# Cybersicherheit: Lösungsansätze für eine sicherere digitale Welt

*Von Darren Guccione, CEO und Mitbegründer* von Keeper Security

**München, 25. Juli 2023** Die Digitalisierung hat dazu geführt, dass ein Großteil des Alltags und Geschäftslebens der Menschen online stattfindet – potenziell geschützt durch Hunderte von Passwörtern, biometrischen Daten, PINs oder andere Formen der Authentifizierung. Dabei kann die Bedeutung von Cybersicherheit in der digitalen Welt heute nicht hoch genug eingeschätzt werden. Angesichts der rasanten technologischen Entwicklung und der zunehmenden Zahl von Cyberbedrohungen stehen Unternehmen und Einzelpersonen bei der Sicherung ihrer sensiblen Daten zahlreichen Herausforderungen gegenüber.

Eine der weniger beachteten Schwierigkeiten besteht darin, dass die Komplexität und Dimension der Cybersicherheitslandschaft oft als überwältigend empfunden werden. Deshalb fühlen sich viele entweder unsicher oder wissen überhaupt nicht, wie sie sich wirksam schützen können. Laut einer kürzlich durchgeführten Umfrage gab einer von drei Befragten zu, sich überfordert zu fühlen, wenn es darum geht, Maßnahmen zur Verbesserung der Cybersicherheit zu ergreifen. Deshalb muss der Frage nachgegangen werden, inwieweit Cybersicherheit die Menschen überfordert, und welche Lösungen es gibt, um sich zu schützen, etwa mittels eines Passwortmanagers.

**Die wachsende Komplexität der Cybersicherheit**
Die Cybersicherheit wird aufgrund mehrerer Faktoren immer komplexer. In erster Linie haben Umfang und Raffinesse der Cyberbedrohungen erheblich zugenommen. Zudem entwickeln Kriminelle ihre Taktiken ständig weiter und nutzen Schwachstellen in Software, Netzwerken und menschlichem Verhalten erbarmungslos aus. Von Phishing-Angriffen bis hin zu Ransomware-Vorfällen sind Cyberkriminelle geschickt darin, sich unbefugten Zugang zu persönlichen und sensiblen Daten zu verschaffen.

Darüber hinaus bringt das exponentielle Wachstum der digitalen Landschaft neue Herausforderungen mit sich. Die Verbreitung von mit dem Internet verbundenen Geräten sowie dem Internet of Things (IoT) hat die Angriffsfläche noch vergrößert und bietet mehr Ansatzpunkte für potenzielle Verstöße, vor denen sich die Nutzer wappnen müssen. Darüber hinaus hat die weit verbreitete Einführung von Cloud Computing und Remote-Arbeitsplätzen die Sicherung von Daten und die Gewährleistung des Datenschutzes komplexer gemacht.

Unternehmen haben natürlich ihre eigenen IT-Sicherheitsabteilungen oder Fachleute, die für die tiefgreifenden technischen Cybersicherheitsmaßnahmen zuständig sind, wie etwa die Konfiguration von Firewalls, Endpoint-Schutz inklusive Reaktion und sogar die Suche nach Bedrohungen und das Sammeln von Informationen. Für den durchschnittlichen Mitarbeiter jedoch liegt die Navigation in dieser komplexen Cybersicherheitslandschaft weit außerhalb des Rahmens seiner normalen täglichen Arbeit. Gerade für ihn kann die Erwartung, sich über die neuesten Bedrohungen, Software-Patches und bewährten Sicherheitsverfahren zu informieren erdrückend sein – vor allem für Menschen ohne IT-Hintergrund.

**Vereinfachung der Cybersicherheit**
Ein Tool, das die Cybersicherheit auch für einzelne Menschen erheblich vereinfachen kann, ist ein Passwortmanager. Passwörter sind eine wichtige Verteidigungslinie gegen unbefugten Datenzugriff, und schwache oder wiederverwendete Passwörter sind nach wie vor eine häufige Schwachstelle für viele. Der diesjährige Verizon Data Breach Index Report stellt fest, dass 74 Prozent aller Sicherheitsverletzungen auf menschliches Versagen zurückzuführen sind. Ein Passwortmanager bietet eine bequeme und sichere Lösung zur Verwaltung und Generierung starker, eindeutiger Passwörter für jedes Online-Konto.

