CYBERARK®
The Identity Security Company

WHITEPAPER

Vier Wege zur Sicherung von Identitäten im Zuge der Entwicklung von Privilegien

Inhaltsverzeichnis

Wahrscheinlich könnten Sie angesichts der dynamischen Bedrohungslandschaft ein wenig Guidance gebrauchen, wenn Sie ein IT- oder Security Experte sind.

Zumindest die Netzwerkadministratoren, die die Systeme Ihres Unternehmens warten, setzen die für ihre Arbeit wichtigen Technologien angemessen ein – und verfügen oft über eine entsprechende Ausbildung. Die Risiken im Zusammenhang mit ihrem Zugang sind erheblich, aber Sie können sich darauf verlassen, dass sie einige Dinge wissen:

- Ihre Basis privilegierter Nutzer
- Wie Sie sie durch PAM-Kontrollen (Privileged Access Management) schützen können
- Die Tatsache, dass sie nur eine kleine *Teilmenge* Ihrer Belegschaft sind, die geschützt werden muss – nicht das gesamte Unternehmen

Dasselbe gilt für Ihre Techniker, die mit der Cloud arbeiten, Ihre Sicherheitsexperten und andere Beteiligte mit privilegiertem Zugriff.

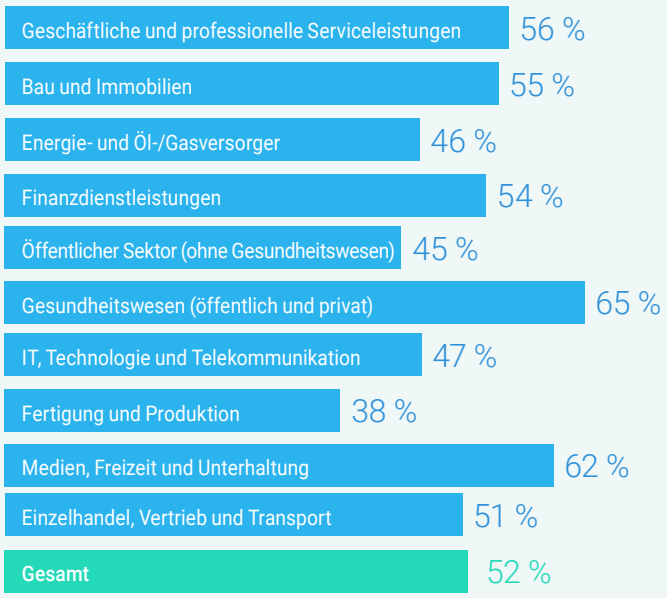
Aber was ist mit dem neu eingestellten Sales Operations Manager, der uneingeschränkten Zugriff auf die Daten Ihrer Kunden hat? Oder mit dem HR-Administrator, dessen Aufgabe seit kurzem die Verwaltung vertraulicher Mitarbeiterdaten in Workday ist?

Jeder Nutzer kann unter bestimmten Bedingungen privilegierte Berechtigungen erhalten. Dazu gehören Mitarbeiter, die Geschäftsanwendungen verwenden, mit denen sie auf die Ressourcen zugreifen und Aktionen durchführen können, die Angreifer ausnutzen wollen. Egal, ob Sie ein CIO oder ein PAM-Administrator sind, Sie werden diese Entwicklung der Privilegien wahrscheinlich regelmäßig beobachten.

Der Schutz der Identitäten Ihrer Nutzer – von der Sicherung der Authentifizierung über die Gewährung, Zertifizierung und den Widerruf des Zugriffs – ist von entscheidender Bedeutung. Aber es ist nicht einfach, da die Anzahl der Benutzer und Anwendungen, die geschützt werden müssen, laufend zunimmt. Was in vielen Fällen *nicht* wächst, sind die Mittel, die Sie für die Sicherung dieser Ressourcen bereitstellen können.

