Betriebssichere Rechenzentren

Leitfaden

Version 2

BITKOM

Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Albrechtstraße 10 A 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org
Ansprechpartner:	Holger Skurk Tel.: 030.27576-250 h.skurk@bitkom.org
Verantwortliches BITKOM-Gremium:	AK Rechenzentrum & IT-Infrastruktur
Redaktion:	Holger Skurk
Redaktionsassistenz:	Biliana Schönberg
Gestaltung / Layout:	Design Bureau kokliko / Anna Müller-Rosenberger (BITKOM)
Copyright:	BITKOM 2010
Titelbild:	Alejandro Mendoza, istockphoto.com

Betriebssichere Rechenzentren

Leitfaden

Version 2

BITKOM

Inhaltsverzeichnis

1 Einleitung

Die Planung, Ausführung und der Betrieb von IT-Infrastrukturen für unternehmenswichtige Anwendungen in betriebssicheren Rechenzentren stellen eine Herausforderung dar. So ist nicht nur die Auswahl von IT-Geräten zu berücksichtigen, auch die Ausführung des Rechenzentrums und der daraus resultierenden Anforderungen an Bauart und Baugröße, elektrische Leistung, Wärmeabführung, Verkabelung, Sicherheit und Verfügbarkeit sowie die Anschaffungs- und Betriebskosten sind entscheidende Faktoren.

Der vorliegende Leitfaden bietet eine Hilfestellung für die Planung und Implementierung eines Rechenzentrums. Damit ergänzt er existierende Standards und Vorschriften, die als Unterstützung herangezogen werden können.

Diese sind in ihren Forderungen oft sehr allgemein gehalten, der Leitfaden geht daher weiter und gibt konkrete Hinweise für die Gestaltung eines Rechenzentrums.
Er ergänzt die Matrix „Planungshilfe Betriebssicheres Rechenzentrum“, die wie der Leitfaden auf der BITKOM-Webseite zum kostenfreien Download zur Verfügung steht. Die Inhalte der Matrix sind in Auszügen in den Unterkapiteln des Leitfadens dargestellt. Der Leitfaden und die Planungshilfe ersetzen allerdings keinesfalls eine fachkundige Beratung und Unterstützung durch erfahrende Berater und Fachplaner.[1]

1 Es ist eine ständige Überarbeitung des Leitfadens durch den BITKOM-Arbeitskreis Betriebssicheres Rechenzentrum & IT-Infrastruktur vorgesehen. Dabei erfolgt sowohl eine Anpassung an die aktuellen Entwicklungen in Technik und bei sonstigen Rahmenbedingungen als auch eine Erweiterung, z.B. um Themen wie Anforderungen der Versicherungsbranche, Gefahrenmanagement, Prozesse und Services.

2 Verfügbarkeit eines Rechenzentrums

Die fortschreitende Entwicklung und Integration der Informationstechnologie in allen Geschäftsbereichen bedeutet, dass sich heutzutage kein Unternehmen einen Ausfall derselben leisten kann. Noch vor wenigen Jahren konnten viele Unternehmen mit einem, auch mehrstündigen, Ausfall ihrer IT Infrastruktur „überleben", heute steigt die Zahl derer, für die eine kontinuierliche Verfügbarkeit der IT unverzichtbar ist, stark an. Gemäß einer Studie der Meta Group kann ein 10-tägiger Ausfall von Schlüssel-Systemen der IT ein Unternehmen so nachhaltig schädigen, dass es mit 50% Wahrscheinlichkeit innerhalb der nächsten drei bis fünf Jahre vom Markt verschwindet.

Verfügbarkeitsklassen – US Uptime Institut

Tier-Klassen	Einführung	Erklärung
Tier I	60er Jahre	einfacher Stromversorgungspfad, einfache Kälteversorgung, keine redundanten Komponenten 99,671 % Verfügbarkeit
Tier II	70er Jahre	einfacher Stromversorgungspfad, einfache Kälteversorgung, redundante Komponenten 99,741 % Verfügbarkeit
Tier III	Ende der 80er	mehrere Pfade vorhanden, aber nur einer aktiv redundante Komponenten Wartung ohne Unterbrechung möglich 99,982 % Verfügbarkeit
Tier IV	1994	mehrere aktive Strom- u. Kaltwasserverteilungspfade, redundante Komponenten fehlertolerant 99,995 % Verfügbarkeit

Quelle: US Uptime Institut: Industry Standards Tier Classification

Bei der Erstellung und Erweiterung oder auch Überprüfung eines IT-Konzeptes ist heute von entscheidender Bedeutung, wie die Verfügbarkeit der IT-Infrastruktur des Unternehmens eingeschätzt wird. Die sich daraus ergebende Grundsatzfrage lautet:

„Wie hoch sind die maximalen tolerierbaren Ausfallzeiten der IT des Unternehmens?"

Als Konsequenz aus den wachsenden Anforderungen an die Verfügbarkeit einer IT-Infrastruktur erhöhen sich nicht nur die Anforderungen an die IT-Systeme selbst, sondern vor allem an eine kontinuierliche Sicherstellung der Umgebungsbedingungen und der Versorgung. Redundanzen in der Klima- und Stromversorgung, doppelte Einspeisungen und unterbrechungsfreie Wartungen der Systeme haben sich als Standard für hochverfügbare IT Infrastrukturen etabliert.

Bevor jedoch die mit der Planung und der Auslegung der technischen Komponenten für die angestrebte Verfügbarkeit begonnen wird, sind zusätzliche Betrachtungen hinsichtlich der Risikobewertung und der Standortwahl unumgänglich. Hierzu zählen insbesondere die möglichen Arealrisiken , welche geographisch (Luftverkehr, Hochwasser etc.), politisch (Kriege, Konfliktherde, Terror etc) und in Form der nachbarlichen Beziehungen (feuergefährdete Betriebsstätten wie Tankstellen, Chemiekalienlager etc.) Einfluß auf die Wahrscheinlichkeit eines potentiellen Ausfalls haben können. Weiterhin sollten auch potentielle deliktische Angriffe von eigenen Mitarbeitern und auch von außerhalb des Unternehmens in die Gesamtbetrachtung einfließen.

Eine Forderung nach hoher Verfügbarkeit beinhaltet jedoch nicht nur die Auseinandersetzung mit technischen Lösungsmöglichkeiten, sondern verlangt vom Betreiber auch Ansätze und Ausführungen für eine umfassende organisatorische Struktur. Dazu zählt z.B. die Bereithaltung von geschultem Servicepersonal, von Ersatzteilen oder eines Wartungsvertrages. Hinzu kommen auch genaue Instruktionen über das Verhalten im Fehler- oder Notfall. Weiterhin muss eine solche Struktur auch eine schnelle, exakte und zielgerichtete Kommunikation und eine nachvollziehbare Protokollierung der Ereignisse ermöglichen.

Der Begriff „Verfügbarkeit“ bezeichnet die Wahrscheinlichkeit, dass ein System zu einem gegebenen Zeitpunkt tatsächlich wie geplant benutzt werden kann. Damit ist Verfügbarkeit ein quantitativ fassbares und bestimmbares Maß. Man unterscheidet zwischen qualitativen Verfügbarkeitsklassen wie in nachfolgender Tabelle „Verfügbarkeitsklassen nach HV-Kompendium (des BSI)“ aufgeführt. Damit ist die Verfügbarkeitsklasse eines Dienstes ein Maß für seine Qualität hinsichtlich der Dimension Verfügbarkeit mit der Einheit Stunde/Jahr

Ein System wird als verfügbar bezeichnet, wenn es in der Lage ist, die Aufgaben zu erfüllen, für die es vorgesehen ist. Die Verfügbarkeit wird als Verhältnis aus fehlerbedingter Stillstandszeit (= Ausfallzeit) und Gesamtzeit eines Systems bemessen.

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

Berechnet man mit der obigen Formel die Verfügbarkeit im Zeitraum eines Jahres, so bedeutet eine Verfügbarkeit von 99,99% beispielsweise eine Stillstandszeit von 52,6 Minuten.

99 % * 87,66 Stunden/Jahr
99,9 % * 8,76 Stunden/Jahr
99,99 % * 52,6 Minuten/Jahr
99,999 % * 5,26 Minuten/Jahr
99,9999 % * 0,5265 Minuten/Jahr

Das Bundesamt für Sicherheit in der Informationstechnik hat folgende Verfügbarkeitsklassen definiert:.

Verfügbarkeitsklasse	Bezeichnung	Kumulierte, wahrscheinliche Ausfallzeit pro Jahr	Auswirkung
VK 0 ~95%	Keine Anforderungen an die Verfügbarkeit	ca. 2-3 Wochen	Hinsichtlich der Verfügbarkeit sind keine Maßnahmen zu treffen. Die Realisierung des IT-Grundschutzes für die anderen Grundwerte wirkt sich förderlich auf die Verfügbarkeit aus.
VK 1 99,0%	Normale Verfügbarkeit	Weniger als 90 Std.	Hinsichtlich der Verfügbarkeit erfüllt die einfache Anwendung des IT-Grundschutzes (BSI 100-1 und BSI 100-2) die Anforderungen
VK 2 99,9%	Hohe Verfügbarkeit	Weniger als 9 Std.	Die einfache Anwendung des IT-Grundschutzes ist zu ergänzen durch die Realisierung der für hohen Verfügbarkeitsbedarf empfohlenen Bausteine, z.B. die Bausteine B 1.3 Notfallvorsorge, B 1.8 Behandlung von Sicherheitsvorfällen und die Anwendung der Risikoanalyse auf der Basis von IT-Grundschutz (BSI 100-3).
VK 3 99,99%	Sehr hohe Verfügbarkeit	Unter 1 Std.	Realisierung der nach IT-Grundschutz für ausgewählte Objekte empfohlenen Maßnahmen mit besonderem Einfluss auf den Grundwert Verfügbarkeit, z.B. die Maßnahme M 1.28 USV im Serverraum oder M 1.56 Sekundär-Energieversorgung im Rechenzentrum, ergänzt durch HV-Maßnahmen aus dem HV-Kompendium
VK 4 99,999%	Höchste Verfügbarkeit	ca. 5 Min.	IT-Grundschutz ergänzt durch Modellierung nach dem HV-Kompendium. IT-Grundschutz als Basis wird zunehmend durch HV-Maßnahmen ersetzt und ergänzt.
VK 5 100%	disastertolerant	–	Modellierung nach dem HV-Kompendium. IT-Grundschutz dient weiterhin als Basis für die vorstehenden Bereiche sowie die anderen Schutzwerte Integrität und Vertraulichkeit.

Tabelle 1: Verfügbarkeitsklassen nach BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Bewertungssystem für Rechenzentren VAIR (Verfügbarkeitsanalyse der Infrastruktur in Rechenzentren) entwickelt. Unter www.vair-check.de können RZ-Betreiber anonym und kostenlos die Daten der Infrastruktur Ihres Rechenzentrums eingeben und die Ausfallsicherheit des Rechenzentrums überprüfen.

3 Einfluss von Sicherheitsstandards auf die Gestaltung von Rechenzentren

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 wichtigsten Normen aus dem Bereich ISMS (Information Security Management Systems) sowie ITIL (IT Infrastructure Library) und der Sarbanes-Oxley-Act werden hier vorgestellt.

3.1 ISO 27001 / ISO 27002:2008

Die seit Oktober 2005 geltende Normenreihe ISO/IEC 27001 dient dem Schutz von Informationen als Geschäftswerte vor Bedrohungen. Sie gewinnt an Bedeutung, da sie die Basis schafft, um Unternehmen in die Lage zu versetzen, Anforderungen dritter Instanzen zu genügen. Das sind beispielsweise gesetzliche Anforderungen (wie KonTraG, HGB sowie GoB, GoBS, GDPdU, BDSG, TMG, TKG, StGB),), vertragliche Anforderungen (z.B. von Kunden) oder sonstige Anforderungen. Die Norm ersetzt die bisher bekannte britische Standardnorm BS 7799-2, die im Februar 2006 ersatzlos zurückgezogen wurde.

In der betriebswirtschaftlichen Fachsprache wird der Begriff Compliance verwendet, um die Einhaltung von Gesetzen und Richtlinien, aber auch freiwilligen Kodizes in Unternehmen zu bezeichnen

Die ISO/IEC 27001 unterstützt das Aufsetzen eines Prozesses für den Aufbau und das Betreiben eines Sicherheits-Management-Systems. Dieser Prozess der stetigen Verbesserung arbeitet in den vier bekannten Schritten: „Plan, Do, Check, Act“, “, wie dies auch von der ISO 9001 (Qualitätsmanagement) her bekannt ist.

Eine wesentliche Hilfe wird auch durch die vom BSI (Bundesamt für Sicherheit in der Informationstechnik) seit vielen Jahren fortentwickelten Grundschutz-Handbücher (Leitfäden und Kataloge) nach „ISO 27001, basierend auf IT-Grundschutz“ geboten. Die Bausteine in den Katalogen sind sehr wertvoll bei der Umsetzung eines Informationssicherheits-Managementsystems.

In der Planungphase des Prozesses (PLAN-Phase) wird das ISMS geplant. Vor allem werden hier der Anwendungsbereich und Grenzen des ISMS festgelegt und dann von Management freigegeben. Hier wird unter anderem eine Risikoanalyse durchgeführt. Diese ermittelt, welche Systeme und Applikationen in Bezug auf die Aufrechterhaltung des Geschäftsbetriebes eines Unternehmens von Bedeutung sind und wie hoch die Abhängigkeit von entsprechenden Systemen und Applikationen ist. Abgeleitet aus den Ergebnissen werden Aussagen über den Schutzbedarf getroffen und der Verfügbarkeitsanspruch an entsprechende Systeme und Applikationen ermittelt.

Die Implementierungsphase (DO-Phase) beinhaltet konkrete Maßnahmen zur Risikominimierung und RisikoerkennungRisikoerkennung mittels eines Risikobehandlungsplanes. Die ISO 27002:2008 (früher 17799) gibt als „Leitfaden für das Informationssicherheits-Management“ wertvolle Hinweise für die Erfüllung der in der ISO 27001 aufgeführten „Controls/Maßnahmen“. Sie ist praktisch die Anleitung zur Umsetzung der ISO 27001.Hier werden unter dem Punkt 9 „Physische und umgebungsbezogene Sicherheit“ auch die Maßnahmen und Umsetzungsvorschläge für Räume und Infrastrukturen benannt. Zertifizierungen erfolgen nur auf Grund der ISO 27001 bzw. nach BSI ISO 27001, basierend auf IT-Grundschutz

Im Rahmen eines regelmäßigen Monitorings und periodisch stattfindender Audits (CHECK-Phase) werden

implementierte Maßnahmen regelmäßig überprüft, um Verbesserungspotentiale abzuleiten (zum Beispiel Monitoring-Mechanismen des Brandschutzes, Brandschutztests).

In der vierten Phase (ACT-Phase) werden die Maßnahmen umgesetzt, die im Vorfeld als Verbesserungen definiert wurden.

3.2 ITIL

Eine wichtige Größe bei der Planung und dem Betrieb eines „Betriebssicheren Rechenzentrums" ist das „IT-Service-Management". Seit Ende der 80er Jahre gibt es Best Practice Empfehlungen für IT-Service Management, als die Central Computer and Telecommunications Agency der britischen Regierung (früher CCTA, heute OGC) die ersten Elemente der IT-Infrastructure Libary (ITIL) veröffentlichte. Die schriftlich niedergelegten Richtlinien reichen von detaillierten Ratschlägen zu einzelnen Prozesse innerhalb der ITIL über Verfahrensregeln bis zur jetzt neu erschienenen Norm ISO 20000 (früher BS 15000).

Bei bestehenden Rechenzentren orientieren sich Kunden auch an einem Service-Management-System nach ITIL. Dienstleistungsrechenzentren sehen sich des Öfteren mit Ausschreibungen konfrontiert, die im teilnehmenden Unternehmen ITIL voraussetzen.. Zwei Kernbereiche sind dabei immer enthalten:

- Service-Support
- Service-Delivery

Das Regelwerk ist auf alle IT-Organisationen in allen Unternehmen – gleich welcher Größe – anwendbar.

3.3 Sarbanes Oxley Act und SAS 70

Der Sarbanes Oxley Act (SOX) ist ein US-Gesetz zur Verbesserung der Unternehmensberichterstattung und wurde als Folge der Bilanzskandale von Unternehmen wie Enron oder Worldcom erlassen. Das seit 30. Juli 2002 gültige Gesetz hat nicht nur Auswirkungen auf Finanzdaten, sondern fordert auch die Sicherheit im IT-Bereich.

Das Gesetz gilt zunächst für alle an amerikanischen Börsen notierten Unternehmen. Dann aber auch für Nicht-US Unternehmen, die eine an einer amerikanischen Börse notierte Mutter- oder Tochtergesellschaft haben.

Im Rahmen des Sarbanes-Oxley Acts müssen Unternehmensprozesse beschrieben, definiert und Kontrollverfahren festgelegt werden, die das Risiko eines falschen Bilanzausweises minimieren sollen. Die Prüfung von Unternehmen durch zugelassene Wirtschaftsprüfer erfolgt dabei nach der „SAS 70" Frageliste. Diese wiederum basiert im Wesentlichen auf dem Regelwerk „Cobit 4.1" der ISACA (USA). Hat ein Unternehmen, für welches SOX als Forderung zutrifft, zum Beispiel einzelne Systeme oder gar die gesamte IT ausgelagert (Outsourcing), schlägt die SAS-70-Frageliste auch auf den entsprechenden Provider durch, die Verantwortung bleibt immer beim jeweiligen Auftraggeber. In diesem Fall besteht die Möglichkeit, dass Wirtschaftsprüfer des Kunden im Service-Rechenzentrum nach SAS 70 prüfen oder das Rechenzentrum selbst die Prüfung durchführen lässt. Der Bericht des Wirtschaftsprüfers darf nicht älter als sechs Monate ab Zeitpunkt des Jahresabschlusses des Kunden sein. Deshalb müssen SOX-Prüfungen im Wesentlichen zweimal jährlich durchgeführt werden, was einen sehr hohen Aufwand bedeutet.

Auf internationaler Ebene wurden mögliche Konflikte des Sarbanes-Oxley Acts mit nationalen Vorschriften diskutiert. Eine Lösung der Konflikte ist derzeit noch weitestgehend ungeklärt. Es ist aber ein „Euro-SOX" in Arbeit. Ausserdem ist das IDW (Institut der Wirtschaftsprüfer) dabei, seine Vorgaben für die Prüfungsanforderungen an Cobit 4.1 zu orientieren.

3.4 Bewertung der Standards

Die dargestellten Standards werden häufig von Kunden, Zertifizierungsgesellschaften, Wirtschaftsprüfern und anderen Institutionen überprüft. Man kann darüber

streiten, ob durch Sarbanes Oxley und SAS 70 ein Rechenzentrum betriebssicherer wird – die in der ISO/IEC 27002:2008 und ISO/IEC 27001:2005 enthaltenen allgemeinen Forderungen nach Maßnahmen zur Verbesserung der Sicherheit sind aber durchweg berechtigt und sinnvoll. ITIL und ISO 20000 sichern und verbessern die Prozesse eines Rechenzentrums nachweislich. Im Bereich Öffentlicher Auftraggeber wird oft die Zertifizierung nach BSI verlangt – hier ist allerdings der Aufwand für Dokumentation und Betrieb des ISMS sehr hoch. Besser ist die Kombination von ISO 27001 mit Anlehnung an IT-Grundschutz (wo sinnvoll), also nicht die Zertifizierung durch das BSI, Bonn.

4 Basis der IT-Infrastruktur: Das Rack

Ob separates Rechenzentrum oder einzelner Serverschrank: Die Basis für eine sichere Unterbringung der IT-Systeme bildet immer das Rack. Da die IT-Systeme in den meisten Unternehmen aus standardisierten 19-Zoll-Komponenten bestehen, bieten skalierbare und flexible Rack-Systeme in dieser Bauweise die beste Wahl beim Aufbau einer tragfähigen IT-Infrastruktur. Sie gewährleistet das passgenaue Zusammenspiel von System- und Supportkomponenten wie Stromversorgung und Klimatisierung. Ob ein Unternehmen seine IT-Systeme in einem eigenen Rechenzentrum oder als Stand-alone-Lösung in einzelnen Serverschränken unterbringt, hängt von den Anforderungen an die IT und den baulichen Voraussetzungen ab. Für beides gelten aber gleiche Brandschutz- und weitere Sicherheitsnormen, denn sie sollen die ITK-Systeme und -Daten in ihrem Inneren schützen.

4.1 Sicherer Serverschrank

Ein sicherer Serverschrank sollte möglichst modular aufgebaut sein. Er ermöglicht dem Unternehmen angemessene Sicherheit bei überschaubaren Kosten. Ein modularer Schrank kann bei Bedarf ab- oder umgebaut werden und an anderer Stelle eingesetzt werden. Auch bei einem Umzug hat ein solch flexibles System Vorteile beim Transport und der Neuaufstellung.

