CONTINUM

GROSSBRAND IM RECHENZENTRUM – WELCHE LEHREN SOLLTEN GEZOGEN WERDEN?

In den frühen Morgenstunden des 10. März 2021 brach im Rechenzentrum SBG2 des französischen Kommunikationsdienstleisters OHV in Straßburg ein Feuer aus.

VON JULIAN SAYER

Der Brand konnte nicht mehr unter Kontrolle gebracht werden, das fünfstöckige Datacenter mit Platz für rund 12.000 Server brannte völlig aus. Auch das benachbarte Rechenzentrum SBG1 wurde teilweise zerstört. Die Folgen sind für den Cloudbetreiber sowie dessen Kunden verheerend.

Die Notwendigkeit von Maßnahmen zur Fortführung des Geschäftsbetriebs im Katastrophenfall ist durch dieses Ereignis bei vielen Geschäftsverantwortlichen ins Gedächtnis gerufen worden. Zu schnell jedoch gingen die meisten wieder zum Tagesgeschäft über – sie selbst waren schließlich nicht betroffen.

Durch den Brand verschwanden insgesamt 3,6 Millionen Websites aus dem Netz. Laut dem britischen Internetdienstleister Netcraft waren etwa 18 Prozent aller mit OVH verbundenen IP-Adressen nicht mehr erreichbar.

Das besonders Bittere, neben dem Ausfall der IT-Systeme über mehrere Wochen, sind die unwiderruflich verloren gegangenen Daten vieler Kunden. Welche Lehren können nun drei Monate danach aus dem Unglück gezogen werden? Sollte man womöglich auf Clouddienste generell verzichten?

Julian Sayer,
Vorstand bei der Continum AG. Foto: ZVG

Sicherlich nicht, denn das Rad der IT-Geschichte lässt sich nicht zurück drehen. Jedoch ist zu berücksichtigen, dass sich hinter der Cloud ein Netzwerk mehrerer Rechenzentren und letztlich eine Server-Hardware befindet, die ausfallen kann. Ausschlaggebend ist, wie der Cloudanbieter auf Ausfälle, Störungen und Katastrophen vorbereitet ist und ob Backups für den Fall der Fälle vorhanden sind.

Ein Rechenzentrum (RZ) ist ein komplexes Gebilde mit viel Technik wie zum Beispiel Strom-/ Notstromversorgung, Klimatechnik, Brandschutz und Feuerlöschanlage sowie Zugangskontrolle und Einbruchsicherung, um die Ausfallrisiken soweit es geht zu minimieren. Der RZ-Betreiber ist dafür verantwortlich, dass die Technik funktioniert und regelmäßig gewartet wird. Die ISO27001-Zertifizierung ist ein wichtiges Qualitätszeugnis, das den Kunden des RZ-Betreibers Sicherheit geben soll und zeigt, dass das RZ in puncto Datensicherheit ordentlich betrieben wird. Häufig ist es am Ende eine Vertrauensfrage, inwieweit man sich als Kunde auf den RZ-Betreiber verlässt. In der Regel sind die Risikokonzepte der nach ISO27001 betriebenen RZs in Ordnung, insbesondere im Vergleich zu den Konzepten im eigenen mittelständischen Betrieb.

Katastrophen verheerenden Ausmaßes kann es jedoch auch in großen RZs geben wie sich jüngst gezeigt hat. Da sich Ausfälle nicht vermeiden lassen, kommt der richtigen Backup-Strategie eine wichtige Rolle zu.

An dieser Stelle ist nochmals zu erwähnen, dass die Verantwortung für die Backup-Strategie stets beim Kunden und nicht beim RZ-Betreiber liegt. Je nach tolerierbarer Ausfallzeit können unterschiedliche Strategien erforderlich sein. Genügt bei einem kleineren Handwerksbetrieb gegebenenfalls die tägliche Sicherung der Daten in einem separaten Brandabschnitt, so bedarf es in anderen Unternehmen mit höherer IT-Abhängigkeit ausgereiftere, zuverlässigere, automatisierte und überwachbare Prozesse.

Als Leitfaden seien die Empfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnologie) genannt. In der Praxis hat sich ein zweistufiges Backupkonzept bewährt. Die erste Backup-Kopie wird vom RZ-Betreiber in einem separaten Brandabschnitt abgelegt. Die zweite Kopie wird in einem sogenannten georedundanten Rechenzentrum, welches sich nach BSI außerhalb eines Bombenradius befinden sollte, gespeichert. So sind im Fall der Fälle mindestens zwei Backupkopien an unterschiedlichen Standorten vorhanden und das Risiko von unwiderruflich verloren gegangenen Daten ist minimiert. Dieses pragmatische Backup-Konzept ist auch unter wirtschaftlichen Gesichtspunkten für die meisten Mittelständler leicht adaptierbar.

Bei Unternehmen mit einem eigenen Rechenzentrum eignet sich die Buchung eines sogenannten Cloud-Backups beim RZ-Betreiber des Vertrauens, sodass auch in diesen Fällen stets zwei Backup-Kopien an unterschiedlichen Standorten vorhanden sind.

Julian Sayer ist Vorstand für Vertrieb, Marketing und Entwicklung des Freiburger Hostingunternehmens und Cloud Solution Providers Continum AG. Als AWS und Microsoft Azure Partner versteht sich die Continum AG als „Anwalt" des Kunden und unterstützt Unternehmen auf dem sicheren Weg in die Cloud.