RSA

Top Trends Identity Security 2025

Schrittweiser Fortschritt, exponentielle Auswirkungen

Januar 2025

RSA.com

Inhaltsverzeichnis.

Zusammenfassung: Mehr ist mehr.

Wo waren Sie am 19. Juli 2024?

Mit etwas Glück waren Sie nicht auf Reisen. An diesem Tag stürzten Berichten zufolge aufgrund einer Kombination aus einem CrowdStrike-Update und Einschränkungen in Microsoft-Umgebungen 8,5 Millionen Windows-Systeme ab, 10.000 Flüge wurden verspätet oder gestrichen und Fortune-500-Unternehmen erlitten direkte Verluste in Höhe von über 5 Milliarden US-Dollar. Wichtig ist, dass der Ausfall nicht auf Cyberkriminelle oder Bedrohungsakteure zurückzuführen war. Stattdessen fiel einfach die Infrastruktur aus – und als dies geschah, ging fast alles kaputt.

Dieser eine Tag wirft seine Schatten auf das Jahr 2025 und lässt erahnen, was wir in diesem Jahr in Sachen Sicherheit erwarten. Nicht, weil wir denken, dass sich die Einzelheiten wiederholen, sondern weil sich die Gesamtsituation seit letztem Juli nicht wirklich stark verändert hat.

Unternehmen werden in diesem Jahr weitgehend über die gleichen Technologien und Fähigkeiten verfügen wie im letzten Jahr. Sie werden weiterhin Fortschritte bei der Implementierung der Multi-Faktor-Authentifizierung (MFA), der Bereitstellung einer passwortlosen Authentifizierung und die Nutzung von KI in ihren Tech-Stacks verfeinern. Und sie werden weiterhin in hybriden Umgebungen arbeiten und immer mehr maschinelle Identitäten erzeugen. Gleichzeitig werden Bedrohungsakteure weiterhin Passwörter angreifen, ihre eigenen KI-Instanzen für Angriffe verwenden und versuchen, Wege zur Umgehung von MFA zu finden. Forscher werden weiterhin schrittweise Fortschritte bei neuen Technologien wie dem Quantencomputing machen, und Sicherheitsexperten werden sich weiterhin auf Bedrohungen vorbereiten, die in zehn Jahren noch auftreten werden.

Im Großen und Ganzen werden 2025 dieselben Systeme, Fähigkeiten, Risiken und Bedrohungen auftreten wie 2024. Wir erwarten bei keiner dieser Variablen eine Revolution. Stattdessen erwarten wir Entwicklungen in allen Bereichen.

Wenn jedoch ein einziges Software-Update Millionen von Computern zum Absturz bringen kann, wie es im Jahr 2024 der Fall war, werden Entwicklungen zu Revolutionen. Selbst wenn 2025 keine neuen, bahnbrechenden Technologien auf den Markt kommen, werden inkrementelle Fortschritte mit vernetzten Systemen, einer wachsenden Zahl von Nutzern und Agenten und einer KI, die schneller als jeder Mensch Entscheidungen treffen und Ergebnisse erzeugen kann, im Jahr 2025 exponentielle Auswirkungen haben.

Wir erwarten, dass es im Jahr 2025 von allem mehr geben wird: mehr MFA, mehr passwortlose Authentifizierung, mehr KI in Cybersicherheits-Stacks und mehr Benutzer (insbesondere mehr maschinelle Benutzer) sowie mehr Angriffe auf Passwörter und mehr Datenschutzverletzungen, die noch größeren Schaden anrichten.

Hinzu kommt eine neue US-Präsidentschaft mit veränderten Prioritäten in Sachen Cybersicherheit sowie neue globale Vorschriften, die nach dem Vorfall vom 19. Juli die Widerstandsfähigkeit betonen. Wir erwarten ein größeres, lauteres und riskanteres Jahr 2025.

