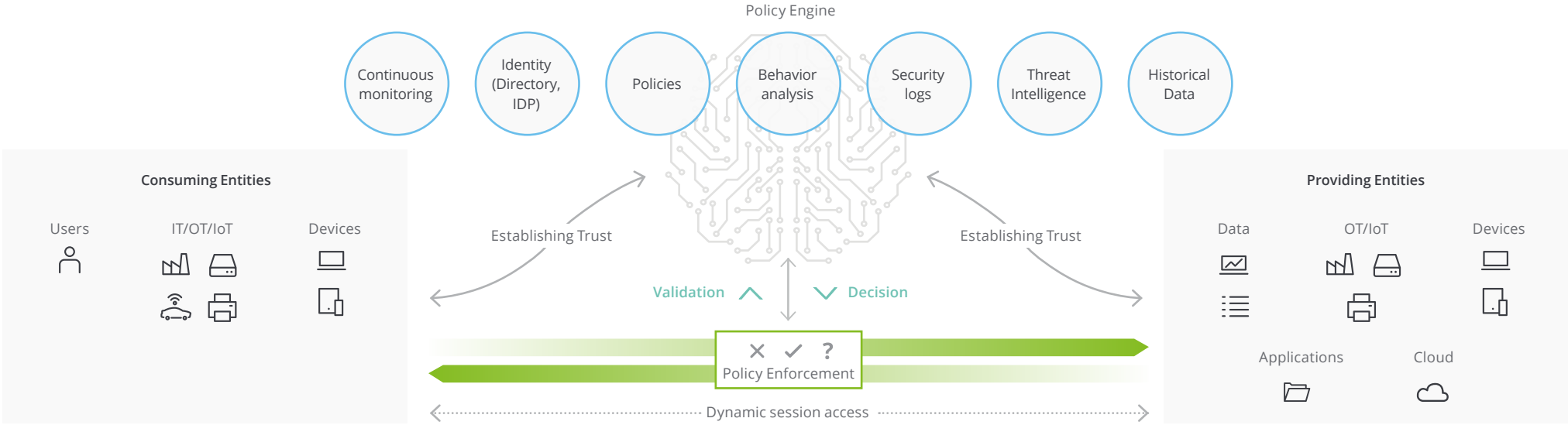
Increased number of breakouts to support hybrid environments (e.g. Cloud/SaaS) and increased reliance on monitoring. East/West protection

Zero Trust Cyber Security



Network perimeter has been removed. Trust is established for every interaction and constantly revalidated

How does Zero Trust work?



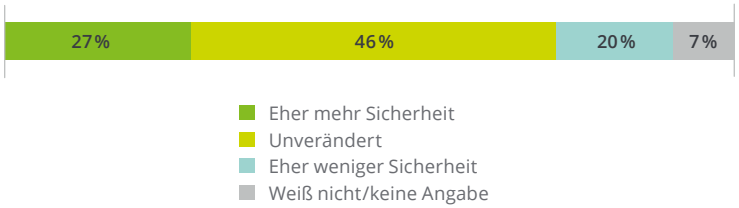
05

AI vs. AI – Artificial Intelligence als Chance und Risiko

Artificial Intelligence (AI) hat im vergangenen Jahr einen regelrechten Boom erlebt. Vor allem die rasanten Fortschritte bei generativer AI eröffnen spannende Möglichkeiten auf allen Ebenen. Zugleich birgt der niederschwellige Zugang auf beruflichen und privaten Endgeräten aber auch ein nicht zu unterschätzendes Sicherheitsrisiko für Unternehmen.

Die befragten Unternehmen jedenfalls sind hinsichtlich der von AI ausgehenden Möglichkeiten und Risiken im Bereich Cyber Security zwiegespalten. Während 27 % denken, dass die Technologie mehr Cyber-Sicherheit bringen wird, erwarten 20 %, dass durch AI die Gefahren weiter steigen. 46 % der Unternehmen gehen davon aus, dass sich Risiken und Möglichkeiten langfristig ausgleichen und der fortschreitende Einsatz von AI keine Änderungen in der Cyber Security bringt.

