Bericht

KMU im KI-Zeitalter: Wege durch die Komplexitäten der Cybersicherheit zu mehr Resilienz

Mit Forschungen und Analysen von

Sage

IDC

Methodik und Kontext der Erhebung

Joel Stradling
Senior Research Director,
European Security, IDC

Dieser Bericht stützt sich auf die Ergebnisse einer weltweiten Studie, die von IDC im Auftrag von Sage durchgeführt wurde und bei der 2.210 kleine Unternehmen in acht Märkten befragt wurden.

Die von IDC-Analyst Joel Stradling verfasste Studie zum Thema „KMU im KI-Zeitalter: Wege durch die Komplexitäten der Cybersicherheit zu mehr Resilienz“, die im IDC InfoBrief (März 2026; IDC #EUR254487126) veröffentlicht wurde, untersucht, wie KMU auf aktuelle und aufkommende Herausforderungen im Bereich Cybersicherheit reagieren.

Sie beleuchtet ihre wichtigsten Bedenken und Sicherheitsstrategien in Bezug auf KI und Lösungen von Drittanbietern. Darüber hinaus werden die strategischen Veränderungen identifiziert, die erforderlich sind, um von einer reaktiven Verteidigung zu proaktiver Sicherheit und einer nachhaltigen, risikoorientierten Cyber-Resilienz zu gelangen.

Die Studie umfasste die folgenden Branchen: Finanzdienstleistungen, Gesundheitswesen, Telekommunikation, Energie, Fertigung, Rohstoffe, Einzelhandel, Software und Informationsdienstleistungen, Transport und Reisen, Unternehmens- und Personaldienstleistungen, Bildung, Behörden, gemeinnützige Organisationen, Wirtschaftsprüfung und Steuern, Bauwesen sowie Gastgewerbe und Freizeit.

Quelle: IDC-InfoBrief, „SMBs in the Age of AI: Navigating Cyber Complexity and Building Resilience,“ gesponsert von Sage, April 2026, IDC Doc #EUR254487126.

Von der Erhebung erfasste Länder

- Kanada
- Spanien
- USA
- Portugal
- Frankreich
- Vereinigtes Königreich
- Deutschland
- Südafrika

Unternehmensgröße

1–9
Kleinstunternehmen

10–99
Kleinunternehmen

100–499
Mittelständische Unternehmen

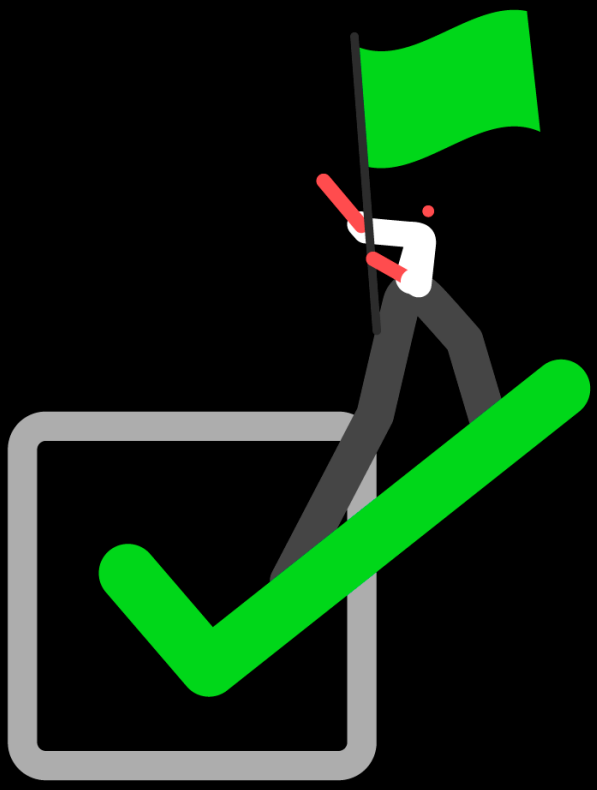
KI sollte für jedes kleine und mittlere Unternehmen eine Wachstumschance darstellen, nicht nur für diejenigen mit den besten Sicherheitsressourcen. Kleinere Unternehmen sind nach wie vor zurückhaltender, da die sichere Einführung in der Praxis immer noch eine Herausforderung darstellt. Wenn wir wollen, dass mehr kleine und mittlere Unternehmen von KI profitieren, müssen wir die Einführung von Cybersicherheit durch integrierte Sicherheitsvorkehrungen, klarere Leitlinien und praktische Unterstützung vereinfachen.“

Gustavo Zeidan
Chief Information Security Officer, Sage

Inhaltsverzeichnis

Zusammenfassung

Kleine und mittlere Unternehmen (KMU) erhöhen ihre Investitionen in die Cybersicherheit und treiben die Einführung von KI voran. Dennoch hinken die Sicherheitsmaßnahmen vielerorts dem Tempo des Wandels hinterher, wodurch sie einem erhöhten Risiko ausgesetzt sind, da die Bedrohungen schneller zunehmen als ihre Resilienz.



Dieser Bericht basiert auf einer Umfrage unter 2.210 KMU in acht Märkten und untersucht, wie kleine und mittlere Unternehmen auf die sich wandelnden Herausforderungen im Bereich der Cybersicherheit reagieren. Ein besonderer Schwerpunkt liegt dabei auf der Einführung von KI und den Risiken durch Drittanbieter. Cybersicherheit ist für KMU mittlerweile eine zentrale geschäftliche Priorität.

In dieser Studie geben 52 % der KMU an, dass die Gewährleistung von Cybersicherheit und Datenschutz eine ihrer obersten Prioritäten für die nächsten zwölf Monate ist – nach dem Unternehmenswachstum (59 %) an zweiter Stelle und deutlich vor dem Ausbau der KI-Nutzung (33 %). Gleichzeitig erwarten 60 % eine Erhöhung ihrer Ausgaben für Cybersicherheit, was eine klare Handlungsabsicht signalisiert.

Bei vielen KMU halten die Maßnahmen jedoch noch nicht mit den Risiken Schritt. Etwa die Hälfte gibt an, jedes Jahr einen Cybervorfall zu erleben, und proaktive Sicherheitsmaßnahmen sind insbesondere bei kleineren Unternehmen nach wie vor begrenzt,. So bezeichnen nur 13 % der Kleinstunternehmen und 21 % der kleinen Unternehmen ihren Ansatz als proaktiv, während es bei den mittelständischen Unternehmen 48 % sind.

KI erhöht den Druck. Zwar schafft sie keine völlig neuen Risiken, macht bekannte Bedrohungen jedoch schneller, überzeugender und schwieriger zu bewältigen. Viele KMU, insbesondere kleinere Unternehmen, befinden sich noch in den frühen Phasen der Vorbereitung auf KI-bezogene Bedrohungen. 84 % der Kleinstunternehmen und 65 % der kleinen Unternehmen geben an, unvorbereitet zu sein oder sich erst am Anfang der Vorbereitung zu befinden.

Gleichzeitig geben 22 % an, über keine spezifischen Sicherheitsmaßnahmen für KI-Anwendungen zu verfügen; bei den Kleinstunternehmen steigt dieser Anteil sogar auf 44 %.

SaaS-Lösungen von Drittanbietern und Risiken in der Lieferkette stellen einen großen blinden Fleck dar. Obwohl SaaS-Tools in KMU-Ökosystemen allgegenwärtig sind, überwachen 43 % der Kleinstunternehmen Drittanbieter nicht regelmäßig oder kontinuierlich, sondern verlassen sich auf statische Zertifizierungen oder einmalige Überprüfungen. Dadurch wird die Echtzeit-Transparenz hinsichtlich Anbieterrisiken eingeschränkt und die Wahrscheinlichkeit erhöht, dass Sicherheitslücken unentdeckt bleiben, bis es zu Beeinträchtigungen kommt.

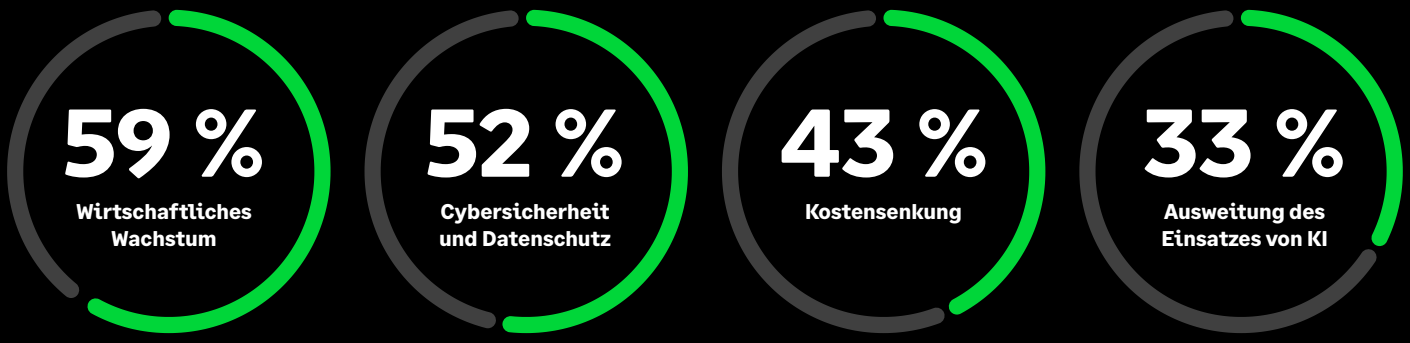
Die Ergebnisse weisen auf eine klare Notwendigkeit hin: KMU brauchen keine zusätzliche Komplexität. Sie benötigen einfachere, praktischere Wege, um reaktive, toolbasierte Sicherheit hinter sich zu lassen und das Risikomanagement zu einem festen Bestandteil des Geschäftsalltags zu machen.

Das bedeutet, Sicherheit von Anfang an zu integrieren, die tägliche Disziplin zu stärken und den Fokus auf klare Verantwortlichkeiten, regelmäßige Überwachung und die Sensibilisierung der Mitarbeitenden zu legen – und zwar auf eine Weise, die der Größe des Unternehmens entspricht. Dies richtig zu handhaben ist nicht nur für einzelne Organisationen wichtig, sondern auch für das Vertrauen der Kunden, die Lieferketten und die Resilienz des gesamten digitalen Ökosystems.

Cybersicherheit ist für KMU mittlerweile eine zentrale Priorität – doch konkurrierende IT-Anforderungen belasten die Budgets

Auf die Frage nach ihren wichtigsten geschäftlichen Prioritäten für die nächsten 12 Monate nannten mehr als die Hälfte der KMU (52 %) Cybersicherheit und Datenschutz – damit liegen diese Themen knapp hinter dem Unternehmenswachstum (59 %) und vor Kostensenkungen (43 %). Dies deutet auf einen deutlichen Mentalitätswandel hin. Cyberrisiken werden nicht mehr als rein technisches Problem betrachtet, sondern als wesentliches geschäftliches Anliegen.

Die wichtigsten geschäftlichen Prioritäten für dieses Jahr:



Geplante Aufstockung des Sicherheitsbudgets in den nächsten 12 Monaten:

51 % 1–9 Kleinstunternehmen

59 % 10–99 Kleinunternehmen

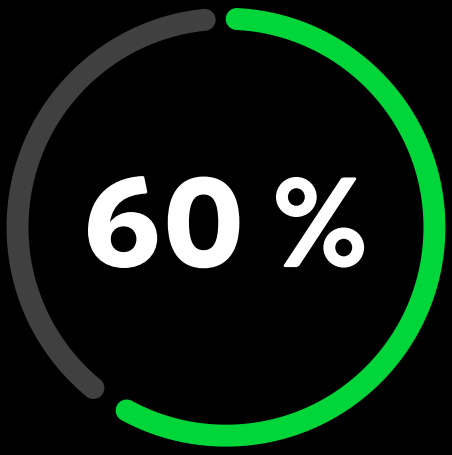
65 % 100–499 Mittelständische Unternehmen

Sage

Diese Absicht wird durch geplante Investitionen untermauert. Sechs von zehn KMU (60 %) geben an, dass sie in den nächsten 12 Monaten mit einem Anstieg ihrer Ausgaben für Cybersicherheit rechnen. Dies deutet sowohl auf ein Bewusstsein für das Problem als auch auf eine Bereitschaft zum Handeln hin. Konkurrierende Herausforderungen, darunter Kostenkontrolle und die beschleunigte Einführung von KI (33 %), führen jedoch dazu, dass die Fortschritte uneinheitlich ausfallen.

Infolgedessen rückt Cybersicherheit zwar eindeutig auf der Prioritätenliste nach oben, doch führen höhere Ausgaben nicht immer zu einer besseren Vorbereitung. Das erklärt, warum im gesamten KMU-Markt weiterhin Lücken in Bezug auf Vertrauen, Governance und Umsetzung bestehen.

Die Daten deuten auf eine wachsende Kluft zwischen Absicht und Umsetzung hin. Cybersicherheit ist wichtiger denn je, doch vielen KMU fällt es schwer, sie konsequent umzusetzen.



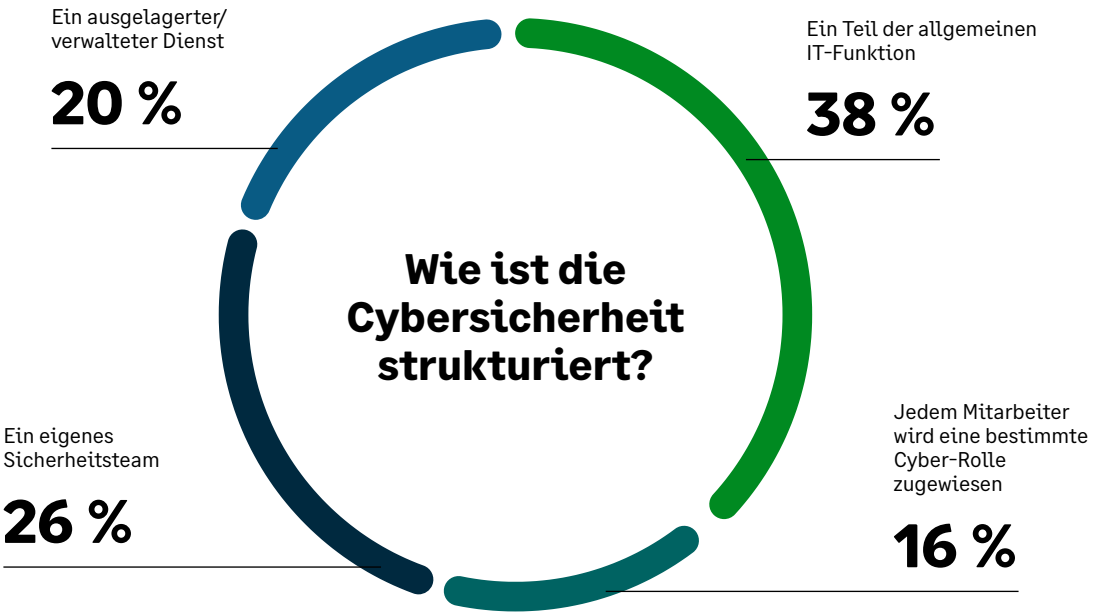
der KMU geben an, dass sie in den nächsten 12 Monaten ihre Ausgaben für Cybersicherheit erhöhen werden

Die Sicherheits-Governance ist in den meisten KMU nach wie vor eher hemdsärmelig – was die Wirkung steigender Investitionen einschränkt

Für die Mehrheit der KMU (38 %) sind die Zuständigkeiten im Bereich Cybersicherheit nach wie vor nur vage definiert und in den allgemeinen Aufgabenbereich der IT-Abteilung eingebettet, anstatt durch klare Zuständigkeiten, formelle Überprüfungszyklen oder dokumentierte Prozesse gestützt zu werden.

