KEEPER | Pressemitteilung

Kein Privileged Access Management im Einsatz?
Diese sieben Risiken drohen

Von Pawel Jankowski, Senior Account Executive EMEA bei Keeper Security

Cyberangriffe verursachen immer höhere Schäden – laut Cobalt könnten die weltweiten Kosten bis 2029 auf 15,63 Billionen US-Dollar steigen. Ein zentraler Schwachpunkt in vielen Unternehmen bleibt das fehlende Privileged Access Management (PAM). Ohne PAM wachsen Risiken wie Datenschutzverletzungen, Insider-Bedrohungen und Compliance-Verstöße deutlich an. Der Grund: Privilegierte Konten mit weitreichenden Rechten und Zugriff auf sensible Daten sind Hauptziele der Angreifer. PAM-Lösungen schaffen Transparenz und Kontrolle darüber, wer, wann, wie und auf welche Ressourcen zugreift – und mindern so das Risiko erheblich. Doch was genau droht Unternehmen, die auf PAM verzichten?

Datenschutzverletzungen – ein teurer Albtraum

Privilegierte Konten, wie die von Administratoren, werden oft unzureichend überwacht – ein Umstand, den Cyberkriminelle gezielt ausnutzen. Wird ein solcher Zugang kompromittiert, drohen nicht nur Datenabflüsse, sondern auch Rufschädigung, Kundenverluste, juristische Konsequenzen und millionenschwere wirtschaftliche Schäden. Ein Beispiel ist die AT&T-Sicherheitsverletzung im Jahr 2024: Bei diesem Vorfall wurden durch einen schlecht gesicherten Cloud-Dienstleister 7,6 Millionen aktuelle und 70 Millionen ehemalige Kundendatensätze von AT&T entwendet und verursachte gravierende Folgen für das Unternehmen.

Eine PAM-Lösung wirkt dem gezielt entgegen, indem sie Zugangsdaten in einem sicheren, verschlüsselten Tresor speichert, privilegierte Sitzungen überwacht und aufzeichnet sowie das Prinzip der minimalen Rechte durchsetzt.

Insider-Bedrohungen – unterschätzte Gefahr von innen

Nicht alle Gefahren kommen von außen. Häufig sind es Mitarbeitende, Dienstleister oder Partner, die – absichtlich oder aus Nachlässigkeit – Sicherheitslücken verursachen. Ohne PAM fehlt Unternehmen der notwendige Überblick über kritische Zugriffe. PAM schafft Abhilfe durch die Echtzeitüberwachung privilegierter Sitzungen, die konsequente Vergabe feingranularer Rechte sowie die Einrichtung automatischer Warnmeldungen bei verdächtigem Verhalten. So lässt sich nicht nur Missbrauch schneller erkennen, sondern auch abschreckend auf potenzielle Täter wirken.

Fehlende Kontrolle über Zugriffsrechte

In vielen Unternehmen bleiben privilegierte Rechte dauerhaft bestehen – oft, obwohl sie längst nicht mehr benötigt werden. Ohne PAM ist es kaum möglich, das Prinzip der minimalen Rechte konsequent umzusetzen. Die Folgen: Cyberkriminellen bieten sich unnötig große Angriffsflächen und es entstehen durch zu viele Rechte vermeidbare Risiken für die Angestellten im Unternehmen. Moderne PAM-Lösungen ermöglichen es, Zugriffe rollenbasiert zu vergeben, zeitlich begrenzt über sogenannte Just-in-Time-Zugriffe zu gewähren und über vollständige Sitzungsaufzeichnungen mögliche Missbrauchsfälle nachvollziehbar zu machen. Damit wird die Zugriffskontrolle nicht nur effizienter, sondern auch sicherer.

