Brandschutz: Wie schützt man Rechenzentren vor Feuer, Herr Faulhaber?

Brände sind nach wie vor eine der Ursachen für Ausfälle von Rechenzentren. Besonders die hohe Dichte an elektrischer Leistung von mitunter mehreren Megawatt erhöht die potenzielle Brandgefahr. Lichtbögen, Kurzschlüsse, Schwelbrände oder defekte Komponenten können schwere Folgen nach sich ziehen. Wir haben mit Joachim Faulhaber, Produktmanager & Fachbereichsleiter Data Center bei TÜViT, über den jüngsten Fall eines Cloud-Rechenzentrum-Großbrandes und Brandschutz als zentrales Element der Risikovorsorge gesprochen.

Herr Faulhaber, die jüngsten Ereignisse in Straßburg haben gezeigt, wie schnell ein Brand in einem Rechenzentrum ausbrechen und zu einem verheerenden Großbrand heranwachsen kann. Wie können solche Brände aus Ihrer Sicht verhindert oder zumindest das Brandrisiko reduziert werden?

Der aktuellste Rechenzentrumsbrand macht natürlich vor allem eines deutlich: Auch hinter einer Cloud stecken letztendlich physische Rechenzentren, die ausfallen können und damit die Cloud-Dienste massiv einschränken. Gerade der Brandschutz spielt angesichts der Energiedichte zur Versorgung der IT-Technik eine zentrale Rolle, stellt Betreiber von Rechenzentren gleichzeitig aber auch vor eine besondere Herausforderung. Denn Maßnahmen des Brandschutzes müssen von Anfang an berücksichtigt und konsequent umgesetzt werden. So sollte zum Beispiel die Technik kleingliedrig auf mehrere Räume, brandschutztechnisch getrennt, verteilt werden, eine geeignete Brandmeldeanlage nach dem Stand der Technik sowie ein Brandfrühesterkennungssystem zur Erkennung von Bränden in der Entstehungsphase eingesetzt werden. Es gibt eine Reihe von Kriterien dieser Art, die Betreiber von Rechenzentren kennen und berücksichtigen sollten, um ihre Räumlichkeiten wirkungsvoll zu schützen. Orientierung geben können dabei unter anderem die Kriterienkataloge Trusted Site Infrastructure (TSI) oder EN 50600.

Was unterscheidet eigentlich den gewöhnlichen Brandschutz von Gebäuden mit dem, der in Rechenzentren zum Einsatz kommt?

Der Schutzbedarf in einem Rechenzentrum bezieht sich auf Personal, Ausstattung, Daten und Diensteverfügbarkeit. Der Personal- und Ausstattungsschutz wird in der Regel durch die konventionellen Brandschutzmaßnahmen, wie zum Beispiel Einrichtung von Brandabschnitten, Brandüberwachung und ggf. Sprinklerung, abgedeckt. Hierbei wird die Maxime verfolgt, dass der Schaden an der Ausstattung nicht unbedingt verhindert, aber begrenzt wird. Bei dem Schutz der Daten und der Diensteverfügbarkeit geht es darum, den Brand zu verhindern (Materialien, Sauerstoffabsenkung), bzw. frühzeitig in seiner Entstehungsphase zu erkennen und zu bekämpfen (Brandfrühesterkennung, Gaslöschanlage).

Durch eine redundante Verteilung der Versorgungsinfrastruktur ist es möglich, den Brand so zu isolieren, dass eine Versorgung der IT-Anlagen über die nicht betroffenen Räume dennoch möglich ist. Grundsätzlich sind die Brandschutzmaßnahmen in einem Rechenzentrum aufwändiger und müssen unter Berücksichtigung oben genannter Schutzziele konzeptionell geplant werden.

Was würden Sie Betreibern von Rechenzentren in Sachen Brandschutz demnach raten?

Wie in vielen anderen Bereichen gilt auch hier: Vorsicht ist besser als Nachsicht. Selbstverständlich gibt es gesetzliche Bestimmungen, die es umzusetzen gilt, oder Forderungen von Versicherern, die Einfluss auf die Höhe des Versicherungsbeitrages haben. Darüber hinaus sollten RZ-Betreiber ihre Brandschutz-Maßnahmen für die besonderen Belange im Rechenzentrum ergänzen und nicht bei der konventionellen Ausstattung belassen. Denn mit einem Brand gehen im Zweifelsfall nicht nur hohe Kosten für die Wiederherstellung der Datenbestände einher, sondern auch Reputationsschäden.

Um so ein Szenario – und weitere – möglichst zu vermeiden, empfiehlt es sich bereits bei der Planung einen Brandschutzsachverständigen mit Kenntnissen aus dem Rechenzentrumsumfeld hinzuzuziehen und auf Kriterienkataloge wie den TSI.STANDARD zurückzugreifen. Zusätzlich gewinnt man ein höheres Maß an Vertrauen, wenn man sein Rechenzentrum durch einen unabhängigen Dritten wie TÜViT regelmäßig prüfen und zertifizieren lässt.

Jetzt stellt der Brandschutz am Ende des Tages nur einen Aspekt der physischen Sicherheit und Verfügbarkeit von Rechenzentren dar. Was sollten Betreiber noch beachten?

Das ist richtig. Aus diesem Grund verfolgen wir bei TÜViT mit dem TSI.STANDARD einen ganzheitlichen Ansatz, der einschlägige EN- und DIN-Normen – insbesondere die DIN EN 50600 – aber auch VDE-Vorschriften und VdS-Publikationen berücksichtigt.

Hier findet sich natürlich auch das Thema Brandschutz wieder, steht aber gleichgewichtet neben neun weiteren Bewertungs-Bereichen, die jeweils einen Satz von Anforderungen in Form von Kriterien enthalten. Betrachtet werden in diesem Zusammenhang auch das Umfeld, die Baukonstruktion, die Sicherheitssysteme & -organisation, die Struktur der Verkabelung, die Energieversorgung, die raumlufttechnischen Anlagen, die Betriebs-Organisation, die Dokumentation und der Rechenzentrumsverbund, wenn anwendbar.

Ziel dieses ganzheitlichen Ansatzes ist es, das eigene Rechenzentrum durch die Umsetzung und Erfüllung der unterschiedlichen Anforderungen optimal abzusichern und auf diese Weise eine möglichst hohe Verfügbarkeit zu gewährleisten.