



In hybriden IT-Landschaften ist flexible Disaster Recovery wichtiger denn je

*Eine anpassungsfähige Datenwiederherstellung sollte elementarer
Bestandteil von Datenschutzkonzepten sein*

Eine von [Arcserve](#) beauftragte [unabhängige Befragung](#) unter IT-Führungskräften ergab, dass 80 Prozent schon einmal von Ransomware betroffen waren. Während 82 Prozent der Betroffenen angaben, dass sie den Schaden innerhalb von 48 Stunden beheben konnten, war dazu knapp ein Fünftel nicht in der Lage. Problematisch ist auch, dass bis zu 30 Prozent der Daten bei einem erfolgreichen Ransomware-Angriff nicht wiederhergestellt werden konnten.

Das ist nicht nur ärgerlich und teuer, sondern auch riskant. So werden die durchschnittlichen Ausfallkosten bei großen Unternehmen auf [9.000 US-Dollar](#) pro Minute geschätzt. [60 Prozent](#) der kleineren Unternehmen unterliegen zudem der Gefahr, innerhalb von sechs Monaten nach einer Datenschutzverletzung oder einem Cyberangriff den Betrieb einstellen zu müssen. Prävention und schnelle Wiederherstellung die einzigen Möglichkeiten, die Kosten und Folgen einer solchen Katastrophe zu minimieren.

Die Welt ist hybrid

Laut Statista wird der Hybrid-Cloud-Markt 2027 ein Volumen von [262 Milliarden US-Dollar](#) erreichen und der Markt für Rechenzentren bis 2029 auf 212 Milliarden US-Dollar wachsen. Der Grund: Sowohl lokale und als auch Cloud-Umgebungen haben ihre Vorteile und werden zunehmend nebeneinander betrieben. Schutz bieten zuverlässige Disaster Recovery (DR)-Lösungen, wie [Arcserve Unified Data Protection \(UDP\) 10](#), die eine flexible und kostengünstige Datenwiederherstellung ermöglichen .



Darauf kommt es bei der Umsetzung einer Datenschutzstrategie für hybride IT-Umgebungen an:

1. Effiziente Datenwiederherstellung

Mehrere Datenquellen und Backup-Ziele: Wichtig ist, dass die Data-Recovery-Lösung eine breite Palette von Datenquellen und Backup-Zielen, sowohl vor Ort als auch in der Cloud, unterstützt.

Flexible Bereitstellungsoptionen: Es hilft, wenn die die DR-Software sowohl als Standalone-Lösung aber auch vorinstalliert in einer Appliance erworben werden.

Vielseitige Lizenzierungsoptionen: Um eine Wiederherstellungslösung skalieren zu können, sollte darauf geachtet werden, dass sich das Lizenzierungssystem der Recovery-Lösung an unterschiedliche Umgebungen anpassen lässt und nur die Lizenzen bezahlt werden, die wirklich genutzt werden.

2. Verbesserte Datensicherung, beschleunigte Wiederherstellung

Security Scan: Mehr Sicherheit entsteht, wenn Backup-Dateien vor der Wiederherstellung auf Malware gescannt werden. So lässt sich die erneute Infektion des Systems verhindern und Business Continuity bestmöglich gewährleisten. Erfolgt ein solcher Prozess in Echtzeit, ist das für die Qualität des Backups umso besser.

Virtueller Ad-hoc-Standby: Wer sowohl die Komplexität einer Datenwiederherstellung als auch die damit verbundenen Kosten reduzieren möchte tun gut daran, auf ein virtuelles Ad-hoc-Standby zu setzen. Damit lassen sich VMs nach Bedarf initiieren und die Business Continuity optimal unterstützen.



One-to-Many-Replikation: Eine in die Wiederherstellungssoftware integrierten One-to-Many-Replikation versetzt Unternehmen in die Lage, die Replikation von Backup-Daten gleichzeitig an mehreren Standorte durchzuführen. Das verringert das Risiko eines Single Point of Failure und bietet zusätzlichen Schutz im Falle standortspezifischer Katastrophen.

Flexible Datenwiederherstellung in hybriden Landschaften

Moderne Wiederherstellungsplattformen sind darauf ausgerichtet, komplexe IT-Landschaften, die zunehmend unterschiedliche Datenquellen, Backup-Standorte und Infrastrukturen umfassen, abzusichern. Sie unterstützen sowohl lokale als auch in Cloud-Umgebungen gespeicherte Daten und bietet flexible Preis- und Bereitstellungsoptionen. Mit diesen DR-Lösungen lassen sich die wachsenden Anforderungen an die Verwaltung und den Schutz standortübergreifender Umgebungen bewältigen und Unternehmensdaten vor den zunehmenden Ransomware-Bedrohungen zu schützen.

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

###



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

Alex Plotnikov
Arcserve
alex.plotnikov@arcserve.com

Agenturkontakt

TC Communications
Arno Lücht
+49 157 524 437 49
Thilo Christ
+49 171 622 06 10
arcserve@tc-communications.de