Das soll Sie nicht abschreckend wirken. Im Gegenteil: Unternehmen sollten weiterhin in Cybersicherheit und Infrastrukturkapazitäten investieren, die ihnen helfen, einen perfekten Sturm zu überstehen. Sie sollten sich an der Vergangenheit orientieren, wo die meisten Datenschutzverletzungen durch Schwachstellen in der Identitätsinfrastruktur eines Unternehmens verursacht wurden. Das kann ein Passwort sein, das anfällig für Kompromittierungen ist, eine fehlende Implementierung von MFA oder ein Angreifer, der eine andere Schwachstelle im Identitätslebenszyklus eines Unternehmens ausnutzt, um sich seitlich zu bewegen, mehr Berechtigungen zu erhalten und mehr Schaden anzurichten. Ebenso werden vernetzte Systeme, die auf einzelnen Schwachstellen basieren, genau das tun. Widerstandsfähige Systeme werden gedeihen, wenn fragile Systeme versagen.

Ich weiß nicht, welches Datum die Cybersicherheit im Jahr 2025 definieren wird. Aber ich weiß, dass dieser Tag kommen wird – und er könnte bald kommen. Ich fordere Sie auf, nicht zu warten, um herauszufinden, wann es soweit sein wird, sondern jetzt Maßnahmen zu ergreifen, um sich vorzubereiten.

Rohit Ghai
RSA-CEO

“MFA wird im Jahr 2025 überall sein.“

Neues Jahr, gleiche Probleme

...unsere Beobachtungen zeigen, dass schlechte Passwortpraktiken seit bereits 2009 eine der Hauptursachen für Datenschutzverletzungen sind..“

Verizon-Bericht zu Untersuchungen zu Datenlecks 2022

„Anmeldeinformationen haben in den letzten fünf Jahren stark an Boden gewonnen, da die Verwendung gestohlener Anmeldeinformationen zum beliebtesten Einstiegspunkt für Sicherheitsverletzungen geworden ist.“

Verizon 2023 – Untersuchungsbericht zu Datenlecks

“In den letzten 10 Jahren wurden bei fast einem Drittel (31 %) der Sicherheitsverletzungen gestohlene Anmeldedaten verwendet.”

Verizon 2024 – Untersuchungsbericht zu Datenlecks

Ein 60 Jahre altes Problem wird auch im Jahr 2025 noch bestehen.

Digitale Passwörter werden seit den 1960er Jahren verwendet, als Fernando Corbató eine Möglichkeit suchte, mit der mehrere Benutzer ein Computersystem über ihren eigenen privaten Zugang bedienen können. In den Jahrzehnten seitdem haben sie sich in nahezu jedem Aspekt unseres Lebens festgesetzt.

Daran wird sich auch 2025 nichts ändern. Passwörter werden weiterhin verwendet und Bedrohungsakteure werden sie nutzen, wann immer es möglich ist. Angesichts der allgegenwärtigen MFA, die Cyberkriminelle dazu zwingt, ihre Taktiken anzupassen, und der KI, die Password-Spraying-Angriffe automatisieren kann, erwarten wir im Jahr 2025 einen deutlichen Anstieg von durch Passwörter verursachten Datendiebstählen.

Aber die Dinge ändern sich. Der RSA ID IQ Report 2025 ergab, dass 61 % der Organisationen im nächsten Jahr die Einführung einer passwortlosen Authentifizierung planen. Die Ergebnisse der Umfrage spiegeln größere Trends wider: Die passwortlose Authentifizierung gewinnt an Boden und wird bis Ende des Jahres weithin beliebt sein. Verbraucher werden den traditionellen Anmeldeprozess mit Benutzername und Passwort als umständlich empfinden und Wettbewerbsdruck auf Organisationen ausüben, ihre Authentifizierungsprozesse weiterzuentwickeln.

Unternehmen werden mit dieser Vorliebe für passwortlose Authentifizierung nur schwer zurechtkommen. Sie müssen Wege finden, um die Nachfrage der Benutzer zu befriedigen, ohne dass Compliance-Auflagen eine passwortlose Authentifizierung vorschreiben, ohne dass es einen vereinbarten passwortlosen Standard gibt und ohne dass Abläufe gestört werden, die auf einer Authentifizierung nach dem Motto „Etwas, das man weiß“ basieren. Dieser Druck wird es Unternehmen erschweren, eine unternehmenstaugliche passwortlose Authentifizierung zu implementieren – und kann dazu führen, dass sie Passwörter aus Prozessen entfernen, in denen sie bisher effektiv funktioniert haben.

