AUGUST 2021

PROPERTY MATTERS



Rechenzentren – ein unterschätztes Risiko?

von Leo Ronken, Gen Re, Köln

Zunehmend findet eine Verlagerung von IT-Infrastrukturen hin zu Cloud-basierten Lösungen statt.[1] Es wird erwartet, dass sich bis zum Jahr 2024 mehr als 45 % der IT-Ausgaben von traditionellen zu Cloud-Lösungen verlagern.[2] Die Gründe dafür liegen in den geringeren Kosten sowie erweiterten Datenanalyse- und Kooperationsmöglichkeiten. Befeuert wird diese Entwicklung durch die zunehmende Digitalisierung von Unternehmensprozessen, die mit steigenden Anforderungen an die ständige Betriebsbereitschaft und Verfügbarkeit der IT-Anlagen und Infrastruktur einhergeht. Damit werden Rechenzentren immer mehr zum zentralen Nervensystem der Wirtschaft. Sollte ein Rechenzentrum ausfallen, hat dies weitreichende Konsequenzen. Neben den Risiken für die Sicherheit und Verfügbarkeit der gespeicherten Daten kann ein solcher Ausfall, insbesondere wenn er nicht kurzfristig behoben werden kann, für den Betreiber sowie die Nutzer des Rechenzentrums große finanzielle Schäden und Reputationsverluste bis hin zu Betriebsschließungen nach sich ziehen. Aus versicherungstechnischer Sicht spielt deshalb neben einer adäquaten Sachdeckung die Versicherung der Folgen einer Betriebsunterbrechung (BI – Business Interruption) eine wesentliche Rolle.

Die Ursachen, die zum Ausfall eines Rechenzentrums führen können, sind vielfältig: von einem Cybervorfall bis hin zu klassischen Schäden, verursacht bspw. durch Brand, Wasser, Naturgefahren oder Vandalismus. Dieser Artikel befasst sich im Wesent-

Inhalt

lichen mit den klassischen Schadenursachen, insbesondere Brandereignissen. Dabei werden neben Empfehlungen zu Brandschutzmaßnahmen Hinweise für die Ermittlung des Gefährdungsexposures sowie zum Underwriting aus Sicht der Sachversicherung gegeben.

Arten von Rechenzentren

Rechenzentren (teils auch Datencenter genannt) sind Räumlichkeiten, in denen in großem Umfang Daten und Anwendungen von einem oder mehreren Unternehmen gespeichert und verarbeitet werden. Gleichzeitig wird der Begriff für die Organisation verwendet, die die IT verwaltet. Dazu wird ein Netzwerk von Rechen- und Speicherressourcen genutzt.

Man unterscheidet zwischen externen und internen Rechenzentren, d. h. Rechenzentren von Dienstleistern und unternehmenseigene Rechenzentren (Inhouse Data Center). Beide nutzen vergleichbare Rechneranlagen und Infrastrukturen.

Wesentliche Bestandteile zum Betrieb eines Rechenzentrums/IT-Netzwerks sind:

- Server (Hardware bestehend aus CPU, Arbeitsspeicher, Festplatten)
- aktive Netzwerkkomponenten (Router, Switches, Firewalls, Controller mit aktivem Stromanschluss)
- passive Netzwerkkomponenten (Verkabelung, Stecker, Buchsen ohne eigenen Stromanschluss)
- Racks (Metallgehäuse zur Aufnahme der Serverhardware sowie der Netzwerkkomponenten)

Hinzu kommen Infrastruktur-, Energieversorgungs-, Klima- und Lüftungstechnik sowie entsprechende Sicherheitseinrichtungen.

Mittlerweile gibt es weltweit eine Vielzahl von kleineren und größeren bis hin zu global agierenden Anbietern, die unterschiedliche IT-Lösungsstrukturen für das Management von Daten und Prozessen anbieten. Diese kann man grob wie folgt beschreiben:

- Hosting/dezidierte Server – Unternehmen nutzen Server oder Server Racks des Rechenzentrumanbieters.
- Cloud-Dienst – Unternehmen bilden die gesamte IT-Struktur ihres internen Rechenzentrums auf dem Rechenzentrum eines Dienstleistungsunternehmens ab.
- Managed-Dienste – statt der gesamten IT-Struktur werden nur einzelne Dienstleistungen eines Cloud-Anbieters genutzt.

Im Rahmen einer Cloud-basierten Lösung unterscheidet man verschiedene Formen:

