RSA

RSA.com

RSA ID IQ-Report 2026

Der RSA Identity Security Pulse Check

Inhaltsverzeichnis.

Zusammenfassung.

Im RSA ID IQ Report 2026 wurden über 2.000 Experten weltweit gebeten, detailliert anzugeben, wie oft die Identitätssicherheit sie im Stich gelassen hat, wie viel sie in diesem Fall verloren haben und welche Schwachstellen sie am meisten fürchten.
Ihre Aussagen waren alarmierend: Die Identitätspolitik von Unternehmen **versagte in mehr Unternehmen als im Vorjahr**, was zu noch größerem finanziellen Schaden führte. Wenn die Verantwortlichen nicht handeln, werden die Risiken für ihre Unternehmen noch größer – und die Folgen dieser Risiken werden noch kostenintensiver.
Die Daten zeigen **eine wachsende Lücke in der Identitätssicherheit**. Die meisten Organisationen nutzen immer noch **veraltete Lösungen**, die den neuen Herausforderungen nicht gerecht werden.

Die meisten Benutzer verlassen sich zur Authentifizierung immer noch auf Passwörter. Ihre Organisationen berichten von häufigeren Sicherheitsverletzungen und höheren Verlusten. Gleichzeitig werden sie bei der Umstellung auf passwortloses Arbeiten durch komplexe Betriebsumgebungen und anspruchsvolle Anwendungsfälle behindert.
Unternehmen verfügen nicht über die notwendigen Fähigkeiten, um sich gegen Social Engineering zu schützen und Angriffe auf ihre IT-Helpdesks zu umgehen, obwohl diese Taktik zu einem immer größeren Risiko wird. Und obwohl Unternehmen die Identität von Menschen, Maschinen und Diensten überwachen, zeigt die Häufigkeit von Datenschutzverletzungen deutlich, dass sie diese Informationen nicht nutzen, um Risiken proaktiv oder effektiv zu reduzieren.

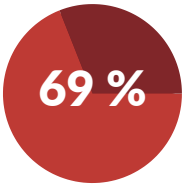
Vielleicht liegt es an diesen wachsenden Risiken, dass Experten berichten, dass sie sich voll und ganz auf KI für die Cybersicherheit konzentrieren.
Branchenübergreifend glauben immer mehr Nutzer, dass **KI eher zur Cybersicherheit beiträgt als Cyberkriminalität zu ermöglichen**. Mehr Unternehmen als je zuvor planen, KI in ihre Cybersicherheits-Infrastruktur zu integrieren. Die meisten Unternehmen geben zudem an, dass agentenbasierte KI für die Cybersicherheit die wichtigste Funktion sein wird.

Ich lasse die Ergebnisse für sich sprechen. Obwohl diese Informationen an sich schon nützlich sind, ist es wichtig, dass Führungskräfte entsprechend handeln, indem sie **der passwortlosen Authentifizierung Priorität einräume**n, moderne Methoden zum Schutz vor Helpdesk-Betrug implementieren, Identitätsrisiken proaktiv erkennen und beheben, bevor sie zu Sicherheitsverletzungen werden, und KI als Kraftmultiplikator nutzen, um schnellere Entscheidungen zu automatisieren.
Der erste Schritt zur Lösung eines Problems besteht darin, sich einzugestehen, dass es eines gibt. Der RSA ID IQ Report 2026 macht deutlich, dass es bei den meisten Organisationen große Bedenken hinsichtlich der Identitätssicherheit gibt.
Die **Identitätssicherheit versagt in zu vielen Unternehmen** einfach zu oft. Die Wahrscheinlichkeit eines Verstoßes – und die Kosten der Untätigkeit – sind schlicht zu hoch, um den Status quo aufrechtzuerhalten.

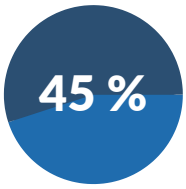
Greg Nelson, CEO, RSA

Die wichtigsten Ergebnisse des RSA ID IQ Reports 2026

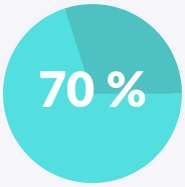
Der RSA ID IQ Report 2026 enthält Informationen von 2.120 Experten aus den Bereichen Cybersicherheit, Identitäts- und Zugriffsmanagement (IAM), IT und anderen Bereichen. Zu den wichtigsten Ergebnissen gehören:



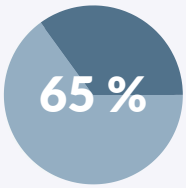
der Organisationen meldeten in den letzten drei Jahren einen identitätsbezogenen Verstoß, ein Anstieg um 27 Prozentpunkte gegenüber 2025



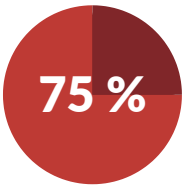
der Organisationen gaben an, dass identitätsbezogene Datenschutzverletzungen sie mehr kosten als die durchschnittliche Datenschutzverletzung



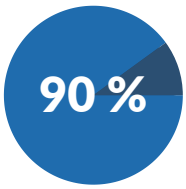
der Organisationen gaben an, dass ihnen Identitätsverletzungen erheblichen Schaden zugefügt haben



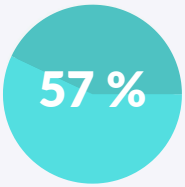
der Unternehmen gaben an, dass sie ernsthaft besorgt seien, dass ihr IT-Helpdesk oder Servicedesk einen Social-Engineering-Angriff nicht stoppen könne.



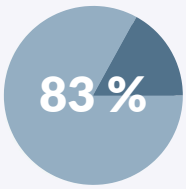
der Organisationen arbeiten in hybriden Umgebungen, ein Anstieg um 5 Prozentpunkte ab 2025



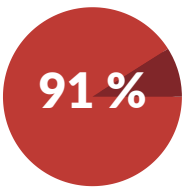
der Organisationen berichteten von Herausforderungen bei der Umstellung auf eine passwortlose Authentifizierung



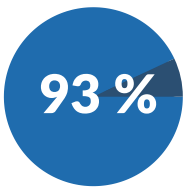
der Organisationen verwenden weiterhin Passwörter als primäre Authentifizierungsmethode



der Organisationen glauben, dass KI mehr zur Cybersicherheit beitragen wird als zur Bekämpfung von Cyberkriminalität. Dies entspricht einem Anstieg von 3 Prozent seit 2025.



der Organisationen planen, im nächsten Jahr irgendeine Form von KI in ihren Tech-Stack zu implementieren, ein Anstieg um 12 Prozentpunkte seit 2025



der Organisationen haben noch nicht die optimale Zero-Trust-Reife erreicht

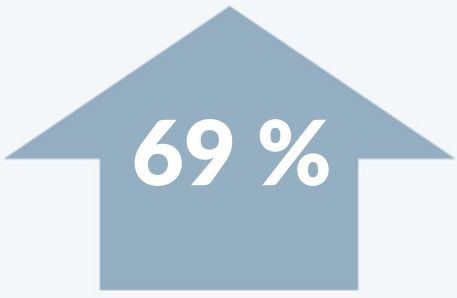
Mehr Identitätsdiebstahl verursachte in diesem Jahr noch mehr Schaden

Die Analyse der Umfrageantworten ergab, dass Organisationen in diesem Jahr mehr Verstöße aufgrund von Identitätssicherheitsmängeln erlitten: 69 % der Organisationen meldeten in den letzten drei Jahren einen Verstoß, ein Anstieg um 27 Prozentpunkte seit dem RSA ID IQ Report 2025.

Diese Verstöße traten nicht nur häufiger auf, sondern richteten auch größeren Schaden an und hatten höhere Kosten. Mehr als ein Fünftel (21 %) aller Befragten gaben an, dass ein Identitätsdiebstahl sie zwischen 5 und 10 Millionen US-Dollar kostete, während fast ein Viertel (24 %) angab, dass die Kosten eines Identitätsdiebstahls 10 Millionen US-Dollar überstiegen. Die Zahl der Verstöße mit Kosten von mehr als 10 Millionen US-Dollar stieg im Vergleich zum Vorjahresbericht um drei Prozentpunkte.

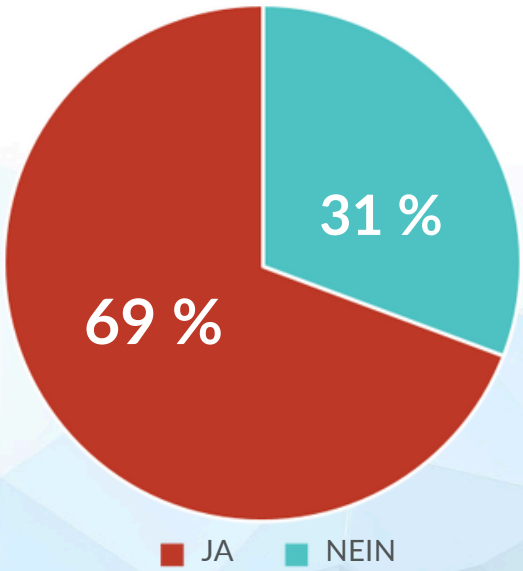
Das sind alarmierende Zahlen. Besonders besorgniserregend sind sie im Vergleich zu den weltweiten Durchschnittskosten für einen Datendiebstahl, der durch einen beliebigen Angriffsvektor verursacht wird:

Der IBM Cost of Data Breach Report 2025 ergab, dass ein durchschnittlicher Verstoß Kosten in Höhe von 4,44 Millionen US-Dollar verursacht. Identitätsfehler verursachen Unternehmen erhebliche Kosten. Kein Wunder also, dass 70 % aller Befragten die Schwere eines Verstoßes mit vier oder fünf auf einer fünfstufigen Skala bewerteten.



der Organisationen berichteten von ein Identitätsverstoß in den letzten 3 Jahren, ein Anstieg um 27 Prozentpunkte

Hat Ihre Organisation in den letzten drei Jahren eine Verletzung der Identitätsdaten erlebt?

