



## **Backup Awareness Monat: Was Unternehmen tun müssen, um ihre Daten zu schützen**

Der „Backup Awareness Month“ im Juni rückt das Thema Backup in vielen Unternehmen in den Vordergrund. Dafür gibt es gute Gründe, denn laut IT Governance wurden bis Mai dieses Jahres 9.478 öffentlich bekannt gewordene Datenschutzverletzungen und Cyberangriffe verzeichnet. Dabei wurden über [35 Milliarden](#) Datensätze geknackt. Auch der Arcserve-Partner Sophos berichtet in seinem aktuellen [Ransomware-Report](#), dass 59 Prozent der Unternehmen im vergangenen Jahr von Ransomware betroffen waren. Die Bedrohungslage ist also nach wie vor kritisch.

Unabhängig von der Größe und der Branchenzugehörigkeit eines Unternehmens, stellen Backups die einzige Möglichkeit dar, um sicherzustellen, dass Daten geschützt bleiben, wenn sie von Ransomware verschlüsselt werden, eine Sicherheitslücke entsteht oder die Daten versehentlich gelöscht werden.

### **Backup sollte oberste Priorität haben**

Für ein solides Backup haben sich mittlerweile mehrere Verfahren in Unternehmen etabliert. Die Sicherung von Unternehmensdaten beginnt mit einer [3-2-1-1-Strategie](#). Diese vier Grundpfeiler beschreiben das Aufbewahren von drei Kopien der Backup-Daten auf zwei verschiedenen Medien (z. B. Band oder Festplatte), wobei eine Kopie extern gespeichert wird (an einem anderen Ort oder in der Cloud). Die letzte „1“ ist im Kampf gegen die Cyberkriminalität entscheidend und steht für Unveränderbarkeit beziehungsweise Immutability. Diese Kopie der Datensicherung kann beispielsweise in einem WORM-Format (Write-Once-Read-Many-Times) oder auf einem Speicher, der nicht verändert



oder gelöscht werden kann, gespeichert werden. Erst damit ist sichergestellt, dass Cyberkriminelle die Backup-Daten nicht verschlüsseln können und eine rasche Wiederherstellung der Systeme erfolgen kann.

## **Unveränderlichkeit der Daten**

Für einen soliden Daten-Backup- und Disaster Recovery-Plan ist auch die Unveränderlichkeit der Daten unabdingbar. [Sophos beispielsweise berichtet](#), dass bei 94 Prozent der Unternehmen, die letztes Jahr von Ransomware betroffen waren, Cyberkriminelle während des Angriffs auch versucht haben, die Backups zu hacken. In den Bereichen staatliche und kommunale Verwaltung, Medien, Freizeit und Unterhaltung sind es sogar 99 Prozent.

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. Entscheidend ist, dass keine unbefugten Personen oder Malware, weder von intern noch von extern, Zugang zu den Backup-Daten haben.

## **Disaster-Recovery-Plan entwickeln und aktualisieren**

Backups nutzen Unternehmen gar nichts, wenn sie keine Möglichkeit haben, die darin gesicherten Daten wiederherzustellen. Deshalb sollten Unternehmen ihren Disaster-Recovery-Plan in regelmäßigen Abständen überprüfen, beziehungsweise einen Plan erstellen, sollte dieser noch nicht vorliegen. Für die Erstellung eines Disaster-Recovery-Plans hilft diese [Schritt-für-Schritt-Anleitung](#).



## **In passende Backup-Technologien investieren**

Jedes Unternehmen ist einzigartig und hat spezifische Anforderungen in Bezug darauf, wie lange es sich das Unternehmen leisten kann, keinen Zugriff auf seine Daten zu haben (Recovery Time Objective) und wie viele Daten es eventuell verlieren könnte (Recovery Point Objective). Durch die Zusammenarbeit mit einem fachkundigen Technologiepartner erhalten Unternehmen Zugang zur benötigten der Erfahrung und Beratung, um die effektivsten Technologien und Lösungen in Bezug auf Backup und Disaster Recovery für Ihr Unternehmen auszuwählen.

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](https://arcserve.com) und folgen Sie Arcserve auf [Twitter](#) oder [LinkedIn](#).

# arcserve®

Protect what's **priceless.**

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



## **Unternehmenskontakt**

Alex Plotnikov

Arcserve

[alex.plotnikov@arcserve.com](mailto: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](mailto:arcserve@tc-communications.de)