- Private Clouds
  Die Cloud-Infrastruktur wird nur für eine Institution von dieser Institution oder einem Dritten betrieben. Dabei ist die IT-Struktur mit isoliertem Zugriff nur einem Endnutzer oder einer Nutzergruppe zugewiesen.
- Public Clouds
  Die Cloud-Infrastruktur eines Anbieters wird dabei von der Allgemeinheit oder einer großen Gruppe, beispielsweise einer ganzen Industriebranche, genutzt. Öffentliche Clouds basieren in der Regel auf IT-Infrastrukturen, die nicht dem Endnutzer gehören. Zu den größten öffentlichen Cloud-Anbietern gehören Amazon-Web-Services, Alibaba Cloud, IBM Cloud, Google Cloud und Microsoft Azure.
- Community Cloud
  Die Cloud-Infrastruktur wird von mehreren Institutionen geteilt, die ähnliche Interessen haben (betrieben von einer dieser Institutionen oder einem Dritten).
- Hybrid Cloud
  Hierbei werden über eine standardisierte Schnittstelle mehrere Cloud-Infrastrukturen genutzt. Es handelt sich um eine einzelne IT-Umgebung, die aus mehreren Bereichen besteht, die über LAN (Local Area Network), WAN (Wide Area Network), VPN (Virtual Private Network) und/oder APIs (Application Programming Interface) verbunden sind. Sie können sehr komplexe Strukturen aufweisen. IT-Systeme werden automatisch zu einer Hybrid-Cloud, wenn Anwendungen frei zwischen mehreren separaten, aber miteinander verbundenen Umgebungen migriert werden können.

Außerdem werden Rechenzentren/Cloud-Angebote mit verschiedenen Servicemodellen betrieben, die man grob wie folgt unterscheiden kann:

- Infrastruktur als Service (Infrastructure as a Service, IaaS)
  IT-Ressourcen wie Rechenleistung, Datenspeicher oder Netze werden als Dienst angeboten. Ein IaaS-Anbieter bietet bei Bedarf Zugriff auf die wichtigsten IT-Ressourcen wie Computer (virtuelle oder dedizierte Hardware), Netzwerke und Speicher über das Internet. Ein Cloud-Kunde kauft/mietet diese virtualisierten und in hohem Maß standardisierten Services und baut darauf eigene Services zum internen oder externen Gebrauch auf. So kann ein Cloud-Kunde z. B. darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.

- Plattform als Service (Platform as a Service, PaaS)
  Ein PaaS-Provider stellt eine komplette Infrastruktur bereit und bietet dem Kunden auf der Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden. So kann die Plattform z. B. Mandantenfähigkeit, Skalierbarkeit, Zugriffskontrolle, Datenbankzugriffe etc. als Service zur Verfügung stellen. Der Kunde hat dabei keinen Zugriff auf die darunterliegenden Schichten wie das IT-Betriebssystem und die Hardware, er kann aber auf der Plattform eigene Anwendungen laufen lassen, für deren Entwicklung der Cloud-Betreiber in der Regel eigene Hardware- und Softwaretools anbietet.
- Software als Service (Software as a Service, SaaS)
  Dahinter verbirgt sich ein Cloud-basiertes Servicemodell, mit dem man auf ein Standard-Softwareprodukt zugreifen kann, das von einem Dienstanbieter (Cloud Service Provider) betrieben und verwaltet wird. Sämtliche Angebote von Anwendungen, die den Kriterien des Cloud-Computing entsprechen, fallen in diese Kategorie. Dem Angebotsspektrum sind hierbei keine Grenzen gesetzt. Beispiele sind Kontaktdatenmanagement, Finanzbuchhaltung, Textverarbeitung oder Kollaborationsanwendungen.

Die Servicemodelle unterscheiden sich auch im Einfluss des Kunden auf die Sicherheit der angebotenen Dienste. Bei IaaS hat der Kunde die volle Kontrolle über das IT-System vom Betriebssystem aufwärts, da alles innerhalb seines Verantwortungsbereichs betrieben wird, bei PaaS hat er nur noch Kontrolle über seine Anwendungen, die auf der Plattform laufen, und bei SaaS übergibt er die Kontrolle an den Cloud Service Provider.

Weitere geläufige Unterscheidungen ergeben sich aus ihrem Zweck, z. B. Notfallrechenzentrum, Backup-Rechenzentrum, Datencenter.

Allen Formen gemeinsam ist, dass die IT-Rechenzentren eine möglichst hohe Zuverlässigkeit und insbesondere Verfügbarkeit ihrer Dienste garantieren. Dabei bezieht sich die Verfügbarkeit auf die Wahrscheinlichkeit, dass ein System zu einem gegebenen Zeitpunkt tatsächlich wie geplant benutzt werden kann. Die Verfügbarkeit bemisst sich dabei als Verhältnis aus Ausfallzeit (Downtime) und Gesamtzeit eines Systems.

$$\text{Verfügbarkeit (in Prozent)} = \left(1 - \frac{\text{Ausfallzeit}}{\text{Produktionszeit + Ausfallzeit}}\right) \cdot 100$$

Hierzu wurde in den 1990er-Jahren vom Uptime Institute in den USA die Tier-Klassifzierung weltweit als Standard eingeführt.[3] Dabei stellt die Tier-1-Klassifizierung eine Verfügbarkeit von 99,671 % oder, anders ausgedrückt, eine maximal erlaubte Ausfallzeit von 28,8 Stunden pro Jahr dar bis hin zur Tier-4-Klassifizierung mit einer Verfügbarkeitsanforderung von 99,995 % (max. Ausfallzeit von 26,3 Stunden/Jahr) inklusive der Wartungszeiten. Je höher die Anforderungen des Anwenders an die Verfügbarkeit eines Rechenzentrums sind, desto stärker steigen die Kosten zur Erfüllung der dafür notwendigen Sicherheits- und Redundanzbedingungen.