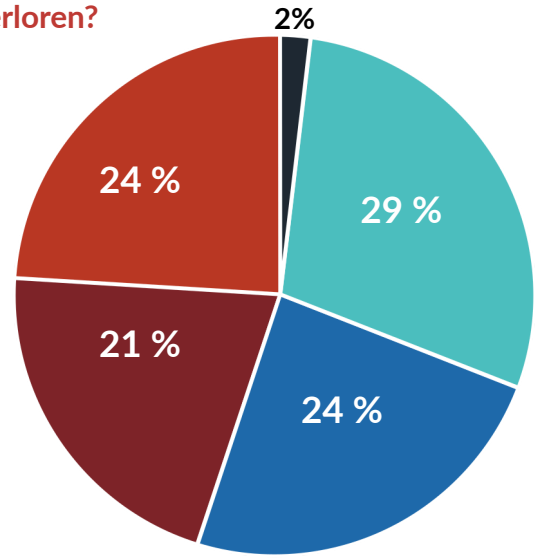


24 %

der Unternehmen, die einen Identitätsdiebstahl erlebten, gaben an, dass die Kosten des Verstoßes

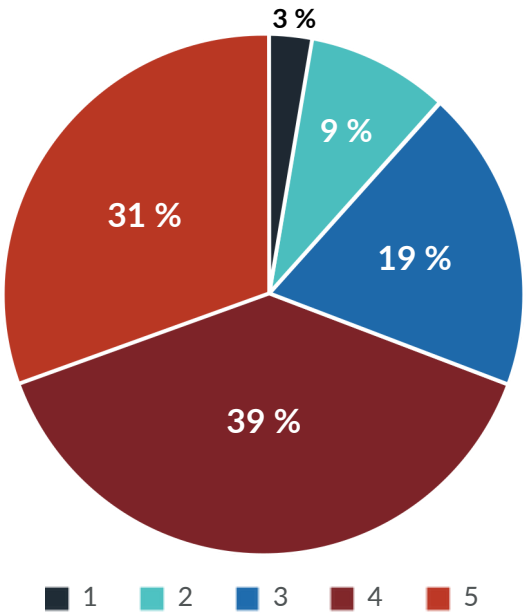
über 10 Mio. USD, ein Anstieg um 3 Prozentpunkte, gegenüber 2025 ergaben

Wie viel Geld hat Ihr Unternehmen Ihrer Meinung nach in den letzten drei Jahren **aufgrund von Datenverstößen im Zusammenhang mit Identitätsdaten verloren?**



Ich weiß nicht | Weniger als 1 Mio. USD | Zwischen 1 und 5 Millionen US-Dollar | Zwischen 5 und 10 Millionen US-Dollar | Über 10 Millionen US-Dollar

Wenn Sie in den letzten drei Jahren einen Identitätsverstoß erlebt haben, bewerten Sie die Schwere der Auswirkungen auf Ihre Organisation von 1 bis 5.



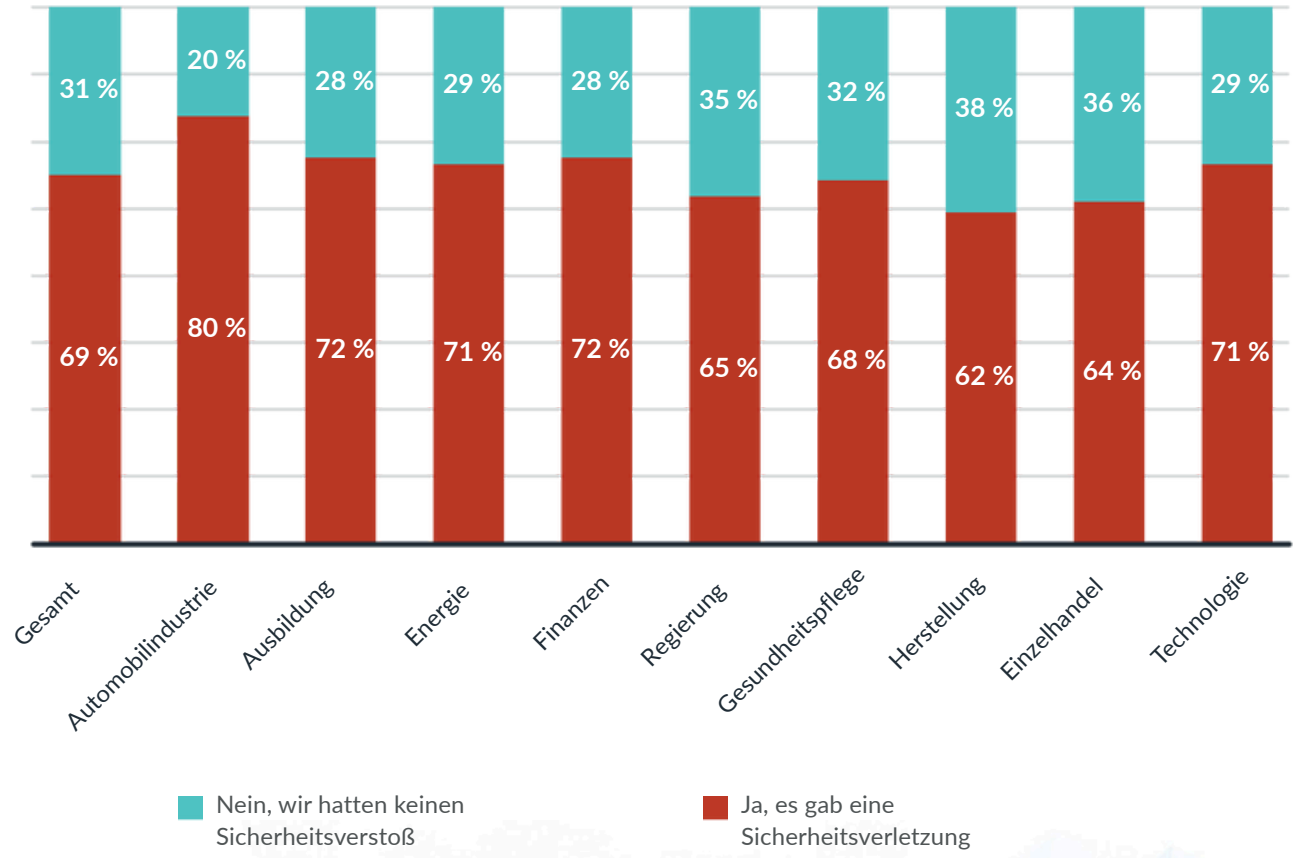
4,44 $ Millionen

Globaler Durchschnitt der Kosten aller Datenschutzverletzungen gemäß dem IBM Cost of a Data Breach Report 2025

Sicherheitsverletzungen nach Sektor

Bei der Betrachtung der Datenleckraten nach Branchen zeigt sich, dass die Automobilindustrie (80 %), der Finanzsektor (72 %), die Energie- und Versorgungswirtschaft (71 %) sowie die Technologiebranche (71 %) die höchste Datenleckrate aufweisen. Einzelhandel (64 %) und Fertigung (62 %) sind die am wenigsten betroffenen Branchen.

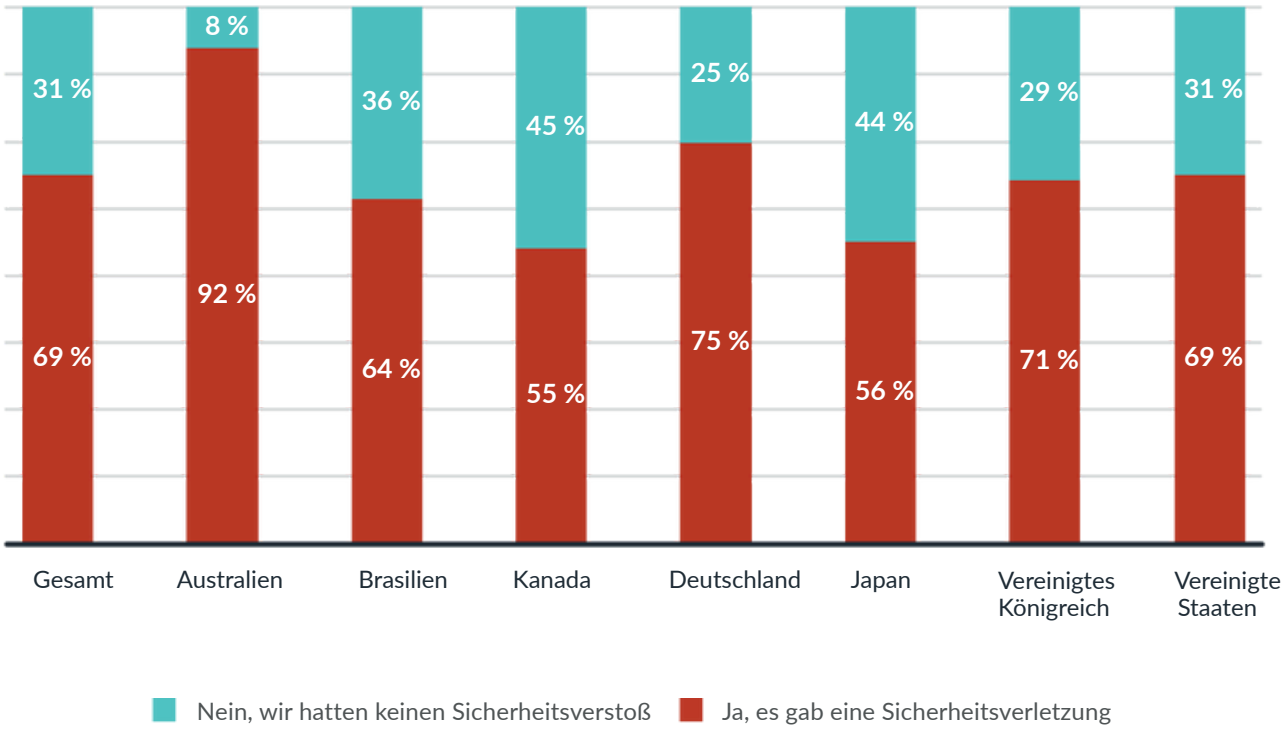
Nach Sektor: Gab es in Ihrer Organisation in den letzten drei Jahren einen Identitätsverstoß?



Sicherheitsverletzungen nach Land

Nach Ländern betrachtet meldeten Australien (92 %), Deutschland (75 %), Großbritannien (71 %) und die USA (69 %) in den letzten drei Jahren die meisten identitätsbezogenen Verstöße, während Japan (56 %) und Kanada (55 %) die wenigsten Fälle meldeten. Wir erläutern später im Bericht, wie bestimmte Praktiken mit der Häufigkeit und den Auswirkungen dieser Verstöße korrelieren.

