Bild: Shutterstock / Titima Ongkantong

Privileged Account Management (PAM)

Hohes Risiko: Nutzer mit privilegierten Konten

Je weitreichender die Rechte eines Nutzers, desto attraktiver ist sein Konto als Angriffsziel.

Es war der Super-GAU für die Hotelkette Marriott: Der Konzern musste Ende 2018 bekannt geben, dass ihm Daten von bis zu einer halben Milliarde Gästen gestohlen wurden. Im Fall von 327 Millionen Personen waren das Informationen wie Name, E-Mail-Adresse, Anschrift, Passnummer, Geburtsdatum und Aufenthaltszeitraum. Bei weiteren Gästen konnten Hacker auch verschlüsselte Kreditkartendaten erbeuten, zum Teil wohl inklusive der Dateien zur Entschlüsselung.

Betroffen war die Tochtermarke Starwood, zu der unter anderem Westin, Sheraton und Le Méridien gehören. Marriott hatte Starwood im Jahr 2016 gekauft – und damit auch die seit 2014 infiltrierte Datenbank des Unternehmens übernommen.

40 %
der Unternehmen setzen bei Passwörtern auf unsichere Verfahren

Quelle: CyberArk

Entscheidend an diesem Vorfall ist: An die sensiblen Kundendaten gelangten die Kriminellen über gekaperte privilegierte Accounts, die ihnen dank ihrer weitreichenden Rechte den Zugriff auf vertrauliche Informationen erlaubten.

Mit einer Lösung für Privileged Account Management beziehungsweise Privileged Access Management (PAM) wäre das nicht passiert. Sie zeichnet alle Administrator-Sitzungen auf und untersucht sie auf verdächtige Aktivitäten. Als zentrales Zugangsportal für alle privilegierten Zugriffe bietet PAM einen hohen Automatisierungsgrad beim Session- und Passwort-Management. Zudem sorgt es für die Überwachung und Kontrolle während des Zugriffs auf das Zielsystem selbst.

Besonderer Schutz notwendig

Privilegierte Benutzer-Accounts wie „Administrator“ oder „root“ weisen grundsätzlich den direkten Weg zu wertvollen Daten und zu den Kronjuwelen eines Unternehmens. IT-Teams geben über diese Zugänge Daten im Netzwerk frei, installieren Software oder überwachen wichtige Netzwerkgeräte zum Schutz vor Bedrohungen. „Privilegierte Nutzer bewegen sich im Inneren der IT-Systeme. Sie haben praktisch den Schlüssel zum Königreich und können auf sämtliche Kundendaten zugreifen oder Funktionen beeinflussen“, erläutert Pascal Jacober, Sales Manager für die DACH-Region bei Ping Identity, einem auf Identitätslösungen spezialisierten Unternehmen. „Das Problem: Diese Super-User oder Admins können auch Logs löschen und damit ihre Spuren verwischen.“

Die Schäden sind also groß, wenn Unbefugte in den Besitz administrativer Zugangsdaten gelangen. Denn dann können sie sich in unternehmenskritischen Systemen, Applikationen und Daten frei bewegen und nach Belieben schalten und walten. Deshalb müssen Unternehmen privilegierte Konten besonders sichern. Die hohe Relevanz des Themas bestätigen auch die Marktforscher von Gartner. Sie haben Privileged Access Management bereits zum zweiten Mal in Folge als wichtigstes Sicherheitsprojekt für Unternehmen eingestuft.

IAM reicht nicht

Doch warum ist es notwendig, die privilegierten Benutzerkonten mit einer speziellen Lösung zu schützen? Reicht eine klassische Lösung für Identity und Access Management (IAM) zur Verwaltung von Identitäten und deren Zugriffsrechten nicht aus?

Bild: Ping Identity

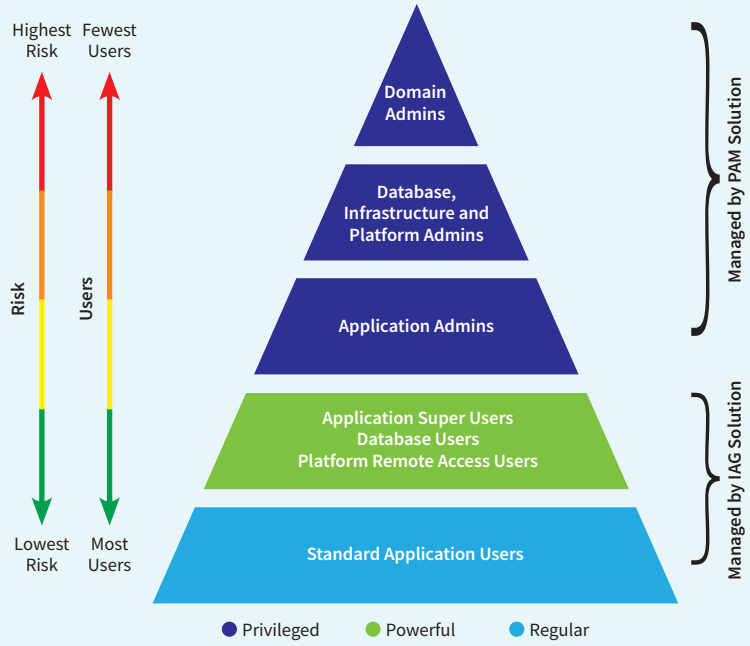
„Privilegierte Nutzer bewegen sich im Inneren der IT-Systeme. Sie haben praktisch den Schlüssel zum Königreich und können auf sämtliche Kundendaten zugreifen.“