Möglichkeiten von AI in der Cyber Security



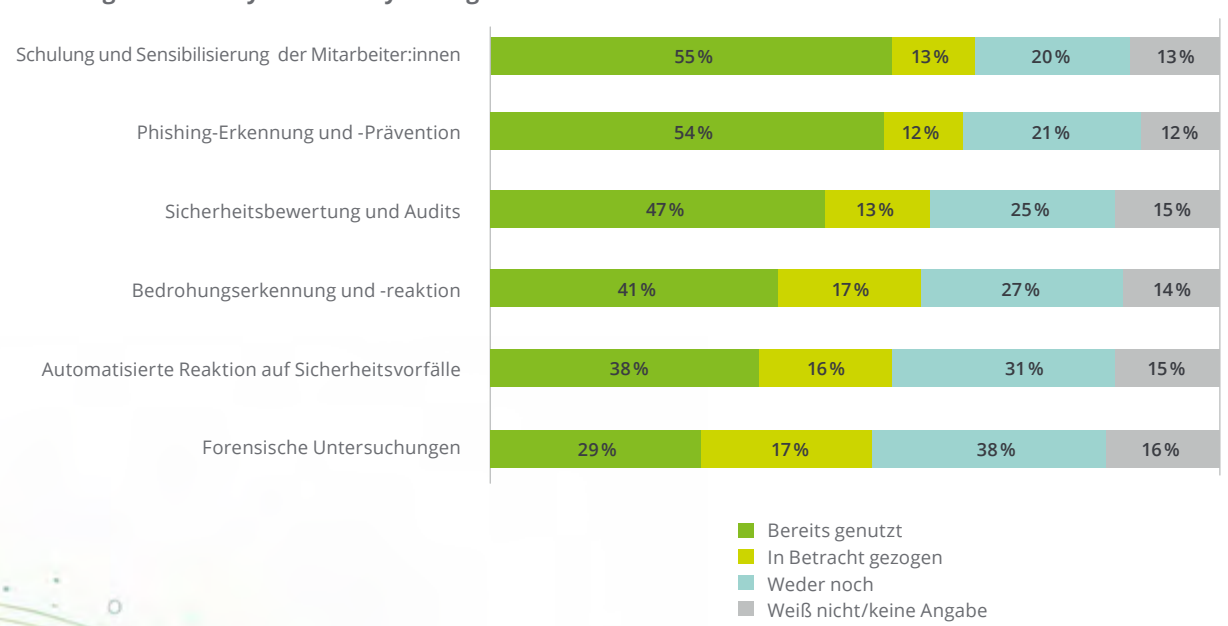
„Noch haben vergleichsweise wenig Unternehmen Cyber-Risiken mit AI in Verbindung gebracht. Wir vermuten, dass AI für viele zwar als praktisches Werkzeug wahrgenommen wird, jedoch werden im Laufe der kommenden Jahre viele mit den spezifischen Cyber-Risiken von AI konfrontiert sein, die im Augenblick noch wenig gesehen werden."

Christoph Hofinger | Geschäftsführer | Foresight

Nutzung von AI im Cyber Security Management

Das Nutzungspotenzial von AI im Cyber Security Management wird von den befragten Unternehmen als sehr vielversprechend bewertet. Der Großteil gibt an, dass AI bereits eine zentrale Rolle bei ihren Cyber-Security-Maßnahmen spielt.

So verwenden 55 % der teilnehmenden Unternehmen AI bereits zur Schulung und Sensibilisierung ihrer Mitarbeiter:innen. 54 % nutzen sie zur Phishing-Erkennung und -Prävention, 47 % zur Sicherheitsbewertung sowie Audits und 41 % zur Bedrohungserkennung und -reaktion. 38 % der Unternehmen geben zudem an, mit AI automatisiert auf Sicherheitsvorfälle zu reagieren. 29 % führen forensische Untersuchung mit AI durch.



Deloitte Cyber Insights

Die Ergebnisse unserer Umfrage zeigen die hohe Geschwindigkeit, mit der Hersteller AI in ihre Sicherheitsprodukte integriert haben. Damit wird die Technologie zu einem essenziellen Element der Cyber Security Strategy für österreichische Unternehmen. Für rund die Hälfte der Befragten ist AI bereits integraler Bestandteil ihrer Cyber-Security-Systeme. Damit ist evident: Unternehmen haben das große Cyber-Sicherheitspotenzial von AI erkannt.

Unsere Empfehlung

Vor der Implementierung von AI sollten Sie unbedingt sicherstellen, dass diese regelkonform und transparent eingesetzt wird. So wird vermieden, dass die AI selbst zur Sicherheitslücke wird oder gegen geltende Regularien (z.B. NIS 2, AI Act, DSGVO, DORA und Cyber Resilience Act) verstößt. Führen Sie vor einem flächendeckenden AI-Einsatz Tests & Assessments durch, um zu untersuchen, wie Daten verwendet, abgespeichert und gesichert werden, um möglichem Missbrauch vorzubeugen.