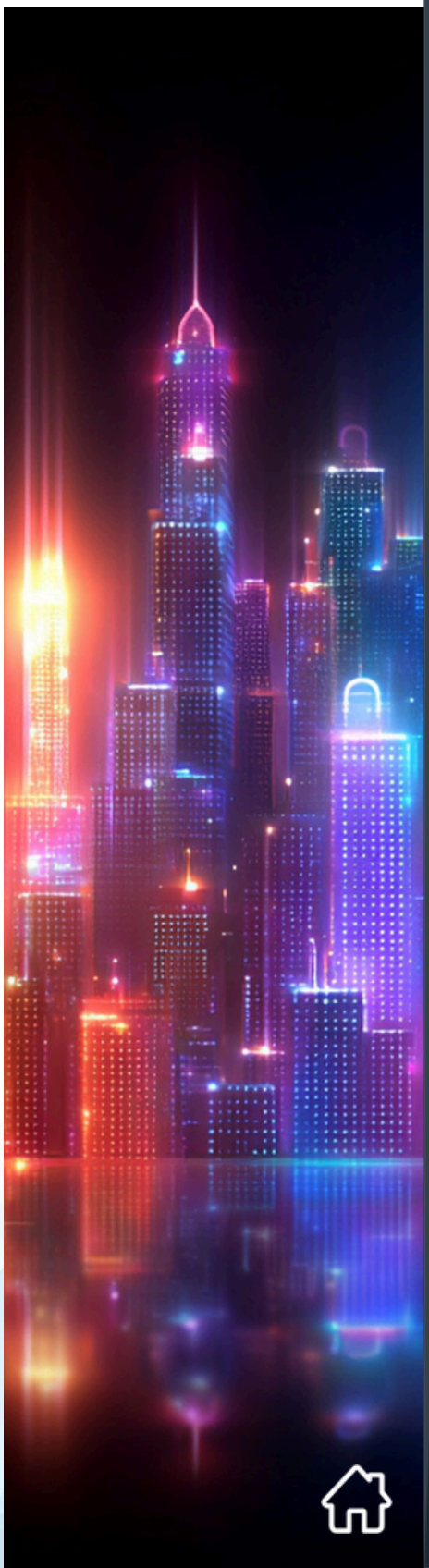
Nach Land: Gab es in Ihrer Organisation in den letzten drei Jahren einen Identitätsverstoß?



Zero Trust „Fortschritt“

Während nur 7 % der Unternehmen angeben, dass sie die optimale Zero-Trust-Reife für Identitäten gemäß der CISA-Definition erreicht haben, glaubt die Mehrheit – 57 % –, dass sie die „fortgeschrittene“ Zero-Trust-Stufe erreicht haben, die Folgendes umfasst:

- Phishing-resistente MFA
- Konsolidierung und sichere Integration von Identitätsspeichern
- Automatisierte Identitätsrisikobewertungen
- Bedarfs-/sitzungsbasierter Zugriff



Dieses Vertrauen wird durch die Tatsache widerlegt, **dass 69 % der Organisationen gehackt wurden und 70 % angaben, dass diese Hackerangriffe schwerwiegend waren.**

Dies soll Unternehmen nicht davon abhalten, ihre Zero-Trust-Strategie zu verfeinern – ganz im Gegenteil. Vielmehr sollte die Kluft zwischen dem von Unternehmen angenommenen Stand auf ihrem Zero-Trust-Weg und der Häufigkeit von Sicherheitsverletzungen eine Warnung für Sicherheitsverantwortliche sein, mehr für ihren Schutz zu tun.

Die Cybersicherheitsrisiken, die Experten schlaflose Nächte bereiten

Die Befragten nannten Phishing als den Bedrohungsvektor, der das größte Cybersicherheitsrisiko für ihr Unternehmen darstellt. Und es gibt gute Gründe, Phishing Priorität einzuräumen: Phishing (das zum Diebstahl von Anmeldeinformationen führt) und die Verwendung gestohlener Anmeldeinformationen gehören Jahr für Jahr zu den häufigsten und schwerwiegendsten Angriffen. Eine der besten Möglichkeiten, Phishing zu vermeiden, besteht darin, die Anmeldeinformationen zu entfernen, die Phisher zu stehlen versuchen: Anstatt gemeinsame Geheimnisse zu verwenden, sollten Unternehmen eine phishing-resistente, passwortlose Authentifizierung implementieren.

192 Tage

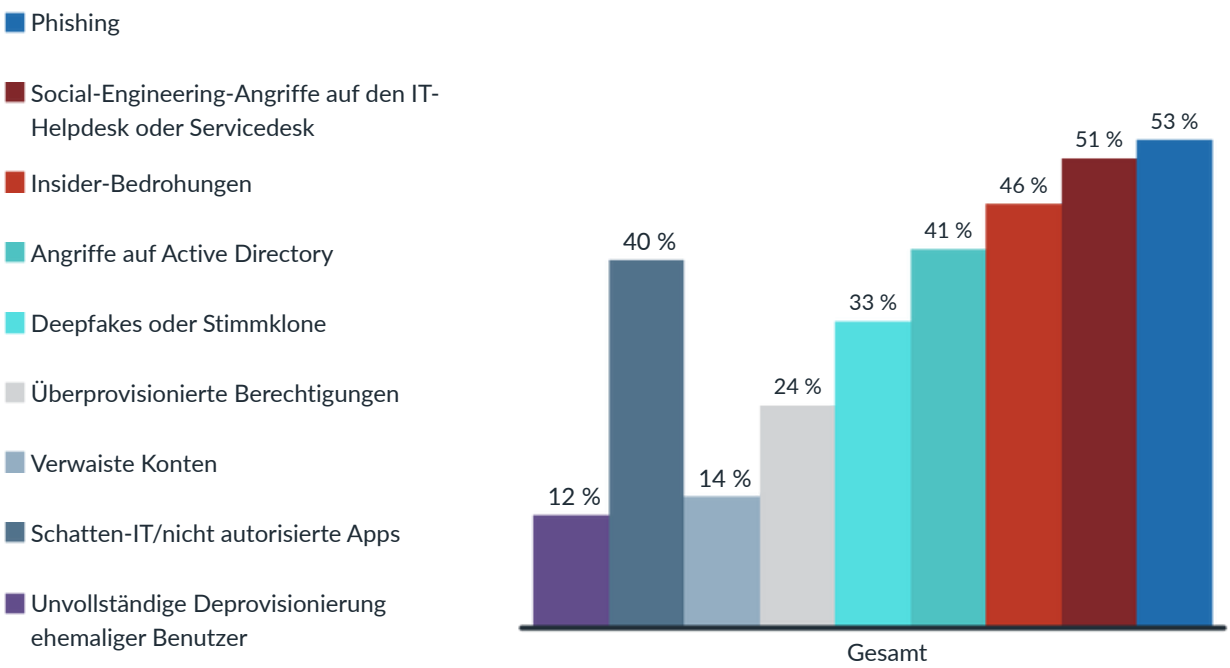
Durchschnittliche Zeit, die Organisationen benötigen um einen durch Phishing verursachten Verstoß zu identifizieren und einzudämmen

4,8 $ Million USD

Durchschnittliche Kosten von Datenverstößen, die durch Phishing verursacht wurden

IBM-Cost of a Databreach Report 2025

Phishing ist zwar ein dauerhaftes Cybersicherheitsrisiko, doch neue Cybersicherheitsrisiken gewinnen schnell an Bedeutung. 51 % der Befragten gaben an, dass Social-Engineering-Angriffe auf den IT-Helpdesk oder Servicedesk das größte Risiko für ihr Unternehmen darstellen.



Ihr Helpdesk braucht Hilfe

Angesichts der schlagzeilenträchtigen Helpdesk-Angriffe auf MGM Resorts, Caesars Entertainment Group, Marks & Spencer, Co-op und House of Dior gibt es gute Gründe, diesem Risiko Priorität einzuräumen. Wie Scattered Spider und andere Cyberkriminelle-Gruppen gezeigt haben, besteht ein erhebliches Risiko, wenn Cyberkriminelle versuchen, die Multi-Faktor-Authentifizierung (MFA) zu umgehen, indem sie als legitimer Benutzer einen IT-Helpdesk oder Servicedesk anrufen und den Helpdesk bitten, neue Konten zu erstellen, die MFA zu sperren oder neue Benutzer oder Geräte zu registrieren. Tatsächlich stuften Cybersicherheitsexperten Social-Engineering-Angriffe auf IT-Helpdesks als das größte Risiko für ihr Unternehmen ein.

Dieses Risiko wird noch dadurch verstärkt, dass Unternehmen schlicht keine neueren, Phishing-resistenten Methoden verwenden, um die Identität der Benutzer zu überprüfen.
Die meisten Organisationen nutzen ältere Methoden zur Benutzerauthentifizierung: 58 % der Organisationen verwenden Passwörter, 50 % OTP und 46 % shared secrets. Im Vergleich dazu gaben nur 36 % an, eine bidirektionale Authentifizierung zu verwenden, bei der sich beide Parteien gegenseitig verifizieren können, und nur ein Viertel (25 %) gab an, risikobasierte Lösungen zur Priorisierung von Benutzern und Anwendungsfällen zu verwenden.

Ältere Methoden für Sicherstellung der Identität der Benutzer

58 %
der Organisationen verwenden Passwörter

50 %
verwenden **OTP**

Neuere Methoden für Sicherstellung der Identität der Benutzer

36 %
Verwenden bidirektionale Identitätssicherung

25 %
Verwenden risikobasierte Lösungen

Wer ruft an?

Seit 2023 BlackCat, ALPHV, Scattered Spider und andere Cyberkriminelle Gruppen das IT-Helpdesk-Personal von Unternehmen durch Social Engineering dazu gebracht haben, MFA-Bypass-Angriffe zu starten, sind erhebliche Schäden und Verluste entstanden:

MGM Resorts
$145M

Caesars Entertainment:
$15M

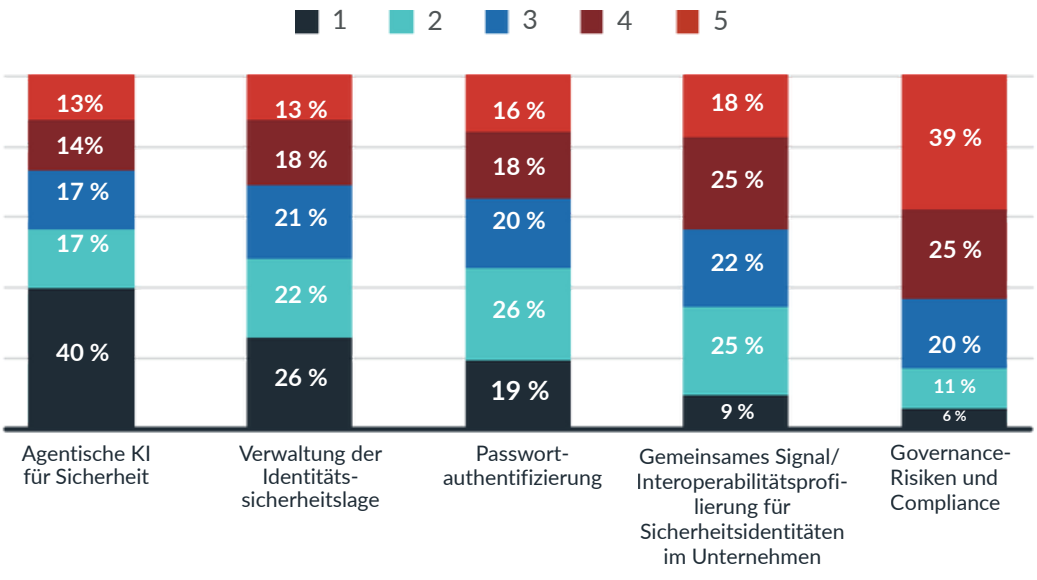
Marks & Spencer:
£300M

Ein Drittel (33 %) der Nutzer gab an, dass neue Techniken wie Deepfakes oder Stimmklone das größte Risiko für ihr Unternehmen darstellen. Diese Taktiken könnten sich ohne moderne Methoden zur Verhinderung von MFA-Bypass-Angriffen als wirksamer erweisen.
Einige der anderen Risiken, die Experten am meisten fürchten, konzentrieren sich auf die Phasen des Identitätslebenszyklus und die schleichende Ausweitung von Berechtigungen. Insider-Bedrohungen (46 %), Schatten-IT und nicht bereitgestellte Anwendungen (40 %) sowie übermäßig bereitgestellte Berechtigungen (24 %) stehen bei den Benutzern als vorrangige Risiken im Vordergrund.
Diese Probleme können durch unzureichende Transparenz hinsichtlich Identitätsrisiken, manuelle Prozesse im Identitätslebenszyklus und rückwirkende Risikominderung noch verschärft werden.