Schadenbetrachtungen

In Rechen- und Datenzentren befindet sich eine Vielzahl von Geräten mit hoher elektrischer Leistungsaufnahme mit entsprechenden Netzteilen und Anschlussleitungen, die insbesondere bei Defekten oder Überlastung anfällig für einen Brand sind. Die in einem Rechenzentrum notwendige Klima- und Lüftungstechnik zur Abführung der enormen Wärmeentwicklung der Server, verursacht durch eine steigende Integration und Packungsdichte bei Prozessoren und ITK-Systemen sowie sonstigen elektrischen Geräten, erschweren die Entdeckung und erfolgreiche Bekämpfung eines Brands durch herkömmliche Maßnahmen wie passive Brandmeldesensoren sowie Feuerlöschanlagen.

Kommt es beispielsweise in einem Rechenzentrum zu einem Entstehungsbrand, der nicht unverzüglich entdeckt und erfolgreich gelöscht wird, ist damit zu rechnen, dass Daten unwiederbringlich zerstört werden und nicht mehr vom Anwender abgerufen werden können. Dadurch entsteht ein erheblicher Schaden nicht nur für den Betreiber des Rechenzentrums, sondern insbesondere für die an das Rechenzentrum angeschlossenen Anwender. Hinzu kommen enorme Kosten, um einen Schaden schnellstmöglich zu beheben und die Verfügbarkeit des Rechenzentrums wiederherzustellen. Gemäß einer Veröffentlichung von Statista betrugen laut einer Umfrage bei 25 % der 1.200 Befragten die durchschnittlichen stündlichen Kosten für kritische Serverausfälle in den Jahren 2019 und 2020 zwischen USD 301.000 und USD 400.000, bei 15 % (2019) bzw. 17 % (2020) mehr als USD 5 Millionen.[4]

Brände sind nach wie vor eine der Hauptursachen für Ausfälle von Rechenzentren. Die hohe Dichte an elektrischer Leistung von mitunter mehreren Megawatt erhöht die potenzielle Brandgefahr, verursacht u. a. durch Lichtbögen, Kurzschlüsse, Schwelbrände oder defekte Komponenten.

Am 10. März 2021 ereignete sich in einem Rechenzentrum eines großen Cloud-Anbieters mit mehr als 100.000 Servern in Straßburg, Frankreich, ein Großschaden, vermutlich im

dreistelligen Millionenbereich. Der Brand brach in einem der vier Gebäude am Standort aus. Auf einer Grundfläche von 500 m² und fünf Stockwerken befanden sich ca. 12.000 Server. Die Ursache ist weiterhin ungeklärt. Anfangs wurde ein technischer Defekt vermutet.[5] Nach einiger Zeit griff der Brand auf ein zweites Datencenter über und zerstörte mehrere Serverräume vollständig. In der Folge mussten alle Datencenter am Standort abgeschaltet werden, was dazu führte, dass Millionen von Webseiten offline waren.[6] In manchen Fällen führte dies zu einem vollständigen Verlust aller gespeicherten Anwenderdaten, denn eine Vielzahl von Usern hatte aus Kostengründen darauf verzichtet, ihre Daten regelmäßig vom Cloud-Anbieter sichern zu lassen. Am 19. März 2021 ereignete sich ein zweiter Brand in den Batterieräumen des teilweise beschädigten Rechenzentrums.[7] Daraufhin wurde entschieden, dieses Rechenzentrum nicht wieder ans Netz zu bringen.

Mit dem Einsatz von mehr als über 100 Spezialisten versuchte man, den Schaden zu begrenzen. Nach der Installation von zusätzlichen 15.000 Servern hoffte man, das Rechenzentrum am 22. März wieder starten zu können. Tatsächlich konnte man von den ursprünglich vier Rechenzentren lediglich zwei am 26. März 2021 in Betrieb nehmen.[8] Dabei wurden auch unbeschädigte bzw. gereinigte Racks aus den zerstörten Rechenzentren in den beiden verbleibenden Rechenzentren verwendet. Den Ruß von den Anlagen und Platinen zu entfernen, bedeutete einen erheblichen Aufwand. Laut dem Betreiber des Rechenzentrums werden für die Reinigung eines Servers ca. sieben Stunden benötigt.[9]

Wesentlich zu dem Schadenausmaß beigetragen haben nach Meinung von Brandschutzexperten die Konstruktion der Gebäude sowie das Fehlen von automatischen Feuerlöschanlagen.

Der Verzicht auf die regelmäßige Sicherung der Anwendungsdaten scheint kein Einzelfall zu sein, wie eine Recherche des Bayerischen Rundfunks ergeben hat. Danach verzichten auch andere Cloud-Betreiber und deren Kunden aus Kostengründen teilweise auf essenzielle Sicherheits- und Brandschutzmaßnahmen.[10]

Effektive Schutzmaßnahmen

An ein Rechenzentrum werden je nach vereinbarter Verfügbarkeit und Sicherheitsbedürfnis die unterschiedlichsten Anforderungen gestellt. Dies reicht von Zugangs-, Daten- und Brandschutz bis zum Schutz gegen Naturgefahren, terroristische Anschläge sowie politische Gefahren. Die Schutzanforderungen können dabei so hoch sein, dass die Rechenzentren in Bunkeranlagen untergebracht und zu Hochsicherheitstrakten ausgebaut sind, die auch Schutz gegen militärische und terroristische Angriffe bieten.

