KEEPER | Pressemitteilung

Weihnachten steht vor der Tür – So lässt sich dem Cybersecurity-Terror vorbeugen

Teilen Sie Freude, aber keine persönlichen Informationen. Keeper Security bietet Best Practices für den Schutz der Privatsphäre und Sicherheit in der Weihnachtszeit.

MÜNCHEN, 21. DEZEMBER 2023 – Die Weihnachtszeit ist geprägt von der Freude am Schenken. Immer öfter liegt die neueste Technologie unter dem Weihnachtsbaum: von innovativen Gadgets, die die Kreativität anregen, bis hin zu interaktiven Geräten. Sie alle bringen die Familie zusammen und so kann technisches Spielzeug die Festtage noch spannender und interessanter machen. Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Cyber-Security-Lösungen zum Schutz von Passwörtern und Passkeys, möchte in diesem Jahr das Bewusstsein für die Bedeutung des Schutzes persönlicher Daten und der Privatsphäre schärfen, damit es nach den Festtagen kein böses Erwachen gibt.

Inmitten der Freude und Aufregung, die neue technische Geräte mit sich bringen, ist es von entscheidender Bedeutung, wirkungsvolle Praktiken zum Schutz der Privatsphäre und der digitalen Sicherheit umzusetzen. Denn die Feiertage sind eine Zeit, in der Cyberkriminelle besonders aktiv sind und unvorsichtiges Handeln gnadenlos ausnutzen.

„Während wir in der Weihnachtszeit die Freude am Schenken genießen, ist es wichtig, sich der Risiken bewusst zu sein, die mit technischen Geräten verbunden sind. Von der Datenerfassung bis hin zu Sicherheitslücken können diese Tools eine ernsthafte Bedrohung für die Privatsphäre und Sicherheit mit sich bringen", so Darren Guccione, CEO und Mitbegründer von Keeper Security. „Deshalb sollte jeder konkrete Schritte unternehmen, um sein heimisches Netzwerk und die technischen Geräte zu schützen, damit der Zauber der Weihnachtszeit schlussendlich nicht die Online-Sicherheit der gesamten Familie gefährdet."

Im Rahmen seines Engagements für die Datensicherheit empfiehlt Keeper folgende Vorsichtsmaßnahmen:

- **Schützen Sie neue Geräte**: Die meisten IoT-Geräte werden mit voreingestellten Passwörtern geliefert, die sofort geändert werden sollten. Erstellen Sie ein sicheres und eindeutiges Passwort für das jeweilige Gerätekonto, das Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthält. Ein Passwort-Manager hilft bei der Erstellung komplexer Passwörter und speichert sie sicher in einem verschlüsselten Tresor.

- **Sichern Sie Ihr WiFI-Netzwerk:** Vergewissern Sie sich, dass Ihr WiFi-Netzwerk durch ein sicheres Passwort geschützt ist. Ändern Sie den Netzwerknamen so, dass er nicht der Standardname ist. Aktivieren Sie die Verschlüsselung in den Einstellungen Ihres Routers und aktualisieren Sie die Software Ihres Routers regelmäßig. Wenn Sie das WiFi-Passwort freigeben müssen, tun Sie dies über ein verschlüsseltes Freigabetool wie

Keeper's One-Time Share und ändern Sie Ihr Passwort, nachdem die Gäste gegangen sind.

- **Überprüfen Sie die Datenschutzeinstellungen:** Stellen Sie sicher, dass bei Ihrem neuen Spielzeug die Datenerfassung begrenzt ist und den Vorschriften entspricht. Überprüfen Sie außerdem die Berechtigungseinstellungen, um unnötigen Zugriff auf Funktionen wie Kameras oder Mikrofone zu verhindern. Aktivieren Sie, sofern vorhanden, die Optionen zum Löschen von Daten.

- **Aktualisieren Sie Firmware und Software:** Stellen Sie sicher, dass Ihre intelligenten Spielzeuge mit den neuesten Firmware- und Software-Updates ausgestattet sind. Die Hersteller veröffentlichen regelmäßig Updates, um alle Sicherheitslücken zu schließen, die von Cyberkriminellen ausgenutzt werden könnten. Gehen Sie dafür in die Einstellungen, um manuell zu aktualisieren oder automatische Updates zu aktivieren.

- **Verwenden Sie die Kindersicherung:** Durch die Aktivierung und Anpassung der Kindersicherung können Sie den Zugang zu altersgerechten Inhalten verwalten, Online-Interaktionen einschränken und potenzielle Risiken durch bösartigen Akteure, die Ihr Kind schikanieren oder ausnutzen wollen, verringern.

- **Aktivieren Sie die Multi-Faktor-Authentifizierung:** Die Implementierung von MFA ist eine proaktive Maßnahme, die sicherstellt, dass nur autorisierte Benutzer ein Spielzeug oder Gerät steuern und mit ihm interagieren können. Das minimiert ebenfalls das Risiko eines unbefugten Zugriffs oder einer Manipulation durch Kriminelle.

- **Kommunizieren Sie mit Ihren Kindern:** Eine von Keeper durchgeführte Studie ergab, dass 30 Prozent der Eltern noch nie mit ihren Kindern über Cybersicherheit gesprochen haben. Sprechen Sie mit Ihrer Familie über eine gute Cyber-Hygiene und den Umgang mit altersgerechten Inhalten. Außerdem sollten Sie für eine sinnvolle Begrenzung der Bildschirmzeit Sorge tragen.

Um die mit den „Technik-Geschenken“ verbundenen Datenschutz- und Sicherheitsrisiken zu minimieren, ist es wichtig, die Datenpraktiken der einzelnen technischen Spielzeuge zu kennen und die Geräteeinstellungen zu aktualisieren. Nur so lassen sich mögliche Schwachstellen identifizieren und die Sicherheit erhöhen. Indem wir wachsam sind und uns informieren, können wir die Weihnachtsstimmung nicht nur genießen, sondern auch darauf vertrauen, dass der zukünftige Umgang mit den neuen Gadgets sicher ist.

###

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 Keeper: 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