Die Cybersicherheitsfunktionen, die Benutzer priorisieren

Agentische KI für Sicherheit war mit großem Abstand die erste Wahl unter den Nutzern: 40 % der Befragten gaben an, dass dies für sie oberste Priorität habe. Identity Security Posture Management (ISPM) – ein neues Cybersicherheits-Framework, mit dem Unternehmen Risiken verwalten, Richtlinien durchsetzen und die Compliance in immer komplexer werdenden Umgebungen stärken können – wurde als zweitwichtigste Funktion genannt und stand bei 26 % der Befragten an erster Stelle.

Bewerten Sie die folgenden Cybersicherheitsfunktionen auf einer Skala von 1 bis 5.



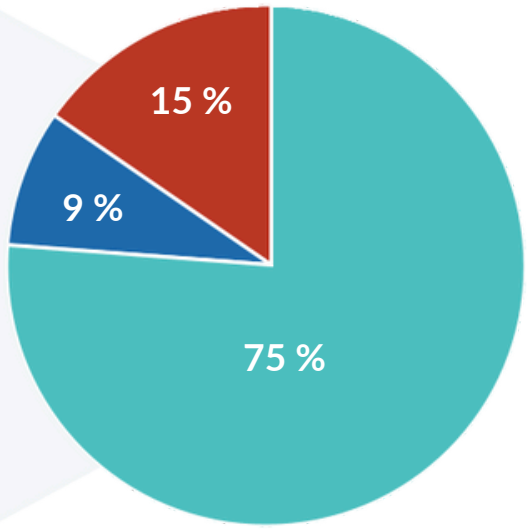
Betriebsumgebungen

Die meisten Unternehmen arbeiten in hybriden Umgebungen und nutzen eine Mischung aus Cloud- und lokalen Ressourcen. Unternehmen müssen sicherstellen, dass alle Benutzer, Geräte, Berechtigungen und Umgebungen ausreichend geschützt sind.

75 %

der Organisationen arbeiten im Hybridmodus - **ein Anstieg um 5 Prozentpunkte**

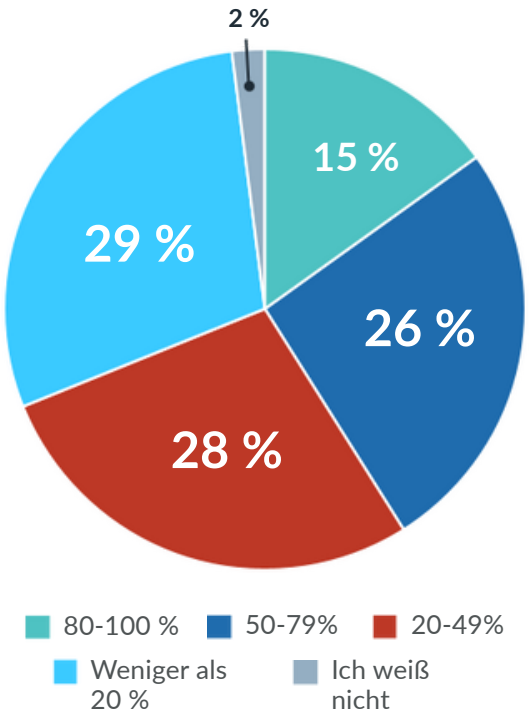
In welchen der folgenden Umgebungen unterstützen Sie Anwendungen und Benutzer?



Hybrid (Cloud und vor Ort) Nur Cloud Nur vor Ort

Passwörter – und Passwortrisiken – bestehen weiterhin

Welcher Prozentsatz Ihrer Benutzer verwendet hauptsächlich passwortlose Formfaktoren zur Authentifizierung?



Die meisten Organisationen verwenden keine passwortlose Authentifizierung als primäre Methode. Das sind gute Neuigkeiten für Cyberkriminelle: Die Verwendung gestohlener Anmeldeinformationen ist Jahr für Jahr die häufigste Ursache für Datenschutzverletzungen. Komplexe Umgebungen und gemischte Anwendungsfälle sowie Benutzergruppen machen es für Unternehmen zu einer Herausforderung, umfassende passwortlose Lösungen bereitzustellen.

Die anhaltende Nutzung passwortbasierter Authentifizierung korreliert mit häufigeren und kostspieligeren Datendiebstählen. Australische Organisationen verzeichneten eine der niedrigsten Raten bei der Einführung passwortloser Authentifizierung im Vergleich zum Vorjahr. 50 % der australischen Organisationen befinden sich noch in der Anfangsphase. Australische Unternehmen leiden außerdem unter der höchsten Rate an identitätsbezogenen Datenverstößen pro Land (92 % der Unternehmen meldeten einen Verstoß in den letzten drei Jahren), den schwerwiegendsten Folgen (47 % gaben an, dass der Verstoß großen Schaden verursacht habe) und den höchsten finanziellen Verlusten (44 % gaben an, dass ein Verstoß sie mehr als 10 Millionen Dollar gekostet habe).

Im Gegensatz dazu wurde in Japan die höchste Anzahl an Fällen gemeldet, in denen passwortlose Authentifizierung als primäre Methode verwendet wurde (37 % der Unternehmen gaben an, diese Methode in mindestens 80 % der Fälle zu verwenden). Japan verzeichnet auch eine der niedrigsten Raten an identitätsbezogenen Datenschutzverletzungen (56 % der Unternehmen) und weniger schwerwiegende Folgen.

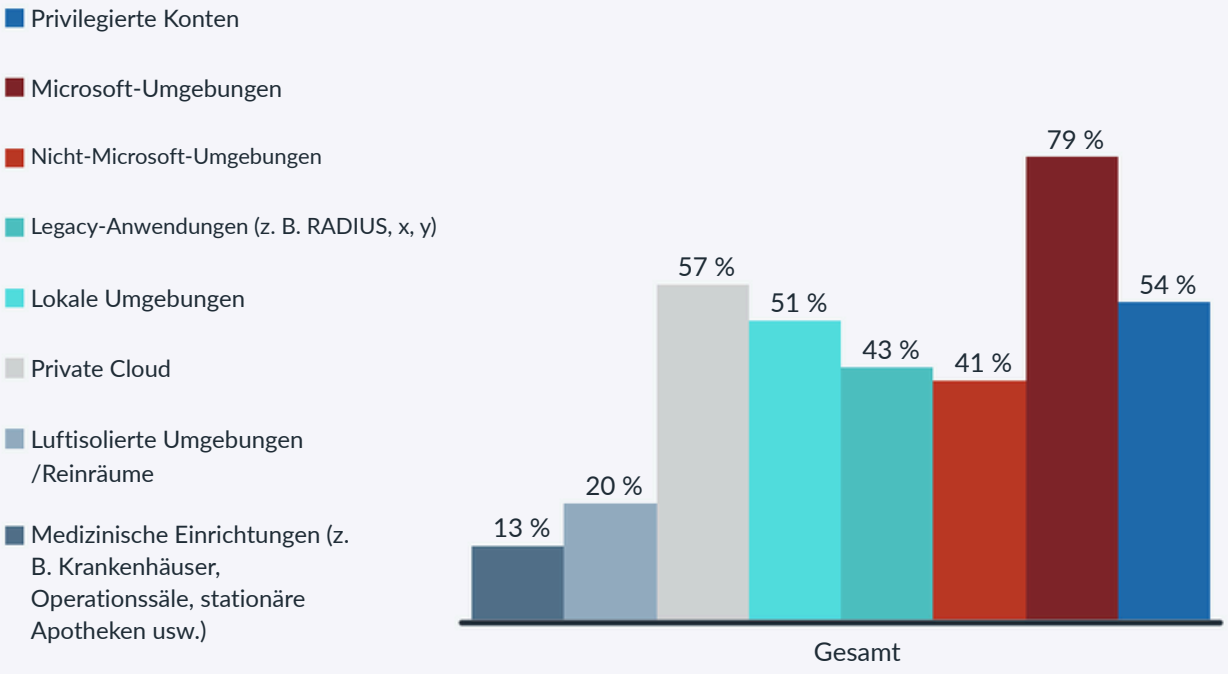
	Australische Organisationen	Japanische Organisationen
Rangfolge der gesamten passwortlosen Nutzung nach Land.	#5	#1
Prozentsatz der Benutzer, die passwortlos als primäre Authentifizierungsform verwenden.	10 %	37 %
Hat einen Verstoß gemeldet.	92 %	56 %
Prozentsatz derjenigen, die den Verstoß als schwerwiegenden Schaden gemeldet haben (5 von 5).	47 %	44 %
Prozentsatz der Verstöße, die mehr als 10 Millionen US-Dollar kosten.	24 %	28 %

> **Komplexe Umgebungen und gemischte Anwendungsfälle sowie Benutzergruppen machen es für Unternehmen zu einer Herausforderung, umfassende passwortlose Lösungen bereitzustellen.“**

Was verlangsamt den passwortlosen Betrieb?