Eine Orientierung zum wirkungsvollen Schutz von IT-Anlagen geben dabei u. a. die Kriterienkataloge Trusted Site Infrastructure (TSI)[11] oder EN 50600[12]. Der Schutzbedarf in einem Rechenzentrum bezieht sich auf Personal, Ausstattung, Daten und Verfügbarkeit. Hierbei unterscheidet man grob zwei Ansätze:

- konventionelle Brandschutzmaßnahmen, z. B. die Einrichtung von Brandabschnitten, Brandüberwachung und Sprinklerung. Hierbei wird die Maxime verfolgt, dass der Schaden an der Ausstattung nicht unbedingt verhindert, aber begrenzt wird;
- betriebsartenspezifische Brandschutzmaßnahmen, die auf den Schutz der Daten und Verfügbarkeit des Rechenzentrums sowie seiner Dienste abzielen. Insbesondere geht es darum, einen Brand zu verhindern (z. B. Auswahl der Baustoffe und Bauteile, Reduzierung der Sauerstoffkonzentration in den betreffenden Räumen) bzw. ihn bereits in seiner Entstehungsphase zu erkennen und zu bekämpfen (z. B. Installation von Brandfrüherkennungsanlagen oder einer automatischen Gaslöschanlage) oder durch redundante Systeme, Versorgungsstrukturen und weitere Standorte, die Auswirkungen eines Schadenereignisses auf die Verfügbarkeit des Rechenzentrums sowie die Sicherheit der Daten sicherzustellen.

Um den Umfang dieses Beitrags nicht zu sprengen, befassen sich die folgenden Hinweise und Empfehlungen vorwiegend mit Maßnahmen gegen die Entstehung, Ausbreitung und Folgen eines Brands.

Bauliche Brandschutzmaßnahmen

Durch bauliche Maßnahmen sollen die Ausbreitung von Feuer oder Rauch und die Ausdehnung über mehrere Räume oder Gebäude hinweg verhindert bzw. begrenzt werden. Wesentliche Bausteine des baulichen Brandschutzes sind dabei die Bauart, Komplex-/Brandwände, feuerbeständige Wände sowie die feuerbeständige Abschottung von Transaktionen aller Art durch brandschutzwirksame Trennungen.

Bauart

Für die Errichtung des Gebäudes sowie die Inneneinrichtung sollten möglichst keine brennbaren Baustoffe und Bauteile verwendet werden. Diese erhöhen die Brandlast und führen

zu einer schnelleren Ausbreitung von Feuer, Rauch und Hitzestrahlung, die das empfindliche IT-Equipment beschädigen oder zerstören. Sollte der Brand ein Gebäude erfasst haben, ist in der Regel von einem Groß- wenn nicht sogar Totalschaden des Rechenzentrums auszugehen. In einem solchen Fall kann die Feuerwehr sich nur darauf konzentrieren, die Nachbargebäude zu schützen.

Brand-/Komplextrennwände

Brand- und Komplextrennwände unterteilen ein Gebäude in Abschnitte, sodass sich ein Brand nicht auf benachbarte Abschnitte ausweiten kann. Sie stellen damit eine wichtige bauliche Brandschutzmaßnahme dar, denn sie verhindern oft den Totalverlust eines Gebäudes und dessen Inhalt. Des Weiteren ermöglichen sie der Feuerwehr eine effektivere Brandbekämpfung. Gerade bei Rechenzentren sollte ein Gebäude in verschiedene Komplex-/Brandabschnitte aufgeteilt sein, um im Schadenfall einen Teil der IT-Struktur zu retten.

Technische Räume

Technische Räume beinhalten die Infrastruktur für den Betrieb der IT. Hierzu gehören Wasser-, Heiz-, Energieversorgung (z. B. Transformatoren, Unterverteilungen, Notstromversorgung) und Lüftungs-/Klima-, Telekommunikations- sowie Netztechnik. Sie sollten jeweils in eigenen feuerbeständig abgetrennten Räumen untergebracht sein, damit ein Brand in einem dieser Räume sich nicht weiter ausbreiten kann.

Wand- und Deckendurchbrüche

Durchbrüche in Wänden und Decken im Zuge von Komplex- und Brandschutzwänden sowie feuerbeständigen Wänden sollten mindestens feuerbeständig durch entsprechende Maßnahmen abgeschottet werden, um eine Ausbreitung eines Brands zu verhindern. Dies gilt auch für Durchführungen von Installationskanälen, Rohrleitungen, Fenstern und Türen sowie Wasser- und Gasleitungen. Dabei können Kabel- und sonstige Versorgungskanäle durch eine brandsichere Verkleidung/Verlegung zusätzlich geschützt werden, um einen Funktionserhalt für 30 bis 90 Minuten zu sichern. Es sollte darauf geachtet werden, dass die Schutzmaßnahmen neben der Feuerbeständigkeit auch Rauchgasdichtigkeit gewährleisten. Hierfür stehen je nach Anwendungsfall verschiedene Möglichkeiten zur Verfügung, z. B. Brandschutzkissen, Dämmschichtbildner, Ausbildung der Kanäle aus nicht brennbarem Material, Verwendung von brandhemmenden elektrischen Leitungen und Kabeln, Kabelschotts.