Wie kann Ihr Team diese Herausforderung trotz aller Widrigkeiten bewältigen?

Branchenaufteilung: Durchschnittlicher Prozentsatz der Mitarbeiter, die Zugriff auf sensible Unternehmensdaten erhalten



Quelle: CyberArk Identity Security Threat Landscape Report 2022

PAM-Kontrollen zum Schutz privilegierter Anmeldedaten und Sessions bleiben weiterhin von entscheidender Bedeutung. In modernen Unternehmen können IT- und Sicherheitsteams jedoch zusätzliche Maßnahmen ergreifen, um die Risiken im Zusammenhang mit erweiterten Berechtigungen zu minimieren. Hierzu gehören:

- Erweiterung intelligenter Privilegienkontrollen von Ihrem PAM-Programm auf Ihre gesamte Belegschaft: Schutz der Passwörter der Mitarbeiter und Sicherung von Sessions mit hohem Risiko in Webanwendungen.
- Automatisierung komplexer Aufgaben bei der Orchestrierung von Prozessen für die Verwaltung aller Identitäten, von der Bereitstellung bis zum Entzug der Berechtigungen.
- Routinemäßige Zertifizierung des Zugriffs auf privilegierte Konten zur Erfüllung von Audit- und Compliance-Anforderungen und zur Einhaltung des Prinzips des Least-Privilege-Zugriffs.

Lesen Sie weiter, um mehr über vier Sicherheitsebenen zu erfahren, die Ihnen helfen können, Ihr Unternehmen angesichts der Entwicklung zu mehr privilegierten Berechtigungen vor Bedrohungen zu schützen.

1. Bieten Sie unternehmensgerechte Sicherheit für die Passwörter Ihrer Mitarbeiter

Angreifer zielen in der Regel auf die Zugangsdaten aller Personen in Ihrem Unternehmen ab, die Zugriff auf die von ihnen gesuchten Ressourcen haben. Sie werden es auf den SSH-Schlüssel eines Netzwerkadministrators abgesehen haben. Sie versuchen auch, an das Passwort eines NetSuite-Nutzers zu gelangen. Beide Arten von Anmeldedaten können es ihnen ermöglichen, Daten zu stehlen oder einen Angriff zu starten.

> 82 % der Sicherheitsverletzungen betreffen den menschlichen Aspekt, zu dem die vielen Möglichkeiten gehören, wie Mitarbeiter ihre Passwörter speichern, auf sie zugreifen und sie an häufig genutzte Geschäftsanwendungen weitergeben.[1]

Was können Unternehmen dagegen tun? Der erste Schritt besteht darin, das Problem zu verstehen.

Um die Verwendung von Passwörtern zu reduzieren, setzen viele Unternehmen auf Single Sign-On (SSO) als schützende Grundlage. Leider unterstützen viele Apps SSO nicht und verwenden keine modernen Identitätsprotokolle.

Das Problem hat Auswirkungen auf andere Bereiche. Mitarbeiter nutzen häufig browserbasierte Passwortmanager oder Passwortmanager-Tools für Privatanwender. Dies bringt zwei Probleme mit sich:

1. Diese Funktionen mögen für Start-ups oder kleine Unternehmen praktikabel sein. Sie sind jedoch nicht für die Absicherung großer, komplexer Unternehmen konzipiert und bieten oft nicht die Kontrollen und die Transparenz, die IT- und Sicherheitsteams benötigen.
2. Der DIY-Ansatz, den Mitarbeiter in der Regel verfolgen, ist ein wichtiges Beispiel für Schatten-IT, die Sicherheitsexperten den Überblick erschwert und Risiken birgt.

Was ist die Lösung? Anwendung intelligenter Privilegienkontrollen auf *alle* Identitäten.