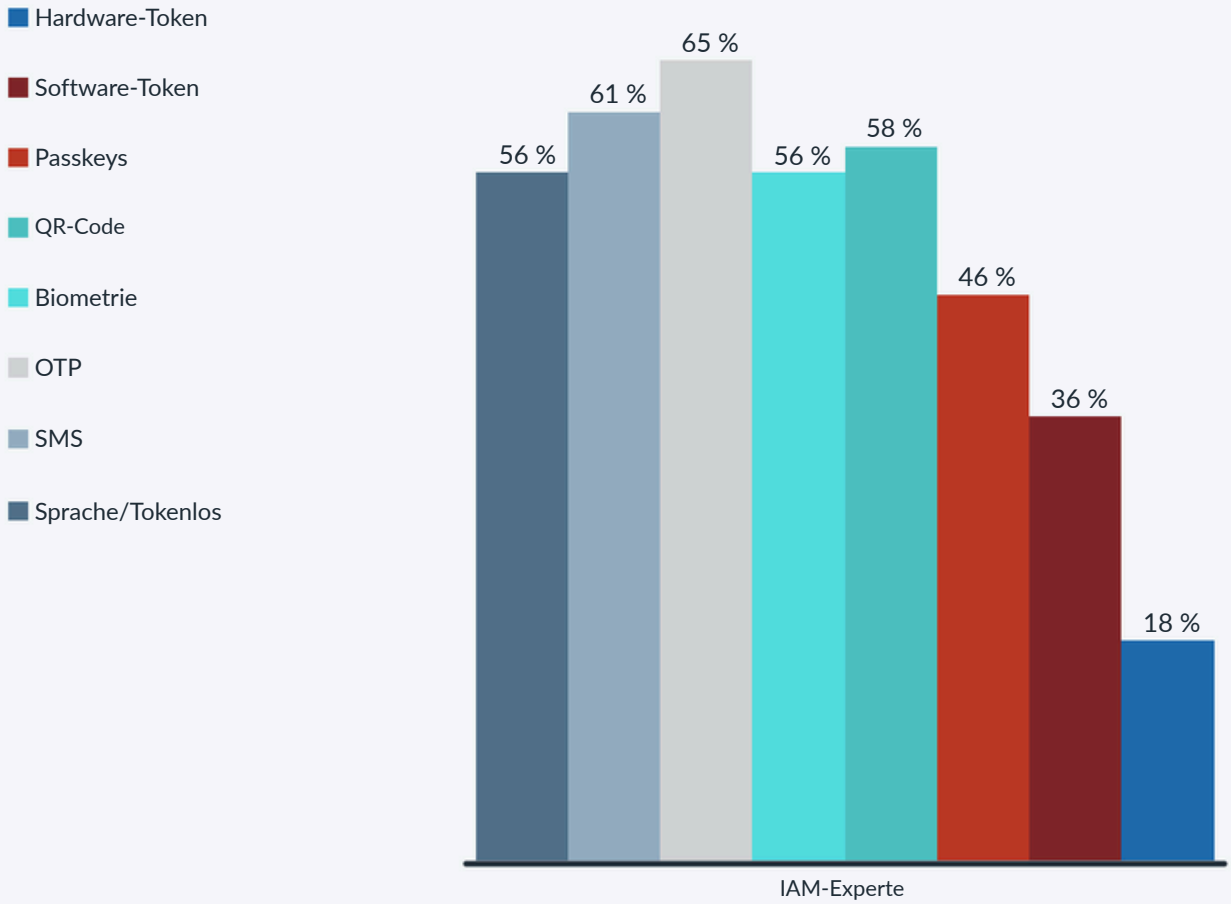
Bei der Einführung passwortloser Systeme müssen die meisten Unternehmen ein breites Spektrum an Benutzern und Anwendungsfällen berücksichtigen. Wir sind überzeugt, dass dies eine große Herausforderung für Unternehmen darstellt, da passwortlose Systeme noch immer hinterherhinken.

Welche der folgenden Umgebungen, Benutzergruppen oder Anwendungsfälle unterstützt Ihre Organisation?



Da die meisten Organisationen in hybriden Umgebungen arbeiten und unterschiedliche Benutzer und Anwendungsfälle unterstützen müssen, bereiten sich Identitätsspezialisten darauf vor, eine Vielzahl von Formfaktoren zu verwenden, um jedem Benutzer eine passwortlose Authentifizierung zu ermöglichen.

Welchen der folgenden Formfaktoren möchten Sie zur Implementierung passwortloser Lösungen verwenden?



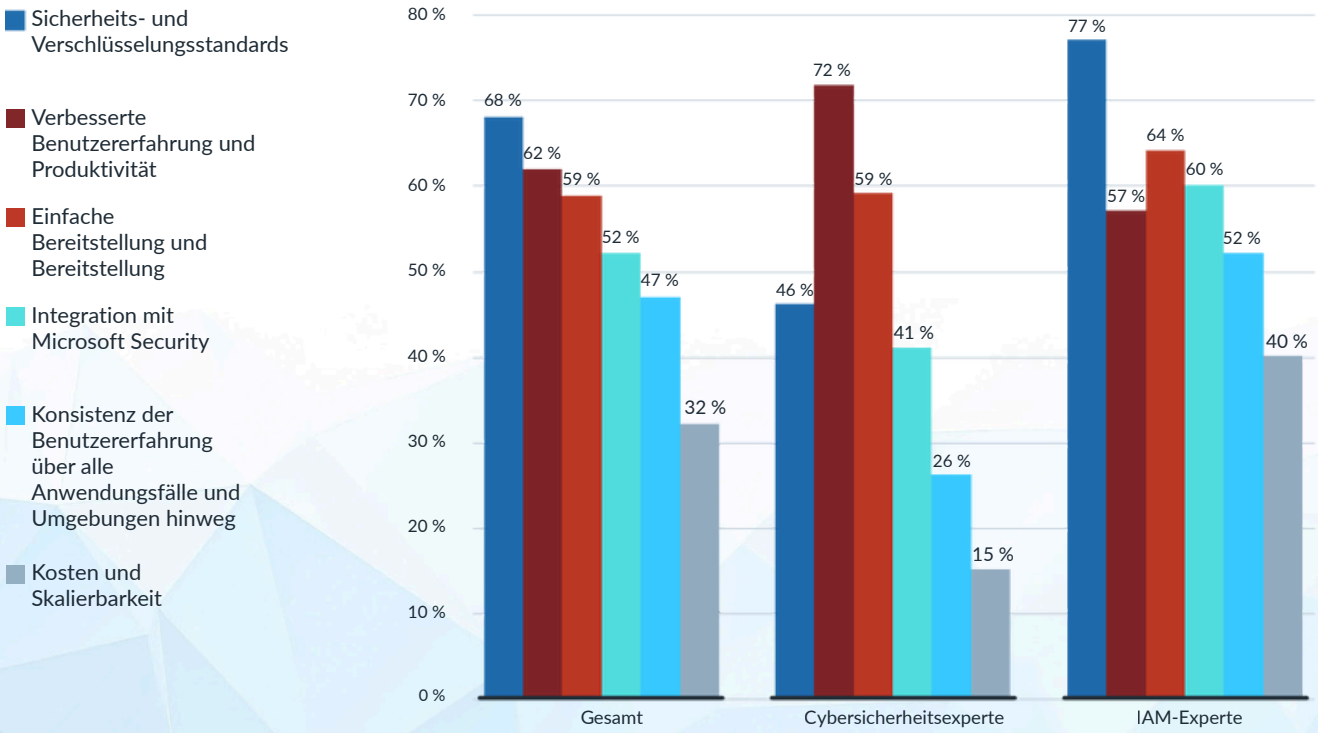
Der Kampf um passwortloses Anmelden

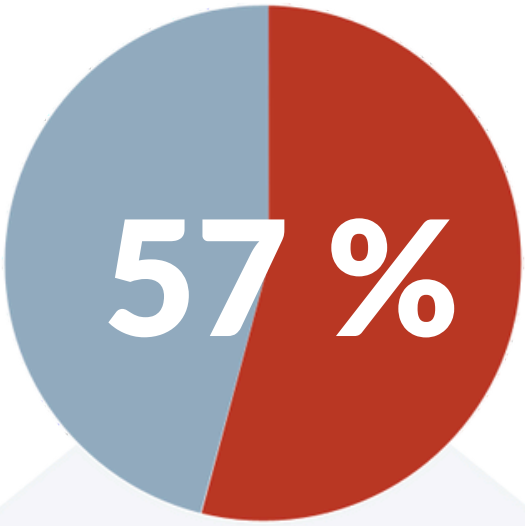
Fast alle (90 %) der Befragten gaben an, dass sie bei der Einführung passwortloser Lösungen durch bestimmte Herausforderungen ausgebremst würden. Diese Benutzer müssen sich jedoch nicht mit einer bestimmten Herausforderung auseinandersetzen. Stattdessen gibt es drei: 57 % der Befragten gaben an, dass Sicherheitsbedenken die Einführung passwortloser Lösungen verlangsamen, 56 % äußerten Bedenken hinsichtlich der Benutzerfreundlichkeit und 52 % nannten die fehlende vollständige Plattformunterstützung (einschließlich Legacy-Apps und Drittanbietersystemen) als Haupthindernis für die Einführung passwortloser Lösungen.

Dies sind alles wichtige Punkte, die Unternehmen überwinden müssen, um passwortloses Arbeiten effektiv zu implementieren. Interessanterweise spielen praktische Einschränkungen eine weitaus geringere Rolle: Nur 47 % der Nutzer gaben an, nicht über das nötige Geld für die Implementierung von passwortlosem Arbeiten zu verfügen.

Es gibt keine eindeutige Herausforderung, der sich Unternehmen stellen müssen. Um den unterschiedlichen Prioritäten der Experten im Bereich der passwortlosen Sicherheit gerecht zu werden (und die Herausforderungen zu bewältigen, die sie an der Einführung dieser Lösung hindern), müssen Unternehmen ein Gleichgewicht zwischen Sicherheits- und Verschlüsselungsstandards, verbesserter UX und Benutzerfreundlichkeit finden.

Welche Faktoren sind Ihnen bei der Auswahl einer passwortlosen Lösung am wichtigsten?





von Organisationen verwenden kein Passwort als primäres Authentifizierungsmittel

Neues Jahr, gleiches Problem

Passwörter sind Jahr für Jahr eine der Hauptursachen für Datenlecks:

Verizon Data Breach Investigations Report 2025: Missbrauch von Anmelde-informationen „ist immer noch häufigster Vektor."

Verizon Data Breach Data Breach Investigations Report 2024: „In den letzten 10 Jahren tauchten bei fast einem Drittel (31 %) der Datenlecks gestohlene Anmeldeinformationen auf."

Verizon-Bericht zu Untersuchungen zu Datenschutzverletzungen 2023: „Anmeldeinformationen haben in den letzten fünf Jahren stark an Bedeutung gewonnen, da die Verwendung gestohlener Anmeldeinformationen zum beliebtesten Einstiegspunkt für Datenschutzverletzungen geworden ist."

Im Verizon Data Breach Investigations Report 2022: wurde festgestellt, dass schlechte Passwortpraktiken in den letzten fünfzehn Jahren jedes Jahr „eine der Hauptursachen für Datenschutzverletzungen" waren.