Technische Brandschutzmaßnahmen

Technische Brandschutzmaßnahmen sind für ein Rechenzentrum essenziell, denn sie sollen entweder eine Brandentstehung verhindern (z. B. Sauerstoffreduzierungsanlage) oder einen Brand schnellstmöglich entdecken, bekämpfen und im Idealfall löschen, um den Brandschaden so gering wie möglich zu halten. Der Schutz sollte dabei das gesamte Rechenzentrum einschließlich der Infrastrukturräume umfassen.

Automatische Feuerlöschanlagen

Automatische Feuerlöschanlagen, speziell konzipiert und ausgelegt auf die Besonderheiten eines Rechenzentrums, sind im Hinblick auf die hohen Sicherheitsanforderungen an ein Rechenzentrum absolut notwendig, denn sie können einen Entstehungsbrand verhindern oder zumindest entdecken und automatisch bekämpfen (z. B. Sauerstoffreduzierungs-, Inertisierungs-, Gaslösch-, Sprinkleranlagen). Dabei sind Sprinkler- bzw. Feuerlöschanlagen, die mit Wasser arbeiten, bei elektrischen/elektronischen Komponenten nicht optimal. In diesem Fall sind Inertgas-Feuerlöschanlagen zu bevorzugen. Sie fluten den betroffenen Bereich mit einem nicht brennbaren Gas wie Kohlendioxid, Stickstoff oder inerten Gasgemischen. Dabei wird die Sauerstoffkonzentration im Raum abgesenkt, wodurch die Flammen erstickt werden. Bei der Planung einer Löschanlage mit gasförmigen Löschmitteln muss eine Raumdruckentlastung berücksichtigt werden, um den entstehenden kurzzeitigen Druckanstieg oder -abfall abzuleiten.

Zunehmend in den Fokus rücken Sauerstoffreduzierungsanlagen für den Schutz von Rechnerräumen, sofern nicht die ständige Anwesenheit von Personal im betreffenden Raum notwendig ist. Sie gelten ebenfalls als Brandvermeidungssystem und erzeugen in einem Rechenzentrum durch Einleiten von Stickstoff eine permanent sauerstoffreduzierte Atmosphäre. Dadurch kann die Entstehung eines offenen Feuers ausgeschlossen werden. Um die konstante Reduktion des Sauerstoffgehalts aufrechtzuerhalten, sollte der so geschützte Raum möglichst dicht konstruiert sein, damit nicht permanent Stickstoff in großem Stil zugeführt werden muss.

Eine Herausforderung für den Brandschutz in Rechenzentren stellen geschlossene Serverschränke dar, die über ein integriertes Kühlsystem verfügen und im Umluftbetrieb arbeiten. Schmor-, Schwel- und Glimmbrände können von außen praktisch nicht mehr entdeckt werden, da Rauch nur in sehr geringer Menge nach außen dringt. Ebenso kann

aber gasförmiges Löschmittel nicht von außen in diese Schränke gelangen. Für derartige Serverschränke sollten kompakte Branddetektions- und Löschsysteme eingesetzt werden, die z. B. in Form eines 19“-Einschubs integriert werden.

Automatische Brandentdeckung

Um einen Brand so schnell wie möglich zu entdecken, sollte in allen Räumen eine automatische Brandmeldeanlage mit direkter Alarmierung einer ständig besetzten Stelle, z. B. Kontrollwarte des Rechenzentrums, Leitstelle der Feuerwehr, installiert sein. Besonders effektiv sind sog. Rauchansaugmelder, bei denen die Luft im Raum bzw. Rack ständig angesaugt und auf mögliche Rauchpartikel überprüft wird. Sie sind weitgehend fehlalarmsicher und reagieren schon auf geringste Rauchmengen. So können Schwelbrände durch verschmorte Kabel entdeckt und gemeldet werden, bevor es zu einem offenen Brandausbruch kommt.

Herkömmliche Brandmeldesysteme (Punkt- oder Linienmelder), bei denen Sensoren in der Nähe oder an der Decke von Gebäuden angebracht sind, reagieren dagegen möglicherweise nicht in den frühen Stadien von Rauch und Feuer, da der Rauch durch die installierte Lüftungs- und Klimatisierungstechnik meist erst spät in die Nähe der Brandmelder gelangt.

Organisatorische und betriebliche Maßnahmen

Organisatorische und betriebliche Maßnahmen umfassen alle Maßnahmen, mit denen der Betreiber des Rechenzentrums versucht, die Risiken für die Enstehung eines Brands zu verringern, z. B. durch Training der Beschäftigten und Sicherheitsanweisungen für das Verhalten im Schadenfall sowie einen Einsatzplan für die Feuerwehr. Damit sollen die Voraussetzungen für eine schnellstmögliche und effektive Brandbekämpfung sowie für eine schnelle Wiederherstellung der Verfügbarkeit des Rechenzentrums geschaffen werden.

