arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Einzelhandel: Mit dieser Verteidigungsstrategie schützen Unternehmen ihre Daten in der Weihnachtssaison vor Ransomware-Attacken

Von Florian Malecki, Executive Vice President Marketing, Arcserve

Für die Feiertage planen Cyberkriminelle schon heute Ransomware-Attacken. Nicht zuletzt aufgrund des explosionsartigen Wachstums des Online-Shoppings sind Einzelhändler zu einem Hauptziel von Hackern geworden. Laut dem Sophos-Report "State of Ransomware in Retail 2022" meldeten Einzelhändler im letzten Jahr einen Anstieg von Ransomware-Angriffen von 75 Prozent. Aus dem Bericht geht auch hervor, dass im Jahr 2021 77 Prozent der Einzelhandelsunternehmen betroffen waren, gegenüber 44 Prozent im Jahr 2020. Nur 28 Prozent der befragten Einzelhändler geben an, dass sie einen Angriff abwehren konnten, bevor ihre Daten verschlüsselt wurden. Die durchschnittlichen Wiederherstellungskosten nach einem Ransomware-Angriff im Einzelhandel betrugen 2022 1,27 Millionen US-Dollar, und die durchschnittliche Lösegeldzahlung belief sich auf 226,044 US-Dollar.

Einzelhändler sind ein dankbares Ziel für Cyberkriminelle, denn Ausfallzeiten bedeuten für kleine Unternehmen enorme Schäden. Deshalb sind sie auch eher bereit, Lösegelder zu zahlen, wenn ein Angriff ihre Systeme und das Business zum Erliegen bringt. Das gilt insbesondere während der Weihnachtszeit, die für die meisten Einzelhändler zu den verkaufsstärksten Tagen zählen. Angreifer haben es nicht zuletzt deshalb auf Einzelhändler abgesehen, um an die persönlichen Kunden- und Zahlungsdaten zu gelangen, die sie dann für Betrügereien nutzen oder an Betrüger im Dark Web verkaufen.

arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Da Ransomware-Angriffe zunehmen und ihre Auswirkungen immer gravierender werden, müssen Einzelhändler umso dringender Maßnahmen ergreifen, um schnell und effektiv auf einen Angriff reagieren zu können und so Schäden abzuwenden. Im Folgenden werden drei Möglichkeiten beschreiben, wie Einzelhandelsunternehmen böswillige Angreifer besser abwehren können.

1. Gute Cyber-Hygiene praktizieren

Eine gute Cyber-Hygiene erfordert kontinuierliche Anstrengungen. Einzelhändler sollten deshalb eine Vorgehensweise einführen, die dafür sorgt, dass ihre Mitarbeiter konsequent an die Sicherheitsmaßnahmen erinnert werden. Sie sollten ihre Betriebssysteme und Software überwachen, um sicherzustellen, dass sie regelmäßig aktualisiert und gepatcht werden. Es ist hilfreich, wenn das Netzwerk mit den bestmöglichen Sicherheitslösungen, wie u.a. Firewalls, Endpoint-Sicherheit, Multifaktor-Authentifizierung (MFA) und Privileged Access Management (PAM), geschützt sind.

Und nicht zuletzt sollte ein effektiver Sicherungs- und Wiederherstellungsplan implementiert sein. Einzelhändler, die über einen zuverlässig funktionierenden Backup- und Wiederherstellungsplan verfügen, sind weniger gefährdet, bei einem Angriff Datenverluste zu erleiden. Zu einem soliden Plan gehören regelmäßige Tests der Sicherungsabbilder, damit etwaige Probleme rechtzeitig identifiziert und behoben werden können.

2. Cyber-Versicherung in Betracht ziehen

Eine Cyber-Versicherung bietet eine Entschädigung für Verluste und Strafen, die durch Cyber-Angriffe verursacht werden. In der heutigen Zeit ist eine solche Versicherung ein Muss für jedes Unternehmen. Der oben zitierte

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Sophos-Bericht stellt fest, dass die meisten Einzelhändler ihre Schutzmaßnahmen derzeit um eine Cyber-Versicherung erweitern. Aber sollten sie noch keine derartige Versicherung haben, wird es immer schwieriger, sie abzuschließen. Cyberangriffe sind inzwischen so häufig und kostspielig, dass sich die Versicherungsgesellschaften langsam zurückziehen. Die Entschädigungen, die sie auszahlen müssen, sind höher als die Prämien, die sie verlangen können. Die Anbieter schränken daher die Zahl der von ihnen abgeschlossenen Cyber-Versicherungspolicen ein und werden bei der Auswahl der Unternehmen, die sie versichern, immer wählerischer.