Infolgedessen erfolgt die Sicherheitsarbeit oft reaktiv und wird eher durch Vorfälle ausgelöst, als dass sie routinemäßige geschäftliche Praxis ist.

Diese Lücke in der Governance ist einer der Gründe, warum höhere Ausgaben für Cybersicherheit nicht immer zu einer besseren Vorsorge führen. Ohne klare Verantwortlichkeiten, routinemäßige Überwachung und operative Disziplin ist es selbst bei gut gemeinten Investitionen schwierig, eine nachhaltige Risikominderung zu erzielen – insbesondere, da KI und Tools von Drittanbietern das Risiko erhöhen.



Um diese Lücke zu schließen, müssen **KMU die Sicherheit zu einem festen Bestandteil ihres Geschäftsalltags machen** – mit klaren Zuständigkeiten, regelmäßigen Überprüfungen und praktischen Prozessen, die sich im Laufe der Zeit skalieren lassen.

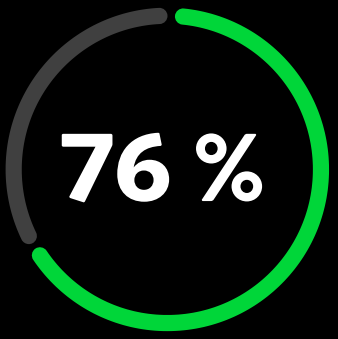
Die meisten KMU verfügen zwar über die richtigen Sicherheitstools, haben jedoch Schwierigkeiten, diese konsequent einzusetzen

Die wichtigsten technischen Sicherheitsmaßnahmen sind in den meisten kleinen und mittleren Unternehmen mittlerweile Standard, doch in Bereichen wie der Softwareverwaltung, der Mitarbeiterschulung und der Planung von Maßnahmen zur Reaktion auf Sicherheitsvorfälle bestehen weiterhin Herausforderungen.

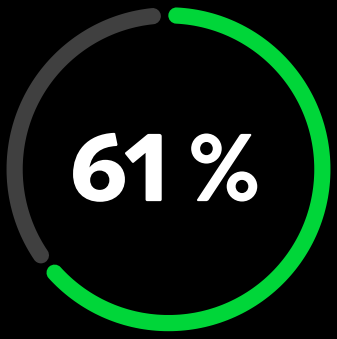
Folglich hängt die Reife im Bereich der Cybersicherheit weniger von der Einführung neuer Kontrollmaßnahmen ab als vielmehr von der Verankerung der erforderlichen operativen Disziplin, um die Wirksamkeit bestehender Sicherheitsvorkehrungen im Zuge der geschäftlichen Entwicklung aufrechtzuerhalten.

Um ihre Cybersicherheitslage zu stärken, sollten KMU einen stärkeren Fokus auf Daten-Governance, Sicherheitskontrollen und Transparenz legen. Mit zunehmender Unternehmensgröße sind hierfür stärker formalisierte Überprüfungszyklen, klar definierte Verantwortlichkeiten und durchgängig dokumentierte Prozesse im gesamten Unternehmen erforderlich.

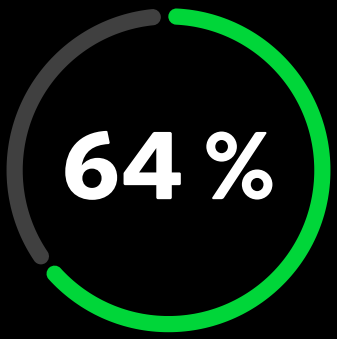
Indikatoren für die Betriebssicherheit:



überprüfen ihre Cybersicherheit regelmäßig

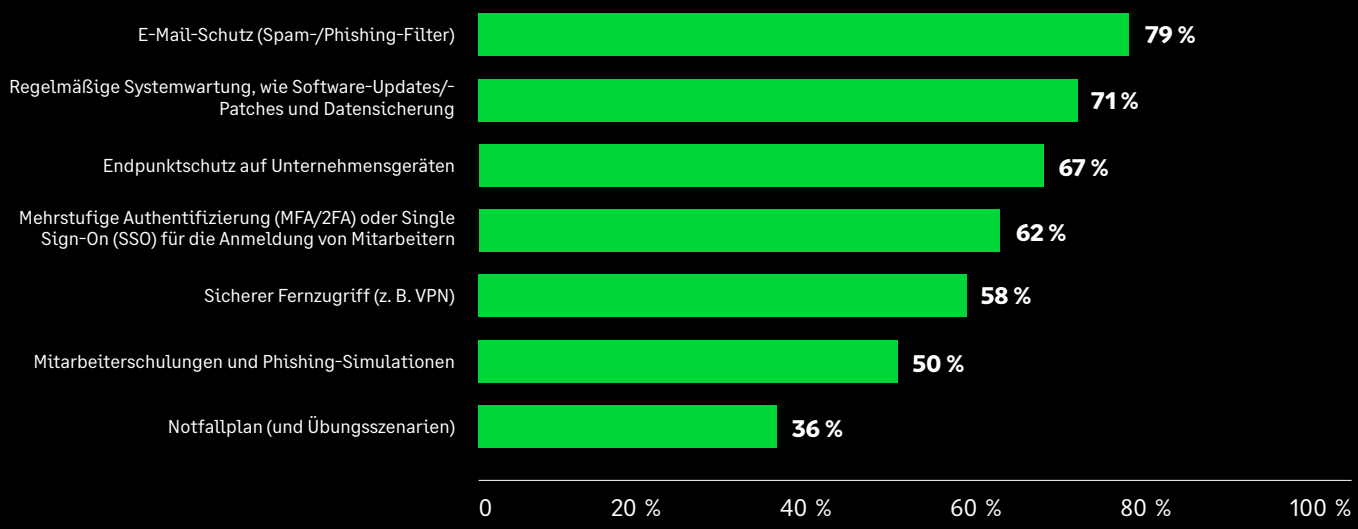


sagen, dass die Mitarbeiter darin geschult sind, Cyberrisiken zu erkennen



überprüfen vor der Auftragsvergabe sorgfältig die Sicherheit von Drittanbietern

Welche Maßnahmen zur Cybersicherheit sind derzeit in Kraft?



Sage

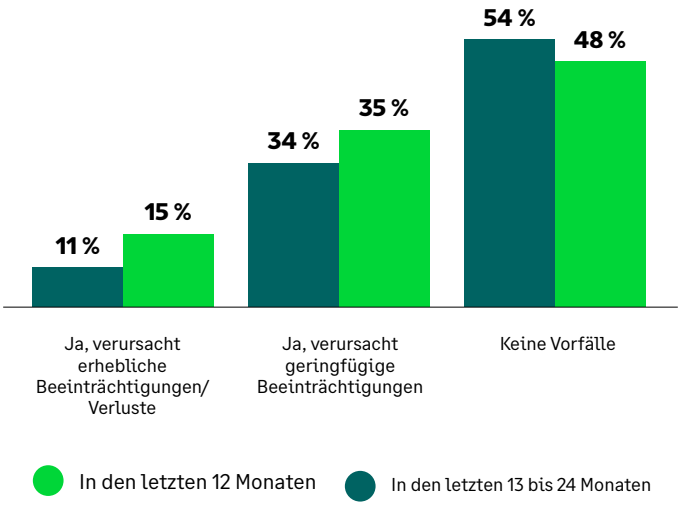
Wenn die Sicherheitsvorkehrungen hemdsärmelig sind, führen Zwischenfälle zu Störungen

Für kleine und mittlere Unternehmen sind Cyberrisiken keine gelegentlichen Beeinträchtigungen mehr. Sie stellen eine permanente geschäftliche Herausforderung dar, die durch ein breiteres und weniger vorhersehbares Spektrum an Bedrohungen geprägt ist: von Phishing und Social Engineering bis hin zu Insiderrisiken, Risiken durch Dritte und Schwachstellen in der Lieferkette.

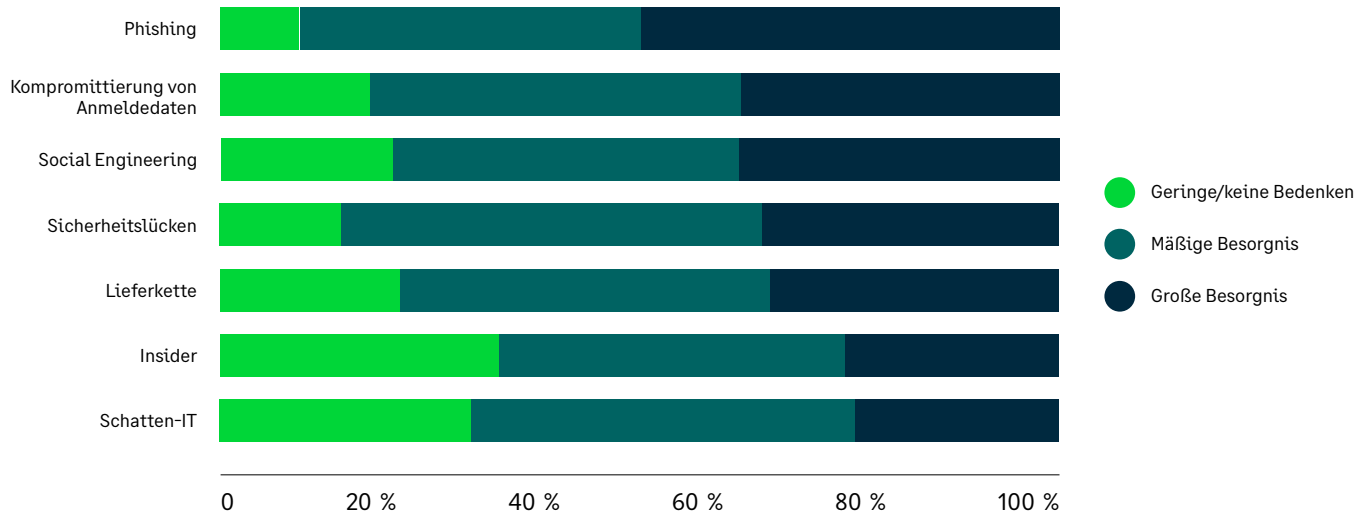
Je größer dieses Risiko wird, desto weniger hängt die Resilienz davon ab, jeden einzelnen Vorfall zu verhindern, und desto mehr davon, Störungen gut bewältigen zu können.

Dadurch verlagert sich der Fokus von den Vorfällen selbst auf die Qualität der Reaktion: Wie schnell werden Probleme erkannt, wie effektiv werden sie eingedämmt und in welchem Umfang kann sich das Unternehmen erholen, während gleichzeitig das Vertrauen, der Cashflow und die Geschäftskontinuität gewahrt bleiben?

Vorfälle im Bereich der Cybersicherheit oder Datenschutzverletzungen



Bedenken hinsichtlich der folgenden Risiken



Für KMU bedeutet dies, **einfache und wiederholbare Verfahren einzuführen**, um Probleme frühzeitig zu erkennen, schnell zu reagieren, die Auswirkungen zu begrenzen und den Geschäftsbetrieb aufrechtzuerhalten, wenn es zu Beeinträchtigungen kommt.

Sich rasch entwickelnde Bedrohungen und eingeschränkte Transparenz erhöhen das Cyberrisiko für KMU

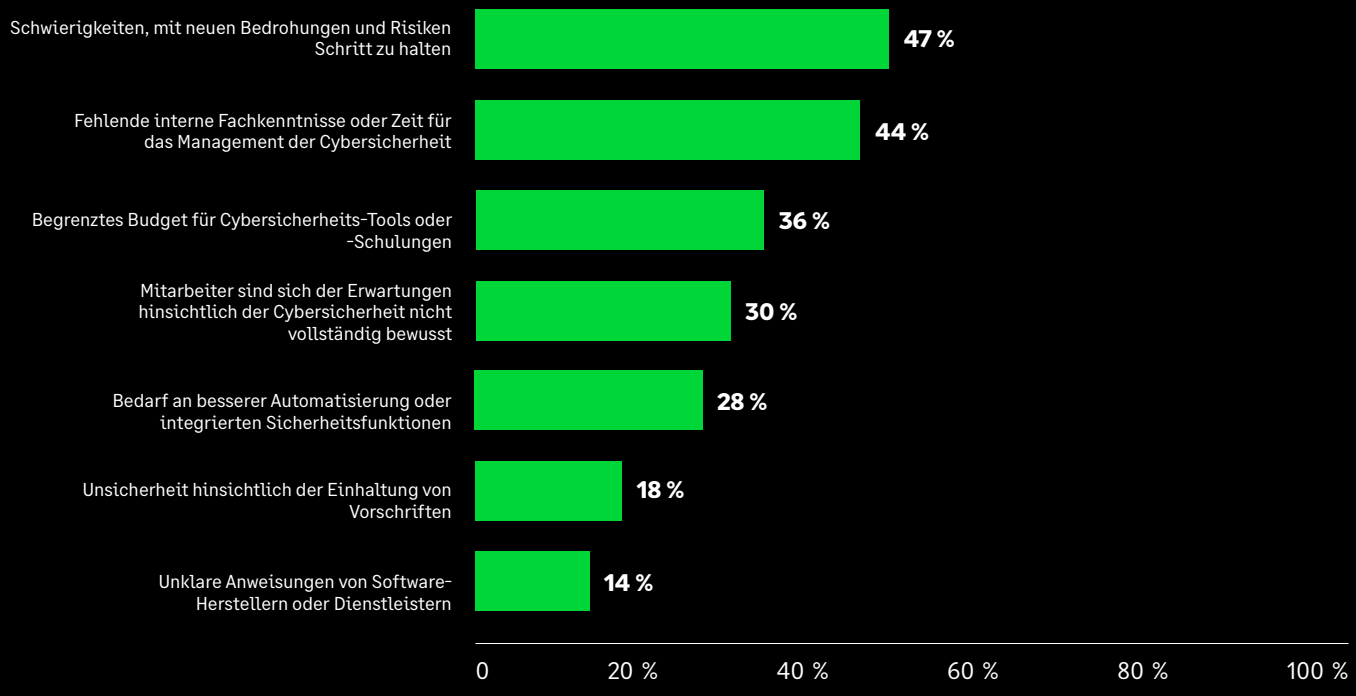
Fast die Hälfte der KMU (47 %) führt das Schritt halten mit neuen Bedrohungen und Risiken als ihre größte Herausforderung im Bereich Cybersicherheit an.