Aus der Vielzahl von Möglichkeiten hier nur ein kurzer Überblick über diejenigen, die für viele Betriebsarten gelten: die Ausweisung von Rettungs- und Angriffswegen für die Feuerwehr, Notfallabschaltpläne, IT-Wiederanlaufpläne, Brandschutzordnungen, Feuerwehr-, Brandschutz-, Rettungswegepläne, Betriebsanweisungen, Beschilderung/Kennzeichnung von Standorten für Erstbrandbekäpfungsmittel (z. B. Feuerlöscher, Wandhydranten), Anweisungen zur Vermeidung unnötiger Brandlasten, Rauchverbot, Erlaubnisscheine für feuergefährliche Arbeiten, Einweisung von Fremdfirmen, Besucherregelung, Schulungen der Mitarbeiter in Sicherheitsfragen.

Betriebsunterbrechungsmaßnahmen

Aufgrund der hohen Verfügbarkeitsanforderungen sowie der zu erwartenden hohen Ausfallkosten erfordern Maßnahmen für ein Rechenzentrum ein besonderes Augenmerk, um eine Betriebsunterbrechung zu vermeiden bzw. auf ein Mindestmaß zu reduzieren. Hierzu gehört es beispielsweise, dass Infrastruktur-/Versorgungskomponenten, die für den Betrieb unverzichtbar sind, redundant ausgelegt werden, so z. B. die Stromversorgung, Klimatisierung und Internetanbindung. Damit soll verhindert werden, dass bei einem Ausfall der Betrieb des Rechenzentrums eingestellt werden muss. Je nach der geforderten Verfügbarkeit eines Rechenzentrums kann es notwendig sein, ein zweites, räumlich getrenntes Rechenzentrum parallel zu unterhalten, in dem die Anwendungen und Daten permanent gespiegelt werden, sodass bei Ausfall eines Rechenzentrums das zweite nahezu nahtlos den Betrieb übernehmen kann.

Zu den Kernmaßnahmen sollte ein regelmäßiger Backup-Prozess gehören, um im Schadenfall notwendige Daten und Programme schnellstmöglich wieder zur Verfügung zu haben. Hierbei orientiert sich die Backup-Strategie an den Erfordernissen der Datensicherheit sowie der Verfügbarkeit, die von ggf. wöchentlichen Daten- und Programmsicherungen über tägliche, stündliche oder sogar permanenten Backups ausgehen. Die Backup-Sicherungen sollten dabei an einem anderen Ort gelagert werden. Bei erhöhten Anforderungen an die Verfügbarkeit einer Rechenzentrumsleistung sollten die permanenten Backup-Sicherungen über geografisch voneinander entfernt liegende Rechenzentren erfolgen, um auch hier bei einem größeren Schadenereignis (z. B. eine Explosion, Naturkatastrophe oder einem regionen-, länder- oder kontinenteübergreifenden Schadenereignis) auf eine Ausweichmöglichkeit zurückgreifen zu können und damit die Verfügbarkeit der Daten und Anwendungen sicherzustellen.

Um die Auswirkungen nach einem Schadenereignis so gering wie möglich zu halten, sollte zwingend ein sog. Business Continuity Plan erstellt werden. Dieser benennt alle wichtigen Schritte und die Verantwortlichen im Schadenfall. Ziel ist es, so schnell wie möglich den Betrieb wiederherzustellen. Ein solcher Plan sollte regelmäßig überprüft und getestet werden.[13]

Weitere Schutzmaßnahmen

Selbstverständlich ist ein Brand nur eine Schadenursache, die in einem Rechenzentrum zu erheblichen Schäden führen kann. Wie bereits ausgeführt, sind für ein umfassendes Sicherheitskonzept eines Rechenzentrums viele weitere Kriterien zu beachten, um ein Gefährdungspotenzial auszuschließen oder zu verringern. Da eine umfassende Darstel-

lung den Rahmen dieses Artikels sprengen würde, sollen beispielhaft weitere Schutzmaßnahmenüberlegungen nur kurz angerissen werden. Hierzu zählen u. a.:

- sorgfältige Standortwahl, um vor politischen Gefahren, Natur- (Erdbeben, Flut, Hagel, Sturm, Erdrutsch, Erdsenkung), Infrastruktur-, Nachbarschaftsgefahren gesichert zu sein
- Schutzmaßnahmen gegen Sabotage, Datenmissbrauch und Hacking (Cybervorfälle)
- Schutzmaßnahmen gegen unerlaubten Zugang, Einbruch oder Diebstahl durch entsprechende Zugangskontrollsysteme, wie Dreifaktorauthentifizierung über Code, Chip- und Biometrie-Erkennung, Zugang mithilfe von Kontrollsystemen und Iris-Scanner, permanente Zugangskontrolle, z. B. Videoüberwachungssysteme, Bewegungssensoren, Alarmsysteme und geschultes Sicherheitspersonal
- Schutzmaßnahmen gegen Schäden durch Erschütterungen, Chemikalien
- Schutzmaßnahmen gegen Medienaustritte wie Kühlflüssigkeiten und Leitungswasser

Hinweise für das Underwriting

Bei der Versicherung eines Rechenzentrums sollte besondere Aufmerksamkeit der Betriebsunterbrechungsversicherung sowie Schäden durch Brand und Wasser gewidmet werden. Daneben können Naturgefahren in exponierten Gegenden eine weitere essenzielle Bedrohung darstellen. Für ein Exposure-orientiertes Underwriting sollte immer ein aktueller Besichtigungsbericht vorliegen, möglichst nicht älter als zwei Jahre, denn Technologie, Infrastruktur und insbesondere Betriebsunterbrechungsszenarien unterliegen einem ständigen Wandel.

