Eine kurze Einleitung ins Thema Rechenzentrum

Stephan Frey und Roger Weber, Co-Leiter der asut-Fachgruppe Data Center Infrastructure & Aihua Ries-Liu, OLOR AG

In den meisten Unternehmen werden alle wesentlichen strategischen und operativen Funktionen und Aufgaben durch IT massgeblich unterstützt oder sind sogar ohne IT nicht auszuführen. Die IT-Systeme der Unternehmen selbst und auch deren Anbindung an externe Netze müssen in einer angemessenen Umgebung und Infrastruktur betrieben werden. Nur so lässt sich die nötige Verfügbarkeit der IT sicherstellen. Die Anforderungen an die Leistungsfähigkeit dieser Systeme und der Netzumgebung steigen stetig an. Um diesem Leistungsbedarf gerecht zu werden, um entsprechende Reserven vorzuhalten und um die IT auch wirtschaftlich betreiben zu können, haben die Unternehmen ihre IT-Landschaft in Rechenzentren konzentriert.

Begriff Rechenzentrum

Laut BSI werden als Rechenzentrum die für den Betrieb von komplexen IT-Infrastrukturen (Server- und Speichersysteme, Systeme zur Datensicherung, aktive Netzkomponenten und Telekommunikationssysteme, zentrale Drucksysteme usw.) erforderlichen Einrichtungen (Klimatechnik, Elektroversorgung, überwachende und alarmierende Technik) und Räumlichkeiten (Rechnersaal, Räume für die aktiven Netzkomponenten, Technikräume, Archiv, Lager, Aufenthaltsraum usw.) bezeichnet.

Die Abgrenzung vom Rechenzentrum zum Serverraum besteht vor allem darin, dass in einem Rechenzentrum eine räumliche Trennung der IT-Systeme und der unterstützenden Infrastruktur (Elektroversorgung, Klimatechnik usw.) obligatorisch ist. Ein Rechenzentrum sollte insgesamt einen Sicherheitsbereich bilden, der in sich noch mindestens in den organisatorisch und physisch getrennten Sicherheitsbereich «Infrastruktur» und «IT» aufgeteilt wird.

Gesetze und Sicherheitsstandards

Die Integrität und die dauernde Verfügbarkeit von Daten und IT-Systemen sind eine notwendige Voraussetzung für die Aufrechterhaltung der Geschäftsprozesse. Dies wird im schweizerischen Recht an vielen Stellen angesprochen. Die Art und der Umfang der zu treffenden Sicherheitsmassnahmen sind gemäss geltenden Normen und Standards umzusetzen (Art. 7 DSG und Art. 8 VDSG). Die rasante Veränderung und die Weiterentwicklung der IT erfordern eine kontinuierliche Anpassung der Sicherheitslösungen an die neuen Technologien und Bedrohungen und führen zu einer zunehmenden Komplexität der IT-Sicherheitsaktivitäten.

Eine grosse Anzahl von Sicherheitsstandards kommt bei der Planung und Gestaltung von Rechenzentren zur Anwendung. Sie stellen einerseits eine Hilfestellung für den Verantwortlichen dar, definieren andererseits aber auch Anforderungen. Die gängigsten Standards sind ISO 27001/ISO 27002:2008, ITIL (IT Infrastructure Library), Basel III und des Sarbenes-Oxley-Act.

Planung und Konzeption

Betrachtet man die IT-Infrastruktur und die unterschiedlichen Funktionsbereiche der IT, können mit einer durchdachten Konzeption wesentliche Sicherheitsrisiken der physischen Sicherheit reduziert oder sogar ausgeschlossen werden. Eine entscheidende Rolle spielen einerseits die Standorte der IT-Bereiche und andererseits die räumliche Zuordnung der unterschiedlichen Funktionen zueinander.

Die Konzeption einer IT-Infrastruktur und somit auch die Standortauswahl eines Rechenzentrums basieren auf dem jeweiligen Datensicherungskonzept eines Unternehmens, das die Verfügbarkeitsanforderungen und unternehmenspolitische Ausrichtung widerspiegelt. Folgende Kriterien müssen bei Betrachtung der physischen Sicherheit eines Standortes berücksichtigt werden:

- Geringes Gefährdungspotenzial durch benachbarte Nutzungen, angrenzende Gebäudebereiche oder Funktionen
- Vermeiden von Risiken durch Medien-, Versorgungsleitungen, Erschütterungen, Chemikalien, die eine Beeinträchtigung der physischen Sicherheit der IT-Systeme darstellen

• Vermeiden möglicher Gefahren durch Elementarrisiken (Wasser, Sturm, Blitzeinschlag, Erdbeben) – Abschätzung regionaler Besonderheiten
• Rechenzentrum als separater, eigenständiger Funktionsbereich
• Schutz vor Sabotage durch «geschützte» Lage
• Einschätzung des Gefahrenpotenzials aufgrund der gesellschaftlichen Stellung des Unternehmens

