arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

Cyberrisiko senken: 5 Tipps für ein sicheres Backup und Wiederherstellen von Daten

Von Sven Richter, Marketing Manager DACH bei Arcserve

Eine effektive Datensicherheitsstrategie für Unternehmen besteht nicht aus isolierten Sicherheitslösungen, sondern aus einem abgestimmten Ökosystem. Dazu gehören klassische Security, Identitäts- und Zugriffsmanagement, Authentifizierungsverfahren, Zero-Trust-Lösungen und Schulungen der Mitarbeiter. Einen besonderen Stellenwert nehmen allerdings die Datensicherung und Wiederherstellung ein, denn sie ist die Versicherung, um die Business Continuity auch im Falle eines Angriffs zu gewährleisten.

Die wichtigen Rollen von Backup und Wiederherstellung zeigen sich nicht zuletzt in der neuesten NIS-2-Releglung, die ab Oktober dieses Jahres die Cyber-Resilienz von vielen Unternehmen und Organisationen verbessern soll. Dafür müssen die Backup-Strategien überprüft werden und es muss sichergestellt sein, dass sie den verschärften Vorschriften entsprechen. Wesentlich sind die Implementierung sicherer, zuverlässiger Backup- und Wiederherstellungsverfahren, eine regelmäßige Überprüfung der Backup-Integrität und die Gewährleistung, dass die gesicherten Daten vor unbefugtem Zugriff – vor allem vor Cyberkriminellen und Ransomware – geschützt sind.

Priorität auf Business Continuity

Ganz gleich welche Backup-Optionen gewählt werden, letztlich geht es darum, die Daten und IT-Systeme im Ernstfall zuverlässig und schnell wiederherzustellen. Daraus folgen zwei Ziele: eine maßgebliche Reduzierung des Risikos und eine zuverlässige Business Continuity, die unabhängig von der Art und Intensität des Katastrophenfalls funktioniert. Um diese zu erreichen, sollten Unternehmen und Organisationen fünf wichtige Aspekte beachten:

arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

1. **Die Fähigkeit der Wiederherstellung**

Eine Datensicherung ist nur dann gut, wenn die Daten wiederhergestellt werden können. Dazu müssen Unternehmen, Organisationen oder Dienstleister die Gültigkeit und den Zustand der Daten überprüfen. Die Überwachung von Backups und die Validierung von Logs oder Berichten stellt sicher, dass die Backups durchgeführt wurden und dass die Widerherstellbarkeit der Daten gesichert ist. Zudem liefern Logs und Berichte wertvolle Erkenntnisse darüber, ob bösartige Zugriffsversuche stattfanden, damit diese frühzeitig gestoppt werden können.

2. **Dynamische Skalierung**

Ein Unternehmen oder eine Organisation kann morgen schon andere Anforderungen an das Backup oder die Business Continuity haben als heute. Die Marktkonsolidierung, das exponentielle Datenwachstum und viele weitere Aspekte ändern die Bedürfnisse. Daher sollten Lösungen für Backup und Wiederherstellung nicht nur robust im Sinne der Cyber-Resilienz sein, sondern sich auch flexibel und dynamisch an die Geschäftsentwicklung anpassen.

3. **Cloud ja, Aber bitte sicher**

Die Cloud ist für die Datensicherung eine bewährte Lösung. Um allerdings Cyber-Resilienz zu erreichen, gilt es einige Aspekte zu beachten. Dazu gehören eine Cloud-Strategie für das Offsite-Offloading oder die Replikation in die Cloud. Zudem ist es wichtig, den passenden Cloud-Anbieter zu wählen. Neben der Wahl des wirtschaftlich passenden Anbieters mit einem adäquaten Set an Cloud-Backup-Lösungen ist immer auch die Compliance von entscheidender Bedeutung. Ein guter Ansatz ist es, dass bei einer Cloud-Backup-Strategie das Unternehmen oder die Organisation die Kontrolle behält. Dazu gehört auch das 3-2-1-1-Verfahren (3 Kopien der Daten, 2 verschiedene Medien, 1 offsite und 1 auf unveränderlichem Speicher).

4. **Letzte Verteidigungslinie: Unveränderlicher Speicher**

arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

Die Unveränderlichkeit von gesicherten Backup-Daten ist ein enorm wichtiger Aspekt einer Cyber-Resilienz-Strategie. Sie bietet zusätzlichen Schutz gegen böswillige Aktivitäten und Angriffe. Egal mit welcher Technologie der unveränderliche Speicher realisiert wird – beispielsweise mit unveränderlichen Objekt-basierten Snapshots, mit einer WORM-Technologie oder mit Hilfe eines Air-Gap-Verfahrens – ist es von entscheidender Bedeutung, dass keine unbefugten Personen oder Malware, weder von intern noch von extern, Zugang zu den Backup-Daten haben.

5. Bewährte Best Practices

Die Umsetzung bewährter Praktiken ist eine gute Strategie, um Business Continuity im Katastrophenfall zu wahren. Die Beachtung der „Best Practices" stellt nicht nur sicher, dass die Daten angemessen geschützt sind, sondern gibt Unternehmen und Organisationen auch die Gewissheit, dass wiederherstellbare Daten für die Business Continuity verfügbar sind.

Wenn diese fünf Aspekte umgesetzt und erreicht sind, kann von einer wirksamen Cyber-Resilienz für das Backup und die Wiederherstellung ausgegangen werden – die nebenbei auch das Einhalten aktueller Regelwerke, wie beispielsweise NIS-2, maßgeblich unterstützt.

Folgen Sie Arcserve auf LinkedIn oder X und lesen Sie unsere neuesten Artikel zum Thema Datenschutz und -management im Arcserve Blog.

###

arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

Über Arcserve

Arcserve ist der Pionier für einheitliche Daten-Resilienz-Lösungen. Seit mehr als 40 Jahren vertrauen fast 150.000 Kunden und über 30.000 Vertriebspartner in 150 Ländern auf Arcserve, um ihre Datenresilienz zu stärken, verlorene Daten wiederherzustellen und die Kontinuität ihres Geschäftsbetriebs zu gewährleisten. Mit einem einheitlichen Ansatz für Datensicherung und -wiederherstellung, erstklassigem technischen Support und dem niedrigen Total Cost of Ownership (TCO) hilft Arcserve Unternehmen, ihre Daten zu verwalten, zu schützen und - was am wichtigsten ist - in jeder Situation wiederherzustellen.

Erfahren Sie mehr unter arcserve.com und folgen Sie Arcserve auf Twitter oder LinkedIn.

Unternehmenskontakt

Jock Breitwieser

Arcserve

+1 408.800.5625

jock.breitwieser@arcserve.com

Agenturkontakt

TC Communications

Arno Lücht

+49 157 524 437 49

Thilo Christ

+49 171 622 06 10

arcserve@tc-communications.de