KI-gestützte Angriffe, zunehmend ausgefeilte Phishing-Angriffe sowie eine stärkere Nutzung von Cloud- und SaaS-Diensten lassen sowohl die Geschwindigkeit als auch die Komplexität von Cyberrisiken steigen – häufig schneller, als interne Kapazitäten sich daran anpassen können.

Gleichzeitig fehlt vielen KMU ein klarer, umfassender Überblick über ihre größten Risiken. Begrenzte Fachkompetenzen, konkurrierende operative Prioritäten und Budgetbeschränkungen erschweren die Aufrechterhaltung einer kontinuierlichen Überwachung oder einer strukturierten Risikobewertung. Infolgedessen werden Cyberrisiken oft nur allgemein wahrgenommen, aber im Tagesgeschäft nicht aktiv gemanagt.

Diese Kombination aus sich rasch entwickelnden Bedrohungen und einem unvollständigen Überblick erhöht die Wahrscheinlichkeit erheblich, dass Probleme zu spät erkannt, uneinheitlich priorisiert oder erst nach dem Eintreten von Beeinträchtigungen behoben werden. Für KMU mit hemdsärmeliger Governance und uneinheitlicher operativer Disziplin entsteht dadurch eine anhaltende Diskrepanz zwischen wahrgenommenem Risiko und tatsächlicher Gefährdungslage.

Welche der folgenden Aussagen beschreibt die größten Herausforderungen, denen sich Ihre Organisation beim Management der Cybersicherheit gegenübersieht, am besten?



Um den Fortschritt zu beschleunigen, sollten KMU Lösungen priorisieren, die den betrieblichen Aufwand reduzieren, darunter Automatisierung, integrierte Sicherheitsvorkehrungen und externe Unterstützung, die auf ihre begrenzten Ressourcen abgestimmt sind.

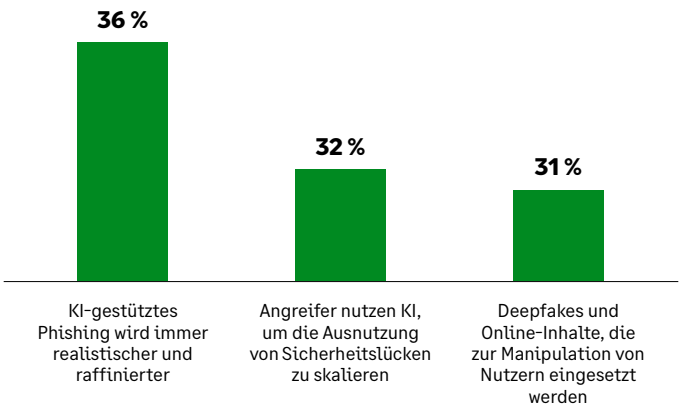
KI-gestützte Bedrohungen entwickeln sich schneller weiter als die Sicherheits-praktiken kleiner und mittlerer Unternehmen

Künstliche Intelligenz verschärft die ohnehin schon schwierige Cybersicherheitslage, und kleinere Unternehmen sind am wenigsten darauf vorbereitet, damit Schritt zu halten.

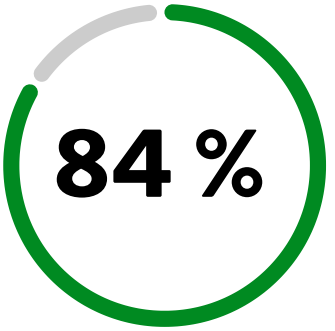
Am stärksten gefährdet sind Kleinst- und Kleinunternehmen: Eine schwächere alltägliche Kontrolle, eine weniger konsequente Überwachung und ein geringeres Sicherheitsbewusstsein der Mitarbeitenden machen sie anfälliger. Denn KI erhöht sowohl die Geschwindigkeit als auch das Ausmaß von Angriffen. Sicherheitsmaßnahmen, die in der Vergangenheit vielleicht noch ausreichten, verlieren zunehmend an Wirksamkeit, da sich die Bedrohungen immer schneller weiterentwickeln.

KMU sollten daher bei den Grundlagen ansetzen: ein stärkeres Sicherheitsbewusstsein, praktische Schutzmaßnahmen und klarere Methoden, um Risiken frühzeitig zu erkennen und zu bewältigen. Doch das ist nur ein Teil der Lösung. Da sich KI-bezogene Bedrohungen weiterentwickeln, benötigen Unternehmen zudem einfachere Möglichkeiten zur Automatisierung routinemäßiger Sicherheitsaufgaben. So können sie den manuellen Aufwand reduzieren und ihre begrenzten IT- und Sicherheitskapazitäten in den Bereichen mit dem größten Risiko einsetzen.

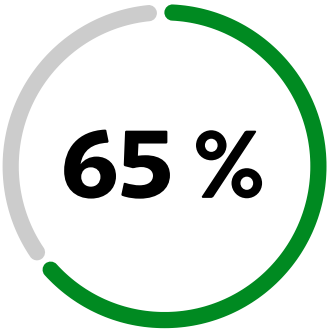
Die drei größten Bedenken hinsichtlich neuer KI-Risiken



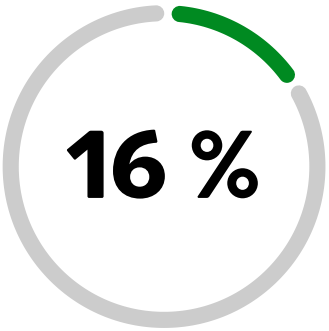
Noch nicht vorbereitet oder erst in der Anfangsphase der Vorbereitung auf KI-bezogene Bedrohungen:



Kleinstunternehmen



Kleinunternehmen



Mittelständische Unternehmen

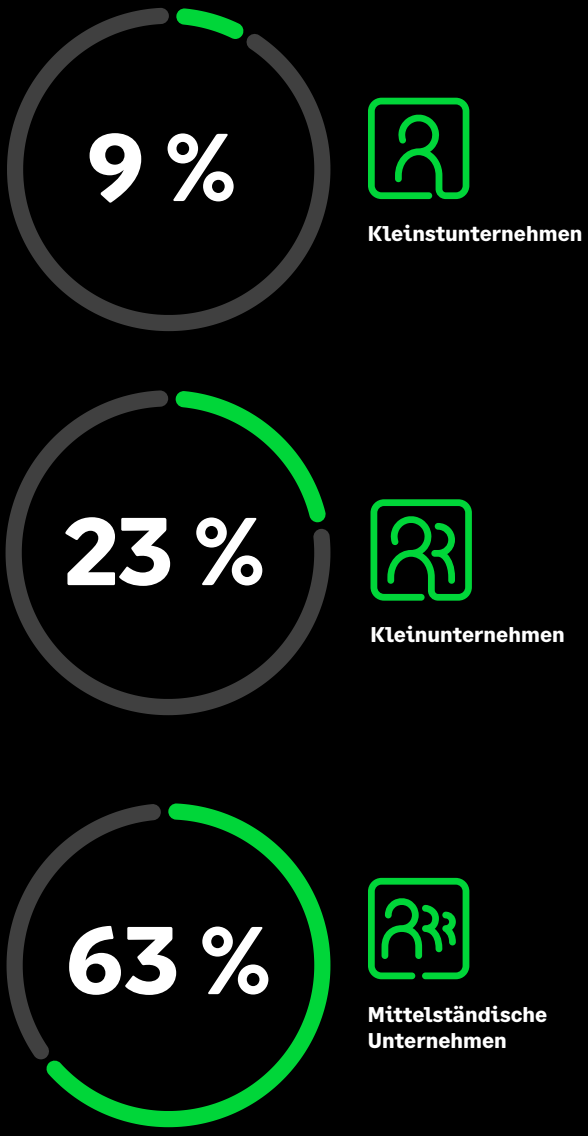
Insbesondere **für weniger erfahrene KMU sind Aufklärung und Sensibilisierung nach wie vor von entscheidender Bedeutung.** Sicherheitsverantwortliche sollten praktischen, leicht umsetzbaren Maßnahmen Vorrang einräumen, die den Teams bei der Erkennung und Minderung KI-bezogener Risiken helfen, ohne dabei unnötige Komplexität zu verursachen.

Sage

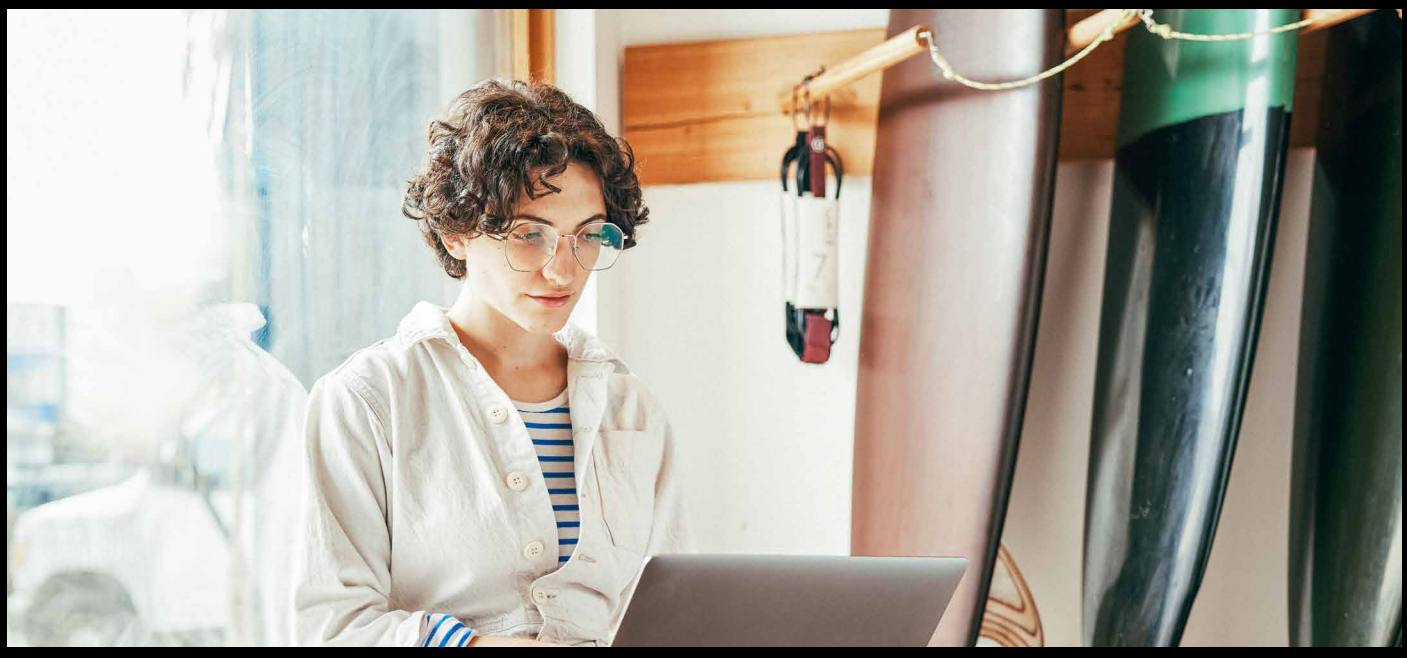
KMU setzen auf KI, um neue Chancen zu nutzen – trotz steigender Sicherheitsrisiken

Ein erheblicher Anteil der KMU sieht in KI Chancen, während ein noch größerer Anteil der Ansicht ist, dass KI das Cyberrisiko erhöht. Die Wahrnehmung variiert je nach Unternehmensgröße. Mittelständische Unternehmen betrachten KI eher als Chance.

KI als Geschäftschance:

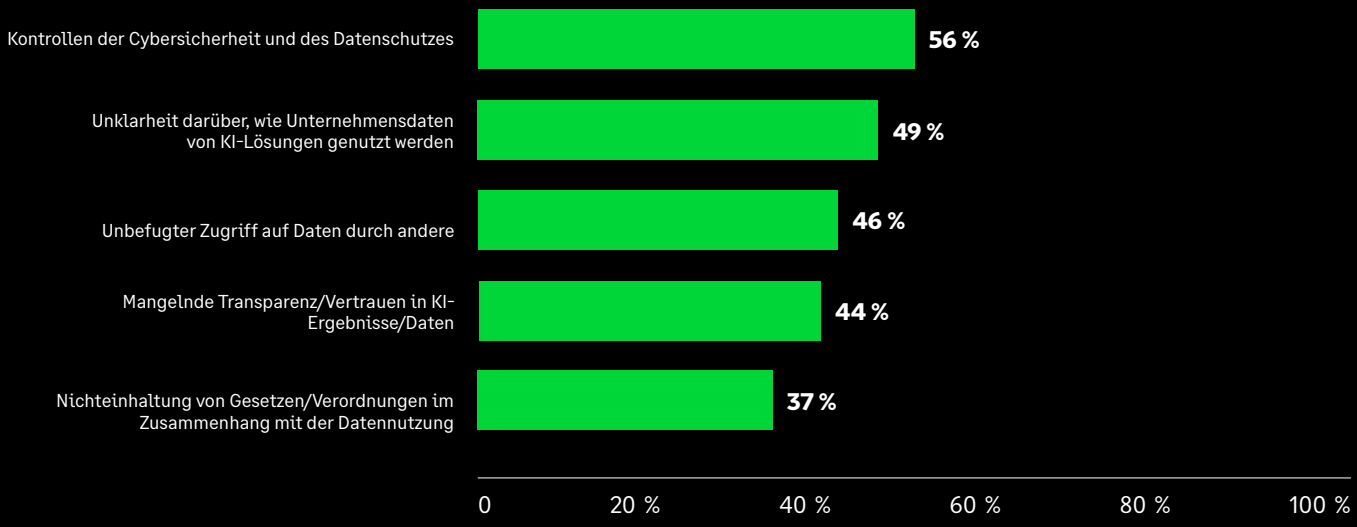


Kleinst- und Kleinunternehmen gehen beim Einsatz von KI mit größerer Vorsicht vor. Dies spiegelt eher Unterschiede im Vertrauen in Sicherheitsmaßnahmen und Governance wider als in den Ambitionen.



Bei der Einführung von KI bestehen Bedenken hinsichtlich Datensicherheit, Governance und Transparenz. Ohne klare Einsicht in die Art und Weise, wie Daten genutzt und geschützt werden, stehen viele KMU der Ausweitung des KI-Einsatzes weiterhin skeptisch gegenüber.

Welche der folgenden Aussagen beschreibt Ihre größten Bedenken hinsichtlich der Einführung oder Nutzung von KI in Ihrem Unternehmen am besten?



Da KI zunehmend in den täglichen Geschäftsbetrieb integriert wird, benötigen kleine und mittlere Unternehmen einen klaren Überblick darüber, wo und wie sie eingesetzt wird, sowie festgelegte Rahmenbedingungen zur Steuerung der damit verbundenen Risiken. Dazu gehört die Erfassung aller KI-Tools und -Systeme im gesamten Unternehmen sowie die Einrichtung geeigneter Kontrollmechanismen, Richtlinien und Verantwortlichkeiten auf Führungsebene. Ohne diese Maßnahmen kann das Tempo der KI-Einführung die Fähigkeit eines Unternehmens zur Risikosteuerung übersteigen. Das führt zu einer erhöhten Gefährdung, anstatt einen Mehrwert zu schaffen.

