Deloitte.

Together makes progress

Cyber Security Report 2026

Inhalt

01 Vorwort

Cyber-Angriffe auf Unternehmen nehmen weltweit kontinuierlich zu – sowohl in ihrer Häufigkeit als auch in ihrer Komplexität. Digitale Geschäftsmodelle, vernetzte Infrastrukturen und hybride Arbeitsformen erweitern die Angriffsflächen erheblich. Gleichzeitig professionalisieren sich Angreifer und nutzen automatisierte und AI-gestützte Methoden, um Sicherheitslücken gezielt auszunutzen. Eine wirksame Cyber-Sicherheitsstrategie wird damit zum entscheidenden Wettbewerbs- und Resilienzfaktor.

Wie sich die österreichischen Unternehmen in dem aktuell angespannten Umfeld schlagen, ob ihre Sicherheitsstrategien wirksam sind und wie sie sich diesbezüglich für die Zukunft aufstellen, steht im Fokus der vorliegenden Studie. Mit den Ergebnissen wollen wir aber nicht nur Einblicke in den Status quo geben, sondern auch konkrete Impulse liefern, wie Unternehmen ihre Cyber Security wirksam weiterentwickeln und ihre Handlungsfähigkeit im Ernstfall stärken können. Denn eines sei schon verraten: Ein Großteil der Befragten kann derzeit einen vollständigen Betriebsausfall aufgrund eines Cyber-Angriffes nicht ausschließen.

Wir wünschen eine anregende Lektüre.

Karin Mair | Georg Schwondra | Christoph Hofinger

Karin Mair
Managing Partner |
Technology & Transformation und
Strategy, Risk & Transactions

Georg Schwondra
Partner | Cyber

Christoph Hofinger
Geschäftsführer | Foresight

02 Key Findings

Ransomware-Angriffe nehmen zu, Ressourcen werden aber nicht aufgestockt

Immer häufiger berichten Unternehmen von nahezu täglichen Ransomware-Angriffsversuchen. Die Kriminellen agieren dabei immer professioneller. Nicht einmal ein Viertel kann nach einem erfolgreichen Angriff die Daten wiederherstellen. Dennoch wollen viele ihre Budgets für Cyber-Security derzeit nicht aufstocken.

Unternehmen vertrauen ihren Systemen, Evidenz dafür ist oft unklar

Obwohl die Mehrheit der Unternehmen einen Betriebsstillstand aufgrund eines Cyber-Angriffes nicht ausschließen kann, beurteilen zwei Drittel (66 %) die eigene IT-/Datensicherheit als absolut oder sehr sicher. Hier wird eine Diskrepanz sichtbar. Entscheidend ist jedenfalls, dieses Sicherheitsgefühl durch regelmäßige Tests, klare Verantwortlichkeiten und messbare Nachweise in der Praxis zu validieren.

Cyber-Abwehr funktioniert oft, doch Daten-Wiederherstellung bleibt schwierig

Die Qualität der Abwehrmaßnahmen hat sich in den letzten Jahren deutlich verbessert. Die große Mehrheit von 80 % kann Angriffe durch technische Infrastrukturmaßnahmen verhindern. Doch kommt es zu einer Datenverschlüsselung, gelingt das Backup-Restore und die Entschlüsselung deutlich seltener. Hier zeigt sich einmal mehr die zunehmende Professionalität der Angreifer.

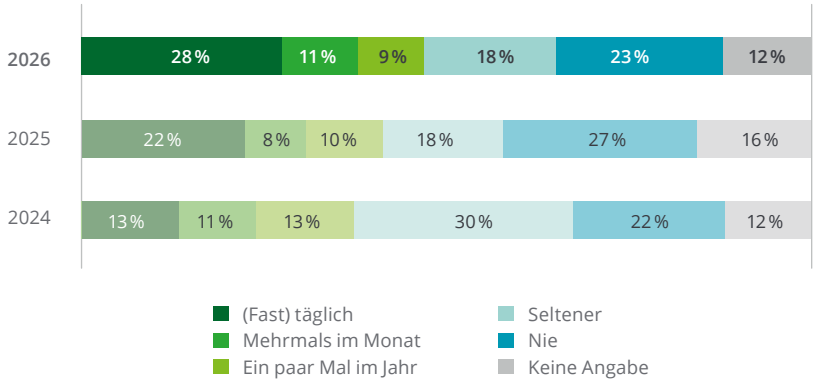
Hot Topic Regulatorik - Betroffenheit und Umsetzungsstand sind oft unklar

Viele Unternehmen sind sich unsicher, ob sie von zentralen Vorgaben wie zum Beispiel der NIS II oder dem AI Act betroffen sind. Jene, die betroffen und sich darüber bewusst sind, haben zudem oft nur lückenhaft Vorbereitungen getroffen.

03 Erhöhter Druck: Zahl der Ransomware-Attacken steigt an

Die Cyber-Bedrohungslage spitzt sich weiter zu: Ransomware-Attacken auf Unternehmen sind keine seltene Ausnahme mehr, sondern werden mittlerweile als wiederkehrende Belastung wahrgenommen. Nahezu ein Drittel (28 %) der Befragten berichtet von fast täglichen Ransomware-Angriffen. Seit 2024 hat sich der Anteil der Unternehmen, die nahezu täglich von Ransomware-Angriffen betroffen sind, mehr als verdoppelt.

Häufigkeit von Ransomware-Attacken



Deloitte Cyber Insights

Aus unserer Beratungspraxis wissen wir, dass erfolgreiche Ransomware-Angriffe auf unvorbereitete Unternehmen gravierende Folgen haben können. Besonders betroffen sind hochautomatisierte Betriebe, Unternehmen mit Just-in-Time-Produktion oder geringen finanziellen Reserven. In solchen Fällen führen die Cyber-Angriffe oft zu Produktionsstillständen oder millionenschweren Verlusten, die die Existenz gefährden oder in die Insolvenz führen können.

Die zunehmenden Angriffe haben auch direkte Relevanz für die Betriebsfähigkeit der Unternehmen. So können zwei Drittel derzeit nicht ausschließen, dass es aufgrund einer Cyber-Attacke zu einem wochenlangen totalen Stillstand ihres Betriebes kommt. Dadurch können Produktionsausfälle entstehen und Dienstleistungen wegfallen, was wiederum erhebliche Auswirkungen auf Kundinnen und Kunden, aber auch die finanzielle Stabilität des Unternehmens hat und im weiteren Verlauf sogar Arbeitsplätze gefährden kann. Dies macht einmal mehr deutlich, wie wichtig eine funktionierende Cyber Security im Unternehmen ist.

Massive Cyberattacken, die zu wochenlangem, totalen Stillstand führen

Deloitte Empfehlung

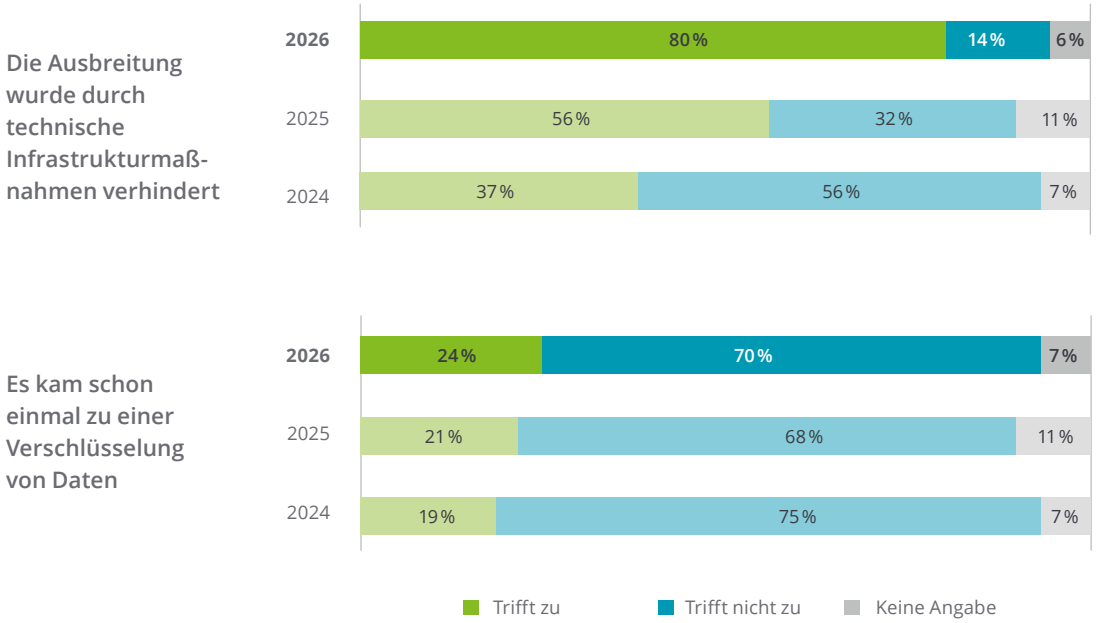
Für Unternehmen geht es nicht um die Frage, ob ein Cyber-Vorfall eintritt, sondern wann dieser passiert. Reines Risikomanagement greift daher zu kurz. Viel mehr braucht es ein wirksames Business Continuity Management (BCM). Durchdachte Notfallpläne, klar definierte Verantwortlichkeiten und regelmäßige Übungen sind entscheidend, um im Ernstfall handlungsfähig zu bleiben und Schäden zu minimieren. Dabei muss BCM als unternehmensweites Programm verankert werden und alle relevanten Funktionen einbeziehen, vom operativen Betrieb über die Fachbereiche bis hin zur Geschäftsführung und zum Aufsichtsrat. Neben technischen Tests sollten auch Tabletop-Exercises durchgeführt werden, damit Entscheidungswege, Prioritäten und Eskalationsmechanismen unter Zeitdruck geübt und verbessert werden.

04 Technisches Dilemma: Wiederherstellung der Daten wird schwieriger

Hinsichtlich des technischen Schutzes zeigt sich ein zweigeteiltes Bild: Einerseits gelingt deutlich mehr Unternehmen, Ransomware-Angriffe technisch besser einzudämmen. Der Anteil der Unternehmen, die berichten, dass die Ausbreitung durch technische Infrastrukturmaßnahmen verhindert werden konnte, stieg in den vergangenen zwei Jahren deutlich an und liegt aktuell bei 80 %.

