

Cloud auf Nummer sicher – Redundanz im Rechenzentrum

Das aktuelle Ereignis eines Brands in einem französischen Rechenzentrum macht es notwendig auf die Wichtigkeit von Redundanzen insbesondere für Cloud-Lösungen einzugehen.

Vorteile der Datensicherung in der Cloud

Cloud-Lösungen sind praktisch und aus der Geschäftswelt nicht mehr wegzudenken. Bis vor nicht allzu langer Zeit haben nahezu alle Unternehmen eigene Serverräume unterhalten. Diese erforderten nicht nur entsprechende Raumkapazitäten, sondern auch Know-how im Bereich Sicherheit und Kühlung. Mit der Bereitstellung von Diensten aus der Cloud werden sowohl die „harten“ als auch die „soften“ Faktoren gelöst. Zunächst zu den harten Faktoren: Wer seine Daten in die Cloud auslagert, benötigt keine eigene Serverstruktur mehr wie im bisherigen Ausmaß. Unternehmen sparen an Raumressourcen und den dazugehörigen Mietkosten. Sie entlasten zudem die IT-Abteilung, denn der Serverraum muss nicht mehr ständig überwacht und einsatzbereit gehalten werden. Zu den soften Nebeneffekten der Lagerung in der Cloud gehört die Sicherung der Daten im jeweiligen Rechenzentrum nach Datenschutzstandards, die Sicherung gegen Hackerangriffe durch dedizierte Firewalls und der Service automatischer Updates für dort gelagerte Anwendungen.

Die Daten, die in eine Cloud ausgelagert werden, sind von unterschiedlicher Natur. Es gibt Unternehmen, die inzwischen ihre komplette Datenstruktur in der Cloud lagern – ob als Backup oder direkte Services aus der Cloud. Auch Telefonielösungen können ausgelagert werden. Damit kennen wir uns aus.

Wir stellen uns im Folgenden ein „Worst-Case-Szenario“ für eine Cloud-Anwendung vor, die komplett in der Cloud gehostet wird. In unserem Beispiel eine Cloud-Telefonanlage.

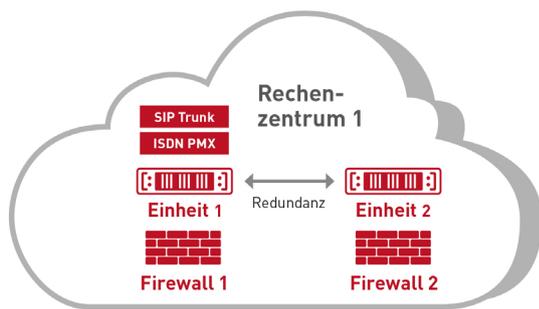
Worst-Case: Ein Rechenzentrum fällt aus

Der Grund für den Ausfall eines Rechenzentrums muss nicht immer ein Brand sein. Auch eine Baustelle kann ein Grund sein, wenn ein Bagger beispielsweise eine Hauptzuleitung kappt. Es handelt sich dann möglicherweise zwar „nur“ um einen Ausfall von wenigen Stunden oder Minuten. Das kann aber für viele Geschäftszweige schon ausreichen, um extreme Störungen und letzten Endes auch Einbußen zu verzeichnen. Wir stellen uns ein Unternehmen vor, das darauf angewiesen ist, ständig in Kommunikation mit seinen Kunden zu sein. Ein Störfall tritt ein: Im schlimmsten Fall brennt das Rechenzentrum ab. Alle Server und die darauf gespeicherten Daten sind vernichtet. Der Schaden ist irreparabel.

Wenn das Unternehmen in Kooperation mit einem Dienstleister, die Leistung – in unserem Fall die Cloud-Telefonanlage – lediglich in einem Rechenzentrum abgelegt hat, muss es von Null anfangen. Die Anlage muss in einem neuen Rechenzentrum, das es erstmal zu finden gilt, komplett neu aufgesetzt werden. Was können Unternehmen tun, um dieses Szenario zu verhindern?

Ein Netz mit doppeltem Boden schaffen

Es ist elementar, für relevante Programme oder Daten ein Backup beziehungsweise ein redundantes System aufzubauen. Das erfordert zwar mehr Ressourcen und erhöht auch die Kosten. Allerdings ergibt ein redundanter Aufbau immer dann Sinn, wenn kritische Komponenten im Spiel sind. Solch eine kritische Komponente kann beispielsweise die Telefonanlage sein. Eine einfache Redundanz ist immer empfehlenswert. Diese wird in den meisten Fällen so gelöst, dass eine zweite physikalische Einheit im gleichen Rechenzentrum aufgebaut wird. Fällt die erste Einheit aus, übernimmt direkt die zweite. Das sorgt für eine deutlich höhere Verfügbarkeit und stellt die kostengünstigste Art der Redundanz dar.