KMU legen bereits jetzt den Grundstein für die Einhaltung der KI-Vorschriften

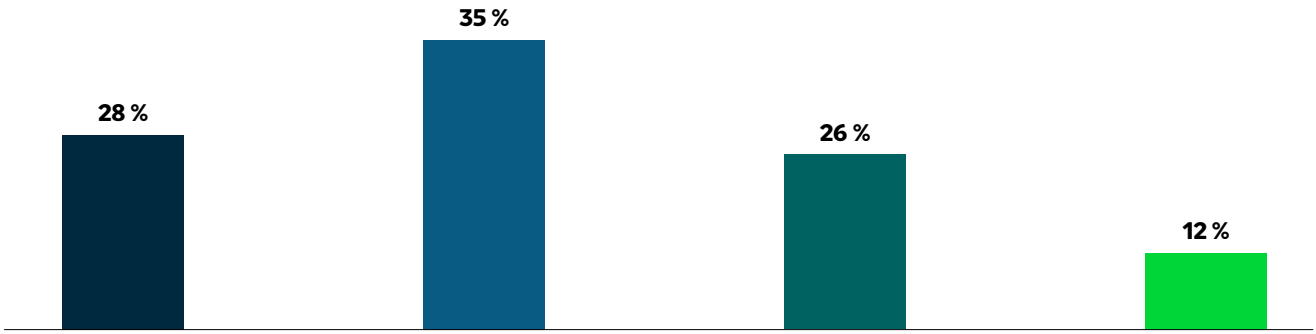
Da immer mehr Vorschriften und Standards im Bereich der KI entstehen, beginnen viele kleine und mittlere Unternehmen damit, Grundlagen für die Einhaltung dieser Vorschriften zu schaffen.

Rahmenwerke wie nationale KI-Vorschriften und freiwillige Verhaltenskodizes sollen Unternehmen dabei unterstützen, übergeordnete politische Leitlinien in praktische, alltägliche Sicherheits- und Governance-Maßnahmen umzusetzen. Immer mehr Regierungen erkennen, dass grundlegende Software- und KI-Sicherheitspraktiken nicht nur von großen Unternehmen, sondern entlang der gesamten Lieferkette umfassend umgesetzt werden müssen. Länder wie das Vereinigte Königreich konzentrieren sich auf praktische und verhältnismäßige Ansätze.

Ein Beispiel hierfür ist der „Software Security Code of Practice“ und das damit verbundene „Software Security Ambassadors Scheme“, die im Rahmen des Cyber-Aktionsplans der britischen Regierung ins Leben gerufen wurden. Das Programm bringt Organisationen des öffentlichen und privaten Sektors – darunter auch Sage – zusammen, um die Umsetzung grundlegender Software-Sicherheitsprinzipien voranzutreiben, praktische Erfahrungen bei der Umsetzung auszutauschen und eine verbesserte Resilienz der gesamten Wirtschaft zu fördern.

> KMU sind das Rückgrat der britischen Wirtschaft. Doch wir wissen, dass sich viele von ihnen mit Investitionen in die Cybersicherheit schwertun, während die Zahl der Cyberbedrohungen steigt. Die Verbesserung der Cyberresilienz im gesamten Vereinigten Königreich ist deshalb eine Priorität der Regierung. Aus diesem Grund hat unser National Cyber Security Centre das „Cyber Action Toolkit“ entwickelt, um KMU dabei zu unterstützen, ihre Cyberabwehr zu stärken. Wir empfehlen allen Unternehmen, unser hochwirksames „Cyber Essentials“-Programm zu nutzen. Es trägt zum Schutz vor gängigen Online-Bedrohungen bei und verringert das Risiko, Opfer eines kostspieligen und geschäftsstörenden Cyberangriffs zu werden.“
>
> **Liz Kendall MP, britische Staatssekretärin für Wissenschaft, Innovation und Technologie**

Bereitschaft von KMU zur Einhaltung von KI-Vorschriften und Sicherheitsstandards



Nicht vorbereitet
Kaum oder gar kein Bewusstsein für bzw. keine Planung hinsichtlich KI-Vorschriften oder -Standards

Erste Schritte
Kenntnis der anstehenden Anforderungen; erste Gespräche oder Planungen laufen bereits

In Bearbeitung
Aktuelle Entwicklung von Richtlinien, Kontrollmechanismen und Governance-Strukturen zur Einhaltung der Vorschriften

Gut vorbereitet
Es sind bereits Prozesse und Sicherheitsvorkehrungen vorhanden, um den neuen Anforderungen gerecht zu werden

Initiativen wie diese zeigen kleinen und mittleren Unternehmen einen pragmatischen Weg auf: die Ausrichtung an anerkannten Rahmenwerken, die Auswahl von Partnern, die sich für eine sichere Entwicklung einsetzen, sowie die frühzeitige Verankerung grundlegender Sicherheitspraktiken angesichts der zunehmenden Verbreitung von KI.

Sage

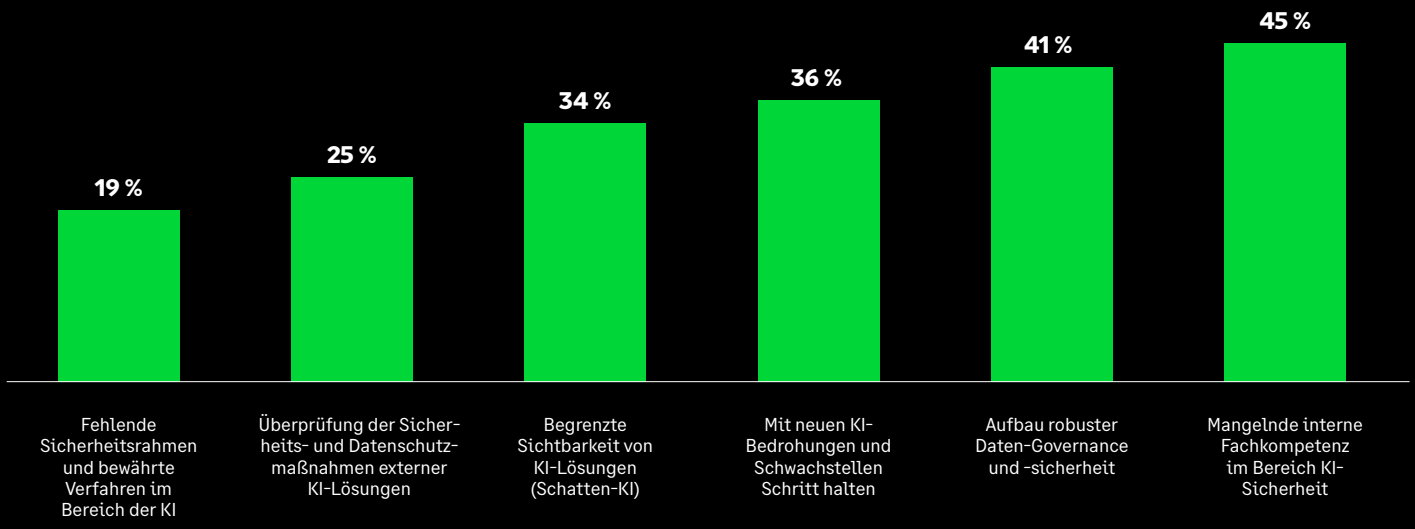
Die Herausforderungen im Bereich KI-Sicherheit für KMU konzentrieren sich auf Qualifikationslücken, Datenschutz und sich rasch verändernde Bedrohungen

KI deckt bei KMU nicht nur eine technologische Lücke auf, sondern auch eine Kompetenzlücke. Viele Unternehmen führen KI schneller ein, als sie die Risiken verstehen, ihre Anfälligkeit einschätzen oder die Sicherheit von Drittanbietern beurteilen können.

Dies ist insbesondere für kleinere Unternehmen eine Herausforderung, in denen die Verantwortung häufig bei einem einzigen IT-Spezialisten oder einem Team aus Generalisten liegt.

Datenschutz und sich rasch entwickelnde Bedrohungen verschärfen diese Herausforderung zusätzlich. Da KI-Tools auf den Zugriff auf Unternehmens- und Kundendaten angewiesen sind, können mangelnde Transparenz und unzureichende Kontrolle das Risiko schnell erhöhen. Gleichzeitig ermöglichen KI-Tools die schnellere, überzeugendere und schwerer zu bewältigende Durchführung bekannter Angriffe, sodass viele KMU Mühe haben, Schritt zu halten.

Die größten Herausforderungen beim Schutz von KI- und GenAI-Anwendungen sowie der entsprechenden Infrastruktur



Für KMU mit begrenzten Fachressourcen ist die Praxisnähe entscheidend. Beschränken Sie den Einsatz von KI auf zugelassene Tools, legen Sie einfache Regeln für die Eingabe von Daten fest, überprüfen Sie die KI-Nutzung regelmäßig und greifen Sie auf vertrauenswürdige Anbieter oder externe Partner zurück, wenn das interne Fachwissen begrenzt ist. Dies trägt zur Risikominderung bei, anstatt die Komplexität zu erhöhen.

Die unzureichende Überwachung von SaaS-Anbietern setzt viele KMU Risiken aus

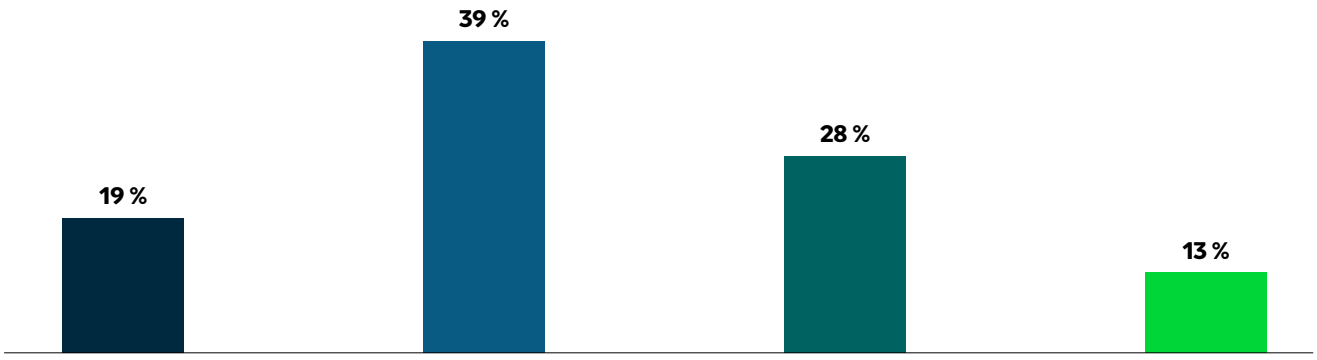
SaaS-Anwendungen und Plattformen von Drittanbietern bilden mittlerweile das Herzstück vieler KMU-Betriebe, doch die Sicherheitsüberwachung erfolgt oft nur sporadisch.

In vielen Unternehmen wird das Lieferantenrisiko nur zu Beginn einer Geschäftsbeziehung oder bei Vertragsverlängerung überprüft, statt es kontinuierlich zu überwachen. Dies führt zu Lücken in der Transparenz, erhöht das Risiko und steigert die Wahrscheinlichkeit, dass Probleme erst erkannt werden, wenn bereits Beeinträchtigungen aufgetreten sind.

Kleinst- und Kleinunternehmen sind besonders gefährdet, da ein erheblicher Anteil angibt, Drittanbieterdienste kaum oder gar nicht regelmäßig zu überwachen. Infolgedessen bleiben potenzielle Probleme möglicherweise unentdeckt, bis es zu Störungen kommt.

Erfahrenere KMU setzen hingegen auf zentralisierte Zugriffskontrollen, ein klar definiertes Management des Benutzerlebenszyklus und regelmäßige Lieferantenüberprüfungen. Dadurch können sie Anomalien besser erkennen und früher reagieren. Angesichts der Ausweitung von SaaS-Ökosystemen und der Einführung KI-gestützter Tools durch externe Anbieter deuten die Ergebnisse darauf hin, dass die Betrachtung der Sicherheit bei Drittanbietern als fortlaufenden Prozess – und nicht als einmalige Überprüfung – von zunehmender Bedeutung ist.

Wie oft überprüfen KMU die Sicherheit von SaaS-Anbietern (Software-as-a-Service)?



Nicht überwacht
Sicherheit wird nur bei der Einführung überprüft

Stichproben
Überprüfungen, die gelegentlich oder bei Auftreten von Problemen durchgeführt werden

Regelmäßige Überprüfungen
Jährliche oder halbjährliche Neubewertungen

Kontinuierliche Überwachung
Automatisierte Tools oder regelmäßige Kontrollen, die in die Sicherheitsprozesse integriert sind

Die Verbesserung der Sicherheit im Zusammenhang mit SaaS-Lösungen von Drittanbietern beginnt für kleine und mittlere Unternehmen mit besserer Disziplin im Alltag: Sie sollten wissen, welche Tools genutzt werden, kontrollieren, wer darauf zugreifen darf, nicht mehr genutzte Konten umgehend löschen und auf nicht autorisierte Apps oder ungewöhnliche Aktivitäten achten. Insbesondere für kleinere Teams ist ein einfacher, einheitlicher Ansatz, der von vertrauenswürdigen Anbietern oder Managed Services unterstützt wird, effektiver, als selbst ein komplexes Überwachungsmodell aufzubauen.

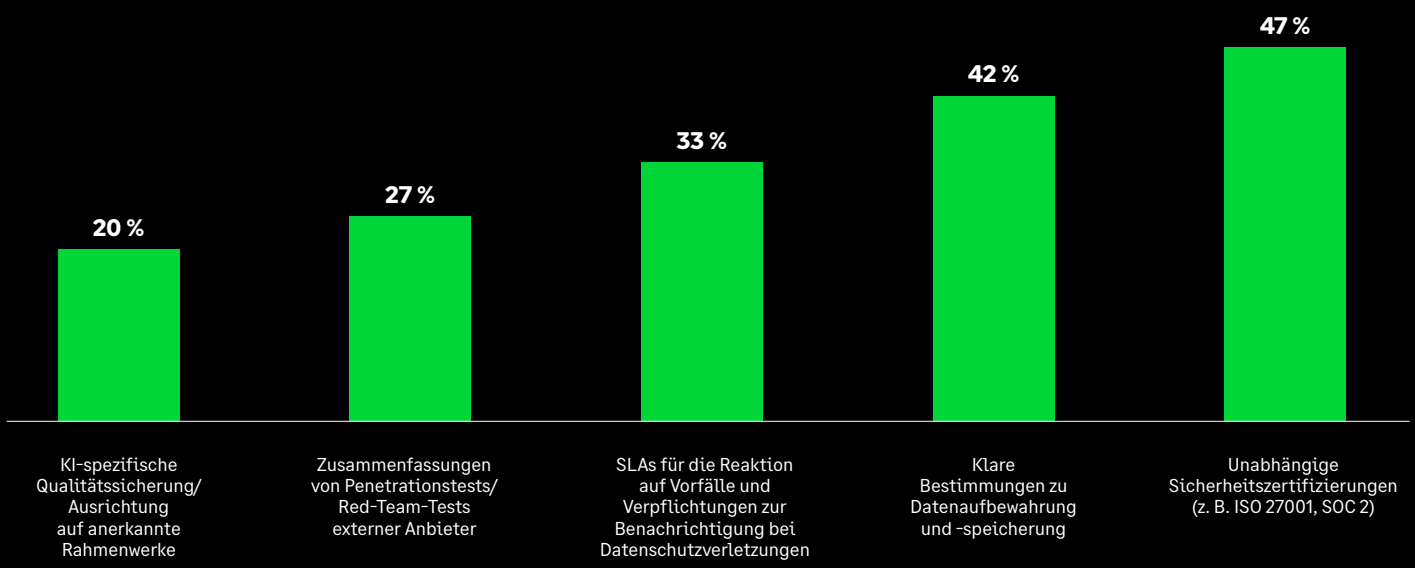
KMU vertrauen bei der Bewertung von Drittanbietern auf klare, überprüfbare Nachweise

Da SaaS- und KI-gestützte Dienste immer stärker in die Abläufe von KMU integriert werden, hängt das Vertrauen in die Anbieter zunehmend von Nachweisen ab, die klar, vertraut und leicht zu überprüfen sind.

