Privileged Access Management (PAM)

Professionelle Verwaltung privilegierter Zugriffe

In Unternehmen und ihren IT-Umgebungen sind privilegierte Nutzer und Systeme besonders schützenswert. Privilegierte Konten führen jedoch zu massiven Compliance und Sicherheitsrisiken und sind deshalb das bevorzugte Angriffsziel von Hackern. Aus diesem Grund ist es für Unternehmen von essenzieller Bedeutung, privilegierte Zugriffe effektiv und sicher zu verwalten.

PAM Inhalte und Anforderungen

Privileged Access Management, kurz PAM, ist die Verwaltung privilegierter Nutzerkonten. Das sind administrative Konten, die der Verwaltung und Kontrolle von Systemen und Netzwerken dienen (z. B. E-Mailkonten, Microsoft Exchange Server). Da diese administrativen Konten Zugriffe auf kritische Informationen erlauben, werden sie als privilegiert bezeichnet. Sie sind daher Ziel der meisten Hackerattacken, mit denen sich Zugriff auf diese Accounts und ihre sensiblen Unternehmensdaten verschafft wird. Besonders in größeren Unternehmen existiert meist eine große Anzahl an administrativen Konten, auf die dazu oft auch noch von mehreren Nutzern zugegriffen wird. Hinzu kommt, dass administrative Accounts und damit auch so genannte Service Accounts in den meisten Unternehmen ein leichtes Angriffsziel bieten, da die Kennwörter nie oder sehr selten gewechselt werden. PAM schützt Ihr Unternehmen vor vorsätzlichem, aber auch unbewussten Missbrauch privilegierter Zugänge. Dabei umfasst es zwei wesentliche Bereiche: das Password Management und das Session Management für privilegierte Accounts. So werden sowohl die privilegierten Zugriffe als auch die administrativen Aktivitäten (Sitzungen), gesichert, aufgezeichnet und verwaltet.

Die wichtigsten ToDos auf einen Blick

Für eine sichere Verwaltung von privilegierten Konten sind die folgenden Aufgaben empfehlenswert zu erledigen:

- Führen Sie eine Bestandserfassung Ihrer privilegierten Konten durch, einschließlich der Benutzer und Systeme, die diese verwenden.
-

Stellen Sie sicher, dass Ihre privilegierten Kennwörter zuverlässig gespeichert sind.

- Setzen Sie strenge Verwaltungsprozesse zur Änderung von Kennwörtern für privilegierte Konten durch.
- Sorgen Sie nach Möglichkeit für klare Verantwortlichkeiten und gewähren Sie nur das erforderliche Mindestmaß an Berechtigungen.
- Prüfen Sie die Nutzung von privilegierten Zugriffen regelmäßig.

Ein zentrales Element im PAM-System ist der Tresor. In ihm sind die "Geheimnisse" aufbewahrt. Er ist damit der kritischste Teil. Geheimnisse wie Passwörter werden von der PAM-Lösung verwaltet, z. B. durch das Erzwingen einer regelmäßigen Passwortrotation.

Die Vorteile von PAM auf einen Blick

Erfüllung von Compliance Anforderungen

Privilegierte Benutzer mit hohem Risiko, riskantem Verhalten und ungewöhnlichen Ereignissen werden eindeutig identifiziert. Hacker-Attacken über administrative Accounts werden abgewehrt.

Effiziente Erstellung von Überwachungsberichten

Es erfolgt die Überwachung der Systemzugriffe von externen Dienstleistern und internen Anwendern. Diese sind als Reports jederzeit abrufbar zur Dokumentation der Aufrechterhaltung der Integrität.

Vereinfachung der Verwaltung privilegierter Konten und Sitzungen

Der automatisierte Passwortwechsel von administrativen Accounts und Service Account sowie das zentrale Passwort-Management für Netzwerk, Server, Applikationen und Service Accounts vereinfachen die Verwaltung.

Abmilderung des potenziellen Schadens von Sicherheitsverstößen

Die „Weitergabe“ von Passwörtern ist nicht möglich und die Bedienung für Administratoren vereinfacht sich durch Single-Sign-On.

Verbesserter Schutz für sensible Daten und Unternehmensinformationen

Die Aufzeichnung der Admin-Session sorgt für eine Qualitäts-Optimierung und den Qualitäts-Nachweis. Datenpannen und Ausfallzeiten werden durch unkontrollierte Zugriffe reduziert. Es wird eine volle Zugriffs-Transparenz gewährleistet.

ASCONSIT: Wir setzen auf ganzheitliche PAG-Lösungen!

Die Umsetzung von PAM ist ein wichtiger Bestandteil von IT-Sicherheitsstrategien, um die Sicherheit von IT-Systemen und Daten zu erhöhen, indem die Angriffsfläche für Cyberkriminelle reduziert wird. Zusammen mit einem eindeutigen Account-Zugriff und einem vereinheitlichen Lifeycyle Management im IAM und GRC ist die privilegierte Account Governance (PAG) umgesetzt. Damit ist der umfassendste Schutz von Identitäten und privilegierten Konten sicher gestellt.

Vertrauen Sie mit IAM, GRC und PAM auf die ganzheitlichen PAG-Lösungen von ASCONSIT und das Know-how der Prozess-Spezialisten!