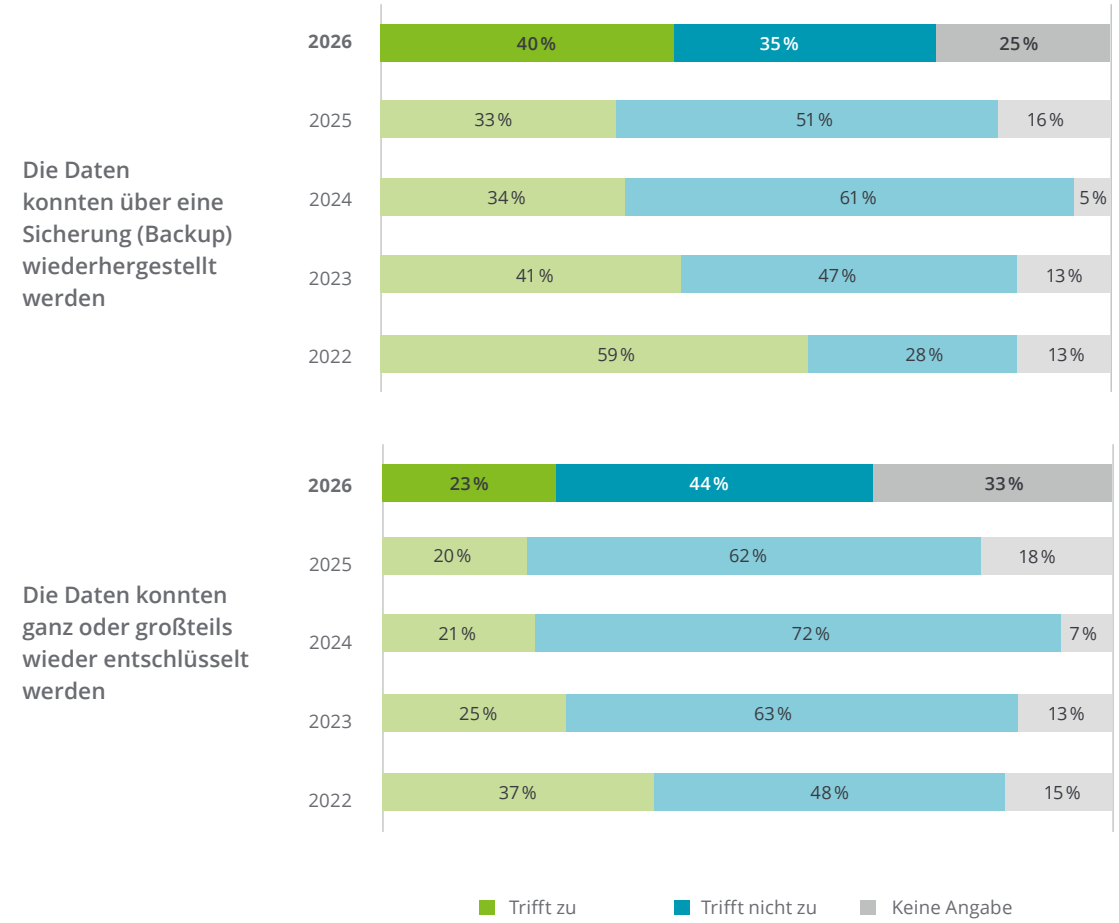
Andererseits bleibt das Risiko einer Datenverschlüsselung bestehen: Knapp ein Viertel (24 %) gibt an, dass es schon einmal zu einer Verschlüsselung von Daten gekommen ist.

Auswirkungen von Ransomware-Attacken



Herausfordernd bleibt vor allem die Wiederherstellung der Daten nach einem erfolgreichen Angriff. In 40 % der Fälle konnten Daten über eine Sicherung zurückgewonnen werden. Eine Entschlüsselung gelang nur in 23 % der Fälle. Auffällig ist zudem die merklich ansteigende Unsicherheit bei diesen beiden Punkten. Beim Backup-Restore liegt der Anteil jener, die keine Angabe machen konnten, bei 25 %, bei der Entschlüsselung bei 33 %.

Auswirkungen von Ransomware-Attacken



Deloitte Cyber Insights

Die Entwicklung seit 2022 deutet auf zwei parallele Effekte hin:
Zum einen verbessern viele Unternehmen ihre technischen Schutzmaßnahmen und die Fähigkeit, Angriffe einzudämmen. Das spiegelt sich auch in den höheren Containment-Werten der jüngsten Vergangenheit wider. Zum anderen ist die Wiederherstellung der Daten deutlich schwieriger geworden, weil moderne Ransomware zunehmend auch Backup- und Wiederherstellungsumgebungen gezielt angreift. Dadurch sinken auch die Werte hinsichtlich erfolgreichen Backup-Restores und Entschlüsselungen im Vergleich zu 2022.

Auffällig ist zudem die steigende Unsicherheit bei Backup-Restore und Entschlüsselung der letzten Jahre. Das ist ein Hinweis darauf, dass Recovery in vielen Organisationen nicht durchgängig über klare Verantwortlichkeiten, belastbare Dokumentation und regelmäßige Tests gesteuert wird. Wenn im Ernstfall nicht sicher beantwortet werden kann, ob und wie gut Wiederherstellung funktioniert, ist das ein Governance-Risiko und erschwert eine schnelle, koordinierte Rückkehr zum Normalbetrieb.

Damit wird klar: Unternehmen profitieren heute von Investitionen in Prävention und Eindämmung des Schadens. Entscheidend für die Widerstandsfähigkeit ist aber, ob sie nach einem erfolgreichen Angriff rasch wieder handlungsfähig werden. Dazu braucht es robuste, gut geschützte Backups und regelmäßige Backup-Restore-Tests, die die Wiederherstellbarkeit im Ernstfall nachweislich belegen.

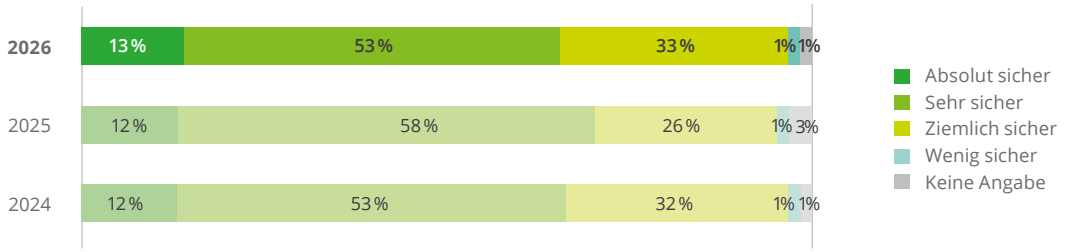
„Wenn Angriffe häufiger werden, reicht es nicht, sie nur einzudämmen. Entscheidend ist, ob Unternehmen die Fähigkeit haben nach einem Vorfall rasch zum Normalbetrieb zurückkehren. Genau hier sehen wir bei vielen Unternehmen noch Aufholbedarf.“

Georg Schwondra| Partner | Cyber

05 Hohes Selbstbewusstsein: Unternehmen vertrauen ihren Systemen

Laut unserer Studie haben die Unternehmen sehr großes Vertrauen in die Sicherheit ihrer Daten und IT-Systeme. Mehr als die Hälfte (53 %) bewertet diese als sehr sicher, ein Drittel (33 %) als ziemlich sicher. Überraschenderweise gehen 13 % sogar davon aus, dass ihre Daten und IT-Systeme absolut sicher sind.

Sicherheit der Daten und IT-Systeme



Deloitte Cyber Insights

Die Ergebnisse verdeutlichen eine klare Diskrepanz: Zwar bewerten viele Unternehmen ihre Daten und IT-Systeme als (sehr) sicher, gleichzeitig können sie einen mehrwöchigen Stillstand infolge eines schweren Cyber-Angriffs nicht vollständig ausschließen. Zudem haben 46 % der Unternehmen noch nie von Zero Trust gehört oder planen keine entsprechende Umsetzung. Dies legt nahe, dass Sicherheit häufig als Schutz im laufenden Betrieb verstanden wird, während Resilienz, Krisenfestigkeit und Wiederanlauf getrennt davon betrachtet werden.

Ein hohes Sicherheitsgefühl ist grundsätzlich ein positives Signal und zeigt, dass sich die Unternehmen mit dem Thema auseinandersetzen. Wenn das Sicherheitsgefühl jedoch zur Selbstüberschätzung führt, kann das ein Risiko darstellen. Denn folglich werden Prioritäten geändert, Investitionen aufgeschoben und Vorbereitungen für seltene, aber geschäftskritische Szenarien nicht mit der nötigen Konsequenz umgesetzt. Dieser Effekt kann die Widerstandsfähigkeit schwächen, obwohl sich die Organisation subjektiv gut aufgestellt fühlt.

Deloitte Empfehlung

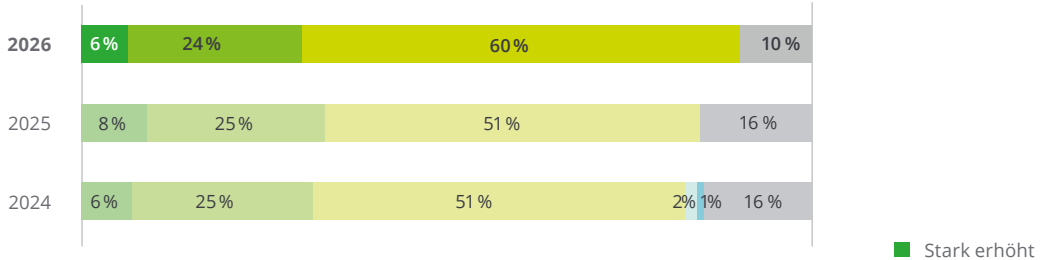
Die Cyber Security und ihr Reifegrad sollten niemals über das subjektive Sicherheitsgefühl gesteuert werden. Ein Reifegrad-Assessment nach anerkannten Standards als Ausgangspunkt hilft, die Sicherheitslage korrekt einzuschätzen. Im laufenden Betrieb geben Kennzahlen wie beispielsweise die Patch-Compliance-Rate, Phishing-Click-Rate, durchschnittliche Zeit bis zur Erkennung oder Eindämmung eines Sicherheitsvorfalls sowie die Anzahl kritischer Risiken und deren Behandlungsstatus einen guten Überblick über den Sicherheitsstatus des Unternehmens.

06 Mehr Druck, weniger Spielraum: Ressourcen werden nicht aufgestockt

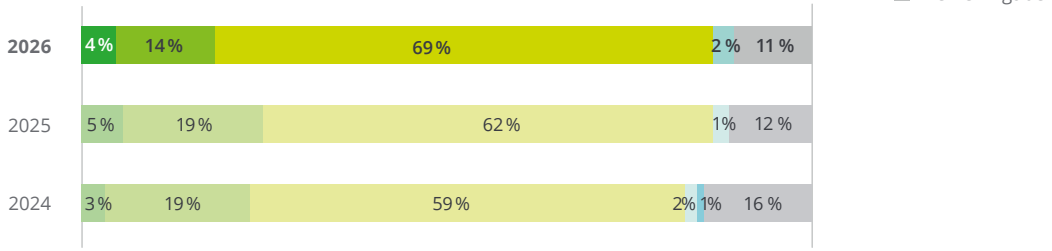
Genügend Ressourcen sind eine zentrale Voraussetzung, um mit der aktuellen Bedrohungslage und zukünftigen Entwicklungen Schritt zu halten. In den befragten Unternehmen lässt sich jedoch eine deutliche Diskrepanz zwischen der veränderten Bedrohungslage und der Entwicklung der Ressourcen feststellen. Denn trotz steigender Anforderungen will die Mehrheit aktuell nichts bei den Sicherheitsbudgets ändern.

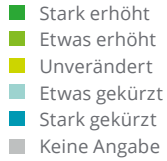
60 % der Befragten wollen ihre Ausgaben für Technik und Prozesse auf dem Niveau des letzten Jahres halten. Die Personalaufwendungen wollen 69 % auf dem Stand von 2025 belassen.