Speichern vs. Sichern

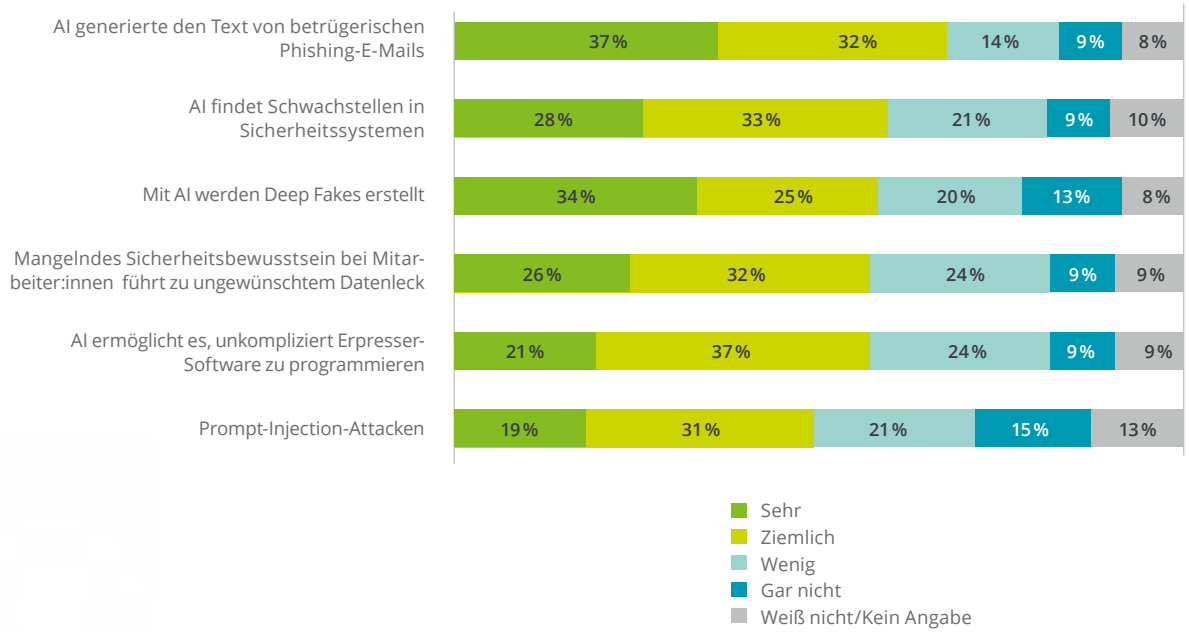
Speichern ist der Vorgang, bei dem Daten auf einem Speichermedium, wie Festplatten, SSDs, oder in der Cloud, abgelegt werden, um Informationen für die zukünftige Nutzung verfügbar zu machen. Beim Sichern von Daten handelt es sich um die Umsetzung von Sicherheitsmaß-nahmen wie regelmäßigen Backups, Verschlüsselungen, Zugriffskontrollen und anderen Sicherheitsrichtlinien. Es zielt darauf ab, die Integrität, Verfügbarkeit und Vertraulichkeit der gespeicherten Daten zu gewährleisten.

AI als Tool für Cyber Crime

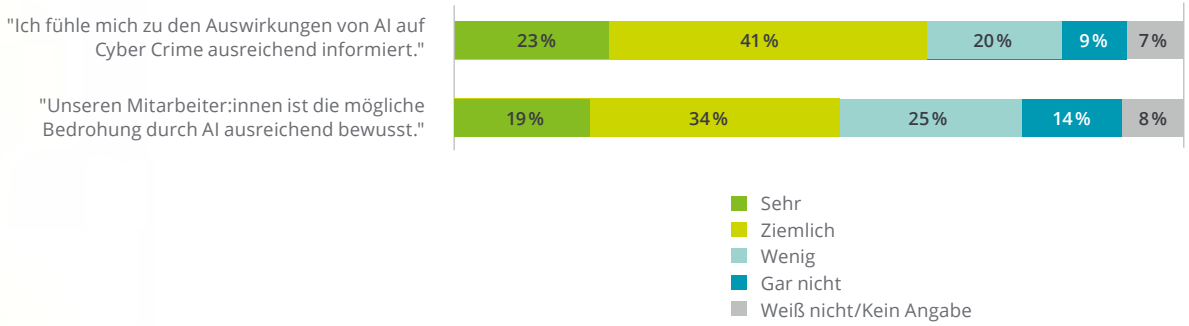
Nicht nur Unternehmen, sondern auch Angreifer:innen haben das Potenzial von AI erkannt. Am größten wird die Gefahr, die von AI im Kontext der Cyber-Kriminalität ausgeht, im Verfassen von betrügerischen Phishing-E-Mails gesehen. Mehr als die Hälfte der Befragten schätzt außerdem das mangelnde Sicherheitsbewusstsein ihrer Mitarbeiter:innen hinsichtlich der AI-gestützten Risikoszenarien als wesentlichen Gefahrenfaktor ein.

