KEEPER | Pressemitteilung

Keeper Security veröffentlicht globalen Insight-Report "Securing Privileged Access: Der Schlüssel zur modernen Unternehmensverteidigung"

Die Umfrageergebnisse zeigen, dass 49 Prozent der Unternehmen mit Privileged Access Management weniger Sicherheitsvorfälle im Zusammenhang mit dem Missbrauch von Privilegien melden.

MÜNCHEN, 24. Juli 2025 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Software für Privileged Access Management (PAM) zum Schutz von Passwörtern und Passkeys, privilegierten Konten und Endpunkten sowie Geheimnissen und Remote-Verbindungen, veröffentlicht heute seinen neuen Insight Report "Securing Privileged Access: Der Schlüssel zur modernen Unternehmensverteidigung".

Da sich Unternehmen auf ein immer komplexeres Netzwerk von Benutzern, Anwendungen und Infrastrukturen verlassen, ist die Verwaltung privilegierter Zugriffe zur Verhinderung von Cyberangriffen sowohl kritischer als auch komplizierter geworden. Die rasche Einführung von Cloud-, Hybrid- und Multi-Vendor-Umgebungen in Kombination mit der zunehmenden Raffinesse und KI-gestützten Cyberangriffen erhöht den Bedarf an Lösungen, die sichere, skalierbare und zentralisierte Zugangskontrollen durchsetzen können.

Der Keeper Insight Report untersucht die Beweggründe von Unternehmen für die Einführung von PAM, die häufigsten Hindernisse für den Einsatz und die Funktionen, die Unternehmen für die Sicherung des Zugangs in der heutigen Cybersicherheitslandschaft als wesentlich erachten. Die Ergebnisse basieren auf einer weltweiten Umfrage unter 4.000 IT- und Sicherheitsverantwortlichen in den Vereinigten Staaten, Europa und Asien.

„Jedes System, ob in der Cloud, on-premises oder remote, ist ein potenzieller Eintrittspunkt, der adaptive und sichere Kontrollen zur Abwehr moderner Bedrohungen erfordert“, sagt Darren Guccione, CEO und Mitbegründer von Keeper Security. „Modernes, zero-trust PAM mindert nicht nur das Risiko, sondern ermöglicht es Unternehmen, von einer reaktiven Verteidigungshaltung zu einer proaktiven, durchdringenden Kontrolle überzugehen.“

Die wichtigsten Ergebnisse des Berichts:

- **PAM erhöht die Sicherheit:** Mehr als die Hälfte (53 Prozent) der Unternehmen, die PAM implementiert haben, berichten von einem verbesserten Schutz sensibler Daten. Der Diebstahl von Zugangsdaten ist nach wie vor eine der häufigsten Ursachen für Sicherheitsverletzungen, was die entscheidende Rolle von PAM als Schutzmaßnahme unterstreicht.
- **Vorfälle von Berechtigungsmissbrauch gehen zurück:** Weltweit meldeten 49 Prozent der Befragten, die eine PAM-Lösung einsetzen, einen Rückgang der Sicherheitsvorfälle im Zusammenhang mit dem Missbrauch von Berechtigungen.
- **Hindernisse für die Einführung bleiben bestehen:** Die Komplexität der Implementierung wurde von 44 Prozent der Befragten weltweit als eine der größten Herausforderungen genannt, was den Bedarf an benutzerfreundlichen und einfach

zu implementierenden Lösungen unterstreicht. Auch in Bezug auf Geschäftskultur und Bewusstsein gibt es noch Lücken.

- **On-Premises-Umgebungen sind out:** 94 Prozent der Unternehmen arbeiten heute in hybriden oder Cloud-first-Umgebungen. Mit der Entwicklung der Infrastruktur müssen auch die Zugriffskontrollen angepasst werden - dies erfordert anpassungsfähige PAM-Plattformen.
- **Menschliches Versagen bleibt ein Risikofaktor:** Selbst wenn Tools vorhanden sind, gibt es immer noch riskante Praktiken. Von den Nicht-PAM-Benutzern speichern immer noch 8 Prozent ihre Anmeldedaten in Tabellenkalkulationen. 13 Prozent der Unternehmen überprüfen den privilegierten Zugriff nur einmal im Jahr oder seltener, womit dauerhafte Berechtigungen über längere Zeiträume nicht überprüft werden. Unternehmen benötigen umfassende Informationen über das Verhalten der Endanwender, um die Sicherheit zu gewährleisten.

„Eine solide Sicherheitslage erfordert sowohl die richtigen Systeme als auch die richtigen menschlichen Verhaltensweisen“, so Guccione. "Ein Unternehmen wird nie vollständig geschützt sein, wenn Benutzer Kontrollen umgehen oder wichtige Überprüfungen auslassen. Aus diesem Grund müssen aufschlussreiche Risikoanalysen und die Schulung der Endanwender Teil einer erfolgreichen PAM-Strategie sein."

Wenn PAM vollständig implementiert ist, bietet es messbare Vorteile für das gesamte Unternehmen. Die Befragten berichten von besserem Datenschutz, weniger Cyber-Vorfällen und besserer Compliance. Eine PAM-Lösung wie KeeperPAM ist für die heutigen verteilten Mitarbeiter entwickelt. Es bietet eine sichere Speicherung von Anmeldeinformationen, einen Zero-Trust-Netzwerkzugang, nahtlose Integrationen und eine Echtzeitüberwachung, die für Cloud- und Hybrid-Umgebungen entwickelt ist. In der heutigen identitätsgesteuerten Bedrohungslandschaft, in der der Zugriff von überall und zu jeder Zeit möglich ist, ist die Kontrolle privilegierter Konten von grundlegender Bedeutung für den Schutz kritischer Systeme und Daten.

Weitere Einblicke und den vollständigen Keeper Security Insight Report finden Sie hier: https://www.keepersecurity.com/de_DE/PAM-key-to-modern-enterprise-defense-report/

Um Keeper zu nutzen, besuchen Sie keepersecurity.com.

Methodik
Diese Studie wurde von Keeper Security in Zusammenarbeit mit dem unabhängigen Marktforschungsunternehmen OnePoll durchgeführt. Die Studie befragte 4.000 IT- und Sicherheitsentscheider in Unternehmen mit 250 oder mehr Mitarbeitern in den USA, Großbritannien, Frankreich, Deutschland, Japan, Australien, Neuseeland und Singapur. Die Befragung wurde zwischen dem 25. März und dem 11. April 2025 online durchgeführt.

###

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