Die Modularität hat ebenso eine Bedeutung für die Erweiterung bei Einhausungslösungen oder Klimatisierungskonzepten.

Bei der Planung eines sicheren Serverschrankes – wie auch für ein betriebssicheres Rechenzentrum – sind folgende Eigenschaften für die durchgängige Sicherheit und Verfügbarkeit der Systeme notwendig:

- Sicherstellen einer gleich bleibenden Temperatur und Luftfeuchtigkeit durch eine Präzisions-Klimatisierung
- Sicherstellen der Stromversorgung durch unterbrechungsfreie Stromversorgung (USV) und gegebenfalls zusätzlicher Notstromversorgung
- Schutz gegen Femdzugriff (Verschluss-Systeme, netzwerküberwachter Rackzugang, biometrische Datenerfassung)
- Brandvorsorge und -reaktion
- Einbindbarkeit der Module in ein zentrales Monitoring- und Management-System

Ein wichtiger Punkt bei allen Rack-Lösungen ist das Thema Stabilität. Durch die hohe Packungsdichte moderner Server-Systeme und Speicherlösungen sowie durch die enthaltenen Netzteile, werden je nach Einsatzfall Server-Racks mit bis zu 1.000 kg Tragkraft benötigt. Dementsprechend müssen auch Geräteböden und Gleitschienen für hohe Lasten ausgelegt sein. Bis zu 150 kg pro Boden oder Schiene können derzeit realisiert werden.

Ein weiteres wichtiges Thema ist die Kabeleinführung. Bei immer schnelleren Netzen in Verbindung mit Kupferverkabelung ist es unerlässlich, Strom- und Datenkabel getrennt voneinander einzuführen, damit sie sich nicht gegenseitig durch Störeinstrahlung beeinflussen. Bei der Rackauswahl sollte unbedingt auch auf ein einfach zu integrierendes Stromverteilungs-System geachtet werden, denn letztlich ist die Stromversorgung die Voraussetzung für eine verfügbare IT. Eine abgesicherte Niederspannungs-Unterverteilung sollte ebenfalls vorhanden sein, wie auch ein flexibles Stromverteilungssystem im Rack, das sowohl mit der Netzstromversorgung als auch mit einer unterbrechungsfreien Stromversorgung (USV) abgesicherten Versorgung verbunden werden kann. Moderne Lösungen bringen bis zu 88kW in ein Rack. Möglich wird dies durch vier unabhängige, dreiphasige Strom-Einspeisungen, die eine sichere Stromversorgung auch bei steigenden Anforderungen garantieren.

Mit steigender Serverleistung und Packungsdichte im Rack, ist die Bedeutung von Belüftungskonzepten wie perforierte Türen und Abschottungen zwischen Warm- und Kaltbereichen im Rack enorm gestiegen.Weitere leistungssteigernde, energetisch optimierte Lösungen können durch Kalt- bzw. Warmgangeinhausungskonzepte, die

zur Racklösung gehören, umgesetzt werden.Bei extremen Verlustleistungen im Rack sind wassergekühlte Lösungen in Form von Luft-/Wasserwärmetauschern unumgänglich.

Beides, Stromabsicherung und Klimatisierung, lassen sich durch in die Infrastruktur integrierte Sensoren überwachen. Kabelgebunden oder über Funk registrieren die Fühler die Feuchtigkeit, die Temperatur, aber auch die Leistungsaufnahme der Server Ein modernes sensorenbasiertes Überwachungssystem übernimmt möglicherweise auch die Zugangssteuerung gleich mit.

4.1.1 Inventarisierung im Serverschrank

In Rechenzentren – besonders ab einer bestimmten Größe – ist es schwer, den Überblick über die vorhandenen Hardware-Komponenten zu behalten. Zwar ist es heute möglich, mit jedem intelligenten IT-Device zu kommunizieren, aber die physische Zuordnung zum Rack und der entsprechenden Höheneinheit ist problematisch. Auch die Gerätestruktur in den einzelnen Schränken mit Servern, Lüftern, USV, etc. ist häufig nicht transparent. Vor diesem Hintergrund gestaltet sich die Inventarisierung und stetige Aktualisierung der Daten über die Verteilung der Komponenten im Rechenzentrum aufwendig und meist auch zeitraubend. In vielen Fällen wird die vorhandene manuell erfasste Dokumentation nicht auf Richtigkeit überprüft. Diese Angaben sind aber notwendig, um gerade im Fehlerfall Entscheidungen treffen zu können.

Ein weiteres Problem ist die Halbwertszeit der erhobenen Informationen: Die Erfassung und Aktualisierung stellt immer eine Momentaufnahme des RZ-Inventars dar. Eine effiziente Rackbelegung und transparente Komponentenadministration bedürfen jedoch ständig aktueller und somit verlässlicher Daten.

Um immer auf aktuelle Inventurdaten zurückgreifen zu können, gibt es moderne Inventarisierungssysteme direkt im Rack, um die Komponentenbestückung der 19“ Ebene komplett berührungslos zu erfassen.

Die Darstellungen der Rackkonfigurationen stehen zum einen visuell auf einer Webseite des zugehörigen Überwachungssystems zu Verfügung, zum anderen ist eine Listenform abrufbar, ein Datenim-/export über das XML-Dateiformat ist ebenfalls möglich. Diese Datensätze können dann z.B. in externen Datenbanken weiterverarbeitet werden und erleichtern die tägliche Arbeit bei der Optimierung eines Rechenzentrums ganz erheblich.

4.2 Netzwerktechnik

Zu einer vollständigen Betrachtung von Rechenzentren unter Sicherheitsaspekten gehört neben den Servern auch das Thema Netzwerktechnik. Viele Unternehmen haben bereits ihre Telefonanlagen auf Voice over IP (VoIP) umgestellt. Virtualisierte Clients sind der nächste Schritt. Damit werden immer mehr geschäftskritische Basisdienste über die Datenleitungen abgewickelt, die mit Power over Ethernet (PoE) auch die Stromversorgung der Endgeräte übernehmen. Mit der wachsenden Bedeutung der Netzwerktechnik für einen störungsfreien Geschäftsbetrieb, steigen auch hier die Sicherheitsanforderungen.

Wie bei den Servern bildet auch bei der Netzwerktechnik das Rack die Grundlage der Unterbringung. Da die aktiven Komponenten ebenfalls auf 19 Zoll standardisiert sind, basieren Netzwerkschränke in der Regel auf der gleichen Plattform. Auch was Stabilität sowie Brandschutz und Zugangskontrolle angeht, herrschen hier vergleichbare Anforderungen. Da die im Gebäude verbaute Netzwerkinfrastruktur aber in der Regel für mehr als 10 Jahre angelegt ist, empfiehlt es sich, bei der Anschaffung der Netzwerkschränke langfristig zu planen und auf Flexibilität beim Zubehör zu achten. So lassen sich auch zukünftige Entwicklungen sicher abdecken. Denn beim Innenausbau bestehen deutliche Unterschiede zwischen den Racks.

Durch das häufige Umswitchen an den Anschlussstellen der Netzwerkkomponenten, den sogenannten Ports, müssen die Kabel in den Netzwerkschränken deutlich häufiger neu verlegt werden als das in Serverschränken der Fall ist. Diese auch MACs (Moves, Adds, Changes) genannten Bewegungen und die steigende Portdichte lassen dem

Kabelmanagement besondere Bedeutung zukommen. Das beginnt bei den Dachblechen und Sockeln. Einfaches Einführen an diesen Stellen erleichtert die Nachrüstung und sorgt für kurze Kabelwege. Rangierkanäle und Führungspaneele schaffen eine saubere Feinverteilung im Rack. Dabei sollte gerade beim Kabelmanagement auf die Stabilität der Komponenten Wert gelegt werden. Denn moderne stromführende Netzwerkkabel sind deutlich schwerer und steifer als ihre Cat-5-Vorgänger.

Ein Thema, das bei Netzwerkschränken derzeit an Bedeutung gewinnt ist die Klimatisierung. Switches und Router werden leistungsfähiger und produzieren mehr Abwärme. Daher ist auch hier auf die Ausbaumöglichkeiten zu achten. Das Spektrum reicht von passiver Klimatisierung über Dachbleche, Entlüftungsaufsätze oder doppelwandige Gehäuse über Lüfter bis hin zu Dachkühlgeräten.

4.3 Betriebssicheres Rechenzentrum

Neben den oben bereits genannten, grundsätzlichen Anforderungen an ein betriebssicheres Rechenzentrum (BRZ), gibt es bei den baulichen Maßnahmen noch viele Projektdetails zu klären.

Als Erstes sollte eine genaue Risiko- und Schwachstellenanalyse im Unternehmen erarbeitet werden, die mögliche Gefahren für die IT-Systeme aufzeigt. Das betrifft die Zuständigkeit für die Planung und den Bau eines Rechenzentrums, die Zugangsberechtigungen bis hin zu regelmäßigen Sicherheitsüberprüfungen durch unabhängige Auditoren.

In die Planung, den Bau und den Betrieb eines Rechenzentrums sind verschiedene Verantwortliche eingebunden. Neben IT-Fachleuten sind das auch Gebäudespezialisten wie Architekten, Bauingenieure sowie Fachplaner für Klima, Energie oder Gefahrenabwehr, die Organisationsabteilung und nicht zuletzt die Geschäftsführung.

Die physikalischen Anforderungen an ein Rechenzentrum bestehen nicht nur aus den reinen IT-Themen wie Anzahl und Typ der einzusetzenden Server, Netzwerk- und Speichergeräte, sondern auch aus der Gefahrenvermeidung und -abwehr.

Zur möglichen Ausstattung des Rechenzentrums gehört ein modularer (weil erweiter-/ veränderbar), feuerfester, möglichst zertifizierter Sicherheitsraum. Auch der Einsatz einer stabilen, mehrschichtigen Feuerschutztür mit gleichen Schutzwertigkeiten wie der Sicherheitsraum ist Pflicht. 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 kommen die entsprechend dimensionierte autarke Löschanlage mit Überdruck- und Klimaschiebern, die personenbezogene Zutrittskontrolle mittels Kartenleser oder biometrischen Methoden und eine Überwachung der Peripherie des Rechenzentrums durch LAN-Videotechnik.

Für den flexiblen Ausbau von Rechenzentren ist es von Vorteil, mit Planern und Lieferanten zusammen zu arbeiten, die eine langfristige Verfügbarkeit der Produkte sicherstellen können.

5 Energie, Klimatisierung und Kühlung

5.1 Energieversorgungsunternehmen (EVU) - Stromverteilung und Einspeisung ins Unternehmen

5.1.1 Ausgangssituation

Eine entscheidende Bedeutung beim Betreiben von Serverschränken oder ganzen Rechenzentren kommt der Stromversorgung zu.

Die Kette der Stromversorgung beginnt bei den Stromversorgungsunternehmen, die Primärenergie erzeugen und liefern. Die Primärenergieerzeuger transportieren den Strom mittels Leitungen über Hochspannungsmasten zu den Mittelspannungsstationen. Von den Mittelspannungsstationen wird der Strom über Erdkabel bis zu den Transformatorstationen geführt. Transformatorstationen befinden sich meist in größeren Gebäuden sowie am Straßenrand auf speziell dafür eingerichteten Grundstücken.

Große Rechenzentren mit mehreren 1.000 Quadratmetern Rechenzentrumsfläche haben vielfach eine zusätzliche Einspeisung über eine zweite Mittelspannungsstation, so dass eine volle Redundanz – also die mehrfache Auslegung zur Erhöhung der Verfügbarkeit - sogar bis zu den Kraftwerken besteht.

Mögliche Ursachen für eine Unterbrechung der Stromversorgung können sein:

- technische Fehler in den Geräten (zum Beispiel Servern und deren Komponenten)
- technische Fehler in der Stromverteilung (zum Beispiel Leitungen, Unterverteilungen)
- Fehler in den Stromersatzlösungen (zum Beispiel Netzersatzanlagen auch Notstromdiesel genannt, batteriegepufferte unterbrechungsfreie Stromversorgungsanlagen (USV-Anlagen))
- Prozessbedingte Fehler (zum Beispiel Fehler in der Konzeption der Stromversorgung, logistische FehlerBeispiele aus der Vergangenheit zeigen, wie dramatisch Situationen eskalieren können, wenn die Stromversorgung länger ausfällt und keine Stromersatzlösung vorhanden ist. Die allgemeine Stromversorgung kann in großen Gebieten für mehrere Tage zum Erliegen kommen. Anhand solcher Schadensmeldungen ist leicht verständlich, wie notwendig gerade in unternehmenskritischen Bereichen, zum Beispiel der IT, eine autarke Stromversorgung ist.

Für den Bau von Rechenzentren existieren keine vorgefertigten Stromversorgungslösungen aus der Schublade. Es gibt jedoch einige Prinzipien für die Stromversorgung, die individuell anzupassen sind. Die Herausforderung für den Planer besteht darin, diese Prinzipien auf den Kunden, seine Wünsche und Bedürfnisse und nicht zuletzt auch auf sein Budget hin umzusetzen.

5.1.2 Funktionsweise der Infrastruktur

Zur Stromversorgung gibt es so genannte Ringleitungen, deren Strom in den Trafostationen auf 400 V herunter transformiert und über Kabel oder Stromschienen über die Niederspannungshauptverteilung und Normalnetzverteilung ins Rechenzentrum gelangen. Die Normalnetz-Unterverteilung versorgt auch die unterbrechungsfreien Stromversorgungsanlagen (USV) mit Strom.

Der Ausgang der USV Anlagen wird über die USV Unterverteilungen geführt und von dort aus zu den einzelnen Serverschränken. Dafür sind z. B. im Doppelfußboden Abzweigdosen oder Abgangskästen vorgesehen. Von den Abzweigungen beziehungsweise den Abgangskästen erfolgt die Versorgung mittels weiterer Leitungen bis zu den Netzteilen (NT) der Server im Schrank. Bei nur einer USV Anlage werden die Netzteile A und B gemeinsam versorgt, bei zwei USV Anlagen jeweils getrennt. Das steigert die Verfügbarkeit durch eine 2 x N Versorgung.

5.1.3 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten

RZ Kategorie	EUV-Einspeisung Serverschrank bis zu 5 kW	EUV-Einspeisung Serverschrank ab 5 kW bis zu 30 KW	EUV-Einspeisung Rechenzentrum / Serverraum 500 bis zu 2500 Watt/qm	zulässige RZ Ausfallzeit*
A	Standard			72 h
B	Standard			24 h
C	Redundante Einspeisungen			1 h
D	Redundante Einspeisungen			10 min
E	Redundante Einspeisungen von verschiedenen Umspannwerken			0 min

Tabelle 2 aus BITKOM-Matrix „Planungshilfe betriebssicheres Rechenzentrum“ – EVU Einspeisung

Die Kategorien A und B sind zurzeit in vielen Betrieben des Mittelstandes realisiert, oftmals sogar ohne Einspeisemöglichkeit für eine mobile Netzersatzanlage (NEA). Diese Variante stellt bei genauer Betrachtung jedoch keine wirkliche Sicherheit dar und vertraut lediglich den Energieversorgern. Immer wieder hört man die Aussage, “.....es wird schon nichts passieren. Bisher ist auch noch nie etwas passiert....“. Fällt jedoch nur ein Glied aus der Versorgungskette aus, ist sofort die gesamte EVU-Einspeisung unterbrochen und die Stromversorgung muss über die USV Anlage vorgenommen werden. Die Überbrückungszeit einer USV-Anlage ist in aller Regel stark begrenzt. Sie ist abhängig von der Anzahl der vorhandenen Batterien und der zu erbringenden Leistung. Ein Ausfall von mehr als 30 Minuten kann im Allgemeinen mit einer USVöAnlage nicht überbrückt werden. In diesem Falle sollte automatisch eine funktionierende Rechner-Shutdown-Routine eingeleitet werden, die Benachrichtigungen absetzt, Daten speichert, Applikationen schließt und letztendlich die Rechner ordnungsgemäß herunterfährt.

Bei der Planung ist also besonders darauf zu achten, dass die Überbrückungszeit der USV Anlage größer ist als die Zeit, die für den Transport und Anschaltung einer mobilen NEA anfällt. Bei obiger Konstellation werden in der Regel Batterien eingesetzt.

Die Kategorie C bietet ein höheres Sicherheitspotential. Hier erfolgt die Stromversorgung bereits ab der Niederspannungshauptverteilung in redundanter Ausführung. Fällt ein Versorgungsweg hinter der Niederspannungshauptverteilung aus, wird automatisch über den zweiten, redundanten Weg versorgt. Fällt der primäre Energieversorger aus, ist die Stromversorgung immer noch über die mobile Netzersatzanlage sichergestellt.

Bei der Kategorie C kommt im Gegensatz zur Kategorie A und B eine zweite USV mit zwei eigenen USV-Unterverteilungen hinzu. Hierdurch ist bereits eine redundante Versorgung von den USV-Anlagen bis zu den Netzgeräten der Server möglich.

Die Kategorie D zeichnet sich gegenüber der Kategorie C dadurch aus, dass die Versorgung über zwei verschiedene Trafostationen und der jeweils nachgeschalteten, ebenfalls redundanten Infrastruktur sichergestellt wird. Außerdem übernimmt im Falle eines Stromausfalls seitens des Energieversorgers die stationäre Netzersatzanlage die elektrische Versorgung. Diese Kategorie stellt eine sehr hohe Sicherheitsstufe dar.

Die Kategorie E ist das „non plus ultra“. Es existiert nicht nur eine zusätzliche Redundanz über eine zweite Netzersatzanlage, sondern auch noch eine zusätzliche Einspeisung aus einer weiteren unabhängigen

Mittelspannungsstation. Allerdings muss fast immer die zweite Kabelzuführung von einer anderen Mittelstation durch den jeweiligen Primärenergieversorger erst hergestellt werden. Das bedeutet, dass eventuell mehrere Kilometer Kabel neu zum Standort des Rechenzentrums verlegt werden müssen, was sehr kostenintensiv ist und bereits bei der Kalkulation berücksichtigt werden sollte.

Unabdingbar zum Erhalt der Verfügbarkeit ist die regelmäßige Prüfung und Wartung der kompletten Infrastruktur durch qualifiziertes Personal sowie die Beachtung der Vorgaben, und Richtlinien zum Betrieb der Anlagen.

5.2 Stromverteilung im Unternehmen

5.2.1 Ausgangssituation

Über die Elektroverteilungen werden die Leistungen des Normalnetzes, des Generators und der USV an die zu versorgenden Geräte, Anlagen und Beleuchtung weiter geleitet. Um eine höhere Verfügbarkeit zu gewährleisten, können auch zwei Elektroverteilungen eingesetzt werden

5.2.2 Funktionsweise der Infrastruktur

Bei der Elektroverteilung versorgt das Normalnetz die Gebäudeinfrastruktur inklusive Aufzügen, Beleuchtung – außer Notlichtanlagen nach VDE0108 – Kompressoren in DX-Klimaanlagen (DX= direct expansion) und Kaltwassersätzen sowie weitere Installationen. Bei einem Netzausfall kommt es zu einer Unterbrechung dieser Stromversorgung, bis ein vorhandener Generator startet und durch einen automatischen Umschalter die Versorgung wieder herstellt.

Alle Elektroverteilungen müssen mit einer Eingangssicherung versehen sein. Die Größe und Ausführung der Elektroverteilung richtet sich nach der zu verteilenden Leistung, der gewünschten Anzahl von Stromkreisen und der Leistung pro Stromkreis. Siehe dazu untenstehende Tabelle:

Idealerweise erfolgt die Absicherung innerhalb der Stromleiste selektiv, d.h. die Ausgänge werden nicht von einer Gesamtsicherung sondern von mehreren Sicherungen entweder einzeln, oder in Gruppenschaltung überwacht. Dadurch wird im Fehlerfall nicht die gesamte Stromleiste, sondern lediglich der betroffene Ausgang oder die jeweilige Gruppe vom Netz getrennt. Die Sicherungen können sowohl als Schmelzsicherung als auch als Sicherungsautomat ausgeführt werden. Der typische Aufbau in einem Schrank erfolgt normalerweise durch zwei getrennte Stromleisten die einen redundanten Betrieb der IT-Systeme ermöglichen.

Übersicht der Leistungsklassen:

Phasen	Maximale Stromstärke	Maximale Leistung
Eine	16 A	3,6 kW
Eine	32 A	7,2 kW
Drei	16 A	11 kW
Drei	32 A	22 kW

(Weitere Kombinationen mit zwei Phasen sind ebenfalls möglich, sind in Deutschland aber nicht gebräuchlich)

Moderne Geräte zur Energieverteilung (PDU) verfügen zusätzlich über Mess- oder Schaltfunktionen sowie einen Netzwerkanschluss für ein erweitertes Energiemanagement. Zusätzlich bieten diverse Modelle noch über eine Umgebungsüberwachung mit diversen Sensoren, z.B. für Temperatur- und Luftfeuchtigkeitsmessung.