KMU legen größten Wert auf unabhängige Zertifizierungen, einen transparenten Umgang mit Daten und klare Verpflichtungen zur Reaktion auf Vorfälle. Diese bieten ihnen die Gewissheit, dass zentrale Sicherheitsmaßnahmen vorhanden sind. Technischere, KI-spezifische Aussagen mögen fortschrittlich klingen, sind für kleinere Unternehmen jedoch oft schwieriger zu bewerten.

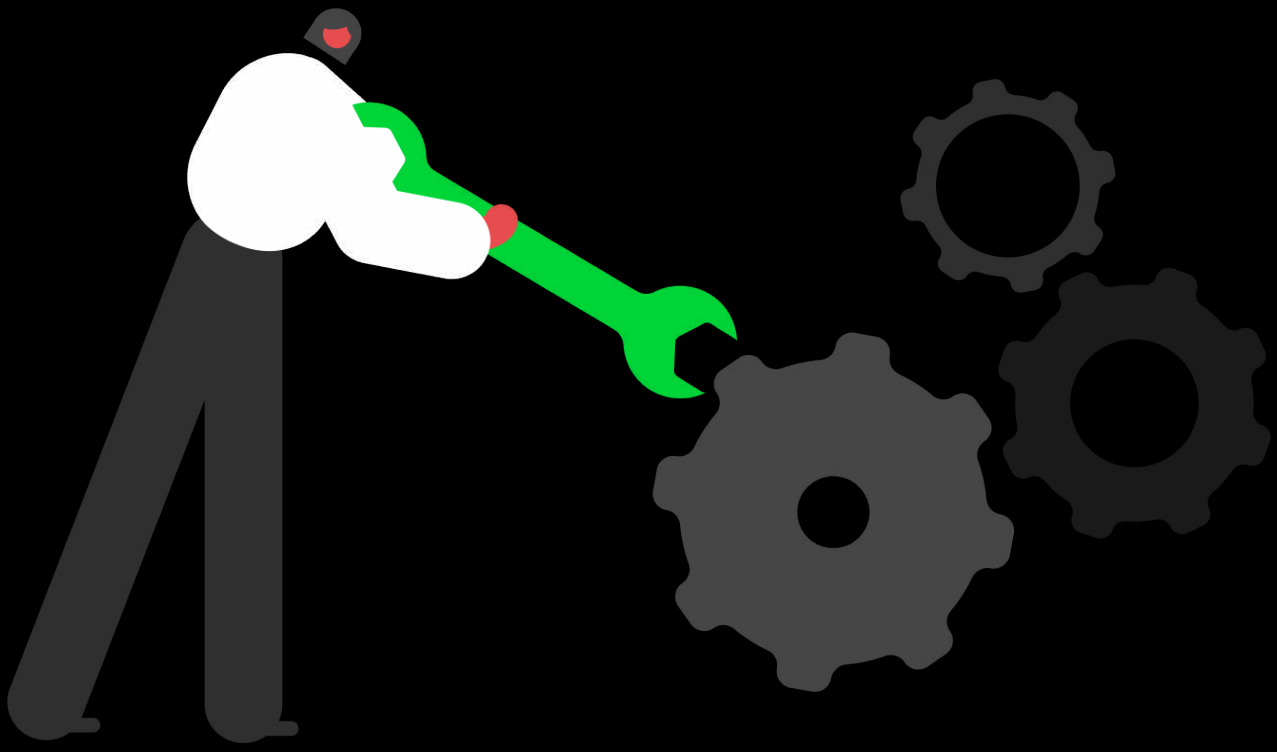
Das macht Klarheit zu einem Wettbewerbsvorteil. Anbieter, die in einfachen Worten erklären können, wie Kundendaten geschützt werden, wo sie gespeichert werden und was im Fehlerfall geschieht, können einfacher Vertrauen gewinnen.

Nachweise, die Vertrauen in die KI-Sicherheit und die verantwortungsvollen Praktiken eines Drittanbieters schaffen



KMU sollten Anbietern den Vorzug geben, die klare, überprüfbare Nachweise darüber vorlegen, wie sie ihre Sicherheit sicherstellen, und diese regelmäßig überprüfen, anstatt es als einmalige Kontrolle zu betrachten.

Erkenntnisse in Taten umsetzen



Sage

Kleinstunternehmen: Mit einfachen, skalierbaren Maßnahmen die Resilienz stärken

Angesichts der zunehmenden Verbreitung von KI ist es von entscheidender Bedeutung, die Verantwortlichkeiten, Überprüfungszyklen und grundlegenden Governance-Strukturen zu stärken. Die Maßnahmen sollten kostengünstig und einfach umzusetzen sein. Dabei sollte der Schwerpunkt auf Einfachheit und einem minimalen Verwaltungsaufwand liegen.

Kurzfristige Maßnahmen

Cybersicherheitslage
Verantwortlichkeiten festlegen: Ernennen Sie einen Sicherheitsbeauftragten und erstellen Sie eine einfache Checkliste für die Reaktion auf Vorfälle, die Eskalation, Backups und externe Unterstützung abdeckt.

KI-Sicherheit
Zugriff auf KI-Systeme sichern: Beschränken Sie den Zugriff auf KI-Systeme auf autorisiertes Personal, ermöglichen Sie eine einfache Protokollierung von Aktivitäten und setzen Sie die Verwendung sicherer Passwörter durch, um Risiken angesichts der zunehmenden Nutzung von KI zu minimieren.

Mittelfristige Pläne

Cybersicherheitslage
Routinen etablieren: Regelmäßige Sicherheitsüberprüfungen einführen, die Zugriffsrechte, Software-Updates, Backups und Tools von Drittanbietern umfassen.

KI-Sicherheit
Regeln festlegen und Mitarbeiter schulen: Regeln für den Umgang mit Daten und Zugriffsprotokolle formalisieren, Mitarbeiterschulungen anbieten und die Grundlagen für eine skalierbare KI-Sicherheit schaffen.

Langfristige Überlegungen

Cybersicherheitslage
Verringerung der Abhängigkeit von internen Fachkräften: Konsolidierung und Standardisierung von Kontrollmaßnahmen, wobei kostengünstige, gebündelte oder verwaltete Dienste Vorrang haben sollten, um den betrieblichen und finanziellen Aufwand zu senken.

KI-Sicherheit
Einführung von Überwachungsmaßnahmen: Einrichtung einer grundlegenden kontinuierlichen Überwachung und Durchführung grundlegender Sicherheitsüberprüfungen der KI-Lösungen von Anbietern. Auswahl von Anwendungen, die vertrauenswürdig und der Sicherheit verpflichtet sind.

Sage

Kleine Unternehmen: Mehr Sicherheit durch Struktur und Disziplin

Kleine Unternehmen müssen Sicherheitsprozesse und die KI-Governance strukturieren. Mit der zunehmenden Verbreitung von KI wird die Formalisierung und konsequente Anwendung von Sicherheitsmaßnahmen zum entscheidenden Faktor bei der Minimierung unkontrollierter Risiken.

Kurzfristige Maßnahmen

Cybersicherheitslage
Formalisierung der Risikotransparenz: Führen Sie ein regelmäßiges Sicherheitsreporting ein, legen Sie fest, wer für wichtige Entscheidungen verantwortlich ist, und stellen Sie sicher, dass Vorfälle und Zugriffsprüfungen auf Führungsebene besprochen werden.

KI-Sicherheit
Transparenz der KI-Ressourcen: Führen Sie ein aktuelles Verzeichnis von KI-Modellen, Agenten, Datensätzen und Diensten. Überwachen Sie die Nutzung nicht autorisierter oder „Schatten"-KI-Anwendungen.

Mittelfristige Pläne

Cybersicherheitslage
Professionalisierung des Sicherheitsbetriebs: Richtlinien teamübergreifend einheitlich anwenden, Risikoprüfungen durch Dritte vor der Beauftragung von Anbietern einführen und bestehende Tools straffen, um die Komplexität zu reduzieren.

KI-Sicherheit
Sichere KI-Interaktionen: Eingaben und Ausgaben validieren, um Prompt-Injection, Jailbreaks und Datenlecks zu verhindern.

Langfristige Überlegungen

Cybersicherheitslage
Integration von Sicherheitsaspekten in geschäftliche Entscheidungen: Sicherheit in Beschaffungsentscheidungen, digitale Initiativen und Expansionspläne einbeziehen, damit sich das Risikomanagement parallel zum Unternehmenswachstum weiterentwickelt.

KI-Sicherheit
Vorsorge für KI-Vorfälle: Notfallplan für KI-Ausfälle oder -Sicherheitsverletzungen dokumentieren und testen. Ein strukturiertes Lieferantenrisikomanagement einführen.

Mittelständische Unternehmen: einheitliche Umsetzung von Sicherheits-maßnahmen im gesamten Unternehmen

Mittelständische Unternehmen verfügen über gut strukturierte Sicherheitsvorkehrungen – mit fest zugewiesenen Rollen, proaktivem Management und einer formellen Überwachung durch Dritte. Der nächste Schritt besteht darin, sicherzustellen, dass diese Reife im Zuge der zunehmenden Digitalisierung und des wachsenden Einsatzes von KI konsistent skaliert wird.

Kurzfristige Maßnahmen

Cybersicherheitslage
Verschärfung bestehender Kontrollen: Erfassung kritischer Ressourcen und wichtiger Lieferanten, teamübergreifende Überprüfung der Zugriffsrechte sowie Identifizierung sich überschneidender oder unzureichend genutzter Sicherheitstools.

KI-Sicherheit
KI-Risikomanagement: Formalisierung eines KI-Sicherheitsrahmens, der Transparenz in Bezug auf KI und Daten, eine kontinuierliche Überwachung auf Systemanomalien sowie ein strukturiertes Lieferantenrisikomanagement umfasst.

Mittelfristige Pläne

Cybersicherheitslage
Standardisierung der Sicherheitspraktiken: Anwendung einheitlicher Kontrollmaßnahmen und Regeln in allen Abteilungen, Einführung strukturierter Lieferantenüberprüfungen, regelmäßige Berichterstattung über wichtige Risikoindikatoren an die Geschäftsleitung.

KI-Sicherheit
Einhaltung gesetzlicher Vorschriften: Sicherstellung, dass der Einsatz von KI den Datenschutz- und KI-Vorschriften entspricht. Einbeziehung von KI-Aspekten in bestehende Rahmenwerke zur Gewährleistung der Sicherheit.

Langfristige Überlegungen

Cybersicherheitslage
Einbindung der Sicherheit in die Unternehmensführung: Integration der Cybersicherheit in die Beschaffung, die Geschäftskontinuität und die strategische Planung, damit sich der Schutz parallel zum Wachstum des Unternehmens weiterentwickelt.

KI-Sicherheit
Adversarial Testing: Prüfung von KI-Systemen auf ihre Resilienz gegenüber Adversarial- oder Red-Team-Angriffen.

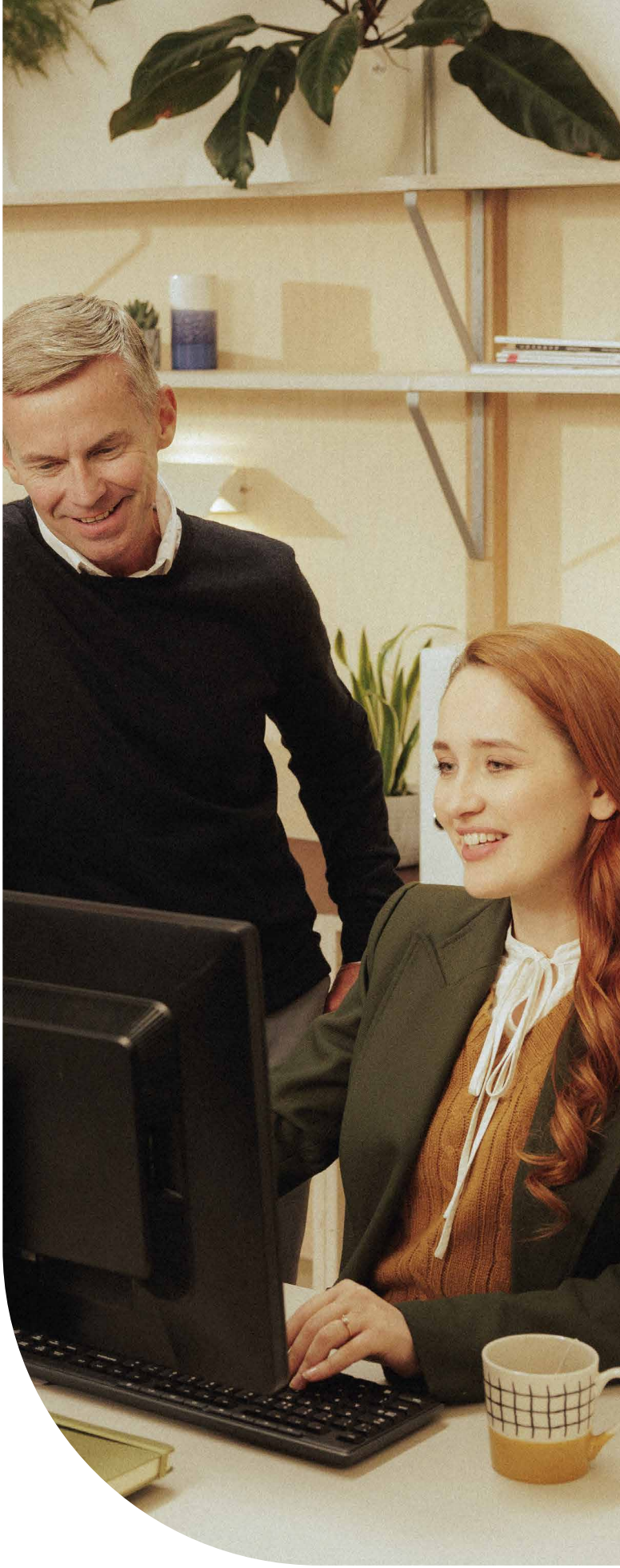
Mitteilung von Sage

Sage setzt sich seit Langem für kleine und mittelständische Unternehmen ein und ist sich deren Chancen und Herausforderungen bewusst. Dieser Bericht zeigt, dass Cybersicherheit mittlerweile eine zentrale geschäftliche Priorität für KMU darstellt. Sie steht auf der Unternehmensagenda gleich hinter dem Wachstum. Dies verdeutlicht, wie eng Cyberresilienz heute mit Vertrauen, Geschäftskontinuität und langfristigem Erfolg verbunden ist.