Ihre Mitarbeiter speichern Passwörter vielleicht in leicht zugänglichen Tabellen. Aber was wäre, wenn Sie stattdessen sicherstellen könnten, dass Passwörter in einem geschützten, zentralen Vault gespeichert werden, wie Sie es bei den Anmeldedaten von IT-Administratoren tun würden? Hier sind einige Möglichkeiten, die grundlegenden Elemente Ihrer PAM-Strategie in einen umfassenden Passwortschutz zu erweitern:

- Sichere Speicherung von Passwörtern in Anmeldedaten-Vaults, unabhängig davon, ob sie in der Cloud oder in On-Premise-Vaults gehostet werden, mit End-to-End-Verschlüsselung während der Übertragung oder im Ruhezustand
- Automatischer Passwortabruf in Echtzeit aus der Cloud oder dem Vault, inspiriert von Just-in-Time-Kontrollen
- Schnelles und sicheres automatisches Ausfüllen zentral gespeicherter Passwörter in den Anmeldeformularen von Webanwendungen
- Automatisierte Generierung neuer Passwörter, die stark, komplex und einzigartig sind
- Die Möglichkeit, einzuschränken, welche Nutzer Anmeldedaten anzeigen, bearbeiten oder teilen können – und Zeitlimits festzulegen, wie lange Nutzer auf Passwörter zugreifen können, die mit ihnen geteilt wurden
- Automatische Übertragung des Eigentums an Passwörtern, wenn der Haupteigentümer eines Kontos das Unternehmen verlässt – ohne Verlust der Verwahrungskette
- Die Möglichkeit, nicht nur Passwörter, sondern auch textbasierte Elemente wie Lizenzschlüssel und PINs zu sichern

[1] Verizon DBIR Report, 2022

2. Sichern Sie die Sessions Ihrer Nutzer in Geschäftsanwendungen

Da sich Privilegien weiterentwickeln, sollten Sie beachten, dass alltägliche Nutzer mehr als nur allgemeinen Zugriff auf Apps erhalten, die sensible Ressourcen hosten – sie können während ihrer App-Sitzungen riskante Maßnahmen durchführen.

Beispielsweise müssen die Mitglieder des Finanzteams selten Sicherheitsschulungen für den Zugriff auf die Bankkonten eines Unternehmens absolvieren. Aber die meisten von ihnen erhalten ohnehin Zugang, damit sie ihre Arbeit erledigen können: Bankkontonummern einsehen, Überweisungen einreichen und vieles mehr.

> Fast die Hälfte (48 %) der Unternehmen hat nur begrenzte Möglichkeiten, Datenprotokolle einzusehen und Nutzeraktivitäten zu prüfen.[2]

Wie viel Einblick haben Sie in die Fähigkeit Ihrer Mitarbeiter, Unternehmensdaten innerhalb einer einzigen App-Sitzung zu ändern, zu löschen, herunterzuladen oder zu verteilen? Und was steht auf dem Spiel? Denken Sie an diese Fälle:

- Eine böswillige Insidertätigkeit, etwa von einem ehemaligen Angestellten eines Versicherungsunternehmens, der noch Zugang zu Finanzanträgen hat und Änderungen an den Aufzeichnungen des Versicherungsnehmers vornehmen kann
- Ein externer Bedrohungsfall, bei dem ein Angreifer Daten über geistiges Eigentum über die Virtual Collaboration App eines Herstellers findet, stiehlt und vertreibt

Beides kann in der heutigen Bedrohungslandschaft leicht passieren – 80 % der Unternehmen geben beispielsweise an, dass Endnutzer den Zugriff auf Geschäftsanwendungen missbraucht oder missbraucht haben.[3]

Das Problem: Vielen Unternehmen mangelt es an zentraler Transparenz und an Tools zur Entschärfung solcher Probleme. Die Apps selbst bieten zwar einige Steuerelemente, diese sind aber oft begrenzt und nicht mit anderen Apps verträglich.

