DIE GRÖSSTEN RISIKEN BEIM BETRIEB OHNE PAM

Die Auswirkungen eines unverwalteten privilegierten Zugriffs gehen weit über die Cybersicherheit hinaus. Sicherheitsvorfälle mit privilegierten Konten können Betriebsabläufe stören, das Vertrauen der Kunden schädigen und erhebliche finanzielle Verluste verursachen.

Schon ein einziges kompromittiertes privilegiertes Konto kann Folgendes verursachen:

- SYSTEMAUSFÄLLE
- DATENLECKS
- RANSOMWARE-ANGRIFFE
- VERLUST VON GEISTIGEM EIGENTUM
- FINANZIELLE VERLUSTE
- GESCHÄFTS-UNTERBRECHUNG
- REPUTATIONS-SCHÄDEN

Da Organisationen zunehmend digital vernetzt sind, wächst das operative Risiko im Zusammenhang mit privilegiertem Zugriff stetig.

1 UNKONTROLLIERTER ZUGRIFF SCHAFFT SICHERHEITSLÜCKEN

Ohne zentrale PAM-Kontrollen verlieren Organisationen oft die Übersicht darüber, wer Zugriff auf kritische Systeme hat und wie diese Privilegien genutzt werden. Im Laufe der Zeit häufen sich übermäßige Berechtigungen, gemeinsame Administrator-Konten und vergessene Anmeldedaten in der Umgebung an.

DIESE KONTROLLLÜCKE ERHÖHT DAS RISIKO FÜR:

- Unbefugten Zugriff auf sensible Systeme
- Insider-Bedrohungen und Missbrauch von Privilegien
- Diebstahl von Anmeldedaten und laterale Bewegung
- Menschliche Fehler durch übermäßige Berechtigungen
- Kompromittierte Administrator-Konten

Angreifer zielen gezielt auf privilegierte Anmeldedaten ab, da diese direkten Zugriff auf kritische Infrastrukturen und wertvolle Unternehmensdaten ermöglichen.

2 ZUNEHMENDE KOMPLEXITÄT IN MODERNEN IT-UMGEBUNGEN

Moderne Organisationen arbeiten in hybriden Infrastrukturen, die On-Premises-Systeme, Cloud-Plattformen, SaaS-Anwendungen, Remote-Zugriffsechnologien und Dienste von Drittanbietern kombinieren. Die Verwaltung privilegierter Zugriffe über diese miteinander verbundenen Umgebungen ohne zentrales PAM wird immer schwieriger.

Das Ergebnis sind häufig fragmentierte Sichtbarkeit, verwaiste Konten, nicht verwaltete Anmeldedaten und zunehmende Sicherheitslücken. Mit der Erweiterung digitaler Ökosysteme wächst auch die Komplexität des Privilegienmanagements.

3 ERHÖHTES RISIKO VON ANMELDEDATEN-DIEBSTAHL

Privilegierte Anmeldedaten sind Hauptziele für Phishing-Angriffe, Malware, Ransomware und Credential Dumping. Wenn Passwörter in Tabellenkalkulationen, lokalen Dateien, Browser-Erweiterungen oder unverwalteten Tresoren gespeichert werden, können sie von Angreifern leicht gestohlen werden.

Sobald privilegierte Anmeldedaten kompromittiert sind, können Angreifer Sicherheitskontrollen deaktivieren, Ransomware einsetzen, auf vertrauliche Informationen zugreifen, sich lateral in Systemen bewegen und Geschäftsabläufe stören. Organisationen ohne PAM bemerken Sicherheitsverletzungen oft erst, nachdem erheblicher Schaden bereits entstanden ist.

4 INSIDER-BEDROHUNGEN UND MENSCHLICHE FEHLER

Nicht jeder Sicherheitsvorfall wird von externen Angreifern verursacht. Mitarbeiter mit übermäßigen Rechten können absichtlich oder versehentlich erheblichen Schaden anrichten. Fehlkonfigurationen, unbefugte Änderungen, versehentliche Löschungen oder unzureichende Genehmigungen können die Betriebsabläufe beeinträchtigen.

PAM HILFT, INSIDER-RISIKEN ZU REDUZIEREN DURCH:

- Durchsetzung des Prinzips der minimalen Berechtigung
- Einschränkung unnötiger Berechtigungen
- Überwachung privilegierter Sitzungen
- REC — Aufzeichnung administrativer Aktivitäten
- Automatisierung von Genehmigungs-Workflows

Dies verbessert die Sicherheits-Transparenz und Verantwortlichkeit erheblich.

5 COMPLIANCE- UND AUDIT-HERWUSFORDERUNGEN

Regulatorische Rahmenwerke wie NIS2, DORA, GDPR, ISO 27001 und viele branchenspezifische Standards verlangen zunehmend von Organisationen, strenge Zugriffskontrollen umzusetzen, privilegierte Aktivitäten zu überwachen und detaillierte Prüfprotokolle zu führen.

- Ohne PAM wird der Nachweis von Compliance erheblich schwieriger.
- Organisationen riskieren fehlgeschlagene Audits, Bußgelder und erhöhte rechtliche und operative Risiken.
- Mangelnde Rechenschaftspflicht für privilegierte Aktionen.
- Unzureichende Überwachung sensibler Systeme.
- Mangelnde Transparenz bei privilegierten Aktivitäten beeinträchtigt die Reaktionsfähigkeit bei Sicherheitsvorfällen.

PAM IST NICHT OPTIONAL. ES IST UNVERZICHTBAR.

Schützen Sie Ihre kritischen Systeme, reduzieren Sie Risiken und stärken Sie Ihre Sicherheitslage mit Privileged Access Management.