Pascal Jacober
Sales Manager DACH
bei Ping Identity
www.pingidentity.com/de

„Die Grenzen zwischen IAM und PAM sind fließend. Manche IAM-Lösungen decken zwar auch PAM-Funktionen ab, jedoch nicht in der Tiefe und Breite, die für den Schutz privilegierter Accounts wirklich notwendig wäre“, differenziert Matthias Zacher, Senior Consulting Manager bei IDC. IAM-Lösungen decken laut Zacher den Basis-User im Business-Kontext ab (Wer darf was?) und weisen den Mitarbeitern Rechte gemäß ihrer Rolle und Position im Unternehmen zu – über den gesamten Lebenszyklus hinweg (Joiner – Mover – Leaver). „Das bleibt an der Oberfläche, da sich die normalen Nutzer auf dem System bewegen und nicht in den inneren Kern gelangen“, so Zacher weiter.

Pascal Jacober von Ping Identity bestätigt diese Sichtweise. „IAM und PAM sind zwei verschiedene Welten. IAM berechtigt Personen auf hoher Ebene ausschließlich zu den ihnen zugewiesenen Tätigkeiten und stellt die Beweisbarkeit von digitalen Identitäten sicher. PAM geht tiefer und verhindert, dass Administratoren und andere privilegierte Accounts ihre Rechte missbrauchen.“

Nutzertypen und Risikograd



An der Spitze der Nutzer-Pyramide: Domain-Administratoren können über das Active Directory auf alle Geräte und Konten im Unternehmen zugreifen. Daher besteht bei ihnen das höchste Risiko.

com! professional 1/20 Quelle: KPMG Schweiz

Jede Menge Privilegierte

Neben den internen Administratoren und Super-Usern verfügen auch externe IT-Dienstleister, Service-Provider, Entwickler oder externe Partner (zum Beispiel Zulieferer, Vertriebspartner und Kunden) über Konten, mit denen sie die Integrität von Daten, Systemen oder kompletten Prozessen beeinflussen können. Da privilegierte Accounts oft auch anonymisiert sind (Benutzername: Admin), nutzen häufig mehrere Personen denselben Account. So lässt sich nicht nachvollziehen, wer welche Aktion ausgeführt hat. Zudem gibt es in den meisten Unternehmen mehr Anwendungen, die einen privilegierten Zugriff für die Ausführung von Aufgaben benötigen, als Mitarbeiter mit privilegierten Zugriffsrechten.

„Damit sind nicht nur die Passwörter von Administratoren und anderen Super-Usern relevant für die Sicherheit, sondern auch Software- und System-Accounts, also auch in Anwendungen, Skripts oder Konfigurationsdateien gespeicherte Passwörter. Diese ▶

liegen oft im Klartext vor und werden nur selten geändert“, kritisiert Pascal Jacober.

Hinzu kommt, dass immer mehr IT-Systeme, IoT-Geräte oder auch Steuerungs-Software etwa für Industrieanlagen über offene Schnittstellen automatisiert miteinander kommunizieren, Geschäftsprozesse ausführen und Daten austauschen. Für den Zugriff auf Business-Applikationen oder geschäftskritische Daten benötigen die Maschinen oder Software-Roboter Zugangsdaten, oft sogar privilegierte Rechte. Auch diese Zugangsdaten sind für Hacker ein attraktives Ziel.