Zur Bewertung des Sachrisikos sollten zumindest folgende Informationen vorliegen:

- Art des Rechenzentrums und Beschreibung der Leistungen und Services einschließlich der Verfügbarkeitsanforderung
- Adresse des Standorts
- Anordnung und Belegung/Nutzung der einzelnen Gebäude
- Wert der Gebäude, Anlagen inklusive der dafür notwendigen Infrastruktur
- bestehende Naturgefahrengefährdung am Standort des Rechenzentrums
- vorhandene präventive Schutzmaßnahmen für Flexa (fire, lightning, explosion, aircraft) sowie weitere Gefahren, die unter den angefragten Versicherungsschutz fallen (z. B. Feuer, Wasser, Einbruch, Diebstahl, Sabotage, Naturgefahren), ferner die Beschreibung der Bauart, der verwendeten Baustoffe und Bauteile, vorhandene Komplex-/Brandabschnittstrennungen sowie feuerbeständig abgetrennte Bereiche, technische, betriebliche, organisatorische, präventive sowie abwehrende Schutz- und Sicherheitsmaßnahmen

Neben der Beschreibung und Bewertung des Sachrisikos sollte insbesondere das Betriebsunterbrechungsrisiko im Fokus stehen. Besondere Exposure-Merkmale sind hierbei:

- erwartete bzw. vertraglich vereinbarte Verfügbarkeit
- Ersatzbeschaffungszeiten für beschädigte IT-Systeme, z. B. Server, sowie für den Betrieb des Rechenzentrums notwendiger Infrastrukturanlagen wie Transformatoren, Energie-, Lüftungs-, Klima-, Kommunikations- und Netzwerktechnik
- Zeitraum für den Wiederaufbau der Gebäude, Räume, Serveranlagen sowie der Energie- und weiteren notwendigen Infrastruktur, insbesondere Wiederherstellung der Kommunikations- und Netzwerktechnik sowie die Zeit für den Wiederanlauftest
- Ausfallzeit, bis die geplanten Notfallmaßnahmen greifen (Business Continuity Plan) und die Kunden wieder entsprechend bedient werden können, z. B. Umschaltung auf ein Ausweich-/Backup-Rechenzentrum
- Backup-Strategie des Unternehmens sowie benötigte Zeit zum Rückspielen der Backups
- eventuelle Vertragsstrafen bei einem durch das Rechenzentrum ausgelösten Schadenereignis

Ferner lohnt sich ein Blick in das Wording des zugrunde liegenden Versicherungsvertrags einschließlich der Ein-/Ausschlussklauseln sowie der vereinbarten Erstrisikosummen. Insbesondere sollten in diesem Zusammenhang folgende Themen betrachtet werden:

- Sind Cybervorfälle und deren Folgen, aber auch andere Gefahrentatbestände in den bestehenden Versicherungsvertrag miteingeschlossen? Z. B. Terrorismus, innere Unruhen, Elektronik-, Energieausfall-, finanzielle Folgeschäden, vorsätzliche Handlungen, Datenschutzverletzungen, Vertragsstrafen sowie Folgen von Non-physical-Damage-Ereignissen.
- Inwieweit können in einem Schadenfall ggf. weitere Versicherungsverträge, z. B. Haftpflicht-, Elektronik-, Daten-/

Software-, Einbruch-/Diebstahl-, Vertrauensschaden-, Cyber-, aber auch Rück-/Auswirkungsvereinbarungen kumulieren, auch von Dritten, die in Geschäftsbeziehung mit dem Rechenzentrumsbetreiber bestehen? Letzteres wird sich nicht zweifelsfrei feststellen lassen, daher sollte die daraus entstehende Unsicherheit über mögliche Kumulszenarien in die Kapazitätsüberlegungen miteinfließen.

Weiterhin sollte die Entschädigungsleistung bei den Underwriting-Betrachtungen berücksichtigt werden. Hierzu gehören:

- Art der Entschädigungsleistung (z. B. Tagessatz, Einmalsumme)
- Dauer der Entschädigungsleistung (Haftzeit)
- vereinbarte Mehrkosten, z. B. für die Benutzung anderer Anlagen, Anwendung anderer Arbeitsverfahren, Umrüstungen bzw. Wiederinstandsetzung, notwendige Umprogrammierungen sowie Inanspruchnahme von Lohn- und Dienstleistungen zur Krisenbewältigung bis zur gänzlichen Wiederherstellung des Regelbetriebs
- vertraglich vereinbarte, im Schadenfall fällige Strafzahlungen sowie Kosten für die Wiederherstellung erlittener Reputationsverluste

vereinbarte forensische Kosten für das Suchen, Auffinden von Schadenursachen sowie die Wiederherstellung der Daten sowie Kosten für notwendige Sachverständige zur Feststellung der Entschädigungspflicht und -leistung.

