KEEPER | Pressemitteilung

Sicherheit beim Bereitstellen und Teilen von Zugangsdaten: Keeper Security führt zeitlich begrenzten Zugriff sowie sich selbst zerstörende Datensätze ein

Die neuen Zugriffs- und Freigabefunktionen von Keeper gewährleisten Compliance und schützen vor Verstößen.

MÜNCHEN, 9. April 2024 –Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Anmeldedaten, privilegiertem Zugang und Remote-Verbindungen, stellt zwei neue Funktionen für den privilegierten Zugang vor: den zeitlich begrenzten Zugriff (Time-Limited Access) sowie sich selbst zerstörende Datensätze (Self-Destructing Records). Diese Funktionen wurden extra für den verschlüsselten Zugriff auf Datensätze und deren Freigabe entwickelt. Sie bieten eine schnelle und sichere Zugriffsberechtigung sowie die Möglichkeit, zuvor vergebene Rechte rückgängig zu machen. Das reduziert die Anhäufung unnötiger Privilegien und verringert die potenzielle Angriffsfläche eines Unternehmens.

Da Unternehmen durch die zunehmende Geschäftsdynamik unter Druck stehen, sind sichere Lösungen, die sensible Daten und Systeme schützen, gefragter denn je. Wenn es um die Einhaltung rechtlicher Vorschriften geht, ist die Verwaltung privilegierter Zugriffsrechte ein entscheidender Faktor. Nur so können Unternehmen die Sicherheit und Integrität sensibler Daten, in Übereinstimmung mit Compliance-Vorgaben, gewährleisten. Durch die beiden Funktionen für einen zeitlich begrenzten Zugriff und sich selbst zerstörende Datensätze stellt Keeper zweierlei sicher: Zum einen, dass die Anwender bei Bedarf Zugriff auf benötigte Anmeldeinformationen und Dateien erhalten und zum anderen, dass Berechtigungen automatisch entzogen oder angepasst werden, sobald der Zeitrahmen überschritten oder das Projekt abgeschlossen ist. Diese exakte Kontrolle über Berechtigungen sowie die Zugriffsverwaltung erleichtert die Einhaltung von Compliance-Vorschriften.

„Die Bereitstellung eines zeitlich begrenzten Zugriffs und selbstzerstörender Datensätze ist ein signifikanter Fortschritt für das Teilen von Berechtigungen sowie für die Risikobewältigung, die durch die Zunahme von Privilegien entstehen", sagt Craig Lurey, CTO und Mitbegründer von Keeper Security. „Diese Funktionen versetzen sowohl Einzelpersonen als auch Unternehmen in die Lage, Informationen sicher zu teilen und bieten zugleich ein Maximum an Kontrolle über den Datenzugriff."

Der zeitlich begrenzte Zugriff erlaubt es Anwendern der Keeper Plattform, Datensätze für einen bestimmten Zeitraum sicher freizugeben. Dabei kann es sich um jeden beliebigen Datensatz im Tresor eines Nutzers handeln, einschließlich Anmeldeinformationen, Dateien oder Zahlungsinformationen. Nach Ablauf dieses Zeitraums wird der Zugriff automatisch widerrufen, ohne dass eine der beiden Parteien weitere Maßnahmen ergreifen muss. In Verbindung mit dem Keeper Secrets Manager (KSM) können Benutzer die automatische Rotation eines gemeinsam genutzten Berechtigungsnachweises nach Ablauf des Zugriffs planen. So lässt sich das Risiko eines unbefugten Zugriffs minimieren und der Missbrauch

von Berechtigungen verhindern – eine vorteilhafte Funktion, gerade für die Zusammenarbeit mit Dritten.

Selbstzerstörende Datensätze löschen sich automatisch, nachdem der Empfänger den freigegebenen Datensatz geöffnet hat. Die Vernichtung erfolgt innerhalb eines bestimmten Zeitraums oder spätestens, nachdem der Empfänger den Datensatz fünf Minuten lang angesehen hat - je nachdem, was zuerst eintritt. Ein typisches Anwendungsszenario hierfür ist beispielsweise das Onboarding von Mitarbeitern, etwa wenn die IT-Abteilung die Anmeldedaten für einen neuen Mitarbeiter freigeben muss. Die IT-Abteilung kann einen Datensatz mit Anmeldedaten beruhigt weitergeben, denn nach Erhalt wird der ursprüngliche Datensatz zerstört. Damit ist das Risiko, dass weitere, unberechtigte Personen Zugriff auf die Anmeldedaten des Mitarbeiters erlangen, beseitigt. Diese Funktion erhöht nicht nur die Sicherheit, sondern hält auch eine saubere Datenumgebung für eine leichte Identifizierung und Verwaltung von relevanten Informationen aufrecht.

Weitere Informationen über zeitlich begrenzten Zugriff und selbstzerstörende Datensätze finden Sie hier.

###

Über Keeper Security:
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die erschwinglichen und benutzerfreundlichen Lösungen von Keeper basieren auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer auf jedem Gerät zu schützen. Unsere Privileged-Access-Management-Lösung der nächsten Generation ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in jede Technologieumgebung integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern sowie Tausenden von Unternehmen und ist der führende Anbieter von erstklassigem Passwort- und Passkey-Management, Geheimnisverwaltung, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging.

Erfahren Sie mehr unter KeeperSecurity.com
Folgen Keeper: 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