Einfache Redundanz im gleichen Rechenzentrum

Alternativ kann die zweite Einheit in einem anderen Rechenzentrum aufgebaut werden. Das bedeutet, dass das zweite Rechenzentrum mit der ersten Einheit verbunden sein muss. Denn diese müssen miteinander „sprechen“. Hier kann eine Verbindung per Internet oder VPN hergestellt werden. Eine andere Möglichkeit ist der Aufbau einer dedizierten Datenleitung zwischen den Rechenzentren. Das zieht höhere Kosten mit sich, bietet aber auch einen außerordentlichen Schutz. Fällt das erste Rechenzentrum aus, übernimmt die Einheit im zweiten Rechenzentrum. Dieser „Schwenk“ kann manuell eingeleitet werden oder automatisiert innerhalb weniger Sekunden erfolgen.

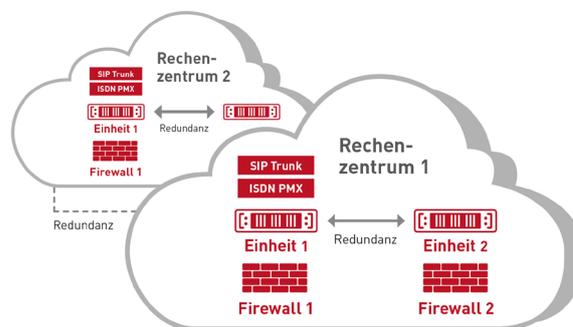


Einfache Redundanz mit Backuplösung im zweiten Rechenzentrum

Wie bereits oben erwähnt, muss ein Worst-Case-Szenario wie der Brand eines Rechenzentrums nicht der einzige Grund für einen Ausfall sein. Anbieter, die vorausschauend planen, achten beispielsweise darauf, dass die gewählten Rechenzentren für Backupsysteme an unterschiedlichen Stromnetzen hängen. Kommt im Stadtteil des ersten Rechenzentrums ein Stromausfall vor, bleibt das zweite Rechenzentrum davon unberührt. Zwar bieten Rechenzentren für solche Fälle eine autarke Stromversorgung durch eigene Stromspeicher an, aber auch diese sind nicht unbegrenzt verfügbar. Meist reichen diese Stromreserven für wenige Minuten bis zu einer oder zwei Stunden.

Um höchste Ausfallsicherheit zu gewährleisten, können Systeme auch doppelt redundant abgesichert werden.

Eine doppelte Redundanz ist eine Kombination aus einer Absicherung im gleichen und in einem weiteren Rechenzentrum, die physisch komplett voneinander getrennt sind. Sie besteht aus zwei Systemen mit insgesamt vier Einheiten, die sich miteinander abgleichen. Fällt das Hauptsystem aus, übernimmt das zweite System im selben Rechenzentrum. Fällt das komplette Rechenzentrum aus, übernimmt das dritte System im zweiten Rechenzentrum. Sollte selbst das dritte System ausfallen, übernimmt das vierte System im zweiten Rechenzentrum. Eine doppelte Redundanz ist die kostenintensivste Variante eines Redundanzaufbaus, erhöht aber hochgradig die Verfügbarkeit und Ausfallsicherheit. Dieses System haben wir für die byon vTK gewählt.



Doppelte Redundanz in zwei physisch getrennten Rechenzentren

Welches Redundanzsystem für das jeweilige Unternehmen das richtige ist, muss individuell entschieden werden. Dabei kommt es darauf an, wie wichtig die in der Cloud abgelegten Daten für die Unternehmensabläufe und das jeweilige Kerngeschäft sind und wie deren Verfügbarkeit aussehen soll. Es ist hilfreich, im Vorfeld eine Kosten-Nutzen-Rechnung anzustellen, bei der die Kosten für einen Ausfall pro Minute den Kosten des Redundanzsystems gegenübergestellt werden. Egal, ob Unternehmen einen externen Anbieter suchen oder ihre Systeme selbst verwalten: Der Brand des Rechenzentrums in Straßburg macht deutlich, dass kritische Systeme heutzutage auf jeden Fall eine Redundanz besitzen sollten.

Es lohnt sich, vor der Nutzung einer Cloud-Lösung von externen Dienstleistern zu prüfen, wie die Sicherheitskonzepte der dazugehörigen Serverstruktur aufgesetzt sind.

Checkliste für ein Sicherheitsszenario

- Firewallkonzept
- Datenschutz je nach Standort (den höchsten Schutz bieten Rechenzentren innerhalb der EU)
- Redundanzen
- Getrennte Stromversorgung der Rechenzentren