Die Lösung besteht darin, Kontrollen, die normalerweise für die Sicherung von Sitzungen privilegierter Benutzer verwendet werden, auf die Aktivitäten der Mitarbeiter in Webanwendungen anzuwenden. Fähigkeiten, auf die man achten sollte

- Überwachen und erfassen Sie kontinuierlich die Aktivitäten eines Nutzers in bestimmten Applikationen, indem Sie einen schrittweisen Audit-Trail erstellen, in dem Aktionen wie Mausklicks oder bestimmte Tastenanschläge Screenshots und relevante Metadaten auslösen.
- Durchsuchen Sie alle aufgezeichneten Sitzungen mithilfe von Freitexteingaben und filtern Sie Sicherheitsereignisse nach Datum und Aktion. Der Sitzungs-Audit-Trail kann Kontext und eine Aufschlüsselung der vor, während und nach einem Sicherheitsereignis ergriffenen Maßnahmen liefern.
- Identifizieren Sie, wann eine Hochrisiko-Session nicht geschlossen wird und eine erneute Authentifizierung erforderlich ist, um sicherzustellen, dass die Person, die die Web-Session gestartet hat, auch diejenige ist, die die Anwendung verwendet.
- Verhindern Sie, dass Mitarbeiter bestimmte Maßnahmen wie das Herunterladen oder Kopieren von Daten durchführen, um das Risiko einer Datenausschleusung zu verringern.

[2, 3] The Hidden Gap in Web Application Security: User Sessions, CyberArk, 2022 (basierend auf einer Umfrage von Censuswide unter 900 Sicherheitsentscheidern und Führungskräften, die von CyberArk in Auftrag gegeben wurde)

3. Stärkung der Audit- und Compliance-Fähigkeiten für privilegierten Zugriff

Ihre PAM-Administratoren und Prüfer werden wahrscheinlich Folgendes bestätigen: Die Sicherstellung und der Nachweis von Compliance ist ein Problem. Zusätzlich zum Schutz des Unternehmens vor Bedrohungen verwalten IT- und Sicherheitsteams häufig einen oder mehrere der folgenden Bereiche:

- Transparenz für interne und externe Audits sicherstellen
- Erfüllung von Anforderungen in komplexen Branchen- und Regierungsvorschriften wie PCI DSS, HIPAA und SWIFT
- Nachweis der Compliance und Erstellung umfassender Berichte und/oder Analysen

156

Länder (80 % der Welt) haben Rechtsvorschriften zur Cyberkriminalität erlassen[4]

Über 130

Staaten auf der ganzen Welt haben Datenschutzgesetze erlassen[5]

Die Arbeit, die mit der Einhaltung von Vorschriften, der Erfüllung von Meldepflichten und der Vermeidung von Strafen verbunden ist, nimmt zu. Gleichzeitig sind die Risiken eines unkontrollierten Zugriffs, verwaister Konten und des Verschleierns von Privilegien weitreichend. Denken Sie nicht nur an die Auswirkungen eines Verstoßes selbst, sondern auch daran, wie die Nichteinhaltung von Vorschriften Ihren Betrieb beeinträchtigen kann.

Die Gesamtkosten für Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union sind auf fast 3,1 Mrd. Euro gestiegen, mehr als doppelt so hoch wie der Wert der 2021 verhängten Geldbußen.[6]

Wie erhalten Sie die Transparenz und Kontrolle, die Sie benötigen? Diese Frage bezieht sich auf eine Reihe von Anliegen, darunter:

- Die Berechtigungen, die Mitarbeiter haben, müssen risikoreiche administrative Aufgaben ausführen.
- Die Berechtigungen, die Ihre privilegierten Nutzer haben, um auf Safes und privilegierte Konten zuzugreifen.
- Die Berechtigungen und IAM-Berechtigungen, die Ihre Entwickler und Operations Teams in Cloud-Umgebungen haben.

