KEEPER | Pressemitteilung

Keeper Security ruft zum Handeln auf: In der vierten Woche des Aktionsmonats für Cybersicherheit legt Keeper den Fokus auf Software-Updates

Keeper ruft Einzelpersonen und Organisationen auf, größten Wert auf aktuelle Software zu legen und automatische Updates zu aktivieren.

MÜNCHEN, 21. Oktober 2024 – In der vierten Woche des Aktionsmonats für Cybersicherheit betont Keeper Security wie wichtig es ist, Software auf dem neuesten Stand zu halten, um sich vor neuen Bedrohungen zu schützen. Als ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Cybersicherheitssoftware zum Schutz von Passwörtern, Passkeys, privilegiertem Zugang, Geheimnissen und Remote-Verbindungen fordert Keeper Verbraucher und Unternehmen gleichermaßen dazu auf, regelmäßige Software-Updates als eine entscheidende Aufgabe zur Stärkung ihrer Online-Sicherheit durchzuführen.

Während des gesamten Aktionsmonats für Cybersicherheit hat Keeper praktische Tipps gegeben, die Einzelpersonen und Unternehmen dabei helfen, ihr digitales Leben zu schützen. Dazu gehören die Erstellung sicherer, eindeutiger Passwörter und die Verwendung eines Passwortmanagers, die Aktivierung der Multi-Faktor-Authentifizierung (MFA), wo immer dies möglich ist, und die Wachsamkeit gegenüber Phishing-Betrug. Als eine weitere Best Practice betont Keeper in dieser Woche die Wichtigkeit, jede Software regelmäßig zu aktualisieren.

Um das allgemeine Cyberrisiko zu reduzieren, beheben Software-Updates für Betriebssysteme und Anwendungen bekannte Schwachstellen, die von Cyberkriminellen ausgenutzt werden können. Dass Sicherheits-Patches, die bestimmte Schwachstellen beseitigen, für den Schutz der Nutzer unerlässlich sind, bestätigt der Insight Report 2024 von Keeper Security. Die Befragung bestätigt, dass 92 Prozent der IT-Führungskräfte weltweit einen Anstieg der Cyberangriffe im Vergleich zum Vorjahr verzeichnen, was die Notwendigkeit proaktiver Maßnahmen unterstreicht. Durch die Aktivierung automatischer Updates wird sichergestellt, dass kritische Patches zeitnah eingespielt werden, was das Risiko einer verzögerten Durchführung minimiert.

„Der Aktionsmonat für Cybersicherheit ist ein Aufruf an alle - vom einzelnen Anwender bis hin zu Unternehmen auf der ganzen Welt -, Maßnahmen zu ergreifen und bewährte Verfahren für die Cybersicherheit umzusetzen“, so Darren Guccione, CEO und Mitbegründer von Keeper Security. „Es ist wichtig, Software und Geräte mit den neuesten Sicherheits-Patches auf dem neuesten Stand zu halten, da die Angreifer ihre Techniken ständig weiterentwickeln. Regelmäßige Updates und das Beheben von Schwachstellen sind einfache, aber wirksame Maßnahmen zur Abwehr von Cyber-Bedrohungen.“

Unternehmen sollten der Patch-Verwaltung Vorrang einräumen und sicherstellen, dass Schwachstellen, insbesondere solche, die aktiv ausgenutzt werden, sofort behoben werden. Dokumentierte Patch-Implementierungsprozesse mit Protokollen für kritische Updates sind entscheidend für die Risikoreduzierung.

Im Rahmen des Aktionsmonats für Cybersicherheit - und darüber hinaus - ermutigt Keeper Security Einzelpersonen und Unternehmen, sich zu aktiv zu informieren und Schritte zur Stärkung ihrer Cybersicherheit einzuleiten.
In der Bildersammlung sehen Sie, wie das Keeper-Team den Aktionsmonat der Cybersicherheit in die Tat umsetzt.

###

Über Keeper Security:
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die intuitiven Lösungen von Keeper basieren auf einer End-to-End-Verschlüsselung, um jeden Anwender auf jedem Gerät und an jedem Standort zu schützen. Die Keeper Zero-Trust-Plattform für die Verwaltung von privilegierten Zugängen ist in wenigen Minuten einsatzbereit. Sie lässt sich nahtlos in jeden Technologie-Stack integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern und Tausenden von Unternehmen und ist führend bei der Verwaltung von Passwörtern, Passkeys und Geheimnissen, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Erfahren Sie, wie die Zero-Trust- und Zero-Knowledge-Lösungen vor Cyber-Bedrohungen schützen auf KeeperSecurity.com.

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