



Unveränderlicher Speicher: zentraler Bestandteil jeder IT-Sicherheitsstrategie

Florian Malecki, Vice President – International Marketing, Arcserve

In einer kürzlich von Dimensional Research durchgeführten Umfrage gaben 96 Prozent der IT-Entscheidungssträger an, dass sie sich über Ransomware-Angriffe Sorgen machen. Danach sind nur 20 Prozent der Chief Information Security Officers sehr zuversichtlich, dass sich sein Unternehmen von einem Ransomware-Angriff erholen kann. Da die Angreifer zunehmend trickreich vorgehen, haben CISOs den Schutz ihres Unternehmens mit Präventionslösungen wie Firewalls, Identitäts- und Zugriffsmanagement und Passwörtern verstärkt. Eine Herausforderung aber bleibt bestehen: der sichere Datenspeicher.

Die Bedeutung des unveränderlichen Speichers

Wenn ein Unternehmen Opfer eines Cyberangriffs wird, ist jede Sekunde Ausfallzeit geschäftsschädigend und teuer. Laut [Gartner](#) kann der finanzielle Verlust rund 5.000 Euro (5.600 US-Dollar) pro Minute betragen. Präventionsmaßnahmen für die Sicherheit sind deshalb unerlässlich. CISOs benötigen dafür zuverlässige Schutzmechanismen, um das primäre Ziel der Datensicherheit und -verfügbarkeit zu erreichen. Wie gut das gelingt, hängt auch von der Datenspeicherung und -sicherung ab.

Bei einem Cyberangriff sind sowohl Speicher- als auch Backup-Lösungen Hauptziele der Hacker. Daher sollten nicht nur die Prävention mit Security-Lösungen, sondern auch die Speicherlösungen unter Berücksichtigung der Richtlinien für die Datensicherheit oberste Priorität haben. Eine besondere Rolle spielen hierbei Backup- und unveränderlicher Speicher. Sie schützen die Daten im Falle eines Angriffs – oder einer anderen Katastrophe – und bilden die letzte Verteidigungslinie für die Sicherheit und Verfügbarkeit der Daten.





Unveränderlichkeit der Daten für optimale Sicherheit

Die Umsetzung einer ganzheitlichen Datensicherheit mit Hilfe von unveränderlichem Speicher ist von entscheidender Bedeutung für die Resilienz. Kein Unternehmen kann Cyberangriffe vollkommen ausschließen. Allerdings können die negativen Auswirkungen weitgehend neutralisiert und damit die wichtige Geschäftskontinuität sichergestellt werden.

Das Problem ist, dass Angreifer sowohl die Dateien als auch die Wiederherstellungspunkte von Backups auf einem klassischen Speichermedium verschlüsseln können. Der wichtigste Schritt, um sich vor den Folgen einer Ransomware zu schützen, sind daher regelmäßige Backups auf unveränderlichem Speicher. Ein unveränderliches Snapshot ist eine Kopie von Daten, die weder von Ransomware, noch von einem Benutzer geändert oder gelöscht werden kann. Damit ist ein Unternehmen in der Lage, Daten nach einer Beschädigung oder Löschung, einem Ransomware-Angriff oder anderen Problemen sicher und schnell wiederherzustellen.

Ein weiterer Vorteil besteht darin, dass Benutzer verlorene oder beschädigte Daten sogar selbständig im Windows Explorer oder im Apple Finder wiederherstellen können. Es sind keine Restore-Operationen aus den Backups des Vortags seitens des IT-Personals nötig.

Arcserve OneXafe bietet genau das und ist eine effiziente und unveränderliche Datenspeicherlösung. Zudem nutzt die Lösung die Vorteile einer Inline-Deduplizierung und Datenkomprimierung, um den Bedarf an das Speichervolumen zu reduzieren.





Fazit: Strategie jetzt anpassen

CISOs sollten nicht nur ihre Teams hinsichtlich potenzieller Sicherheitsrisiken sensibilisieren. In Unternehmen geht es auch darum, das Bewusstsein für die Bedeutung des Datenspeichers zu schärfen. Richtlinien für die Datensicherheit beschränken sich oft nur auf das Wesentliche und sind für die heutige Gefahrenlage meist nicht robust genug.

Verschlüsselte oder gestohlenen Daten sind für Cyberkriminelle eine enorme Geldquelle. Daher stellt sich viel weniger die Frage, ob man Opfer einer Ransomware-Attacke wird, sondern viel mehr, wann dies geschieht. Unternehmen, die noch nicht auf unveränderlichem Speicher setzen und bisher noch kein Opfer von Ransomware waren, hatten einfach nur Glück. Daher sollte die Strategie für Daten- und Informationssicherheit spätestens jetzt mit einem ganzheitlichen Ansatz und mit unveränderlichem Speicher angepasst werden.

Folgen Sie Arcserve auf [LinkedIn](#) oder [Twitter](#) und lesen Sie unsere neuesten Artikel zum Thema Datenschutz und -management im Arcserve [Blog](#).

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