Keeper Security veröffentlicht Studie über die Dokumentation und Offenlegung von Cybersecurity-Katastrophen

Die Studie zeigt, dass 40 Prozent der Unternehmen bereits einen Cybersecurity-Vorfall erlitten haben, 48 Prozent davon jedoch nicht den zuständigen Behörden gemeldet wurden.

MÜNCHEN, 26. September 2023 – Keeper Security, führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Anmeldedaten, privilegiertem Zugang und Remote-Verbindungen, veröffentlicht heute die Ergebnisse seiner Untersuchung zu Cybersecurity-Katastrophen: Incident Reporting & Disclosure. Die Ergebnisse zeigen, dass bei der Meldung von Cybersecurity-Angriffen und -Verletzungen, sowohl an interne Führungskräfte als auch an externe Behörden, Defizite weit verbreitet sind.

Dokumentation von Cybersecurity-Vorfällen ist unzureichend
Die Studie von Keeper zeigt, dass es trotz der wachsenden Bedrohung durch Cyberattacken an Richtlinien für die Meldung von Cybervorfällen mangelt. 74 Prozent der Befragten gaben an, dass sie sich Sorgen machen, dass ihr Unternehmen von einer Cybersecurity-Katastrophe betroffen werden könnte. 40 Prozent der Befragten sagten, dass ihr Unternehmen schon einmal eine Cyber-Katastrophe erlebt hat. Trotz dieser Erfahrung sowie zahlreicher Bedenken wird die Meldung von Sicherheitsverletzungen an das Unternehmensleitung und an die zuständigen Behörden häufig unterlassen.

- **Externe Berichterstattung:** 48 Prozent der Befragten wussten von einem Cybersicherheitsangriff, den ihr Unternehmen nicht an die zuständigen externen Behörden gemeldet hat.

- **Interne Meldung:** 41 Prozent der Cyberangriffe wurden der internen Leitung nicht gemeldet.

Unternehmenskulturen räumen Cybersicherheit keine Priorität ein
Trotz potenzieller, finanzieller und rufschädigender Langzeitfolgen überwiegen unzureichende Offenlegungs- und Transparenzpraktiken. Das Versäumnis, Meldung zu machen, beruht größtenteils auf der Angst vor den kurzfristigen negativen Folgen für den Ruf des Unternehmens (43 Prozent) sowie vor finanziellen Auswirkungen (40 Prozent).

Die Befragten wiesen zudem darauf hin, dass die Unternehmensleitung ein starkes Interesse an der Cyberlage zeigen und ihnen ausreichend IT- und Sicherheitsfachleute bereitstellen müsse, damit die Meldung von Angriffen sowie eine adäquate Reaktion auf dieselben möglich ist.

- Insgesamt 48 Prozent der Befragten sind der Meinung, dass sich die Führungsebene weder für einen Cyberangriff interessiert (25 Prozent) noch darauf reagieren würde (23 Prozent).

- Fast ein Viertel aller Befragten (22 Prozent) gab an, dass ihr Unternehmen "kein System" habe, um Verstöße an die Unternehmensleitung zu melden.

"Die Zahlen verdeutlichen, dass die Unternehmen ihre Kultur in Bezug auf die Cybersicherheit signifikant ändern müssen, schließlich geht es um eine gemeinsame Verantwortung", so Darren Guccione, CEO und Mitbegründer von Keeper Security. "Die Verantwortung beginnt an der Spitze, und die Führungskräfte müssen eine Unternehmenskultur schaffen, die der Meldung von Cybersecurity-Vorfällen Priorität

einräumt. Andernfalls setzen sie sich selbst rechtlichen Verpflichtungen und kostspieligen finanziellen Strafen aus und gefährden Mitarbeiter, Kunden, Stakeholder und Partner."

Best Practices
In einer Zeit großer Sicherheitsrisiken ist es entscheidend, bei der Dokumentation von Cyber-Katastrophen auf Transparenz und Ehrlichkeit zu setzen sowie Best Practices, Guidelines und Prozesse für den Schutz vor laufenden Bedrohungen einzuführen. Eine der wirksamsten Methoden zur Verhinderung von Cyber-Katastrophen, ist etwa die Verwaltung von Passwörtern und privilegierten Zugängen. Sie ist einfach, bietet den Unternehmen zugleich aber einen elementaren Schutz.

Den Download zum vollständigen Bericht gibt es hier.

Methode
Keeper beauftragte ein unabhängiges Marktforschungsunternehmen mit der Befragung von 400 IT- und Sicherheitsverantwortlichen in Nordamerika und Europa, um deren Erfahrungen mit Cybersecurity-Vorfällen, der Dokumentation sowie der Datenwiederherstellung zu gewinnen. Ein unabhängiges Forschungsunternehmen führte die Umfrage im Jahr 2023 durch. Keeper definiert "Cybersecurity-Katastrophen" als jedes Ereignis, das die Vertraulichkeit, Integrität oder Verfügbarkeit eines Informationssystems ernsthaft beeinträchtigt.

Über Keeper Security Inc.
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.

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