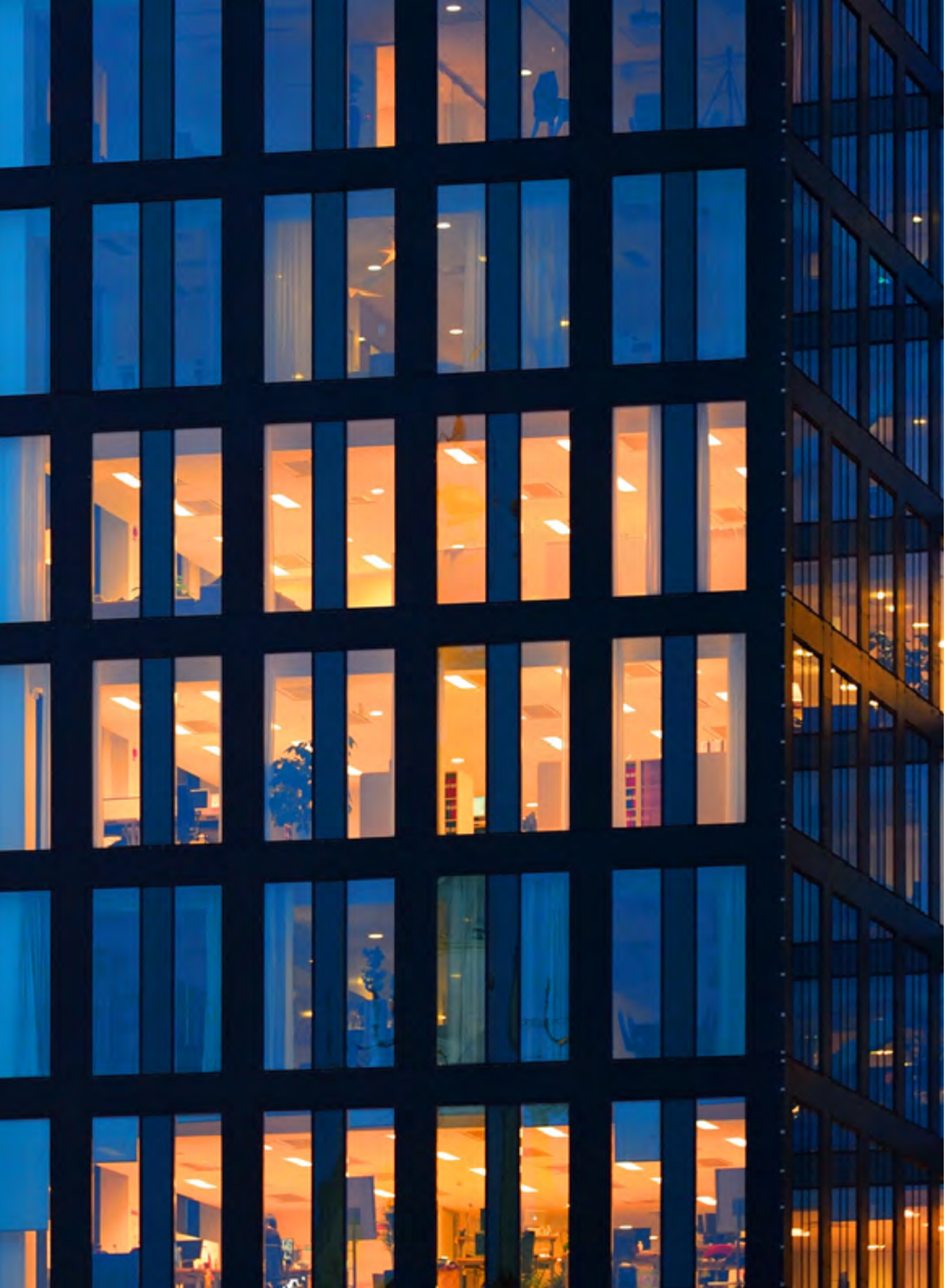
Budgetveränderungen Technik und Prozesse



Budgetveränderungen Personal







Deloitte Cyber Insights

Die Unternehmen vertrauen ihrer Cyber Security und haben weitestgehend auch gute Erfahrungen damit gemacht. Eine Aufstockung an Ressourcen steht für die meisten derzeit – auch aufgrund der aktuell angespannten wirtschaftlichen Lage – nicht am Plan. Um dennoch weiterhin Cyber-Sicherheit zu gewährleisten und bereits geschlossene Sicherheitslücken nicht wieder zu öffnen, müssen vorhandene Mittel stärker priorisiert und gezielt dort eingesetzt werden, wo Resilienz und Handlungsfähigkeit im Ernstfall messbar verbessert werden kann.

„Die erhöhten Budgets der letzten Jahre zeigen klare Wirkung und spiegeln sich in einer deutlich gestiegenen Resilienz der Unternehmen wider. Dennoch zeigt die aktuelle Bedrohungslage klar: Wer auch morgen gut aufgestellt sein will, muss Budgets entsprechend anpassen. Investitionen in Cyber Security sind ein Muss."

Karin Mair | Managing Partner | Technology & Transformation und Strategy, Risk & Transactions

„Cyber-Risiken sind ein Business-Risiko. Wenn die Bedrohungslage zunimmt, müssen Unternehmen ihre Ressourcen so ausrichten, dass Prävention, Reaktion und Wiederanlauf auch bei laufendem Geschäftsbetrieb funktionieren. Das gelingt nur, wenn Budgets und Prioritäten die kritischen Fähigkeiten tatsächlich stärken."

Georg Schwondra| Partner | Cyber

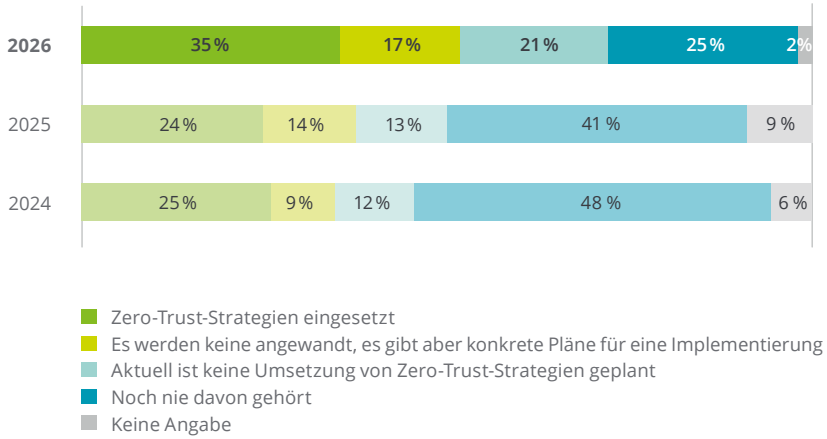
07 Zero Trust: Ansatz etabliert sich zunehmend

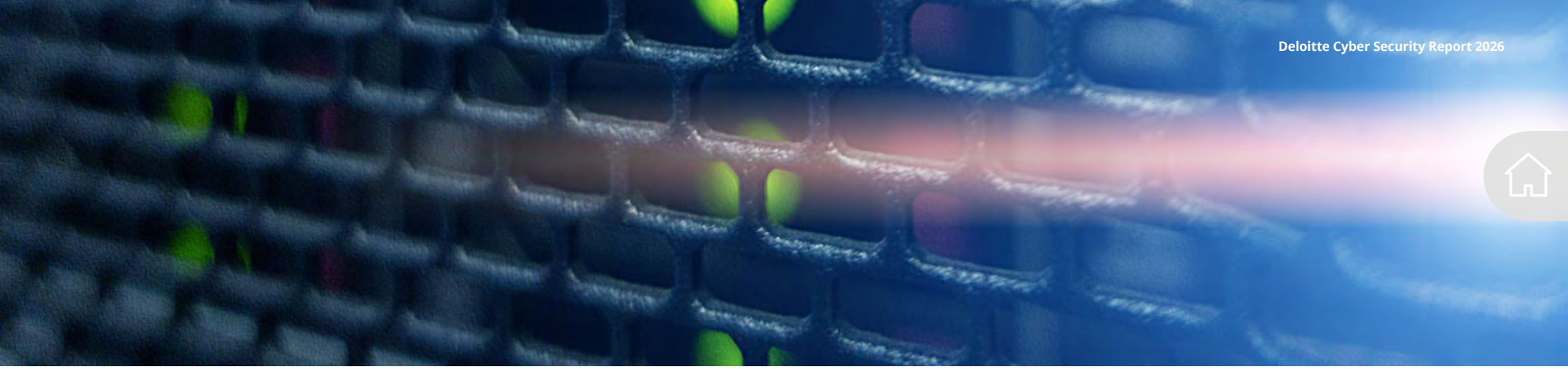
Die Grundidee des Zero-Trust-Ansatzes ist die Überprüfung von Zugriffen mit einem Minimum an Vertrauen. Dieses wird nicht pauschal vergeben, sondern ist jeweils beim einzelnen Zugriff zu evaluieren. Dabei spielt es keine Rolle, ob die zugreifende Person oder das zugreifende System sich außerhalb oder innerhalb des Unternehmensnetzes befindet.

Die Ergebnisse zeigen, dass der Ansatz in Österreich zunehmend an Bedeutung gewinnt. So hat sich die Zahl jener Unternehmen, die davon noch nichts gehört haben, innerhalb von zwei Jahren nahezu halbiert (2024: 48 %; 2026: 25 %).

35 % der befragten Unternehmen setzen Zero-Trust-Strategien zudem bereits ein, weitere 17 % haben konkrete Pläne für eine Implementierung. Gleichzeitig gibt es weiterhin Unternehmen (21 %), die noch keine Umsetzung dieses wichtigen Ansatzes planen.

Zero Trust Security





Deloitte Cyber Insights

Gemäß der Zero-Trust-Methode wird eine verstärkte Zugriffskontrolle implementiert und das Vertrauen in implizite Vermutungen reduziert. In der Konsequenz wird es für potenzielle Angreifer viel schwieriger, sich innerhalb der IT-Umgebung unbemerkt fortzubewegen und Schäden zu verursachen.

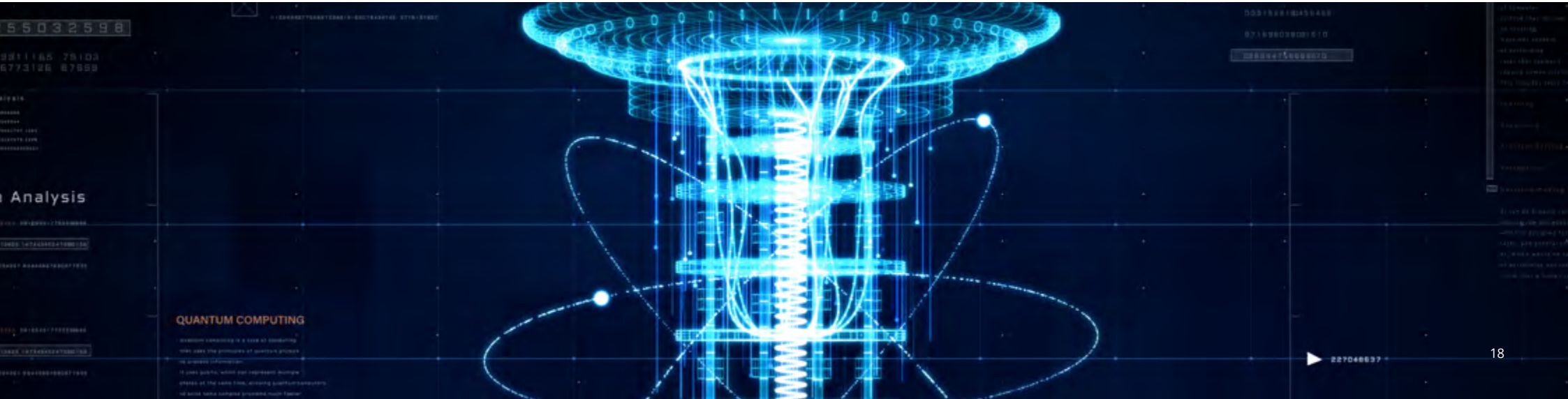
Ein Viertel der Unternehmen kennt den Ansatz noch nicht und weitere 21 % planen keine Umsetzung. Damit bleibt in vielen Unternehmen erhebliches Potenzial ungenutzt. Das ist ein Zustand, der sich im Sinne einer umfassenden Cyber Security dringend ändern sollte. Denn die Umsetzung von Zero-Trust-Strategien scheitert selten am Willen, sondern meist an fehlender struktureller, technologischer und organisatorischer Reife. Erst wenn Transparenz, das nötige Wissen, klare Verantwortlichkeiten und eine realistische Transformations-Roadmap vorhanden sind, kann Zero Trust erfolgreich umgesetzt werden.