Fazit

Rechenzentren werden zunehmend zum zentralen Nervensystem für die Wirtschaft. Sollte ein Rechenzentrum ausfallen, hat dies in der Folge weitreichende Konsequenzen, nicht nur für den Betreiber des Rechenzentrums, sondern auch für die daran angeschlossenen Unternehmen. Aus diesem Grund ist es zunehmend wichtig, dass Rechenzentren über einen optimalen Schutz verfügen, um Schäden jeglicher Art zu verhindern.

Neben anderen Gefahren stellt nach wie vor ein Brandereignis eine massive potenzielle Bedrohung für die Verfügbarkeit eines Rechenzentrums dar. Durch vorbeugende präventive Brandschutzmaßnahmen kann dieses Risiko deutlich vermindert werden.

Auch für den Sachversicherungs-Underwriter ist es zunehmend von Interesse, das tatsächliche Gefährdungsexposure für ein Rechenzentrum zu ermitteln, um eine fundierte Underwriting-Entscheidung treffen zu können. Dazu gehört es, sog. Neben- sowie Naturgefahren mitzuberücksichtigen. Wichtig ist, dass für ein Exposure-orientiertes Underwriting ein aktueller Besichtigungsbericht vorliegt, da gerade bei Rechenzentren die Technologie, Infrastruktur und insbesondere Betriebsunterbrechungsszenarien einem ständigen Wandel unterliegen.

Weiterführende Literatur

Eckpunktepapier, Sicherheitsempfehlungen für Cloud-Computing-Anbieter – Mindestanforderungen in der Informationssicherheit
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile&v=8

Über den Autor

Leo Ronken *ist Senior Underwriting Consultant in der Abteilung Global Underwriting der Gen Re in Köln.*
Tel. +49 221 9738 939
E-Mail: leo.ronken@genre.com

Endnoten

1 Der Begriff des Cloud-Computings ist nicht einheitlich definiert; eine Definition der US-amerikanischen Standardisierungsstelle NIST (National Institute of Standards and Technology) beschreibt den Begriff als ein Modell, das es erlaubt, bei Bedarf jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können.The NIST Definition of Cloud Computing, https://csrc.nist.gov/publications/detail/sp/800-145/final.

2 Gartner Research, Cloud Shift Impacts All IT Markets, 26.10.2020.

3 www.uptimeinstitute.com/tiers.

4 Average cost per hour of enterprise server downtime worldwide in 2019, hrsg. von Thomas Alsop, 7.12.2020, https://www.statista.com/statistics/753938/worldwide-enterprise-server-hourly-downtime-cost/.

5 Christian Schubert: Millionen Webseiten von Brand beim Cloud-Betreiber betroffen, FAZ 11.3.2021, https://www.faz.net/aktuell/wirtschaft/digitec/brand-bei-cloud-betreiber-millionen-von-webseiten-betroffen-17238989.html; https://www.reuters.com/article/us-france-ovh-fire/fire-breaks-out-in-ovh-building-in-strasbourg-france-idUSKBN2B20NU.

6 Brand im Rechenzentrum: Warum eine Cloud-Strategie so wichtig ist, 7.4.2021, https://www.handelsblatt.com/technik/it-internet/it-dienstleister-brand-im-rechenzentrum-warum-eine-cloud-strategie-so-wichtig-ist/27074336.html?ticket=ST-2013868-D2EGJuwQcuHBElHfpaHF-ap1.

7 OVH to Shutter Second Strasbourg Data Center After Smoke Incident, Rich Miller, 20.3.2021, https://datacenterfrontier.com/ovh-to-shutter-second-strasbourg-data-center-after-smoke-incident/.

8 Philipp Anz, 26. März 2021, Erstes OVH-Rechenzentrum in Straßburg nimmt Betrieb wieder auf, https://www.inside-it.ch/de/post/erstes-ovh-rechenzentrum-in-strassburg-nimmt-betrieb-wieder-auf-20210326.

9 RZ-Brand in Straßburg ist noch nicht bewältigt, 14.4.2021, https://www.inside-channels.ch/de/post/rz-brand-in-strassburg-ist-noch-nicht-bewaeltigt-20210414.

10 Sind Daten in der Cloud wirklich sicher?, BR24, https://www.br.de/nachrichten/netzwelt/sind-daten-in-der-cloud-wirklich-sicher,SRq2lbb.

11 https://www.tuvit.de/de/leistungen/rechenzentren-colocation-cloud-infrastrukturen/trusted-site-infrastructure/.

12 https://www.din.de/de/meta/suche/62730!search?query=DIN+EN+50600.

13 Weitere Ausführungen sowie Hinweise zur Erstellung eines Business Continuity Plans: Business Continuity Management (BCM) – noch nie so wertvoll wie heute, General Reinsurance AG August 2020, https://www.genre.com/knowledge/publications/pmint20-3-de.html.

The people behind the promise®

genre.com | genre.com/perspective | Twitter: @Gen_Re

General Reinsurance AG
Theodor-Heuss-Ring 11
50668 Köln
Tel. +49 221 9738 0
Fax +49 221 9738 494