Pressemitteilung

Keeper Security stellt „Verify Mode“ und neue Browser-Steuerungen vor, um Phishing und Missbrauch von Anmeldedaten zu verhindern

Neue Funktion validiert die Verwendung von Anmeldedaten direkt bei der Eingabe und hilft Unternehmen, Phishing-Angriffe zu stoppen, bevor Anmeldedaten kompromittiert werden.

MÜNCHEN, 27. April 2026 – Keeper Security, die führende Plattform für Zero-Trust- und Zero-Knowledge-Identitätssicherheit sowie Privileged Access Management (PAM), kündigt veröffentlicht heute ‘Verify Mode‘, eine neue Anti-Phishing-Funktion in Version 17.8 der Browser-Erweiterung. Verify Mode bietet eine Echtzeit-Validierung wo Anmeldedaten eingegeben werden und verhindert so, dass Nutzer Passwörter auf bösartigen oder unbekannten Websites eingeben.

Da die Häufigkeit und Raffinesse von Phishing-Angriffen steigen, bleibt der Diebstahl von Anmeldedaten einer der effektivsten Wege für den unbefugten Zugriff auf Unternehmenssysteme. Laut einer Studie von Verizon waren 60 Prozent der Sicherheitsverletzungen auf menschliches Versagen zurückzuführen, etwa durch Missbrauch von Anmeldedaten oder Phishing-Betrug. Moderne Organisationen, die in Cloud-, Hybrid- und Remote-Umgebungen agieren, sind zunehmend diesen Bedrohungen ausgesetzt. Der neue, optionale Verify Mode sorgt für eine aktive Kontrolle direkt bei der Eingabe von Anmeldedaten und reduziert so die Abhängigkeit von der alleinigen Einschätzung der Nutzer.

„Phishing-Attacken zielen auf den Moment ab, in dem Nutzer ihre Anmeldedaten eingeben“, erklärt Darren Guccione, CEO und Mitgründer von Keeper Security. „Selbst gut geschulte Mitarbeiter können von überzeugend gefälschten, bösartigen Webseiten getäuscht werden. Verify Mode ändert das, indem es die Verwendung von Anmeldedaten in Echtzeit validiert und sicherstellt, dass Passwörter nur auf vertrauenswürdigen Domains eingegeben werden. Dadurch wird die Sicherheit von Anmeldedaten von einer passiven Speicherung zu einem aktiven Schutz verlagert.“

Echtzeitschutz gegen Missbrauch von Anmeldedaten

Verify Mode überwacht die Eingabe von Passwörtern im Browser und prüft, ob die Zielseite mit dem entsprechenden Eintrag im Keeper Vault des Nutzers übereinstimmt. Wird eine Abweichung erkannt, erhalten Nutzer sofort eine Warnung, bevor die Anmeldedaten übermittelt werden, inklusive klarer Details und der Option, fortzufahren oder abzubrechen.

Verify Mode bietet konfigurierbare Schutzstufen, die an die Risikotoleranz der Organisation angepasst werden können:

- **Mittel:** Warnt Nutzer, wenn aus dem Vault kopierte Anmeldedaten auf einer anderen Seite als der gespeicherten eingefügt werden.
- **Hoch:** Warnt Nutzer, wenn ein Passwort auf einer nicht im Vault gespeicherten Seite eingefügt wird.
- **Maximal:** Erfordert eine Bestätigung, bevor Passwörter auf beliebigen Seiten, inklusive vertrauenswürdiger Seiten, eingefügt werden.

Diese Steuerungsoptionen ermöglichen es Sicherheitsteams, starken Schutz mit einer nahtlosen Nutzererfahrung in verschiedenen Rollen und Umgebungen zu verbinden.

Ausweitung von Zero Trust auf die Nutzung von Anmeldedaten
Verify Mode erweitert Keeper Securitys Zero-Trust-Ansatz über die reine Speicherung von Anmeldedaten und setzt auf Echtzeit-Durchsetzung bei deren Verwendung. Durch die Validierung jeder Interaktion erhalten Organisationen eine bessere Kontrolle darüber, wie und wo Anmeldedaten genutzt werden.