Gleichzeitig wird dabei oft übersehen: Richtig eingeführt erhöht Zero Trust nicht nur das Sicherheitsniveau, sondern reduziert auch Komplexität, etwa durch klarere Zugriffsmodelle, standardisierte Prozesse und bessere Transparenz über Systeme und Berechtigungen. Das schafft die Grundlage, künftige sicherheitsrelevante und organisatorische Herausforderungen auch mit dem bestehenden Team zu bewältigen.

08 Quantencomputer: Erste Entwicklungen und ihre Folgen

Ähnlich wie der Zero-Trust-Ansatz noch vor einigen Jahren sind heute die Entwicklung und Folge von Quantencomputern noch nicht im Bewusstsein vieler Unternehmen angekommen. Tatsächlich eröffnet diese neue Generation an Rechnern aber zahlreiche Möglichkeiten, kryptografische Verschlüsselungen, welche heute als sicher erachtet werden, zu knacken. Nur rund ein Viertel der Unternehmen (24 %) hat sich aktuell aber mit diesen Sicherheitsfolgen auseinandergesetzt. Für die kommenden Jahre ist aber auch in diesem Zusammenhang mit einem steigenden Bewusstsein zu rechnen.

Mögliche Sicherheitsfolgen des Einsatzes von Quantencomputern



Deloitte Cyber Insights

Quantencomputer sind eine neue Generation von Rechnern, die bestimmte mathematische Probleme deutlich schneller lösen können als heutige Systeme, weil sie nicht mit klassischen Bits (0 oder 1), sondern mit sogenannten Qubits arbeiten, welche eine Superposition von 0 und 1 gleichzeitig ermöglichen. Sie werden heutige Rechner zwar nicht ersetzen, können aber konkrete Probleme, die für klassische Rechner praktisch unlösbar sind, potenziell in Minuten lösen. Dies schließt perspektivisch auch heute eingesetzte kryptografische Verfahren ein, die etwa beim Online-Banking, bei VPN-Verbindungen oder bei digitalen Signaturen genutzt werden. Besonders kritisch ist dabei „Harvest now, decrypt later" (jetzt speichern, später entschlüsseln): Angreifer speichern bereits heute große Mengen an verschlüsselten Daten, um diese später mit Quantencomputern zu entschlüsseln, etwa sensible Forschungsdaten, personenbezogene Informationen, Bankdaten oder vertrauliche staatliche Kommunikation mit langen Schutzfristen.

Entsprechend gewinnt Post-Quantum-Kryptografie (PQC) strategisch an Bedeutung. In Europa nimmt die EU eine aktive Rolle ein, insbesondere über die EU Kommission mit der Förderinitiative Quantum Technologies Flagship sowie über die EuroHPC Joint Undertaking, die den Aufbau europäischer Quanten- und Hochleistungsrechenkapazitäten vorantreibt. Parallel arbeitet die Industrie gemeinsam mit Standardisierungsgremien an quantensicheren Verfahren.

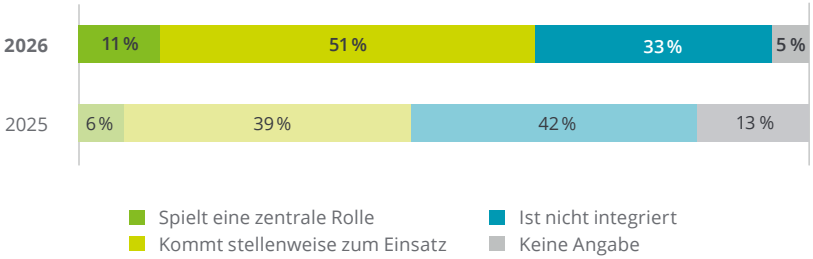
Das Umfrageergebnis ist daher als Frühindikator zu verstehen, dass dieses langfristige Kryptografie-Risiko in vielen Organisationen noch nicht systematisch in die Security-Planung einfließt. Quantencomputing wird häufig als Zukunftsthema wahrgenommen und gegenüber akuten Bedrohungen wie Ransomware oder Recovery-Maßnahmen nachrangig priorisiert. Kryptografische Abhängigkeiten werden dadurch oft erst im Zuge von Modernisierungen oder regulatorischen Anforderungen sichtbar und müssen dann unter Zeitdruck adressiert werden. Deshalb ist es sinnvoll, bei Updates oder Erneuerungen von Kryptografiekomponenten Post-Quantum-Kryptografie bereits heute mitzuberücksichtigen, um spätere Umstellungen planbarer und mit geringerem Risiko umzusetzen.

09 AI in der Cyber Security: Mehr Einsatz, aber selten zentral

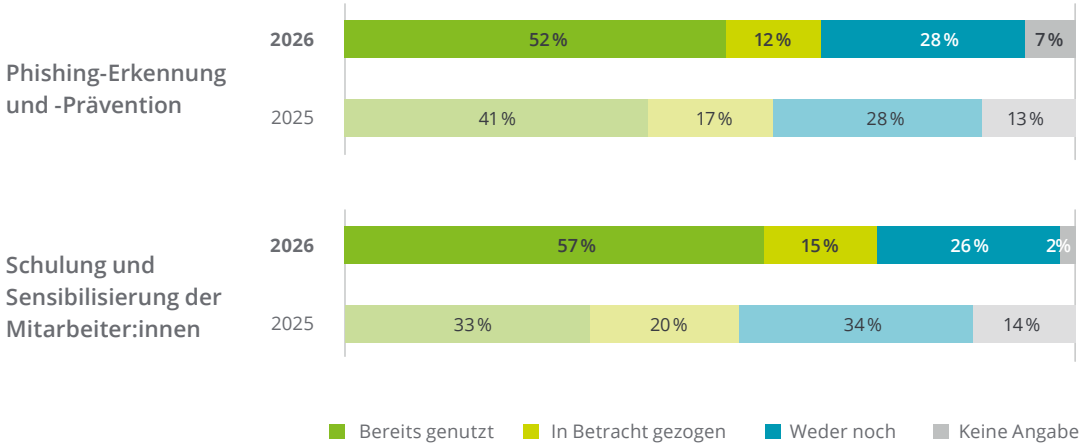
Artificial Intelligence (AI) hat in der Cyber Security bereits Einzug gehalten, wenngleich meist nur als Unterstützung in einzelnen Bereichen und nicht als Herzstück des gesamten Sicherheitsprogramms. In der Befragung gaben 11 % der Unternehmen an, dass AI in der Cyber Security eine zentrale Rolle spielt. 51 % setzen AI stellenweise ein. Gleichzeitig berichten 33 % , dass sie AI in diesem Bereich noch nicht integriert haben.

Am sichtbarsten ist der Einsatz von AI dort, wo Aufgaben klar abgrenzbar und gut skalierbar sind. Bei der Erkennung und Prävention von Phishing nutzen die Technologie bereits 52 %, weitere 12 % ziehen den Einsatz in Betracht. Bei Schulungen und Sensibilisierung liegt die aktuelle Nutzung bei 57 %, weitere 15 % planen den Einsatz.

AI in der Cyber Security

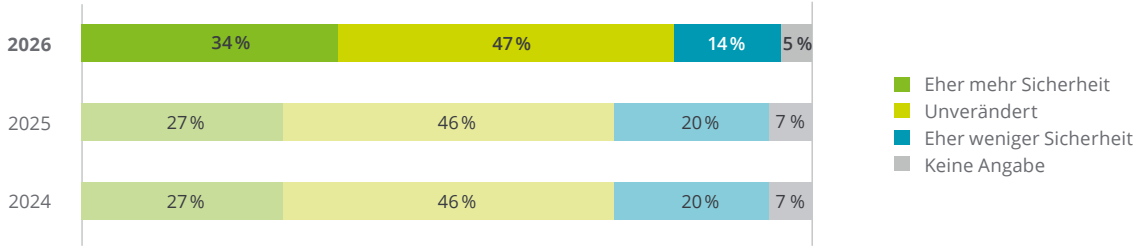


Nutzung von AI im Cybersecurity-Management



Die Erwartungen an AI in der Cyber Security sind durchmischt. Während rund ein Drittel (34 %) durch den Einsatz von mehr Sicherheit ausgeht, rechnet knapp die Hälfte (47 %) mit keiner Veränderung, 14 % befürchten sogar eine höhere Gefahr, die durch den Einsatz ausgeht. Insgesamt lässt sich zudem im Vergleich zum Vorjahr ein gestiegenes Vertrauen in AI feststellen.

Möglichkeiten von AI in der Cyber Security



Deloitte Cyber Insights

Insgesamt deuten die Ergebnisse auf eine steigende Reifephase bei AI hin. Viele Unternehmen nutzen AI bereits dort, wo sie schnell skaliert und operativ unterstützt, etwa bei Phishing oder Awareness. Gleichzeitig zeigt sich aber auch, dass AI selten als tragendes Element eines Sicherheitsprogramms etabliert ist.
Das passt zu einem pragmatischen Vorgehen: Zuerst werden punktuelle Use-Cases ausgeführt, sobald Verantwortlichkeiten, Datenbasis und Qualitätskriterien geklärt sind, erfolgt dann die schrittweise Integration.

Im Jahresvergleich zeigen die Ergebnisse, dass das Vertrauen in AI von 2024 auf 2025 deutlich gesunken ist und erst in diesem Jahr wieder signifikant ansteigt. Das liegt vor allem daran, dass viele Organisationen AI zunächst als sehr innovativ wahrgenommen und frühe Pilotierungen gestartet haben. Danach folgte bei manchen im Jahr 2025 eine Phase der Ernüchterung, auch weil der Übergang von ersten Experimenten zum tatsächlich nutzbringenden Einsatz anspruchsvoll ist. Mit der wachsenden Reife und Leistungsfähigkeit von AI nimmt aber sowohl ihre Integration in operative Prozesse als auch ihre Anwendung im Bereich Cyber Security bei unseren Kundinnen und Kunden zu.

