KuppingerCole Report

WHITEPAPER

von Matthias Reinwarth | März 2019

PATECCO Privileged Access Management Dienstleistungen

Der Begriff Privilege Management beschreibt eine Reihe kritischer Cyber-Sicherheitskontrollen zur Eindämmung der Risiken, die privilegierter Zugriff innerhalb eines Unternehmens mit sich bringt. Wer die Kontrolle über privilegierte Nutzer, erweiterte Zugriffsrechte und gemeinsam genutzte Konten behalten möchte, benötigt eine optimal integrierte Lösung, die Risikominimierung, klar definierte Prozesse sowie eine gut ausgeführte Implementierung bietet.

von **Matthias Reinwarth**
mr@kuppingercole.com
Februar 2019

Im Auftrag von PATECCO GmbH

Inhaltsverzeichnis

Einschlägige Forschung

Leadership Compass: Adaptive Authentication - 79011
Architecture Blueprint: Access Governance and Privilege Management - 79045
Advisory Note: How to Assure Cloud Services - 72563
Leadership Compass: Privilege Management - 72330 (Aktualisierung ausstehend)
KuppingerCole Hot Topic Area Privilege Management

1 Einleitung

Traditionell ist die Verwaltung von Identitäten und deren Zugriff auf IT-Systeme innerhalb eines Unternehmens in unterschiedliche Disziplinen aufgeteilt. Business-Anwender, die so genannten Standardnutzer, werden innerhalb des herkömmlichen Identity-and-Access-Management-Systems (IAM) verwaltet und in jüngerer Zeit mithilfe von Access-Governance- und Access-Analytics-Systemen erfasst. Der Begriff Privileged Access Management (PAM) bezeichnet Technologien, die administrative Konten verwalten, erweiterte Berechtigungen überwachen und einschränken und die Verwaltung gemeinsam genutzter Konten unterstützen. In der Vergangenheit hat sich Privilege Management aus der Verwaltung gemeinsam genutzter Konten und Passwörter entwickelt.

In den letzten Jahren hat sich das Verständnis von Privilege Management maßgeblich verändert. Verschiedene IT-Software-Hersteller haben ihre Produktpalette deutlich erweitert, während diverse Übernahmen unter anderem dazu geführt haben, dass Infrastruktur-Provider eine breitere Produktpalette offerieren und sich so von spezialisierten Nischenanbietern zu Marktführern entwickeln konnten. Innerhalb der letzten fünf bis zehn Jahre hat Privilege Management das durch IAM-, Corporate Governance- oder Security-Teams zur Verfügung angebotene Portfolio von Identitäts- und Zugriffsfunktionen ergänzt.

Warum sollte sich ein Angreifer damit zufriedengeben, den Account eines gewöhnlichen Nutzers zu übernehmen, wenn er stattdessen ganze Segmente einer IT-Infrastruktur als unrechtmäßiger Administrator übernehmen kann?

Die Verwaltung privilegierter Nutzer, bei KuppingerCole Privilege Management genannt, ist für ein Unternehmen eine wichtige Maßnahme. Ein Insider kennt sich häufig besser aus und ist mit den Prozessen und der technischen Landschaft vertrauter. Sobald sich nun ein Außenstehender Zugriff auf ein Insider-Konto verschafft, stehen ihm dieselben Möglichkeiten zum Angriff offen. Ein böswilliger Insider (oder ein gekapertes Konto) mit privilegierten Zugangsdaten kann erheblichen Schaden anrichten, zum Beispiel:

- Löschen, Ändern oder Lesen sämtlicher E-Mails und anderer Kommunikationsaufzeichnungen
- Ändern oder Einsehen von Gehaltsinformationen sämtlicher Mitarbeiter
- Weitergabe geistigen Eigentums
- Weitergabe vertraulicher Daten, einschließlich persönlicher Informationen, an Aktionäre oder Hacktivisten

Nicht nur die Bedrohungen haben sich verändert und sind größer geworden. In den letzten zehn Jahren haben sich Businessanforderungen und IT massiv weiterentwickelt. Geschäftsmodelle befinden sich im ständigen Wandel, die allgegenwärtige Digitalisierung hat Unternehmen, ihre Netzwerke und ihre Applikationsinfrastruktur komplett transformiert. Neue Infrastrukturkonzepte in der Cloud, von Infrastructure as a Service bis hin zu völlig neuen Angeboten wie Business Software as a Service, schaffen eine Vielzahl neuer administrativer Konten. Auf Mobilgeräten basierende neue Applikationen und Plattformen kreieren einerseits

neue Arbeitskonzepte und Geschäftsmodelle und stellen andererseits IAM und Privilege Management vor neue Herausforderungen.

In Zeiten zunehmender Cyberangriffe und Datenschutzverletzungen ist es offensichtlich, dass diese Vorfälle mit privilegierten Nutzerkonten in Zusammenhang stehen. Darüber hinaus lassen Analysen der jüngsten sicherheitsrelevanten Ereignisse darauf schließen, dass großangelegter Datendiebstahl häufig durch Nutzer mit erweiterten Privilegien, typischerweise administrative Nutzer, verursacht wird. Es überrascht also nicht, dass Zugriffsmanagement nicht nur ein Thema für Führungskräfte (CIOs und CISOs) ist, sondern immer mehr zu einem Bereich wird, mit dem sich auch Auditoren und Regulatoren auseinandersetzen müssen. Positiv lässt sich feststellen, dass sich Privilege Management (und damit Investitionen in diesem Bereich) überaus günstig auf die gesamte Risikominimierung auswirkt im Vergleich zu anderen Arten von IT- und Sicherheits-technologien.