Compliance-Lücken und Prüfungsprobleme

Datenschutzgesetze wie die DSGVO fordern umfassende Kontrollen beim Zugriff auf sensible Daten – ein Bereich, in dem viele Unternehmen ohne PAM an ihre Grenzen stoßen. Ohne einheitliche Protokollierung und Nachverfolgbarkeit wird der Nachweis bei Audits zur

Herausforderung. Eine PAM-Lösung hilft dabei, indem sie vollständige Prüfpfade erstellt, jede privilegierte Handlung aufzeichnet und die Durchsetzung von Richtlinien automatisch unterstützt. Das erleichtert nicht nur die Einhaltung gesetzlicher Vorgaben, sondern auch die Vorbereitung auf externe Prüfungen beziehungsweise Audits.

Fehlende Transparenz – gefährliche Blindstellen
Ohne PAM bleibt oft unklar, wer auf welche Systeme zugreift und zu welchem Zweck. Diese Intransparenz verursacht gefährliche Lücken: Verdächtige Aktivitäten bleiben unentdeckt oder werden zu spät erkannt. PAM schließt diese Lücken, indem es privilegierte Sitzungen live überwacht, Administratoren Eingriffsrechte in aktive Sitzungen einräumt und Protokolle nahtlos an SIEM-Systeme weiterleitet. So wird eine proaktive Sicherheitsstrategie möglich, statt nur auf Vorfälle zu reagieren.

Operative Risiken und menschliche Fehler
Die manuelle Verwaltung privilegierter Zugriffe ist nicht nur ineffizient, sondern auch fehleranfällig. Veraltete Zugangsdaten, unklare Zuständigkeiten und verzögerte Zugriffsvergabe führen zu Sicherheitslücken und organisatorischen Problemen. PAM automatisiert zentrale Prozesse wie Passwortrotation, Nutzer-Provisionierung und verschlüsselte Verbindungen für sicheren Systemzugang. Dadurch wird nicht nur der administrative Aufwand reduziert, sondern auch die Fehleranfälligkeit deutlich verringert.

Hohe Folgekosten bei Sicherheitsvorfällen
Ein Datenleck ist teuer: Laut IBM beliefen sich 2024 die durchschnittlichen Kosten einer Datenschutzverletzung auf 4,88 Millionen US-Dollar – Tendenz steigend. Diese Summe umfasst nicht nur die technische Wiederherstellung und Rechtsberatung, sondern auch Bußgelder, Betriebsausfälle und Kundenverluste. Im Vergleich dazu ist PAM eine kosteneffiziente Investition, um das Risiko von Anfang an zu minimieren. Wer unbefugten Zugriff verhindern kann, muss sich später nicht um Schadensbegrenzung kümmern.

Fazit: PAM ist Pflicht
Privileged Access Management ist längst kein optionales IT-Tool mehr, sondern ein essenzieller Baustein moderner Unternehmenssicherheit. Es schützt vor Angriffen, minimiert interne Risiken, erleichtert Audits und senkt langfristig die Betriebskosten. Nicht nur Großkonzerne, auch mittelständische und kleinere Unternehmen sollten PAM in ihre Sicherheitsstrategie integrieren – bevor ein Schaden eintritt.

###

Über Keeper Security:
Keeper Security verändert die Cybersicherheit für Millionen von Einzelpersonen und Tausende von Unternehmen weltweit. Die intuitive Cybersicherheitsplattform von Keeper ist mit einer End-to-End-Verschlüsselung ausgestattet und genießt das Vertrauen von Fortune-100-Unternehmen, um jeden Benutzer auf jedem Gerät und an jedem Standort zu schützen. Unsere patentierte Zero-Trust- und Zero-Knowledge-Lösung für das Privileged Access Management vereint die Verwaltung von Unternehmenspasswörtern, Geheimnissen und Verbindungen mit Zero-Trust-Netzwerkzugriffen und Remote-Browser-Isolation. Durch die Kombination dieser wichtigen Identitäts- und Zugriffsverwaltungskomponenten in einer einzigen cloudbasierten Lösung bietet Keeper beispiellose Transparenz, Sicherheit und Kontrolle und gewährleistet gleichzeitig die Einhaltung von Compliance- und Audit-Anforderungen. Erfahren Sie unter KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Folgen Sie Keeper auf Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de