10 Hot Topic Regulatorik: Betroffenheit und Umsetzung werden oft falsch eingeschätzt

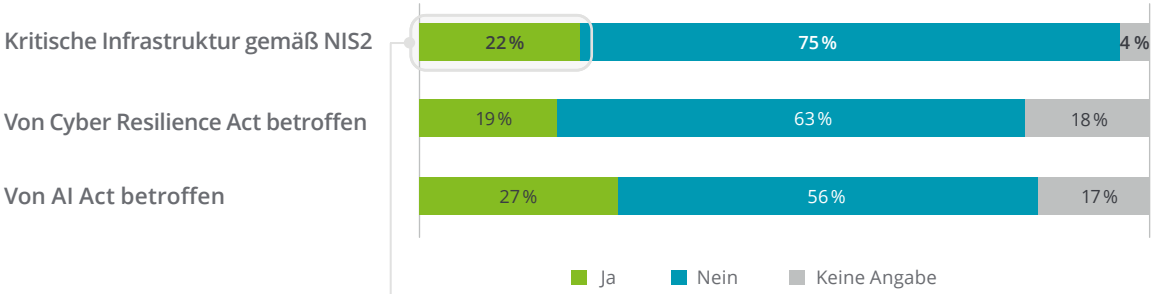
Im österreichischen Unternehmensumfeld besteht erhebliche Unsicherheit darüber, welche der neuen europäischen Regulierungen auf die eigene Organisation tatsächlich Anwendung finden. Besonders relevant ist dies bei NIS2, dem Cyber Resilience Act und dem AI Act, da Unternehmen ihre regulatorische Betroffenheit hier weitgehend selbst beurteilen müssen.

Diese Unsicherheit zeigt sich auch in den Ergebnissen der Befragung, denn nur 22 % ordnen sich als kritische Infrastruktur gemäß NIS2 ein, 19 % sehen sich vom Cyber Resilience Act betroffen und 27 % vom AI Act. Gleichzeitig überwiegt jeweils die Einschätzung, nicht betroffen zu sein, und zusätzlich gibt es einen nennenswerten Anteil ohne Angabe, was insgesamt die tendenziell niedrige Einschätzung der Betroffenheit erklärt.

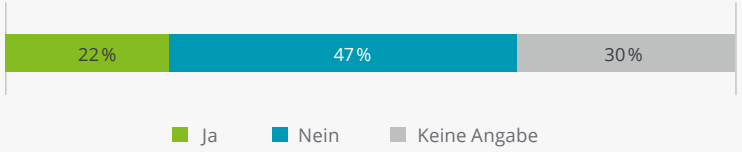
Anders verhält es sich beim Resilienz kritischer Einrichtungen Gesetz (RKEG), basierend auf der entsprechenden EU-Richtlinie, da hier die zuständigen Behörden die kritischen Einrichtungen identifizieren und die betroffenen Unternehmen aktiv informieren. In der Praxis überschneiden sich die Adressatenkreise von RKEG und NIS2, da die betroffenen Unternehmen auch in den Anwendungsbereich von NIS2 fallen. Umgekehrt gilt dies jedoch nicht, da nicht jedes Unternehmen, das unter NIS2 fällt, zugleich vom RKEG betroffen ist.

Diese unterschiedliche Betroffenheitslogik erhöht in der Praxis das Risiko, regulatorische Pflichten verspätet, unvollständig oder fehlerhaft zu erfassen. Gerade dort, wo die Einordnung primär bei den Unternehmen selbst liegt, kommt der strukturierten Betroffenheitsprüfung eine zentrale Bedeutung zu.

Einschätzung zur Anwendung europäischer Regulierungen auf das eigene Unternehmen

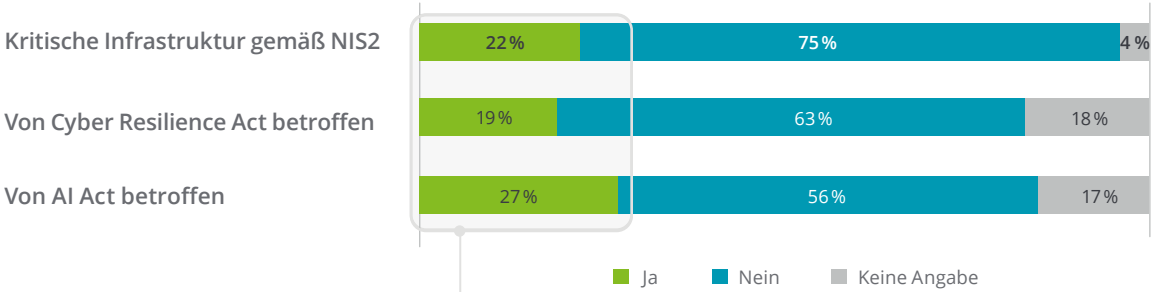


Einschätzung zur Anwendung der Richtlinie zur Resilienz Kritischer Einrichtungen (RKEG)*

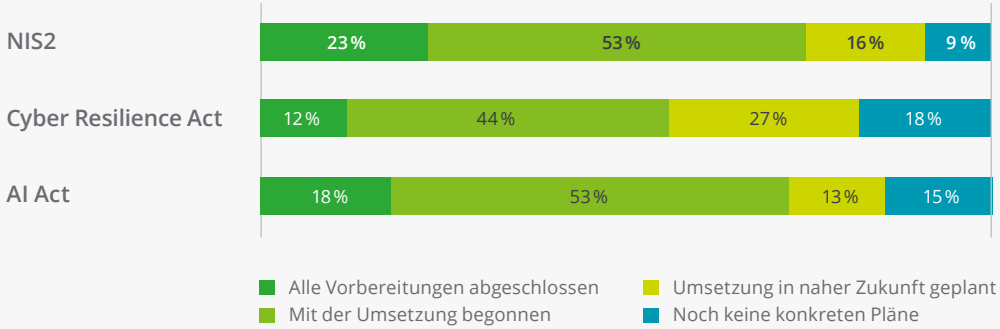


* Basis: Alle Unternehmen, die angeben von NIS2 betroffen zu sein (76 Unternehmen)

Unter den Unternehmen, die angeben, von der NIS2 bzw. dem NISG betroffen zu sein, berichten 23 %, bereits sämtliche Vorbereitungen abgeschlossen zu haben, 53 % befinden sich in der Umsetzungsphase, 16 % planen die Umsetzung in naher Zukunft und 9 % verfügen bislang über keine konkreten Pläne. Auffällig an den Zahlen ist, dass rund ein Viertel der Unternehmen angibt, die Umsetzung bereits abgeschlossen zu haben. Gleichzeitig hat rund jedes zehnte Unternehmen bislang noch nicht einmal mit der Planungsphase begonnen und das, obwohl ihnen bewusst ist, dass sie unter die Bestimmungen von NIS2 bzw. dem NISG fallen. Die Umsetzung komplexer gesetzlicher Regelungen nimmt üblicherweise mehrere Jahre in Anspruch, wie wir aus der Beratungspraxis wissen.



Status zur Umsetzung*



* Basis: Alle Unternehmen, die angeben betroffen zu sein
(NIS2 - 76 Unternehmen; Cyber Resilience Act - 66 Unternehmen; AI Act - 96 Unternehmen)

Deloitte Cyber Insights

Regulatorische Anforderungen entwickeln sich für viele Unternehmen zu einem Katalysator für den Aufbau belastbarer Governance-Strukturen. Vielen Unternehmen ist aber nicht bewusst, dass sie von einer solchen überhaupt betroffen sind. Wird die Betroffenheit nicht sauber analysiert und klassifiziert, lassen sich Prioritäten, Budgets und Nachweisstrukturen nicht zielgerichtet und wirksam ausrichten.

Ein wesentlicher Unterschied für diese Unsicherheit bei der Betroffenheit ist die veränderte Systematik. Während früher, wie etwa bei NISG vom Jahr 2018, der Betreiber durch die zuständige Behörde mittels Bescheid offiziell ermittelt und benachrichtigt wurde, obliegt es nun den Unternehmen selbst, ihre mögliche Betroffenheit eigenständig zu prüfen und gegebenenfalls zu melden. Auffällig ist in diesem Zusammenhang vor allem die wahrgenommene Betroffenheit hinsichtlich des AI Acts. In der Befragung geben lediglich 27 % an, von diesem betroffen zu sein. Gleichzeitig nutzen 62 % der Unternehmen AI in ihrer Cyber Security, was im Umkehrschluss wiederum bedeutet, dass die Richtlinie sehr wohl auf sie anwendbar ist. Hier braucht es dringend mehr Aufklärungsarbeit seitens der Behörden.

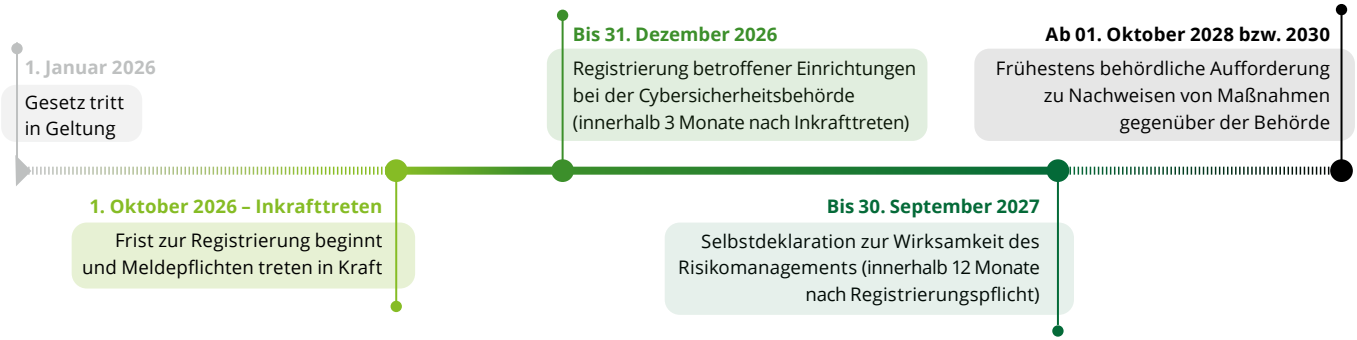
Die Ergebnisse des Umsetzungsstatus legen wiederum nahe, dass es in Teilen der Wirtschaft zu einer gewissen Selbstüberschätzung kommen könnte. Angesichts der hohen Komplexität der europäischen Regulierungen und anhand unserer Beratungspraxis erscheint der Anteil jener Unternehmen, die bereits ein vollständiges Compliance-Niveau erreicht haben wollen, vergleichsweise hoch.

Möglicherweise beziehen sich viele der befragten Unternehmen bei der Angabe, die Vorbereitungen abgeschlossen zu haben, eher auf die strategischer als auf die operativer Ebene. Das kann etwa eine erste Risikoanalyse oder die Definition interner Zuständigkeiten sein, ohne dass alle geforderten technischen und organisatorischen Maßnahmen tatsächlich umgesetzt oder dokumentiert sind.