Der Begriff Privilege Management beschreibt eine Reihe kritischer Cyber-Sicherheitskontrollen zur Eindämmung der Risiken, die der privilegierte Zugriff innerhalb eines Unternehmens mit sich bringt.

Dieses Whitepaper beschreibt, wie Privilege Access Management in eine umfangreiche IAM-Architektur integriert werden kann. Es bietet einen Überblick über die wesentlichen Komponenten, aktuellen Erweiterungsoptionen und Trends in diesem Bereich. Der letzte Abschnitt zeigt die Bedeutung einer angemessenen Umsetzung von Privileged Access Management in einem Anwenderunternehmen am Beispiel der Beratertätigkeit von PATECCO und dessen Leistungsspektrum auf.

2 Kernpunkte

- KuppingerCole definiert Privileged Access Management
- Beschreibung der Integration von Privileged Access Management in eine Gesamt-IAM-Architektur
- Identifizierung zentraler Kundenherausforderungen, die Privilege Access Management in Informationssicherheitsunternehmen zu einem Schwerpunktthema gemacht haben
- Beschreibung gemeinsamer Merkmale von Privileged-Access-Management-Produkten
- Betrachtung der organisatorischen Voraussetzungen für einen erfolgreichen Einsatz von Privilege Access Management
- Überblick über die von PATECCO angebotenen Dienstleistungen zur Durchführung erfolgreicher Privilege-Access-Management-Projekte und die Bereitstellung nachhaltiger PAM-Lösungen

3 Privileged Access Management aus der Architekturperspektive

Privileged-Access-Management-Tools sind so konzipiert, dass sie Szenarien wie die gemeinsame Nutzung von Konten, die Überwachung privilegierter Aktivitäten und die kontrollierte Erweiterung von Zugriffsprivilegien ermöglichen. Eine konsequente Implementierung zur Erfüllung dieser Anforderungen muss sich in einer entsprechenden Architektur niederschlagen, die wiederum einen angemessenen Anteil innerhalb einer Gesamt-IAM-Architektur ausmachen muss.

Die KuppingerCole IAM/IAG Reference Architecture bietet eine umfangreiche und sich ständig weiterentwickelnde Grundlage zur Ableitung und Implementierung von standardisierten und zugleich angemessen individualisierten, in eine Gesamtunternehmensarchitektur integrierten IAM/IAG-Architekturen. Sie basiert auf einer grundlegenden architektonischen Unterscheidung zwischen vier übergeordneten Funktionsbereichen.

Diese sind:

- Administration
- Audit & Analytik
- Authentifizierung
- Authorisation

Davon ausgehend wird einem oder mehreren dieser Bereiche eine Auswahl separater IAM-Architekturkomponenten zugewiesen. So entsteht eine vollständige, verständliche und flexible Gesamtarchitektur.

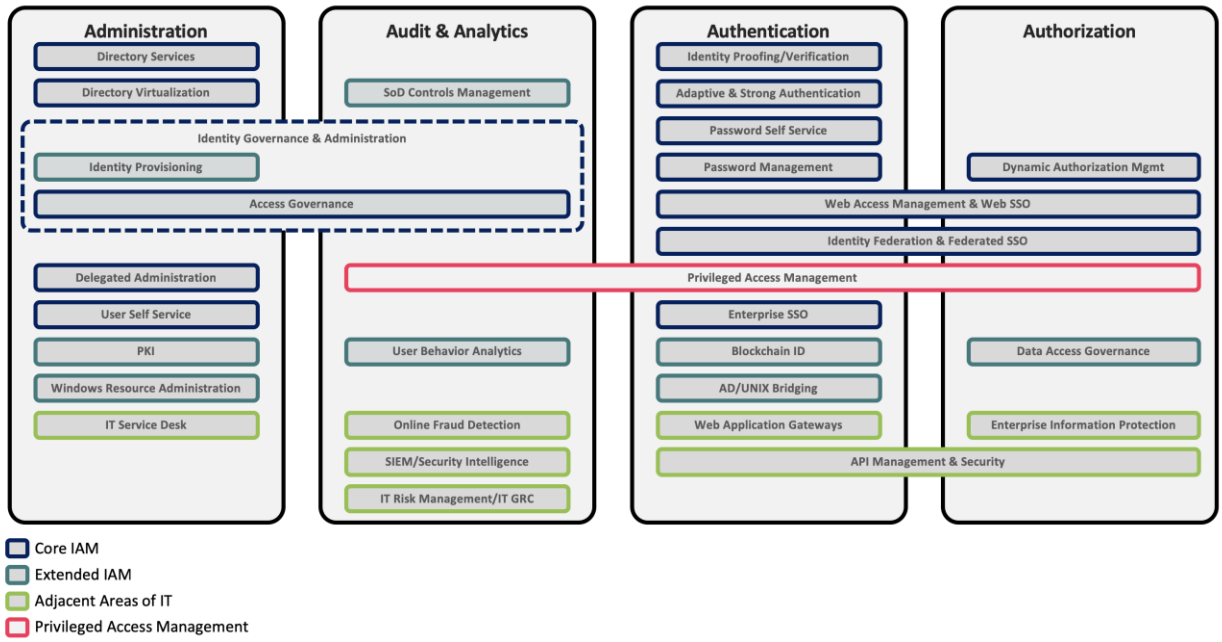

Abb. 1: Privileged Access Management als Teil der KuppingerCole IAM/IAG Reference Architecture

Die Komponenten werden als

- unverzichtbar (Core IAM)
- komplementär (Extended IAM) oder
- peripher (Adjacent Areas of IT) eingestuft

wobei von einer effektiven konzeptionellen Verankerung der IAM- / IAG-Architektur in einer Gesamtunternehmensarchitektur ausgegangen wird.