Viele Unternehmen werden abgewiesen, weil sie die immer strengeren Anforderungen nicht erfüllen. Wenn Unternehmen eine Cyber-Versicherung abschließen möchten, stehen die Chancen für den Abschluss einer Versicherung besser, wenn sie gut über die aktuellen Anforderungen informiert sind. Eine gängige Anforderung sind wirksame Cyber-Sicherheitsmaßnahmen, wie beispielsweise ein solider Plan zur Datensicherung und -wiederherstellung. Dies wird ihnen helfen, die Versicherer davon zu überzeugen, dass ihr Unternehmen kein überproportionales Risiko darstellt.

Einzelhandelsunternehmen sollten, wie andere Unternehmen auch, eine Lösung für die Datensicherung und -wiederherstellung sowie für die unveränderliche Speicherung einsetzen, die Informationen kontinuierlich schützt, indem sie alle 90 Sekunden einen Snapshot erstellt. So können sie ihre Daten auch dann wiederherstellen, wenn Cyberkriminelle diese überschreiben.

3. Auf Zero Trust setzen

Wie andere Unternehmen auch, müssen Einzelhändler sich vor internen und externen Bedrohungen schützen. Sie müssen sicherstellen, dass ihre

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Mitarbeiter Sicherheitsprotokolle befolgen und dass ihre Kunden echte Kunden sind und keine Hacker oder Betrüger. Gleichzeitig müssen sie den Kunden das Einkaufen so einfach wie möglich machen und dabei Kundendaten, wie z. B. Kreditkarteninformationen, bestmöglich schützen.

"Zero Trust" ist eine zunehmend populäre Cyber-Sicherheitsphilosophie, die die Einzelhandelsunternehmen vor Cyberangriffen schützen kann. Zero-Trust geht davon aus, dass alle Benutzer ein potenzielles Risiko darstellen, und gewährt den Benutzern nur die Berechtigungen, die nötig sind, um ihre Aufgaben und Operationen durchzuführen. Mehr nicht. Bei Zero Trust werden nur die Mindestberechtigungen zum richtigen Zeitpunkt gewährt, um eine Aufgabe zu erledigen. Diese Berechtigungen können dann unmittelbar nach Abschluss einer Transaktion wieder entzogen werden.

Zero Trust funktioniert auch bei der Datensicherung, und die gute Nachricht ist, dass die Implementierung für die Datensicherung durch eine einfache Erweiterung der bereits im Netzwerk vorhandenen Sicherheitsmaßnahmen erreicht werden kann. Durch Hinzufügen dieser zusätzlichen Sicherheitsebene können Einzelhandelsunternehmen den Schaden im Falle einer Datenverletzung oder eines Cyberangriffs minimieren. Selbst wenn Cyberkriminelle auf eine Datenbank zugreifen und Benutzernamen sowie Kennwörter in die Hände bekommen, werden sie wahrscheinlich nicht in der Lage sein, diese zusätzliche Verteidigungsschicht zu durchdringen.

Fazit

Einzelhandelsunternehmen bereiten sich jetzt auf das Weihnachtsgeschäft vor. Auch Cyberkriminelle rüsten sich und planen eine Angriffswelle, die vielen Unternehmen das Weihnachtsgeschäft ruinieren kann. Deshalb müssen Unternehmen des Einzelhandels ihre Daten sichern und die persönlichen Informationen ihrer Kunden schützen. Wenn sie die obigen

arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Empfehlungen befolgen, sind sie auf dem besten Weg, genau das zu erreichen.

Unternehmenskontakt
Jock Breitwieser
Arcserve
+1 408.800.5625
jock.breitwieser@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 8081 9546-19
Thilo Christ
+49 8081 9546-17
arcserve@tc-communications.de
www.tc-communications.de