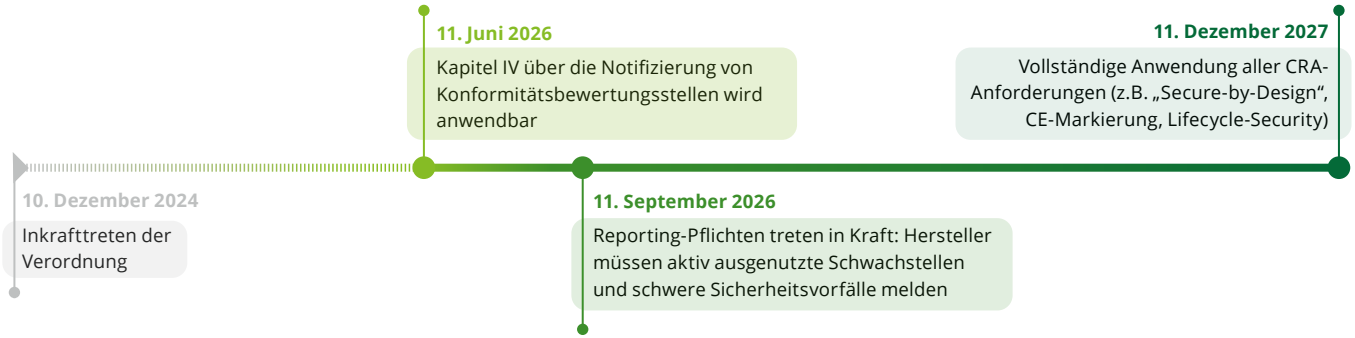
Deloitte Empfehlung

Unternehmen müssen ihre Betroffenheit von den unterschiedlichen Regelwerken unbedingt klären. Nur so lässt sich eine objektive Betrachtung des Status quo der Maßnahmenumsetzung vornehmen, eine Gap-Analyse zu Zielanforderungen durchführen und daraus priorisierte Handlungsmaßnahmen ableiten. Auf dieser Basis kann eine umsetzbare Roadmap erstellt werden, die Projekte und Ressourcenbedarf zusammenführt und Synergien bei der Umsetzung berücksichtigt. So können Unternehmen Regulatorik als Chance nutzen, um eigenen IT- und AI-Systeme resilienter, effizienter und vertrauenswürdiger zu machen, was Kosten sparen, Innovation fördern und neue Marktchancen öffnen kann.

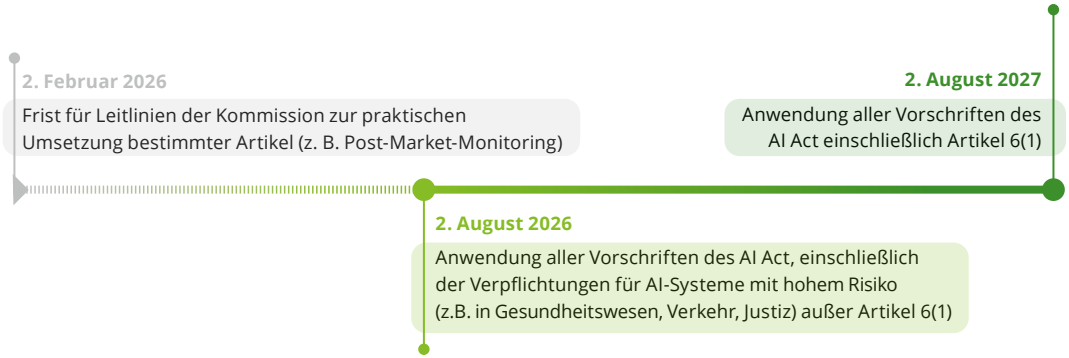
Das **Netz- und Informationssystem-sicherheitsgesetz 2026 (NISG 2026)** ist die österreichische Umsetzung der EU-NIS-2-Richtlinie. Es verpflichtet „wesentliche“ und „wichtige“ Einrichtungen zu einem strukturierten Cyber-Risikomanagement, Meldepflichten bei Sicherheitsvorfällen sowie zu Governance- und Nachweispflichten gegenüber der Behörde. Betroffen sind unter anderem Unternehmen aus den Bereichen Energie, Verkehr, Gesundheit, Finanzwesen, Trinkwasser und digitale Infrastruktur, außerdem IT-Dienstleister sowie größere Unternehmen aus weiteren definierten Sektoren, abhängig von Größe und Kritikalität.



Der **Cyber Resilience Act** ist eine EU-Verordnung mit Fokus auf Produkte mit digitalen Elementen. Ziel ist es, „Secure-by-Design“ verbindlich zu machen: Hersteller müssen Sicherheits-anforderungen über den gesamten Produkt-lebenszyklus erfüllen, Schwachstellen managen und schwere Sicherheitsvorfälle melden. Betroffen sind vor allem Hersteller, Importeure und Händler von Software, Hardware und IoT-Produkten, die in der EU in Verkehr gebracht werden.



Der **Artificial Intelligence Act (AI Act)** ist die erste umfassende EU-Regulierung für künstliche Intelligenz und verfolgt einen risikobasierten Ansatz. Je nach Risikokategorie gelten unterschiedliche Anforderungen, von Transparenzpflichten bis hin zu strengen Vorgaben für sogenannte Hochrisiko-AI, zum Beispiel in kritischer Infrastruktur, in der Personalrekrutierung oder in der Medizin. Betroffen sind Anbieter, Importeure und Händler von AI-Systemen, die in der EU eingesetzt oder bereitgestellt werden, aber auch Betreiber, welche AI im Unternehmen einsetzen, inkl. Chatbots, wie z.B. ChatGPT, Gemini oder Copilot.



11 Handlungsempfehlungen

Die Ergebnisse des Cyber Security Report 2026 zeigen ein klares Spannungsfeld: Während die Angriffsdichte steigt, gelingt es Unternehmen immer besser, Attacken einzudämmen. Herausfordernd bleibt jedoch die Wiederherstellung der Daten nach einem erfolgreichen Angriff. Auf die zugespitzte Bedrohungslage reagieren Unternehmen nur punktuell. Die meisten planen keine Aufstockung ihrer Ressourcen.

Neue Technologien wie AI werden auch in der Cyber Security präsenter, ein flächendeckender Einsatz steht aber noch aus. Regulatorische Anforderungen schaffen zusätzlichen Handlungsdruck. Vor diesem Hintergrund bündeln wir die wichtigsten Empfehlungen zu einem umsetzbaren Maßnahmenpaket, das Wirksamkeit und Handlungsfähigkeit im Ernstfall erhöht.

1. Resilienz und Wiederanlauf priorisieren

Unternehmen sollten ihren Fokus nicht nur auf die Schadenseindämmung legen, sondern ebenso darauf, den Normalbetrieb nach einem Angriff schnell wiederherzustellen. Grundlage dafür ist eine sogenannte Business Impact Analyse. Sie klärt, welche Prozesse kritisch sind, welche Abhängigkeiten bestehen und wie lange ein Ausfall zu verkraften ist. Darauf aufbauend werden Wiederanlaufziele definiert, etwa wie schnell Prozesse wieder funktionieren müssen und welcher Datenverlust maximal akzeptabel ist. Diese Ziele werden in sogenannten Backup- und Wiederanlaufplänen mit klaren Verantwortlichkeiten verankert. Anschließend werden robuste Backup- und Wiederherstellungsmechanismen umgesetzt und die Umgebungen gezielt geschützt. Entscheidend ist, diese regelmäßig zu testen und die Ergebnisse konsequent zu dokumentieren und verbessern. Ergänzend sollten Tabletop-Exercises durchgeführt werden. In diesen Entscheidungsübungen im kleinen Kreis trainiert das Top-Management Priorisierung, Kommunikation und Eskalation, um im Ernstfall schneller und sicherer handeln zu können.

2. Governance, Nachweise und Priorisierung schärfen

Ein hohes Sicherheitsgefühl ist nur dann in der Praxis belastbar, wenn es durch überprüfbare Nachweise gestützt wird. Dafür braucht es einen kontinuierlichen Investitionswillen sowie einen strukturierten Blick auf den Reifegrad. Zentrale Fragen in diesem Zusammenhang sind: Wo steht das Unternehmen aktuell? Welches Zielniveau ist für kritische Prozesse realistisch und notwendig? Und wo bestehen die wichtigsten Sicherheitslücken? Ein Abgleich mit definierten Zielen hilft, Entscheidungen zu objektivieren. Maßnahmen werden dann nicht „nach Bauchgefühl", sondern nach Geschäftsauswirkung, Umsetzbarkeit und Nachweisbarkeit priorisiert.

3. Regulatorik als Teil der Sicherheitsstrategie verstehen

Sind Betroffenheit und Pflichten im Zusammenhang mit Regulatorik unklar, entsteht ein Governance-Risiko. Eine strukturierte Betroffenheitsanalyse schafft hier die Grundlage und ordnet ein, welche rechtlichen Anforderungen tatsächlich relevant sind und welche Nachweise erbracht werden müssen. In einer Gap-Analyse werden anschließend Abweichungen objektiv festgehalten. Die identifizierten Lücken werden in einem Maßnahmenplan priorisiert und in einer Roadmap gebündelt. So werden Verantwortlichkeiten, Zeitplan und Nachweise mess- und anpassbar.

4. AI in der Cyber Security effektiv nutzen

AI sollte in der Cyber Security zuerst dort eingesetzt werden, wo sie konkret unterstützt und der Nutzen gut messbar ist, etwa bei der Erkennung verdächtiger E-Mails oder bei Schulungen. Damit der Einsatz sicher und effizient bleibt, helfen einfache Leitplanken: Unternehmen starten mit wenigen, klar definierten Anwendungsfällen und erweitern diese erst dann, wenn sie zuverlässig funktionieren. Datenquellen und Zugriffe werden bewusst geregelt, um Fehlinterpretationen und neue Risiken zu vermeiden. Entscheidungen mit hoher Auswirkung bleiben beim Menschen, während AI Hinweise und Vorschläge liefert. Gleichzeitig wird die Wirksamkeit laufend überprüft, etwa anhand von Fehlalarmen und der Ergebnisqualität. Zuletzt werden Zuständigkeiten sowie Änderungen an Regeln oder Modellen klar festgelegt und nachvollziehbar dokumentiert.

5. Zero Trust schrittweise ausbauen

Zero Trust ist ein praktischer Sicherheitsansatz, bei dem jeder Zugriff konsequent geprüft wird. Für die Umsetzung empfiehlt sich ein stufenweises Vorgehen: Im ersten Schritt wird ein Zero-Trust-Konzept definiert. Dazu gehören ein klares Zielbild, der Geltungsbereich für kritische Anwendungen und Daten, eindeutig zugewiesene Verantwortlichkeiten sowie Regeln, mit denen sich die Umsetzung steuern und überprüfen lässt. Im zweiten Schritt werden Identität und Gerätesicherheit als Eintrittskriterium festgelegt. Ein Zugriff auf die Systeme wird nur mit starker Authentifizierung, etwa durch Multi-Faktor-Authentifizierung (MFA) und kontextabhängigen Regeln, erlaubt. Diese kann zum Beispiel von Rolle, Standort oder Sicherheitszustand des Geräts abhängig sein. Anschließend werden Zugriffe möglichst kurz vergeben und laufend überprüft. Systeme und Zugänge werden sinnvoll getrennt, Rechte so knapp wie möglich gehalten. Dadurch wird auch die Ausbreitung eines Vorfalls begrenzt und der Schaden bleibt selbst dann überschaubar, wenn Zugangsdaten kompromittiert werden.

12 Fazit

Österreichs Unternehmen haben Cyber Security als zentralen Faktor für stabile Betriebsfähigkeit erkannt und ihre Sicherheitsprogramme in vielen Bereichen weiterentwickelt. Gleichzeitig wird deutlich, dass sich die Bedrohungslage weiter zuspitzt und Angriffe zunehmend als dauerhafte Belastung wirken. Damit verschiebt sich der Fokus weg von der reinen Abwehr einzelner Vorfälle hin zur Frage, wie belastbar Organisationen unter anhaltendem Druck bleiben und wie schnell sie nach einem Vorfall wieder betriebsfähig werden.

Schadenseindämmung allein reicht dafür nicht aus. Entscheidend ist, ob Wiederanlauf, Datenwiederherstellung und Krisenabläufe im Ernstfall zuverlässig funktionieren und nicht nur konzeptionell vorhanden sind. Effiziente und sichere Backup- und Recovery-Ansätze, regelmäßige Wiederherstellungstests sowie klar definierte Wiederanlaufziele und Verantwortlichkeiten sind dafür zentrale Bausteine. Nur durch geübte Abläufe lässt sich vermeiden, dass ein hohes subjektives Sicherheitsgefühl in der Praxis zur Selbstüberschätzung wird.