Da in Rechenzentren die meisten IT-Geräte in 19“-Schränke eingebaut werden,. ergibt sich die Frage, wo die Elektroverteilung positioniert werden soll und wie die Stromkabel an die 19“-Schränke herangeführt werden. Elektroverteilungen gibt es als Wandeinbau- und Aufputzversionen, separate Schränke und als in 19“-Schrank integrierte Ausführungen. Oft werden die Kabel durch den Doppelboden geführt, der aber auch als Kaltluftführung genutzt wird. Die Luftführung kann beeinträchtigt werden und der Zugang zu den Kabeln wird erschwert. Eine Kabeleinführung von unten durch eine Doppelbodenplatte in den 19“-Schrank verhindert das. Alternativ

können Kabel in Kabeltrassen oder über Stromverteilungssysteme an der Decke oder den Wänden geführt werden, was eine Einführung von oben in den 19“-Schrank erfordert. Integrierte Elektroverteilungen bieten den Vorteil bereits nahe an der Verwendungsstelle zu stehen und so auf kurzem Wege die 19“-Schränke zu erreichen. Eine Kabelführung auf dem Dach der 19“-Schränke ist möglich, soweit eine getrennte Verlegung von Strom- und Datenkabeln vorgesehen wird.

Ein besonderes Augenmerk ist auf die Stromverteilerleisten in den Schränken zu legen. Durch die moderne kompakte Bauweise der Geräte können heutzutage viele Systeme in einen Schrank eingebaut werden. Im Extremfall kann ein Schrank mit beispielsweise 42 Höheneinheiten (HE), mit 42 Servern a‘ 1 HE und je zwei Netzteilen pro Server eingesetzt werden. Dafür müssen dann insgesamt 84 Steckdosen zur Verfügung gestellt werden.

5.2.3 Intelligente Steckdosenleisten

Beim Management auf Rackebene zählen besonders Übersichtlichkeit, Ordnung und einfache Handhabung. Idealerweise verfügen die in einem Data Center eingesetzten Steckdosenleisten über unterschiedliche laienbedienbare Einsteckmodule, beispielsweise für länderspezifische Systeme. In diesem Fall haben auch international arbeitende Organisationen die Option, in all ihren Niederlassungen dieselben Steckdosenleistentypen zu verwenden ohne für den Umbau der Systeme jeweils Fachpersonal einsetzen zu müssen. Bei aktuellen Steckdosenleisten lassen sich die Module im laufenden Betrieb austauschen. Solche High-End-Systeme verfügen in der Regel auch über HTTP- beziehungsweise SNMP-Überwachungs- und Managementoptionen sowie eine Benutzerverwaltung, die garantiert, dass nur autorisiertes Personal die Steckdosenleiste konfiguriert. Diese modularen Systeme ermöglichen eine Grundausstattung der Racks durch eine vertikale Trägerschiene mit dreiphasiger Einspeisung. In diese Schiene können die verschiedenen Einsteckmodule einfach eingerastet werden. Das reduziert den Verkabelungs- und Montageaufwand maßgeblich.

Schließlich gibt es, z.B. für Hosting-Unternehmen, die auf eine hohe Genauigkeit der Energiekostenverteilung pro Server (in einem Rack) darstellen müssen, seit kurzem amtlich geeichte Steckdosenmodule. Auch für die Elektro-Unterverteilung sind solche geeichten Messgeräte verfügbar.

5.2.4 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten

RZ Kategorie	EUV-Einspeisung Serverschrank bis zu 5 kW	EUV-Einspeisung Serverschrank ab 5 kW bis zu 30 KW	EUV-Einspeisung Rechenzentrum / Serverraum 500 bis zu 2500 Watt/qm	zulässige RZ Ausfallzeit*
A	Standard, Anbindung der Server über USV- und Normalnetz empfehlenswert			72 h
B	Standard, Anbindung der Server über USV- und Normalnetz empfehlenswert			24 h
C	Redundante Ausführung (A und B)			1 h
D	Redundante Ausführung (A und B)			10 min
E	Redundante Ausführung			0 min

Tabelle 3 aus BITKOM-Matrix „Planungshilfe betriebssicheres Rechenzentrum“ – Verteilung

Redundanzbildung hängt von der Anzahl der Netzteile in den IT-Geräten ab. Eine gute Voraussetzung für eine hohe Verfügbarkeit sind zwei Netzteile pro Gerät, die redundant ausgelegt sind. Bei Ausfall eines Netzteils ist dann das verbleibende in der Lage, das IT-Gerät normal weiter zu versorgen. Diese zwei Netzteile pro Gerät sollten über zwei getrennte Stromverteilerleisten an zwei getrennten Stromkreisen von der Elektroverteilung versorgt werden. Eine weitere Steigerung der Verfügbarkeit lässt sich durch die Verwendung zweier getrennter Elektroverteilungen erreichen, die von zwei getrennten USV- Anlagen über zwei getrennte Transformatoren und zwei getrennte Generatoren versorgt werden.

5.2.5 Schutzmaßnahmen und Hochverfügbarkeit

In Rechenzentren werden höchste Verfügbarkeitsanforderungen gestellt. Entsprechend ist die Energieversorgung nachhaltig sicherzustellen. Geradezu selbstverständlich ist die Forderung, dass die Stromversorgung des Rechenzentrums selbst und aller Bereiche im gleichen Gebäude, zu denen Datenkabel laufen, als TN-S System ausgeführt sein muss. Unbedingt nötig für den sicheren Betrieb ist eine permanente Selbstüberwachung eines „sauberen" TN-S Systems (z. B. mit RCMs) und die Aufschaltung der Meldungen an eine ständig besetzte Stelle, z. B. an die Leitzentrale. Die Elektrofachkraft erkennt dann über entsprechende Meldungen den Handlungsbedarf und kann durch gezielte Servicemaßnahmen Schäden vermeiden.

Für den Leitungsschutz müssen alle Elektroverteilungen mit einer Eingangssicherung versehen sein. Die Größe und Ausführung der Elektroverteilung richtet sich nach der zu verteilenden Leistung, der gewünschten Anzahl von Stromkreisen und der Leistung pro Stromkreis. Es werden ein- und dreiphasige Stromkreise unterschieden. Typische Versorgungsgrößen sind 16 A, einphasig (cirka 3,5 kW), 32 A einphasig (cirka 7 kW) oder für Hochleistungsschränke auch 32 A dreiphasig (22 kW). Ein besonders schwieriges Thema ist die so genannte. „Selektive Sicherungsauslegung", die es ermöglicht auch bei einem Kurz- oder Erdschluss eines IT-Gerätes in einem Schrank diesen sicher abzutrennen, ohne weitere Schränke und IT-Geräte in Mitleidenschaft zu ziehen.

Für den Personenschutz gibt es neue Anforderungen für den zusätzlichen Schutz für Endstromkreise mit Steckdosen. Seit dem 01.06.2007 gilt die DIN VDE 0100-410:2007-06 -Schutz gegen elektrischen Schlag- für neu zu errichtende Anlagen. Änderungen und Erweiterungen von bestehenden Anlagen sind nach dieser Norm auszuführen.

Diese Norm schreibt für alle Steckdosen in Wechselspannungssystemen den zusätzlichen Schutz durch Fehlerstrom-Schutzeinrichtungen (RCDs) vor, wenn die Benutzung von Laien und zur allgemeinen Verwendung bestimmt ist. Es muss sichergestellt sein, dass das sofortige Beheben von Fehlern/Schäden durch eine Elektrofachkraft, auch an den angeschlossenen elektrischen Geräten/Verbrauchsmitteln/Betriebsmitteln, gegeben ist. Dies erfordert ein permanentes Monitoringsystem und organisatorische Maßnahmen zur schnellen Fehlerbehebung.

Eine permanente Differenzstrom-Überwachung erfüllt die aktuelle Schutzmaßnahmennorm und bietet zusätzlich einen erhöhten Brandschutz, auch ohne Abschaltung durch ein RCD.

5.3 Unterbrechungsfreie Stromversorgung (USV)

5.3.1 Ausgangssituation

Die Ursachen für einen Stromausfall sind oft banal: Schon einfache Spannungsschwankungen oder Kurzausfälle im Stromnetz können reichen, um Hard- oder Software zu schädigen oder so zu stören, dass schwere Fehler in den IT-Prozessen auftreten. Unregelmäßigkeiten im Netz sind zwar selten, aber durchaus häufiger, als gemeinhin angenommen.

Um die möglichen negativen Folgen solcher kurzer Stromausfälle zu vermeiden, werden USV- Systeme eingesetzt. Sie filtern Störungen, wie Spannungsstöße oder Spannungseinbrüche und überbrücken Unterbrechungen im Netz. Dadurch werden Übertragungsfehler, Rechnerabstürze, Programmfehler und Datenverluste reduziert.

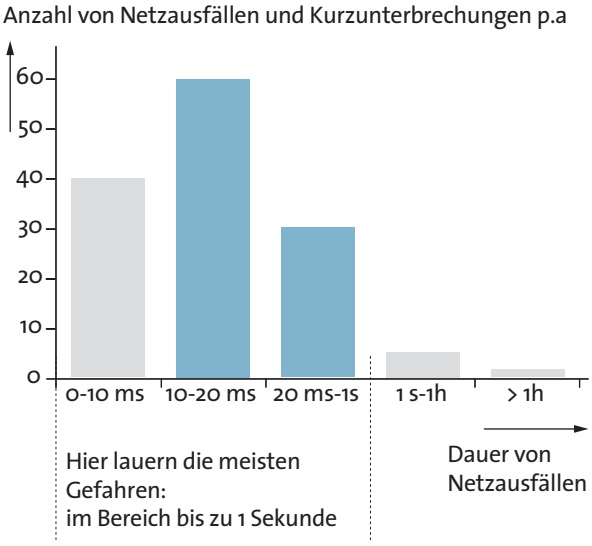


Abbildung 1: Häufigkeit von Netzstörungen bezogen auf deren durchschnittliche Dauer

Die Investitionen in die deutschen Stromversorgungssysteme haben seit den 80er Jahren um circa 40 Prozent abgenommen. Die durchschnittliche Ausfallzeit ist in den letzten Jahren von zuvor 15 Minuten auf jetzt 23 Minuten pro Jahr gestiegen. Durch den ansteigenden Einsatz regenerativer Energien erreichen die Netze zunehmend ihre Kapazitätsgrenze. Die Gefahr von Engpässen und Blackouts nimmt zu. Zu diesen Ergebnissen kommt die neue VDE-Studie zur Versorgungsqualität.

5.3.2 Technologien von USV- Systemen

USV- Systeme unterscheiden sich durch unterschiedliche Technologien. Die am häufigsten eingesetzte Technologie ist die statische USV- Anlage. Als Energiespeicher kommen wiederaufladbare (Sekundär) Zellen (Akkumulatoren) zum Einsatz. Bei einer Verschaltung aus zwei oder mehreren miteinander verbundenen Zellen spricht man von einer Sekundärbatterie oder auch nur von einer wiederaufladbaren Batterie. Bei Netzausfall wird die Energie des Speichers über einen statischen Umformer (Wechselrichter) am Ausgang der USV-Anlage für die kritischen Verbraucher bereit gestellt. Die Überbrückungszeit wird durch die Last und die Kapazität der Akkumulatoren bestimmt. Typische Überbrückungszeiten liegen im Bereich von 10 bis maximal 30 Minuten.

Die zweite Technologie ist die dynamische USV-Anlage mit und ohne Hubkolbenverbrennungsmotor. Als Energiespeicher dient je nach Bauform ein kinetischer Massenspeicher oder ebenfalls eine Akkumulatorenanlage. Die dynamische USV-Anlage stellt die Energie des Speichers über einen rotierenden Umformer (Generator) am Ausgang der USV-Anlage für die kritischen Verbraucher zur Verfügung. Bei einem kinetischen Speicher ist die Überbrückungszeit von der Last der IT-Geräte und der kinetischen Energie des Speichers (Masse und Geschwindigkeit) abhängig. Sie bewegt sich im Sekundenbereich.

Die dynamische USV-Anlage mit Verbrennungsmotor vereint eine USV- Anlage und eine Netzersatzanlage und kann somit auch Netzausfälle über einen längeren Zeitraum überbrücken.

5.3.3 Funktionsweise

Statische USV-Typen werden in 3 Kategorien aufgeteilt. In der europäischen Norm EN62040-3 werden die Klassifizierung und die zugehörigen Bestimmungsmethoden für statische USV-Systeme definiert und beschrieben.

Netzstörungen	Zeit	EN 62040-3	USV-Lösung	Ableiter-Lösung
1. Netzausfälle	> 10 ms	VFD Voltage + Frequency Dependent	Klassifizierung 3 passiver Standby-Betrieb (Offline)	.....
2. Spannungs-schwankungen	< 16 ms			.....
3. Spannungsspitzen	4 ... 16 ms			.....
4. Unterspannungen	kontinuierlich	VI *) Voltage Independent	Klassifizierung 2 Line-Interactive-Betried	.....
5. Überspannungen	kontinuierlich			.....
6. Spannungsstöße (Surge)	< 4 ms	VFI Voltage + Frequency Independent	Klassifizierung Double Conversion Betreib (Online) Deltawandler	.....
7. Blitzeinwirkungen	sporadisch			Blitz und Überspan-nungsschutz IEC 60364-5-534
8. Spannungs-verzerrung (Burst)	periodisch			.....
9. Spannungs-oberschwingungen	kontinuierlich			.....
10. Frequenzen-schwankungen	sporadisch			.....

*) Alternative Techniken sind in der Lage, die Netzstörungen Nr. 1 bis Nr. 9 zu beherrschen.

Tabelle 4: Arten von Netzstörungen und die passenden USV-Lösungen nach EN62040-3 (Ref.: „Unterbrechungsfreie Stromversorgung European Guide“; Hsgr. ZVEI 2004

Dynamische USV-Anlagen mit und ohne Verbrennungs-motoren unterliegen der DIN 6280-12.

Für den Einsatz in Rechenzentren sollten grundsätzlich statische USV- Anlagen mit der Klassifizierung „VFI“ nach EN64040-3 bzw. Diesel USV- Anlagen nach DIN 6280-12 eingesetzt werden.

Statische USV-Anlagen nach dieser Klassifizierung sind im Leistungsbereich von 10 kVA bis 1600 kVA verfügbar und können je nach Fabrikat bis zu einer Leistung von 4800 kVA parallel geschaltet werden.

Diesel USV- Anlagen sind in einer Leistung von 200 bis 1750 kVA verfügbar. Sie können den Nieder- und Mittelspannungsbereich abdecken. Sie sind vielfach parallelschaltbar.

5.3.4 USV-Redundanz

Folgende Redundanzen werden beim Einsatz von USV-Anlagen angewendet.

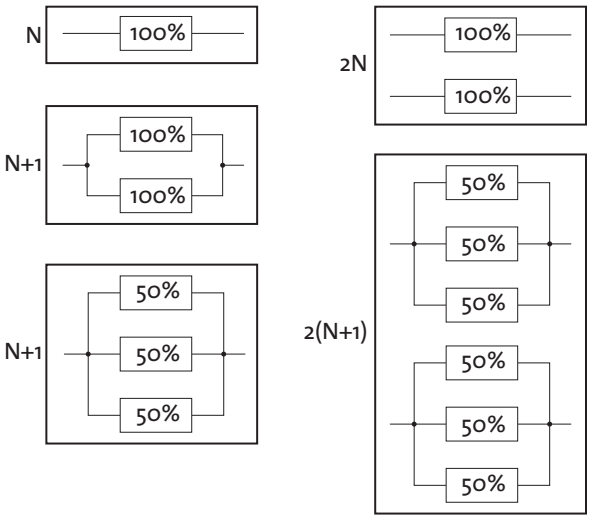


Abbildung 2: Redundanzen beim Einsatz von USV-Lösungen

5.3.5 Elektronischer Bypass / Handbypass - Serviceumgehung

Der elektronische Bypass hat die Aufgabe, die Verbraucher unterbrechungsfrei vom Netz auf den Wechselrichter der USV- Anlage (sichere Schiene) und zurück zu schalten. Bei Fehlern im Wechselrichterbetrieb oder bei großen Überlasten schaltet der elektronische Bypass die Verbraucher unterbrechungsfrei auf das Netz zurück. Der elektronische Bypass kann je nach Ausführung in der USV- Anlage integriert (Einzelblock und Modularblock) aber auch als externes Bauteil (Parallelblock mit externem elektronischem Bypass) ausgeführt werden. Zur Bildung einer Redundanz (N+1) kann auch ein weiterer elektronischer Bypass parallel geschaltet werden.

Jede USV- Anlage sollte über einen Handbypass bzw. eine Serviceumgehung verfügen. Über den Handbypass kann die USV- Anlage zu Wartungs- und Servicearbeiten spannungsfrei geschaltet werden. Ist der Handbypass in der Anlage integriert, liegt an den Eingangs- und Ausgangsklemmen der USV- Anlage auch im Bypassbetrieb Spannung an. Die Anlage kann nicht ohne Abschaltung der Verbraucher getauscht werden. Beim Einsatz eines externen Handbypasses bzw. einer Serviceumgehung kann die USV- Anlage ohne Abschaltung der Verbraucher getauscht werden. Bei einer Parallelschaltung von Modularblöcken oder Parallelblöcken ist der Handbypass bzw. die Serviceumgehung grundsätzlich auf die maximale Verbraucherlast auszulegen.

5.3.6 Energiespeicher

Kinetische Energiespeicher werden fast ausschließlich durch die Hersteller der USV-Anlagen ausgelegt bzw. dimensioniert. Die erzielbaren Überbrückungszeiten liegen im Bereich von Sekunden, so dass sich der Einsatzbereich auf Diesel USV-Anlagen bzw. in Verbindung mit schnell startenden Netzersatzanlagen beschränkt.

Zu den elektrochemischen Speichern, die in Verbindung mit USV-Anlagen eingesetzt werden, gehören Blei- und Nickelcadmiumbatterien. Der Einsatz von Lithium-Ionen-Batterien hat sich noch nicht durchgesetzt. Nickelcadmiumakkumulatoren sind relativ unempfindlich gegen erhöhte Umgebungstemperaturen, sind jedoch auf Grund der Umweltbelastung umstritten.

Der am häufigsten eingesetzte Energiespeicher in USV-Systemen ist die Bleibatterie. Bleibatterien sind stark temperaturempfindlich. Niedrige Temperaturen verringern die Batteriekapazität und somit die Überbrückungszeit bzw. die Leistung, hohe Temperaturen verringern die Lebensdauer (auch: Gebrauchsdauer). Die optimale Umgebungstemperatur beträgt 20°C.

Je nach Technologie, Materialeinsatz und weiterer Faktoren ergeben sich unterschiedliche Gebrauchsdauern von Batterieanlagen. Gemäß Eurobat bezieht sich die Gebrauchsdauer auf eine Umgebung von 20°C und Laborbedingungen. Folgende Gebrauchsdauernsind spezifiziert
3 – 5 Jahre – Standard Commercial
6 – 9 Jahre – General Purpose
10 – 12 Jahre – High Performance
12 Jahre und länger – Longlife

Um einen sicheren Betrieb der Stromversorgung zu gewährleisten, muss die Batterieanlage regelmäßig geprüft und vor dem Ende der Gebrauchsdauer ersetzt werden. Weiterhin muss beachtet werden dass die Batterie während der Nutzungsdauer an Kapazität verliert. Eine Auslegung auf sehr kurze Überbrückungszeiten birgt die Gefahr, dass die bereits gealterte Anlage die geforderte Leistung nicht mehr zur Verfügung stellen kann und die USV-Anlage abschaltet. In sicherheitsrelevanten Bereichen ist eine Überdimensionierung (Faktor 1,25) gefordert, damit am Ende der Gebrauchsdauer noch immer eine ausreichend hohe Kapazität zur Verfügung steht.

Wenn bei dem USV-System auf Redundanz verzichtet wird, sollte jedoch das Batteriesystem mindestens in zwei Strängen aufgebaut werden. Die erzielbare Überbrückungszeit eines Stranges ist nur ein Teil der geplanten Überbrückungszeit. Damit wird erreicht, dass zumindest die Netzausfälle bis zu wenigen Sekunden abgesichert sind. Für hochverfügbare Rechenzentren ist das jedoch kein geeignetes Mittel.

5.3.7 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten

Wichtigste Auslegungsfaktoren eines USV-Systems sind der elektrische Leistungsbedarf der angeschlossenen kritischen Verbraucher und die Aufstellungsgegebenheiten. Für die Überbrückung von Netzausfällen muss ein Energiespeicher wie z. B. ein Batteriesystem (Schrank oder Gestell mit Trenn- und Sicherungseinrichtungen) oder ein Schwungmassenspeicher (Flywheel) passend zur Stromversorgungsumgebung geplant werden.Darüber hinaus spielen das Redundanzkonzept und die Möglichkeiten der Ein- und Ausgangsversorgung eine wichtige Rolle.