Bild: CyberArk

„Ohne eine durchgängige Privileged-Access-Management-Strategie, die zentrale Einfallstore für Angriffe schließt, bleibt ein Unternehmen hochgradig gefährdet.“

Michael Kleist
Regional Director DACH
bei CyberArk
www.cyberark.com

Das Problem ist, dass vielen Unternehmen nur unzureichend bekannt ist, in welchen IT-Bereichen sich privilegierte Accounts und Zugangsdaten überhaupt befinden. Das zeigt der „CyberArk Global Advanced Threat Landscape 2019 Report“, der schwerpunktmäßig die Themen Privileged-Access-Management-Strategien und -Lösungen im Unternehmenseinsatz untersucht. Nur 40 Prozent der Befragten nannten hier Desktops, Notebooks und mobile Geräte, 37 Prozent IoT, 36 Prozent geschäftskritische Applikationen wie ERP oder CRM und 34 Prozent IaaS- und PaaS-Umgebungen. Und nur 28 Prozent ordnen RPA privilegierte Konten zu, 22 Prozent Containern. Tatsache ist aber, dass es privilegierte Accounts und Zugangsdaten in allen genannten Bereichen gibt.

Unterschätzte Gefahren

„Diese Unkenntnis hinsichtlich des Verbreitungsgrades privilegierter Benutzerkonten und Zugangsdaten ist besorgniserregend. Nach wie vor unterschätzen Unternehmen die mit Cloud, IoT, RPA oder DevOps verbundenen Sicherheitsgefahren. Für Angreifer besteht deshalb oft ein leichtes Spiel, denn sie kennen diese Schwachstellen offenbar besser als die Unternehmen“, warnt Michael Kleist, Regional Director DACH bei CyberArk. „Ohne eine durchgängige Privileged-Access-Management-Strategie, die zentrale Einfallstore für Angriffe schließt, bleibt ein Unternehmen hochgradig gefährdet.“

Der Umfrage von CyberArk zufolge nutzen immerhin rund 60 Prozent der befragten deutschen Unternehmen eine Privileged-Access-Management-Lösung. Die restlichen 40 Prozent setzen hingegen auf Verfahren wie die Speicherung von Passwörtern in Word- oder Excel-Dokumenten auf Shared-Servern, Notebooks oder USB-Sticks. Ein regelmäßiger, manueller Wechsel der Passwörter ist damit nahezu unmöglich, da in Unternehmen oft Hunderte von Systemen existieren, auf die mit privilegierten Zugangsdaten zugegriffen wird. Zudem sind manuelle Prozesse zeitaufwendig und häufig fehlerhaft.

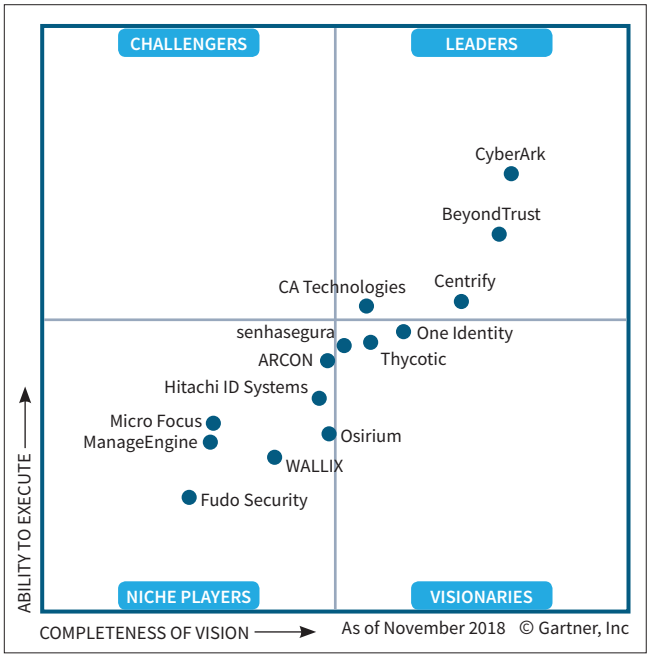
Ein weiteres interessantes Ergebnis des Threat Landscape Reports von CyberArk: Obwohl 96 Prozent der Befragten erklären, dass die IT-Infrastruktur und kritische Daten erst dann vollständig geschützt sind, wenn privilegierte Konten und Zugangsdaten gesichert sind, verfolgen viele Firmen keine durchgängige PAM-Strategie. Nur 47 Prozent haben eine entsprechende Strategie für geschäftskritische Applikationen, 42 Prozent für Cloud-Infrastrukturen. Noch schlechter sieht es beim Thema IoT aus (33 Prozent).

Risiko lokale Admin-Rechte

Darüber hinaus unterschätzen viele Unternehmen auch das Risiko von lokalen Administratorrechten auf dem PC, der immer noch das Einfallstor Nummer eins für Hacker darstellt. Jeder Rechner in einer Firma enthält standardmäßig integrierte Administratorkonten. Oft werden Hunderte von Rechnern mit einem identischen Passwort verwaltet, das nicht regelmäßig geändert wird. Zudem ist das Passwort oft auch dem Endanwender bekannt. „Jeder Nutzer mit lokalen Windows-Administratorrechten kann praktisch uneingeschränkt agieren. Er kann nicht lizenzierte Software herunterladen, jedes mögliche Programm verwenden oder Systemkonfigurationen ändern“, warnt Michael Kleist.