Mit dem breiteren Einsatz von AI entsteht zudem ein neues Spannungsfeld. AI kann die Abwehr unterstützen, wird aber auch von Angreifern genutzt und erhöht damit die Anforderungen an Cyber Security aus Unternehmenssicht. Zugleich gewinnt Zero Trust weiter an Relevanz, der Ansatz reduziert implizites Vertrauen und schränkt die Bewegungsfreiheit von Angreifern in der Umgebung ein, was die Cyber Security bedeutend steigert. Auch die Regulatorik wirkt als Cyber-Security-Treiber in Unternehmen, setzt aber voraus, dass Betroffenheit und Umsetzungsstatus sauber eingeordnet und als Programm gesteuert werden.

Die Ergebnisse unterstreichen, dass Ressourcen und Priorisierung eng zusammenhängen. Wenn Budgets und Kapazitäten nicht im gleichen Maß wie der Bedrohungsdruck wachsen, müssen Maßnahmen konsequent dort ansetzen, wo sie Wirksamkeit und Resilienz messbar erhöhen. Cyber Security ist damit kein abgeschlossener Prozess, sondern eine kontinuierliche Management-Aufgabe, die laufende Anpassung, Tests und klare Governance verlangt. Unternehmen, die Resilienz, Nachweisfähigkeit und Wiederanlauf konsequent stärken, reduzieren Risiken spürbar und sichern langfristig Stabilität, Vertrauen und Wettbewerbsfähigkeit.

13 Methode & Sample

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

Erhebungsmethode:
Standardisierte Telefonbefragung (CATI)

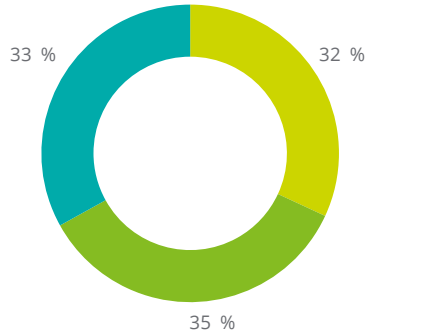
Befragungszeitraum:
Dezember 2025 und Jänner 2026

Stichprobe:
351 Unternehmen

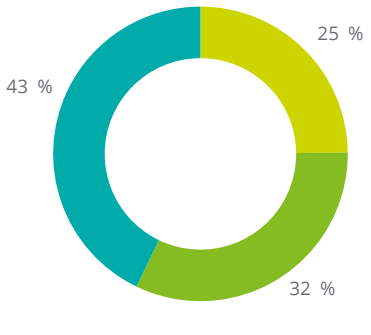
Gewichtung:
Nach Anzahl der Mitarbeiter:innen und Region

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

Branche



Unternehmensgröße



14 Kontakt & Impressum

Karin Mair
Managing Partner |
Technology & Transformation und
Strategy, Risk & Transactions

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

Georg Schwondra
Partner |
Cyber

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

Herausgegeben von:
Deloitte Consulting GmbH

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

Unter redaktioneller Mitarbeit von:
Armin Nowshad und Theresa Kopper

Grafik und Layout:
Claudia Hussovits

15 Anhang

- NISG 2026
- Cyber Resilience Act
- AI Act

NISG 2026

Das österreichische Gesetz zur Sicherung von Netz- und Informationssystemen gemäß der EU-Richtlinie NIS2

Was ist NISG 2026?

Das Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) ist ein österreichisches Bundesgesetz zur Umsetzung der dazugehörigen EU-Richtlinie und regelt erstmals verbindliche Mindestanforderungen an Cyber-Security-Maßnahmen sowie verpflichtende Meldeprozesse für Unternehmen und Einrichtungen in ausgewählten kritischen und wirtschaftlich relevanten Sektoren in Österreich.

Während sich frühere Regelungen primär auf klassische Betreiber kritischer Infrastrukturen konzentrierten, erfasst das NISG 2026 nun auch eine Vielzahl von Industrie-, Digital- und Dienstleistungsunternehmen, sofern sie in bestimmten Sektoren tätig sind und definierte Größenkriterien erfüllen.

Für Unternehmen bedeutet das:

- verpflichtende organisatorische und technische Sicherheitsmaßnahmen,
- formalisierte Meldeprozesse bei Cybervorfällen,
- sowie eine stärkere Einbindung der Unternehmensleitung in die Steuerung der Cyber Security.

Da der operative Anwendungsbeginn am **01.10.2026** liegt, müssen betroffene Organisationen bereits jetzt interne Zuständigkeiten klären, Reporting-Prozesse aufsetzen und die Maßnahmenumsetzung vorbereiten.

Wer ist betroffen?

Das Gesetz unterscheidet:

- **Wesentliche Einrichtungen** und
- **Wichtige Einrichtungen**

Erfasst sind Organisationen aus insgesamt **18 Sektoren** gem. § 2 NISG 2026, u.a. Energie, Verkehr, Gesundheitswesen, digitale Infrastruktur, öffentliche Verwaltung sowie verarbeitendes Gewerbe.

Die Einstufung erfolgt in der Regel anhand von:

- Unternehmensgröße (Mitarbeiteranzahl, Umsatz und Bilanzsumme)
- wirtschaftlicher Bedeutung,
- sowie sektoraler Kritikalität.

Wichtig

Auch Unternehmen, welche nicht als „wesentliche“ oder „wichtige“ Einrichtung eingestuft sind, können über Lieferketten- und Vertragsanforderungen indirekt betroffen sein. NISG-pflichtige Unternehmen müssen Sicherheitsrisiken entlang der Lieferkette berücksichtigen und geben entsprechende Cyber-Security-Maßnahmen und Meldepflichten häufig an ihre Zulieferer weiter.

Kernpflichten für betroffene Einrichtungen

Governance
CyberSecurity wird zur Leitungsaufgabe, indem das Management die Umsetzung und Wirksamkeit der Risikomanagementmaßnahmen sicherstellen und überwachen muss.

Risikomanagementmaßnahmen
Einrichtungen müssen u.a. Risikoanalysen durchführen sowie u. a. Maßnahmen zu

- Reaktion auf Sicherheitsvorfälle,
- Business Continuity und
- Lieferketten- und Zugriffssicherheit (z.B. Mehrfaktor-Authentifizierung)

implementieren.

Meldepflichten bei Cyber-Vorfällen
Bei erheblichen Sicherheitsvorfällen gelten gestufte Meldefristen:

- Frühwarnung: bis 24h nach Kenntnisnahme
- Vorfallsmeldung: bis 72h nach Kenntnisnahme
- Abschlussbericht: spätestens einen Monat nach der Übermittlung der Vorfallsmeldung

Registrierung & Nachweisführung
Betroffene Einrichtungen müssen sich innerhalb von drei Monaten ab Inkrafttreten (§ 29 Abs. 3) registrieren und strukturierte Angaben elektronisch an die zuständige Behörde übermitteln.

Aufsicht & Sanktionen

Die Einhaltung des NISG 2026 wird durch die neue nationale **Cybersicherheitsbehörde** (dem Bundesministerium für Inneres nachgeordnete organisatorische Behörde) überwacht.

Sanktionsrahmen:

- **Wesentliche Einrichtungen:** bis zu 10 Mio. EUR oder 2 % weltweiter Jahresumsatz
- **Wichtige Einrichtungen:** bis zu 7 Mio. EUR oder 1,4 % weltweiter Jahresumsatz

(je nachdem, welcher Betrag höher ist)

Was Unternehmen jetzt konkret tun sollten

01 Betroffenheitsanalyse durchführen

02 Rollen & Verantwortlichkeiten festlegen

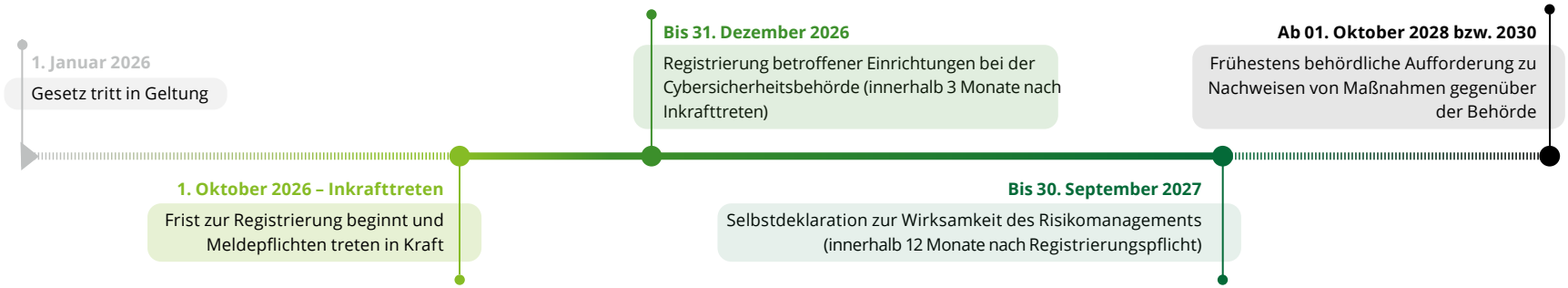
03 Gap-Analyse gegenüber gesetzlichen Anforderungen durchführen

04 Berichtspflichten bei Sicherheitsvorfällen definieren und vorbereiten

05 Registrierung & Nachweisfähigkeit sicherstellen

06 Umsetzungs-Roadmap erstellen

Timeline



Cyber Resilience Act (CRA)

Die EU-Verordnung zur Cyber-Sicherheit von Produkten mit digitalen Elementen

Was ist der CRA?

Der Cyber Resilience Act (CRA) ist die EU-Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Hardware und Software wie zum Beispiel vernetzte Geräte, Apps oder eingebettete Software) und deren Remote-Datenverarbeitungslösungen.

Erstmals werden EU-weit verbindliche Anforderungen u. a. an:

- die sichere Entwicklung („security by design"),
- das Schwachstellenmanagement sowie
- die Bereitstellung von Sicherheitsupdates

für Produkte festgelegt, die in der EU in Verkehr gebracht oder bereitgestellt werden.

Während sich bestehende Regelungen primär auf Organisationen (z.B. NIS2) konzentrieren, adressiert der CRA direkt die Cyber-Sicherheit von Produkten selbst über deren gesamten Lebenszyklus hinweg.

