KEEPER | Pressemitteilung

Cyberbedrohungen machen dem Einzelhandel das Leben schwer -
Fünf Maßnahmen mit denen sich Retail-Unternehmen schützen können

Der Online-Handel wird von Cyberkriminellen überaus häufig ins Visier genommen, da hier wertvolle, personenbezogene Daten oder Kreditkarteninformationen verarbeitet werden. Zu den häufigen Bedrohungen gehören Ransomware-Angriffe, Social Engineering, Systemeinbrüche aber gelegentlich auch Insider-Bedrohungen. Daten, die auf diese Art und Weise geklaut werden, werden dann über das Darknet angeboten, um damit beispielsweise betrügerische Finanztransaktionen abzuwickeln. Damit Online-Händler nicht die verehrenden Auswirkungen eines Cyberangriffs bewältigen müssen, können sie sich vor derartigen Risiken schützen, indem sie auf das Zero-Trust-Prinzip und auf weitere wichtige Schutzmechanismen setzen.

1. Implementieren von Zero-Trust-Sicherheit

Zero-Trust-Sicherheit ist ein Sicherheitsframework, bei dem sämtliche Identitäten ständig verifiziert werden müssen, was den Zugriff auf sensible Daten extrem eingrenzt. Mit Zero-Trust-Sicherheit haben Administratoren zudem einen besseren Überblick über die Benutzeraktivitäten, sie verfügen über stärkere Kontrollmöglichkeiten und das Risiko für passwortbasierte Cyberangriffe wird minimiert.

2. Regelmäßige Datensicherung

Regelmäßige Datensicherungen sind wichtig, um die Folgen von Cyberangriffen zu verringern. Wenn beispielsweise im Rahmen eines Ransomware-Angriffs Daten verschlüsselt werden, lässt sich mit speziell geschützten Sicherungskopien schnell dafür sorgen, dass das Business wie gewohnt weitergehen kann. Mit regelmäßigen Datensicherungen können Einzelhändler den Datenzustand von vor dem Angriff schnell wiederherstellen. Das minimiert sowohl die Ausfallzeiten als auch die Notwendigkeit, überhaupt mit den Cyberkriminellen in Verhandlungen treten zu müssen.

3. Das Prinzip der geringsten Privilegien (PoLP)

Das Prinzip der geringsten Privilegien stellt sicher, dass Benutzer nur den Zugriff erhalten, der für ihre Arbeit erforderlich ist und es hilft sicherzustellen, dass die Mitarbeitenden keinen unnötigen Zugriff auf privilegierte Daten haben. Das ist wichtig, denn je mehr Mitarbeitende auf sensible Informationen zugreifen können, desto größer ist dienAngriffsfläche für Cyberkriminelle.

Eine einfache Möglichkeit, PoLP zu implementieren, ist die Verwendung einer Privileged Access Management ,(PAM)-Lösung. Eine PAM-Lösung kann Cyberkriminelle daran hindern, sich seitwärts durch das Netzwerk eines Unternehmens zu bewegen. Neben der Reduzierung externer Bedrohungen kann eine PAM-Lösung auch Insider-Bedrohungen minimieren, da ein Benutzer durch die Implementierung von PoLP nur Zugriff auf das hat, was er für seine Arbeit benötigt.

4. Implementieren von Firewalls und Intrusion Detection Systems (IDS)

Eine Firewall schützt Netzwerke vor externen Bedrohungen, indem sie den Netzwerkverkehr kontrolliert und filtert. Ob softwarebasiert oder hardwarebasiert – Firewalls tragen dazu bei, dass Netzwerke vor externen Bedrohungen geschützt sind.
Zusätzlich zu Firewalls kann ein Intrusion Detection System (IDS), das den Netzwerkverkehr ständig auf verdächtige Aktivitäten überwacht, indem es nach ungewöhnlichem Verhalten sucht, das Netzwerk eines Unternehmens vor unbefugtem Zugriff schützen. Ein IDS versendet Echtzeitwarnungen, noch bevor ein Schaden überhaupt entstehen kann.

5. Schulungen: Best Practices für die Cybersicherheit
Um sich vor Cyberbedrohungen zu schützen, sollten die Mitarbeitenden zur Cybersicherheit geschult und ihr Sicherheitsbewusstsein verbessert werden. Dazu gehört auch die Aufklärung der Mitarbeitenden über Phishing. In anschließenden Phishing-Tests mit Fake-Phishing-E-Mails kann bewertet werden, wie Mitarbeitende auf potenzielle Bedrohungen reagieren. Nach der Durchführung des Tests helfen die Ergebnisse dabei, die nötigen Schulungen zu bestimmen.

Am besten können sich Retail-Unternehmen vor potenziellen Cyberbedrohungen schützen, indem sie eine Zero-Trust-Strategie implementieren, Daten regelmäßig sichern und eine PAM-Lösung wie beispielsweise KeeperPAM® einführen. Mit KeeperPAM kann ein Unternehmen PoLP implementieren und sicherstellen, dass Benutzer und Systeme nur den Zugriff haben, der für ihre Rollen erforderlich ist. Die Lösung verringert die Angriffsfläche und damit das Risiko, dass Cyberkriminelle Zugriff auf sensible Informationen erhalten.

###

Über Keeper Security:
Keeper Security verändert die Cybersicherheit für Millionen von Einzelpersonen und Tausende von Unternehmen weltweit. Die intuitive Cybersicherheitsplattform von Keeper ist mit einer End-to-End-Verschlüsselung ausgestattet und genießt das Vertrauen von Fortune-100-Unternehmen, um jeden Benutzer auf jedem Gerät und an jedem Standort zu schützen. Unsere patentierte Zero-Trust- und Zero-Knowledge-Lösung für das Privileged Access Management vereint die Verwaltung von Unternehmenspasswörtern, Geheimnissen und Verbindungen mit Zero-Trust-Netzwerkzugriffen und Remote-Browser-Isolation. Durch die Kombination dieser wichtigen Identitäts- und Zugriffsverwaltungskomponenten in einer einzigen cloudbasierten Lösung bietet Keeper beispiellose Transparenz, Sicherheit und Kontrolle und gewährleistet gleichzeitig die Einhaltung von Compliance- und Audit-Anforderungen. Erfahren Sie unter KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

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