Mit Passwortmanagern müssen sich die Benutzer keine komplexen Passwörter merken. Und im Gegensatz zur Speicherung von Passwörtern in einem Browser, die bequem erscheinen mag, bieten Passwortmanager ein viel höheres Maß an Schutz. Die Anwender speichern Passwörter sicher in einer verschlüsselten Datenbank, auf die nur mit einem Master-Passwort, einer einmaligen Anmeldung oder einer biometrischen Authentifizierung zugegriffen werden kann. Durch die Automatisierung des Ausfüllens von Anmeldedaten sparen Passwortmanager zudem Zeit und verringern das Risiko menschlicher Fehler.

Darüber hinaus bieten Passwortmanager oft Zusatzfunktionen, wie beispielsweise die sichere Freigabe von Passwörtern im Team, die Integration der Zwei-Faktor-Authentifizierung und die Analyse der Passwortstärke. Diese Funktionen erhöhen die allgemeine Sicherheit und vereinfachen die Verwaltung mehrerer Online-Konten.

Wenn Mitarbeiter dazu angehalten werden, sowohl zu Hause als auch im Büro einen Passwortmanager zu verwenden, trägt das erheblich zu einer besseren Cybersicherheit und einer Risikominderung bei.

**Einfache Lösungen für mehr Cybersicherheit**
Passwortmanager sind zwar ein sehr wirkungsvolles Instrument für die Cybersicherheit, aber nur ein Teil des Gesamtpuzzles. Um die erdrückende Wirkung der nötigen Cybersicherheitsmaßnahmen auf die Mitarbeiter deutlich zu reduzieren, können mehrere andere Strategien angewendet werden:

> **Bildung und Sensibilisierung:** Die Förderung und Ausweitung von Aufklärungs- und Sensibilisierungskampagnen zur Cybersicherheit kann dem Einzelnen helfen, fundiertere Entscheidungen in Sachen Online-Sicherheit zu treffen. Indem die Risiken identifiziert und bewährten Verfahren verstehen werden, kann jeder einzelne aktiv Maßnahmen zum Schutz seiner digitalen Identität ergreifen.
>
> **Benutzerfreundliche Schnittstellen:** IT-Unternehmen sollten benutzerfreundlichen Schnittstellen den Vorzug geben, um die Nutzer besser durch die Sicherheitseinstellungen zu leiten und klare Erklärungen zu potenziellen Risiken zu liefern. Die Vereinfachung komplexer Sicherheitskonfigurationen hilft den Nutzern zudem, sich besser zurechtzufinden.
>
> **Automatisierung und künstliche Intelligenz (KI):** Der Einsatz von Automatisierung und künstlicher Intelligenz (KI) kann die Bemühungen um mehr Cybersicherheit verstärken. KI-gestützte Systeme können Anomalien aufspüren, potenzielle Bedrohungen identifizieren und in Echtzeit reagieren, so dass der Einzelne sich nicht mehr um die Überwachung der Sicherheitsereignisse kümmern muss, um ggfs. darauf zu reagieren.

Auch wenn das Thema Cybersicherheit anspruchsvoll ist, gibt es Möglichkeiten, den Umgang damit zu erleichtern. Da Passwörter einen großen Teil der "mentalen Belastung" ausmachen, mit der Mitarbeiter bei ihrer Arbeit konfrontiert sind, bieten Passwortmanager eine überaus praktische Möglichkeit, einerseits die Online-Sicherheit zu erhöhen und dabei andererseits die Passwortverwaltung zu vereinfachen. Dafür ist ein ganzheitlicher Ansatz erforderlich. Aufklärung, benutzerfreundliche Schnittstellen, Automatisierung und Zusammenarbeit sind allesamt wichtige Komponenten, um die Cybersicherheit Einzelner sowie ganzer Unternehmen besser handhabbar zu gestalten. Durch die Umsetzung dieser Lösungen und die Förderung eines größeren Cybersecuritybewusstseins lässt sich gemeinsam eine sicherere digitale Welt schaffen.

**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 Passwortmanagement, 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