Die Vorliebe der Verbraucher für passwortloses Arbeiten und das Fehlen eines globalen Standards werden auch die breiteren Kämpfe im Ökosystem beeinflussen, da Google, Meta, Apple und Microsoft weiterhin ihre eigenen passwortlosen Standards vorantreiben und um die Vorherrschaft gegenüber den anderen ringen.

> Cyberkriminelle werden **immer noch Wege finden, MFA zu umgehen.“**

> **44 %**
>
> der 2025 RSA ID IQ-Teilnehmer schätzten, dass die Gesamtkosten identitätsbezogener Datenschutzverletzungen die Kosten typischer Vorfälle übersteigen“

Die allgegenwärtige MFA wird Cyberkriminelle im Jahr 2025 dazu zwingen, ihre Bemühungen zu intensivieren.

Ein weiterer Trend, der die Cybersicherheit im Jahr 2025 verändern wird, ist unserer Erwartung nach, dass viel mehr Organisationen eine allgegenwärtige Multi-Faktor-Authentifizierung (MFA) einführen werden. Angesichts der Ankündigung von Plänen von Google und Microsoft, die MFA vorschreiben, der regulatorischen Auflagen für MFA und Phishing-resistente Authentifizierung sowie spektakulärer Vorfälle wie dem Datendiebstahl bei United Healthcare wird MFA im Jahr 2025 allgegenwärtig sein. Wir erwarten außerdem, dass Finanzinstitute aufgrund von SIM-Swapping und Angriffen auf Telekommunikationsunternehmen ihre Nutzung von SMS-basierter MFA reduzieren werden und dass Meta dem Beispiel von Google und Microsoft folgen und MFA vorschreiben wird.

Die schlechte Nachricht ist, dass Unternehmen trotz universeller MFA und des langsamen Vormarschs der passwortlosen Verfahren immer noch mit der Schwäche von Passwörtern umgehen müssen. Selbst mit Fortschritten wie MFA, FIDO und anderen passwortlosen Innovationen beginnen viele Unternehmenssysteme immer noch mit Passwörtern und bauen darauf auf oder verwenden Passwörter als Wiederherstellungs-mechanismus, wenn ein System kompromittiert wird..

MFA allein verhindert keine Datenschutz-verletzungen. Onboarding von Benutzern und Authentifikatoren ist in vielen Bereichen nicht stark genug, und Authentifikatoren sind nur so stark wie das Vertrauen, das während des Onboarding-Prozesses in sie gesetzt wird. Cyberkriminelle werden immer noch Wege finden, MFA durch Angriffe zu umgehen, die auf die Registrierung und die Wiederherstellung von Anmeldeinformationen abzielen, Session Hijacking und Social Engineering von IT Helpdesks.

Im Jahr 2025 wird es nicht mehr ausreichen, dass Unternehmen nur das Nötigste tun, um die Compliance-Vorschriften einzuhalten. Ein „Check-the-Box“-Ansatz für die Cybersicherheit wird einfach nicht funktionieren, wenn Bedrohungsakteure belohnt werden, wenn sie über den Tellerrand hinausschauen. Unternehmen werden eine ganzheitlichere Sichtweise der Sicherheit benötigen, die mit MFA beginnt und alle relevanten Vorschriften berücksichtigt - aber damit nicht endet.

Wir gehen zwar nicht davon aus, dass Bedrohungsakteure auf bewährte Angriffe wie Phishing oder Social Engineering verzichten werden, glauben jedoch, dass sich Bedrohungsakteure an die allgegenwärtige MFA anpassen werden, indem sie andere Punkte im Identitätslebenszyklus häufiger und dringlicher angreifen. Die Organisationen, die ihre Identitätskomponenten vereinheitlicht haben, werden besser darauf vorbereitet sein, diese Angriffe zu erkennen und zu stoppen und im Jahr 2025 sicher zu bleiben.

> Erwarten Sie im Jahr 2025 **mehr KI-gesteuerte Password-Spraying- und Social-Engineering-Angriffe.**“

Im Jahr 2025 wird die KI an Glanz verlieren und ihre Fähigkeiten verfeinern.

