Ransomware-Schutz für Remote-Büros und Außenstellen

Es ist selten, dass ein Unternehmen seine Daten nur in einem einzigen zentralen Rechenzentrum organisiert. Insbesondere in Wachstumsphasen ist es typisch, dass ROBO-Umgebungen (Remote Office/Branch Office) eingerichtet werden, um die Expansion zu realisieren. Diese Umgebungen vor Ransomware zu schützen ist besonders schwierig, da sich Außenstellen oft weit entfernt vom primären Rechenzentrum befinden und nur selten über genug technisches IT-Personal verfügen. Doch auch diese Dependancen müssen vor Ransomware geschützt sein. Florian Malecki, Senior Director International Product Marketing bei Arcserve, gibt vier Tipps zum Schutz vor Ransomware selbst in entlegensten Unternehmenseinheiten.

1. Auf Ransomware-Prävention fokussieren

Zunächst müssen auch in den Außenstellen grundlegende Vorkehrungen gegen Ransomware getroffen werden. Genau wie in der Unternehmenszentrale sollten auch hier Firewalls, Spamfilter, Antivirenprogramme und Antimalware-Tools verwendet werden, wobei die Software stets auf dem neuesten Stand sein sollte. Auch der Abschluss einer Ransomware-Versicherung inklusive eines Versicherungsschutzes für die Außenstellen kann in Erwägung gezogen werden. Am wichtigsten ist aber, dass die Mitarbeiter die Bedrohung durch Ransomware verstehen. Sie sollten geschult werden, damit sie beispielsweise riskante E-Mails oder Phishing-Attacken erkennen und wissen, welche Schritte im Falle eine Infizierung zu unternehmen sind.

2. Backup- und Wiederherstellungsstrategie für Remote-Standorte entwickeln

Es ist vielleicht nicht immer möglich, Remote-Netzwerke vor einem Ransomware-Befall zu schützen. Allerdings kann eine robuste Backup- und Wiederherstellungsstrategie den Betrieb aufrechterhalten, auch wenn Systeme verschlüsselt werden. Für jedes Netzwerk ist es wichtig, zunächst die Wiederherstellungsziele festzulegen. Für alle Standorte sollte definiert sein, wie viel Datenverlust toleriert werden kann (Recovery Point Objective) und wie viel

Ausfallzeit akzeptabel ist (Recovery Time Objective). Die jeweiligen Lösungen müssen in der Lage sein, diese Ziele zu erfüllen, um Daten effektiv zu schützen.

3. Den generellen Sinn eines ROBO-Datenschutzes verstehen

Sobald die Ziele festgelegt sind, gilt es, die Voraussetzungen zu definieren, die die Lösung erfüllen muss. Abgesehen von den Wiederherstellungszielen sollten drei wesentliche Punkte für Außenstellen berücksichtigt werden:

- **Flexibles Backup:** Die Lösung sollte virtuelle und physische Maschinen sichern. Die Speicherung der Backups sollte lokal erfolgen und zugleich einfach in die Cloud replizierbar sein.
- **Wiederherstellungsoptionen:** Je nach Schweregrad des Vorfalls sollte es möglich sein, die Wiederherstellung lokal am Standort oder aus der Cloud durchzuführen. Es ist wichtig, flexible und schnelle Wiederherstellungsoptionen zu haben, um kritische Ziele zu erreichen.
- **Fernverwaltung:** Möglicherweise gibt es mehrere Niederlassungen mit unterschiedlichen IT-Umgebungen und Wiederherstellungszielen. Die Lösung sollte eine effektive Verwaltung mit individuellen Zielen der einzelnen Standorte ermöglichen. Dabei ist es wichtig, über ein robustes Set von Management-Tools zu verfügen, auf das IT-Administratoren ortsunabhängig zugreifen können. Dieses System sollte es zulassen, per Fernzugriff verschiedene Richtlinien an verschiedenen Standorten zu implementieren und Zweigstellen wiederherzustellen.

4. Appliances für Disaster Recovery as a Service (DRaaS) verwenden

Weil Außenstellen oftmals nicht über die Ressourcen oder das technische Personal verfügen, um Server oder komplexere Umgebungen zu verwalten, verwenden viele Administratoren Appliances für das Backup und die Wiederherstellung. Sobald die Appliance mit dem Internet verbunden ist, können IT-Spezialisten die Daten aus der Ferne schützen, indem sie Backup-Zeitpläne und Aufbewahrungsrichtlinien festlegen. Im Falle eines Hardwareausfalls oder eines Security-Vorfalls können sie die Appliance für ein sofortiges Failover verwenden. Und da sich Daten von einer Appliance in die Cloud replizieren lassen, kann sogar die gesamte Zweigstelle in die Cloud verlagert werden.

Datenverlust durch Ransomware verhindern

ROBO-Umgebungen sind besonders anfällig für Datenverlust und Ausfallzeiten, da selten technisches Personal vor Ort ist, um die Systeme schnell wiederherzustellen. Hinzu kommt die wachsende Bedrohung durch Ransomware. Backup- und Wiederherstellungs-Appliances erleichtern es Administratoren, Datenverluste durch Ausfälle oder Ransomware zu verhindern, selbst wenn sie nicht vor Ort sind.

Folgen Sie uns auf Twitter, LinkedIn und Facebook oder lesen Sie die neuesten Artikel zum Thema Datensicherung und Datenwiederherstellung in unserem Blog.

###

Über StorageCraft, ein Unternehmen von Arcserve

StorageCraft, ein Unternehmen von Arcserve, bietet das breiteste Spektrum an Best-in-Class-Lösungen für die Verwaltung, den Schutz und die Wiederherstellung aller Daten, unabhängig von Größe, Standort oder Komplexität. Das einheitliche Lösungsportfolio des Unternehmens, bestehend aus Arcserve- und StorageCraft-Technologie, beseitigt die Komplexität und bietet gleichzeitig erstklassigen, kosteneffizienten, agilen und massiv skalierbaren Datenschutz und Sicherheit für alle Datenumgebungen. Dazu gehören On-Premise-, Off-Premise- (einschließlich DRaaS, BaaS und Cloud-to-Cloud), Hyper-Converged- und Edge-Infrastrukturen. Mit über Jahrzehnte preisgekrönten Technologielösungen und einem kontinuierlichen Fokus auf Innovation können Partner und Kunden sicher sein, dass sie stets auf Next-Generation Datenumgebungen und Infrastrukturen aufbauen. Als ein Unternehmen von Arcserve ist StorageCraft zu 100% auf den Channel ausgerichtet und in über 150 Ländern vertreten.
Weitere Informationen finden Sie unter storagecraft.com/de.

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
storagecraft@tc-communications.de
www.tc-communications.de