esatus AG
The CISO Consulting Company

Privileged Access Management:

Die große Sache im Identity & Access Management?

Durch die stetig steigende digitale Vernetzung in Unternehmen spielen Vertraulichkeit und Verantwortungsbewusstsein der Mitarbeiter eine immer größere Rolle. Für Angreifer ist es derzeit noch zu einfach, an Anmeldeinformationen von Domänenadministratorkonten zu gelangen. Für Unternehmen wiederum ist es schwierig, solche Angriffe nachträglich zu erkennen. Ein Missbrauch von System- und Netzwerkzugangskonten erlaubt Zugriff auf unzählige – oftmals sensitive – Informationen. Zugleich sind diese Konten in vielen Fällen ungenügend verwaltet. Um Datenschutzverletzungen zu verhindern und Zugriffschancen für Angreifer zu minimieren, ist es das Ziel des Privileged Access Management, Zugriffe zu kontrollieren und zu überwachen. In diesem Whitepaper wird erläutert, was Privileged Access Management ist, welche Schritte bei der Einrichtung erfolgen und worin der Unterschied zum Identity Management liegt.

Einleitung

Unternehmen und Behörden werden immer häufiger Opfer von kostspieligen Datenschutzverletzungen. Experten sehen den Grund in zwei wesentlichen Unsicherheitsfaktoren:

- Die Zugriffsmöglichkeiten auf Systeme durch privilegierte Benutzer werden nicht verwaltet.
- Die Nutzung kompromittierter Anmeldeinformationen.

Ein privilegierter Benutzer ist eine Person, die administrativen Zugang auf kritische Systeme hat. Das Wort 'privilegiert' ist nicht zufällig gewählt: Es sagt aus, dass nur vertrauenswürdige Personen Zugang erhalten. Nur diejenigen, die als vertrauenswürdig (verantwortungsbewusst) angesehen werden, können demnach vertraulich mit Rechten umgehen, Systemkonfigurationen durchführen, Software installieren, Benutzerkonten sichern oder auf sichere Daten zugreifen. Doch natürlich ist es aus der Sicherheitsperspektive nicht sinnvoll, jedem bedingungslos zu vertrauen. Daher müssen auch die Zugriffe der privilegierten Benutzer kontrolliert und überwacht werden.

Wenn Administratoren Benutzern Zugriffsrechte erteilen, müssen sie sich gleichzeitig an Compliance-Vorgaben halten. Unterlaufen Benutzern von privilegierten Konten Fehler oder missbrauchen sie die Konten bewusst, können diese Datenschutzverletzungen z.B. zu Betriebsunterbrechungen und Datenverlusten führen. Dies kann das Unternehmen finanziell sowie hinsichtlich der Reputation schwer schädigen. Vielen IT-Abteilungen fehlt jedoch das nötige Personal, um alle Mitarbeiter zu kontrollieren, gerade wenn diese bei Dritten angestellt sind. Auch Umstände wie eine erhöhte Personalfluktuation, die zunehmende Arbeit in Home Offices sowie Büros in anderen Teilen der Welt verstärken das beschriebene Sicherheitsproblem.

Diese Ausgangslage, kombiniert mit dem stetigen Wachstum an Systemen und Benutzergruppen, verpflichtet Unternehmen im Rahmen Ihrer IT Governance, alternative Möglichkeiten für die Verwaltung der Zugriffsrechte zu finden. An dieser Stelle setzt das Privileged Access Management an.

Was ist Privileged Access Management (PAM)?

Privileged Access Management (PAM) ermöglicht eine bessere Überwachung, mehr Transparenz und eine spezifischere Steuerung privilegierter Zugänge zu Systemen und Netzwerken. PAM versetzt Unternehmen in die Lage zu wissen, wer als privilegierter Administrator/Benutzer agiert und welche Tätigkeiten er ausführt. Es schützt Organisationen und Unternehmen auf diese Weise vor versehentlichem oder vorsätzlichem Missbrauch der privilegierten Zugänge. Dies ist besonders wichtig, wenn das Unternehmen wächst.