Die vorgegebene Struktur, die Lokalisierung der Bausteine innerhalb der Funktionsbereiche und die Kategorisierung innerhalb einer bestehenden Unternehmensarchitekturlandschaft liefern sowohl eine konzeptionelle Leitlinie als auch den erforderlichen Grad von Freiheit bei Entwurf, Verifizierung und Bewertung von System- und Prozesslandschaften für IAM / IAG und damit verbundene Architekturbereiche.

PAM hat sich zu einer der wichtigsten IAM-Technologien entwickelt, die eine direkte Bedeutung für und Auswirkung auf das Cybersicherheitsprogramm eines Unternehmens haben.

In den letzten Jahren hat sich Privileged Access Management zu einem der wichtigsten Cybersecurity-Bereiche innerhalb des Identity and Access Managements bei der Identifizierung, Sicherung und Verwaltung von privilegierten Zugangsdaten in der Gesamt-IT-Umgebung von Unternehmen entwickelt. Früher als technologische Option zur Optimierung der administrativen Effizienz mithilfe der Verwaltung von Passwörtern und anderen vertraulichen Informationen betrachtet, versteht man heute unter PAM eine Reihe maßgeblicher Technologien zur Verhinderung von Sicherheitsverstößen und des Diebstahls von Zugangsdaten. Inzwischen sind sich Security-and-Risk-Management-Verantwortliche ebenso wie die Leiter von Infrastructure-and-Operation-Abteilungen (ISO) in sämtlichen Branchen der Bedeutung von PAM für zahlreiche Sicherheits- und Betriebsvorteile bewusst.

Dies spiegelt sich deutlich in der Tatsache wider, dass Privilege Access Management drei der vier übergeordneten Funktionsbereiche abdecken. Die PAM-Funktionen stehen in direktem Zusammenhang mit den Bereichen “Audit & Analytics”, “Authentication” und “Authorization”. Selbstverständlich hängt PAM gleichzeitig stark von den administrativen Funktionen ab, dem vierten übergeordneten Funktionsbereich. Diese Funktionen und Services sind typischerweise außerhalb der Kern-PAM-Funktionen angesiedelt und werden von “Identity Provisioning”, “Access Governance”, “User Self Service” und “Delegated Administration” für privilegierte Konten und deren Berechtigungen abgedeckt.

In diesem Zusammenhang sollte unbedingt klar definiert werden, welche Module welche Aufgaben übernehmen: Die Bereitstellung von einmaligen und vertrauenswürdigen Identitäten im IAM ist eine unerlässliche Grundlage. Diese Funktion wird jedoch vom Directory-Services-Baustein als Teil der Gesamt-

Referenzarchitektur bereitgestellt. Den Identitäten werden in einem Access-Management-System von Verantwortlichen sowie durch Lifecycle-Prozesse Genehmigungen zugeteilt. Gleichzeitig werden erweiterte Privilegien gewährt, über separate Privilege-Management-Schnittstellen verwaltet und können mit eigenständigen Identitäten verbunden werden.

Zu diesem Zweck sind eindeutig definierte technische Schnittstellen erforderlich, die Informationen über die vom Privilege Management zugeteilten Genehmigungen mit übergeordneten IAM-Systemen abgleichen. Daher ist es notwendig, Informationen über privilegierte Nutzerkonten-, Gruppen- und Zugangsdaten aus dem Privilege-Management-System zu sammeln oder direkten Zugriff darauf zu haben.

Idealerweise kann die Privilege-Management-Infrastruktur als hoch spezialisiertes Zielsystem für die Access-Management-and-Access-Governance-Infrastruktur betrachtet werden, die ihm ermöglicht, erweiterte Zugriffsrechte auf IT-Systeme und von IT-Systemen zu gewähren, neu zu bestätigen und aufzuheben.

4 Privileged-Access-Management-Lösung: Funktionalitäten und Kompetenzen

Der Begriff Privilege Management beschreibt eine Reihe kritischer Cyber-Sicherheitskontrollen zur Eindämmung der Risiken, die der privilegierte Zugriff innerhalb eines Unternehmens mit sich bringt. Diese privilegierten Konten erlauben ihren Nutzern unbegrenzten und häufig unkontrollierten Zugriff auf die IT-Assets eines Unternehmens.

Dies verletzt nicht nur fundamentale Sicherheitsgrundsätze wie das Least-Privilege-Prinzip, sondern schränkt auch in erheblicher Weise die Möglichkeit ein, individuelle Verantwortlichkeiten für privilegierte Aktivitäten zuzuordnen. Privilegierte Konten stellen aufgrund ihres erweiterten Zugriffs auf sensible Daten und kritische Vorgänge eine signifikante Bedrohung für den gesamten Sicherheitsstatus eines Unternehmens dar. Aus diesem Grund sollten Sicherheitsverantwortliche ein größeres Augenmerk auf die Identifizierung und Verwaltung dieser Konten legen, um das Sicherheitsrisiko durch deren Missbrauch zu minimieren.

Privileged-Access-Management-Tools sind auf derartige Szenarien ausgelegt und bieten spezialisierte Verfahren und Prozesskontrollen, um die digitalen Assets eines Unternehmens durch Verhinderung des Missbrauchs von privilegiertem Zugriff besser zu schützen.