Für den Aufbau des USV-Systems kann aus einer ganzen Reihe unterschiedlicher Konzepte gewählt werden. Kleinere, einzelne USV-Geräte setzt man gern zur Absicherung weniger Server und IT-Speichersysteme ein. Unterschieden werden kann zwischen USV-Schrank oder Towergerät mit integrierter Batterie, oder externem Batteriepack, oder als Rackvariante für den Einbau im 19“-Schrank. Größere USV-Systeme als Einzelblock- oder Parallelanlagen, zumeist mit externen Batterieschränken, Batteriegestellen oder Schwungmassenspeicheranlagen, werden meist in eigenen Betriebsräumen aufgestellt und betrieben. Hierbei bietet ein modernes wassergekühltes USV-System eine kostengünstige und effiziente, direkte USV-Klimatisierung ohne besondere Raumklimatisierung. Weitere Vorteile der USV-eigenen Betriebsräume sind Vermeidung von dicken Stromkabeln in Rechnerräumen, sowie der Einbringung von Batterien als Brandlast in den Rechnerraum. Die modularen USV-Systeme verbinden Servicefreundlichkeit und die schnelle Anpassungsmöglichkeit auf sich häufig ändernde Maximalleistunganforderungen. Allerdings sollte die Anzahl der eingesetzten Module beachtet werden, da die Verfügbarkeit mit zunehmender Komplexität der Anlage abnimmt.Beim Einsatz von USV-Systemen in Serverschränken oder als eigenes USV-Rack in gemeinsamen Räumen mit IT-Equipment muss bei den Alarm- und Brandschutzeinrichtungen die zusätzliche Brandlast durch die Akkus berücksichtigt werden.

RZ Kategorie	USV			zulässige RZ Ausfallzeit*
	Serverschrank	Serverschrank	Rechenzentrum / Serverraum	
	bis zu 5 kW	ab 5 kW bis zu 30 KW	500 bis zu 2500 Watt/qm	
A	Standard, mind. 10 Minuten Überbrückungszeit, Maximaldauer abhängigvon der kontrollierten Shutdownzeit der Server	Standard, mind. 1 Stunde Überbrückungszeit, Maximaldauer abhängigvon der kontrollierten Shutdownzeit der Server		72 h
B	Standard, mind. 10 Minuten Überbrückungszeit (inkl. Ventilation), Maximaldauer abhängigvon der kontrollierten Shutdownzeit der Server	Standard, mind. 1 Stunde Überbrückungszeit, Maximaldauer abhängigvon der kontrollierten Shutdownzeit der Server		24 h
C	Redundant (n+1), 10-20 Minuten Überbrückungszeit			1 h
D	Redundant (n+1), 10-20 Minuten Überbrückungszeit			10 min
E	Redundant (n+1), 10-20 Minuten Überbrückungszeit			0 min

Tabelle 5: aus BITKOM-Matrix „Planungshilfe betriebssicheres Rechenzentrum" – USV

Je nach Energiedichte und gewählter Überbrückungszeit kann es erforderlich sein, Lüftungsgeräte, Kühlwasserpumpen oder auch Kühlaggregate/Kompressoren über eine USV- Anlage zu versorgen. Anstelle von Kühlaggregaten/Kompressoren kann auch über einen Speicher die benötigte Energiemenge zur Kühlung während der Überbrückungszeit zur Verfügung gestellt werden. Erfolgt bei hohen Leistungsdichten keine Kühlung, kommt es zur Überhitzung und Abschaltung der IT- Geräte, ohne dass die ausgelegte Überbrückungszeit für einen eventuell geplanten Shutdown genutzt werden kann

5.3.8 Besonderheiten

Wichtige Projektierungsmerkmale für Dimensionierung und Installation eines USV-Systems sind:

- Ausgangs-Nennleistung bei gefordertem Lastleistungsfaktor (heute mind. 0,95)
- Anschlussgrößen wie Eingangs- und Ausgangs-/-Spannung, -Frequenz
- Ströme, Leiterquerschnitte und Anschlussmöglichkeiten für Ein- und Ausgänge der USV
- Wirkungsgrad und Verlustleistung für die unterschiedlichen Lastverhältnisse während typischer Betriebszyklen (z. B. Tag/Nacht, Werktag/Wochenende), Beachtung der Energieeffizienzen
- Angaben zur Absicherung der USV für die verschiedenen Betriebsmodi
- Rückwirkungen auf den Netzeingang und Eingangs-Leistungsfaktor. Allerdings müssen auch die Rückwirkungen der angeschlossenen Last bei Bypassbetrieb der USV berücksichtigt werden
- verfügbare Überbrückungszeit einer Batterieanlage, bzw. Schwungmassenspeichers, bei tatsächlicher Last
- Maximal verfügbare Überbrückungszeit einer Batterieanlage, bzw. Schwungmassenspeichers, bei Nennlast
- Angaben zum Energiespeicher und zum Lade-/Entladeverhalten
- Zulässige Umgebungsparameter wie Betriebstemperatur und Luftfeuchtigkeit; realisierter Schutzgrad; Anforderungen an Brandschutz und Klimatisierung
- Geräuschentwicklung
- Schutz zur elektromagnetischen Verträglichkeit (EMV)
- Abmessungen und Gewichte

Eine genaue Analyse der einzelnen Merkmale kann nicht Ziel des Leitfadens sein, da die Gegebenheiten bei der RZ-Stromversorgung stets eine detaillierte Planung erforderlich machen. Einige Abhängigkeiten seien hier exemplarisch erwähnt:

- die Bedeutung der angeschlossenen Batterie/Schwungmassenspeicher für die Überbrückungszeit

bei Netzausfall, wenn ein Notstromaggregat verfügbar ist.
- die Beachtung des Eingangs-Leistungsfaktors für die Dimensionierung eines Notstromaggregats. Dabei sollte der Betrieb über USV-Leistungselektronik und der Betrieb über den Bypass beachtet werden.
- der Einfluss des USV-Ausgangsleistungsfaktors auf die Möglichkeiten moderne Schaltnetzteile auch bei voller Beanspruchung zu versorgen
- die Leistungsbeschränkung bei Betrieb in großen Höhen.
- die Effizienz über einen typischen Betriebszyklus (Auslastungsschwankungen) zu berücksichtigen, um realistische Betriebskostenabschätzungen zu erhalten

Der Preis einer USV hängt ab von Ausstattungsdetails wie Filter, Transformatoren, Lüfter, elektronischem Bypass, integrierter oder externer Handumgehung, unterschiedlichen Schaltungskonzepten. Eine Preiskalkulation von Best-practise-Lösungen ist für USV-Systeme sehr komplex und erfordert eine aufwändige Analyse der Gegebenheiten, Randbedingungen, Abhängigkeiten und die Berücksichtigung einer Vielzahl von Einzelparametern.

5.4 Notstrom

5.4.1 Stromerzeugungsaggregate für die Ersatzstromversorgung (Notstrom) bei Netzausfall.

Eine störungsfreie Versorgung mit elektrischer Energie wird durch Stromlieferanten nicht jederzeit und an jedem Standort gewährleistet und in ihren, Standard-Verträgen schließen die Energieversorgungsunternehmen (EVU) jegliche Haftung aus. Kurze Unterbrechungen oder lang anhaltende Stromausfälle müssen deshalb durch Notstromanlagen überbrückt werden, um den Betrieb eines Rechenzentrums mit den dazugehörigen technischen Anlagen wie Klima, Strom und Sicherheit aufrecht zu halten.

Zulässige Ausfallzeiten haben bei der Planung von Notstromanlagen höchste Priorität. Entsprechend werden Notstromaggregate in verschiedenen Gruppen unterteilt:
- Aggregate ohne geforderte Lastübernahmezeit. Die Anlagen werden manuell in Betrieb gesetzt. Diese Anlagen sind für einen automatischen Betrieb im Rechenzentrumsbereich ungeeignet.
- Aggregate für eine zu fordernde Lastübernahmezeit. Dabei handelt es sich um eine Unterbrechung, die kleiner als 15 Sekunden sein muss, bis das Aggregat nach automatischer Inbetriebsetzung die Versorgung übernimmt. Eine DIN-Norm regelt die Anforderungen für Stromerzeugungsaggregate mit Verbrennungsmotoren für Sicherheitsstromversorgungen in Krankenhäusern und in baulichen Anlagen für Menschenansammlungen. Diese Norm sollte auch als Mindestanforderungen für Stromerzeugungsaggregate im Bereich von Rechenzentren angesehen werden.
- Aggregate mit Kurzunterbrechung als Schaltbereitschaftsaggregate. Dabei geht es um eine Unterbrechungsdauer, die kleiner als eine Sekunde sein soll. Diese Anlagen werden in Rechenzentren nicht mehr eingesetzt, da eine Unterbrechungdauer von weniger als eine Sekunde nicht erforderlich ist.
- Aggregate für unterbrechungsfreie Stromversorgung als Diesel USV-Anlagen. Hierbei erfolgt die Lastübernahme bei Netzausfall ohne Unterbrechung.

5.4.2 Notstromversorgungen

In den beiden letzten Fällen sind Sonderausführungen von Stromerzeugungsaggregaten notwendig, die als Bereitschaftsaggregat mit einem Energiespeicher versehen sind. Dieser muss fortlaufend gespeist werden. Mit den dafür entstehenden Betriebskosten bezahlt der Verbraucher seine erhöhte Versorgungssicherheit.

Für Bereitschaftsaggregate gibt es verschiedene Ausführungsversionen in der Kombination zwischen Dieselmotor, Schwungrad, elektrischer Maschine und entsprechenden Kupplungen.

Bereitschaftsaggregate werden immer dann benötigt, wenn eine Unterbrechungszeit, wie sie durch den Einsatz einfacher Ersatzstromaggregate verursacht würde, für die sichere Weiterführung des Betriebsablaufs beim Verbraucher nicht vertretbar wäre.

Am häufigsten kommen die an zweiter Stelle genannten Anlagen im Rechenzentrum zum Einsatz. Die nachfolgenden Ausführungen beziehen sich auf diese Anlagen

5.4.3 Auslegung der Notstromanlage

Für die Auslegung der Aggregateleistung sind folgende Faktoren bestimmend:

- Summe der angeschlossenen Verbraucher
- Gleichzeitigkeitsfaktor
- Einschaltströme und der Einschalt- cos phi der Verbraucher
- Netzrückwirkungen der Verbraucher (Gleichrichtertechnologie der USV-Anlagen bzw. Frequenzumformer)
- Zulässiges dynamisches Verhalten
- Reserve für Erweiterungen
- Zuschlag für abweichende Umgebungsbedingungen

Verbraucherleistung

Bei der Addition der Verbraucherleistung ist darauf zu achten, dass Scheinleistung und Wirkleistung anzugeben sind.

Gleichzeitigkeitsfaktor

Die Aggregatleistung ist bei Rechenzentren mit dem Gleichzeitigkeitsfaktor 1 auszulegen, da sommers wie winters alle Verbraucher den Betrieb des Rechenzentrums aufrechterhalten müssen.

Einschaltverhalten

Das Anlauf- und Einschaltverhalten von Elektromotoren, Transformatoren, großen Beleuchtungsanlagen mit Glühlampen beeinflussen die Aggregatleistung.
Bei Asynchronmotoren kann die Scheinleistung die bis zu 6-fache, die Wirkleistung die 2-3-fache Nennleistung erreichen. Die Möglichkeit einer zeitlich gestaffelten Zuschaltung kann die erforderliche Aggregatleistung deutlich verringern. Alle verfügbaren Maßnahmen zur Begrenzung der Anlaufleistung sollten ausgeschöpft werden.

Dynamisches Verhalten

Das dynamische Verhalten des Aggregats bei voller Lastzuschaltung und bei zu erwartenden Lastwechseln im Betrieb ist auf die zulässigen Werte der Verbraucher abzustimmen.

Die Erfüllung der geforderten Werte kann eine Überdimensionierung von Motor, Generator oder beiden erfordern.

Umgebungsbedingungen

Die Motorbezugstemperatur liegt gemäß DIN 6271 bei 27° C. Handelt es sich um höhere Betriebstemperaturen, muss der Motor größer dimensioniert werden. Die Reduktionsfaktoren der Motoren sind zu erfragen.

5.4.4 Empfohlene Notstromversorgung in Abhängigkeit zu den zulässigen Ausfallzeiten

RZ Kategorie	Notstrom Serverschrank bis zu 5 kW	Notstrom Serverschrank ab 5 kW bis zu 30 KW	Notstrom Rechenzentrum / Serverraum 500 bis zu 2500 Watt/qm	zulässige RZ Ausfallzeit*
A	optional			72 h
B	optional			24 h
C	Redundant, verfügbarkeit in 15 Sekunden, Brennstoffvorrat: 24 Stunden			1 h
D	Redundant, verfügbarkeit in 15 Sekunden, Brennstoffvorrat: 72 Stunden			10 min
E	Redundant, verfügbarkeit in 15 Sekunden, Brennstoffvorrat: 72 Stunden			0 min

Tabelle 6: aus BITKOM-Matrix „Planungshilfe betriebssicheres Rechenzentrum“ - Notstrom

Es besteht die Möglichkeit, Leihaggregate von den jeweiligen Energieversorgungsunternehmen zu beziehen, die über einen Außenanschluss bei Wartungen und Reparaturen die Notstromversorgung gewährleisten. Für unvorhergesehene Stromausfälle sind Leihaggregate keine Lösung, da nicht sicher gestellt ist, ob zum entsprechenden Zeitpunkt Leihgeräte überhaupt zur Verfügung stehen.

Raumplanung/Detailplanung für Notstromaggregate

Für die Raumplanung/ Detailplanung sind folgende Details zu berücksichtigen:

- Einzuhaltende Vorschriften (DIN VDE, VDS, WHG, TA Lärm, TA Luft, VAws, TRbF, VDN...)
- Grundsätzlicher Aggregateaufbau/Ausführung (stationäres Einbau-, Container- oder Haubenaggregat)
- Auslegung der Tankanlage (Tagestank und Vorratstank)
- Auslegung der Abgasanlage
- Motorkühlung (Vorbaukühler, Tischkühler und Einsatz von Wärmetauschern)
- Notstromsteuerung/Schaltanlagen
- Immissionsschutz

Grundsätzliche Raumanforderungen

Der Raum für die Aufstellung eines Notstromaggregates ist ein elektrotechnischer Betriebsraum. Er ist in F90 Qualität zu schützen und stellt einen eigenen Brandabschnitt dar. Zur Zuführung der Kühl- und Verbrennungsluft sowie zur Abführung der erwärmten Kühlluft sind entsprechende Lüftungsöffnungen vorzusehen. Diese Öffnungen müssen direkt nach außen führen. Auf Grund der erforderlichen Lüftungsquerschnitte sind Räume ohne Außenwände ungeeignet. Gegebenenfalls müssen Lüftungskanäle in F90 Qualität geschaffen werden die direkt nach außen führen. Zur Vermeidung von Luftkurzschlüssen dürfen Zu- und Abluftöffnung nicht unmittelbar nebeneinander angeordnet werden. Der Aggregateraum muss gegen Hochwasser und zum Umweltschutz als Auffangwanne ausgebildet sein mit einer umlaufenden Schwelle von 10 cm mit 3-fach ölfestem Anstrich. Diese Wanne muss auf Leckage überwacht werden. Die Raumgröße muss einen Fluchtweg von 1m Breite zulassen, die Raumtüren sind mindestens in T30 Qualität mit einem Panikschloss auszuführen.

Einzuhaltende Vorschriften

Die aufgeführten Vorschriften und Gesetze dienen einerseits zur Sicherstellung der ordnungsgemäßen Funktion der Anlage sowie der Betriebssicherheit und dem Umweltschutz. Von den genehmigenden Behörden können auch noch weitere Auflagen und Forderungen erhoben werden. Grundsätzlich sollte der Dialog mit den Behörden schon frühzeitig während der Planungsphase gesucht werden.

Eine besondere Bedeutung hat der Lärmschutz. Nachstehend aufgeführt sind Daueremissionsrichtwerte für Emmissionsorte außerhalb von Gebäuden.

Industriegebiet	70 dB(A)	
Gewerbegebiet	tags 65 dB(A)	nachts 50 dB(A)
Kern-, Dorf- und Mischgebiete	tags 60 dB(A)	nachts 45 dB(A)
Wohn- und Kleinsiedlungsgebiete	tags 55 dB(A)	nachts 40 dB(A)
Reine Wohngebiete	tags 50 dB(A)	nachts 35 dB(A)
Kurgebiete für Krankenhäuser / Pflegeanstalten	tags 45 dB(A)	nachts 35 dB(A)

Beurteilt wird der Restschallpegel in einer entsprechenden Entfernung, nicht am Emmisionsort.

Grundsätzlicher Aggregateaufbau/Ausführung

Bei Aggregateaufbau /Ausführung gibt es drei Möglichkeiten. Bei einem Einbauaggregat wird die komplette Anlage im Gebäude installiert. Schnittstellen nach Außen stellen die Zu- und Abluftöffnungen, die Abgasanlage und eventuell ein außen liegender Tischkühler dar. In dieser Ausführung sind Leistungen im Bereich von weinigen kVA bis weit in den MVA Bereich möglich. Ein Containeraggregat kommt häufig zum Einsatz, wenn im Gebäude nur ungenügende Platzverhältnisse vorhanden sind oder andere Umstände gegen den Einsatz im Gebäude sprechen. Wie bei einem stationären Einbauaggregat sind Leistungen im Bereich von weinigen kVA bis weit in den MVA Bereich möglich. Als dritte Aufführung gibt es Haubenaggregate. Ihr Einsatz erfolgt meistens bei Leistungen von wenigen kVA bis zu einigen hundert kVA. Vorteil liegt in der Platz sparenden Ausführung. Ein Nachteil ist die nicht ganz einfache Zugänglichkeit aller Anlagenteile im Wartungs- oder Störungsfall. Die folgenden Abbildungen zeigen Netzersatzanlagen im Gebäude und im Container.

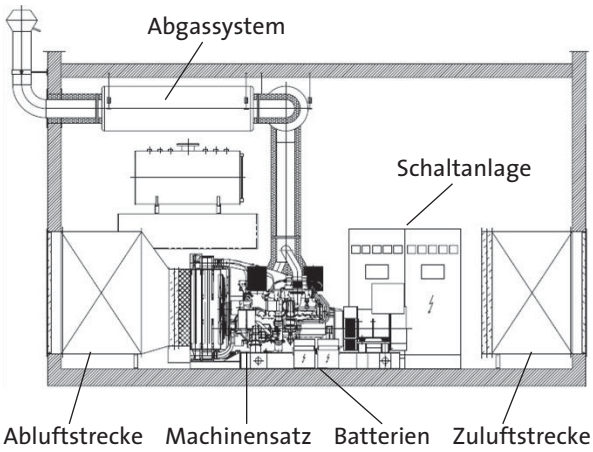


Abbildung 3: Netzersatzanlage im Gebäude

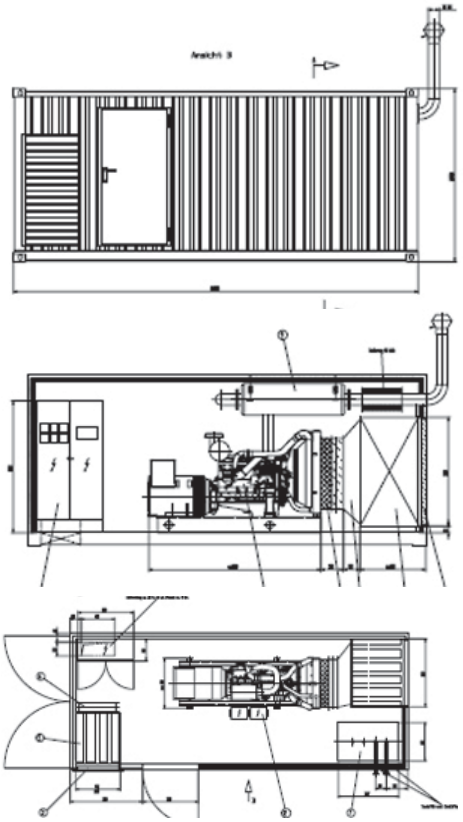


Abbildung 4: Netzersatzanlage im Container

Auslegung Tankanlage

Grundvoraussetzung für die Bestimmung der Tankgröße ist die erforderliche Betriebszeit sowie die Leistung der Anlage. Eine Kraftstoffmenge unter 5000 Liter kann im Aggregateraum gelagert werden. Werden mehr als 5000 Liter benötigt ist ein separater Lagerraum in F90 Qualität bzw. ein Tank für die oberirdische Lagerung außerhalb des Gebäudes oder ein Erdtank vorzusehen. Der Tagestank wird als einwandiger Tank mit Auffangwanne ausgeführt. Er ist so zu montieren dass ein statischer Druck am Einspritzsystem des Motors anliegt. Der Lagertank ist als doppelwandiger Tank auszuführen bzw. ist der Lagerraum als Auffangwanne für den gesamten Inhalt auszubilden. Sind zwischen dem Tagestank und dem Vorratstank Kraftstoffleitungen vorgesehen, die nicht auf der kompletten Länge eingesehen werden können, so sind diese doppelwandig auszuführen. Die doppelwandigen Leitungen, die Auffangwannen sowie Hülle bei doppelwandigen Tanks sind auf Leckage zu überwachen. Eine Tankanlage ist folgendermaßen aufgebaut:

Auslegung Abgasanlage

Die Nennweite der Abgasanlage richtet sich nach der Nennleistung des Notstromaggregates, der geplanten Rohrleitungslänge, der Anzahl und Art der Richtungsänderungen sowie der geforderten Schalldämpfung. Abgasanlagen von Notstromaggregaten sind Drucksysteme und erreichen Temperaturen von bis zu 500°C. Sie sind so zu dämmen, dass jegliche Gefahr für Personen und Sachwerte ausgeschlossen ist. Eine Abgasanlage ist folgendermaßen aufgebaut:

Auslegung Motorkühlung

Bis zu einem Leistungsbereich von ca. 1150 kVA ist eine Motorkühlung mittels Vorbaukühler möglich. Das bedeutet dass die komplette Kühlluft durch den Aggregateraum geführt werden muss. Ab einer Leistung von ca. 800 kVA besteht die Möglichkeit, einen Teil der Motorwärme über einen Tischkühler abzuführen. In diesem Fall verringert sich die Kühlluftmenge, die durch den Aggregateraum geführt werden muss. Ist der Höhenunterschied zwischen Dieselmotor und Tischkühler größer 10 m, ist der Einsatz eines Wärmetauschers zur Verringerung des Druckes auf den Kühlkreislauf des Motors erforderlich. Der Aufbau von Motorkühlung und externen Kühlsysteme in Abhängigkeit vom Höhenunterschied zwischen Dieselmotor und Kühlkreislauf kann folgendermaßen dargestellt werden:

Auslegung Notstromsteuerung/Schaltanlagen

Jedes Aggregat verfügt mindestes über eine Notstromsteuerung. Die Notstromsteuerung übernimmt folgende Aufgaben.

