Keeper Security warnt Einzelhändler vor Cybergefahren im Weihnachtsgeschäft

Bewährte Methoden von Keeper zum Schutz sensibler Systeme und Kundendaten für die wichtigste Verkaufszeit des Jahres.

München, 14. November 2023 – Der Black Friday und Cyber Monday im November sowie das darauffolgende Weihnachtsgeschäft läuten die vermutlich heißeste und lukrativste Phase in der Geschäftswelt des Einzelhandels ein. Die hohen Verkaufszahlen und Umsätze locken jedoch auch Cyber-Kriminelle an, die den Einzelhandel gezielt mit Cyberangriffen attackieren. Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Anmeldedaten, privilegiertem Zugang und Remote-Verbindungen, hat für kleine Unternehmen einige bewährte Verfahren für die Cybersicherheit zusammengestellt, damit sensible Systeme und wertvolle Kundendaten auch während des Weihnachtsgeschäfts geschützt bleiben.

Cyber-Kriminelle nutzen eine Reihe unterschiedlicher Taktiken, um sich gerade in hektischen Zeiten Zugang zu Systemen und wertvollen Daten zu verschaffen, beispielsweise mit Phishing-Angriffen, Ransomware, Malware oder der Kompromittierung von Geschäfts-E-Mails. Um die Sicherheit der Kundendaten und Transaktionen auch während des Vorweihnachtsgeschäfts zu gewährleisten, sollten sich Unternehmen aktiv auf Cyberbedrohungen vorbereiten. Für den Einzelhandel bietet sich ein mehrschichtiger Ansatz für mehr Cybersicherheit an.

- **Mitarbeiterschulung** - Laut dem Data Breach Report von Verizon beruhen 74 Prozent der Sicherheitsverletzungen auf menschlichem Versagen, beispielsweise Social Engineering, gestohlene Zugangsdaten oder einfache Fehler, wie etwa das Verlegen von Passwörtern. Cyber-Security-Schulungen sollten in den Unternehmen fester Bestandteil sein. Zudem sollten Phishing-Tests und weiterführende Trainings regelmäßig durchgeführt werden, damit die Mitarbeiter stets über die neuesten Arten der Cyberbedrohungen auf dem Laufenden bleiben.

- **Regelmäßige Software-Updates –** Um Unternehmen vor bekannten Schwachstellen zu schützen, muss sichergestellt sein, dass alle Systeme und Softwarelösungen, einschließlich POS-Terminals (Point of Sale) und E-Commerce-Plattformen, über die aktuellsten Sicherheits-Patches verfügen. Zudem schützt eine regelmäßig aktualisierte Antiviren- und Security-Software vor den neuesten Bedrohungen.

- **Absicherung sensibler Systeme** - Um eine sichere Zahlungsabwicklung zu gewährleisten, müssen vertrauenswürdige Tools und ein isoliertes Zahlungssystem verwendet werden. Ebenso wichtig ist ein gutes Access Management, mit dem sich der Zugriff auf privilegierte Systeme und Konten sicher umsetzen lässt, beispielsweise für die IT oder Gehaltsabrechnungen. Dabei sollte nach dem Prinzip der geringsten Privilegien vorgegangen werden, um sicherzustellen, dass Mitarbeiter nur Zugriff auf die Systeme und Konten haben, die sie für ihre Arbeit benötigen. Außerdem empfiehlt sich die Einrichtung eines Intrusion-Detection-Systems zur Erkennung und Verhinderung von Eindringlingen und um verdächtige Aktivitäten sowie potenzielle Bedrohungen zu überwachen.

- **Schutz der Kundendaten** - Regelmäßige Backups und die Kontrolle des Datenzugänge beziehungsweise Benutzerrechte sollten durch einen Administrator überwacht werden. Gleichzeitig sollten die existierenden Datenerhebungspraktiken und Richtlinien überprüft werden, um sicherzustellen, dass die gesammelten Benutzerinformationen richtig

verstanden werden. Außerdem empfiehlt es sich Daten, die nicht benötigt werden, zu löschen. In diesem Zusammenhang sollten Kundeninformationen, die nicht unbedingt benötigt werden, erst gar nicht gesammelt werden.

- **Implementierung eines unternehmensweiten Passwortmanagers** - Schwache und kompromittierte Passwörter sind die größte Bedrohung für die Cybersicherheit eines Händlers. Indem IT-Administratoren Einblick in die Passwortpraktiken der Mitarbeiter erhalten und Passwortsicherheitsrichtlinien mit Hilfe eines Passwortmanagers durchsetzen können, wie etwa die Verwendung starker, eindeutiger Passwörter und MFA, wird verhindert, dass Mitarbeiter ihre Anmeldedaten auf Phishing-Seiten eingeben.

- **Absicherung des WiFi-Netzwerks** – Ein Netzwerk sollte mit einem sicheren Passwort, das mindestens 16 Zeichen lang ist und eine zufällige Mischung aus Buchstaben, Zahlen und Sonderzeichen enthält, gesichert sein. Wenn eine Verschlüsselung bisher noch nicht aktiviert ist, lässt sich das in den Verwaltungseinstellungen des Internet-Providers aktualisieren. Die meisten Router haben bereits eine integrierte Firewall – es geht lediglich darum, dass diese auch aktiviert ist. Um Remote-Mitarbeiter einzubinden, sollte ein virtuelles privates Netzwerk (VPN) aufgesetzt werden, so dass sich diese von außerhalb mit dem Unternehmen verbinden können.

Mit diesen Maßnahmen können Einzelhändler und kleine Unternehmen sowohl ihre Cybersicherheit verbessern als ihre Systeme und Daten während der intensiven Umsatzphasen wie am Black Friday, Cyber Monday oder der Vorweihnachtszeit besser schützen.

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 Passwort- und Passkey-Management, 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