okta

Der strategische Wert von Identity-Management für CISOs

Angesichts des schwindenden Netzwerkperimeters ist Identity zum zentralen Cybersicherheitsfaktor geworden, was die Sicherheitskonzepte fundamental verändert. Dieser Executive Brief fasst die Erkenntnisse aus einer Studie* zusammen, die von der Enterprise Strategy Group in Zusammenarbeit mit Okta zu dieser Entwicklung durchgeführt wurde. Dies sind die fünf wichtigsten Erkenntnisse zur Bedeutung von Identity-Sicherheit für CISOs:

1. Der CISO geht von der Defensive in die Offensive über
2. CISOs sind heute auch für das strategische Business Enablement verantwortlich
3. CISOs betrachten Identity-Management als größten Schwachpunkt in ihrem Unternehmen
4. CISOs sehen keine einfachen Lösungen für Identity-Sicherheit
5. Unübersichtliche Tech-Stacks verschärfen Identity-Sicherheitsprobleme

okta

WICHTIGE ERKENNTNIS Nr. 1:

Der CISO geht von der Defensive in die Offensive über

Die konventionellen perimeterbasierten Sicherheitsstrategien für Unternehmen sind grundsätzlich defensiv und können mit modernen Arbeitsweisen nicht mehr Schritt halten. Die Studie von ESG zeigt, dass die wichtigsten Aufgaben von CISOs – Risikoquantifizierung/-Reporting, Optimierung von Kontrollen sowie Datenschutz – proaktive Strategien erfordern.

Wichtigste Aufgaben von CISOs

WICHTIGE ERKENNTNIS Nr. 2:

CISOs sind heute auch für das strategische Business Enablement verantwortlich

Wie die ESG-Studie zeigt, betrachten CISOs ihren Verantwortungsbereich heute als strategisch wichtig und setzen stärker auf geschäftskritische Ergebnisse.

Wichtigste Verantwortungsbereiche von CISOs

Optimierung/Weiterentwicklung von Richtlinien für Datensicherheit und Datenschutz (z. B. Zero Trust)

CISOs definieren Erfolgsmetriken neu und betrachten nicht mehr ausschließlich Vorfallzahlen und Reaktionszeiten, sondern legen großen Wert auf die geschäftlichen Vorteile von Sicherheitsmaßnahmen, z. B. die Häufigkeit und Dauer von Ausfällen durch Sicherheitsvorfälle.

Quantifizierung/Demonstration der Vorteile von Sicherheitsmaßnahmen für geschäftliches Wachstum/Ziele

Ein Aufgabenbereich, der bisher hauptsächlich auf Compliance-Metriken konzentriert war, betrachtet die geschäftliche Produktivität und weitere personenbezogene Kennzahlen strategisch.

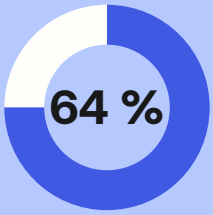
Gewährleistung starker und nahtloser Authentifizierung für Mitarbeiter und Kunden

Identity Governance liegt in der Prioritätenliste nun weit oben, da CISOs laut der Umfrage Verantwortungsbereiche wie die Verwaltung von Anmeldedaten und Zugriffsprüfungen im Hinblick auf den reibungslosen Zugang für Mitarbeiter und Kunden betrachten.

WICHTIGE ERKENNTNIS Nr. 3:

CISOs betrachten Identity-Management als größten Schwachpunkt in ihrem Unternehmen

Trotz des Wechsels von reaktiven zu proaktiven Strategien schätzen rund 66 % der befragten CISOs den Schutz ihres Unternehmens vor Cyberangriffen als schwierig ein. Vor allem jedoch betrachten CISOs die Identity-Sicherheit als ihre größte Schwachstelle und berichten von einer Vielzahl Identity-bezogener Probleme, die ihre Gesamtsicherheit schwächen. Das ist wenig überraschend, da Identity laut Untersuchungen heute der wichtigste Vektor bei Data Breaches ist.



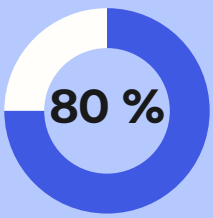
der CISOs schätzen das Stoppen von Cyberangriffen als **schwierig** ein

66 %

der CISOs sagen, dass die **Mehrheit** der **Sicherheitsvorfälle** durch Identities verursacht wird

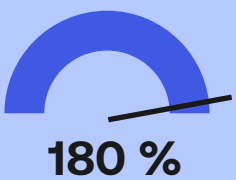
Von CISOs genannte größte Herausforderungen für das Identity-Management, die Cybersicherheitsmaßnahmen behindern

1. Fehlende Möglichkeit zum zuverlässigen Identifizieren und Verhindern von betrügerischen Account-Erstellungen und Anmeldeversuchen im großen Maßstab
2. Keine einheitlichen Identity Governance-Verfahren
3. Fehlende Unterstützung für starke Authentifizierung/ starke Abhängigkeit von Passwörtern
4. Manuelle/ fragmentierte Identity-Prozesse
5. Unzureichende MFA