- Überwachung des Versorgungsnetzes unter Berücksichtigung der zulässigen Toleranzen
- Kommunikation mit dem Motormanagement/ Motorregler
- Start und Stillsetzung des Dieselmotors
- Überwachung des Generatornetzes unter Berücksichtigung der zulässigen Toleranzen

- Überwachung der Motorparameter und Regelung der erforderlichen Parameter
- Verwaltung und Steuerung der erforderlichen Hilfsantriebe (Motorjalousien, Zu- und Abluftventilatoren, Kraftstoffpumpen, Magnetventile, Leckagesonden, Rohrbegleitheizungen, Kühlwasservorwärmung, Starterbatterieladung, Steuerbatterieladung usw.
- Verwaltung der erforderlichen Netz- und Generatorkuppelschalter für den automatischen Betrieb
- Ladung und Überwachung der Batterie

Beim Leistungsteil gibt es folgende Möglichkeiten:

- Der Netz- und Generatorschalter befinden sich in der Notstromsteuerung
- Der Netzschalter befindet sich in der Niederspannungshauptverteilung, der Generatorschalter in der Notstromsteuerung.
- Der Netz- und der Generatorschalter befindet sich in der Niederspannungshauptverteilung, die Überwachung des Generatornetzes erfolgt über externe Spannungsabgriffe, der Generatorschutz wird über Sternpunktwandler realisiert.

Ein beispielhaftes Versorgungsschema sieht wie folgt aus:.

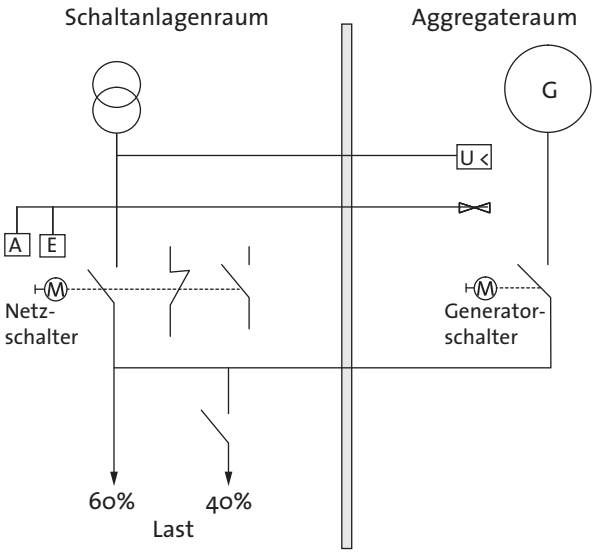


Abbildung 5: Netzüberwachung / Netzumschaltung

5.5 Wartung/Instandhaltung

5.5.1 Wartung/Service USV-Anlagen

Grundvoraussetzung für die Aufrechterhaltung der ordnungsgemäßen Funktion ist die jährliche Wartung gemäß den Vorgaben des Herstellers durch dafür vom Hersteller autorisiertes Fachpersonal. Verschleißteile müssen gemäß Herstellerangaben vor Ablauf Ihrer Gebrauchsdauer erneuert werden.

Auf Grund der häufig eingesetzten, wartungsfrei verschlossenen Bleibatterien wird auf deren Wartung ein nicht so großes Augenmerk gelegt. Die Bezeichnung „wartungsfrei“ bezieht sich jedoch auf das innere der Batterie. Dass bedeutet, dass kein destilliertes Wasser aufgefüllt werden muss. Jedoch müssen sämtliche Verbindungen und die Polschrauben auf das entsprechende Drehmoment geprüft werden. Die Spannungen der einzelnen Batterien sind in Ladeerhaltung und in der Entladephase aufzunehmen und zu protokollieren. Nur anhand dieser Daten kann der Zustand der Batterie beurteilt/bewertet werden. Ebenso wichtig ist die regelmäßige Reinigung der Batterieanlage, um Kriechströme bzw. Kurzschlüsse zu vermeiden.

Ein nicht zu vernachlässigender Sicherheitsaspekt im Störungsfall ist die personelle und zeitliche Verfügbarkeit von entsprechendem Fachpersonal zur Beseitigung von Störungen.

5.5.2 Wartung/Service/Probeläufe Netzersatzanlage

Grundvoraussetzung für die Aufrechterhaltung der ordnungsgemäßen Funktion einer Netzersatzanlage ist die jährliche Wartung gemäß den Vorgaben des Herstellers durch dafür vom Hersteller autorisiertes Fachpersonal sowie die monatlichen Probeläufe. Diese monatlichen Probeläufe müssen zur Sicherstellung der ordnungsgemäßen Funktion mit 50% der Nennlast mindestes eine Stunde dauern und können bei entsprechender Einweisung auch durch den Betreiber selbst durchgeführt

werden. Die Betriebstemperatur der Anlage muss dabei erreicht werden. Als Last kann, wenn vorhanden, ein fest installierter Widerstand dienen, die im Notstromfall zur versorgenden Verbraucher oder das vorhandene Netz mittels Netzparallelbetrieb dienen. Letzteres bedarf allerdings der Zustimmung und Abnahme seitens des Energieversorgungsunternehmens.

Wie auch bei der USV-Anlage sollte die personelle und zeitliche Verfügbarkeit von entsprechendem Fachpersonal zur Beseitigung von Störungen berücksichtigt werden.

5.5.3 Wartung / Prüfung Elektroinstallation

Entsprechend den gültigen Vorschriften (VDE 0105) sowie der Vorschriften der Berufsgenossenschaft müssen elektrische Anlagen in regelmäßigen Abständen geprüft und gewartet werden. Dafür sind die Anlagen spannungsfrei zu schalten und entsprechende wiederkehrende Messungen und Prüfungen durchzuführen. Ggf. sollte eine A/B-Versorgung bereits bei der Planung der Infrastruktur in Erwägung gezogen werden. Somit besteht die Möglichkeit der entsprechenden Freischaltung und Prüfung.

5.6 Klimatisierung

5.6.1 Ausgangssituation

Jedes Kilowatt (kW) elektrische Leistung, das von ITK-Geräten aufgenommen wird, wird als Wärme wieder freigesetzt. Diese Wärme muss aus dem Gerät, dem Schrank und dem Raum geführt werden, um die Betriebstemperaturen konstant zu halten. Zur Ableitung der Wärme werden Klimaanlagen unterschiedlicher Funktionsweise und Leistungsfähigkeit eingesetzt.

5.6.2 Klimatisierung als Herausforderung

Die Klimatisierung von ITK-Systemen ist entscheidend für deren Verfügbarkeit und Sicherheit. Die steigende Integration und Packungsdichte bei Prozessoren und Computer/Server-Systemen verursacht Abwärmemengen, die noch vor wenigen Jahren auf so begrenztem Raum unvorstellbar waren.

Auf dem Markt sind unterschiedliche Klimatisierungslösungen je nach Leistung und Verlustleistung – also Abwärme - der eingesetzten ITK-Komponenten erhältlich. Mit mehr als 130 W/cm∞ je CPU – pro Quadratzentimeter entspricht das zwei Standard-Glühlampen – gewinnt die Aufgabe, Rechen- zentrumsklimatisierung Konturen: Aus dieser Leistungsdichte resultieren heute Wärmelasten von weit mehr als 1kW pro Quadratmeter.

Bei der Klimatisierung von Rechenzentren zeigen sich weitere Herausforderungen. Nach Messungen und Erfahrungen aus der Praxis lassen sich bis zu 8 kW Verlustleistung in einem Rack oder Gehäuse noch mit der klassischen, über den Doppelboden realisierten Klimatisierung per Kühlluftbeherrschen, wie sie in vielen Rechenzentren nach wie vor existiert. Der im klassischen Mainframe-Rechenzentrum eingeführte Doppelboden zeigt sich in seiner Luftführung den heutigen, teils extrem hohen Anforderungen zum Teil allerdings nicht mehr gewachsen.

Nachdem über Jahrzehnte eine Kälteleistung von 1 bis 3 kW pro 19“-Schrank ausreichend war, muss die Kälteleistung heute pro Rack stark erhöht werden können. Moderne IT-Geräte können in einem 19“-Schrank mit 42 Höheneinheiten über 30 kW elektrische Leistung aufnehmen und über 30 kW Wärme abgeben. Ein weiterer Anstieg ist durch die weiter steigende Leistungsfähigkeit bei sinkender Baugröße absehbar.

Damit bestehende Klimatisierungslösungen mit Doppelboden in Ihrer Leistungsfähigkeit verbessert werden können, werden die ITK Komponenten heute mit einer Abschottung versehen un nach dem sogenannten Kaltgang/Warmgang Prinzip angeordnet. Zum Teil werden die Kalt- oder Warmgänge eingehaust, um höhere Wärmeabgaben pro Rack zu ermöglichen.

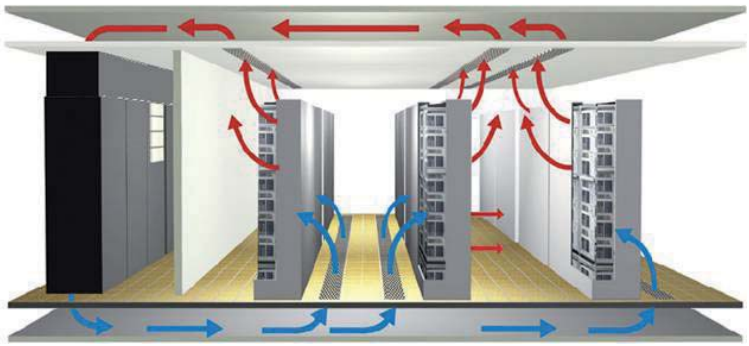


Abbildung 6:. Prinzipielle Darstellung einer Kaltgang-Warmgang Lösung

Als Entscheidungskriterien für eine Klimalösung gelten unter anderem die zu erwartende maximale Verlustleistung, Betriebskosten, Anschaffungskosten, Aufstellbedingungen, Erweiterungskosten, Zukunftssicherheit, Kosten für Ausfallzeiten sowie die physikalische Sicherheit..

5.6.3 Funktionsweise der Umluftklimatisierung

Die Raumkonditionen für die Rechenzentrumsklimatisierung lagen in der Vergangenheit bei ca. 22°C Raumtemperatur und etwa 50% relative Feuchte (r.F.) - aufgrund des Kaltgang/Warmgang Prinzips wird heute von Zuluft- und Abluftbedingungen gesprochen, da die Raumbedingungen im eigentlichen Sinne nicht mehr im gesamten zu klimatisierenden Raum angetroffen werden.

Die Zuluftbedingungen im Kaltgang sollten je nach Anwendung zwischen 20 und bis zu 27°C – die relative Zuluftfeuchte sollte dabei zwischen 40 bis 60% r.F liegen. Eine geringere Luftfeuchtigkeit führt zu elektrostatischer Aufladung, eine hohe Luftfeuchtigkeit zu Korrosion an den elektrischen und elektronischen Komponenten. Betriebsbedingungen mit sehr kalten Temperaturen unter 18°C und hoher Luftfeuchtigkeit, die zur Bildung von Kondenswasser an IT-Geräten führen, sind grundsätzlich zu vermeiden.

Die Klimatisierungssysteme in ITK-Räumen werden mit einem sehr hohen Umluftanteil betrieben. Bei dem Prinzip der Umluftklimatisierung zirkuliert die vom Klimasystem abgekühlte Zuluft zu den ITK-Komponenten, nimmt die Wärme auf und die erwärmte Luft gelangt als Rückluft zur erneuten Abkühlung wieder zum Klimasystem. Lediglich ein kleiner Anteil Außenluft wird in den zu klimatisierenden Raum eingebracht, dieser dient zum Luftaustausch.

Die optimalen Bedingungen im Hinblick auf Temperatur und relative Luftfeuchte lassen sich nur mit Umluftklimageräten, sogenannten Präzisionsklimageräten, erreichen. In diesen Systemen wird die eingesetzte Energie besser genutzt, d.h. in erster Linie wird die Temperatur der Rückluft abgesenkt. Im Gegensatz dazu stehen Komfortklimageräte für Wohn- und Büroräume, wie z.B. Splitklimageräte, die einen großen Teil der eingesetzten Energie permanent für die Entfeuchtung der Umluft einsetzen. Dadurch kommt es zu kritischen Raumbedingungen, aber auch zu erheblich höheren Betriebskosten, daher ist der Einsatz in Rechenzentren nicht wirtschaftlich.

5.6.4 Aufbau der Umluftklimasysteme

Umluftklimasysteme unterscheiden sich hinsichtlich Ihres Aufbaus erheblich. Die Systeme können ganz grob in DX Systeme (Direkt Expansion Systeme) und CW Systeme (Chilled Water Systeme) eingeteilt werden. Beide Systeme können zusätzlich mit einer indirekten freien Kühlung ausgerüstet sein.

DX Systeme

Die Kälteerzeugung ist im Umluftklimaschrank integriert und somit im oder in der Nähe des ITK-Raums angeordnet. Die Umluft wird durch expandierendes Kältemittel direkt abgekühlt und die aufgenommene Wärme wird an der Außeneinheit, dem luftgekühlten Kondensator, wieder abgegeben.

Beim Einsatz der indirekten freien Kühlung kommt im Umluftklimaschrank ein zusätzlicher Wärmetauscher für die freie Kühlung zum Einsatz. Bei niedrigen

Außentemperaturen zirkuliert zwischen dem Umluftklimagerät und der Außeneinheit, dem Rückkühler, lediglich ein Wasser/Glykolgemisch. Dieses Gemisch wird durch die Umluft erwärmt und im Außenbereich, am Rückkühler, wieder abgekühlt. Zwischen dem Umluftkreislauf im ITK-Raum und der Außenluft ist das Wasser/Glykolgemisch zwischengeschaltet, daher wird dieses System indirekte freie Kühlung genannt. Bei hohen Außentemperaturen schaltet das System auf den DX Modus um und die Wärme der Umluft wird zunächst im Klimaschrank auf einen wassergekühlten Kondensator übertragen, bevor die Wärme am Rückkühler an die Außenluft übergeben wird.

DX-Systeme mit oder ohne indirekte freie Kühlung finden für kleinere und mittlere Installationen bis ca. 500kW Wärmelast Anwendung.

CW Systeme

Die Kälteerzeugung ist in den Kaltwassererzeugern integriert, die i.d.R. im Außenbereich installiert sind. Im Gebäude zirkuliert ein Wasser/Glykolgemisch. Im kaltwassergekühlten Umluftschrank wird die Wärme aus der Rückluft an das kalte Wasser/Glykolgemisch übergeben. Das erwärmte Wasser/Glykolgemisch wird im Kaltwassererzeuger wieder abgekühlt und gelangt wieder zum Umluftklimaschrank.

Auch bei diesem System lässt sich eine indirekte freie Kühlung realisieren. Dazu wird im Außenbereich ein zusätzliches Freikühlregister am Kaltwassererzeuger verbaut. Bei niedrigen Außentemperaturen zirkuliert das Wasser/Glykolgemisch zwischen den kaltwassergekühlten Klimageräten und dem Freikühlungsregister. Dabei wird die Wärme der Umluft im Klimagerät aufgenommen und am Freikühlungsregister im Außenbereich wieder abgegeben. Bei hohen Außentemperaturen wird das Wasser/Glykolgemisch über die Kälteerzeugung im Kaltwassererzeuger abgekühlt.

CW-Systeme mit oder ohne indirekte freie Kühlung finden für größere Installationen ab ca. 500kW Wärmelast Anwendung.

5.6.5 Rackanordnung und Umluftführung

Mitentscheidend für die Leistungsfähigkeit von Umluftklimasystemen sind die Rackanordnung und die Luftführung.

So werden heute insbesondere 19" Racks im sogenannten Warmgang/Kaltgangprinzip angeordnet, um die geforderte horizontale Luftdurchströmung der ITK Komponenten bestmöglich nachbilden zu können. In dieser Anordnung ist der Luftstrom gewissermaßen gezwungen auf dem Weg vom Doppelboden zurück zum Klimagerät die Wärme aus den ITK Komponenten aufzunehmen.

Die Leistungsfähigkeit wird durch die Einhausung des Kaltganges oder Warmganges noch weiter getrieben. Von entscheidender Wichtigkeit ist ebenfalls die Höhe des eingesetzten Doppelbodens, über den die Rechenzentrumsfläche mit kalter Zuluft versorgt werden kann. Die Zuluft tritt gezielt über Schlitzplatten oder Gitter im Kaltgang aus. Die Rückluft gelangt nach der Erwärmung durch das ITK Equipment wieder zur erneuten Abkühlung in das Klimasystem.

5.6.6 Direkte Kühlung der Racks

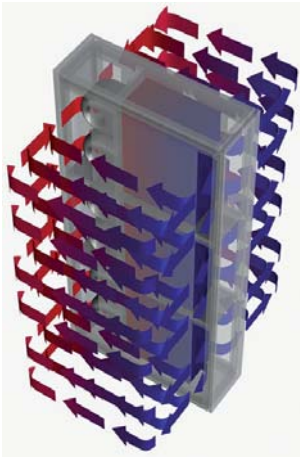


Abbildung 7: Prinzipielle Darstellung wassergekühltes Serverrack

Bei Wärmelasten von mehr als 10 - 15kW pro Rack muss eine direkte Kühlung der Racks vorgenommen werden. Die direkte Kühlung von Racks wird durch in unmittelbarer Nähe der Server angebrachte Wärmetauscher realisiert. In der Regel handelt es sich um kaltwassergekühlte Wärmetauscher, die entweder unter oder neben den 19“ Einbauten angeordnet sind. Auf diesem Weg lassen sich bis zu 40kW pro Rack abführen.

Im Bereich der Racks ist dafür eine Kaltwasser-Infrastruktur vorzusehen. Wassergekühlte Racks sichern für den jeweiligen Serverschrank klimatische Bedingungen und sind somit autark in Bezug auf die Raumklimatisierung.

In Bestandsgebäuden mit niedriger Geschoßhöhe stellen wassergekühlte Serverracks eine gute Möglichkeit da, auch ohne den Einsatz eines Doppelbodens hohe Wärmelasten sicher abzuführen.