4.1 Grundlegende und erweiterte PAM-Funktionen

Die Kernfunktionen von PAM-Tools beinhalten

- Passwortgeschützte Anmeldeverfahren
  Technologie und Prozesse für eine sichere, geprüfte Speicherung von und den Zugriff auf Passwörter sowie ähnliches kryptographisches Schlüsselmaterial.
- Passwortwechsel
  Die Verkürzung der Lebensdauer eines Passworts durch häufige Wechsel, um das Gefährdungsrisiko insbesondere bei kritischen Konten zu reduzieren.

Erweiterte Funktionen wie privilegierte Nutzeranalysen, risikobasierte Sitzungsüberwachung und erweiterter Angriffsschutz werden zum neuen Standard. Angesichts einer immer größeren Angriffsoberfläche und einer von Jahr zu Jahr zunehmenden Anzahl von immer ausgefeilteren Angriffen ist eine integrierte und umfassendere PAM-Lösung notwendig – eine, die ungewöhnliches Verhalten automatisch erkennt und eine automatisierte Schadensbegrenzung einleitet.

Zu den zentralen Herausforderungen, welche den Bedarf an einer Privileged-Access-Verwaltung vorantreiben, zählen:

- Missbrauch gemeinsam genutzter Zugangsdaten
- Missbrauch erweiterter Privilegien durch nicht autorisierte Nutzer
- Hijacking von privilegierten Berechtigungsnachweisen durch Cyberkriminelle
- Missbrauch von Privilegien in Drittsystemen sowie
- Versehentlicher Missbrauch von erweiterten Privilegien durch Nutzer

PAM ist zu einer wichtigen digitalen Risikomanagementdisziplin geworden und unterstützt Sicherheitsverantwortliche durch Kontrollen, die für die Absicherung des privilegierten Zugriffs auf Daten, Anwendungen und Infrastruktur unerlässlich sind.

Darüber hinaus gibt es im Bereich des privilegierten Zugriffs verschiedene weitere Betriebs-, Steuerungs- und regulatorische Anforderungen:

- Auffinden von gemeinsam genutzten Konten sowie Software- und Servicekonten in der gesamten IT-Infrastruktur
- Identifizierung und lückenlose Verfolgung der Inhaberschaft privilegierter Konten während ihres gesamten Lebenszyklus
- Einführung und Verwaltung privilegierter Sitzungen, um Systeme zur Steigerung der operativen Effizienz der Administratoren anzusteuern
- Prüfung, Erfassung und Überwachung von privilegierten Aktivitäten zur Einhaltung gesetzlicher Bestimmungen
- Verwaltung und Überwachung des administrativen Zugriffs auf interne IT-Systeme durch Anbieter von IT-Outsourcing und Managed Services sowie
- Verwaltung und Überwachung des privilegierten Zugriffs auf Cloud-Infrastruktur und Applikationen durch Businessanwender und IT-Administratoren

4.2 Bausteine des PAM-Einsatzes

Folgende Technologien und Werkzeuge sind wichtige Bausteine der aktuellen Privileged-Access-Management-Lösungen. Basierend auf individuellen Anforderungen und den ausgewählten Anbietern bilden sie typischerweise die Grundlage einer praxisgerechten PAM-Architektur.

Shared Account Password Management (SAPM): Diese Kennwortverwaltung für üblicherweise gemeinsam genutzte Konten bietet Technologien zur sicheren Verwaltung von privilegierten Zugangsdaten, einschließlich System-, Service- oder Applikationskonten. SAPM-Produkte bestehen im Kern aus einem verschlüsselten und verstärkten Passwortsafe zur Speicherung von Passwörtern, Schlüsseln und anderen privilegierten Zugangsdaten zugunsten einer kontrollierten, geprüften und richtlinienbasierten Freigabe und Aktualisierung.

Privileged Session Management (PSM): Privileged Session Management liefert die Technologie zur Einrichtung einer privilegierten Sitzung um Systeme gezielt anzusteuern, einschließlich Basisauditing und der Überwachung privilegierter Aktivitäten. PSM-Tools bieten den Zielsystemen außerdem Authentifizierung, Autorisierung und Single Sign-On (SSO).

Application-to-Application Password Management (AAPM): AAPM ist eine Erweiterung der SAPM-Tools zur Verwaltung von Konten, die von Anwendungen oder Systemen zur Kommunikation mit anderen Anwendungen oder Systemen (wie Datenbanken etc.) genutzt werden. Dank der AAPM-Werkzeuge entfallen fest kodierte Zugangsdaten in Anwendungscode, Scripts und anderen Konfigurationsdateien dank eines Verfahrens (üblicherweise APIs) zur Bereitstellung von Zugangsdaten auf Anfrage.

Session Recording and Monitoring (SRM): SRM ist eine Erweiterung der PSM-Tools, die eine erweiterte Prüfung, Überwachung und Bewertung privilegierter Aktivitäten während einer privilegierten Sitzung ermöglichen, einschließlich Keystroke Logging, Videosession-Aufzeichnung, Screen-Scraping, OCR-Übersetzung und anderer Techniken zur Sitzungsüberwachung.

Controlled Privilege Elevation and Delegation Management (CPEDM): Diese Technologie steuert die kontrollierte Erweiterung und richtlinienbasierte Übertragung der Privilegien eines Nutzers auf Superuser-Privilegien zu administrativen Zwecken.

Privileged User Behavior Analytics (PUBA): PUBA verwendet Datenanalysetechniken, um – basierend auf ungewöhnlichen Verhaltensmustern im Vergleich zu etablierten Verhaltensprofilen – Bedrohungen bei administrativen Nutzern sowie Nutzergruppen und Administratorenrollen zu erkennen.