Die Cyber-Awareness ihrer Mitarbeiter:innen bewerten die Befragten unterschiedlich: Rund die Hälfte geht davon aus, dass ihren Angestellten die mögliche Bedrohung durch AI ausreichend bewusst ist. 64 % der teilnehmenden Unternehmen fühlen sich außerdem sehr gut oder ziemlich gut über die Auswirkungen von AI auf Cyber Crime informiert.

AI und Cyber Crime



Aussagen zu AI und Cyber Crime



Deloitte Cyber Insights

Aus unserer Erfahrung wissen wir, dass sich die von AI ausgehenden Gefahren dynamisch entwickeln, und in der Cybersicherheitsstrategie von Unternehmen nicht immer ausreichend berücksichtigt werden. Eine umfassende Cyberstrategie sollte daher explizit die Risiken durch AI adressieren. Um auf die sich ständig ändernde Bedrohungslage adäquat vorbereitet zu sein, ist es ebenso von zentraler Bedeutung, dass die Cyber-Abwehr laufend angepasst wird.

„Regelmäßige Cyber Security Assessments helfen den Status quo zu bewerten sowie Sicherheitslücken zu identifizieren und entsprechend zu schließen."

Georg Schwondra | Partner | Risk Advisory

06

Handlungsempfehlungen

Laufende Weiterentwicklung der Cyber Security

Aktuelle Prognosen weisen darauf hin, dass die Professionalität der mit AI unterstützten Cyber-Angriffe weiter ansteigen wird. Um sich effizient zu schützen, müssen Unternehmen ihre Cyber Security an die veränderte Sicherheitslandschaft anpassen. Dafür braucht es Investitionen in die Verbesserung der Infrastruktur und die laufende Aktualisierung technischer Maßnahmen. Zero-Trust-Mechanismen, wie z.B. eine Multifaktor-Authentifizierung, schützen Ihre Unternehmensdaten, Anwendungen und Infrastruktur effektiver als traditionelle Sicherheitsansätze. Ransomware-sichere und regelmäßig getestete Backups wiederum erhöhen die Chancen, dass Daten im Falle einer Verschlüsselung wiederhergestellt werden können.

Regelmäßige Schulungen und Sensibilisierung von Mitarbeiter:innen

Die verringerte Wirksamkeit technischer Infrastrukturmaßnahmen bei Ransomware-Attacken rücken die Bedeutung von Cyber Awareness in den Mittelpunkt. Regelmäßige Schulungen, Trainings und Sensibilisierung der Mitarbeiter:innen für Cyber-Bedrohungen, sicheres Verhalten beim Benutzen von Unternehmensressourcen sowie Notfall- und Krisenpläne sind essenzielle Präventionsmaßnahmen. Zentrale Erfolgsfaktoren sind die laufende Weiterentwicklung der Inhalte, die regelmäßige Wiederholung sowie das Überprüfen der Wirksamkeit der gelernten Inhalte.

Zusammenarbeit mit Cyber-Security- und AI-Expert:innen

Um mit der dynamischen Veränderung Schritt halten zu können, braucht es das Know-how von Cyber-Security- und AI-Expert:innen. Vertrauenswürdige Partner:innen unterstützen bei der Entwicklung einer ganzheitlichen Cyber-Sicherheits-Strategie, dem Testen von Notfall- sowie Krisenplänen und identifizieren mittels Pentests Sicherheitslücken und schließen diese.