5.6.7 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten

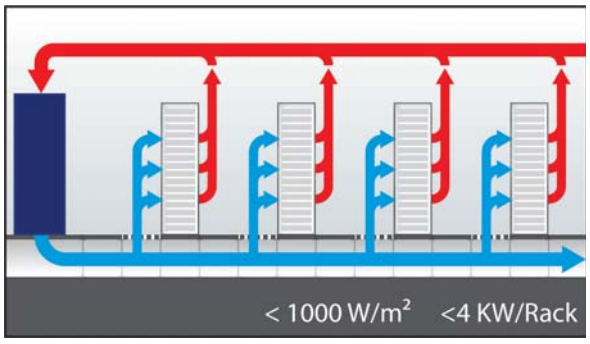
RZ Kategorie	Klimatisierung			zulässige RZ Ausfallzeit*
	Serverschrank	Serverschrank	Rechenzentrum / Serverraum	
	bis zu 5 kW	ab 5 kW bis zu 30 KW	500 bis zu 2500 Watt/qm	
A	Präzisionskühlung	Hochleistungskühlung bzw. Flüssigkeitskühlung Komplette Kalt-/Warmtrennung	Präzisionskühlung	72 h
B	Präzisionskühlung	Hochleistungskühlung bzw. Flüssigkeitskühlung, Rufbereitschaft Fachkraft, bei Schränken mit hoher Leistungsdichte ist eine Redundanz notwendig, USV-Unterstüzung für Ventilation, Komplette Kalt-/Warmtrennung	Präzisionskühlung, Rufbereitschaft Fachkraft	24 h
C	Präzisionskühlung mit redundanter Auslegung	Hochleistungskühlung bzw. Flüssigkeitskühlung, Redundante Auslegung, USV-Unterstüzung für Ventilation, Komplette Kalt-/Warmtrennung	Präzisionskühlung mit redundanter Auslegung	1 h
D	Präzisionskühlung mit redundanter Auslegung, USV-Unterstüzung	Hochleistungskühlung bzw. Flüssigkeitskühlung, Redundante Auslegung, USV-Unterstüzung für Ventilation, Komplette Kalt-/Warmtrennung	Präzisionskühlung mit redundanter Auslegung, USV-Unterstüzung für Ventilation	10 min
E	Präzisionskühlung mit redundanter Auslegung USV-Unterstüzung	Hochleistungskühlung bzw. Flüssigkeitskühlung, Redundante Auslegung, USV-Unterstüzung für Ventilation, Komplette Kalt-/Warmtrennung	Präzisionskühlung mit redundanter Auslegung USV-Unterstüzung für Ventilation Notkühlfunktionen über ein zusätzliches Klimasystem (z.B: Brunnenwasser, Stadtwasser, lüftungsanlage)	0 min

Tabelle 8: aus BITKOM-Matrix „Planungshilfe betriebssicheres Rechenzentrum“ - Klimatisierung

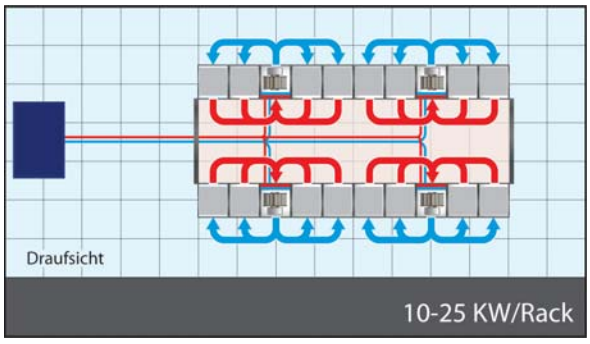
Die bei höheren Leistungen erforderliche Hochleistungskühlung schließt auch eine Kaltgangs- oder Warmgangseinhausung ein.

Mit zunehmender Kühlleistung müssen die Klimatisierungslösungen angepasst werden. Die folgende Abbildung zeigt die Leistungsdichten, die mit verschiedenen Klimatisierungslösungen zurzeit gehandhabt werden können.

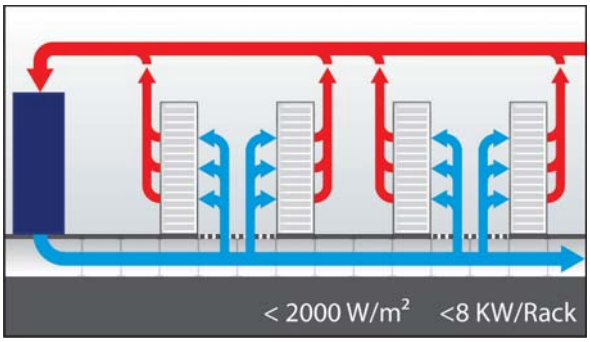
Klimatisierung über den Doppelboden ohne Ordnung der Racks aus lüftungstechnischer Sicht



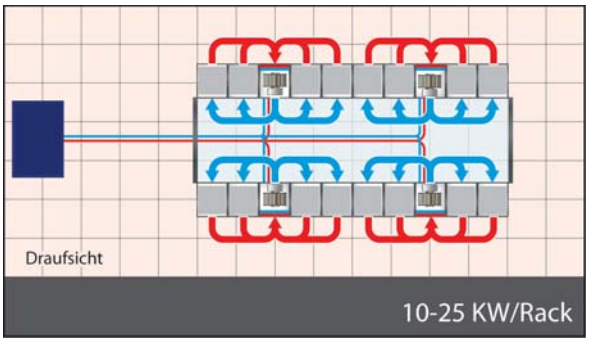
Klimatisierung wassergekühlt Einhausung der Wärmegänge



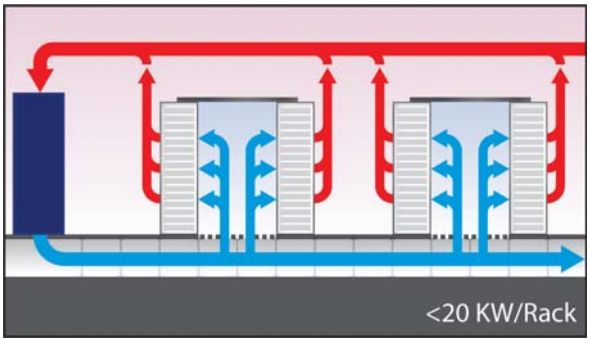
Klimatisierung über den Doppelboden und Ordnung der Racks in kalte/wärme Gänge



Klimatisierung wassergekühlt Einhausung der Kaltgänge



Klimatisierung über den Doppelboden und Einhausung der Kaltgänge



Klimatisierung mit wassergekühlten Rack (geschlossenes System)

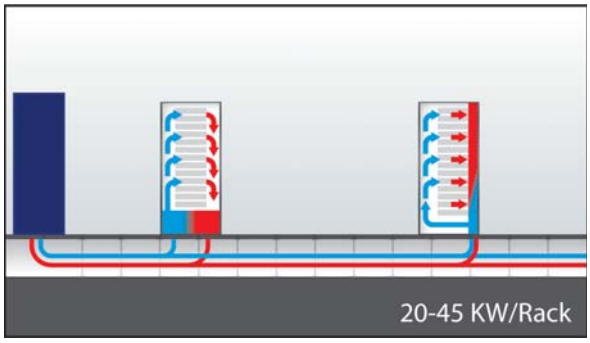


Abbildung 8: Klimatisierungslösungen für verschiedene Kühllasten

5.6.8 Weitere Empfehlungen

Energieeffizienz

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. Ein System mit freier Kühlung wird i.d.R. zu höheren Investitionskosten führen, aber die Mehrkosten werden sich aufgrund der deutlich reduzierten Betriebs- und Wartungskosten in einem kurz- bis mittelfristigen Zeitraum amortisieren.

Skalierbarkeit

In vielen Rechenzentren wird der maximale Endausbau der ITSysteme erst nach einigen Jahren erreicht, daher muss das Klimatisierungssystem entsprechend skalierbar sein. Ein in Teillast betriebenes Kaltwassersystem wird dadurch unter Umständen über Jahre hinweg mit einem schlechten Wirkungsgrad betrieben und kann erst im Endausbau die projektierte Effizienz liefern. Hier sind mitwachsende Lösungen, also modulare Systeme immer im Vorteil.

Redundanz

Aufgrund der zahlreichen mechanischen Komponenten in Klimatisierungssystemen ist stets mit einer Ausfallwahrscheinlichkeit zu rechnen. Redundant angeordnete Klimageräte übernehmen bei Ausfällen die Erzeugung der Kälteleistung und stellen eine nahezu hundertprozentige Betriebssicherheit da. Während des Ausfalls ist die Redundanz im Klimasystem in der Regel nicht mehr vorhanden und korrektive Maßnahmen müssen umgehend eingeleitet werden – anderenfalls besteht das Risiko bei einem weiteren Ausfall die Klimatisierung des Raumes nicht aufrecht erhalten zu können.

5.6.9 Servicekonzept

In den Klimatisierungssystemen werden zum einen Verschleißteile, wie z.B. Filtermatten, Dampfzylinder eingesetzt aber auch viele mechanisch bewegte Komponenten eingesetzt. Daher sind in regelmäßigen Abständen präventive Wartungszyklen vorzusehen. Die Leistungen werden unter anderem in der DIN31051 und der VDMA 24186 beschrieben.

Abhängig vom individuellen Verfügbarkeitsanspruch an die Klimatisierung, gibt es abgestimmte Service-vertragsformen. Die Verträge unterscheiden sich hinsichtlich des Leistungsumfanges:

- Instandsetzungsvertrag
  Tritt nach einem Ausfall oder einem Fehler ein und stellt die Betriebsfähigkeit der Anlage durch nachgelagerte korrektive Serviceleistungen wieder her
- Wartungsvertrag
  Regelmäßige Leistung, die die Verfügbarkeit der Anlage durch präventive Serviceleistungen sicherstellt.
- Instandhaltungsvertrag
  Kombination aus Instandsetzung und Wartung, dieser vereint präventive und korrektive Serviceleistungen
- Vollunterhaltungsvertrag
  vereint Instandhaltung und bietet eine Budgetsicherheit durch gleichbleibende Kosten während der Vertragslaufzeit

Diese Verträge lassen sich zum Teil auch mit einem 24/7 Notdienst kombinieren und sichern vor Ort Antrittzeiten vertraglich zu. Auf diesem Wege kann sichergestellt werden, dass korrektive Maßnahmen umgehend eingeleitet werden und die Verfügbarkeit der Anlage schnellstmöglich wieder hergestellt wird.

6 Brandschutz

„Es entspricht der Lebenserfahrung, dass mit der Entstehung eines Brandes praktisch jederzeit gerechnet werden muss. Der Umstand, dass in vielen Gebäuden jahrzehntelang kein Brand ausbricht, beweist nicht, dass keine Gefahr besteht, sondern stellt für die Betroffenen einen Glücksfall dar, mit dessen Ende jederzeit gerechnet werden muss." Dieser Feststellung eines Oberverwaltungsgerichts bereits aus dem Jahre 1987 ist auch heute noch nichts hinzuzufügen. Daher ist ein zuverlässiges und schnelles Branderkennungs- und Löschsystem oder auch ein Brandvermeidungssystem eine unabdingbare Voraussetzung für den sicheren Betrieb des Rechenzentrums.

Das Löschmittel Wasser ist im Rechenzentrum fehl am Platz. Die Fachfirmen der Branche bieten heute für jeden Bedarfsfall geeignete Löschanlagen an. Bei Neubau oder nachträglicher Absicherung von Rechenzentren ist aber eine genaue Planung und Auslegung der Anlagen wichtig.

6.1 Technischer Brandschutz

Feuer, Rauch, aggressive Rauchgase oder Löschwasser stellen für Rechenzentren eine latente Gefahr dar. Für die Sicherheit ist eine technisch hochwertige Brandfrühesterkennung in Verbindung mit sehr hochwertiger Löschtechnik notwendig. Eine Alternative stellt die Brandvermeidung über die Absenkung des Sauerstoffanteils der Luft dar. Durch Einleiten von Stickstoff wird die Sauerstoffkonzentration exakt auf einen zuvor eingestellten Wert vermindert. Trotzdem bleiben die so geschützten Räume für gesunde Personen begehbar.

Nicht einsetzbar ist dagegen Löschschaum, der IT-Systeme oder deren Netzteile beschädigen würde. Auch Pulverlöschsysteme sind für ein Rechenzentrum mit seinen empfindlichen Geräten ungeeignet, da die Löschung unter Umständen mehr Schaden als der eigentliche Brand verursachen kann. Daher kommen heute fast ausschließlich Gas-Löschmittel zum Einsatz.

6.1.1 Funktionsweise der Infrastruktur

Brandmelder

Für die Branderkennung in IT-Bereichen werden hauptsächlich Rauchmelder eingesetzt, die nach dem Streulichtprinzip arbeiten. Die Streuung eines Lichtstrahls an vorhandenen Rauchpartikeln stellt dabei das Maß für die Rauchdichte dar. Dieses Funktionsprinzip findet sowohl in konventionellen, punktförmigen Rauchmeldern (O-Melder, Punktmelder) wie auch in hochsensiblen Rauchansaugsystemen (Ansaugrauchmelder, Aktivmelder) Einsatz. Der in früheren Jahren eingesetzte, radioaktiv strahlende Ionisationsmelder (I-Melder) ist hingegen fast gänzlich vom europäischen Markt verschwunden.

Welcher Brandmelder am besten geeignet ist, hängt von den Anforderungen des jeweiligen Einsatzbereiches ab. In Bereichen ohne besondere Detektionsanforderungen werden im Allgemeinen Punktmelder eingesetzt. In Rechenzentren hingegen können unter der Raumdecke bis zu 1 Meter starke Warmluftpolster vorherrschen. Diese entstehen durch den Auftrieb der warmen Luft von Klimaanlagen, Netzteil-Ventilatoren sowie Rack-Entlüftungen und können dazu führen, dass Rauch nicht mehr in ausreichendem Maße bis zu den punktförmigen Rauchmeldern gelangt, um einen Brand frühzeitig zu erkennen. In solchen Bereichen, wie auch in stark klimatisierten Räumen sowie in Bereichen mit hohen Deckenhöhen, erreichen Punktmelder schnell ihre Grenzen. Stattdessen empfiehlt sich der Einsatz von hochsensiblen Rauchansaugsystemen.

Für den Schutz von belüfteten IT-Einrichtungen weist der VdS darauf hin, dass eine Brandfrüherkennung mit punktförmigen Rauchmeldern mindestens erschwert oder sogar unmöglich ist. Stattdessen wird auch hier der Einsatz von hochsensiblen aktiven Rauchansaugsystemen empfohlen, da diese die Möglichkeit einer „frühzeitigen und örtlich begrenzten Reaktion" bieten.

Eine neue Herausforderung für den Brandschutz im IT-Bereich stellen moderne Server-Racks dar, die über ein eigenes Kühlsystem verfügen und von der Umwelt gekapselt sind. Entstehender Rauch innerhalb der Racks dringt nur noch sehr verzögert nach außen, was dazu führt, dass eine normale Raumüberwachung mit Rauchmeldern keinesfalls mehr ausreicht. Im Brandfall freigesetztes Löschmittel kann zudem nur sehr verzögert in den Serverschrank eindringen. Für solche Racks bieten Hersteller von Branddetektions- und Lösch-Systemen Anlagen für den Einrichtungsschutz in Form von 19“-Einschüben an. Pro Gerät können bis zu 5 Racks geschützt werden. Auch für diese Anwendung, bei der im Brandfall aufgrund der starken Klimatisierung eine hohe Rauchverdünnung zu erwarten ist, werden mittlerweile vermehrt hochsensible 19“-Rauchansaugsysteme eingesetzt. Diese sind auch mit integrierter Löschanlage, mit externer Löschansteuerung sowie mit integrierter Zweimelderabhängigkeit erhältlich.

Zur Ansteuerung automatischer Löschanlagen sollen Fehlalarme möglichst ausgeschlossen werden. Zu diesem Zweck müssen Brandmelder bei der Raumüberwachung in Zweimelderabhängigkeit installiert werden, das heißt, es müssen zwei Melder einen Alarm geben, bevor dieser weitergeleitet wird. Ein einzelner Melder löst nur einen technischen, internen Alarm aus.

Seit einigen Jahren stellen Hersteller von Branddetektions- und Lösch-Systemen Anlagen her, die einzelne Racks oder ganze Schrankreihen selbstständig auf Brandaerosole überwachen und löschen können. Eine Brandentstehung in stromführenden Schränken kann durch Schmor-, Schwel- und Glimmbrände ausgelöst werden. Gründe hierfür sind oft die Überlastung der Bauteile sowie fehlerhafte und defekte Kontakte. Brände, beispielsweise auf einer Platine, führen, wenn nicht rechtzeitig erkannt, zu Verrußung und Korrosion großer Bereiche der Hardware. Erschwerend kommt hinzu, dass moderne klimatisierte Racks mit sehr hohen Luftwechselraten arbeiten, die jeglichen Rauch sofort verdünnen, der damit für konventionelle Rauchmelder in der Entstehungsphase praktisch nicht zu detektieren ist.

Wie auch in der Brandfrühesterkennung von IT-Räumen, haben hier Brandfrühesterkennungssysteme mit Ansaugrauchmeldern klare Vorteile, da hierbei die Luftproben direkt im Schrank an den Einlässen der Umluft bzw. Klimatisierung entnommen werden können. Moderne Systeme sind heutzutage durch ihre extreme Modularität bestens gerüstet für den Ausbau aller Stufen der Branddetektion und –bekämpfung. Sie sind für EDV-, Server- und Schaltschränke der neuen Generation - geschlossene Schränke mit integrierten Kühlsystemen - bestens geeignet. Sie werden als 19“-Einschub zur hochempfindlichen Branderkennung eingesetzt, geben Steuersignale aus für weiches Herunterfahren und können selbsttätig eine Objektlöschung durchführen. Eine Löscheinheit kann im Gerät integriert sein oder extern angesteuert werden. Als Löschmittel kommen vornehmlich Novec 1230 und Stickstoff zum Einsatz. Stickstoff hat hierbei den Vorteil einer sehr guten Verteilung und verbesserten Haltezeit, während Novec 1230 sehr kompakt und platzsparend in der Bevorratung ist. Es sind Geräte in 19“ Technik am Markt erhältlich, deren Branderkennungsteil von VdS anerkannt wurde und bereits die neuesten Sensibilitätsklassen „A“ und „B“ der DIN-Norm EN 54-20 erfüllen.

Löschanlagen

Die Wirksamkeit und Zuverlässigkeit einer Brandschutzanlage hängt von der risikogerechten Projektierung, Mengenbemessung und Dimensionierung ab.

Gaslöschsysteme werden in die Gruppen Inertgase und chemische Gase unterteilt.

Inertgase:

- Löschung durch Sauerstoff-Entzug

Die Gaslöschtechnik ist für Rechenzentren und deren Geräte die geeignete Technik. Sie beruht auf dem Prinzip des Sauerstoffentzuges. Dabei wird durch das Löschmittel der Sauerstoffanteil der Raumluft so stark reduziert, dass ein Verbrennungsprozess unterbunden wird.

- Kohlendioxid (CO_2)

Kohlendioxid ist in der Atmosphäre vorhanden, wird allerdings wegen der davon ausgehenden Gefährdung von Menschen bei neuen Anlagen nicht mehr eingesetzt.

- Argon (Ar)

Argon ist ein Edelgas und kann aus der Umgebungsluft gewonnen werden. Argon selbst ist nicht giftig, kann aber bei der für eine Löschung erforderlichen Konzentration zu Sauerstoffmangel oder einer Gefährdung durch Brandgase führen.

- Stickstoff (N_2)

Stickstoff ist ebenfalls in der Atmosphäre enthalten. Es ist farb-, geruch- und geschmacklos. Stickstoff ist nicht giftig, kann jedoch eine Gefährdung durch Brandgase und Sauerstoffmangel hervorrufen.

- Löschgas FM-200 (HFC 227ea), Novec 1230

Diese Löschgase entfalten ihre Löschwirkung durch Wärmeabsorption in der Flamme. Hier wirkt eine physikalische Komponente und in geringem Umfang auch eine chemische Komponente. Bei diesen Gasen ist eine Lagerung der Löschmittel-Behälter im eigentlichen Löschbereich unter bestimmten Voraussetzungen zugelassen, was bei der Nachrüstung von vorhandenen Rechenzentren ohne Löschanlage entscheidend sein kann.

Wichtig ist vor allem, dass die Gaslöschtechnik dem Objekt- und Raumschutz entgegenkommt. Wasserschäden treten nicht auf, auch Pulver- oder Schaum-Rückstände werden vermieden. Die Flutung erfolgt bei Inertgasen innerhalb von 120 Sekunden und bei chemischen Gasen innerhalb von 10 Sekunden. Die Löschgase sind elektrisch nicht leitfähig und Kurzschlüsse werden während oder nach der Löschung vermieden.

Zu beachten ist bei Löschanlagen mit gasförmigen Löschmitteln, dass aufgrund der bei einer Auslösung entstehenden Überdrücke eine gesicherte Druckentlastung über Druckentlastungsklappen erforderlich ist. Gemäß den geltenden Vorschriften muss die berechnete Haltekonzentration für 10 Minuten aufrechterhalten werden. Damit es zu keiner Rückentzündung kommen kann, ist es erforderlich, die Stromversorgung im gesamten Rechenzentrum abzuschalten.

Brandvermeidungssystem

Diese Variante reagiert nicht erst bei einem Brand, sondern vermeidet diesen. Die Sauerstoffreduktion wird durch sehr genaue Steuerungen auf einem entsprechenden Level gehalten. Gleichzeitig wird Stickstoff in die Räume geleitet. In dieser Atmosphäre kann die Entstehung eines offenen Feuers ausgeschlossen werden. Die Schutzbereiche bleiben begehbar.