Brandgefährlich wird es, wenn Angreifer in den Besitz lokaler Administratorrechte gelangen. Denn dann können sie weitere Zugangsdaten entwenden und sich sukzessive durch das Firmennetz bewegen, bis sie etwa in den Besitz von Domain-Administrator-Accounts oder anderen privilegierten Benutzerkonten gelangen. Dadurch erhalten Angreifer Zugriff auf die gesamte IT-Infrastruktur.

„Firmen sollten diese lokalen Administratorrechte entziehen, um groß angelegte Cyberangriffe bereits im Keim zu ersticken“, fordert Michael Kleist. „Diese Maßnahme ist ein



Gartner Magic Quadrant for Privileged Access Management: Die wichtigsten Anbieter von PAM-Lösungen Ende 2018.

erster Schritt zur Reduzierung der potenziellen Angriffsfläche. Zudem sollten Unternehmen als Teil jeder Security-Initiative eine umfassende Lösung zum Verwalten, Überwachen und Sichern von privilegierten Konten und Zugangsdaten implementieren."

Wer braucht PAM?

Für kleinere Unternehmen oder Bürogemeinschaften lohnt sich die Anschaffung wohl eher nicht, da sie nur über wenige privilegierte Accounts verfügen. Relevanter wird das Privileged Access Management mit steigender Firmengröße. PAM ist speziell für Unternehmen ratsam, die mindestens eines der folgenden Kriterien erfüllen:

- Externe Dienstleister oder Partner wie Service-Provider, IT-Dienstleister, Entwickler, Zulieferer oder Wartungspersonal haben Zugriff auf Teile der IT-Infrastruktur
- Die IT-Infrastruktur ist komplex und hochgradig vernetzt. Es existiert ein bunter Mix aus privilegierten Benutzerkonten mit unterschiedlichen Administratorengruppen (Domäne, Anwendungen, Server), Super-Usern in den Fachabteilungen und diversen maschinellen System-Accounts
- Einsatz, Management und Überwachung von IoT-Geräten aller Art
- Hoher Grad an vernetzten und automatisierten Prozessen in Produktion, E-Commerce, Marketing und so weiter
- Viele Anwendungen oder virtuelle Maschinen laufen in der Cloud
- Vorgaben und Vorschriften müssen erfüllt werden (ISO 27001, DSGVO, BSI, PCI DSS und so weiter)
- Folgende Sicherheitslösungen sind schon im Unternehmen vorhanden: Multi-Faktor-Authentifizierung, IAM, SIEM (Security Information & Event Management) oder DLP (Data Loss Prevention).

Funktionen einer PAM-Lösung

PAM-Lösungen bieten unter anderen folgende Funktionen:

- Automatisierte Identifikation aller privilegierten User und Accounts
- Zentrales Zugangsportal verhindert direkten Remote-Zugang auf das Zielsystem
- Multi-Faktor-Authentifizierung und Single Sign-On
- Umfangreiche Workflows für Berechtigungen und Ähnliches
- Dokumentation, Kontrolle und Überwachung sämtlicher privilegierten Zugriffe
- Umfangreiche Funktionen für Analytik und Reporting (auch mit KI und maschinellem Lernen)
- Alle Aktivitäten während einer privilegierten Session sind nachvollziehbar und lassen sich auditieren
- Unautorisierte Tätigkeiten werden verhindert (zum Beispiel Start von nicht genehmigten Services oder Anwendungen, Ausführen von Skripts)
- Passwort-Management: Privilegierte Nutzer kennen keine Passwörter mehr, das Passwort wird vor jeder Session neu generiert. Passwörter können beliebig komplex bleiben, rotieren oder automatisch nach jeder Session ausgetauscht werden
- Schnittstellen zu Identity & Access Management (IAM), Data Loss Prevention (DLP), Intrusion-Prevention-Systemen (IPS) und Ähnliches
- Bereitstellung in der Cloud und On-Premise

Bild: BeyondTrust

„Eine PAM-Lösung liefert das zentrale Interface für alle Benutzer, die auditiert mit privilegierten Accounts auf kritischen Systemen mit einheitlichen Workflows und hohem Automatisierungsgrad arbeiten müssen."

Roland Schäfer
Regional Manager
BeyondTrust
www.beyondtrust.com

PAM-Module

Software für Privileged Account Management bietet umfangreiche Funktionen zum Schutz privilegierter Benutzerkonten und Zugangsdaten. Der Bedarf ist da, der Markt wächst. Laut IDC betrug das Marktvolumen für PAM-Lösungen 2019 weltweit rund 810 Millionen Dollar. Bis 2023 sollen die Umsätze jährlich im Schnitt um 13,2 Prozent steigen.