Privilege Account Discovery and Lifecycle Management (PADLM): Hier geht es um Erkennungsverfahren zur Identifizierung gemeinsamer Konten, Softwarekonten, Servicekonten und anderer unverschlüsselter/Klartext-Zugangsdaten in der gesamten IT-Infrastruktur. PADLM-Tools verfügen über Workflow-Funktionen, um die geschäftliche und technische Zugehörigkeit eines Kontos über seinen gesamten Lebenszyklus hinweg zu verfolgen, und können Veränderungen in dessen Status feststellen, um Mitteilungen und notwendige Schadensbehebungsmaßnahmen auszulösen.

Endpoint Privilege Management (EPM): EPM ermöglicht die Verwaltung von Bedrohungen im Zusammenhang mit lokalen Administratorrechten in Windows, MAC oder anderen Endpunkten. EPM-Tools beinhalten im Wesentlichen eine kontrollierte und überwachte Eskalation von Nutzerprivilegien auf Endgeräten und schließen Funktionen wie das Whitelisting von Anwendungen zum Schutz von Endgeräten

ein. Grundsätzlich stellen EPM-Lösungen per Definition in erster Linie drei unterschiedliche Technologien bereit:

a. **Anwendungskontrolle**: Damit können Unternehmen kontrollieren, welche Anwendungen für den Betrieb auf einem Endgerät freizugeben sind. Üblicherweise wird dabei ein Whitelisting von Applikationen angewendet, welches ausschließlich bewährte, im Voraus genehmigte Applikationen listet und für den Betrieb freigibt. Die Anwendungskontrolle schützt Unternehmen effektiv gegen die Probleme einer Schatten-IT.
b. **Sandboxing**: Diese Technologie arbeitet mit der isolierten Ausführung unbekannter Applikationen oder Programme, indem sie die Ressourcen begrenzt, auf die diese zugreifen können (z.B. Dateien, Register etc.). Auch unter dem Begriff Application Isolation bekannt, bietet diese Technologie einen effektiven Schutz gegen Cyberattacken, indem sie die Ausführung schädlicher Programme einschränkt und deren Gefährlichkeit begrenzt.
c. **Privilege Management:** Diese Technologie umfasst das Privilege Management für Nutzer und Anwendungen. Die Verwaltung privilegierter Nutzer besteht in der kontrollierten und überwachten Erweiterung lokaler Administrationsprivilegien. Die Verwaltung privilegierter Applikationen arbeitet mit der ausnahmen- oder richtlinienbasierten Erweiterung administrativer Rechte für die erfolgreiche Ausführung bekannter und genehmigter Anwendungen.

Privileged Access Governance (PAG): PAG gewährt wertvolle Einblicke in den Status eines privilegierten und für die Unterstützung von Entscheidungsprozessen benötigten Zugriffs und schließt Zertifizierungen für privilegierten Zugriff und Vorgaben für ein flexibles Berichtswesen und Dashboards ein.

4.3 Definition individueller PAM-Landschaften

Unabhängig von der Wahl der Werkzeuge sind die wichtigsten Aspekte beim Privilege Management nicht die technischen Fragen oder die Erfassung der Kundenanforderungen insgesamt. Der schlimmste Fehler wäre, die Probleme, die Privilege Access Management auf den Plan gerufen haben, weiterhin zu ignorieren oder zu unterschätzen. Insofern ist der erste Schritt zum Privilege Management nicht die Wahl der Werkzeuge, sondern die Erledigung der Hausaufgaben auf Unternehmensseite.

Eine reduzierte Anzahl an privilegierten Accounts, die Limitierung auf unbedingt erforderliche Zugriffsrechte und sogar die Konsolidierung von IT-Plattformen können helfen, die Gefährdung kritischer Konten zu verringern. Dies schließt die Berücksichtigung aller regulatorischen und rechtlichen Anforderungen ein.

Im Umkehrschluss lässt die Kritikalität privilegierter Konten, welche eine PAM-Lösung erfordert, die entsprechende Ausführung eines derart wichtigen und sicherheitsrelevanten Projekts unweigerlich zu einer hochkritischen Aufgabe werden.

5 PATECCO-Dienstleistungen für Privileged-Access-Management-Lösungen

Der Zugriff auf die Ressourcen und Kompetenzen eines erfahrenen Serviceanbieters kann die Implementierung eines PAM-Projekts und seine Integration in die IT-Infrastruktur eines Unternehmens beschleunigen. Mithilfe von Best Practices und unter Anwendung bewährter Projektabläufe können klar definierte Projektziele schnell erreicht werden.

PATECCO ist ein privates Unternehmen für Serviceleistungen auf den Gebieten Entwicklung, Implementierung und Support von Identity & Access Management-Lösungen. PATECCO hat seinen Unternehmenssitz in Herne und Bochum, Deutschland sowie eine Niederlassung in Sofia, Bulgarien. Im Bereich IAM verfügt PATECCO über mehr als zwanzig Jahre Erfahrung. Die angebotenen Leistungen gehen weit über die traditionellen On-Premises-Lösungen für IAM hinaus und umfassen Cloud-Zugriffssteuerung, Zugriffskontrolle, RBAC, SIEM und PKI. Darüber hinaus bietet PATECCO Managed Services für IAM-Lösungen an, wobei auch PAM Bestandteil der Managed Services ist.

Privileged Access Management als wesentlicher Teil von IAM sowie als separates Angebot gehört zum Unternehmensportfolio mit Mehrwertdienstleistungen für Kunden unterschiedlicher Größe aus Branchen wie Banken, Versicherungen, Chemie, Pharma- und Versorgungsunternehmen. PATECCO hat bereits zahlreiche umfangreiche PAM-Projekte in führenden Unternehmen des Finanz- und Telekommunikationssektors erfolgreich ausgeführt. Aktuell werden die Dienstleistungen vor allem an den Hauptstandorten in Deutschland und in Bulgarien angeboten.