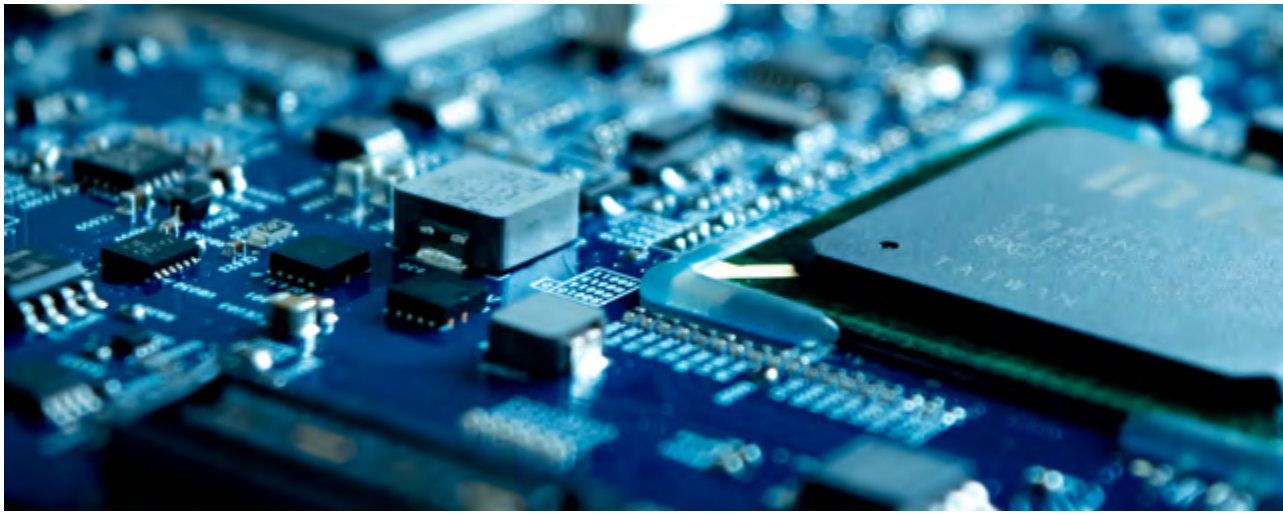
Für Unternehmen bedeutet das:

- verpflichtende Sicherheitsanforderungen bei Entwicklung und Bereitstellung digitaler Produkte,
- formalisierte Meldeprozesse für Schwachstellen und Sicherheitsvorfälle,
- sowie Nachweis- und Konformitätsanforderungen (inkl. CE-Kennzeichnung).

Wer ist betroffen?

Die Verordnung gilt für sogenannte „Produkte mit digitalen Elementen", d.h. Produkte, deren bestimmungsgemäße oder vorhersehbare Nutzung eine direkte oder indirekte Datenverbindung zu Gerät oder Netzwerk umfasst.
Betroffen sind insbesondere:

- Hersteller digitaler Produkte
- Importeure
- Distributoren



Kernpflichten für betroffene Organisationen

Produkt-Governance
Cyber-Sicherheit wird integraler Bestandteil des Produktlebenszyklus, indem Hersteller Sicherheitsanforderungen bereits bei Konzeption, Entwicklung und Wartung berücksichtigen müssen.

Technische und organisatorische Maßnahmen
Hersteller müssen u.a.:

- Sicherheitsrisiken systematisch bewerten,
- Schwachstellen identifizieren und beheben,
- Sicherheitsupdates über einen definierten Supportzeitraum bereitstellen.

Meldepflichten bei Sicherheitsvorfällen
Bei aktiv ausgenutzten Schwachstellen oder schwerwiegenden Sicherheitsvorfällen gelten künftig Meldepflichten gegenüber Behörden über eine zentrale EU-Meldeplattform.

Konformitätsbewertung & Dokumentation
Betroffene Produkte müssen:

- CRA-konform entwickelt werden,
- einer Konformitätsbewertung unterzogen werden,
- sowie mit CE-Kennzeichnung bereitgestellt werden.

Aufsicht & Sanktionen

Die Einhaltung des CRA wird durch nationale **Marktüberwachungs-behörden** überwacht.

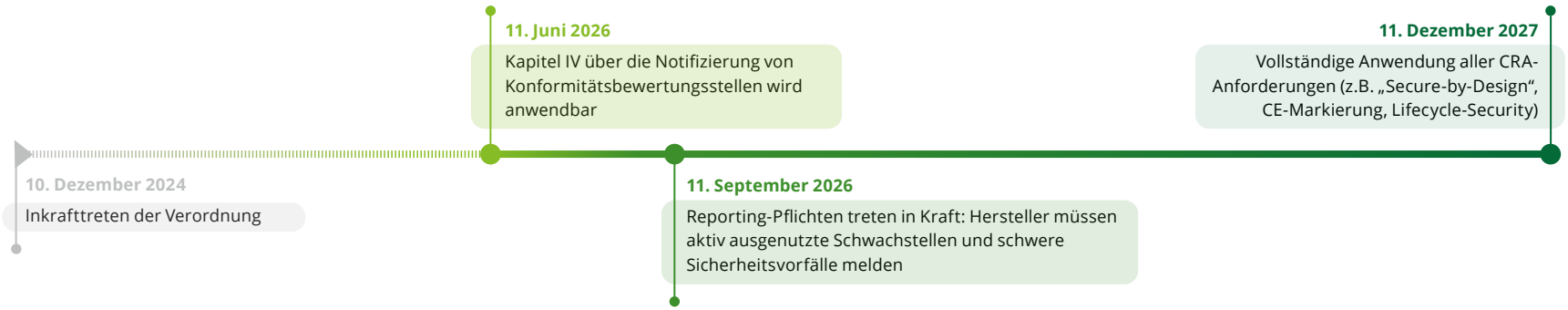
Bei Verstößen können Maßnahmen der Marktüberwachung (z.B. Einschränkung oder Rücknahme vom Markt) angeordnet werden.

Sanktionsregelungen werden von den Mitgliedstaaten festgelegt und im nationalen Vollzug angewandt.

Was Unternehmen jetzt konkret tun sollten

01 Betroffenheitsanalyse für Produkte mit digitalen Elementen durchführen
02 Rollen entlang der Lieferkette (Hersteller / Importeur / Distributor) klären
03 Gap-Analyse gegenüber CRA-Sicherheitsanforderungen durchführen
04 Vulnerability- und Incident-Reporting-Prozesse vorbereiten
05 Konformitätsbewertungs- und Dokumentationsprozesse etablieren
06 Umsetzungs-Roadmap erstellen

Timeline



AI Act

Die EU-Verordnung für Artificial Intelligence (AI) – risikobasierte Anforderungen für Anbieter, Betreiber und weitere Akteure entlang der AI-Wertschöpfung

Was ist der AI Act?

Der AI Act (Verordnung (EU) 2024/1689) ist die **zentrale EU-Regulierung für Artificial Intelligence (AI)** und verfolgt einen risikobasierten Ansatz: Je nach Art des AI-Systems bzw. AI-Modells und dessen Einsatzkontext steigen die regulatorischen Anforderungen – von Transparenzpflichten bis hin zu umfassenden Governance-, Dokumentations- und Kontrollpflichten bei Hochrisiko-AI.

Die Verordnung enthält außerdem Regeln zu:

- verbotenen AI-Praktiken,
- General-Purpose-AI-Modellen (GPAI; allgemein einsetzbare AI-Modelle, z.B. für Text, Bild oder Code),
- sowie ein eigenes Governance- und Aufsichtsregime.

Wer ist betroffen?

Der AI Act erfasst u.a.:

- Anbieter von AI-Systemen und GPAI-Modellen
- Betreiber/Anwender von AI-Systemen in der EU
- Importeure und Distributoren
- Produkthersteller, die AI in Produkte integrieren

Entscheidend ist nicht nur der Sitz des Unternehmens, sondern u. a., ob AI-Systeme/Modelle auf dem EU-Markt bereitgestellt, in Betrieb genommen oder in der EU genutzt werden. Der AI Act hat damit eine marktbezogene EU-Reichweite.

Wichtig

Der AI Act richtet sich nicht nur an AI-Entwickler, sondern auch an Organisationen, die AI-Systeme einkaufen, integrieren oder produktiv einsetzen (z.B. als Betreiber), sofern die regulatorischen Tatbestände erfüllt sind. Der Anwendungsbereich ist damit rollen- und use-case-basiert, nicht primär größenbasiert.

Kernpflichten für betroffene Organisationen

Verbotene AI-Praktiken
Bestimmte AI-Anwendungen sind grundsätzlich verboten, insbesondere in Bereichen mit besonders hohem Risiko für Grundrechte (z.B. bestimmte manipulative/exploitative Praktiken, Social Scoring und bestimmte biometrische Konstellationen).

AI Literacy
Anbieter und Betreiber müssen Maßnahmen setzen, um eine ausreichende AI Literacy (grundlegende AI-Kompetenz im Unternehmen, z.B. sicherer und informierter Umgang mit AI) bei Mitarbeitenden und sonstigen eingesetzten Personen sicherzustellen, abhängig von Kontext, Kenntnissen, Erfahrung und Risiko des Einsatzes.

Hochrisiko-AI: Klassifizierung und Pflichten
Ein AI-System ist u.a. dann Hochrisiko-AI, wenn es in den Anwendungsbereich bestimmter Produktregime fällt (Annex I) oder in Annex III gelistet ist (mit enger Ausnahmelogik).

Für Hochrisiko-AI gelten u.a. Anforderungen zu:

- Risikomanagement
- Daten-/Data Governance
- technischer Dokumentation
- Logging/Aufzeichnung
- menschlicher Aufsicht
- Genauigkeit, Robustheit und Cybersecurity

GPAI-Modelle
Für Anbieter von General-Purpose-AI-Modellen gelten zusätzliche Pflichten (u.a. Dokumentation, Informationen für nachgelagerte Integratoren, Copyright-Policy, Trainingsdaten-Zusammenfassung).

Für GPAI-Modelle mit systemischem Risiko kommen zusätzliche Anforderungen hinzu (u.a. Evaluierung, Risikominderung, Incident-Reporting, Cybersecurity).

Timeline

2. Februar 2026
Frist für Leitlinien der Kommission zur praktischen Umsetzung bestimmter Artikel (z. B. Post-Market-Monitoring)

2. August 2026
Anwendung aller Vorschriften des AI Act, einschließlich der Verpflichtungen für AI-Systeme mit hohem Risiko (z.B. in Gesundheitswesen, Verkehr, Justiz) außer Artikel 6(1)

2. August 2027
Anwendung aller Vorschriften des AI Act einschließlich Artikel 6(1)

Aufsicht & Sanktionen

Der AI Act sieht ein mehrstufiges Governance-Modell vor:

- **EU-Ebene:** u.a. das AI Office bei der Europäischen Kommission
- **Mitgliedstaaten:** nationale zuständige Behörden und ein Single Point of Contact

Für GPAI-Modelle hat die Europäische Kommission exklusive Aufsichts- und Durchsetzungsbefugnisse; die operative Umsetzung erfolgt über das AI Office (Art. 88).

Sanktionsrahmen (Art. 99 / Art. 101):

- **Verbotene AI-Praktiken nach Art. 5:** bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes
- **Bestimmte Verstöße gegen zentrale Pflichten:** bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes
- **Falsche/irreführende Angaben gegenüber Behörden:** bis zu 7,5 Mio. EUR oder 1 % des weltweiten Jahresumsatzes
- **Bereitsteller von GPAI-Modellen:** bis zu 15 Mio. EUR oder 3 % (separates Kommissionsregime)

Was Unternehmen jetzt konkret tun sollten

01 AI-Inventar aufbauen
(entwickelt, eingekauft, integriert, genutzt – inkl. GenAI/Shadow AI)

02 Rollen bestimmen
(Provider / Deployer / Importeur / Distributor / Integrator)

03 Use-Case-Screening gegen Art. 5 / Art. 6 / Art. 50
(Verbote, Hochrisiko, Transparenz) durchführen

04 Governance & Verantwortlichkeiten festlegen

05 Dokumentations- und Nachweisfähigkeit vorbereiten
(insb. bei Hochrisiko-AI und GPAI-Integration)

06 Betriebsprozesse für Monitoring & Vorfälle definieren

07 AI-Literacy-Programm rollen- und risikobasiert starten

Deloitte.