Beim Aufbau eines Rechenzentrums werden die unterschiedlichen Funktionsbereiche (Sicherheitszonen) entsprechend ihres Anspruchs an die Sicherheit und ihrer Wertigkeit für den Funktionserhalt der IT angeordnet. Die Funktionsbereiche lassen sich so einteilen:

• Grundstück
• Halböffentlicher Bereich, angrenzende Büroflächen
• Operationsbereich, Nebenräume der IT
• Technische Anlagen zum Betrieb der IT
• IT- und Netzwerkinfrastruktur

Die einzelnen Sicherheitszonen werden durch Sicherheitslinien getrennt, und diese wiederum werden entsprechend den Sicherheitsanforderungen des Unternehmens ausgebildet.

Der Ausfall eines Rechenzentrums wird als Unternehmensgefährdung bis hin zur Insolvenz angesehen. Um für Katastrophen oder Ausfallzeiten gerüstet zu sein, wird in vielen Unternehmen ein zweites Rechenzentrum, räumlich vom Hauptrechenzentrum deutlich getrennt, in Betracht gezogen.

Infrastruktur/Bau

Die Räumlichkeiten zur Unterbringung der IT und ihrer Infrastruktur sind, wie im Datenschutzgesetz gefordert, dem aktuellen Stand der Technik anzupassen. Nur ein dem Stand der Technik genügendes Rechenzentrum rechtfertigt die getätigten Investitionen in die hard- und softwaretechnische Ausfallsicherheit.

Das Rechenzentrum im Gebäude ist möglichst in einem eigenen Brandabschnitt zu installieren. Es sollte nicht von aussen erkennbar sein.

Die Raumhüllen sollen dem für sensible Räume und für Fluchtwege empfohlenen Feuerwiderstandswert von mind. F90 bzw. F120 entsprechen.

Als Türen der sensiblen Bereiche müssen Objektschutztüren, welche den notwendigen Schutz gegen Feuer, Wasser, korrosive Brandgase und Einbruch bieten, eingesetzt werden.

Stand der Technik sind heute auch andere Gewerke wie beispielsweise ein hermetisch dicht abschliessendes Decke-Wand-Boden-System zum Schutz gegen eindringenden Rauch oder Wasser und eine mehrstufige Brandfrühesterkennung mit multiplen Ansaugstellen, auch im Doppelboden. Hinzu kommt die entsprechend dimensionierte autarke Löschanlage mit Überdruck- und Klimaschiebern.

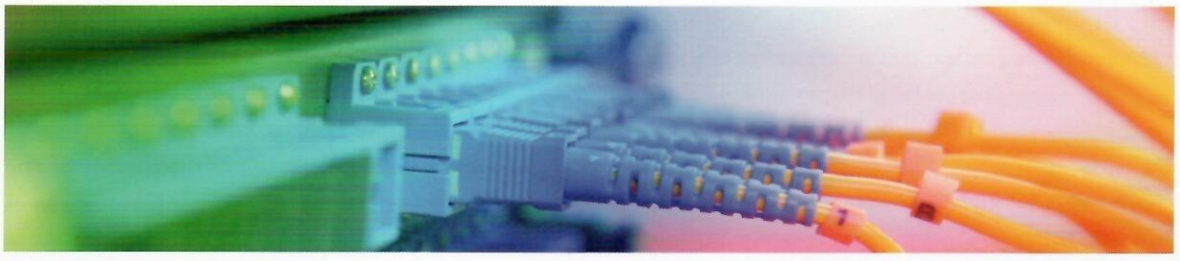
Klimatisierung

Die Klimatisierung der IT-sensiblen Räume ist redundant auszuführen. Die Stationierung der Rückkühleinheiten ist gegen Vandalismus zu schützen. Die Kühlleistungen der eingesetzten Systeme müssen den zukünftigen Bedürfnissen der IT angepasst werden können.

Vor dem Hintergrund der weiterhin steigenden Energiekosten ist bereits in der Planungsphase für ein Klimatisierungssystem der Energieeffizienz besondere Bedeutung zuzuordnen. Dabei sind die Gesamtkosten, also die Investitionskosten für die Neuanlage, und die zu erwartenden Betriebskosten über die gesamte Laufzeit zuzüglich Wartungskosten zu berechnen und zu bewerten.