Die folgenden Abschnitte zeigen einen Überblick über die typischen Phasen eines PAM-Projekts bei der Einführung einer unternehmensweiten Privileged-Access-Management-Lösung gemäß des PATECCO-Standardverfahrens.

5.1 Erfassung der Anforderungen

PATECCO ist händlerneutral und daher gut aufgestellt, um gemeinsam mit seinen Kunden die angestrebte PAM-Landschaft in ihrer Gesamtheit zu gestalten und zu analysieren. Die Auswahl der geeigneten Bausteine aus den im vorherigen Kapitel beschriebenen Funktionen und Technologien ist ein erster wichtiger Schritt, gefolgt von einem angemessenen Design der Zielarchitektur und der erforderlichen Prozesse und Arbeitsabläufe. Dies wird durch die Erfassung von Informationen über die individuellen Kundenanforderungen erreicht.

Der dafür verwendete Fragebogen umfasst verschiedene Aspekte der Prozesse, der technischen Landschaft und der vorhandenen Rahmenbedingungen. Hier finden grundsätzlich Best Practices Anwendung, die auch von KuppingerCole empfohlen werden: Der erste Schritt zum Privilege Management ist nicht die Wahl des Werkzeugs, sondern die Erledigung der Hausaufgaben auf Unternehmensseite.

5.2 Konsolidierung von Identitäten

Die Verwaltung privilegierter Identitäten und deren Zugriff auf kritische Systeme ist nur sinnvoll, wenn sämtliche zu verwaltende Identitäten im Rahmen einer Anfangserhebung eindeutig dokumentiert werden. Hierfür empfiehlt PATECCO, ein PAM-Projekt mit einer Analyse sowie der Bereinigung und Konsolidierung bestehender Identitäten, Rollen, Genehmigungen und lokaler Accounts in allen, insbesondere heterogenen, Ressourcen zu starten.

Nur wenn eine einheitliche und eindeutige Erfassung all dieser Identitäten sichergestellt ist, kann der nächste, im Hinblick auf privilegierten Zugriff sinnvolle Schritt erfolgen. Insbesondere bedeutet dies, dass sich alle Identitäten auch personalisiert in das System einloggen können, sodass dieser eindeutigen Identität sogar in Administrationssystemen Autorisierungen zugeteilt werden können.

Eindeutige, sichere Identitäten, Konten, Rollen und klar definierte Genehmigungen auf einer „Least-Privilege"-Basis sind eine zwingende Voraussetzung für den Start einer erfolgreichen PAM-Implementierung.

Best Practices aus der Projekterfahrung von PATECCO sieht die Anwendung eines Active Directory vor, um UNIX, Linux und LDAP-Identitäten mit einer einzigen, einmaligen ID zwecks eines zentralisierten Identitäten-, Rollen- und Genehmigungsmanagements und einer Kerberos-basierten Authentifizierung zu konsolidieren.

Wenn festgelegt ist, dass die privilegierten Konten auf dieser Grundlage verwaltet werden sollen, ist eine Systembereinigung sowohl nützlich als auch notwendig: Nur aktuell benötigte Konten sollten verwaltet und deren Autorisierungen auf ein Minimum beschränkt werden. Unnötige privilegierte Accounts können und sollten gelöscht oder zumindest deaktiviert werden. Lokale (Windows-) Administratoren werden oft übersehen, sollten jedoch innerhalb eines effizienten Managementkonzepts im Hinblick auf einen einwandfreien Lebenszyklus geprüft werden.

5.3 Anforderung von privilegiertem Zugriff

Die zentrale Herausforderung eines Verwaltungssystems für privilegierten Zugriff ist die Anwendung eines (mindestens) Vier-Augen-Prinzips, welches den Antragsteller und den Genehmiger eindeutig identifiziert sowie eine anschließende Nachverfolgbarkeit ermöglicht. Zu diesem Zweck wird üblicherweise eine workflowbasierte Anfrage gestellt und ein Genehmigungsverfahren benutzt.

Der Zugriff auf die Anwendung von privilegierten Konten ist für Regulatoren in vielen Branchen ein Schlüsselthema, jedoch sollte auch in allen anderen Unternehmen der Zugriff auf kritische Unternehmensressourcen kontrolliert, dokumentiert und überwacht werden, um Sicherheit, Steuerung und Compliance zu optimieren.

5.4 Super User Privilege Management (SUPM)

PATECCO bezeichnet den Einsatz eines „Least-Privilege“-Zugriffsmodells für autorisierte Nutzer mittels Erweiterungstools für die Authentifizierung als Super User Privilege Management (SUPM). Ziel dieses Verfahrens, welches KuppingerCole als Controlled Privilege Elevation and Delegation Management (CPEDM) bezeichnet, ist die Zuteilung einer Minimalzahl an Berechtigungen während der Sitzungslaufzeit. Eine interaktive Sitzung startet mit möglichst wenigen Berechtigungen und diese werden nur bei Bedarf erweitert. Insbesondere soll vermieden werden, auf gemeinsam genutzte Konten mit Hilfe eines modifizierten Autorisierungsmodells zugreifen zu müssen.

Hierfür verwendet PATECCO die Kombination mit Identity Consolidation im Active Directory. Dieses bietet zusätzliche administrative Vorteile, sodass Rollen und Genehmigungen für administrative Anwender zentral verwaltet werden können. Zudem können globale Veränderungen schnell und einheitlich in Windows, Linux und UNIX vorgenommen werden.