Überwachung und Management von Identitätsrisiken

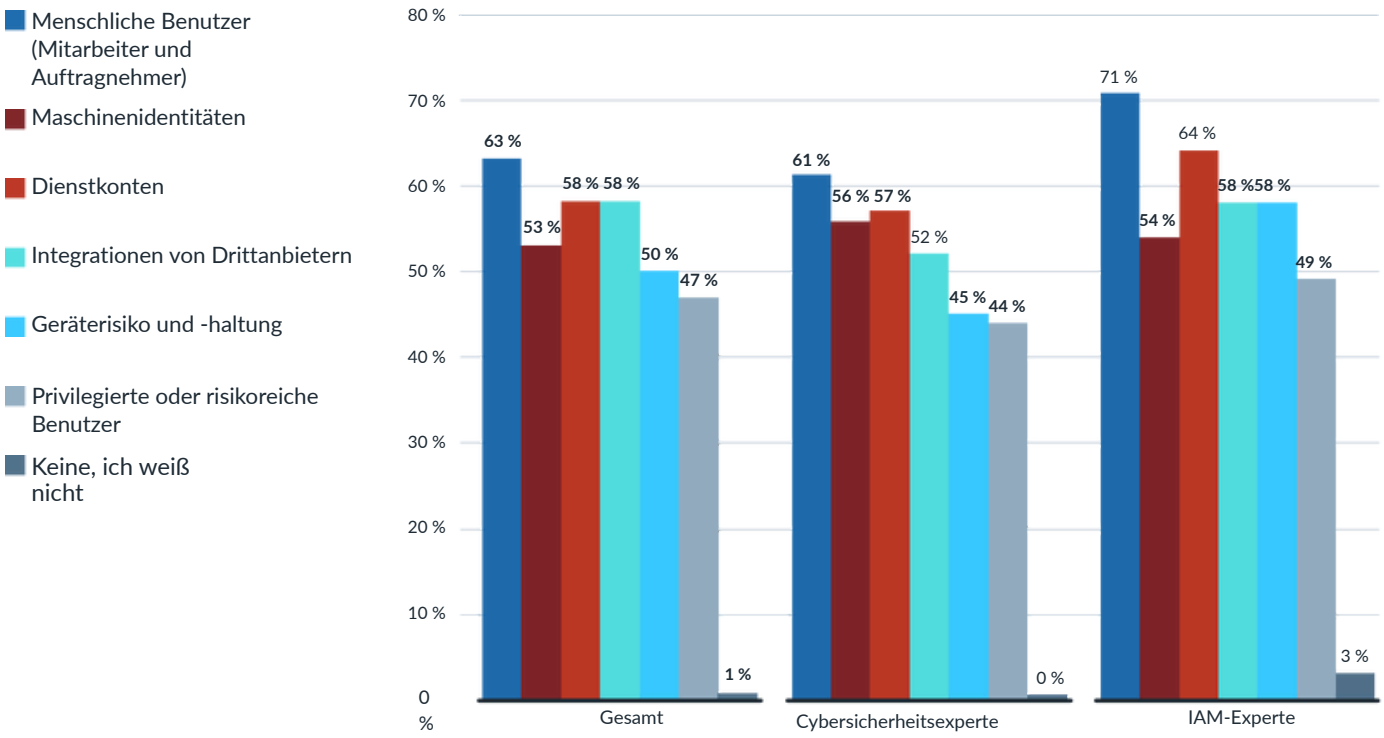
Unternehmen überwachen in hohem Maße Identitätsrisiken über alle Benutzer und Typen hinweg. Die meisten Befragten geben an, menschliche Benutzer, Computerkonten, Servicekonten und Drittanbieterintegrationen zu überwachen. Die Hälfte der Befragten gibt an, auch Geräterisiken und -status zu überwachen. IAM-Experten überwachen diese Konten häufiger auf Identitätsrisiken als ihre Kollegen im Bereich Cybersicherheit.

Es ist ermutigend, dass sich Unternehmen mit der Breite ihrer Angriffsfläche für Identitäten befassen. Doch die Integration all dieser Informationen – und ihre effektive Nutzung – wird eine Herausforderung sein. Bei Tausenden von Berechtigungen pro Konto entsteht eine beträchtliche Menge an Daten, die die Sicherheitsteams analysieren müssen, um Risiken zu erkennen und Maßnahmen zu priorisieren.

Dieser riesige Datenbestand könnte die Prioritäten der Befragten bei Investitionen in Cybersicherheit bestimmen: Mehr als ein Viertel (26 %) der Befragten gaben an, dass ISPM für sie oberste Priorität habe. ISPM kann Unternehmen dabei helfen, ihre Zugriffsrisiken zu bewerten und Maßnahmen zur Risikobegrenzung zu priorisieren.

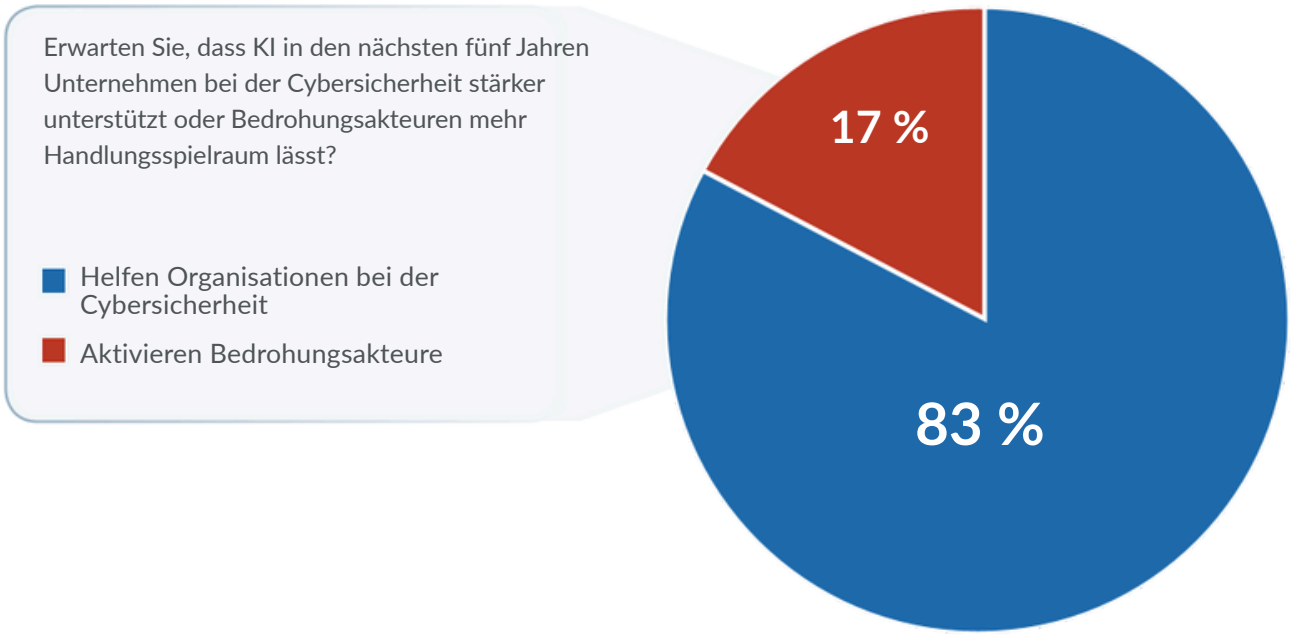
Ein Beispiel dafür, warum Unternehmen ISPM benötigen, um das Wesentliche zu erkennen und Risiken zu minimieren, sind Maschinenidentitäten. Unternehmen, die Maschinenidentitäten überwachen, meldeten die häufigsten Sicherheitsverletzungen mit den größten Auswirkungen und Verlusten. Fast drei Viertel (72 %) der Unternehmen, die Maschinenidentitäten überwachen, meldeten im letzten Jahr eine identitätsbezogene Sicherheitsverletzung. Diese Unternehmen meldeten auch den größten Schaden durch diese Sicherheitsverletzungen: 34 % gaben an, dass die Sicherheitsverletzungen erheblichen Schaden angerichtet haben, und die katastrophalsten Verluste: 27 % meldeten Verluste von über 10 Millionen US-Dollar.

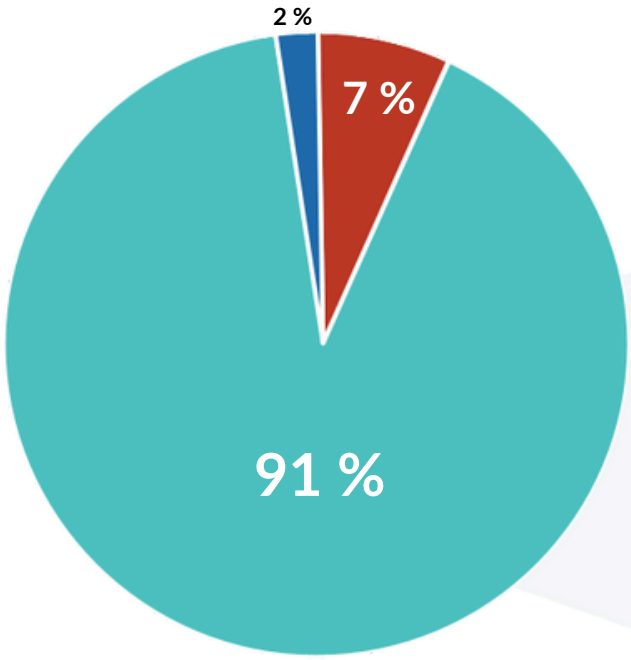
Welche Bereiche überwachen oder bewerten Sie aktiv hinsichtlich Identitätsrisiken?



KI für Cybersicherheit

Es setzt sich zunehmend die Erkenntnis durch, dass KI mehr zur Sicherheit beiträgt als zur Bekämpfung von Cyberkriminalität. 83 % der Nutzer geben an, dass die Technologie eher einen Vorteil für die Unternehmensverteidigung als für die Abwehr von Angriffen darstellt. 91 % der Befragten gaben an, dass sie planen, im nächsten Jahr KI in ihren Technologie-Stack zu implementieren – ein Anstieg um 12 Prozentpunkte seit der letztjährigen Umfrage.
Diese Antworten stimmen mit den Angaben der Benutzer überein, die sie bei den Cybersicherheitsfunktionen als vorrangig erachten: 40 % der Befragten gaben an, dass agentenbasierte KI für die Sicherheit ihre erste Wahl sei, mehr als jede andere Funktion.