Denn je größer und komplexer die IT-Infrastruktur in den Unternehmen ist, desto mehr privilegierte Nutzer sind vorhanden. Dazu zählen nicht nur eigene Mitarbeiter, sondern ebenso autorisierte externe Benutzer. Einige Unternehmen haben zwei bis drei Mal so viele privilegierte Benutzerkonten, wie Mitarbeiter.

Eine PAM-Lösung bietet eine sichere und effiziente Möglichkeit, alle privilegierten Zugriffsrechte für alle relevanten Systeme zu autorisieren und zu überwachen. Privileged Access Management leistet dies durch folgende Prinzipien:

- PAM verwaltet alle Berechtigungen für Benutzer, die auf ein System Zugriff benötigen.
- Zugänge werden nur gewährt, wenn sie benötigt werden. Sie werden deaktiviert, wenn die Notwendigkeit abläuft.
- Es wird unterbunden, dass privilegierter Zugriff über lokale/dezentrale Systempasswörter nutzen.
- Die Zugriffe können zentral und schnell – auch über heterogene Systeme – verwaltet werden.
- PAM erstellt einen unveränderbaren Prüfpfad für jeden privilegierten Zugriff.

PAM-Lösungen können in ihren Architekturen variieren. Üblicherweise umfassen sie jedoch die folgenden Komponenten:

1. Access Manager
   Dieses PAM-Modul regelt Zugriffe auf privilegierte Berechtigungen. Ein privilegierter Benutzer fordert den Zugriff auf ein System über den Access Manager. Dieser kennt die Systeme, auf die der Benutzer zugreifen darf und auf welcher Ebene der Berechtigung er sich befindet.

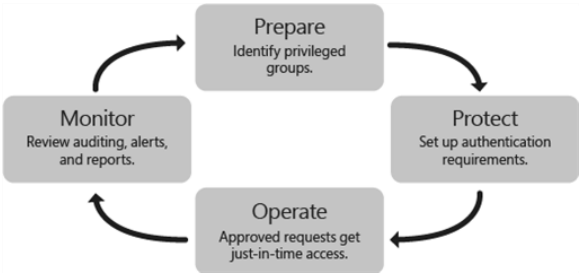
2. Password Vault
   Die Komponente 'Password Vault' verhindert, dass privilegierte Nutzer Zugriff auf Passwörter zu kritischen Systemen erhalten. Dadurch lässt sich beispielsweise das manuelle Überschreiben von Daten unterbinden. Das PAM-System legt dazu das jeweilige Passwort verschlüsselt in der Datenbank ab. Sobald ein User als privilegiert authentifiziert wird, erhält er durch Single-Sign-On (SSO) Zugang zu der jeweiligen Applikation oder Datenressource. Das Passwort bleibt dabei verschlüsselt und im Hintergrund.

3. Session Manager
   Neben der Zugriffskontrolle, die über die ersten beiden Komponenten abgedeckt wird, verfolgen PAM-Lösungen auch die Aktionen, die während einer privilegierten Sitzung ausgeführt werden. Dies leistet die Komponente 'Session Manager'.

Prüfungen privilegierter Zugriffe sind unabdingbar und werden nicht zuletzt auch durch viele Vorschriften und regulatorischer Anforderungen verschiedener Branchen angeordnet. Werden bei der Durchführung von Security Audits Verfehlungen dieser Vorschriften erkannt, kann dies mit empfindlichen Geldstrafen und anderen Maßnahmen sanktioniert werden.

Wie wird PAM eingerichtet?

Für die Einrichtung des Privileged Access Managements sind vier Schritte erforderlich:



Wie PAM eingerichtet wird. Quelle: Microsoft.

1. Vorbereiten
   Die Vorbereitung besteht im Wesentlichen aus der Beantwortung der Frage, welche Gruppen in der bereits bestehenden Gesamtstruktur wesentliche Berechtigungen haben. Anschließend müssen diese Gruppen (ohne Mitglieder) in der geschützten Struktur neu angelegt werden.

2. Schützen
   Es ist essenziell, dass ein Lebenszyklus- und Authentifizierungsschutz, wie z.B. die mehrstufige Authentifizierung (Multi-Factor Authentication) eingerichtet wird. Dieser greift, wenn Benutzer die Just-in-Time-Verwaltung anfordern. Durch die Authentifizierung werden programmgesteuerte Angriffe verwehrt.