Im Dezember 2024 warnte das FBI, dass „Kriminelle generative künstliche Intelligenz (KI) nutzen, um Betrug in größerem Maßstab zu begehen, was die Glaubwürdigkeit ihrer Pläne erhöht. Generative KI reduziert den Zeit- und Arbeitsaufwand, den Kriminelle aufwenden müssen, um ihre Opfer zu täuschen.“`

Das wird sich auch 2025 fortsetzen. Cyberkriminelle werden weiterhin KI und maschinelles Lernen einsetzen, um Einzelpersonen und Organisationen anzugreifen: Die Technologie wird es für Bedrohungsakteure schneller, einfacher und kostengünstiger machen, Angriffe zu starten und zu automatisieren. Erwarten Sie im Jahr 2025 mehr KI-gesteuerte Passwort-Spraying- und Social-Engineering-Angriffe. Wir glauben auch, dass Cyberkriminelle KI in diesem Jahr stärker für biometrische Angriffe einsetzen werden. Da Cyberkriminelle KI verwenden, um Deepfakes zu erstellen und ihre Ziele sozial zu manipulieren, wird Lebendigkeit – natürliche, vor der Kamera und im Moment erfolgende Reaktionen – als Verteidigungslinie gegen diese Angriffe hervortreten.

Auf der Cybersicherheitsseite werden Organisationen beginnen, ihre Begriffe zu definieren, wenn es um KI geht. Der Begriff wird im Jahr 2025 keine so breite Definition mehr haben, da Organisationen ihren KI-Fokus einschränken und bewährte Techniken betonen werden, die Erkenntnisse liefern und Mehrwert liefern können, wie etwa maschinelles Lernen.

Kurzfristig werden Cybersicherheitsteams die Analyse als ersten Anwendungsfall bevorzugen, indem sie ihre eigenen Daten einlesen, um Erkenntnisse zu gewinnen und Maßnahmen zu priorisieren. Unternehmen werden lernen, dass die verschiedenen Ebenen besser in der Lage sind, beobachtetes Verhalten zu erkennen und abzuwehren, wenn sie Signalinformationen austauschen. Unternehmen, die einen ganzheitlicheren Ansatz für ihre Cybersicherheit verfolgen, werden diese Vorteile besser nutzen können, da integrierte Funktionen für den Austausch von Signalen zwischen Systemen gut geeignet sind. Wir gehen auch davon aus, dass die Anbieter anfangen werden, interne Assistenten anzubieten, die den Kunden erklären, wie sie die von ihnen gekaufte Technologie besser nutzen können.

Das Gegenteil ist der Fall: Die Cybersicherheit wird beginnen, die KI-Modelle zu benennen, die für sie nicht akzeptabel sind. So wird die Cybersicherheit beispielsweise keine kommerziell erhältlichen Engines oder große Sprachmodelle verwenden. Und die Unternehmen werden die vernünftige Entscheidung treffen, ihre Daten nicht für das Training öffentlicher KI-Modelle zu öffnen. Anstatt sich auf Dritte zu verlassen, wird die KI, die die Cybersicherheit nutzen wird, speziell von und für die Cybersicherheit entwickelt werden.

Kriminelle nutzen generative künstliche Intelligenz zur Erleichterung von Finanzbetrug.“

Die folgenden Techniken sind Auszüge aus FBI-Alarmnummer: I-120324-PSA

„Kriminelle betten KI-gestützte Chatbots in betrügerische Websites ein, um Opfer dazu zu bringen, auf bösartige Links zu klicken.“

„Kriminelle erstellen kurze Audioclips mit der Stimme einer geliebten Person, um sich in einer Krisensituation als naher Verwandter auszugeben und um sofortige finanzielle Unterstützung zu bitten oder ein Lösegeld zu fordern.“

„Kriminelle erstellen Videos für Echtzeit-Videochats mit angeblichen Firmenmanagern, Strafverfolgungsbeamten oder anderen Autoritätspersonen.“

10x-50x

Faktor, um den Maschinenidentitäten normale Konten übertreffen.”

Maschinelle Identitäten werden 2025 exponentiell wachsen.