Angesichts zunehmender Cyberrisiken müssen sich viele KMU mit begrenzten Zeit-, Personal- und Budgetressourcen behaupten, während KI und Technologien von Drittanbietern immer stärker in den Geschäftsalltag integriert werden. Sie sollten diese Herausforderung nicht alleine bewältigen müssen.

Bei Sage konzentrieren wir uns deshalb darauf, KMU dabei zu unterstützen, wirksame Sicherheitsmaßnahmen umzusetzen. Dazu gehören klare Leitlinien, das „Secure-by-Design“-Prinzip und Transparenz hinsichtlich des Datenschutzes und des Einsatzes von KI. Unser Ziel ist es, KMU in die Lage zu versetzen, Risiken zu mindern und gleichzeitig Technologien zu nutzen, um ihr Wachstum voranzutreiben.

Regierungen, Branchenverbände, Softwareanbieter und Lieferanten sollten eng zusammenarbeiten, um KMU klarere Leitlinien, einfachere Schutzmaßnahmen und praktische Unterstützung zu bieten, die ihren realen Bedürfnissen entsprechen.



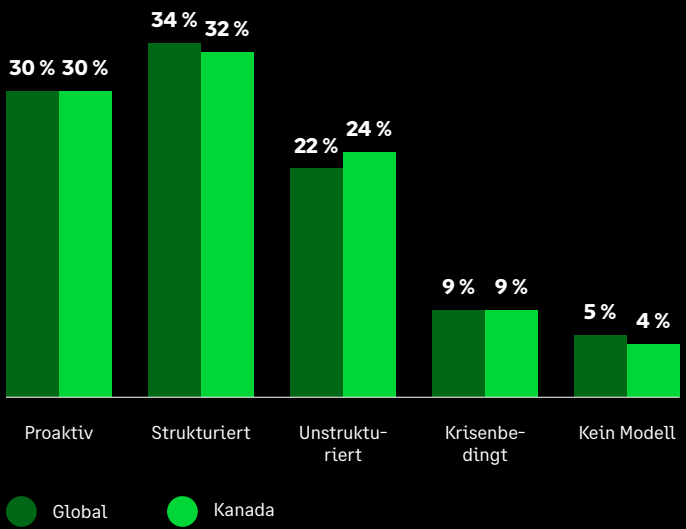
Anhang: Länderprofile

Kanada

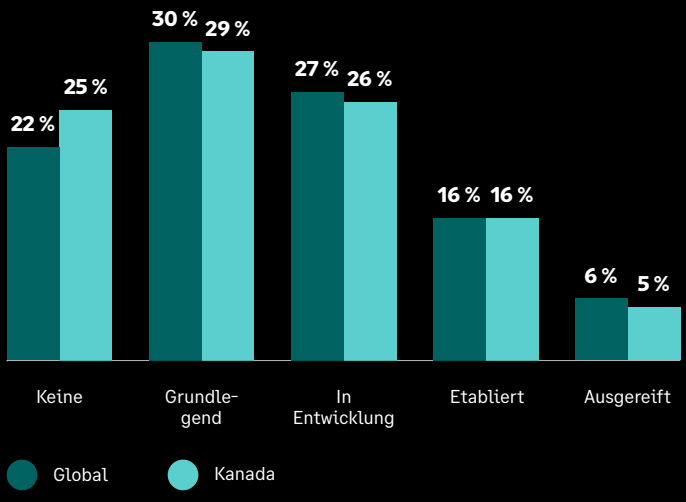
Kanada liegt bei den zentralen Sicherheitsmaßnahmen über dem weltweiten Durchschnitt, was dem Land eine solide Grundlage für den täglichen Schutz bietet und dazu beiträgt, die Zahl der Vorfälle nahe am weltweiten Durchschnitt zu halten.

Bei der KI-Bereitschaft tut sich jedoch eine Lücke auf. Kanada scheint weniger gut darauf vorbereitet zu sein, diese starke Ausgangsbasis in wirksame KI-Sicherheit umzusetzen, was sich in weniger Einführungen praktischer Schutzmaßnahmen, einer geringeren Compliance-Bereitschaft und dem höchsten gemeldeten Mangel an KI-Sicherheitsexpertise zeigt. Der Fokus muss nun von der Aufrechterhaltung der Grundlagen auf den Aufbau der Fähigkeiten, der Aufsicht und der praktischen Schutzmechanismen verlagert werden, die für eine effektivere Bewältigung KI-bezogener Risiken erforderlich sind.

Modell zur Verwaltung der Cybersicherheit



Aktuelles Sicherheitsniveau für KI-gestützte Anwendungen



Cybervorfälle oder Sicherheitsverletzungen im vergangenen Jahr

Kanada	**55 %** Keine Vorfälle	**33 %** Geringfügige Zwischenfälle, die schnell gelöst werden	**10 %** Vorfälle, die zu erheblichen Beeinträchtigungen führen
Global	**54 %** Keine Vorfälle	**34 %** Geringfügige Zwischenfälle, die schnell gelöst werden	**11 %** Vorfälle, die zu erheblichen Beeinträchtigungen führen

Die wichtigsten vorhandenen Sicherheitsmaßnahmen

Kanada	**86 %** E-Mail-Schutz	**82 %** Wartung (Installation von Updates und Backups)	**77 %** MFA/SSO
Global	**79 %** E-Mail-Schutz	**71 %** Wartung (Installation von Updates und Backups)	**67 %** Endpunkt-Schutzmaßnahmen

Zentrale Herausforderungen bei KI-Anwendungen im Sicherheitsbereich

Kanada	**48 %** Unzureichende KI-Sicherheitsex-pertise	**38 %** Starke Datensicher-heit gewährleisten	**41 %** Mit neuen KI-Bedrohungen Schritt halten
Global	**45 %** Unzureichende KI-Sicherheitsex-pertise	**41 %** Starke Datensicher-heit gewährleisten	**36 %** Mit neuen KI-Bedrohungen Schritt halten

Die wichtigsten Schutzmaßnahmen gegen Risiken und Gefahren durch KI

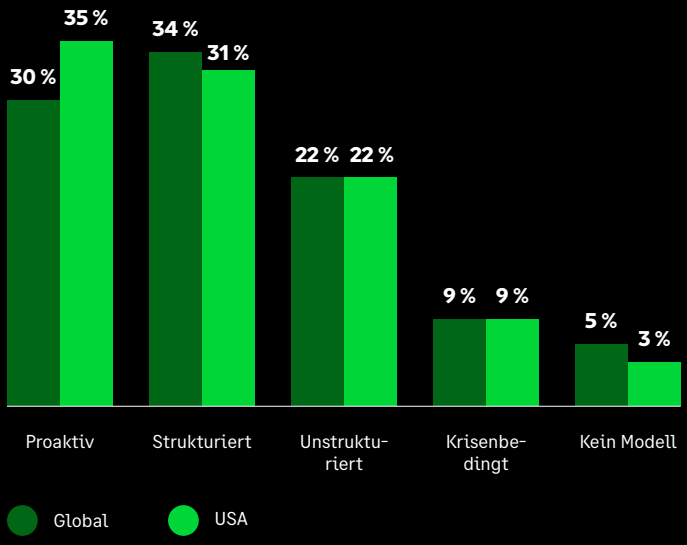
Kanada	**35 %** Klare Richtlinien zum Einsatz von KI	**34 %** Zugelassene KI-Tools mit Administrator-funktionen	**32 %** KI-Tools vor der Einführung testen
Global	**41 %** Klare Richtlinien zum Einsatz von KI	**38 %** Zugelassene KI-Tools mit Administrator-funktionen	**33 %** KI-Tools vor der Einführung testen

USA

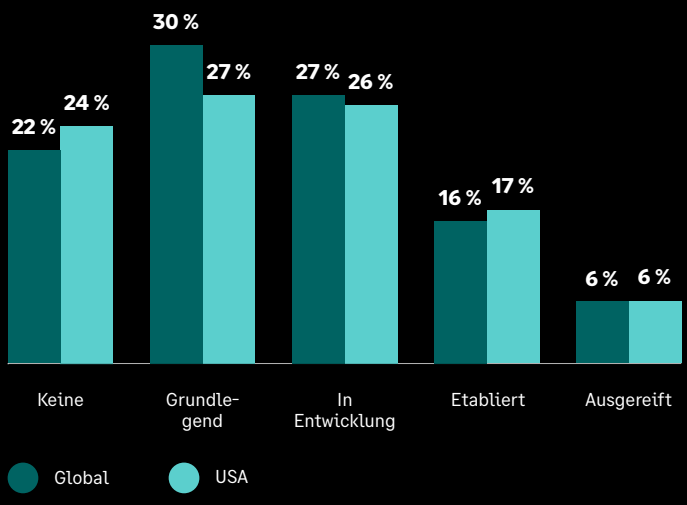
Die Vereinigten Staaten liegen bei der Umsetzung von Cybersicherheitsbewusstsein in eine strukturierte tägliche Praxis über dem globalen Durchschnitt. Dadurch haben sie eine stärkere Ausgangsposition als viele andere Märkte, da KI zunehmend in die Geschäftsabläufe integriert wird.

Der höhere Anteil schwerwiegender Vorfälle deutet jedoch darauf hin, dass der Schwerpunkt nun von der Grundlagenbildung auf die Verbesserung der Resilienz in der Praxis verlagert werden muss – insbesondere in Bezug auf Datensicherheit, Aufsicht und die Fähigkeit, auf sich rasch entwickelnde Bedrohungen zu reagieren.

Modell zur Verwaltung der Cybersicherheit



Aktuelles Sicherheitsniveau für KI-gestützte Anwendungen



Cybervorfälle oder Sicherheitsverletzungen im vergangenen Jahr

USA	55 % Keine Vorfälle	32 % Geringfügige Zwischenfälle, die schnell gelöst werden	13 % Vorfälle, die zu erheblichen Beeinträchtigungen führen
Global	54 % Keine Vorfälle	34 % Geringfügige Zwischenfälle, die schnell gelöst werden	11 % Vorfälle, die zu erheblichen Beeinträchtigungen führen

Die wichtigsten vorhandenen Sicherheitsmaßnahmen

USA	85 % E-Mail-Schutz	71 % Wartung (Installation von Updates und Backups)	69 % Endpunkt-Schutzmaßnahmen
Global	79 % E-Mail-Schutz	71 % Wartung (Installation von Updates und Backups)	67 % Endpunkt-Schutzmaßnahmen

Zentrale Herausforderungen bei KI-Anwendungen im Sicherheitsbereich

USA	43 % Unzureichende KI-Sicherheitsex-pertise	38 % Starke Datensicher-heit gewährleisten	38 % Mit neuen KI-Bedrohungen Schritt halten
Global	45 % Unzureichende KI-Sicherheitsex-pertise	41 % Starke Datensicher-heit gewährleisten	36 % Mit neuen KI-Bedrohungen Schritt halten

Die wichtigsten Schutzmaßnahmen gegen Risiken und Gefahren durch KI

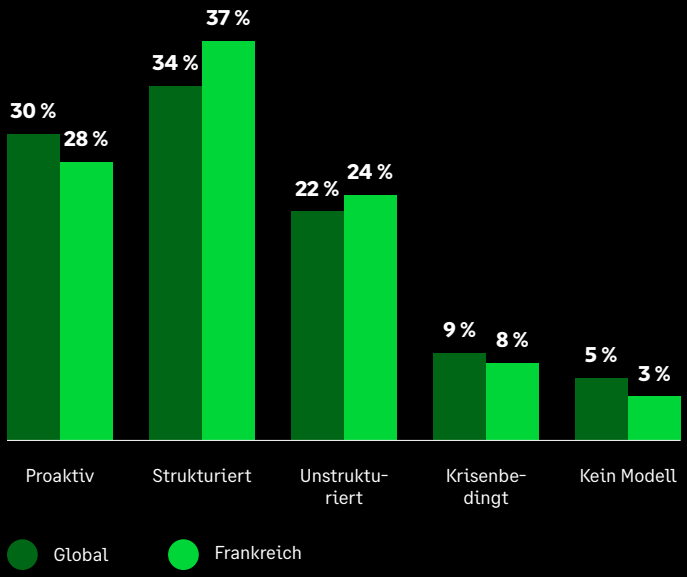
USA	40 % Klare Richtlinien zum Einsatz von KI	39 % Zugelassene KI-Tools mit Administrator-funktionen	34 % KI-Tools vor der Einführung testen
Global	41 % Klare Richtlinien zum Einsatz von KI	38 % Zugelassene KI-Tools mit Administrator-funktionen	33 % KI-Tools vor der Einführung testen

Frankreich

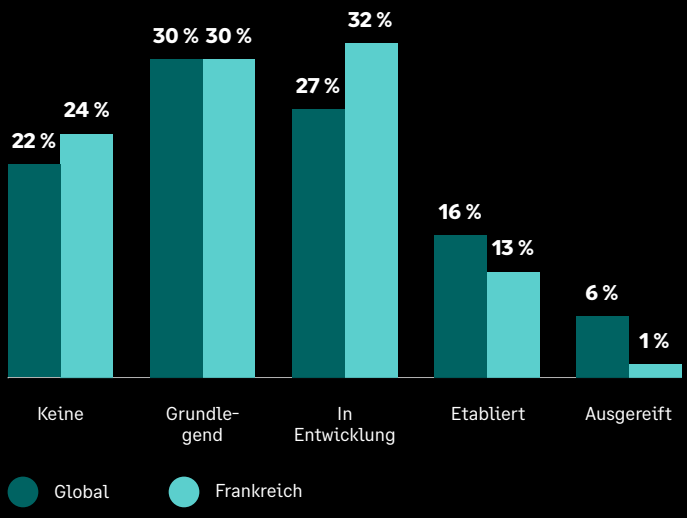
Frankreich ist einem höheren Cyber-Druck ausgesetzt als der weltweite Durchschnitt. Grundlegende Sicherheitsmaßnahmen sind weniger weit verbreitet, der Anteil der Unternehmen, die von erheblichen Beeinträchtigungen berichten, ist höher und der Reifegrad im Bereich der KI-Sicherheit ist geringer. Weniger Unternehmen befinden sich am fortgeschrittenen Ende der Kurve. Dies deutet auf einen Markt hin, in dem die Sicherheitsgrundlagen weniger einheitlich sind und die geschäftlichen Auswirkungen von Cyberrisiken stärker zum Tragen kommen.