„Eine PAM-Lösung liefert das zentrale Interface für alle Benutzer, die auditiert mit privilegierten Accounts auf kritischen Systemen mit einheitlichen Workflows und einem hohen Automatisierungsgrad arbeiten müssen", erläutert Roland Schäfer, Regional Manager beim PAM-Anbieter BeyondTrust. Er unterteilt PAM in folgende drei Komponenten mit jeweils unterschiedlichem Schwerpunkt:

Privileged Session Management (PSM): Darüber werden die einzelnen Sessions mit privilegierten Accounts freigegeben, durchgeführt und überwacht. Wer hat was wann wo gemacht? „Der Remote-Zugriff auf das Zielsystem muss nicht mit Hilfe eines VPN erfolgen, es kann ebenso über einen verschlüsselten https-Tunnel gearbeitet werden. Das Passwort wird nach jeder Session neu generiert und ist dem privilegierten Nutzer unbekannt", so Schäfer. Zentral ist hier auch eine Multi-Faktor-Authentifizierung.

Privileged Identity Management (PIM): Dieses Modul weist regulären Usern automatisiert den privilegierten Account zur Nutzung zu, der für sie basierend auf einer Policy freigegeben wurde. Das gewährleistet, dass nur tatsächlich befugte Personen oder System-Accounts bestimmte Aktionen ausführen.

Privileged Elevation and Delegation Management (PEDM): Mit PEDM lassen sich Policies und Sicherheitsregeln einrichten, die den Aktionsradius von normalen Benutzern, Admins und anderen Super-Usern deutlich einschränken, ohne die Produktivität zu beeinflussen. Auf diese Weise ist es möglich, lokale Administratorrechte im gesamten Unternehmen zu eliminieren. „Über Agenten auf seinem PC erhält der Benut- ▶

zer dann seine Rechte isoliert lediglich für die Applikation, die er gerade für seine Arbeit benötigt", erläutert Roland Schäfer. PAM-Lösungen begleiten grundsätzlich den kompletten Aktionsradius einer privilegierten Identität in jedem Einsatzbereich. Die einzelnen Schritte sind Identifikation, Authentifizierung, Autorisierung, der Zugriff selbst, anschließend Reporting für Transparenz, Auditierung und Governance.

Interview

„Das PAM-Konzept muss zur Sicherheitsstrategie passen"

David Mayer ist Spezialist im Bereich IT-Advisory/Cybersecurity beim österreichischen Ableger der Unternehmensberatung KPMG. Im Interview erklärt er, warum Unternehmen eine Lösung für Privileged Account Management (PAM) brauchen und worauf sie bei der Implementierung achten sollten.

Bild: KPMG

David Mayer

Senior Manager für IT-Advisory/Cybersecurity bei KPMG Österreich
www.kpmg.at

com! professional: *Zur Verwaltung von Identitäten und deren Zugriffsrechten gibt es viele Produkte für Identity und Access Management (IAM). Warum reicht eine IAM-Lösung für die Verwaltung privilegierter Benutzerkonten nicht aus?*

David Mayer: Die Grenzen zwischen IAM und Privileged Account Management (PAM) sind fließend. IAM verwaltet alle Business-Nutzer auf hoher Ebene und weist ihnen entsprechend ihrer Rolle im Unternehmen spezifische Zugriffsrechte zu. Das Thema privilegierte Accounts decken manche IAM-Lösungen derzeit nur teilweise ab. Privilegierte Konten müssen besonders gesichert werden, da Unbefugte auf die wertvollsten Daten im Unternehmen zugreifen können, wenn sie an administrative Zugangsdaten gelangen.

PAM-Lösungen gehen viel tiefer und bieten etwa Funktionen für das Management privilegierter Sessions oder die Freischaltung und Überwachung von Konten bei der dynamischen Passwort-Freigabe für privilegierte Zugriffe.

Privileged Account Management funktioniert aber nur im Rahmen einer umfassenden Sicherheitsstrategie, die umfangreiche technische Maßnahmen und auch Themen wie Security Awareness umfasst.

com! professional: *Welche Firmen brauchen eine PAM-Lösung? Hängt das von der Größe ab?*

Mayer: Ein Admin-Konto ist wegen seiner tiefen Zugriffsrechte grundsätzlich für jeden Angreifer attraktiv, unabhängig von Branche oder Größe des Unternehmens. Die erste Frage lautet: Wie definieren Sie privilegiert? Das bedeutet für jeden etwas anderes. Bei IT- oder zum Beispiel Industrie-Unternehmen kann das der Administrator der Windows-Domäne sein, der über das Active Directory auf alle Geräte und Konten im Unternehmen zugreifen kann. Andere Firmen verstehen darunter jedes Admin-Konto, über das sie interaktiv einen Server betreuen können, sei es Windows, Linux oder Unix. In den Fachabteilungen gibt es auch den SAP-Admin, einen Key User mit vielen Berechtigungen, der nicht der IT zugeordnet ist und daher in vielen PAM-Konzepten nicht mitgedacht wird.