Maschinenidentitäten waren schon immer eine bekannte Unbekannte für die IT: Sie werden verwendet, um Datenbanken, Microservices, Firewalls, Root-/Admin-Konten und nahezu jeden anderen Prozess auszuführen, der nicht an einen Menschen oder ein Gerät gebunden ist. Sie waren anderen Arten von Konten schon immer um mehrere Größenordnungen überlegen.

Im Jahr 2025 dürften diese Zahlen jedoch exponentiell wachsen, da durch das Hinzufügen von Cloud-Diensten oder das Erstellen eines neuen Projekts Hunderte von Maschinenkonten auf Knopfdruck erstellt werden.

Jedes dieser Maschinenkonten hat wiederum eine eigene Reihe von Berechtigungen. Viele dieser Konten agieren unabhängig als Agenten im Namen der Benutzer. Sie authentifizieren sich außerdem mit einer Vielzahl von Mitteln, darunter Kennwörter, Authentifizierungstoken, Sicherheitsschlüssel und x509-Zertifikate. Diese Konten werden meist von Entwicklern und durch Software von Cloud- und SaaS-Anbietern erstellt, nicht durch die internen IT-Abläufe des Unternehmens.

Die wachsende Zahl von Maschinenkonten, die eingeschränkte Sichtbarkeit, wann sie erstellt werden oder wie sie sich authentifizieren, und die zunehmende Erwartung, dass sie ohne Aufsicht agieren, werden Bedrohungsakteuren einen neuen Vorteil verschaffen: Cyberkriminelle werden versuchen, sich als diese Konten auszugeben oder sich als solche anzumelden.

Um Verstöße und seitliche Bewegungen von Bedrohungsakteuren zu verhindern, müssen Unternehmen diese Konten in Echtzeit überwachen und Zero-Trust-Prinzipien wie das Prinzip der geringsten Privilegien anwenden.

Dies kann für einige Organisationen eine Herausforderung darstellen, da die Architekturen für die Erfassung von Zugangsdaten in der Regel nicht auf die Cloud-Konten und -Systeme abgestimmt sind, die diese neuen Maschinenidentitäten generieren. Tatsächlich gehen wir davon aus, dass nicht alle Organisationen in der Lage sind, diese Änderung zu bewältigen, und rechnen damit, dass im nächsten Jahr mehrere Datenlecks mit Kosten von über 10 Millionen US-Dollar zumindest teilweise durch Maschinen-identitäten verursacht werden.

> Die Regulierungsbehörden werden **bei der Bewertung der Widerstandsfähigkeit von Organisationen weniger nachsichtig sein.“**

Was neue globale Vorschriften und eine US-Präsidentenregierung für die Cybersicherheit bedeuten.

Wir gehen zwar davon aus, dass bestimmte Vorschriften des US-Verteidigungsministeriums (DoD), etwa die Cybersecurity Model Certification (CMMC 2.0), in Kraft bleiben, doch der Beginn der zweiten Trump-Regierung wird die Cybersicherheitsagenda in den USA neu ausrichten und die Vorschriften weltweit beeinflussen.

Tatsächlich kann es sein, dass Organisationen einen geringeren Compliance-Aufwand für bestimmte Sicherheitsanforderungen verzeichnen. Wenn das der Fall ist, könnten Organisationen ihre Ausgaben von Initiativen zur Einhaltung gesetzlicher Vorschriften abziehen und stattdessen proaktivere Maßnahmen ergreifen, wie etwa die Migration von öffentlichen Clouds zu privaten Instanzen oder die Rückführung von Daten zurück in die lokalen Systeme, um Kundendaten zu schützen.

Dies kann auch bedeuten, dass Organisationen, die nur das absolute Minimum tun, um die Anforderungen zu erfüllen, ihre Ausgaben für Cybersicherheit zurückfahren – und sich selbst einem Risiko aussetzen. Sollten Organisationen ihre Cybersicherheitsprogramme zurückfahren, können diese Ausgabenänderungen und die weniger strengen Vorschriften dazu führen, dass die Versicherer größere Risiken wahrnehmen und höhere Versicherungsprämien für Cybersicherheit verlangen.