Der nächste Schritt besteht darin, sowohl die Grundlagen als auch die Fähigkeit zu stärken, KI-bezogene Risiken in der Praxis zu bewältigen. Bessere Transparenz, stärkerer Datenschutz und eine besser strukturierte Reaktionsbereitschaft werden dabei entscheidend sein – insbesondere in einem Markt, in dem das Vertrauen offenbar stark davon abhängt, wie gut Unternehmen reagieren können, wenn etwas schiefgeht.

Modell zur Verwaltung der Cybersicherheit



Aktuelles Sicherheitsniveau für KI-gestützte Anwendungen



Cybervorfälle oder Sicherheitsverletzungen im vergangenen Jahr

Frankreich	**51 %** Keine Vorfälle	**33 %** Geringfügige Zwischenfälle, die schnell gelöst werden	**15 %** Vorfälle, die zu erheblichen Beeinträchtigungen führen
Global	**54 %** Keine Vorfälle	**34 %** Geringfügige Zwischenfälle, die schnell gelöst werden	**11 %** Vorfälle, die zu erheblichen Beeinträchtigungen führen

Die wichtigsten vorhandenen Sicherheitsmaßnahmen

Frankreich	**77 %** E-Mail-Schutz	**60 %** Wartung (Installation von Updates und Backups)	**69 %** Endpunkt-Schutz-maßnahmen
Global	**79 %** E-Mail-Schutz	**71 %** Wartung (Installation von Updates und Backups)	**67 %** Endpunkt-Schutz-maßnahmen

Zentrale Herausforderungen bei KI-Anwendungen im Sicherheitsbereich

Frankreich	**48 %** Unzureichende KI-Sicherheitsex-pertise	**43 %** Starke Datensicher-heit gewährleisten	**35 %** Begrenzte Trans-parenz hinsichtlich der eingesetzten KI-Tools
Global	**45 %** Unzureichende KI-Sicherheitsex-pertise	**41 %** Starke Datensicher-heit gewährleisten	**36 %** Mit neuen KI-Bedrohungen Schritt halten

Die wichtigsten Schutzmaßnahmen gegen Risiken und Gefahren durch KI

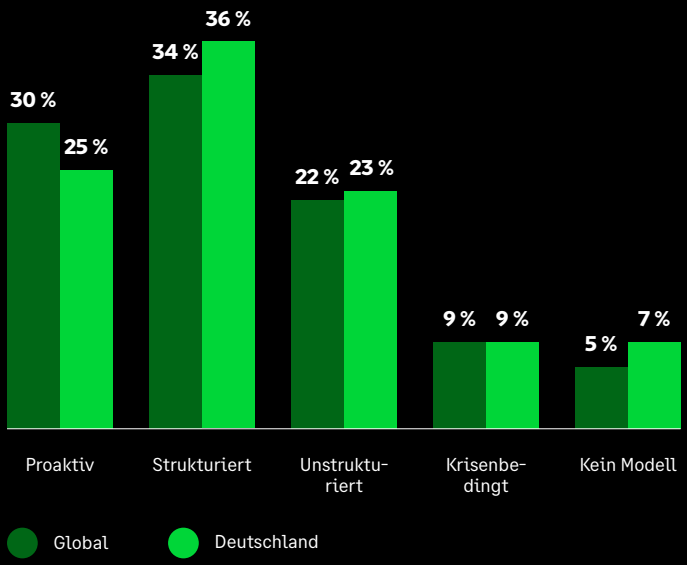
Frankreich	**42 %** Klare Richtlinien zum Einsatz von KI	**38 %** Zugelassene KI-Tools mit Administrator-funktionen	**34 %** KI-Tools vor der Einführung testen
Global	**41 %** Klare Richtlinien zum Einsatz von KI	**38 %** Zugelassene KI-Tools mit Administrator-funktionen	**33 %** KI-Tools vor der Einführung testen

Deutschland

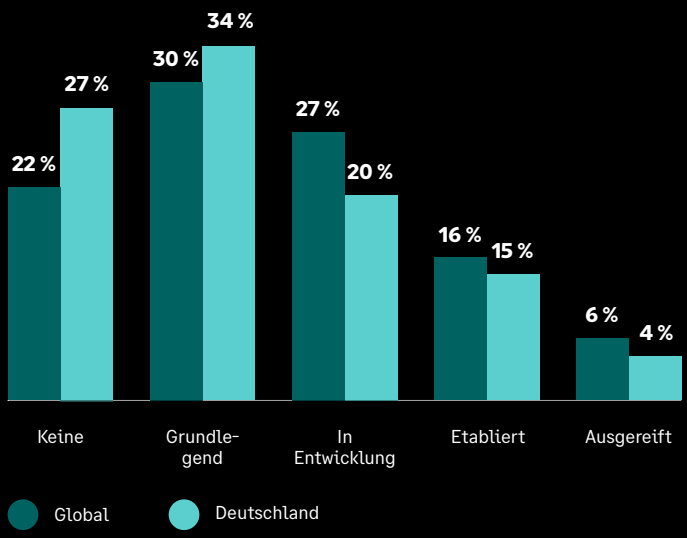
Deutschland zeichnet sich im Vergleich mit dem weltweiten Durchschnitt durch ein vorsichtigeres und stärker auf Compliance ausgerichtetes Profil aus. Zentrale Maßnahmen sind weniger weit verbreitet, das proaktive Management ist schwächer ausgeprägt und der Reifegrad im Bereich der KI-Sicherheit ist nach wie vor niedriger. Viele Unternehmen stehen noch am Anfang. Die Zahl der Vorfälle entspricht in etwa dem weltweiten Durchschnitt, sodass der Druck derzeit weniger spürbar ist. Die Grundlagen für das Management KI-bezogener Risiken sind jedoch noch unterentwickelt.

Deutschlands Priorität besteht darin, den Schritt von der Vorsicht hin zur praktischen Bereitschaft zu vollziehen. Starke Bedenken hinsichtlich der Datennutzung und begrenzte Transparenz bei KI-Tools weisen auf einen Markt hin, der sich auf Kontrolle und Compliance konzentriert. Der nächste Schritt besteht darin, praktische Sicherheitsvorkehrungen zu stärken, die Transparenz bei der KI-Nutzung zu verbessern und sicherzustellen, dass sich Vorsicht in eine stärkere Resilienz umsetzt, während die KI-Einführung zunimmt.

Modell zur Verwaltung der Cybersicherheit



Aktuelles Sicherheitsniveau für KI-gestützte Anwendungen



Cybervorfälle oder Sicherheitsverletzungen im vergangenen Jahr

Deutschland	**54 %** Keine Vorfälle	**36 %** Geringfügige Zwischenfälle, die schnell gelöst werden	**10 %** Vorfälle, die zu erheblichen Beeinträchtigungen führen
Global	**54 %** Keine Vorfälle	**34 %** Geringfügige Zwischenfälle, die schnell gelöst werden	**11 %** Vorfälle, die zu erheblichen Beeinträchtigungen führen

Die wichtigsten vorhandenen Sicherheitsmaßnahmen

Deutschland	**77 %** E-Mail-Schutz	**68 %** Wartung (Installation von Updates und Backups)	**61 %** MFA/SSO
Global	**79 %** E-Mail-Schutz	**71 %** Wartung (Installation von Updates und Backups)	**67 %** Endpunkt-Schutz-maßnahmen

Zentrale Herausforderungen bei KI-Anwendungen im Sicherheitsbereich

Deutschland	**43 %** Unzureichende KI-Sicherheitsex-pertise	**39 %** Starke Datensicher-heit gewährleisten	**37 %** Begrenzte Trans-parenz hinsichtlich der eingesetzten KI-Tools
Global	**45 %** Unzureichende KI-Sicherheitsex-pertise	**41 %** Starke Datensicher-heit gewährleisten	**36 %** Mit neuen KI-Bedrohungen Schritt halten

Die wichtigsten Schutzmaßnahmen gegen Risiken und Gefahren durch KI

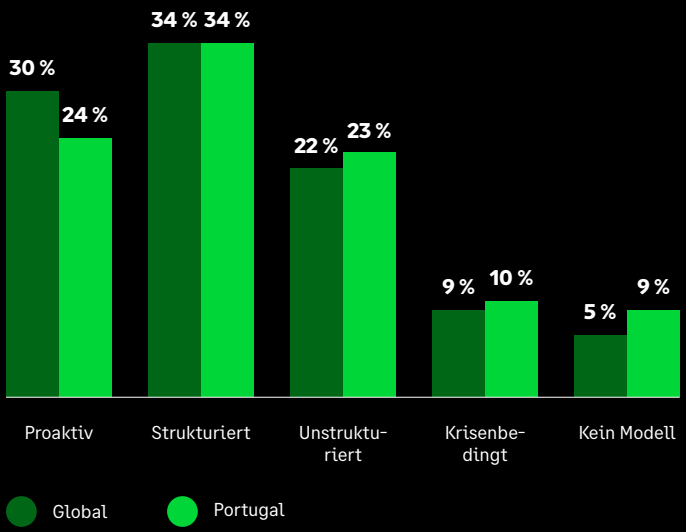
Deutschland	**42 %** Klare Richtlinien zum Einsatz von KI	**32 %** Zugelassene KI-Tools mit Administrator-funktionen	**26 %** Kontrollen zum Schutz sensibler Daten
Global	**41 %** Klare Richtlinien zum Einsatz von KI	**38 %** Zugelassene KI-Tools mit Administrator-funktionen	**33 %** KI-Tools vor der Einführung testen

Portugal

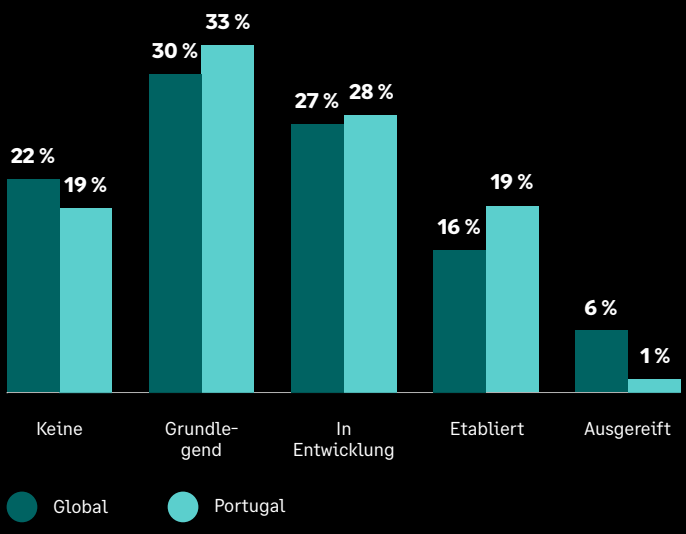
Portugal weist im Vergleich mit dem weltweiten Durchschnitt ein weniger ausgereiftes Sicherheitsprofil auf. Zentrale Sicherheitsmaßnahmen sind weniger weit verbreitet, die Zahl der Vorfälle ist höher und es kommt häufiger zu erheblichen Beeinträchtigungen. Auch der Reifegrad im Bereich der KI-Sicherheit ist nach wie vor uneinheitlich: Viele Unternehmen haben Grundlagen aufgebaut, doch nur sehr wenige haben eine ausgereifte Umsetzung erreicht.

Die Herausforderung für Portugal liegt in der Umsetzung. Nun gilt es, die Grundlagen zu stärken, Unsicherheiten im Umgang mit KI-bezogenen Daten abzubauen und eine konsistentere alltägliche Sicherheitspraxis zu etablieren, um Risiken mit geringeren Beeinträchtigungen bewältigen zu können. Das stärkere Vertrauen in unabhängige Zertifizierungen zeigt zudem, dass der Markt angesichts der zunehmenden Einführung von KI nach klaren externen Vertrauensnachweisen sucht.

Modell zur Verwaltung der Cybersicherheit



Aktuelles Sicherheitsniveau für KI-gestützte Anwendungen



Cybervorfälle oder Sicherheitsverletzungen im vergangenen Jahr

Portugal	**43 %** Keine Vorfälle	**39 %** Geringfügige Zwischenfälle, die schnell gelöst werden	**16 %** Vorfälle, die zu erheblichen Beeinträchtigungen führen
Global	**54 %** Keine Vorfälle	**34 %** Geringfügige Zwischenfälle, die schnell gelöst werden	**11 %** Vorfälle, die zu erheblichen Beeinträchtigungen führen

Die wichtigsten vorhandenen Sicherheitsmaßnahmen

Portugal	**65 %** E-Mail-Schutz	**65 %** Wartung (Installation von Updates und Backups)	**61 %** Endpunkt-Schutz-maßnahmen
Global	**79 %** E-Mail-Schutz	**71 %** Wartung (Installation von Updates und Backups)	**67 %** Endpunkt-Schutz-maßnahmen

Zentrale Herausforderungen bei KI-Anwendungen im Sicherheitsbereich

Portugal	**44 %** Unzureichende KI-Sicherheitsex-pertise	**40 %** Starke Datensicher-heit gewährleisten	**34 %** Begrenzte Trans-parenz hinsichtlich der eingesetzten KI-Tools
Global	**45 %** Unzureichende KI-Sicherheitsex-pertise	**41 %** Starke Datensicher-heit gewährleisten	**36 %** Mit neuen KI-Bedrohungen Schritt halten

Die wichtigsten Schutzmaßnahmen gegen Risiken und Gefahren durch KI

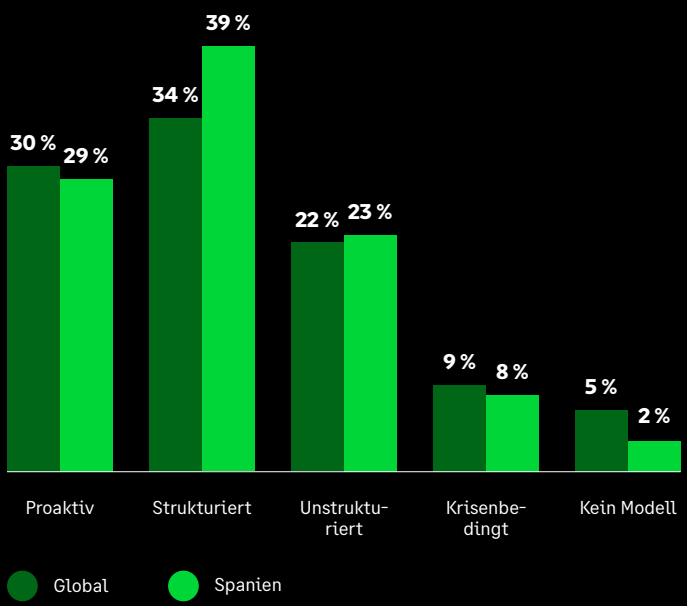
Portugal	**43 %** Klare Richtlinien zum Einsatz von KI	**34 %** Zugelassene KI-Tools mit Administrator-funktionen	**33 %** KI-Tools vor der Einführung testen
Global	**41 %** Klare Richtlinien zum Einsatz von KI	**38 %** Zugelassene KI-Tools mit Administrator-funktionen	**33 %** KI-Tools vor der Einführung testen

Spanien

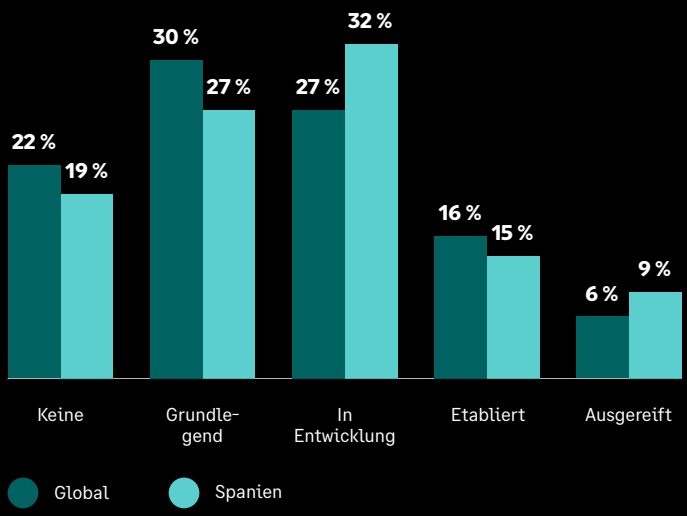
Spanien weist gegenüber dem weltweiten Durchschnitt ein ausgereifteres Sicherheitsprofil auf. Die Zahl der Vorfälle ist geringer, strukturiertes Sicherheitsmanagement ist weiter verbreitet und der Reifegrad im Bereich der KI-Sicherheit ist höher. Immer mehr Unternehmen lassen die Anfangsphase hinter sich und erreichen eine ausgereifte Einführungsphase.

