

Keeper Security-Umfrage: Die meisten Privileged Access Management-Lösungen sind zu komplex

68 Prozent der Unternehmen zahlen für überflüssige Funktionen

München, 14. Februar 2023 - [Keeper Security](#), führender Anbieter von Zero-Trust- und Zero-Knowledge-Cyber-Security-Lösungen zum Schutz von Passwörtern, Daten und Verbindungen, veröffentlicht heute die Ergebnisse des [Keeper Security Insight Reports: Privileged Access Management \(PAM\) Complexity](#). Der globale Bericht führt die Erkenntnisse von IT- und Sicherheitsverantwortlichen zusammen und zeigt den großen Wunsch nach einfach zu implementieren und zu wartenden PAM-Lösungen auf. 84 Prozent der befragten IT-Führungskräfte geben an, dass sie ihre PAM-Lösung im Jahr 2023 optimieren wollen.

Herkömmliche PAM-Lösungen funktionieren nicht

Da die Bedrohungen der Cybersicherheit weiter zunehmen, suchen IT-Führungskräfte nach möglichst effektiven PAM-Lösungen, die Transparenz, Sicherheit, Kontrolle und Reportings für jeden Benutzer und jedes Gerät bieten. PAM ist weit verbreitet: 91 Prozent der Umfrageteilnehmer gaben an, dass ihre Unternehmen ein PAM-Produkt verwenden. Die Ergebnisse zeigen jedoch, dass herkömmliche PAM-Lösungen die Anforderungen der Unternehmen nicht erfüllen. Mehr als zwei Drittel der IT-Manager (68 Prozent) geben an, dass ihre aktuelle Lösung zu kompliziert ist oder zu viele Funktionen hat, die nicht genutzt werden. 87 Prozent der Befragten würden deshalb eine reduzierte PAM-Version bevorzugen – eine, die einfacher zu implementieren und zu nutzen ist.

Weitere Ergebnisse der Security-Umfrage:

- Im Durchschnitt nutzen IT-Teams nur 62 Prozent ihrer aktuellen PAM-Funktionen. 58 Prozent der Befragten sind zudem der Meinung, dass ihre PAM-Lösung überflüssig ist.
- Etwa zwei Drittel der Befragten geben an, dass teure und überflüssige PAM-Funktionen die Komplexität erhöhen und damit die Benutzerzufriedenheit reduzieren.
- Mehr als die Hälfte aller IT-Teams (56 Prozent) geben an, dass sie bereits versucht haben, eine PAM-Lösung einzusetzen, diese aber schlussendlich nicht implementiert haben. Als Begründung gaben davon 92 Prozent an, dass ihnen die PAM-Lösung zu komplex war.
- Die meisten Unternehmen (85 Prozent) bestätigen, dass ihre PAM-Lösung viele Ressourcen für die Verwaltung und Wartung erfordert.
- Zwei Drittel der IT-Führungskräfte (66 Prozent) sagen, dass sie eine bessere PAM-Lösung benötigen, aber 58 Prozent sagen, dass sie keine haben, weil diese zu teuer ist.

„Unternehmen müssen ihre Zugangsdaten, Konten und Sitzungen sichern, um ihre Organisation zu schützen“, sagt Darren Guccione, CEO und Mitbegründer von Keeper Security. „Der Keeper Security Insight Report: Privileged Access Management Complexity zeigt, warum IT- und Sicherheitsverantwortliche mit PAM-Produkten unzufrieden sind. Die Branche braucht moderne, einheitliche PAM-Lösungen, die in Multi-Cloud-IT-Umgebungen und mit verteilt und dezentral arbeitenden Mitarbeitern funktionieren. Diese Lösungen müssen die wesentlichen Funktionen mit Zero-Trust-Sicherheit bieten und gleichzeitig kosteneffizient sowie einfach zu implementieren und ansprechend für den Endanwender sein.“

Straffe PAM-Lösungen stoßen auf neue betriebliche Herausforderungen

Alarmierend ist, dass fast zwei Drittel der IT-Führungskräfte (62 Prozent) sagen, dass die Verschlechterung der wirtschaftlichen Rahmenbedingungen sie voraussichtlich dazu zwingen wird, ihre aktuelle PAM-Lösung zu reduzieren. Die IT- und Sicherheitsverantwortlichen von heute benötigen eine PAM-Lösung, die ihre sensiblen Systeme schützt, ohne dabei die Komplexität durch überflüssige Funktionen zu erhöhen und die Kosten in die Höhe zu treiben. Die Studie zeigt, dass die schnelle Implementierung und Integration, ein attraktiver Preis und eine leichte Bedienung zu den wichtigsten Kriterien der Lösungen gehören.

Ausgehend von den Umfrageergebnissen sind die fünf wichtigsten Vorteile, die IT-Führungskräfte von einer PAM-Lösung erwarten, folgende:

- Verwaltung und Überwachung des Zugriffs privilegierter Nutzer
- Schutz vor der Kompromittierung privilegierter Anmeldedaten durch externe Bedrohungen
- Verhinderung von Datenschutzverletzungen
- Schutz vor versehentlichem oder absichtlichem Missbrauch eines privilegierten Zugriffs durch Unternehmensinsider
- Gewährleistung der Aktualisierung des Zugangs privilegierter Nutzer, um eine "schleichende Privilegierung" zu verhindern

Die Befragten nannten auch die fünf wichtigsten Vorteile einer vereinfachten PAM-Lösung:

- Leichtere Bereitstellung
- Einfachere Integration in andere Systeme
- Kosteneinsparungen
- Konsolidierte Plattform
- Weniger Personalaufwand

Die digitale Landschaft entwickelt sich ständig weiter, ohne dass der IT-Experte darauf Einfluss nehmen kann. Um den Überblick zu behalten und der nächsten Welle von Cyberbedrohungen einen Schritt voraus zu sein, müssen sich IT- und Sicherheitsverantwortliche anpassen und auf Automatisierung setzen, um mit dem sich ständig verändernden Rahmenbedingungen Schritt halten zu können. Während PAM-Lösungen in erster Linie für den Schutz von IT-Mitarbeitern, Führungskräften sowie Forschungs- und Entwicklungsmitarbeitern konzipiert sind, wird auch der Schutz der Endanwender angesichts des beschleunigten digitalen Wandels sowie des aktuellen Sicherheitsklimas immer wichtiger.

Download Keeper Security Insight Report [„Privileged Access Management \(PAM\) Complexity“](#).

Methode

Der Keeper Security Insight Report basiert auf den Antworten von 400 IT- und Sicherheitsverantwortlichen aus Nordamerika und Europa. Ein unabhängiges Forschungsunternehmen führte die Umfrage im Auftrag von Keeper im Januar 2023 durch.



Über Keeper Security Inc.

Keeper Security verändert die Art und Weise, wie Menschen und Organisationen auf der ganzen Welt ihre Passwörter, Geheimnisse und vertraulichen Informationen schützen. Die benutzerfreundliche Cybersecurity-Plattform von Keeper basiert auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer und jedes Gerät zu schützen. Die Lösung ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in die Systemumgebung integrieren, um Datenschutzverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Einhaltung von Vorschriften zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelpersonen und Tausenden von Unternehmen auf der ganzen Welt und ist der führende Anbieter von erstklassigem Passwortmanagement, Geheimnismanagement, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Schützen Sie, was wichtig ist, auf KeeperSecurity.com.

Pressekontakt für Keeper in DACH:

Alexandra Schmidt, +49 170 387 10 64

Thilo Christ, +49 171 622 06 10

keeper@tc-communications.de