KEEPER | Pressemitteilung

Keeper Security ruft zum Handeln auf: In der dritten Woche des Aktionsmonats für Cybersicherheit steht die Multi-Faktor-Authentifizierung im Fokus

Keeper ruft Einzelpersonen und Organisationen auf, im Aktionsmonat für Cybersicherheit die Multi-Faktor-Authentifizierung (MFA) überall zu aktivieren.

MÜNCHEN, 14. Oktober 2024 – Die dritte Woche des Aktionsmonats der Cybersicherheit ist angebrochen und Keeper Security fordert Einzelpersonen sowie Unternehmen gleichermaßen auf, grundlegende Cybersicherheitspraktiken einzuführen und durchzusetzen. Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Cybersicherheitssoftware zum Schutz von Passwörtern, Passkeys, privilegiertem Zugang, Geheimnissen und Remote-Verbindungen, ruft in dieser Woche zur proaktiven Stärkung der Online-Sicherheit auf, indem die Multi-Faktor-Authentifizierung (MFA) aktiv genutzt wird. Aufbauend auf den Tipps der vorangegangenen beiden Wochen – Erkennung von Phishing-Betrug und Verwendung sicherer Passwörter mit einem Passwort-Manager – fügt MFA eine weitere wichtige Schutzebene hinzu, um Konten und Daten zu schützen.

Starke Authentifizierungsverfahren, wie die Verwendung eindeutiger Passwörter und die Implementierung von MFA, sind für die Verbesserung der Online-Sicherheit und die Reduzierung von Cyberrisiken unerlässlich. MFA bietet eine wichtige zusätzliche Schutzebene, die es böswilligen Akteuren erschwert, Konten zu kompromittieren. Selbst wenn die Anmeldedaten eines Kontos in die Hände von Cyberkriminellen gelangen, sind diese ohne den zusätzlichen Authentifizierungsschritt nicht in der Lage, das Konto zu knacken.Trotz der erwiesenen Vorteile wird MFA sowohl von Einzelpersonen als auch von Unternehmen immer noch viel zu wenig genutzt.

„Keeper Security hat den Aktionsmonat der Cybersicherheit ins Leben gerufen, um den notwendigen Wechsel vom Bewusstsein zum echten Handeln einzuleiten, in dem Best Practices für die Cybersicherheit sowohl am Arbeitsplatz als auch zu Hause genutzt werden“, sagt Darren Guccione, CEO und Mitbegründer von Keeper Security. „Die Implementierung von MFA für alle Konten stärkt die Zugriffskontrollen und die Verwaltung von Anmeldeinformationen für Unternehmen erheblich und schützt gleichzeitig Verbraucher vor böswilligen Hackern, die es auf Geräte, Konten und sensible Daten abgesehen haben. Die Durchsetzung grundlegender Best Practices wie die Aktivierung von MFA ist der Schlüssel zur Sicherung unserer digitalen Welt.“

Da sich die Cyberbedrohungslandschaft stetig weiterentwickelt, einschließlich der Zunahme von KI-gestützten Angriffen, kann MFA dabei helfen, raffinierte Angriffe zu vereiteln. MFA stellt sicher, dass selbst fortgeschrittene Techniken, wie Deepfakes oder kompromittierte Anmeldedaten, zusätzlichen Hürden gegenüberstehen. 36 Prozent der Befragten im Keeper Security Insight Report 2024 gaben an, dass die Deepfake-Technologie zu den gefährlichsten neuen Angriffsvektoren gehört, die sie in ihren Unternehmen beobachten.

Auch wenn IT-Führungskräfte und Endanwender im Aktionsmonat der Cybersicherheit Maßnahmen zu MFA durchsetzen, ist es wichtig zu wissen, dass nicht alle MFA-Methoden

gleich effektiv sind. Traditionelle Methoden wie SMS sind im Vergleich zu robusteren Optionen wie Authentifizierungs-Apps oder Hardware-Schlüsseln weniger sicher. Die Verwendung eines Passwortmanagers kann dieses Sicherheitsrisiko mindern, indem er MFA-Codes mit einer integrierten Authentifizierungs-App speichert und automatisch ausfüllt – inklusive einer nahtlosen Benutzererfahrung - und so vor Angriffen wie Social Engineering oder SIM-Swapping schützt.

Keeper hat zum Auftakt des Aktionsmonats der Cybersicherheit darauf hingewiesen, wie wichtig sichere Passwörter und die Verwendung eines zuverlässigen Passwortmanagers sind. Eine Lösung wie Keeper erfüllt diese Anforderungen und vereinfacht den MFA-Prozess. Mit der sicheren Speicherung und Generierung von MFA-Codes hilft ein Passwortmanager sowohl Unternehmen als auch Einzelpersonen, MFA effizient einzusetzen.

Im Rahmen des Aktionsmonats der Cybersicherheit finden Sie bei Keeper Security weitere Aktionspunkte und Ressourcen zur Stärkung Ihres digitalen Lebens.
In unserer 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