5.5 Shared Account Password Management (SAPM)

Bei der Implementierung von PAM-Projekten legt PATECCO großen Wert auf den Schutz der Unternehmensassets. Gemeinsam genutzte Konten sollten prinzipiell vermieden werden, denn die Minimierung von Datenschutzverletzungen ist am effektivsten je kleiner die Angriffsfläche ist.

Insofern sollte die Zahl der privilegierten Konten soweit wie möglich auf Null reduziert und SAPM lediglich für Notfall-Login-Szenarien wie „Break Glass" verwendet werden. Dies trifft auf veraltete und Notfall-Szenarien zu, in denen die Erweiterung von Privilegien nicht sensibel gehandhabt werden kann und in denen ein direktes Log-on als Administrator (z.B. Root) in Ausnahmefällen genehmigt werden muss.

5.6 Application to Application Password Management (AAPM)

Eine wesentliche Schwachstelle besteht bei Programmen, die automatischen Zugriff auf kritische Systeme (wie Provisioning-Systeme oder andere Programme, die Service-Accounts nutzen) erfordern, in der Benutzung von fest kodierten Zugangsdaten im Anwendungscode, in Scripts oder anderen Konfigurationsdateien. Wie in Abschnitt 4.2 beschrieben, bieten AAPM-Tools einen Workaround mit Hilfe eines Verfahrens (typischerweise APIs), das Zugangsdaten auf Anfrage sicher verfügbar macht, indem auf eine sichere Passwortverwaltung zugegriffen wird.

PATECCO unterstützt während der Ausführung eines PAM-Projekts die Implementierung von AAPM als Erweiterung der SAPM-Tools. Dies erleichtert die Verwaltung von Konten, die von Applikationen oder Systemen für die Kommunikation mit anderen Applikationen oder Systemen benutzt werden (wie Datenbanken, Webservices, etc.).

5.7 Zusammenfassung der PATECCO-Dienstleistungen bei einer PAM-Implementierung

PATECCO tritt als händlerneutraler Anbieter von Mehrwertdiensten auf und implementiert PAM-Lösungen mit Hilfe von Produkten von Marktführern wie Thycotic, One Identity, CyberArk und IBM.

Darüber hinaus hat PATECCO Partnerschaften mit Microsoft, IBM (Implementierung von Thycotic-Lösungen) und One Identity aufgebaut.

PAM wird als Kontrollwerkzeug für Informationssicherheit eingesetzt und unterstützt Unternehmen bei der Erfüllung rechtlicher und regulatorischer Compliance-Richtlinien. Zudem trägt es dazu bei, internen Datenmissbrauch bei der Nutzung privilegierter Konten zu verhindern. Im Falle unerwünschten Verhaltens kann dieser Missbrauch mit Hilfe von PAM aufgedeckt und verfolgt werden.

Durch die Implementierung von PAM-Funktionen erhalten privilegierte Nutzer effizienten und sicheren Zugriff auf die von ihnen verwalteten Systeme, während Unternehmen sämtliche privilegierten Anwender in allen relevanten Systemen überwachen können. Somit trägt PATECCO dazu bei, dass die Einhaltung von Audit- und Compliance-Anforderungen gewährleistet ist und kann die Umsetzung von Datenschutzrichtlinien im Zusammenhang mit regulatorischen und rechtlichen Anforderungen (z.B. EU-GDPR) unterstützen.

6 Empfehlungen

Privileged Access Management hat sich von einem reinen Basis- und Sicherheitsbereich mit eingeschränktem Umfang zu einer wichtigen Komponente sowohl im IAM als auch bei der Unternehmenssicherheit entwickelt. Die stetige technologische und architektonische Aktualisierung sowie die gleichzeitige Gewährleistung eines optimalen Schutzes für ein Unternehmen und seine Assets stellt eine permanente Herausforderung dar.

Die Verwaltung erweiterter Rechte und gemeinsam genutzter Konten stellt nicht nur – und noch nicht einmal in erster Linie – ein technisches Problem dar. Die Technologie unterstützt die Umsetzung festgelegter Strategien und Kontrollen. Haben jedoch Unternehmen keinen eindeutigen Plan formuliert, wie diese Technologien wirksam und zur Umsetzung dieses konkreten Plans eingesetzt werden können, dienen Privilege-Management-Tools lediglich als Feigenblatt, um die Defizite in der Unternehmens-IT-Sicherheit zu überdecken.

Wer in Sachen Cybersicherheit und Compliance-Anforderungen stets auf dem aktuellen Stand sein möchte, und das bei moderaten Kosten, sollte sorgfältig planen. Wir empfehlen folgende Punkte zu berücksichtigen:

- **Kontinuierliche Anpassung von PAM an Veränderungen in IT und Unternehmen**
  Ein PAM-System kann nur so effektiv sein wie seine Integration in eine sich stetig entwickelnde IT-Landschaft. Privilegierte Konten und die damit verbundenen Risiken entwickeln sich parallel zu einem sich ständig verändernden System. Somit reflektieren sie konzeptionelle Veränderungen, wie die allgegenwärtige Digitalisierung und die Cloud-Revolution, ebenso wie jeden Hype und Trend (man denke an: DevOps, AI, IoT). Eine kontinuierliche Anpassung an sich ständig ändernde Systeme, ihre Kritikalitäten und administrativen Besonderheiten ist für die Aufrechterhaltung des Sicherheits-niveaus unerlässlich.

