

Verlagern Unternehmen ihre Daten in die Cloud, geben sie damit nicht automatisch die Verantwortung für die Sicherung dieser Daten ab. Das sollte sich mittlerweile herumgesprochen haben. Doch noch immer gibt es in der Cloud bisweilen Backup-Lücken, unter anderem weil Verfügbarkeit und Backup verwechselt werden … | VON SEBASTIAN THEILE



Bildr. Dell

**Über den Autor**

Sebastian Theile ist Data Protection Solutions Software Sales Specialist bei Dell Technologies Deutschland



KOMMENTAR:

# Wer kümmert sich eigentlich ums **Backup von Daten in der Cloud?**

Klar, der Cloud-Anbieter baut seine Infrastrukturen redundant auf und repliziert Daten oder Workloads. Dabei geht es ihm allerdings allein um die Verfügbarkeit – also darum, daß sein Cloud-Service auch dann noch funktioniert, wenn ein System ausfällt oder gestört ist. Unternehmen bekommen davon in der Regel nichts mit und können wie gewohnt mit ihren Daten arbeiten.

Werden diese Daten versehentlich gelöscht, von Cyberkriminellen manipuliert oder von einer Ransomware verschlüsselt, kann der Cloud-Anbieter nicht weiterhelfen. Er besitzt schlicht kein klassisches Backup, das er wieder einspielen könnte, weil dies nicht in seiner Verantwortung liegt.

Das, was an Daten vernichtet oder verändert wurde, findet sich genau in der Form auch in seinen Replikationen wieder, damit er bei Problemen mit einem System unterbrechungsfrei auf ein anderes umschalten kann. Die Sicherung der eigenen Daten obliegt allein dem Unternehmen selbst, und zwar immer – unabhängig davon, ob es sich um IaaS, PaaS oder SaaS handelt.

Vor allem bei SaaS wähnen sich manche Unternehmen nicht in der Pflicht, weil sich der Cloud-Anbieter hier um eigentlich fast alles kümmert, von der Verwaltung der Systeme über die Plattformen bis hin zu den Anwendungen. Die Datensicherung ist dabei aber, wie übrigens auch die Verwaltung von Accounts und Berechtigungen, gemäß dem Prinzip der geteilten Verantwortung (Shared Responsibility) außen vor. Hinzu kommt, dass SaaS-Anwendungen beim Backup nicht selten übersehen werden, wenn ihre Einführung von Fachbereichen vorangetrieben wird, die anschließend die Zugänge und Berechtigungen vergeben. Ein solches Vorgehen mag pragmatisch erscheinen, schafft aber blinde Flecken für die IT-Abteilung.

Letztlich müssen Unternehmen jegliche Cloud-Services in ihre Backup-Strategien einbeziehen und genau prüfen, wie sie dort gespeicherte Daten zuverläßig sichern und wiederherstellen können. Dabei sollten sie insbesondere bei den Backup-Funktionen, die zu einigen Cloud-Angeboten gehören, die Kosten nicht aus dem Blick verlieren, denn abhängig von den Datenmengen, der Häufigkeit der Sicherungen oder den Wiederherstellungsoptionen kann es im Laufe der Zeit durchaus teuer werden. Zudem droht schnell ein Wildwuchs an Backup-Lösungen, der viel Aufwand verursacht und keine konsistenten Richtlinien aufweist, wenn jeder Cloud-Service über eigene Funktionen gesichert wird. Besser sind in der Regel zentralisierte Ansätze.

Diese erleichtern es darüber hinaus meist auch, Sicherungsprozesse zu dokumentieren und Backups in einer anderen Umgebung zu speichern, sodaß sie von den Produktivdaten getrennt sind. Für echte Resilienz gegenüber Cyberattacken ist das eine Grundvoraussetzung, denn wenn die Datensicherungen ebenso wie Produktivdaten manipuliert oder verschlüsselt werden, sind sie schlußendlich wertlos. <<

*Mehr unter:*
***https://www.delltechnologies.com/de-de/blog/***



THE FUTURE OF BUILDING

MESSE MÜNCHEN





BAU 2027

11.–15. Januar 2027
Messe München

Weltleitmesse für Architektur, Materialien, Systeme

bau-muenchen.com

MEHR ERFAHREN