com! professional: *Wie sieht es mit externen IT-Dienstleistern oder technischen Accounts wie Maschinen oder IoT-Geräten aus?*

Mayer: Natürlich haben auch IT-Dienstleister oder Servicetechniker meist aus der Ferne Zugriff auf privilegierte Konten. Firmen sollten diesen Remote-Zugang nur auf Anfrage freigeben und nicht permanent aktiv halten. Über eine PAM-Lösung lässt sich immer nachvollziehen, wer für das Konto verantwortlich ist, wann es freigeschaltet wurde und wer unter diesem Konto was gemacht hat. Dank dieser Informationen bestehen Firmen auch Compliance-Audits.

Mit einer PAM-Software lassen sich auch privilegierte Benutzer von Maschinen oder IoT-Geräten verwalten. Diese sind über Schnittstellen mit verschiedenen Systemen verbunden und laufen oft im privilegierten Umfeld. Dazu gehören beispielsweise technische Service-Accounts für Datenbanken oder automatisierte Service-Accounts, die Daten-Updates oder Batch-Jobs durchführen. Hier werden Passwörter oft jahrelang nicht verändert.

com! professional: *Wie viele privilegierte Accounts gibt es erfahrungsgemäß in Unternehmen?*

Mayer: Das hängt von der Definition der privilegierten Accounts ab, von der Branche und zum Teil auch von der Unternehmensgröße. Der Anteil der privilegierten Nutzer liegt häufig bei etwa bis zu 10 Prozent und ist immer im Verhältnis zu anderen Variablen zu sehen, etwa zur gesamten IT-Abteilung oder den Applikationsbetreuern in den Fachabteilungen. Letztere agieren oft seit Jahren mit privilegierten Rechten im System und bewegen sich in der Schatten-IT. Mit einer PAM-Lösung fallen sie nicht mehr durch das Raster.

com! professional: *Worauf müssen Firmen bei der Auswahl oder Implementierung einer PAM-Lösung besonders achten?*

Mayer: Vor jedem technischen PAM-Konzept und der Auswahl der Hersteller sollten Unternehmen auf Basis der folgenden fünf W-Fragen vorgehen: Wer ist Administrator mit privilegierten Zugriffsrechten? Wann benötigt diese Person Zugriff? Wo befindet sich die Person beim Zugriff? Erfolgt die Einwahl in das System

Hohe Komplexität

PAM kann schnell komplex werden, wenn in einem Unternehmen beispielsweise mehrere Tausend privilegierte Konten unterschiedlichster Art existieren, sei es für Admins, Super-User in Fachabteilungen, externe Dienstleister, System-Accounts oder IoT-Geräte. Dann geht es um Geschwindigkeit, wenn die Passwörter bei jeder Session neu generiert werden oder schnell rollieren sollen. Verschiedene Module ▶

etwa vom Ausland aus oder von einem anderen Ort als üblich, sollten bei der Authentifizierung zusätzliche Faktoren zum Einsatz kommen, weil das Verhalten vom üblichen Muster abweicht. Warum oder zu welchem Zweck greift die Person auf das Konto zu? Worauf oder auf welche Ressourcen erfolgt der Zugriff?

com! professional: *Wo liegen die Grenzen? Welche Herausforderungen gibt es?*

Mayer: Das PAM-Konzept muss grundsätzlich zur gesamten Sicherheitsstrategie und sicherheitstechnischen Architektur des Unternehmens passen. Und Firmen sollten die erwähnten W-Fragen beantworten und die Zugriffsrechte definieren. Bei komplexen Cloud-Infrastrukturen und Wachstum kann es hier durchaus schwierig sein, am Ball zu bleiben. Zudem sollten Firmen sich mit ihrer PAM-Lösung tatsächlich auf den Schutz ihrer Kronjuwelen konzentrieren, also ihr geistiges Eigentum, Finanzdaten oder Kundendaten. Über eine Business-Impact-Analyse finden sie die wirklich wertvollen Daten heraus und vermeiden, „unnötige“ Anwendungen an das PAM anzubinden.

com! professional: *Das heißt: Man sollte die PAM-Lösung nicht zu sehr ausdehnen?*

