TECHNISCHE SCHULDEN IN DER CYBERSICHERHEIT DURCHDRINGEN UNTERNEHMEN

Der ***CyberArk 2022 Identity Security Threat Landscape Report***[1] zeigt das sich rasch ausbreitende Identitätsproblem und die grassierenden technischen Schulden in der Cybersicherheit, die aus einem Ungleichgewicht mit Investitionsprioritäten für digitale Initiativen entsteht.

Digitale Initiativen beeinflussen Sicherheitsprioritäten

73%

der Sicherheitsexperten sagen, dass die Sicherheit zugunsten umfassender Geschäftsinitiativen in den Hintergrund getreten ist

97%

der Unternehmen haben in den letzten 12 Monaten die Einführung mindestens einer IT- oder digitalen Initiative beschleunigt

Menschliche und nicht-menschliche digitale Identitäten wachsen rasant

1:25

Durchschnittlich greifen Mitarbeiter auf mehr als 25 Anwendungen und Konten zu

11x

Maschinelle Identitäten übersteigen menschliche Identitäten um das 11-fache

53% der Mitarbeiter können auf sensible Unternehmensdaten zugreifen

74% der nicht-menschlichen Identitäten oder Bots können auf sensible Daten und Werte zugreifen

DIE ANGRIFFSFLÄCHE 2022

Die am weitesten verbreiteten Angriffsarten

RANSOMWARE

>60%
der Unternehmen waren im vergangenen Jahr von einem Ransomware-Angriff betroffen

2
Durchschnittliche Anzahl von Angriffen bei Organisationen im Gesundheitswesen

SOFTWARE SUPPLY CHAIN

>65%
der Unternehmen waren Opfer eines Angriffs im Zusammenhang mit der Software Supply Chain, der zu Datenverlusten oder kompromittierten Assets führte

88%
der Energie- und Versorgungsunternehmen erlitten einen erfolgreichen Angriff auf ihre Software Supply Chain

Häufigste Ursache für potenzielle Risiken bei der Cybersicherheit

84% Hybrides Arbeiten

80% Neue digitale Services für Kunden oder Bürger

81% Zunehmendes Outsourcing von Remote-Anbietern/ Lieferanten

37% geben an, dass der Zugang zu Anmeldeinformationen der Risikofaktor Nr. 1 für ihr Unternehmen ist

IDENTITÄTSBEZOGENE TECHNISCHE SCHULDEN IN DER CYBERSICHERHEIT AUFGEDECKT

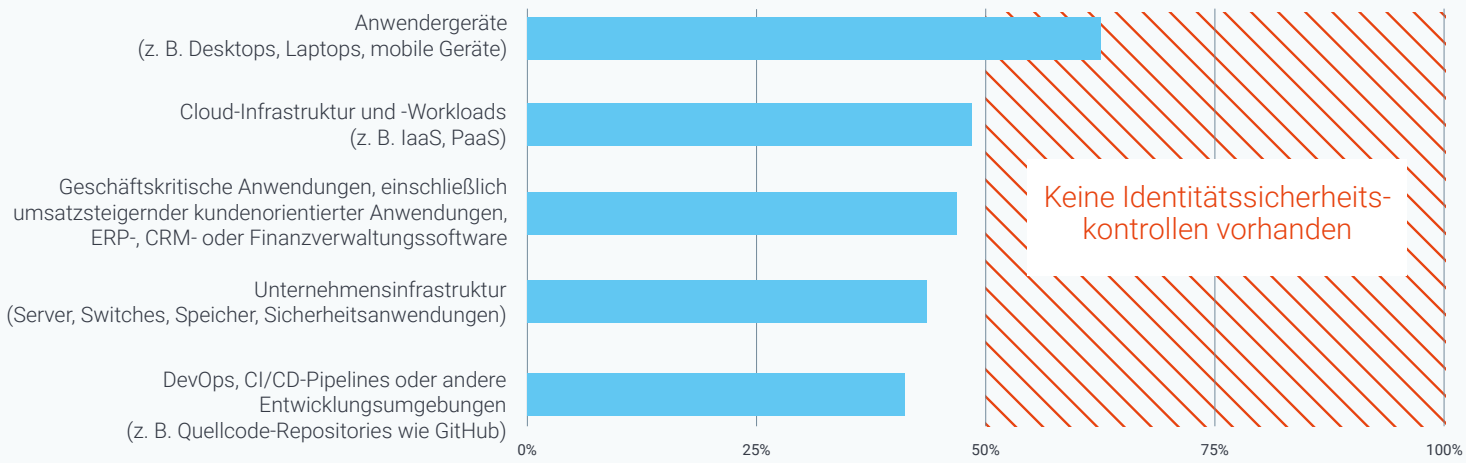
Die Befragten gaben an, dass in wichtigen IT-Umgebungen keine Maßnahmen für die Identitätssicherheit existieren, was das Risiko erhöht.

52%
der Identitäten in geschäftskritischen Anwendungen sind ungeschützt

55%
haben keine Identitätssicherheitskontrollen für Cloud-Infrastrukturen und -Workloads

85%
der Mitarbeiter speichern Secrets an unterschiedlichen Orten in DevOps-Umgebungen

Q. Für welche der folgenden Umgebungen und Geräte hat Ihr Unternehmen Identitätssicherheitskontrollen eingerichtet?



UNTERNEHMEN PRIORISIEREN IDENTITÄTSSICHERHEITSKONTROLLEN ZUR DURCHSETZUNG VON ZERO-TRUST-PRINZIPIEN

59%
priorisieren Tools für die Identitätssicherheit

54%
priorisieren Workload-Sicherheit

45%
priorisieren Datensicherheit

Der CyberArk Identity Security Threat Landscape Report 2022 zeigt, dass Unternehmen durch technische Schulden in der Cybersecurity und fehlende Identitätssicherheitskontrollen zum Schutz ihrer sensiblen Daten und Assets gefährdet sind. Die Einführung eines Zero-Trust-Ansatzes mit dem Least-Privilege-Prinzip wird die Sicherheitslücke verkleinern und die Sicherheitslage des Unternehmens verbessern.

HIER GEHT ES ZUM REPORT

[1]The CyberArk 2022 Identity Security Threat Landscape Report surveyed 1,750 IT security decisions worldwide with organizations of at least 500 employees or more across all private and public sectors.

www.cyberark.com

CYBERARK®