Hier sind einige Best Practices zur Stärkung der Compliance- und Audit-Fähigkeiten:

- Schaffen Sie eine einheitliche Übersicht darüber, wer welche Rechte und Berechtigungen für welche Ressourcen hat, mit Funktionen zum Ermitteln, Anpassen, Zertifizieren und Entziehen des Zugriffs.
- Integrieren Sie Zugriffszertifizierungsprozesse in Ihr PAM-Programm und erfahren Sie kontinuierlich, wer Zugriff auf welche Safes und privilegierten Konten im gesamten Unternehmen hat.
- Automatisieren Sie Verwaltungsprozesse, um Prüfungen und Abgleiche sicherzustellen – zum Beispiel die kontinuierliche Durchsetzung der geringsten Privilegien durch Überprüfungen und Zertifizierungen, die für wiederkehrende Termine vorgesehen sind.
- Nutzen Sie Kontextdaten über Nutzer, damit Manager Risikoeinstufungen bei Zugriffsentscheidungen berücksichtigen können.
- Befähigen Sie Ihr Team und Ihre Prüfer mit Analyse- und Berichtsfunktionen, um potenzielle Compliance-Probleme zu identifizieren, detaillierte Audit-Trails und benutzerdefinierte Berichte zu erstellen.
- Integrieren Sie Compliance-Tools in Ihr gesamtes Framework für Identity Security, um Silos zu vermeiden und die Compliance aller Identitäten, einschließlich privilegierter oder administrativer Konten, sicherzustellen.

[4] Cybercrime Legislation Worldwide, United Nations Conference on Trade and Development, 2022

[5] A Look Ahead at New Data Privacy Regulations: How Do They Compare to ISO/IEC 27701? ISACA, 2022

[6] GDPR Fines and Data Breach Survey, DLA Piper, Januar 2023

4. Automatisieren Sie komplexe Aufgaben bei der Orchestrierung von Identitätsprozessen

Viele Unternehmen werden durch manuelle, fehleranfällige Aufgaben und Prozesse bei der Verwaltung von Identitäten behindert.

Ein wichtiges Beispiel: Die manuelle Erstellung von Workflows und die Integration von Systemen erfordern oft komplexe Codierungen und Skripts. Dieser Ansatz birgt Risiken und ist nicht zukunftsfähig, da Unternehmen wachsen und mehr Anwendungen in ihre Architekturen aufnehmen. Der Code wird mit der Zeit spröde und die Aktualisierung ist kostspielig, wenn sich die Anforderungen ändern.

Sie können Funktionen des Identitätsmanagements rationalisieren, wie z. B. die Definition und Durchsetzung der einzigartigen Rollen, Verantwortlichkeiten, Zugriffsrechte und Berechtigungen Ihrer Nutzer. Der Schlüssel liegt in der Möglichkeit, automatisierte Arbeitsabläufe ohne Code zu erstellen, z. B. für:

MEHR TUN, WENIGER PROGRAMMIEREN

Einige Aufgaben, wie die Zuweisung von Zugriffsrechten für neue Mitarbeiter oder die Erstellung von PAM-Service Accounts, sind ein wichtiger Teil der Arbeit – aber ihr reines Volumen kann Teams von der Sicherung des Unternehmens ablenken.

Sie können Ihr Team mit automatisierten No-Code-Arbeitsabläufen für IT-Aufgaben und Prozesse entlasten wie:

- Erstellen von Service Accounts mit Administratorrechten und Sicherung mit Ihrem PAM-Programm.
- Verwaltung von IT-Tickets.
- Ermöglichung von skalierbarem Fulfillment in ITSM-Tools.

- Onboarding und Offboarding von Mitarbeitern und Admin-Nutzern.
- Bereitstellung und Deaktivierung des Zugriffs für Ihre Identitäten und Konten mit dem höchsten Risiko.
- Definition und Durchsetzung der individuellen Rollen, Verantwortlichkeiten, Zugriffsrechte und Berechtigungen jedes Nutzers.
- Synchronisieren von Identitätsdaten über verschiedene Anwendungen, Directory-Stores und Repositorys hinweg.

