„Ihre Daten in der Cloud sind sicher“ ... Aber sind Sie sicher?
Vier Schritte zum Schutz von Daten vor Katastrophen in der Cloud

Von Florian Malecki, Senior Director, International Product Marketing bei Arcserve

Sind Daten wirklich sicher, wenn sie in die Cloud verlagert werden? Der Brand im OVHcloud-Rechenzentrum in Frankreich am 10. März 2021 zeigt, dass dies nicht immer der Fall ist. Die Feuerkatastrophe hatte für viele Unternehmen ernstzunehmende Folgen und betraf neben dem Verlust von Daten auch den Ausfall von Applikationen, beispielsweise Webseiten von Regierungsbehörden, E-Commerce-Unternehmen oder Banken. Die bittere Erkenntnis aus diesem Vorfall: Während einige der Daten gesichert und gerettet wurden, gingen viele für immer verloren.

Nach wie vor nehmen viele Unternehmen irrtümlicherweise an, dass ihre Daten in der Cloud von ihrem Cloud-Anbieter gesichert und sogar wiederhergestellt werden. Eine aktuelle Umfrage StorageCraft, einem Arcserve Unternehmen, bestätigt dies: Global glauben 44 Prozent der Befragten, dass der Schutz und die Wiederherstellung von Daten in Public Clouds die Aufgabe des Cloud-Anbieters ist. In Deutschland sind sogar 54 Prozent der Umfrage-teilnehmer dieser Meinung – ein fataler Irrtum, denn meist ist dies nicht der Fall.
Daraus ergibt sich die logische Frage, wie es zu dieser Fehleinschätzung kommt. Ein Grund dafür dürfte die weitverbreitete Annahme sein, dass Cloud-Dienste, die heutzutage zahlreich und unkompliziert zur Verfügung stehen, auch sicher und katastrophenfrei sind. Eine einfache Analogie zeigt, wie gefährlich dieser Irrtum ist. Fahrdienste wie Taxis sind

ebenfalls weit verbreitet und einfach zu nutzen. Grundsätzlich schützen die Qualifikation des Fahrers und auch die Technologie des Fahrzeugs den Passagier. Auch um den Kauf von Benzin oder die Wartung des Fahrzeugs muss er sich nicht kümmern. Vor einem Verkehrsunfall ist der Fahrgast jedoch nicht gefeit. Um in diesem Fall geschützt zu sein, muss er selbst handeln und den Sicherheitsgurt während der gesamten Fahrt angelegt haben. Ein großer Teil der Sicherheit des Passagiers liegt also in seiner eignen Verantwortung. Der Sicherheitsgurt ist das Äquivalent zu dem, was viele Cloud-Kunden vergessen: die Absicherung ihrer Daten beim Cloud-Dienstleister.

Mit nur vier grundsätzlichen Regeln lassen sich Missverständnisse vermeiden und Daten in der Cloud wirksam schützen – selbst wenn der Cloud-Anbieter von einer Katastrophe überrascht wird.

1. Wer sich ausschließlich auf andere verlässt, ist verlassen

Bei der Nutzung der Cloud sollten sich Unternehmen darüber im Klaren sein, dass die Verantwortung für die Sicherheit zwischen dem Cloud-Anwender und dem Anbieter geteilt ist. Der Kunde beziehungsweise Anwender ist in erster Linie für den Schutz der Daten verantwortlich, nicht der Service-Provider.

Führende Anbieter wie AWS, Microsoft Azure oder Google Cloud Platform sehen in der Regel die Kerninfrastruktur und -dienste in ihrer Verantwortung. Aber wenn es um die Sicherung von Betriebssystemen, Plattformen und Daten geht, liegt die Pflicht ganz klar in den Händen der Kunden. Unternehmen, die diese einfache Tatsache übersehen oder bewusst ignorieren, haben ein viel höheres Risiko, Datenverluste zu erleiden.