Mayer: Firmen sollten den Prozess klar definieren und sich beim Proof of Concept (PoC) zunächst auf einige wichtige Funktionen fokussieren, die technisch gut überlegt sind. Dazu gehört beispielsweise der Schutz der Service-Accounts durch rollierende Passwörter oder die Überwachung von interaktiven privilegierten Sessions etwa beim Remote-Zugriff auf Server für das Einspielen von Patches. Sind diese grundlegenden Funktionen implementiert, kann die IT das PAM-System entsprechend den Risiken weiter ausbauen

> **„Der Anteil der privilegierten Nutzer liegt häufig bei bis zu 10 Prozent.“**

und eher fortgeschrittene Funktionen wie die verhaltensbasierte Analyse ergänzen. Bei guter Vorbereitung dauert es etwa zwei bis drei Monate, bis ein PoC läuft und die Anwendungen angebunden und getestet sind. Die Komplexität ergibt sich aus der Anzahl der privilegierten Accounts und Anwendungen, dem Einsatz von Cloud-Systemen oder der Vielfalt an heterogenen Systemen mit Windows-Geräten, Linux-Servern oder Mainframes.

com! professional: *Mit welchen Maßnahmen lassen sich privilegierte Konten schützen?*

Mayer: Das beste Admin-Konto ist per Default deaktiviert und wird nur dann aktiviert, wenn man es wirklich braucht. Auch die Passwörter werden bei jeder Aktivierung neu vergeben und verschlüsselt verwaltet. Die Administratoren brauchen die sensiblen Passwörter nicht zu kennen.

Auch dem externen Dienstleister sind die Passwörter nicht bekannt, wenn er sich über die Fernwartung einwählt und per PAM-Lösung den Benutzer freischaltet. Da er damit keine Passwörter

> **„Bei guter Vorbereitung dauert es zwei bis drei Monate, bis ein Proof of Concept läuft.“**

von privilegierten Accounts weitergeben kann, sinkt das Risiko von Missbrauchsfällen deutlich. Weitere Maßnahmen sind Multi-Faktor-Authentifizierung und Single Sign-On.

Ein zentrales Feature ist das Session Management mit Überwachung und Monitoring aller Aktivitäten, die über die PAM-Lösung erfolgen: Wer macht was wann, warum und wie? Beim Erkennen von Verhaltensmustern und Abweichungen kommt mittlerweile maschinelles Lernen zum Einsatz.

Ein wichtiger Grund für das Monitoring sind Compliance-Vorschriften wie die europäische Datenschutz-Grundverordnung oder Audits gemäß der ISO 27001 zum Aufbau eines Managementsystems für Informationssicherheit. Sie erfordern die Dokumentation von Aktivitäten.

com! professional: *Welche Trends außer maschinellem Lernen sehen Sie beim Thema PAM noch?*

Mayer: Der Markt für Privileged Account Management konsolidiert sich und ist in Bewegung. Ich denke, dass auch künftig die Anbieter von IAM-Lösungen und von PAM-Systemen wegen der jeweils hohen Komplexität auf beiden Feldern parallel nebeneinander existieren werden. Möglicherweise werden größere IAM-Hersteller künftig auch PAM-Module in ihre Produkte integrieren. Für das Thema Verwaltung der privilegierten Benutzerkonten ist aber ein noch umfassenderes Know-how erforderlich.

Ein wichtiges Thema ist Cloud-Computing. Die meisten PAM-Anwendungen sind mittlerweile als On-Premise- und als Cloud-Lösung erhältlich. Zudem ist davon auszugehen, dass viele Provider von Cloud-Services künftig selbst Schnittstellen für die Integration in PAM-Lösungen anbieten. Aktuell verfügen viele PAM-Produkte zwar über Schnittstellen, allerdings ist dafür zusätzliche Programmierarbeit notwendig. Wenn die Cloud-Provider aber mittelfristig Standard-Schnittstellen für PAM bieten, entfällt künftig der Aufwand für den Bau von Konnektoren.

für Privilegien in unterschiedlichen Bereichen, etwa für Netzwerke, Datenbanken oder in der industriellen Operational Technology, erhöhen die Komplexität weiter.

„Privileged Account Management ist mehr ein Prozess-Thema als ein technologisches Thema. Firmen können hier viel falsch machen. Sie müssen wissen, welche privilegierten Accounts über welche Zugriffsrechte auf welche Systeme verfügen, und im Vorfeld definieren, was sie mit der PAM-Lösung erreichen wollen", meint Matthias Zacher von IDC. „Zudem gilt es abzuwägen, wie eng sie die Schraube drehen wollen und inwieweit sie Tätigkeiten sowie Geschäfts- und IT-Prozesse mit PAM einschränken." Benutzerfreundlichkeit und Benutzerakzeptanz sind hier kritische Faktoren.