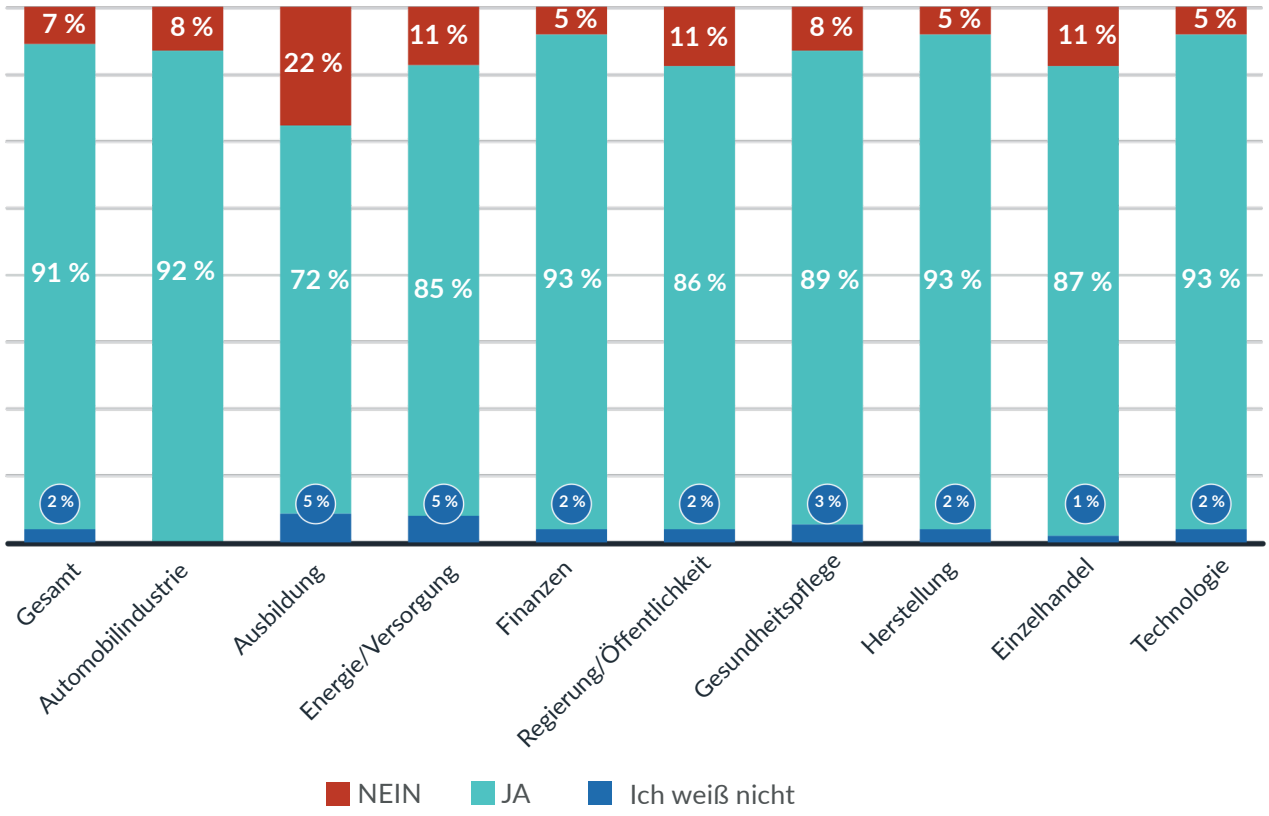


Plant Ihr Unternehmen, im nächsten Jahr Automatisierung, maschinelles Lernen oder andere Formen der KI als Teil seines Cybersicherheits-Stacks zu implementieren?

NEIN JA Ich weiß nicht

Nach Sektoren betrachtet, gibt fast jede Branche an, dass die Wahrscheinlichkeit hoch ist, im nächsten Jahr irgendeine Form von KI in ihren Technologie-Stack zu implementieren. Finanzwesen (93 %), Fertigung (93 %), Technologie (93 %) und die Automobilindustrie (92 %) gaben alle an, dass sie KI in hohem Maße in ihren Technologie-Stack integrieren. Das Bildungswesen (72 %) meldete den niedrigsten KI-Implementierungsgrad.

Nach Branche: Hat Ihr Unternehmen Pläne, im nächsten Jahr Automatisierung, maschinelles Lernen oder andere Formen der KI als Teil seiner Cybersicherheitsmaßnahmen zu implementieren?



Methodik und Stichprobe

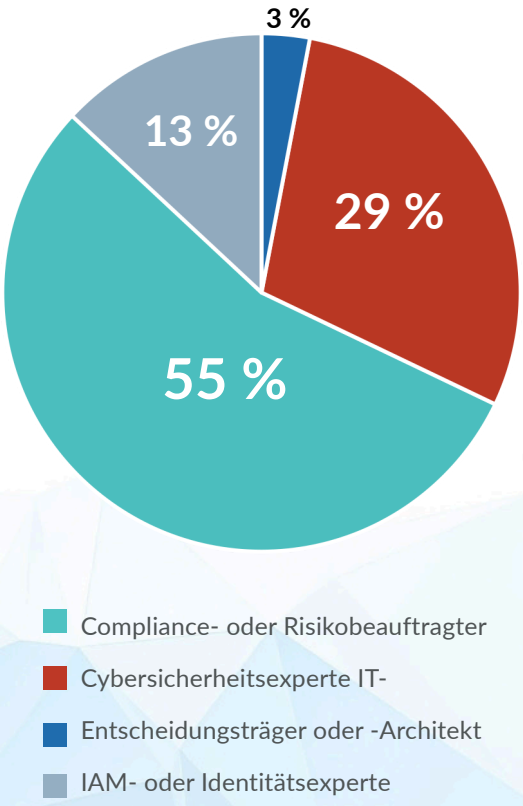
RSA veröffentlichte vom 20. Juli 2025 bis zum 15. August 2025 die RSA ID IQ-Umfrage 2026. Darin wurden Nutzer gebeten, 26 Fragen zu ihren Cybersicherheitsprioritäten, den Risiken für ihre Organisationen, der Häufigkeit und den Auswirkungen identitätsbezogener Datenschutzverletzungen sowie weiteren Faktoren im Identitätsbereich zu beantworten. In diesem Zeitraum erhielten wir 2.120 Antworten aus Australien, Brasilien, Kanada, Deutschland, Japan, dem Vereinigten Königreich und den Vereinigten Staaten.

Die Befragten wurden gebeten, ihre Rolle in ihrer Organisation zu benennen, den Sektor, in dem sie gearbeitet haben, und die Größe ihrer Organisation.

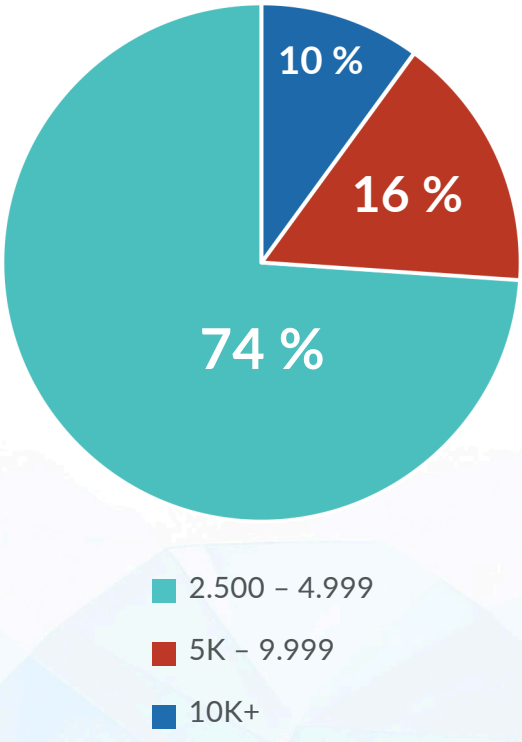
RSA überprüfte alle Antworten und korrelierte einige Antworten mit anderen, um festzustellen, ob zwischen den Antworten Beziehungen bestanden.

Demografie des RSA ID IQ im Jahr 2026

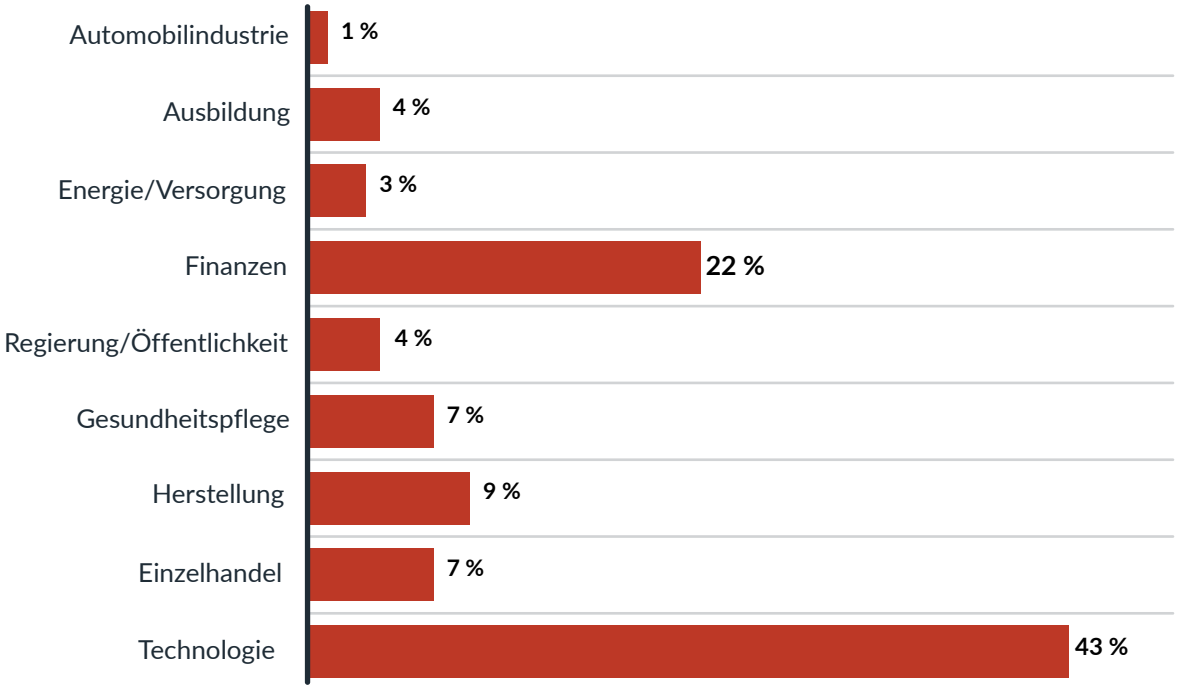
Rolle in der Organisation



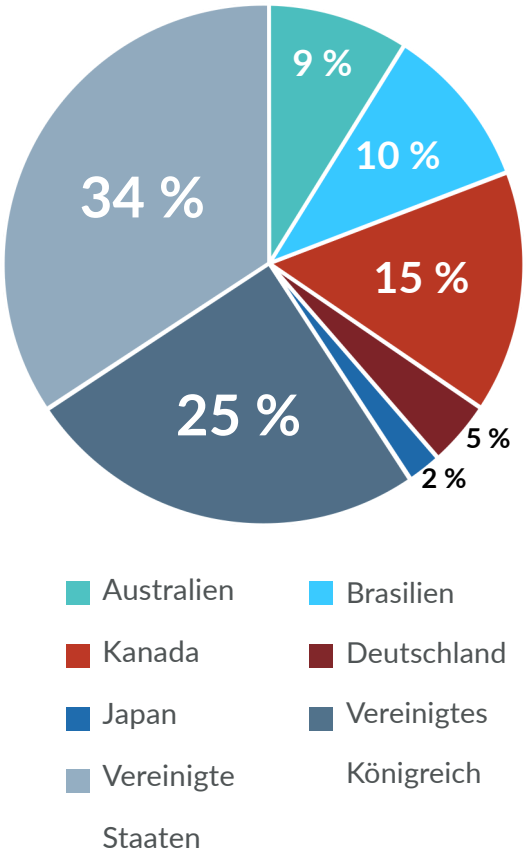
Unternehmensgröße



Branche



Land



RSA ID IQ-Report 2026:

Highlights für Deutschland

Im Vergleich zum Rest der Welt sticht Deutschland hervor, da es häufiger und kostspieligere Identitätsdiebstähle zu verzeichnen hat als andere Länder. Das Land nimmt auch eine Sonderstellung ein, was die Einschätzung der Risiken durch Phishing, Schatten-IT und Insider-Bedrohungen angeht.