Beispielsweise stellt Microsoft in seinen Office-365-Geschäftsbedingungen klar, dass keine Verantwortung für Daten übernommen wird. Es liegt in der Verantwortung des Kunden beziehungsweise Anwenders, seine Daten zu verwalten und zu schützen. Zwar sichert Microsoft die Daten für 30 Tage. Jedoch hat der Anwender keine Kontrolle über die Verfahren oder die Qualität und nach den 30 Tagen gibt der Anbieter jegliche Verantwortung ab. Aus diesem Grund ist es ratsam, Daten eigenständig mithilfe von geeigneten Backup-Restore- beziehungsweise Desaster-Recovery-Lösungen auch langfristig zu schützen.
Geschäftsinhaber und IT-Verantwortliche müssen sich ihrer Verantwortung bewusst sein und sicherstellen, dass sie über geeignete Schutzlösungen verfügen.

2. Eine alte Bekannte hochaktuell: 3-2-1-1-Datenschutzstrategie

Die 3-2-1-1-Strategie besagt, dass man drei Sicherungskopien der Daten auf zwei unterschiedlichen Medien (beispielsweise Festplatte oder Tape) haben sollte, wobei eine dieser Kopien für die Wiederherstellung im Katastrophenfall an einem anderen Ort aufbewahrt wird. Die letzte Eins in dieser Strategie steht für unveränderlichen Objektspeicher.
Unternehmen sollten zu ihrer eigenen Sicherheit eine Cloud-Speicherlösung nutzen, die Daten kontinuierlich sichert und alle 90 Sekunden Snapshots erstellt. Das hat den entscheidenden Vorteil, dass Daten nicht nur schnell, sondern auch nahezu ohne Aktualitätseinbußen wiederhergestellt werden können. Mit unveränderlichem Cloud-Speicher gibt es viele Wiederherstellungspunkte und es ist sichergestellt, dass Daten geschützt sind.

3. Die richtigen Fragen sorgen für Sicherheit

Es gibt wichtige Fragen, die Unternehmen ihrem Cloud-Anbieter stellen sollten. Dazu gehört beispielsweise, welche Verfahren der Anbieter für seine eigene Business Continuity und das Disaster Recovery anwendet. Zudem sollten die Service-Level-Standards klar abgefragt werden und verständlich sein. Eine Service-Verfügbarkeit von 99 Prozent oder 99,999 Prozent macht da einen enormen Unterschied. Bereits zwischen nur einer oder zwei Neunen hinter dem Komma kann die Ausfallzeit für ein Unternehmen pro Jahr zwischen drei vollen Tagen oder 27 Minuten variieren. Dieser Unterschied hat erheblichen Einfluss auf die Sicherheit – und die Business Continuity.

Eine weitere wichtige Frage ist, ob der Cloud-Anbieter eine zusätzliche Datensicherung anbietet, mit der man Daten an verschiedenen geografischen Standorten sichern kann. Und wenn ja: Ist dieser Service integriert? Oder ist es nötig, sich dafür bei einem Drittanbieter anzumelden, um über die individuell passende Datensicherung und einen Notfallwiederherstellungsplan zu verfügen?

Eine oft vergessene, jedoch essenzielle Frage ist, wie einfach es sich gestaltet, zu einem anderen Cloud-Anbieter zu wechseln. Der Wechsel von einem Anbieter zum anderen ist oft viel leichter gesagt als getan.

4. Nichts geht an einem Notfallplan vorbei

Mit dem richtigen und individuell auf das Unternehmen abgestimmten Backup-und-Wiederherstellungsplan lassen sich Daten für den Fall einer Katastrophe effizient schützen. Ein Plan sollte auch die Simulation einer Unterbrechung beinhalten, um das Disaster Recovery im Anschluss zu bewerten. Zudem sind regelmäßige Tests der Backup-Images wichtig, damit etwaige Probleme rechtzeitig und vor einem Ernstfall behoben

werden können. Im Fall des OVHcloud-Brandes war es für Kunden, die über einen Wiederherstellungsplan verfügten, deutlich wahrscheinlicher, einen Schaden durch dauerhaften Datenverlust zu vermeiden.

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
storagecraft@tc-communications.de
www.tc-communications.de