arcserve®
Protect what's priceless.

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

Einzelhändler müssen sich auf Cyberangriffe vorbereiten

Florian Malecki, Vice President International Marketing bei Arcserve

Durch das exponentielle Wachstum beim Online-Shopping sind Einzelhändler zu einem Hauptziel von Cyberkriminellen geworden. Im vergangenen Jahr waren 44 Prozent der Einzelhandelsunternehmen weltweit von einem Ransomware-Angriff betroffen, und viele hatten dadurch einen beträchtlichen finanziellen Schaden. Laut dem aktuellen State of Ransomware in Retail 2021 Report von Sophos betrugen die durchschnittlichen Kosten für die Wiederherstellung nach einem Ransomware-Angriff rund 1,7 Millionen Euro. Zu diesen Kosten gehörten Ausfallzeiten, Personalaufwand, Gerätekosten, Netzwerkkosten, entgangene Geschäftschancen und das Lösegeld, das für die Wiederherstellung der verschlüsselten Daten gezahlt wurde – eine durchschnittliche Zahlung von fast 130.000 Euro.

Kurz vor der Hochsaison am Black Friday bereiten Cyberkriminelle eine neue Angriffswelle vor und für viele Händler bricht eine Zeit an, in der es um alles oder nichts geht. Denn wenn sie mit ihren Sicherheitsvorkehrungen nicht exzellent vorbereitet sind, müssen sie damit rechnen, dass ein Cyberangriff trotz guter Verkäufe einen beträchtlichen Schaden anrichtet. Diese Situation erhöht weiter den Druck auf die Einzelhändler, ihre Daten und Systeme zu sichern und die persönlichen Informationen ihrer Kunden zu schützen.

Die folgenden vier Maßnahmen beschreiben, wie sich Einzelhändler die Cyberkriminellen vom Leib halten und eine profitable Saison erwirtschaften können.

arcserve®
Protect what's priceless.
8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

1: Die richtige Datenspeicherlösung wählen

Einzelhändler müssen eine Vielzahl von Daten verwalten und schützen, von Kundendaten über E-Mail-Adressen bis hin zu Rechnungsinformationen und vielen anderen sensible Daten. Mit der richtigen Datenspeicherlösung können Einzelhändler diese wichtigen Daten schützen, selbst wenn sie Opfer eines Ransomware-Angriffs werden.

Unternehmen sollten sich für eine Lösung mit der Option unveränderlicher Daten entscheiden, die Informationen kontinuierlich schützt, indem sie alle 90 Sekunden Snapshots erstellt. Damit lassen sich Daten auch dann wiederherstellen, wenn sich Ransomware eingeschlichen hat und die Daten überschrieben beziehungsweise verschlüsselt wurden. Mit unveränderlichen Snapshots ist gewährleistet, dass die Daten sicher sind und von jedem beliebigen Wiederherstellungspunkt zurückgespielt werden können.

2: Das schwächste Glied stärken

Neben Firewalls, Endpoint-Schutz, E-Mail-Sicherheit usw. sind auch die Datensicherung und -wiederherstellung wichtige Bestandteile der gesamten IT-Sicherheitslösung. Wenn eine dieser Lösungen nicht korrekt konfiguriert ist oder Sicherheitslücken aufweist, ist dies die schwächste Stelle in der Kette der Schutzfunktionen. Daher gilt es, alle Schutzmaßnahmen in einem Plan zu vereinen und das schwächste Glied zu stärken oder zu eliminieren. Zu diesem Plan gehört auch ein umfassender Sicherungs- und Wiederherstellungsplan. Damit lassen sich die Daten im Katastrophenfall nicht nur schützen, sondern auch in angemessener Zeit wiederherstellen – sowohl bei Cyberangriffen als auch bei vergleichsweise harmlosen Störungen wie Stromausfällen, Naturkatastrophen oder Hardwarefehlern.

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

Der Sicherungs- und Wiederherstellungsplan sollte eine Simulation von Geschäftsunterbrechungen beinhalten, um die Security-Strategie bewerten zu können. Durch regelmäßige Tests der Backup-Images lassen sich potenzielle Probleme bereits vor dem Ernstfall beheben. Einzelhändler, die über einen Wiederherstellungsplan verfügen, sind eher in der Lage, größeren Schaden und dauerhaften Datenverlust zu vermeiden. Mit einem soliden Plan stellen Einzelhändler sicher, dass sie mit ihrem Unternehmen während der wichtigen Black Friday- und Weihnachtssaison erfolgreich sind.

3: Nicht alle Daten sind gleich

Data Tiering ist für Einzelhändler von entscheidender Bedeutung. Bei diesem Ansatz werden weniger häufig genutzte oder weniger wichtige Daten aus Kosten-, Wiederherstellungs- und Verfügbarkeitsgründen auf niedrigere Speicherebenen verschoben. Es ist wichtig, mit Richtlinien zu definieren, welche Daten wichtig sind, wie schnell der Zugriff auf welche Art von Daten erfolgen muss und wie schnell sie im Störfall wiederhergestellt werden müssen. Wenn ein Händler beispielsweise für eine begrenzte Zeit keinen Zugriff auf vergangene Quartalszahlen hat, schadet das dem laufenden Umsatz nicht. Ist hingegen durch einen Hackerangriff die Preisliste kompromittiert oder sind Lieferadressen nicht zugänglich, kann dies unmittelbare und enorme Auswirkungen auf das laufende Geschäft haben. Deshalb ist es wichtig, Daten nach Prioritäten zu ordnen und den Geschäftswert der einzelnen Daten zu verstehen.

4: Daten in der Cloud schützen

Viele Einzelhändler arbeiten mit Cloud-Lösungen und sollten sich im Klaren darüber sein, dass sie gemeinsam mit ihrem Cloud-Anbieter für die Sicherheit verantwortlich sind. Dabei haben beide Seiten unterschiedliche Verantwortungsbereiche. Der Einzelhändler ist in erster Linie für den Schutz seiner Daten in der Cloud

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

verantwortlich, nicht der Dienstanbieter. Anbieter wie Microsoft Azure, Google Cloud Platform und AWS sichern in der Regel die Kerninfrastruktur. Die Sicherung der Daten liegt klar in der Verantwortung des Kunden. Einzelhändler, die sich dieser einfachen Tatsache nicht bewusst sind, haben ein viel höheres Risiko, einen Datenverlust zu erleiden. Sie sollten sicherstellen, dass sie passende Schutzmaßnahmen ergriffen haben, um Cloud-basierte Daten zu sichern. Auch für Backups von Daten in der Cloud sollten sie regelmäßig Tests durchführen und prüfen, ob die Daten im Notfall wiederhergestellt werden können.

Selbst die beste Präventionstechnologie schützt Unternehmen nicht vor Cyberangriffen und den daraus folgenden finanziellen Schäden. Befolgen Unternehmen aber die vier oben genannten Maßnahmen, ist ihr Risiko fuer Datenverlust durch einen Angriff deutlich reduziert, da Cyberkriminelle keine Chance haben, die wertvollen Daten unwiederbringlich zu entwenden oder zu zerstören.

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