Die Herausforderung für Spanien besteht darin, diese Position angesichts der zunehmenden KI-Einführung zu behaupten. Vorrangig ist nun, den Schutz vor Risiken durch menschliches Versagen zu stärken, die Transparenz bei der KI-Nutzung zu verbessern und Lücken in der laufenden Überwachung durch Dritte zu schließen. Nur so kann eine starke Ausgangsposition bewahrt werden, während sich die Bedrohungen weiterentwickeln.

Modell zur Verwaltung der Cybersicherheit



Aktuelles Sicherheitsniveau für KI-gestützte Anwendungen



Cybervorfälle oder Sicherheitsverletzungen im vergangenen Jahr

Spanien	**60 %** Keine Vorfälle	**29 %** Geringfügige Zwischenfälle, die schnell gelöst werden	**10 %** Vorfälle, die zu erheblichen Beeinträchtigungen führen
Global	**54 %** Keine Vorfälle	**34 %** Geringfügige Zwischenfälle, die schnell gelöst werden	**11 %** Vorfälle, die zu erheblichen Beeinträchtigungen führen

Die wichtigsten vorhandenen Sicherheitsmaßnahmen

Spanien	**75 %** E-Mail-Schutz	**72 %** Wartung (Installation von Updates und Backups)	**62 %** Endpunkt-Schutz-maßnahmen
Global	**79 %** E-Mail-Schutz	**71 %** Wartung (Installation von Updates und Backups)	**67 %** Endpunkt-Schutz-maßnahmen

Zentrale Herausforderungen bei KI-Anwendungen im Sicherheitsbereich

Spanien	**42 %** Unzureichende KI-Sicherheitsex-pertise	**36 %** Starke Datensicher-heit gewährleisten	**34 %** Begrenzte Trans-parenz hinsichtlich der eingesetzten KI-Tools
Global	**45 %** Unzureichende KI-Sicherheitsex-pertise	**41 %** Starke Datensicher-heit gewährleisten	**36 %** Mit neuen KI-Bedrohungen Schritt halten

Die wichtigsten Schutzmaßnahmen gegen Risiken und Gefahren durch KI

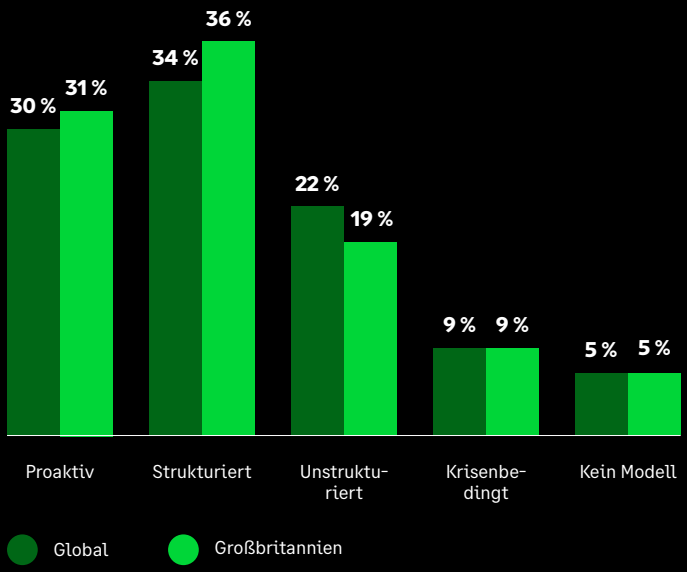
Spanien	**43 %** Klare Richtlinien zum Einsatz von KI	**38 %** Zugelassene KI-Tools mit Administrator-funktionen	**32 %** KI-Tools vor der Einführung testen
Global	**41 %** Klare Richtlinien zum Einsatz von KI	**38 %** Zugelassene KI-Tools mit Administrator-funktionen	**33 %** KI-Tools vor der Einführung testen

Vereinigtes Königreich

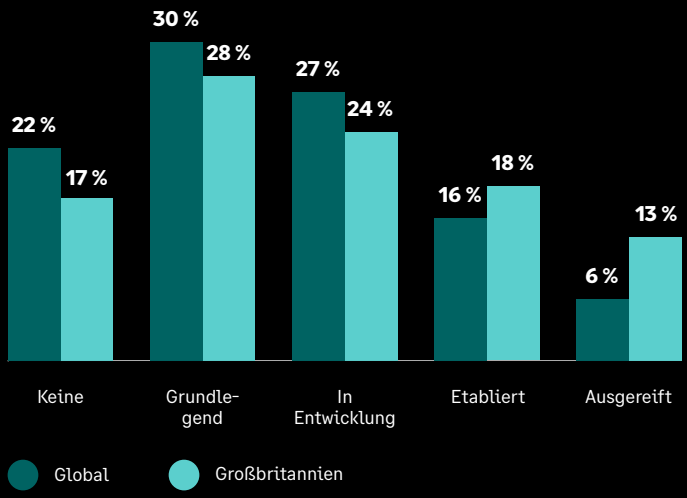
Das Vereinigte Königreich zeichnet sich dadurch aus, dass es im Bereich der KI-Sicherheit schneller und weiter voranschreitet als der weltweite Durchschnitt. Unternehmen sind bei der Umsetzung praktischer Sicherheitsvorkehrungen weiter fortgeschritten, setzen eher auf geprüfte Tools und formelle Richtlinien und haben bereits eine ausgereiftere KI-Sicherheitsstrategie entwickelt. Dies deutet auf einen Markt hin, der nicht abwartet, sondern einen bewussteren Ansatz verfolgt, um sich angesichts der zunehmenden Verbreitung von KI-Risiken vorzubereiten.

Der Fokus liegt nun auf einer strengeren Kontrolle angesichts der zunehmenden KI-Nutzung, insbesondere in Bezug auf Datenschutz, sich rasch entwickelnde Bedrohungsszenarien und die Fähigkeit, eine starke KI-Sicherheitsstrategie in die Praxis umzusetzen. Das etwas höhere Ausmaß an erheblichen Beeinträchtigungen zeigt zudem, dass die Vorbereitungen durch konsequentes Handeln bei auftretenden Vorfällen ergänzt werden müssen.

Modell zur Verwaltung der Cybersicherheit



Aktuelles Sicherheitsniveau für KI-gestützte Anwendungen



Cybervorfälle oder Sicherheitsverletzungen im vergangenen Jahr

Großbritannien	**55 %** Keine Vorfälle	**32 %** Geringfügige Zwischenfälle, die schnell gelöst werden	**13 %** Vorfälle, die zu erheblichen Beeinträchtigungen führen
Global	**54 %** Keine Vorfälle	**34 %** Geringfügige Zwischenfälle, die schnell gelöst werden	**11 %** Vorfälle, die zu erheblichen Beeinträchtigungen führen

Die wichtigsten vorhandenen Sicherheitsmaßnahmen

Großbritannien	**75 %** E-Mail-Schutz	**79 %** Wartung (Installation von Updates und Backups)	**67 %** Endpunkt-Schutzmaßnahmen
Global	**79 %** E-Mail-Schutz	**71 %** Wartung (Installation von Updates und Backups)	**67 %** Endpunkt-Schutzmaßnahmen

Zentrale Herausforderungen bei KI-Anwendungen im Sicherheitsbereich

Großbritannien	**44 %** Unzureichende KI-Sicherheitsex-pertise	**46 %** Starke Datensicher-heit gewährleisten	**37 %** Mit neuen KI-Bedrohungen Schritt halten
Global	**45 %** Unzureichende KI-Sicherheitsex-pertise	**41 %** Starke Datensicher-heit gewährleisten	**36 %** Mit neuen KI-Bedrohungen Schritt halten

Die wichtigsten Schutzmaßnahmen gegen Risiken und Gefahren durch KI

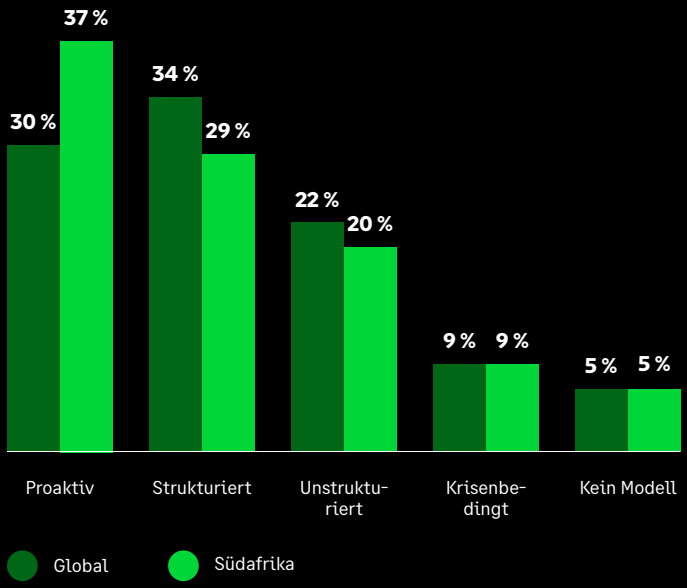
Großbritannien	**43 %** Klare Richtlinien zum Einsatz von KI	**45 %** Zugelassene KI-Tools mit Administrator-funktionen	**38 %** KI-Tools vor der Einführung testen
Global	**41 %** Klare Richtlinien zum Einsatz von KI	**38 %** Zugelassene KI-Tools mit Administrator-funktionen	**33 %** KI-Tools vor der Einführung testen

Südafrika

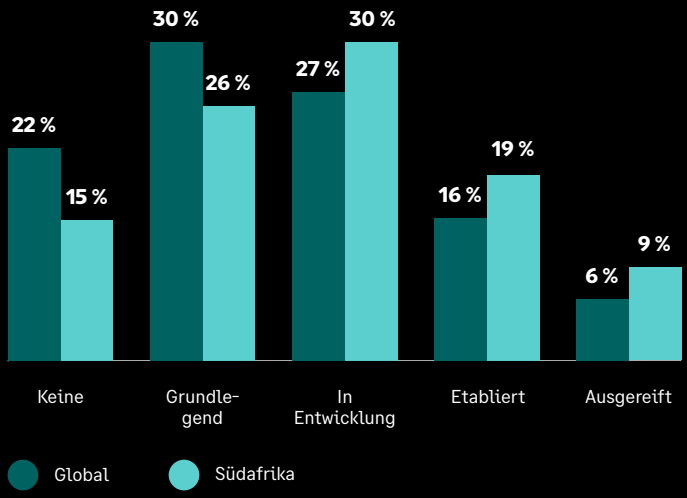
Hinsichtlich des Reifegrads im Bereich KI-Sicherheit liegt Südafrika über dem globalen Durchschnitt. Unternehmen haben ihren Ansatz als Reaktion auf KI mit größerer Wahrscheinlichkeit bereits überarbeitet, verfügen über eine fortgeschrittenere Sicherheitsstrategie für KI-gestützte Anwendungen und unterliegen einer strengeren Überwachung durch Dritte. Dies deutet auf einen Markt hin, der KI-Risiken ernst nimmt und mit zunehmender Verbreitung der Technologie mehr praktische Sicherheitsvorkehrungen trifft.

Die Herausforderung besteht jedoch darin, diese Fortschritte konsistenter umzusetzen. Die grundlegenden Sicherheitsmaßnahmen sind nach wie vor uneinheitlich und die Bedenken hinsichtlich des Datenschutzes sowie sich schnell entwickelnder Bedrohungsszenarien sind weiterhin groß. Der Fokus liegt nun darauf, diese Lücken zu schließen, um mit alltäglichen Sicherheitspraktiken eine widerstandsfähigere KI-Sicherheitslage zu erreichen.

Modell zur Verwaltung der Cybersicherheit



Aktuelles Sicherheitsniveau für KI-gestützte Anwendungen



Cybervorfälle oder Sicherheitsverletzungen im vergangenen Jahr

Südafrika	55 % Keine Vorfälle	35 % Geringfügige Zwischenfälle, die schnell gelöst werden	9 % Vorfälle, die zu erheblichen Beeinträchtigungen führen
Global	54 % Keine Vorfälle	34 % Geringfügige Zwischenfälle, die schnell gelöst werden	11 % Vorfälle, die zu erheblichen Beeinträchtigungen führen

Die wichtigsten vorhandenen Sicherheitsmaßnahmen

Südafrika	75 % E-Mail-Schutz	74 % Wartung (Installation von Updates und Backups)	70 % Endpunkt-Schutz-maßnahmen
Global	79 % E-Mail-Schutz	71 % Wartung (Installation von Updates und Backups)	67 % Endpunkt-Schutz-maßnahmen

Zentrale Herausforderungen bei KI-Anwendungen im Sicherheitsbereich

Südafrika	45 % Unzureichende KI-Sicherheitsex-pertise	44 % Starke Datensicher-heit gewährleisten	37 % Mit neuen KI-Bedrohungen Schritt halten
Global	45 % Unzureichende KI-Sicherheitsex-pertise	41 % Starke Datensicher-heit gewährleisten	36 % Mit neuen KI-Bedrohungen Schritt halten

Die wichtigsten Schutzmaßnahmen gegen Risiken und Gefahren durch KI

Südafrika	45 % Klare Richtlinien zum Einsatz von KI	39 % Zugelassene KI-Tools mit Administrator-funktionen	36 % Kontrollen zum Schutz sensibler Daten
Global	41 % Klare Richtlinien zum Einsatz von KI	38 % Zugelassene KI-Tools mit Administrator-funktionen	33 % KI-Tools vor der Einführung testen

sage.com