aller Data Breaches beginnen mit **kompromittierten Identites**

Verizon Data Breach Investigations Report 2024



Steigerung im Jahres-vergleich bei Identity-basierten Angriffen

Verizon Data Breach Investigations Report 2024

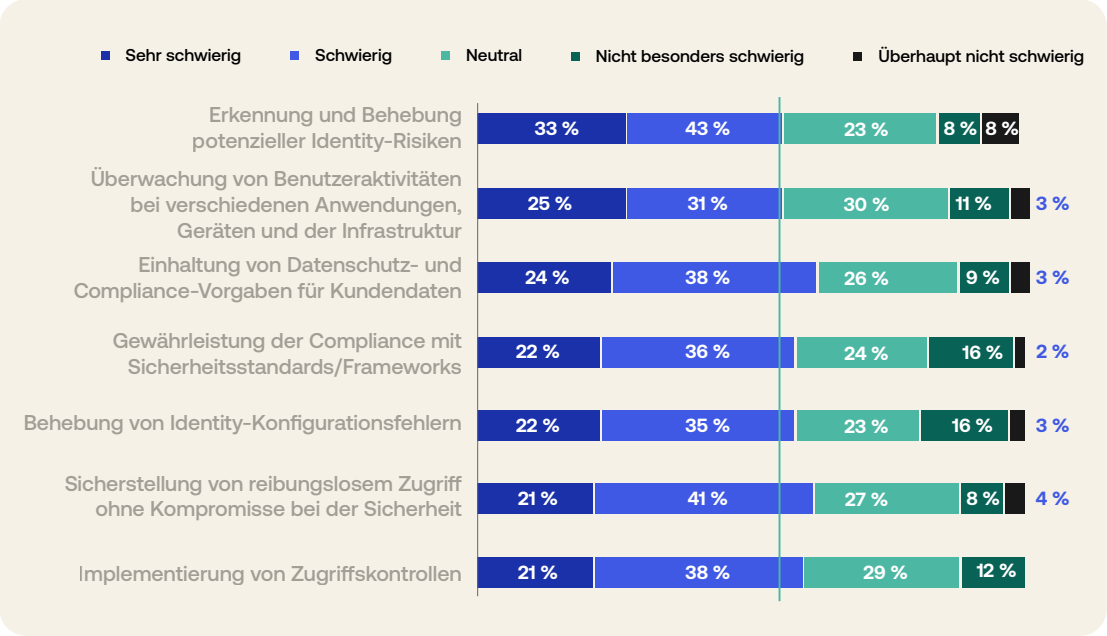
okta

WICHTIGE ERKENNTNIS Nr. 4:

CISOs sehen keine einfachen Lösungen für Identity-Sicherheit

Da Identities bei den meisten Data Breaches eine zentrale Rolle spielen, überrascht es kaum, dass für die überwiegende Mehrheit der befragten CISOs (76 %) die Stärkung der Identity-Sicherheit höchste Priorität hat. Doch warum beheben sie nicht einfach das Problem?

Weil es nicht nur ein einziges Problem gibt, das zu lösen ist. Die CISOs kämpfen bei der Identity-Sicherheit an mehreren Fronten – und für die meisten ist ***jedes Element*** der Identity-Sicherheit eine Herausforderung.



WICHTIGE ERKENNTNIS Nr. 5:

Unübersichtliche Tech-Stacks verschärfen Identity-Sicherheitsprobleme

Ein Aspekt, der sowohl das Business Enablement als auch den Schutz des Unternehmens erschwert, sind unübersichtliche Tech-Stacks. Dezentrale Technologiebereitstellung und SaaS-Wildwuchs sind in typischen Unternehmen eine grassierende Plage. Mittlerweile treten diese Probleme jedoch auch bei Sicherheitstechnologien auf. Die Studie hat gezeigt, dass die meisten Unternehmen mit mehr als 50 unterschiedlichen Cybersicherheitsanbietern zusammenarbeiten. Security-Teams wenden zu viel Zeit für die manuelle Abstimmung der Prozesse und Datenflüsse von Unternehmensanwendungen auf, während CISOs versuchen, bessere Integrationen zu implementieren und Redundanzen zu vermeiden.

Die Studie zeigte auch:

Größte Identity-Sicherheitsrisiken

1. Transparenzlücken zwischen verschiedenen Sicherheitstools
2. Konfigurationsfehler/Accounts mit zu umfangreichen Zugriffsrechten

Größte Hindernisse für reibungslose Zugriffe

1. Lösungsübergreifende Verwaltung von Audit-Trails
2. Komplexität bei der Verwaltung mehrerer Identity-Lösungen

Das typische Unternehmen hat 60 unterschiedliche Cybersicherheitsanbieter

Mit Okta zu einer Identity-zentrierten Sicherheitsstrategie

Die ESG-Studie zeigt ganz klar, dass Identity-Management nicht mehr nur als IT-Funktion betrachtet werden kann, sondern für moderne Unternehmenssicherheit unverzichtbar ist. Die Identity-Plattform von Okta ist darauf ausgelegt, die umfassende Sicherheit und Flexibilität bereitzustellen, die CISOs für einen proaktiven Identity-zentrierten Ansatz benötigen. Okta unterstützt CISOs beim Wechsel von der Defensive zur Offensive – mit zuverlässiger Identity-Sicherheit, die Risiken minimiert, die Komplexität vereinfacht und dynamische Bedrohungen abwehrt.

* Die Studie/Umfrage wurde von Enterprise Strategy Group in Zusammenarbeit mit Okta durchgeführt. Dazu wurden im Januar und Februar 2025 mehr als 150 CISOs in Nordamerika, EMEA und APJ befragt.

Möchten Sie mehr über die Plattform erfahren?

Gerne sprechen wir mit Ihnen über Ihre konkreten Herausforderungen und zeigen Ihnen, die Okta Sie unterstützen kann.

Mehr erfahren