Außerhalb der USA werden Gesetze und Vorschriften wie die EU-Richtlinie 2 über Netz- und Informationssysteme (NIS2) und der Digital Operational Resilience Act (DORA) die Belastbarkeit betonen oder sie als kritische Komponente einbeziehen. Angesichts des CrowdStrike/Microsoft-Ausfalls im letzten Jahr, der rund 8,5 Millionen Geräte betraf, werden die Regulierungsbehörden bei der Bewertung der Belastbarkeit von Organisationen weniger nachsichtig sein.

Zur Vorbereitung sollten Unternehmen Szenarien durchdenken wie: „Was passiert, wenn der MFA-Cloud-Anbieter ausfällt oder nicht mehr verfügbar ist?“ Indem sie solche Situationen durchspielen, können Unternehmen erkennen, wo ihre Abhängigkeiten liegen und welche Prozesse oder Sicherheitskomponenten bei einem Ausfall eines Drittanbieters nicht mehr funktionieren könnten.

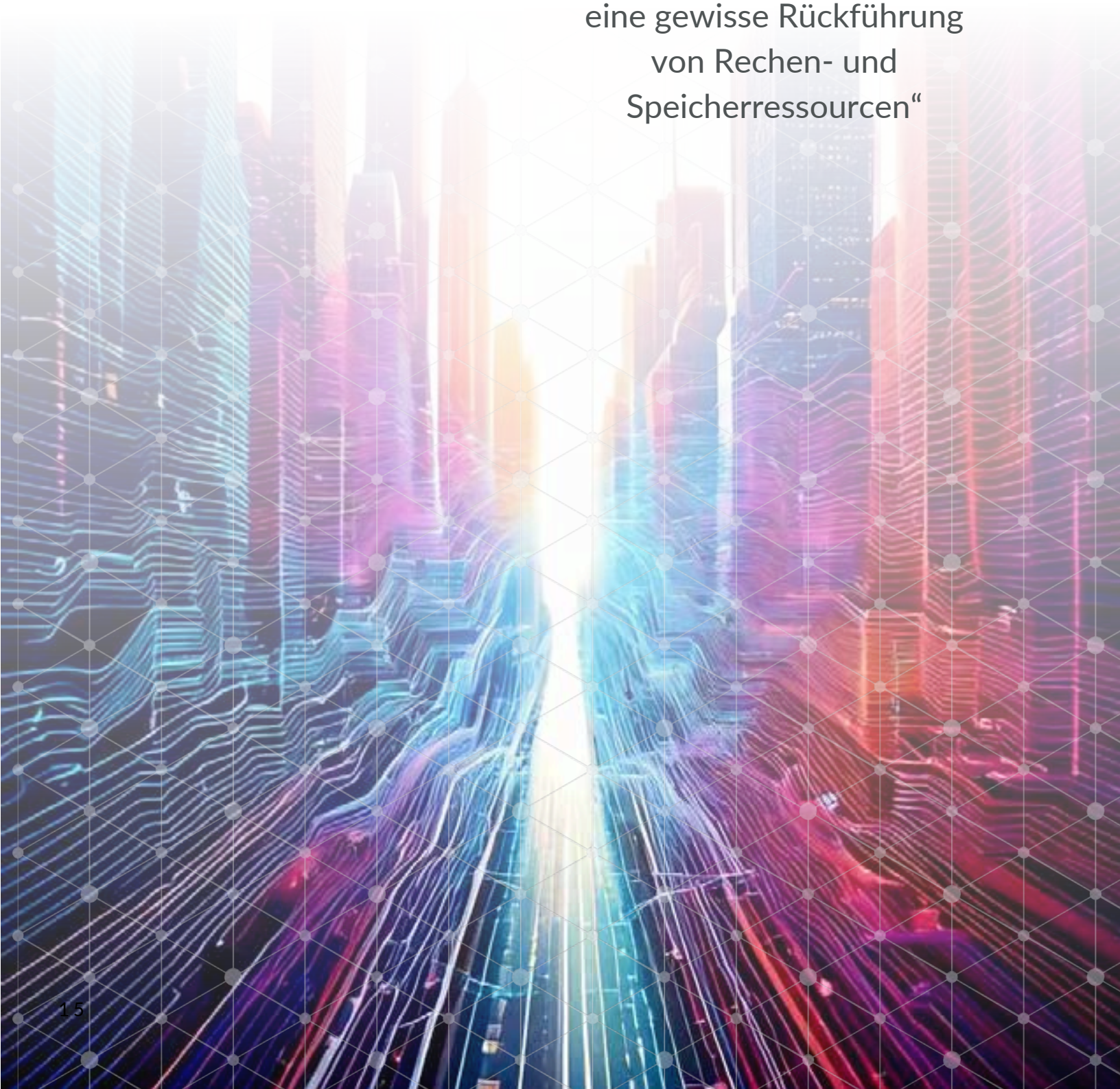
Wenn die Vorschriften abnehmen, werden die Unternehmen, die ihre Dienste aufrechterhalten und die Daten der Verbraucher schützen, herausragen. Diejenigen, die dies nicht tun, werden sich zu unglaubwürdigen Marken entwickeln, die Mitarbeiter und Kunden meiden werden. Widerstandsfähigkeit und Sicherheit werden an und für sich wertvoll sein und den Unternehmen, die sie vorleben, als Markenwert dienen.