Hier ist ein Szenario, bei dem dieser Ansatz helfen kann. Wie können Sie sicherstellen, dass Nutzer, die in Ihrem Unternehmen neue Berechtigungen beantragen, in Nutzergruppen eingeteilt werden, die nicht nur für ihre Aufgaben, sondern auch für ihren Erfahrungsstand geeignet sind? Indem Sie einen automatisierten Workflow erstellen, können Sie die Ausbildungszertifikate eines Mitarbeiters mithilfe einer „Wenn-dann"-Logik bewerten. Ein Beispiel:

- Wenn sie über das entsprechende Ausbildungsniveau für den Zugriff auf und das Durchführen von Maßnahmen in einer kritischen Cloud-Umgebung verfügen, kann der Workflow sie automatisch in die richtige Nutzergruppe einordnen.
- Wenn nicht, kann der Workflow den Zugriff verweigern und eine Benachrichtigung an den Nutzer senden, in der er erklärt, warum – einschließlich einer Angabe, welche Schulung für den Zugriff auf die Gruppe erforderlich ist.

Unternehmen benötigen auch Automatisierungsfunktionen zur kontinuierlichen Erkennung und Reaktion auf Bedrohungen – dies ist unerlässlich, um mit Angriffen auf falsch bereitgestellte, überprivilegierte oder verwaiste Konten Schritt zu halten.

Stellen Sie sich einen automatisierten Workflow vor, der erkennt, wenn ein neuer SSH-Schlüssel in einer privilegierten Session erstellt wird, und Ihrem Team eine Slack-Warnung sendet.

- Mit der gleichen „Wenn-dann"-Logik wie oben beschrieben können Sie diese privilegierte Session automatisch korrigieren.
- In diesem Szenario könnte der Workflow den Zugriff des Nutzers vorübergehend aussetzen, während das Sicherheitsteam den Nutzer untersucht – oder ihn in eine vordefinierte Hochrisiko-Nutzergruppe verschieben.

Fazit:

Indem Sie sich auf die vier Bereiche konzentrieren, die wir besprochen haben, können Sie die Grundlage für den Schutz aller Arten von Identitäten schaffen, da sie Zugang zu den sensiblen Ressourcen erhalten, die Sie vor Bedrohungen schützen.

Wir möchten Ihnen mit einem ganzheitlichen Ansatz für Identity Security helfen, erfolgreich zu sein:

- Messbare Risikominderung erreichen
- Betriebseffizienz ermöglichen
- Den Anforderungen von Audits und Compliance entsprechen

Die **CyberArk Identity Security Plattform** konzentriert sich auf intelligente Privilegienkontrollen und sichert nahtlos menschliche und maschinelle Identitäten, die in Umgebungen von Hybrid- bis Multi-Cloud auf Workloads zugreifen. Des Weiteren automatisiert sie flexibel den Identitätslebenszyklus – alles mit kontinuierlicher Bedrohungserkennung und -prävention, um Zero Trust zu ermöglichen und Least-Privilege-Prinzipien durchzusetzen.

Nächste Schritte

Wenn Sie mit einem Experten von CyberArk sprechen möchten, um Ihre Geschäfts- und Sicherheitsanforderungen zu besprechen, können Sie sich an uns wenden.

VEREINBAREN SIE EIN GESPRÄCH

Um mehr über CyberArk Lösungen zu erfahren, die für die von uns besprochenen Herausforderungen entwickelt wurden, lesen Sie mehr über unsere Fähigkeiten in folgenden Bereichen:

- **Passwortverwaltung für Mitarbeiter**
- **Sicherung von Web-Sessions**
- **Automatisierung von Identitäts-Workflows**
- **Compliance und Berichterstattung**
- **Privileged Access Management**
- **CyberArk Identity Security Plattform**

CYBERARK®
The Identity Security Company