3. Betreiben
   Sobald die Voraussetzungen der Authentifizierung erfüllt sind und die Anforderung autorisiert wurde, wird das Benutzerkonto zeitweise der privilegierten Gruppe – in der geschützten Struktur – beigefügt. Der Administrator verfügt nun, über einen definierten Zeitraum, über alle Rechte und Zugriffsberechtigungen, die der Gruppe zugeschrieben sind. Endet der vordefinierte Zeitraum, wird das Konto aus der Gruppe entfernt.

4. Überwachen
   Beim PAM können die Meldungen und Berichte zu den Anforderungen der privilegierten Zugriffe überprüft werden. So ist es möglich, die Verläufe und somit die Aktivitäten der Nutzer zu kontrollieren. Daraus lässt sich erkennen, ob diese Aktivitäten zulässig waren oder nicht. Auf diese Weise lässt sich Schadsoftware identifizieren und interne Angreifer ermitteln.

Was ist der Unterschied zum Identity oder Access Management?

Privileged Access Management wird häufig mit „Identity Management“ (IdM) verwechselt. Zwar bestehen Anknüpfungspunkte, jedoch sind beide Ansätze differenziert voneinander zu betrachten: Identity Management kontrolliert und überwacht Identitäten und deren Privilegien in einem gesamtheitlichen Kontext und über Ihren vollständigen Lebenszyklus hinweg. Das umfasst z.B. Automatismen in der Rechtevergabe beim Einstieg und Ausscheiden von Mitarbeiten und die regelmäßige Überprüfung ob erteilte Berechtigungen beibehalten werden sollen (nach dem least-privilege Prinzip), sowie die Kontrolle über Berechtigungskombinationen, die eine Gefahr für das Unternehmen darstellen können (Toxic Combinations). Darauf aufbauend können Access Management Systeme die technische Authentifizierung und Autorisierung aller User, welche Zugriff auf ein System benötigen, steuern. Privileged Access Management fokussiert sich hingegen auf die temporäre Vergabe von Zugriffsrechten für gewollte Anwendungsfälle und deren Überwachung. Damit gilt das PAM als eine sinnvolle und etablierte Komponente einer zeitgemäßen IT Governance.

Fazit

Privileged Access Management schafft die Kontrolle über gefährdete Umgebungen durch exklusive Überwachung und Vergabe von privilegierten Zugängen. Durch die Verwendung isolierter privilegierter Zugänge wird das Risiko minimiert, dass Anmeldeinformationen entwendet und missbraucht werden.

Die stetig steigende Relevanz des PAM sowie die damit einhergehende wachsende Anzahl an PAM-Lösungen zwingt Unternehmen dazu, sich verstärkt mit der Thematik auseinanderzusetzen. Sicherheitsverantwortliche in den Unternehmen müssen qualifiziert und geschult sein, um die Kontrolle und Überwachung privilegierter Zugänge zu regeln und geeignete präventive Maßnahmen und Lösungen zu etablieren.

Die **esatus** AG ist ein mittelständisches IT-Beratungsunternehmen. Als „The CISO Consulting Company" ist die esatus AG der qualifizierte, erfahrene und flexible Ansprechpartner für Projekte rund um das Thema Informationssicherheit. Für Kunden werden optimale und individuell gestaltete Lösungen für Herausforderungen in den Bereichen Identity & Access Governance, IT Security, sowie Governance, Risk und Compliance angeboten. Zudem bietet die **esatus** AG eine umfassende Beratung zur Thematik des IT-Sicherheitsgesetzes an, beispielsweise zur Einrichtung einer Meldestruktur. Die Zufriedenheit von Kunden ist der Leitfaden, nachdem sich das gesamte Handeln de Unternehmens richtet.

Herausgeber **esatus** AG

Grafik Seite 2 © Microsoft
https://docs.microsoft.com/de-de/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

Weitere Informationen zum Thema „Privileged Access Management" bei der **esatus** AG finden Sie unter: esatus.com

Stand der Informationen im vorliegenden Whitepaper: Juni 2017