**Wenn die Cloud raucht: Was wir aus dem Brand im OVH-Rechenzentrum lernen können**

Der Großbrand bei einem der größten Cloud-Hoster ist mehr als nur ein Unfall in einem Rechenzentrum. Es ist ein Fall, der viele Fragen über den Stellenwert und das Vertrauen in eine Technologie aufwirft.

In der vergangenen Woche brannte bei Europas größtem Cloud-Anbieter ein fünf Etagen hohes Rechenzentrum mit 12.000 Servern. Bei OVH-Cloud in Straßburg wurden dabei vier Serverhallen zerstört, eine brannte ganz nieder. Hierbei gingen laut [Medienberichten](https://www.golem.de/news/cloud-hoster-ovh-vermutet-usv-als-moegliche-brandursache-2103-154890.html) 3,6 Millionen Websites kurzzeitig vom Netz, darunter Regierungseinrichtungen, Banken, Großkanzleien, aber auch große Spieleanbieter wie Facepunch und viele mehr.

Ein Teil der Daten wurde komplett vernichtet, weil nicht alle Kunden über die (kostenpflichtigen) Backups verfügten, die OVH-Cloud anbietet. In der Regel, so erklärt es ein Experte eines anderen Cloud-Providers, gehöre bei einer Shared Cloud das Backup seitens des Anbieters dazu, bei dedizierten Servern sei es aber Sache des Kunden. Eine Sparsamkeit, die im konkreten Fall richtig teuer für die betreffenden Unternehmen werden kann. Nun mehren sich die Stimmen, die erklären, dass die [Cloud](https://t3n.de/news/googles-verluste-cloud-geschaeft-1354110/) nun mal nicht sicher sei und man doch besser dran sei, wenn man seine Daten bei sich im eigenen Rechenzentrum vorhalte. Doch das ist gleich aus mehreren Gründen falsch.

Zum einen kann eine Cloud-[Infrastruktur](https://t3n.de/magazin/managed-private-cloud-237292/), egal von welchem der großen Anbieter (Amazons AWS-Cloud, Microsofts Azure Cloud, Google Cloud) problemlos so vorgehalten werden, dass nicht nur ausreichende Redundanz bei den Backups erfolgt, sondern dass diese tunlichst auch an unterschiedlichen Standorten erstellt werden. Zum anderen ist es immer noch Sache des Kunden, entweder selbst für Backups zu sorgen oder aber diese (und das wäre eigentlich die elegantere Lösung) durch den Cloud-Anbieter ziehen zu lassen. Genau genommen muss der Cloud-Anbieter im Falle eines solchen Brandes dann gleich auch vom entfernt abgelegten Backup ein weiteres Backup an einem dritten Ort ziehen, um wiederum Redundanz zu erzielen. Dass gerade bei OVH als größter Hoster Europas mit rund 260.000 Servern in knapp zwei Dutzend Rechenzentren ein solcher Schaden entstand, zeigt, wie angreifbar die Cloud trotz aller suggerierten Datensicherheit ist. Das liegt weniger an ihrer Grundidee, sondern eher an Sparmaßnahmen mancher (auch größerer) Unternehmen.

Der Fall zeigt auch, dass verbindliche Regeln und Normen hermüssen, die nicht nur ermöglichen, Unternehmen in die Pflicht zu nehmen, sondern im Zweifelsfall auch dafür sorgen, dass sich wirklich relevante Daten, etwa der öffentlichen Hand, nicht so einfach in Luft auflösen können. Denn das kann – On-Premises-Speicherung hin, Multi-Cloud-Strategie her – in den unterschiedlichsten Infrastrukturkombinationen passieren. OVH-Cloud ist darüber hinaus einer der Hoffnungsträger für Gaia-X, eine europäische Antwort auf die Cloudangebote der Internetriesen aus den USA und China. Das Unternehmen soll demnächst an die Börse gehen und Branchenkenner sprachen zumindest vor dem Vorfall von einem Unternehmenswert in Milliardenhöhe.

Fragen:

Das Beispiel zeigt wie wichtig die Informationstechnologie allgemein für die Wirtschaft ist und welche Auswirkung eine Störung von IT-Dienstleistungen, sogenannten Services hat.

Einzelarbeit:

1. Definieren Sie den Begriff Service und IT-Service Management (ITSM).
2. Welche Bereiche der Wirtschaft wurden bei dem Brand des größten europäischen Rechenzentrums betroffen?
3. Was sagt der Bericht zu Datensicherung der Kunden aus?
4. Im Bezug auf die vorherige Frage macht es einen Unterschied, ob ein Unternehmen den Service „Webhosting“ oder einen virtuellen Server zu Selbstverwaltung (V-Hosting) als Service mietet? Bewerten Sie die Situation im Bericht.



