KEEPER | Pressemitteilung

Europäischer Datenschutztag soll das Bewusstsein für den Umgang mit eigenen Daten schärfen

Je früher die nötigen Schritte für einen besseren Datenschutz eingeleitet werden, umso besser – moderne Passwort-Manager können dabei eine große Hilfe sein.

München, 25. Januar 2024 – Laut einer aktuellen Untersuchung des Digitalverbands Bitkom zum Thema Datensicherheit und Passwörter hat sich gezeigt, dass das eine deutliche Mehrheit (74 Prozent) der befragten Personen auf komplexe Passwörter achtet – ein hoher Wert, der 2022 allerdings noch bei 83 Prozent lag. Zudem gaben 4 von 10 Teilnehmern an, sich Zugangsdaten auf Papier zu notieren. Auffällig ist auch, dass sich die Zwei-Faktor-Authentifizierung noch nicht genügend durchgesetzt hat. Diese Ergebnisse sind in Einklang mit den Untersuchungen von Keeper Security: 34 Prozent der Befragten gaben an, dass sie starke Passwörter verwenden, aber Variationen davon wiederholen. Nur 25 Prozent verwenden starke und eindeutige Passwörter für jedes Konto.
Umso wichtiger ist es, die Menschen am europäischen Datenschutztag im Umgang mit ihren Daten und Passwörtern zu sensibilisieren. Die Experten von Keeper Security haben deshalb einen Leitfaden entwickelt, der hilft, die Datensicherheit mit einem professionellen Passwort-Management effektiv zu verbessern.

Risikominimierung

An erster Stelle sei der Grundsatz genannt, dass man mit persönlichen Daten und mit Passwörtern so vorsichtig und restriktiv wie möglich im Internet umgehen sollte. Unbekannte und dubiose Links in E-Mails oder Online-Nachrichten, die nach persönlichen Daten fragen, sind tabu. Gleiches gilt für unbekannte Anhänge. Mindestens ebenso wichtig sind gute Passwörter und deren Sicherheit. Sie müssen eindeutig sein, komplex aus mindestens zwölf Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen in einer beliebigen Anordnung. Erst dann gilt ein Passwort als sicher und Cyberkriminelle haben keine realistische Chance, das Passwort ihres Opfers zu erraten. Ein guter Grund für einen Passwort-Manager ist es, dass er Anwendern und Unternehmen hilft, die Vielzahl der sicheren Passwörter zu erstellen, zu managen und zu speichern – verschlüsselt und sicher vor unberechtigtem Zugriff.

Passwort-Manager – das Tool der Stunde

Der Schutz von Zugangsdaten beginnt mit deren Sicherung. Soziale Netzwerke, Bankanwendungen, Netzwerkgeräte oder Zugänge ins Unternehmen müssen effizient vor unberechtigtem Zugang geschützt sein. Passwort-Manager wie der von Keeper Security sind für diese Anforderung eine zuverlässige Lösung. Der Anwender kann von jedem seiner Geräte aus auf den Passwort-Manager zugreifen, um seine Passwörter zu erstellen und sicher zu nutzen. Anerkannte Verschlüsselungstechnologien und die Zero-Knowledge-Architektur sorgen dafür, dass niemand außer dem Nutzer Zugriff auf die Inhalte des Passwort-Tresors bekommt. Bei den Passwort-Manager-Lösungen für Unternehmen sind die Tresore der einzelnen Mitarbeiter separiert und in SaaS- oder Cloud-Umgebungen mit zusätzlichen Schutzmechanismen ausgestattet.

Darauf sollten Unternehmen bei der Wahl eines Passwort-Managers achten
Um die Wahl eines Passwort-Managers für Unternehmen zu erleichtern, gibt es fünf Aspekte, auf die Sicherheitsverantwortliche und IT-Administratoren achten sollten. Immerhin geht es darum, das Unternehmen vor Eindringlingen zu schützen und die Passwortsicherheit auch in einem Worst-Case-Szenario aufrecht zu erhalten.

1. **Zero-Knowledge-Security**
   Das bedeutet, dass jeder Nutzer die vollständige Kontrolle über die Ver- und Entschlüsselung aller in seinem Tresor gespeicherten persönlichen Daten hat und dass keine seiner gespeicherten Daten für andere Personen zugänglich sind, nicht einmal für die eigenen IT-Administratoren und schon gar nicht für den Lösungsanbieter.

2. **Verschlüsselung aller Daten im Tresor**
   Wichtig ist ein mehrschichtiges Verschlüsselungssystem, das auf vom Client erzeugten Schlüsseln basiert. 256-Bit-AES-Schlüssel auf Datensatzebene und Schlüssel auf Ordnerebene werden auf dem Client-Gerät generiert, die jeden gespeicherten Datensatz verschlüsseln. Damit sind alle Inhalte des Tresors verschlüsselt, einschließlich Logins, Dateianhänge, TOTP-Codes, Zahlungsinformationen, URLs und benutzerdefinierte Felder.

3. **Effektiver Schutz des Datenschlüssels**
   Der Datenschlüssel ist eines der wichtigsten Elemente in einem Passwort-Tresor. Denn um den Tresor eines Benutzers zu entschlüsseln, muss der Datenschlüssel entschlüsselt werden. Für Benutzer, die sich mit einem Master-Kennwort anmelden, sollte der Schlüssel zum Ent- und Verschlüsseln des Datenschlüssels aus dem Master-Kennwort des Benutzers mithilfe der kennwortbasierten Schlüsselableitungsfunktion (PBKDF2) abgeleitet werden, wobei bis zu 1.000.000 Iterationen durchlaufen werden. Für Benutzer, die sich mit SSO oder passwortloser Technologie anmelden sollte zur Ver- und Entschlüsselung der Daten auf Geräteebene die Elliptic Curve Kryptographie verwendet werden. Ein lokaler privater ECC-256 (secp256r1)-Schlüssel wird zur Entschlüsselung des Datenschlüssels verwendet.

4. **Sicherheit bei SaaS-Passwort-Managern**
   Passwort-Manager als SaaS-Plattform, sollten die Daten bei vertrauenswürdigen und im Idealfall vom Kunden wählbaren Hosting-Dienstleistern speichern. Dabei müssen die Daten und der Zugriff auf die Plattform auf die vom Kunden gewählte Region beschränkt sein. Alle verschlüsselten Daten sollten zusätzlich zur Transport Layer Security (TLS) mit einem 256-Bit-AES-Übertragungsschlüssel verschlüsselt sein, um vor Man-in-the-Middle-Angriffen zu schützen. Der Übertragungsschlüssel wird auf dem Client-Gerät generiert und mittels ECIES-Verschlüsselung über den öffentlichen EC-Schlüssel des Servers an den Server übertragen.

5. **Zertifizierungen und Compliance**
   Passwort-Manager für Unternehmen (idealerweise auch für Privatpersonen) sollten von offizieller Stelle geprüft und zertifiziert sein. Dazu gehören internationale ebenso wie europäische Normen wie beispielsweise SOC 2- und ISO 27001 sowie die Konformität zu DSGVO, CCPA, FedRAMP, StateRAMP oder TrustArc und PCI DSS.

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 Sie Keeper auf Facebook, Instagram, LinkedIn, X, YouTube

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