Die wichtigsten Vorteile für Unternehmen sind:

- **Reduziertes Risiko von angriffsbasierten Sicherheitsverletzungen:** Stoppt Phishing direkt bei der Eingabe.
- **Stärkere Sicherheitsposition:** Setzt kontinuierliche Validierung nach Zero-Trust-Prinzipien durch.
- **Verbesserte Compliance-Bereitschaft:** Belegt die Einhaltung sicherer Praktiken bei Anmeldedaten.
- **Reduzierung menschlicher Fehler:** Senkt eine der Hauptursachen für Sicherheitsverletzungen.

Der Verify-Modus stärkt die einheitliche Identitätssicherheitsplattform von Keeper, die Passwortverwaltung, Geheimnismanagement, die Verwaltung von Endpunktberechtigungen, KI-gestützte Bedrohungserkennung und die Kontrolle privilegierter Zugriffe in einer einzigen, cloudbasierten Lösung vereint, die speziell für moderne Unternehmensumgebungen entwickelt wurde.

Da identitätsbasierte Angriffe weiterhin Nutzer in SaaS-Anwendungen, Cloud- und Remote-Umgebungen ins Visier nehmen, benötigen Organisationen Echtzeit-Kontrollen. Verify Mode bietet diesen Schutz direkt bei der Verwendung von Anmeldedaten, ohne die Nutzererfahrung zu beeinträchtigen.

Zu den weiteren Funktionen der Browser-Erweiterung Version 17.8 gehören die Aufforderung an die Nutzer, den integrierten Passwort-Manager des Browsers zu deaktivieren, sowie die Unterstützung benutzerdefinierter Felder. Bei der ersten Anmeldung oder Installation der KeeperFill-Browser-Erweiterung erscheint eine Aufforderung, Keeper als Standard-Passwort-Manager festzulegen. Dieser optionale Schritt verhindert Konflikte mit dem nativen Passwort-Manager des Browsers und gewährleistet so ein optimales Ausfüllen, ohne dass manuelle Anpassungen erforderlich sind.

Benutzer können jetzt zudem benutzerdefinierte Felder direkt über die Browser-Erweiterung zu Datensätzen hinzufügen und müssen zum Bearbeiten nicht mehr zum Web-Tresor wechseln. Es kann eine unbegrenzte Anzahl benutzerdefinierter Felder hinzugefügt und per Drag-and-Drop einfach neu angeordnet werden, ähnlich wie bei der bestehenden Funktion in Web- und Mobil-Tresoren. Diese Felder können sensible Informationen wie Sicherheitsfragen, PINs oder private Notizen für Anmeldungen speichern und sind standardmäßig aus Datenschutzgründen maskiert.

Verify Mode ist ab sofort in der Keeper-Browser-Erweiterung für Unternehmen verfügbar. Administratoren können die Schutzstufen über die Keeper Admin Console aktivieren und konfigurieren. Weitere Informationen unter KeeperSecurity.com.

###

Über Keeper Security:
Keeper Security ist eines der am schnellsten wachsenden Unternehmen für Cybersicherheitssoftware, das Tausende von Organisationen und Millionen von Menschen in über 150 Ländern schützt. Keeper ist ein Pionier der Zero-Knowledge- und Zero-Trust-Sicherheit für jede IT-Umgebung. Das Herzstück, KeeperPAM®, ist eine KI-unterstützte, Cloud-native Plattform, die alle Benutzer, Geräte und Infrastrukturen vor Cyberangriffen schützt. Keeper wurde für seine Innovationen im Gartner Magic Quadrant für Privileged Access Management (PAM) ausgezeichnet und sichert Passwörter und Passkeys, Infrastrukturgeheimnisse, Remote-Verbindungen und Endpunkte mit rollenbasierten Durchsetzungsrichtlinien, Least-Privilege und Just-in-Time-Zugriff. Erfahren Sie auf KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Erfahren Sie mehr unter 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