- **Integration von PAM und Access Governance**
  Die Integration von Access Governance und Privilege Management auf IAM-Architekturniveau ermöglicht die Definition und Bereitstellung einer großen Auswahl an Kontroll- und Verwaltungsabläufen. Sie überbrückt Kontrollsilos, die typischerweise durch individuell verwaltete Speicher manifestiert werden (Access Governance, Access Warehouse und die Privilege Management-Speicher privilegierter Konten).

  Es gibt Anwendungsfälle, in denen eine effiziente Integrierung durch Zuteilung privilegierter Konten als zusätzliche Nebenkonten zu IAM-verwalteten Identitäten sowie durch die Bereitstellung dieser Konten im PAM-System und/oder dem eigentlichen Zielsystem erreicht werden kann. Optimal ausgeführte Nutzer-Lebenszyklusprozesse im IAM stellen sicher, dass ein nicht mehr benötigter privilegierter Zugriff entzogen wird.

- **Mehr als der traditionelle Administrator**
  Im Wesentlichen gibt es zwei Arten privilegierter Nutzer:
  Privilegierte IT-Anwender – diese haben Zugriff auf die geschäftsrelevante IT-Infrastruktur. Dieser Zugriff wird IT-Administratoren meist über administrative Rollen gewährt, die System-, Software- und Betriebskonten nutzen.
  Privilegierte Business User – diese haben Zugriff auf sensible Daten- und Informationsbestände wie Personalstammdaten, Gehaltsinformationen, Finanzdaten, geistiges Eigentum des Unternehmens, etc. Diese Art von Zugriff wird Anwendungsnutzern typischerweise über Business-Rollen, die Anwendungskonten nutzen, zugewiesen.

- **Mehr als On-Premises**
  Hybrid IT wird derzeit zur neuen Normalität und das muss sich in einer PAM-Strategie widerspiegeln. Administrative, technische und privilegierte Nutzer in AWS, Azure, Salesforce.com, Workday, Office 365, SAP, SAP HANA sowie einer großen Zahl weiterer Cloud-Services zwischen IaaS, PaaS, SaaS, Docker-Plattformen und serverlosen Architekturen müssen in ein umfassendes Hybrid-Sicherheitskonzept eingebunden werden.

- **Integration von PAM in Ihre IT-Sicherheit, Ihr Incident Management und Ihr SOC**
  Fachgerecht konzipierte und ausgeführte Privilege-Access-Management-Prozesse stellen eine reiche Quelle sicherheitsrelevanter Informationen dar. Infolgedessen ist PAM eine Datenquelle für verschiedene Unternehmenssicherheitsinfrastruktur-Systeme. Korrelierte Informationen über Malware-Ausbrüche oder gezielte Netzwerkattacken können somit Warnungen an das Security Operations Center (SOC) und geeignete Maßnahmen auf Unternehmensebene auslösen.

- **Schulung und Sensibilisierung**
  Im Zuge einer ständigen Mitarbeiterfluktuation, sich verändernder Infrastrukturen und einfach durch den Lauf der Zeit geht in Unternehmen zeitgemäßes Wissen, insbesondere über Sicherheitssysteme sowie deren Anwendung und Notwendigkeit, verloren. Die Bedeutung von Schulung und Sensibilisierung kann nicht hoch genug eingeschätzt werden. Statten Sie Ihre Administratoren und privilegierten Business-Anwender mit allen nötigen Kompetenzen für die Verwaltung und Nutzung von PAM aus.

Gegenwärtig und zukünftig bietet Privileged Access Management ein unverzichtbares Kontrollsortiment zum Schutz unseres sprichwörtlichen „Schlüssels zum Königreich“. Sinnvolle Planung und kontinuierliche Optimierung, belastbare Unternehmensrichtlinien, adäquate Abläufe, gutgewählte Technologien und weitgreifende Integration sind Schlüsselfaktoren für Ihren Erfolg. Dasselbe gilt für eine sorgfältige Anforderungsanalyse, eine gut geplante Implementierung sowie genau durchdachte Roll-Out-Prozesse und ein insgesamt einwandfrei ausgeführtes PAM-Projekt.

Oftmals ist es von Vorteil, von den Erfahrungen eines Projektpartners wie PATECCO zu profitieren. Die Überbrückung von spezifischen Anforderungen und technischen wie unternehmerischen Herausforderungen mit Hilfe von Technologie, Compliance, Sicherheit sowie Händler- und Produktexpertise erweist sich oft als wichtige Grundvoraussetzung für eine erfolgreiche PAM-Umsetzung.

7 Urheberrecht

Die Zukunft der Informationssicherheit – Heute

KuppingerCole unterstützt IT-Fachleute bei der Entwicklung von IT-Strategien und den entsprechenden Entscheidungsprozessen mit herausragender Expertise. Als führender Analyst liefert KuppingerCole händlerneutrale Informationen aus erster Hand. Unser Service versetzt Sie in die Lage, maßgebliche Entscheidungen für Ihr Unternehmen bequem und sicher zu treffen.

Als 2004 gegründetes, globales Analystenunternehmen mit Hauptsitz in Europa, ist KuppingerCole auf Informationssicherheit sowie Identity and Access Management (IAM) spezialisiert. KuppingerCole repräsentiert Expertise, Innovationskraft, ausgesprochene Praxisnähe und einen händlerneutralen Blick auf die Marktsegmente der Informationssicherheit, wobei alle maßgeblichen Aspekte erfasst werden: Identity and Access Management (IAM), Governance- & Auditing-Tools, Cloud- und Virtualisierungs-Sicherheit, Informationsschutz, Mobile- sowie Softwaresicherheit, System- und Netzwerksicherheit, Sicherheitsüberwachung, Analyse & Berichtswesen, Steuerung, Organisation und Strategien.

Für weitere Informationen kontaktieren Sie bitte **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com