70 %

der Organisationen arbeiten mit Hybrid-Implementierungen

80 %

der Teilnehmer der IDC-Studie „erwarten in den nächsten zwölf Monaten eine gewisse Rückführung von Rechen- und Speicherressourcen“



> **...**Unternehmen werden **auf alle Post-Quanten-Fähigkeiten gut vorbereitet sein, lange bevor diese eintreten.“**

Quantencomputing wird 2025 keine Bedrohung für die Verschlüsselung darstellen.

Die Quanteninformatik wird auch im Jahr 2025 schrittweise Fortschritte machen. In Anbetracht der erheblichen Ressourcen, die für den Betrieb von Quantencomputern erforderlich sind, des Stands des Quantencomputings (das sich noch überwiegend im Forschungsstadium befindet) und der neuen Richtlinien des NIST wird die Technologie in diesem Jahr jedoch keine nennenswerte Gefahr für die Verschlüsselung darstellen.

Durch die Umsetzung der neuen NIST-Richtlinien sind Unternehmen gut auf alle Post-Quanten-Funktionen vorbereitet, lange bevor diese eintreffen. Die Richtlinien empfehlen, 112-Bit-äquivalente (2048-Bit-Schlüssel) RSA-Schlüssel bis 2030 abzuschaffen und alle RSA-Algorithmen für digitale Verschlüsselungssignaturen bis 2035 zu verbieten. Dasselbe gilt auch für die Elliptic Curve Cryptography: ECDSA und EdDSA werden 2035 ihr Lebensende erreichen.

Der Leitfaden empfiehlt außerdem, die Schlüsselgröße auf 3072- oder 4096-Bit-RSA-Schlüssel zu erhöhen. Dies ist eine relativ einfach umzusetzende Lösung für Unternehmen, die die Lebensdauer der bestehenden Verschlüsselungsstandards um fünf Jahre verlängern wird. Um die neuen Richtlinien zu erfüllen, müssen die Unternehmen neue Schlüsselpaare generieren und neue Zertifikate ausstellen, und die Software, die mit diesen neuen Paaren und Zertifikaten arbeitet, muss längere Schlüsselgrößen unterstützen.

Die neueste Software sollte in der Lage sein, sich an diese neuen Anforderungen anzupassen. RSA wird die NIST-Anleitung befolgen und die Standardkonfigurationen der Produkte bei Bedarf anpassen.