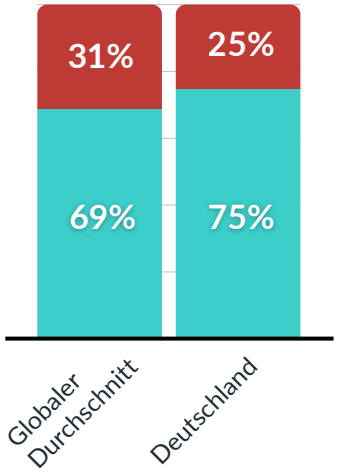
Im Folgenden wird aufgezeigt, wie sich Deutschland im Vergleich zum Rest der Welt im RSA ID IQ-Report 2026 unterscheidet. Diese Highlights basieren auf 111 deutschen Befragten:

Deutsche Unternehmen leiden häufiger unter Identitätsverletzungen als der Rest der Welt

75 % der deutschen Unternehmen gaben an, in den letzten drei Jahren eine Identitätsverletzung erlitten zu haben, sechs Prozentpunkte mehr als im globalen Durchschnitt.

- Nein, wir hatten keine Sicherheitsverletzung
- Ja, es gab eine Sicherheitsverletzung

War Ihr Unternehmen in den letzten drei Jahren von Identitätsdiebstahl betroffen?

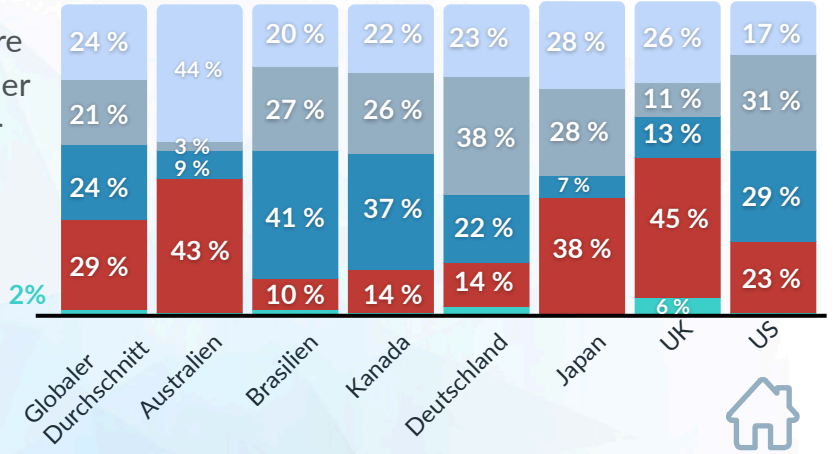


Mehr Verstöße, mehr Verluste

Möglicherweise aufgrund häufigerer Identitätsverstöße melden deutsche Unternehmen mehr Verluste als ihre Kollegen weltweit. Das Land meldet größere finanzielle Verluste als jedes andere Land der Welt, wobei die höchste Konzentration der Verluste zwischen 5 und 10 Millionen US-Dollar liegt.

- Mehr als 10.000.000
- Zwischen 5.000.000 - 10.000.000
- Zwischen 1.000.000-5.000.000
- Weniger als 1.000.000
- Nicht zutreffend / weiß ich nicht

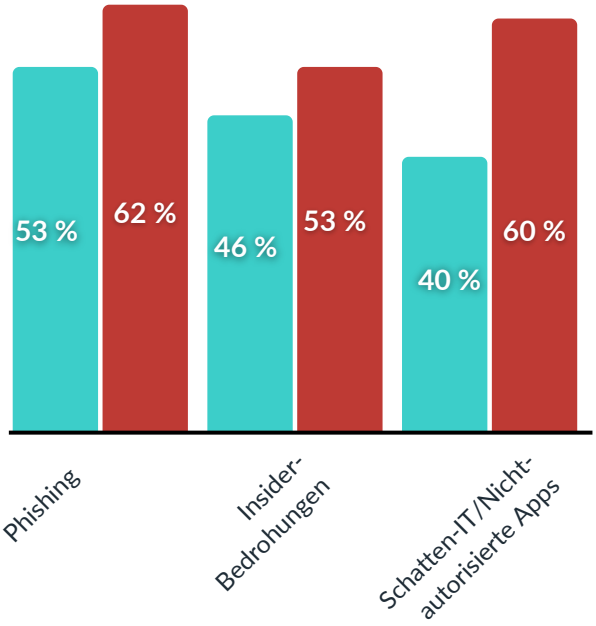
Wie viel Geld hat Ihr Unternehmen Ihrer Meinung nach in den letzten drei Jahren aufgrund von Datenschutzverletzungen im Zusammenhang mit Identitätsdaten verloren?



Phishing, Schatten-IT und Insider-Bedrohungen sind die größten Risiken

Deutsche Unternehmen betrachten Phishing, Schatten-IT und Insider-Bedrohungen als ein deutlich größeres Risiko als ihre Kollegen in anderen Ländern. Identity Security Posture Management (ISPM) und Identity Governance and Administration (IGA) sind wirksame Mittel, um diesen Bedenken zu begegnen.

Welche der folgenden Punkte stellen Ihrer Meinung nach die größten Cybersicherheitsrisiken für Ihr Unternehmen dar?

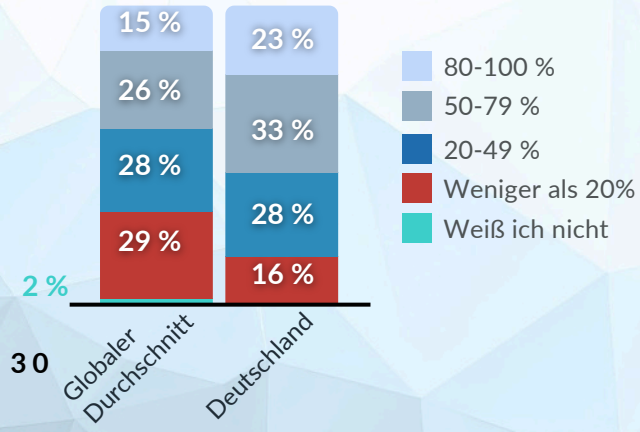


Alles oder nichts beim passwortlosen Zugang

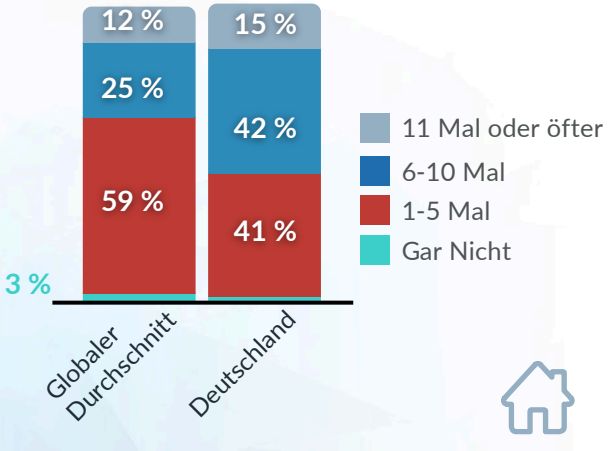
Deutschland macht große Fortschritte beim Übergang zum passwortlosen Zugang: Fast ein Viertel (23 %) der Befragten gibt an, dass ihre Nutzer in mindestens 80 % der Fälle passwortlos als primäre Authentifizierungsmethode verwenden.

Trotz dieser Fortschritte haben die Nutzer deutscher Unternehmen, die keine passwortlose Authentifizierung einsetzen, immer noch eine hohe Passwortbelastung. Deutschland hat den höchsten Anteil an Nutzern, die angaben, ihr Passwort täglich 6 bis 10 Mal für die Arbeit eingeben zu müssen.

Wie viel Prozent Ihrer Nutzer verwenden hauptsächlich passwortlose Formfaktoren, um die Authentifizierung durchzuführen?



Wie oft müssen Sie durchschnittlich pro Tag Ihr Passwort für die Arbeit eingeben?



Von der Information zur Aktion

Der erste Schritt zur Lösung eines Problems besteht darin, sich einzugestehen, dass es eines gibt. Der RSA ID IQ Report 2026 zeigt, dass Identitätsprobleme für viele Unternehmen ein erhebliches Problem darstellen, das zu kostspieligen und schwerwiegenden Datenschutzverletzungen führt.

Unternehmen sollten den Funktionen Vorrang einräumen, die ihre Sicherheit gewährleisten, darunter:

- Passwortlose Authentifizierung, die für jeden Benutzer, in jeder Umgebung und zu jeder Zeit funktioniert
- ISPM zur Erkennung von Risiken und Empfehlung von Maßnahmen.
- Umgebungsübergreifende Unterstützung zum Schutz von Cloud-, Hybrid- und On-Premises-Benutzern
- Bidirektionale Identitätsprüfung zum Schutz des IT-Helpdesks und der Benutzer vor MFA-Bypass-Angriffen und Social Engineering
- Automatisierte Identitätsintelligenz zur dynamischen Risikobewertung und Automatisierung von Reaktionen

Kontaktieren Sie RSA, um diese Funktionen zu testen. Oder überzeugen Sie sich selbst, warum die sichersten Unternehmen der Welt auf RSA setzen: Starten Sie jetzt Ihre kostenlose 45-Tage-Testversion von RSA ID Plus.

Über RSA

RSA bietet unternehmenskritische Cybersicherheitslösungen zum Schutz der sicherheitssensibelsten Organisationen der Welt. Die RSA Unified Identity Platform bietet echte passwortlose Identitätssicherheit, risikobasierten Zugriff, automatisierte Identitätsintelligenz und umfassende Identitätsverwaltung in Cloud-, Hybrid- und lokalen Umgebungen. Über 9.000 Hochsicherheitsorganisationen vertrauen RSA bei der Verwaltung von über 60 Millionen Identitäten, der Erkennung von Bedrohungen, dem sicheren Zugriff und der Einhaltung von Vorschriften.

Für weitere Informationen besuchen Sie unsere Website, um Kontakt zum Vertrieb aufzunehmen, einen Partner zu finden oder mehr über RSA zu erfahren.