6.1.2 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten

RZ Kategorie	Technischer Brandschutz			zulässige RZ Ausfallzeit*
	Serverschrank bis zu 5 kW	Serverschrank ab 5 kW bis zu 30 KW	Rechenzentrum / Serverraum 500 bis zu 2500 Watt/qm	
A	Überwachungseinheit mit Banderkennung		Überwachungseinheit mit Bandfrüherkennung	72 h
B	Überwachungseinheit mit Bandfrüherkennung und Löschtechnik		Brandmeldeanlage, Überwachungseinheit mit Bandfrüherkennung und eigenständiger Löschtechnik	24 h
C	Brandmeldeanlage, Überwachungseinheit mit Brandfrüherkennung und eigenständiger Löschtechnik			1 h
D	Brandmeldeanlage, Überwachungseinheit mit Bandfrüherkennung und eigenständiger Löschtechnik		Brandmeldeanlage, Überwachungseinheit mit Bandfrüherkennung und eigenständiger Löschtechnik/Sauerstoffreduzierungssystem	10 min
E	Brandmeldeanlage, Überwachungseinheit mit Brandfrüherkennung und eigenständiger Löschtechnik in redundanter Ausführung / Sauerstoffreduzierungssystem			0 min

Tabelle 9 aus BITKOM-Matrix „Planungshilfe betriebssicheres Rechenzentrum" – Technischer Brandschutz

Rechenzentren

Liegen die tolerierbaren Ausfallzeiten bei maximal 24 Stunden, reichen Detektions- und Auswerteeinheiten ohne nachgeschaltete Löschanlagen aus. Werden maximale Ausfallzeiten von weniger als einer Stunde gefordert, ist eine nachgeschaltete Löschanlage –mit Gas als Löschmittel unabdingbar. Sind noch geringere oder keine Ausfallzeiten durch ein Feuer tolerierbar, ist die Brandvermeidung mittels Sauerstoff-Reduktion, neben der aktiven Brandfrühesterkennungs- und Gaslöschanlage mit Novec 1230 eine mögliche Alternative.

Die Entscheidung für Gaslöschanlagen oder Brandvermeidungssysteme kann nur nach gründlicher Analyse durch Fachleute erfolgen. Projektierungsmerkmale für die Dimensionierung und Installation einer Löschanlage mit Steuerung sind:

- Festlegung der Anforderungen an die Anlage(n) - tolerierbare Ausfallzeiten usw.
- Festlegung der Detektionseinheiten (Punktmelder, RAS)
- Festlegung der Löschanlage und des Löschmittels
- Stromlosschalten des Rechenzentrums bei Auslösung der Löschanlage
- Eventuell Planung einer Brandvermeidungsanlage
- Berücksichtigung von Kalt-Warmgängen

Serverschränke

Eine Überwachungseinheit mit Branderkennung (Brandfrühesterkennung) detektiert bereits äußerst geringe Mengen von Rauchaerosolen, wie sie in der frühesten Phase der Brandentstehung freigesetzt werden. Dies schafft wertvollen Zeitgewinn, der für organisatorische Maßnahmen (automatischer Telefonruf, Pager etc.) und das Einleiten von Gegenmaßnahmen wie weiches Herunterfahren, Datenauslagerung, selektive Abschaltung oder eventuelle gezielte Objektlöschung unbedingt benötigt wird.

Die Geräteabschaltung bietet im Brandfall die sicherste Alternative gegen ein weiteres Ausbreiten des Brandes bzw. der korrosiven Rauchgase. Eine moderne, weiche Abschaltung bedeutet aber keinesfalls die sofortige Abschaltung der Stromzufuhr. Bei einer weichen

Abschaltung wird mit der frühestmöglichen Brandmeldung ein intelligentes Servermanagement aktiviert, welches die wertvollen Daten schnellstens auf benachbarte Daten- bzw. Serverschränke umleitet. Dies kann allerdings nur über die Kombination einer entsprechenden Software-/Hardware-Umgebung mit einer leistungsfähigen Brandfrühesterkennung erreicht werden. Das endgültige Abschalten der Stromzufuhr erfolgt dann nach Abschluss des Datentransfers.

6.2 Baulicher Brandschutz

Ziel des baulichen Brandschutzes ist das Retten von Menschenleben. Das erfordert höchste Qualität für Material und Verarbeitung sowie eine strikte Einhaltung der Vorschriften und Richtlinien.

Die Grundlagen des baulichen Brandschutzes sind in den Bauordnungen der Länder, den Vorschriften über brandschutztechnische Einrichtungen, Brandschutzkonzepte, Brandwände und Rettungswege festgehalten. Das Brandverhalten von Baustoffen und Bauteilen regelt die DIN 4102, allerdings ohne jede Berücksichtigung der notwendigen Schutzziele, gerade für IT-Rechenzentren

Zu beachten sind die Feuerwiderstandsdauern tragender Bauteile, der Brandschutz in den Elektroinstallationen sowie bei versorgungstechnischen Anlagen. Zu klären sind bei der Planung eines Rechenzentrums auch die feuerwehrtechnischen Möglichkeiten bezogen auf Feuerwiderstandsdauer und Rettungswege. Dabei sind Feuerwehraufzüge und Sicherheitstreppenhäuser zu berücksichtigen. Für ein Rechenzentrum gelten außerdem betriebsspezifische Brandschutzverordnungen.

Brandbekämpfung, Löschmittel und Entrauchung sind ebenfalls Teil der Planungen. Sie betreffen tragbare Feuerlöscher, eine eventuell erforderliche Löschmittel-Rückhaltung u.a..

6.2.1 Schutzziele

Bei der Planung eines Rechenzentrums sind vor allem die Schutzziele zu definieren. In der Planungsphase ist zu klären, ob die Vorschriften, Richtlinien und Schutzziele selbst umgesetzt werden können. Der Einsatz erfahrener Planer ist zu empfehlen, da baulicher und technischer Brandschutz mit den Erfordernissen eines unterbrechungsfreien Rechenzentrumsbetriebes in Einklang gebracht werden müssen. Nachträgliche Ein- und Umbauten verschlingen immense Summen oder führen zu einer eklatanten Erhöhung der Versicherungsprämien im Bereich Feuer- und Elektronik-Versicherung.

6.2.2 Funktionsweise und Raumanforderungen

Bauteile werden nach ihrem Brandverhalten in Feuerwiderstandsklassen eingeteilt. Die Feuerwiderstandsdauerangaben belaufen sich meist auf 30, 60, 90 und 120 Minuten. F 30 heißt z.B., dass beim Brandversuch bis zum Feuerdurchschlag mindestens 30 Minuten vergangen sind, bevor die Wand nicht mehr standhält. Die bauaufsichtliche Bezeichnung für die Klasse F 60 ist „feuerhemmend“, für F 90 „feuerbeständig“.

Wände, Böden und Decken müssen mindestens nach Feuerwiderstandsklasse F90 ausgebildet werden. Türen sind mindestens in T90 -Ausführung zu planen, das heißt, dass Türen 90 Minuten Feuer widerstehen. Auch ein Schutz gegen Rauchgas und Spritzwasser ist unabdingbar.

Kabel- und Installationskanäle vom und zum Rechenzentrum sind wirksam zu schützen. Dabei können Kabelkanäle mit Funktionserhalt nach E30 oder gar E90 gesichert werden. Installationskanäle sind nach I30 oder I90 und selbstständige Lüftungskanäle nach L90 auszubilden. Werden elektrische Leitungen durch feuerbeständige Decken und Wände geführt, müssen die Durchführungen ebenfalls feuerbeständig und rauchgasfest verschlossen, das heißt abgeschottet werden. Diese Abschottungen können unter Umständen auch mittels Brandschutzkissen vorgenommen werden.

Kabeltrassen stellen im Brandfalle ein sehr hohes Risiko dar und sollten wasser- und feuchtigkeitsbeständig beschichtet oder ausgeführt sein. Sie verhindern damit als Dämmschichtbildner recht sicher die Brandausbreitung entlang der Kabel. Die Kabel selbst sollten aus brandhemmendem Material bestehen, das zudem keine aggressiven Rauchgase bildet.

Feuer breitet sich auch schnell und unkontrollierbar über (brennbare) Rohre aus, die an Decken und Wänden geführt sind. Schutz bieten Rohrabschottungen als feuerbeständige und rauchgasdichte Barriere.

Nur eine reine Bauteileprüfung ist allerdings für komplexe und betriebssichere Rechenzentren keinesfalls ausreichend. Die zu errichtenden Räume oder modularen Sicherheitszellen müssen im Falle einer Hochverfügbarkeitslösung einer genormten Systemprüfung nach EN 1047-2 unterzogen werden, ebenso wie die Gewerke der Decken-Wand- und Boden-Wand-Verbindung, der Kabeleinführung, der Überdruckableitung oder des Türbereiches. Die Europa-Norm für die Rechenzentrums-Infrastruktur legt sowohl die Stärke als auch die Zeitdauer von genau definierten Belastungen fest. Der Anwender hat damit die Sicherheit, dass sein gesamtes System und nicht nur eine Wand oder die Tür feuerbeständig ist.

6.2.3 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten

RZ Kategorie	Baulicher Brandschutz			zulässige RZ Ausfallzeit*
	Serverschrank bis zu 5 kW	Serverschrank ab 5 kW bis zu 30 KW	Rechenzentrum / Serverraum 500 bis zu 2500 Watt/qm	
A	Wände, Boden, Decke, Feuerwiderstandsklasse mind. F90, Schutz gegen Rauchgas und Spritzwasser, minds. T90-Türen, Kabelschotts in gleicher Schutzwertigkeit		Wände, Boden, Decke, Feuerwiderstandsklasse mind. F90, Schutz gegen Rauchgas und Wasser, minds. T90-Türen, Kabelschotts in gleicher Schutzwertigkeit	72 h
B	Wände, Boden, Decke, Feuerwiderstandsklasse mind. F90, Schutz gegen Rauchgas und Spritzwasser, minds. T90-Türen, Kabelschotts in gleicher Schutzwertigkeit		Wände, Boden, Decke, Feuerwiderstandsklasse mind. F90, Schutz gegen Rauchgas und Wasser für 30 min, minds. T90-Türen, Kabelschotts in gleicher Schutzwertigkeit	24 h
C	Systemprüfung des baulichen Branschutzes Wände, Boden, Decke, Türen: nach Europanorm EN 1047-2, Schurz gegen Rauchgas und Spritzwasser für 60 min, Kabelschotts in gleicher Schutzwertigkeit		Systemprüfung des baulichen Branschutzes Wände, Boden, Decke, Türen: nach Europanorm EN 1047-2, Schurz gegen Rauchgas und Spritzwasser für 60 min, Kabelschotts in gleicher Schutzwertigkeit	1 h
D	Systemprüfung des baulichen Branschutzes Wände, Boden, Decke, Türen: nach Europanorm EN 1047-2, Schurz gegen Rauchgas und Spritzwasser für 60 min, Kabelschotts in gleicher Schutzwertigkeit		Systemprüfung des baulichen Branschutzes Wände, Boden, Decke, Türen: nach Europanorm EN 1047-2, Schurz gegen Rauchgas und Spritzwasser für 60 min, Kabelschotts in gleicher Schutzwertigkeit	10 min
E	Systemprüfung des baulichen Branschutzes Wände, Boden, Decke, Türen: nach Europanorm EN 1047-2, Schurz gegen Rauchgas und Spritzwasser für 60 min, Kabelschotts in gleicher Schutzwertigkeit			0 min

Tabelle 10: aus BITKOM-Matrix „Planungshilfe betriebssicheres Rechenzentrum“ – Baulicher Brandschutz

Besonderheiten

Folgende Projektierungsmerkmale sollten beachtet werden:

- Festlegung der Schutzziele unter Beachtung der speziellen Anforderungen der IT-Infrastruktur
- Festlegung der baulichen Gegebenheiten
- Planung der Bauausführung – möglichst durch professionellen Planer
- Anfertigen der Lastenhefte für die Einzelgewerke der Ausschreibung
- Sammeln der einlaufenden Angebote, Vergleichen, Auswerten
- Erstellen eines Vergabe-Vorschlages für die Entscheider

7 Flächenkonzeption und Sicherheitszonen für Rechenzentren

Sicherheit der Informationstechnik ist ein weit gefasster Begriff, der sowohl die logische Sicherheit der Daten, die physische Sicherheit der Systeme und die organisatorische Sicherheit der Prozesse beinhaltet. Ziel eines umfassenden Sicherheitskonzeptes ist es, alle Bereiche zu betrachten, Risiken frühzeitig zu erkennen, zu bewerten und Maßnahmen zu ergreifen, so dass die Wettbewerbsfähigkeit eines Unternehmens am Markt nicht gefährdet ist.

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.

Standort der IT-Bereiche

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.

Bei Betrachtung der physischen Sicherheit eines Standortes sollten folgende Kriterien berücksichtigt werden:

- Geringes Gefährdungspotential 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 Gefahrenpotentials aufgrund der gesellschaftlichen Stellung des Unternehmens

Werden alle Risikofaktoren und die unternehmensspezifischen Rahmenbedingungen berücksichtigt, können bei der Konzeption der IT-Infrastruktur bereits im Vorfeld Gefahren ausgeschlossen sowie Aufwände und Kosten vermieden werden.

Aufbau eines Rechenzentrums

Bei der Konzeption und Planung eines Rechenzentrums werden die unterschiedlichen Funktionsbereiche entsprechend ihres Anspruches an die Sicherheit und ihrer Wertigkeit für den Funktionserhalt der Informationstechnik angeordnet.

Die unterschiedlichen Funktionsbereiche lassen sich wie folgt einteilen:

Sicherheits-Zonen	Funktion	Kennzeichnung (Beispiel)
1	Grundstück	Weiß
2	Halböffentlicher Bereich, angrenzende Büroflächen	Grün
3	Operating-Bereiche, Nebenräume der IT	Gelb
4	Technische Anlagen zum Betrieb der IT	Blau
5	IT- und Netzwerkinfrastruktur	Rot

Tabelle 11: Funktionsbereiche eines Rechenzentrums

Anordnung der Sicherheitszonen

Stellt man die unterschiedlichen Sicherheitszonen schematisch dar, ergibt sich beispielhaft das gezeigte Bild: Der IT-Bereich (rot) befindet sich im Inneren und wird durch die angrenzenden Zonen 3 und 4 (gelb/blau) geschützt. Die Sicherheitszonen 1 und 2 (weiß/grün) bilden die Außenschicht. Die einzelnen Sicherheitszonen werden durch Sicherheitslinien getrennt.

Die Sicherheitslinien stellen den überwachten und gesicherten Übergang zwischen den Zonen dar und werden entsprechend den Sicherheitsanforderungen des Unternehmens ausgebildet.

Um mögliche Sabotage zu vermeiden, bietet sich die Trennung der Funktionsbereiche durch eingeschränkte Zutrittsmöglichkeiten zu sensiblen Bereichen an. So erhält zum Beispiel ein Wartungstechniker für die Klimaanlagen oder USV nur den Zutritt zu den Technischen Bereichen (blau) und nicht zum IT-Bereich (rot) des Unternehmens.

Um die Sicherheit der IT-Infrastruktur zu gewährleisten, sind die Standorte der unterschiedlichen Funktionsbereiche und die Einteilung der Sicherheitszonen oder Sicherheitslinien wichtig. Es kann jedoch nur im Gesamtkontext eines umfassenden Sicherheitskonzeptes, das alle Bereiche der IT-Sicherheit betrachtet, eine kontinuierliche IT-Verfügbarkeit realisiert werden.

8 Verkabelung

8.1 Ausgangssituation

Die primäre und originäre Aufgabe von Rechenzentren ist der Betrieb von IT-Anwendungen auf Mainframes und Servern sowie die Datenhaltung und Sicherung auf Speichersystemen.

Aus Sicht der IT ist die entscheidende Anforderung die Verfügbarkeit, also die möglichst unterbrechungsfreie Betriebsfähigkeit der in der Regel unternehmenskritischen IT-Anwendungen. Typischerweise gehören dazu ERP-Systeme, Produktionsanwendungen in Industrieunternehmen, Datenbanken, Büroanwendungen und deren Betriebssysteme, aber auch der Zugang zu Provider-Netzwerken (MAN, WAN) und zum Internet.

Für die IT gilt das ISO-OSI 7 Schichten-Referenzmodell, welches die Anwendung als oberste Schicht definiert und als unterste, den sog. ersten Layer (Schicht), die zum Datentransport notwendige physikalische Infrastruktur, die IT-Verkabelung und die Datentransportgeräte wie z.B. Layer 1 Switches.

Für die Verfügbarkeit, also die Betriebssicherheit von IT-Anwendungen in einem Rechenzentrum ist daher dessen IT-Verkabelung elementar: Ohne funktionierende IT-Verkabelung können IT-Geräte wie Server, Switches und Speicher nicht miteinander kommunizieren und Daten austauschen, diese Daten nicht verarbeiten, vorhalten oder sichern.

Häufig sind IT-Verkabelungen jedoch historisch gewachsen und können den heutigen Anforderungen wie

- hohe Kanaldichten
- hohe Übertragungsgeschwindigkeiten
- unterbrechungsfreie Hardwareänderungen
- Serviceunterstützung
- Lüftungsaspekten

nur schwer genügen.

Strukturierung von IT-Verkabelungen sowie deren sorgfältige und vorausschauende Planung sind daher grundlegende Aufgaben eines Rechenzentrumsbetreibers. Auch gesetzliche Grundlagen wie Basel II oder SOX fordern eine durchgehend stringente Transparenz.

8.2 Normative Grundlagen

Gemeinsam ist allen Normen nach ISO/IEC, EN und TIA, die Forderung nach bzw. die Festschreibung einer strukturierten, anwendungsneutralen IT-Verkabelung. Sie sprechen zudem eindeutige Empfehlungen aus, die IT-Verkabelung redundant auszulegen, um die Betriebssicherheit eines Rechenzentrums auf hohem Niveau sicherzustellen.

Die Planung, Installation und Abnahme der IT-Verkabelung von Rechenzentren wird in der Normenreihe DIN EN 50174 beschrieben. Wesentliche Inhalte sind z.B. der Qualitätsplan, der Potentialausgleich, Sicherheitsabstände von Kupfer-IT-Verkabelungen zu anderen elektrischen Quellen, sowie die die Dokumentation und Abnahme des gesamten Rechenzentrums.

8.3 Qualität/Komponenten-/ Systemauswahl

Aufgrund der maximal hohen Verfügbarkeitsansprüche und der permanent steigenden Übertragungsdatenraten sind die Qualitätsanforderungen an die IT-Verkabelungskomponenten für Rechenzentren vielfach höher als an die in LANs eingesetzten Produkte. Bereits im sehr frühen Planungsstadium sollte der Qualitätsgedanke bei der Auswahl der Systeme berücksichtigt werden, um Leistungsanforderungen wie

- Kabeldesign bei Kupfer und LWL[2]
- Bandbreiten bei Kupfersystemen und LWL-Kabeln

2 LWL= Lichtwellenleiter

- Einfüge und Rückflußdämpfungsbudgets bei LWL
- EMV Festigkeit bei Kupfersystemen
- Updatefähigkeit auf nächst höhere Geschwindigkeitsklassen
- 19“ Schrankdesign

zu genügen.

Die IT-Verkabelungskomponenten können sowohl bei LWL als auch bei Kupfer, werkskonfektionierte betriebsfertige Systeme für sog. „Plug-and-Play Installationen“ sein.

Vorkonfektionierte Systeme haben die höchstmögliche und reproduzierbare Qualität und daher sehr gute Übertragungseigenschaften und eine hohe Betriebssicherheit. Aufgrund der hohen Anforderungen an die Verfügbarkeit, sind im Kupferbereich nur geschirmte Systeme einzusetzen. In den globalen Normen wird mindestens eine Klasse EA Kupferverkabelung gefordert.

Auf die Auswahl der Lieferanten der IT-Verkabelung sollte ebenfalls mit ausreichender Priorität geachtet werden. Die Hauptanforderung an einen verlässlichen Lieferanten ist neben der Qualität der Verkabelungskomponenten auch das Rechenzentrums-Fachwissen, die Erfahrung in der Rechenzentrums-IT-Verkabelung und die nachhaltige Lieferleistung. Idealerweise sollte der Lieferant auch ganzheitliche Planungs- Installations- und Service-Dienstleistungen anbieten

8.4. Struktur

Rechenzentren sind die Nervenzentralen der Unternehmen. Sie unterliegen daher ständigen Veränderungen, getrieben durch die kurzen Lebenszyklen der aktiven Komponenten. Um nicht mit jedem neuen Gerät grundlegende bzw. tiefgreifende Änderungen an der IT-Verkabelung durchführen zu müssen, empfiehlt sich eine übersichtliche und transparente, vom jeweils aktuellen „Gerätepark“ entkoppelte, physikalische IT-Verkabelungsinfrastruktur.