Bild: IDC

„Manche IAM-Lösungen decken auch PAM-Funktionen ab, aber nicht in der Tiefe und Breite, die für den Schutz privilegierter Accounts wirklich notwendig wäre."

Matthias Zacher
Senior Consulting Manager bei IDC
www.idc.com/de

Fazit & Ausblick

Laut Matthias Zacher sollte PAM gut mit anderen Security-Lösungen wie SIEM, DLP oder IPS (Intrusion Prevention Systems) und Schwachstellen-Management integriert sein. „Firmen brauchen Regeln für eine schnelle und idealerweise automatisierte Reaktion, wenn externe oder unbefugte Personen auf ein privilegiertes Benutzerkonto zugreifen wollen. PAM konzentriert sich auf den Zugriff, während SIEM, DLP und IPS die breite Sicht auf die Infrastruktur eines Unternehmens bieten. PAM ist ein fortlaufender Prozess." Alle von com! professional befragten Experten sind sich zudem darin einig, dass KI und ML künftig insbesondere beim Monitoring sowie bei der Analyse und Korrelation der Daten der einzelnen privilegierten Sessions eine große Rolle spielen werden. Ein wichtiger Trend ist auch, dass die Zahl der Maschinen-Accounts weiter zunehmen wird.

Privilegierte Benutzerkonten, etwa von Admins oder maschinellen Accounts, die den Zugriff auf Datenbanken, Maschinen oder Cloud-Anwendungen ermöglichen, sind im Geschäftsalltag unerlässlich. Allerdings stellen sie wegen ihrer weitreichenden Befugnisse ein attraktives Ziel für Cyberkriminelle oder Hacker dar. Wer die Zugangsdaten eines privilegierten Accounts erbeutet, kann auf unternehmenskritische Daten zugreifen oder die IT-Infrastruktur manipulieren und kontrollieren. Daher sollten Firmen diese Konten besonders schützen. Eine IAM-Lösung reicht dafür nicht aus. Firmen sollten das System für das Identitätsmanagement, falls vorhanden, um eine PAM-Lösung zum Schutz der privilegierten Benutzerkonten ergänzen. Diese bietet neben anderen Schutzfunktionen eine automatisierte Übersicht über die Anzahl an privilegierten Accounts, dokumentiert und überwacht die Zugriffe und gewährleistet die effektive Verwaltung von Passwörtern. ■

Jürgen Mauerer/js
js@com-professional.de

Wichtige Anbieter von PAM-Lösungen (Auswahl)

Anbieter	Produkt	Beschreibung
BeyondTrust www.beyondtrust.com	BeyondTrust Privilege Management	Modulare Plattform mit allen möglichen PAM-Funktionen (u. a. Passwortverwaltung, Multi-Faktor-Authentifizierung); Session Management ersetzt VPN durch https-Tunnel
Broadcom www.broadcom.com	Layer7 Privileged Access Management (Vorher CA PAM)	Modulare PAM-Lösung, die alle Administrator-Sitzungen aufzeichnet und auf potenziell verdächtige Aktivitäten überwacht
Centrify www.centrify.com	Zero Trust Privilege	Modulare Plattform mit Komponenten für Passwortverwaltung, Authentifizierung, Monitoring, Session Management oder Threat Analytics
CyberArk www.cyberark.com	Verschiedene Lösungen für PAM	Der PAM-Marktführer bietet ein umfangreiches Portfolio an Lösungen für die Verwaltung und das Monitoring von privilegierten Benutzerkonten an, sowohl aus der Cloud als auch On-Premise. Auch maschinelle Accounts, DevOps-Umgebungen oder Container werden erfasst
Micro Focus www.microfocus.com	NetIQ Privileged Account Manager	Zu den Funktionen der PAM-Lösung gehören gesicherte Passwortarchivierung, privilegierte Kontenüberwachung von Datenbanken, die risikobasierte Kontrolle von Sitzungen privilegierter Konten sowie Audits und Berichte
One Identity www.oneidentity.com	Verschiedene Lösungen für Privileged Access Management	Deckt alle PAM-Facetten ab, von Passwort- und Zugangsverwaltung und Threat Analytics über Multi-Faktor-Authentifizierung und Unix Server Security bis hin zu umfangreichen Reporting-Funktionen
Thycotic www.thycotic.com	Thycotic Privileged Access & Password Management	Modulare PAM-Lösung aus der Cloud oder On-Premise mit Komponenten wie Secret Server, Privileged Behavior Analytics, Password Reset Server oder DevOps Secrets Vault
Wallix www.wallix.com	Wallix Bastion	PAM-Lösung aus verschiedenen Modulen, darunter ein Access- und Session-Manager, ein Passwort-Manager oder ein PEDM-Tool für Least-Privilege-Sicherheit zum Schutz von PCs und Servern