Wichtig ist, dass die Auswirkungen und Anwendungen des Quantencomputings, so vielversprechend es eines Tages für die medizinische Forschung, den Finanzsektor und die Luft- und Raumfahrt sein könnte und so gefährlich es auch für die Verschlüsselung sein könnte, noch immer weitgehend theoretischer Natur sind.
Die Konzentration auf die theoretische Zukunft der Quantenmechanik lenkt von den sehr klaren, aktuellen und technisch einfachen Angriffen ab, mit denen Cyberkriminelle heute Erfolg haben:

- Change Healthcare wurde durch gestohlene Anmeldeinformationen kompromittiert und hatte MFA auf einigen seiner Konten nicht aktiviert
- Scattered Spider überzeugte das IT-Helpdesk-Personal, MFA-Anmeldeinformationen zu deaktivieren oder zurückzusetzen, um einen Ransomware-Angriff zu starten
- Colonial Pipeline wurde teilweise aufgrund eines verwaisten VPN-Kontos gehackt

Quantencomputing erfordert enorme Mittel und Ressourcen. Bei den drei oben aufgeführten Datenlecks – und den zahllosen anderen, die durch Phishing, schwache Anmeldeinformationen oder andere regelkonforme Taktiken verursacht wurden – war dies nicht der Fall.

Ein schönes Problem

„Es dürfte schwierig sein, drei Personen zu nennen, die mehr für die Computertechnik getan haben als Ron Rivest, Adi Shamir und Leonard Adleman. Ihre Namen sind nicht nur mit der Entwicklung einer der am weitesten verbreiteten und langlebigsten Verschlüsselungsmethoden verbunden, sondern auch mit der größten Tech-Konferenz der Welt und dem sichersten Identitätsunternehmen der Welt: RSA Security.

Eine so anerkannte, weit verbreitete und beständige Marke wie RSA zu haben, ist für uns ein großer Vorteil: Unternehmen wissen, dass RSA für Sicherheit steht. Aber wenn man an drei bahnbrechende Technologen gebunden ist, kann es manchmal ein wenig Verwirrung darüber geben, welcher „RSA“ was genau macht.

RSA Security und das RSA-Kryptosystem sind zwei verschiedene Einheiten. RSA Security hat das Public-Key-Kryptosystem im Jahr 2000 öffentlich zugänglich gemacht – unser Unternehmen hat den Standard jahrzehntelang nicht mehr gepflegt.

Obwohl der Algorithmus mit unseren Gründern und unserer Marke in Verbindung gebracht wird, ist er heute nicht Teil unserer Produkte oder Lösungen.“

Jim Taylor, RSA-Leiter für Produkt und Technologie

Gewarnt ist gewappnet.

RSA sichert das Sicherste. Seit Jahrzehnten wenden sich führende Unternehmen aus den Bereichen Behörden, Finanzdienstleistungen, Energie, Gesundheitswesen und anderen Bereichen an RSA, wenn es um Identitäts- und Zugriffsmanagement (IAM) geht, um den Zugriff zu sichern, Risiken zu vermeiden und die Produktivität zu steigern.

Erfahren Sie, warum das so ist, und bereiten Sie sich auf alles vor, was das Jahr 2025 bereithält: **Starten Sie jetzt Ihre RSA® ID Plus-Testversion**, um Ihre Zero Trust-Reife zu beschleunigen, indem Sie die weltweit sicherste Multi-Faktor-Authentifizierung (MFA), den sichersten Zugriff, das sicherste Single Sign-On (SSO), das sicherste Directory und andere wichtige Cybersicherheitsfunktionen in Cloud-, Hybrid- und lokalen Umgebungen implementieren.

Man erkennt uns an der Gesellschaft, in der wir uns bewegen.

9.000+
Kunden

70 %
der Fortune 100 Finanzunternehmen

99,99 %
Betriebszeit

13
US-Bundesministerien

13 Billionen
Ansprüche

40
Jahre der Innovation

Über RSA

Die KI-gestützte RSA Unified Identity Platform schützt die sichersten Organisationen der Welt vor den risikoreichsten Cyberangriffen von heute und morgen. RSA bietet die erforderlichen Identitätsinformationen, Authentifizierungs-, Zugriffs-, Governance- und Lebenszyklusfunktionen, um Bedrohungen vorzubeugen, den Zugriff zu sichern und Compliance zu ermöglichen. Mehr als 9.000 Organisationen, bei denen Sicherheit an erster Stelle steht, vertrauen RSA bei der Verwaltung von mehr als 60 Millionen Identitäten in lokalen, hybriden und Multi-Cloud-Umgebungen. Weitere Informationen finden Sie unter **RSA.com**.