Energieversorgung

Die Energieversorgung hat von der Elektrohauptverteilung zu erfolgen. Eine zweite redundante Stromversorgung ist zu planen. Um die möglichen negativen Folgen kurzer Stromausfälle zu vermeiden, sind USV-Systeme einzusetzen. Redundanzen sind beim Einsatz von USV-Anlagen anzuwenden. Je nach Energiedichte und gewählter Überbrückungszeit kann es erforderlich sein, Lüftungsgeräte, Kühlwasserpumpen oder auch Kühl-



aggregate/Kompressoren über eine USV-Anlage zu versorgen. Kurze Unterbrechungen oder lang anhaltende Stromausfälle sind durch Notstromanlagen zu überbrücken. Eine Netzersatzanlage sollte für einen kontinuierlichen Betrieb vorgesehen werden.

Kabelführungen

Die Trassen der Versorgungsleitungen des Gebäudes, zum Beispiel für Wasser oder Gas, dürfen nicht in unmittelbarer Nähe oder gar durch sensible Bereiche des Rechenzentrums verlaufen. Undichte Stellen können grössere Schäden verursachen, bis hin zum Ausfall des gesamten Informationsverbunds.

Zutritt/Überwachung

Sicherheitstechnisch – zum Schutze von Integrität, Vertraulichkeit und Verfügbarkeit der IT und Daten – sollte die Zutrittskontrolle mittels Kartenlesern, Biometrie usw. den Anforderungen der zu schützenden Bereiche entsprechend ausgelegt werden, dass sie die Identität, Aufenthaltsdauer, Datum und Zeit der eintretenden Person protokolliert und speichert. Durch Installation von Überwachungsmassnahmen und Fernanzeige von Störungen ist dafür vorzusorgen, dass eventuelle Schäden möglichst frühzeitig erkannt und geeignete Massnahmen so rasch eingeleitet werden können, dass die Schadensausbreitung so gering wie möglich ausfällt.

Fremdnutzungen

Sind im gleichen Gebäude verschiedene Unternehmen und Privatpersonen eingemietet, müssen die daraus resultierenden Risiken für ein Rechenzentrum beurteilt werden. Bei einem Gebäude in Fremdbesitz ist eine Einflussnahme auf die Mieterstruktur kaum möglich.

Notfallplanung

Ein Notfall- oder Katastrophenmanagement ist in jeder Konfiguration von Rechenzentren unabdingbar. Jeder Beteiligte muss im Ernstfall wissen, was zu tun und wer zu informieren ist. Die Grundlage dieses Wissens und Handelns ist das Notfallhandbuch, in dem alle relevanten Informationen über das Rechenzentrum, die eingesetzten Systeme und Infrastrukturen, die «schnelle Eingreiftruppe» sowie der Ablaufplan mit den Kontaktdaten aller Personen enthalten sein müssen. Zur Überprüfung der Notfallszenarien sind realistische und periodische Tests durchzuführen.

Durchschnittliche Lebensdauer

Ein Rechenzentrum hat eine durchschnittliche Lebensdauer von 10 bis 15 Jahren. Dann muss es gründlich überholt werden. □

Neue asut-Fachgruppe Data Center Infrastructure

Stephan Frey.

Roger Weber.

Durch das stetige Zusammenwachsen der ICT-Technologien entwickelt sich das Datacenter immer mehr zum Herzen der Telekommunikation. Der Bedarf an Datacenterflächen und -leistungen wird weiter wachsen und sich substanziell verändern. Aktuell existieren in der Schweiz schätzungsweise über 400 Datacenter, wovon etwa 50 mit Flächen von über 500 Quadratmetern (öffentliche wie auch firmeneigene). Die Investitionskosten für den Bau eines Datacenters nach neuesten Standards belaufen sich auf etwa 10000 bis 20000 Franken pro Quadratmeter. Jedes Jahr werden somit rund 200 bis 400 Millionen Franken für Datacenter verbaut. Viele mittlere und grosse Unternehmen müssen in den nächsten Jahren ihre Datacenterinfrastruktur aufrüsten, outsourcen oder neu bauen.

Die asut-Fachgruppe Data Center Infrastructure ist eine unabhängige nationale Drehscheibe rund um Datacenter, welche sich mit Themen wie Standortförderung, Energieeffizienz, Stromversorgung, Services, Datacenter Facility Management und Operations befasst und über einen interdisziplinären Kompetenzpool verfügt. Die Fachgruppe steht unter der Co-Leitung von Stephan Frey, ENKOM AG, und Roger Weber, Emerson Network Power-Knürr AG

Zielsetzungen: Data Center Infrastructure, als jüngste der vier asut-Fachgruppen, hat sich einerseits zum Ziel gesetzt, die Attraktivität für den Datacenterstandort Schweiz zu fördern, andererseits die energieeffiziente Nutzung und Sicherstellung der zukünftigen Stromversorgung sowie den Einsatz von weltweiten Best Practices zu fördern. Somit können Betreiber von konzentriertem Know-how profitieren und Unternehmen, welche in der Schweiz ihre Datacenterinfrastruktur auf- oder ausbauen möchten, auf die Kompetenz dieser Fachgruppe zurückgreifen.