Chancen und Risiken von AI erkennen

Dass AI zahlreiche Vorteile für eine positive Geschäftsentwicklung bringt, liegt für viele Unternehmen auf der Hand. Die neue Technologie hat aber auch enormes Potenzial, die Cyber-Sicherheit von Betrieben zu erhöhen, indem sie etwa Phishing-E-Mails oder Cyber-Gefahren rasch aufzeigt. Gleichzeitig birgt die Integration von AI in die unternehmenseigenen Systeme allerdings auch Risiken. Deshalb muss AI vor dem Einsatz ausreichend getestet werden. Stellen Sie sicher, dass Sie genau wissen, wie Ihre Daten verwendet, wo sie gespeichert und ob sie regelmäßig gesichert werden sowie, dass kein Missbrauch möglich ist. Zu wissen, wo und wie AI-Anwendungen die Daten nutzen, ist essenziell, um Ihr Unternehmen vor möglichem Missbrauch oder potenziellen Gesetzesverstößen zu schützen.

07 Fazit

Österreichische Unternehmen haben die Bedeutung von Cyber Security mittlerweile verinnerlicht und können auf herkömmliche Cyberbedrohungen entsprechend reagieren. Durch die aktuellen Entwicklungen rund um Artificial Intelligence verändert sich das Cyber-Security-Umfeld derzeit aber grundlegend. Während Unternehmen AI vielfach bereits im Kampf gegen Cyber-Kriminelle nutzen, haben die Risiken aufgrund der neuen Technologie noch einmal zugenommen. Traditionelle Sicherheitsstrategien reichen damit heute nicht mehr aus, um der neuen Bedrohungslage adäquat zu begegnen. Vielmehr braucht es einen auf Kontrolle basierenden Ansatz wie Zero Trust, der jeden einzelnen Datenzugriff verifiziert und dadurch die Cyber-Sicherheit auch in einem modernen, dynamischen Umfeld sicherstellt.

In einer Zeit, in der die Wirksamkeit technischer Infrastrukturmaßnahmen abnimmt, wird zudem die Awareness der Mitarbeiter:innen immer essenzieller. Um diese zu gewährleisten, sind qualitativ hochwertige Schulungen in regelmäßigen Abständen das Um und Auf. Die ständige Überprüfung des Wissens in der Praxis ist für die Wirksamkeit im Ernstfall ausschlaggebend.

Um auf einen Angriff rasch reagieren zu können, sollten Unternehmen zudem Krisen- und Notfallpläne bereit haben. Diese müssen regelmäßig getestet und adaptiert werden, damit sie im Ernstfall sofort umsetzbar sind.

Ein gut aufgestelltes Cyber Security Management ist jedenfalls ein zentraler Erfolgsfaktor für Unternehmen. Den aktuellen Herausforderungen gilt es jetzt überlegt und entschlossen gegenüberzutreten. Nur so kann die Cyber-Sicherheit – auch langfristig – professionell gemanagt werden.

08

Methode & Sample

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

Erhebungsmethode:
Standardisierte Telefonbefragung (CATI)

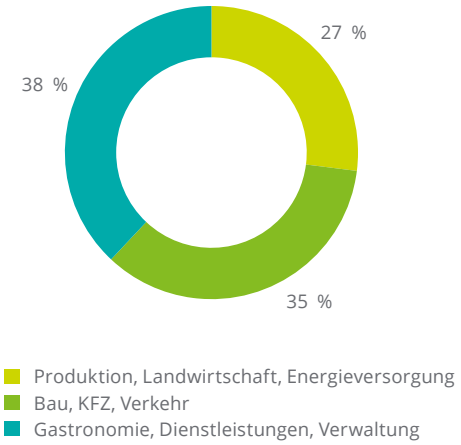
Befragungszeitraum:
Jänner und Februar 2024

Stichprobe:
350 Unternehmen

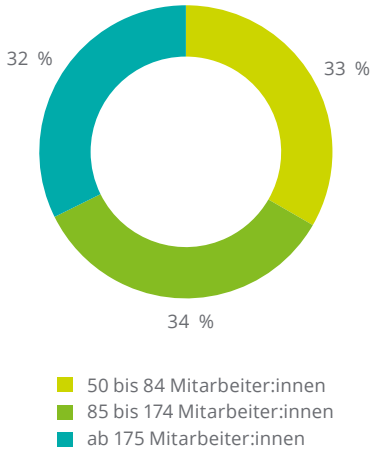
Gewichtung:
Nach Anzahl der Mitarbeiter:innen und Region

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

Branche



Unternehmensgröße



Kontakt

Karin Mair
Managing Partner |
Risk Advisory & Financial Advisory

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

Georg Schwondra
Partner | Risk Advisory

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

Zum digitalen Download der Studie

Impressum

Herausgegeben von:
Deloitte Services Wirtschaftsprüfungs GmbH

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

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

Grafik und Layout:
Claudia Hussovits

Bilder wurden mit AI generiert.

Deloitte.