Diese sollte die jeweiligen Geräte-Standorte mit einer einheitlichen und durchgängigen IT-Verkabelungsstruktur verbinden.

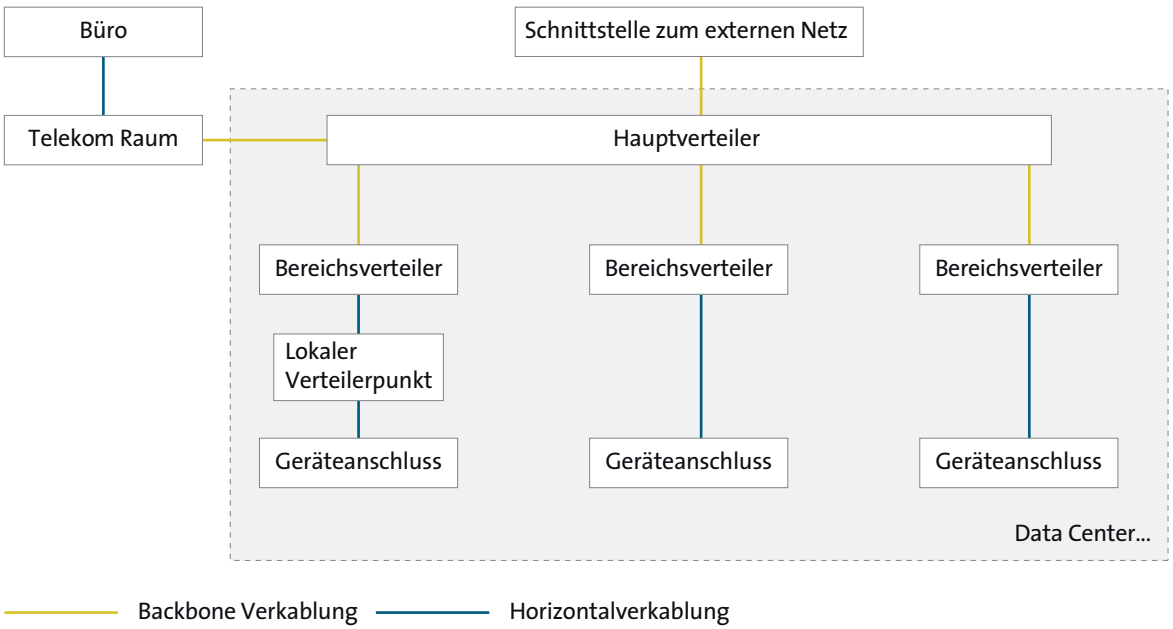


Abbildung 10: Schematische EN 50173-5 / TIA 942 Verkabelungsstruktur

In den Normen DIN EN 50 173-5 und ISO/IEC 24764 wird diese Geräteverkabelung in die Segmente Bereichs- und Geräteanschlussverkabelung, mit der GA (Geräteanschluss) genannten Schnittstelle dazwischen, aufgeteilt. Die aktiven Geräte werden durch möglichst kurze, gerätespezifische Anschlusskabel über die GA-Schnittstelle an die dadurch „geräteneutrale“ Bereichsverkabelung angebunden. Damit muss beim Gerätetausch, der oftmals mit dem Wechsel des Steckgesichts am Gerät verbunden ist, nur das anschlussspezifische Kabel ausgetauscht werden – ohne in die Bereichsverkabelung eingreifen oder rückbauen zu müssen.

Besonderes Augenmerk ist dabei auf Bereiche mit hoher Packungsdichte zu legen.

Auf diese Art werden die mit einem Gerätetausch verbundenen Umverkabelungen sowohl vom finanziellen als auch vom zeitlichen Umfang auf ein Minimum reduziert - und das unter vollständigem Erhalt der definierten Struktur.

Die Horizontalverkabelung sollte, wo erforderlich, in Kupfer und LWL ausgeführt werden, damit verschiedene Geräte angeschlossen werden können. Die Backbone Verkabelung sollte in LWL und Kupfer redundant ausgeführt werden.

In den GA-Schnittstellen sollten für die jeweiligen Packungsdichteanforderungen der anzuschließenden Geräte geeignete Stecksysteme gewählt werden. Die Normen DIN EN 50 173-5 und ISO/IEC 24764 benennen entsprechende Stecksysteme.

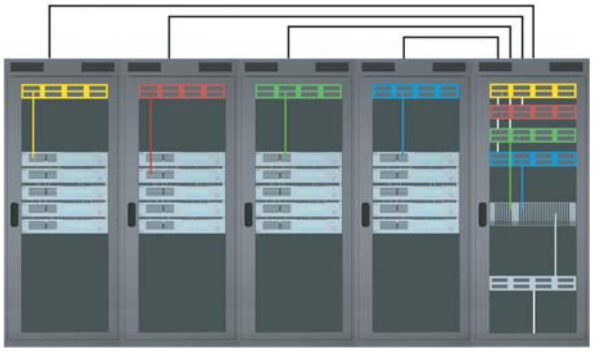


Abbildung 11: Darstellung: Horizontalverkabelung (Cu und LWL) mit Bereichsverteiler (BV) und Server-/Strorageschränken mit Geräteanschlu (GA)

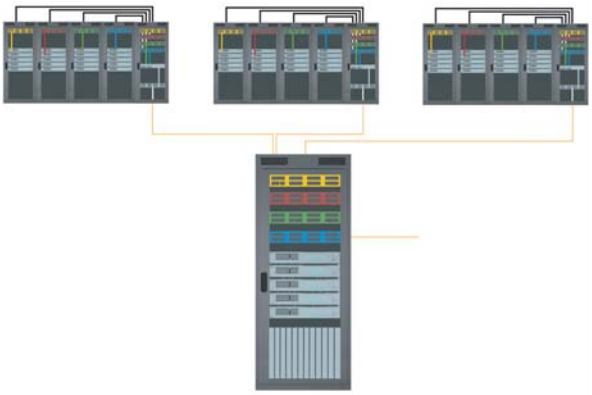


Abbildung 12: Darstellung: Backboneverkabelung (LWL) mit Hauptverteiler (HV) und Anschluss an die Horizontalverkabelung (Cu und LWL) mit Bereichsverteiler (BV) und Server-/Storageschränken mit Geräteanschluss (GA)

8.5 Redundanz und Sicherheit

Die Anforderung der Hochverfügbarkeit bedingt die redundante Auslegung von Verbindungen und Komponenten: So muss Hardware im laufenden Betrieb getauscht werden können und beim Ausfall einer Leitung muss ein Alternativweg die Applikation unterbrechungsfrei übernehmen können.

Daher ist es elementar, dass eine entsprechende gesamtheitliche IT Verkabelungsplatform unter Berücksichtigung von Biegeradien, Sicherung der Performance sowie schneller und zuverlässiger Montage während des Betriebes vorgesehen wird.

Die Verfügbarkeit von Anwendungen kann durch den Einsatz von werkseitig vorkonfektionierten IT-Verkabelungssystemen gesteigert werden. Damit reduziert sich der Aufenthalt von Installationspersonal im Sicherheitsbereich des Rechenzentrums auf ein Minimum sowohl bei der Erstinstallation als auch bei eventuellen Hardwareänderungen und bedeutet einen zusätzlichen Zugewinn bei der Betriebssicherheit. Außerdem sollte darauf geachtet werden, dass alle Produkte im Rahmen eines Qualitätsmanagements geprüft und dokumentiert werden.

Für die Verbindung von Rechenzentren untereinander, z.B. redundante Rechenzentren, Backup-Rechenzentren, oder auch nur die einfache Auslagerung und Sicherung von Daten an einen anderen Standort, ist die Anbindung an und die Sicherheit von MAN und WAN Provider-Netzwerken (Datentransportdienste oder sog. „dark fibers"), oder eigene LWL-Kabelstrecken von immenser Wichtigkeit für die Betriebssicherheit und Verfügbarkeit und ist wie die rechenzentrumsinterne IT-Verkabelung redundant auszulegen.

8.6 Installation

Für einen sicheren und zuverlässigen Betrieb von LWL-IT-Verkabelung im Rechenzentrum, ganz besonders bei deren Installation und bei Patcharbeiten, müssen die durchführenden Techniker auf die Spezifikation der Systeme geschult sein. Bei der Auswahl des 19" Server bzw. -IT-Verkabelungsschrankes und unter Bezug auf Kapitel „4.1 Sicherer Serverschrank " ist aus Verkabelungssicht zu empfehlen, mind. 800 mm breite Schranksysteme einzusetzen. Sie ermöglichen die Installation eines gesamtheitlichen Kabelmanagement in vertikaler und horizontaler Ausrichtung. Die Schranktiefe ergibt sich in der Regel durch die zu installierenden passive und aktive Komponenten. Für passive Verteiler haben sich ebenfalls mind. 800 mm tiefe Schranksysteme bewährt. Für den Einbau aktiver Komponenten empfehlen sich 1000 bis 1200 mm tiefe Schranksysteme.

Der bereits unter dem Sicherheitsgedanken mögliche Vorteil von werkskonfektionierten IT-Verkabelungssystemen zeigt sich bei der Installation in Form von Zeitersparnis. Zu erwähnen ist, dass bei deren Einsatz bei Erweiterungen der Rechenzentrumskapazität durch Zuwachs von IT-Geräten, diese Geräte und somit die eigentlichen IT-Anwendungen, schnellstmöglich miteinander verkabelt und in Betrieb genommen werden können - gleiches gilt auch für Änderungen der Hardware.

8.7 Dokumentation und Beschriftung

Ein wesentliches Mittel zur einfachen Administration der IT-Verkabelung sowie zur sicheren Planung von Umbauten bzw. Erweiterungen ist eine akribisch aktuell gehaltene Dokumentation. Hier gibt es von „individuellen" Excel-Listen bis hin zu ausgereiften softwarebasierten Dokumentationstools eine große Vielfalt an Möglichkeiten. Wichtig ist, dass die Dokumentation immer auf dem aktuellsten Stand ist und der real installierten IT-Verkabelung entspricht. Die Auswahl des Tools ist dem Anwender überlassen.

Eng verbunden mit der Dokumentation ist die eindeutige und – auch unter eingeschränkten Lichtverhältnissen - leicht lesbare Beschriftung der Kabel. Auch hier gibt es zahlreiche Systeme von Identifikationsmöglichkeiten, z.B. von Kabelfähnchen mit austauschbaren Etiketten bis hin zu Barcode-basierten Etikettenlabels. Welche Ausführungsform gewählt wird, hängt von individuellen Anforderungen an. Entscheidend ist, dass die Nomenklatur unternehmenseinheitlich gestaltet ist. Es empfiehlt sich zur Sicherstellung einer eindeutigen Kabelbeschriftung, die Daten zentral zu verwalten.

9 Die Zertifizierung eines betriebssicheren Rechenzentrums

9.1 Das Managementsystem

9.1.1 Der Aufbau eines Managementsystems

Für alle Unternehmen stehen Kundenorientierung, Wirtschaftlichkeit und Wettbewerbsfähigkeit im Vordergrund. Entscheidende Faktoren sind Ressourcenplanung, Fehlervermeidung und ein prozessorientierter Ansatz in der Leistungserbringung.

Internationale Standards wie z.B. ISO/IEC 27001:2005 etc. liefern konkrete Hilfestellung und eine Struktur für die Implementation eines Managementsystems und sind durch neutrale Gesellschaften zertifizierungsfähig.

Ein Managementsystem ist die Basis für die

- Prozessorientierung
- ständige Verbesserung der Geschäftsprozesse (KVP)
- stärkere Kunden- und Lieferantenorientierung
- Interpretation von Wechselwirkungen zwischen den Geschäftsprozessen
- Fehlervermeidung (Präventiv- und Korrekturmaßnahmen) und
- Erfüllung von gesetzlichen Forderungen.

9.1.2 Vorteile eines Managementsystems

Der erfolgreiche Betrieb eines Managementsystems bringt entscheidende Vorteile für das Unternehmen:

- Die Rückverfolgbarkeit der Geschäftsprozesse, Produkte und Dienstleistungen wird verbessert
- Schwachstellen im System werden aufgedeckt
- Risiken werden erkannt, analysiert, minimiert oder abgewandt
- das Unternehmen ist auf Notfälle vorbereitet
- durch eine ständige Kontrolle wird die Fehlerquote gesenkt und damit die Leistungserbringung verbessert. Dies führt und zu einer Kostenreduktion und zu einer höheren Qualität
- die Motivation der Mitarbeiter wird durch klare Regelungen der Verantwortlichkeiten gefördert
- die angemessene Dokumentation der Prozesse schafft Transparenz
- das Kundenvertrauen in die Qualitätsfähigkeit des Unternehmens wird gefördert
- das Firmenimage wird aufgewertet
- die Wettbewerbsfähigkeit wird gestärkt
- die Haftung wird minimiert

9.1.3 Kombination von unterschiedlichen Standards

Der einheitliche Aufbau von ISO Managementsystemen lässt grundsätzlich eine Kombination von mehreren Standards zu. Ist die Kombination zulässig, lassen sich neue Standards einfach implementieren und Synergien über unterschiedliche Bereiche eines Unternehmens nutzen.

Beispiele für Synergien sind die Zusammenführung der Elemente

- Unternehmenspolitik und -ziele
- Managementreview
- bestehende Dokumentation (Namensgebung, Revision, Freigabeverfahren etc.)
- interne Audits
- Bewertung der Fehlerhäufigkeit und -quellen
- Bewertung der Kunden- und Mitarbeiterzufriedenheit
- Bewertung von Lieferanten
- Beschaffungsprozess

9.2 Die Zertifizierung eines Managementsystems

Ist das Qualitätsmanagementsystem dokumentiert und im Unternehmen wirksam eingeführt, kann es durch eine unabhängige, neutrales und zur Zertifizierung berechtigtes Unternehmen zertifiziert werden. Die Zertifizierungsgesellschaft prüft zunächst die Dokumentation und danach das System vor Ort. Der Prüfer (Auditor) verfügt über die erforderlichen Qualifikationen und Berufserfahrung. Das positive Ergebnis führt zu einem Zertifikat, welches in der Regel 3 Jahre gültig ist.

Das Managementsystem wird nach dem Zertifizierungsaudit in jährlichen Überwachungsaudits auf die Wirksamkeit geprüft.

9.2.1 Die Vorteile einer Zertifizierung

Das Zertifikat ist ein neutraler Nachweis über die Wirksamkeit des Managementsystems und kann folgende Vorteile bieten:

- Neukundengewinnung als Türöffner für neue Märkte
- Stärkung der Wettbewerbsfähigkeit
- Stärkung des Vertrauens der Kunden in das Unternehmen
- Verbesserung des Rankings und der Kreditwürdigkeit
- Reduktion des Aufwands für den Nachweis der Qualitätsfähigkeit
- Internationale Anerkennung und Akzeptanz

9.2.2 Der typische Ablauf einer Zertifizierung

Der Wahl der Zertifizierungsgesellschaft sollte ein Informationsgespräch vorausgehen.

Das Informationsgespräch

Inhalt des Informationsgespräches sind grundsätzliche Fragen zur Zertifizierung und Auditierung, zum organisatorischen Ablauf (wie Terminplan und Umfang) und zu den Kosten.

Der Zertifizierungsauftrag

Mit der Beauftragung verpflichtet sich das auftraggebende Unternehmen der Zertifizierungsgesellschaft die erforderliche QM-Dokumentation zur Verfügung zu stellen. Alternativ kann die QM-Dokumentation auch vor Ort geprüft werden. Sofern das Unternehmen es wünscht, kann zusätzlich ein Voraudit durchgeführt werden.

Durchführung des Voraudits

Ziel des Voraudits ist es, zu prüfen, ob die grundsätzlichen Voraussetzungen für die Zertifizierung des Qualitätsmanagementsystems vorliegen. Es wird ermittelt, ob das Zertifizierungsaudit zum geplanten Termin mit Aussicht auf Erfolg durchgeführt werden kann.

Die Untersuchung im Rahmen des Voraudits beinhaltet alternativ die Prüfung des QM-Handbuchs und der dazugehörigen Unterlagen. Grundsätzlich beinhaltet das Voraudit eine stichprobenartige Prüfung und erhebt keinen Anspruch auf Vollständigkeit.

Das Zertifizierungsverfahren

Die Auditoren überprüfen beim Zertifizierungsaudit, ob die dokumentierten Verfahren und Abläufe den Anforderungen des zugrundeliegenden Regelwerkes erfüllen und ob die im Unternehmen definierten Prozesse und Vereinbarungen mit der QM-Dokumentation übereinstimmen.

Das Zertifizierungsaudit besteht aus einer umfassenden Begutachtung. Im Einzelnen ist dies die Prüfung:

- der Dokumentation des QM-Systems,
- der Aufbauorganisation und
- der Umsetzung der dokumentierten Prozesse und deren Wechselwirkungen im Unternehmen.

Bei einer Erst-Zertifizierung wird das Verfahren in 2-Stufen durchgeführt.

In der 1. Stufe werden die wesentlichen Schlüsselelemente geprüft und bewertet, inwieweit das Unternehmen auf die Zertifizierung vorbereitet ist. An dieser Stelle wird auch die QM-Dokumentation des Unternehmens auf Normkonformität geprüft.

In der 2. Stufe wird die Umsetzung und Wirksamkeit des Managementsystems im gesamten Unternehmen geprüft. Werden Abweichungen bei der Begutachtung des Qualitätmanagementsystems festgestellt, so kann die Durchführung eines Nachaudits notwendig werden. Die Zertifikatserteilung wird dann erst nach Behebung aller Abweichungen und dem Unterschreiten der maximalen Anzahl von Feststellungen vom Auditor empfohlen.

Das Ergebnis wird in einem Auditbericht dokumentiert. Auf dieser Grundlage entscheidet das Zertifizierungsgremium der Zertifizierungsgesellschaft, ob ein Zertifikat erteilt wird.

Das Überwachungsaudit

Während der dreijährigen Gültigkeitsdauer des Zertifikates finden jährliche Überwachungsaudits statt.

Inhalt des 1. und 2. Überwachungsaudits ist die stichprobenartige Überprüfung ob:

- die Feststellung(en) aus dem vorangegangenen Audit behoben ist/sind,
- organisatorische Änderungen im Unternehmen vorliegen,
- sich das QM-System geändert hat,
- das Zertifikat und das Zertifizierungslogo korrekt verwendet werden,
- aktuelle Änderungen relevanter Normen, Gesetze und Vorschriften berücksichtigt wurden,
- das Managementsystem weiterhin die Anforderungen erfüllt und
- das Qualitätsmanagementsystem aufrechterhalten wurde und weiter wirksam ist.

Wurden die Überwachungsaudits erfolgreich abgeschlossen, findet nach drei Jahren in einem neuen Verfahren beginnend mit einem Rezertifizierungsaudit die erneute vollständige Überprüfung des QM-Systems statt.

Das Rezertifizierungsaudit

Zum nahtlosen Verlängern der Gültigkeitsdauer des Zertifikates um weitere drei Jahre ist ein Rezertifizierungsaudit erforderlich. Dieses muss vor Ablauf der Zertifikatsgültigkeit durchgeführt werden. Die Anforderungen des Rezertifizierungsaudits sind nahezu identisch zu denen des Zertifizierungsaudits, die Auditierung kann hier allerdings i.d.R. einstufig durchgeführt werden.

9.2.3 Die Wahl des richtigen Zertifizierungspartners

Die Wahl des richtigen Zertifizierungspartners ist entscheidend für den Erfolg des Verfahrens. Wie bei jeder Dienstleistung gibt es eine preisliche Bandbreite. Daher ist es ratsam, mehrere Angebote einzuholen oder das bestehende System mit dem vertrauten Zertifizierungspartner zu erweitern, der das System bereits kennt.

Unter Umständen kann die internationale Ausrichtung der Zertifizierungsstelle ein entscheidender Kostenfaktor sein, wenn z.B. Standorte des Unternehmens im Ausland in das Verfahren aufgenommen werden sollen.

Die Qualifikation der Auditoren ist zwischen den Zertifizierungsstellen auf ähnlich hohem Niveau, da die Zulassung der Auditoren zentral durch Akkreditierungsstellen und ISO Standards geregelt ist.

10 Anhang

■ Auswahl wichtiger Vorschriften und Regelwerke

DIN 6280, Teil 1-15	Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren
T1	Allgemeine Begriffe
T2	Leistungsauslegung und Leistungsschilder
T3	Betriebsgrenzwerte für das Motor-, Generator- und Aggregatverhalten
T4	Drehzahlreglung und Drehzahlverhalten der Hubkolben Verbrennungsmotoren, Begriffe
T5	Betriebsverhalten von Synchrongeneratoren für den Aggregatbetrieb
T6	Betriebsverhalten von Asynchrongeneratoren für den Aggregatbetrieb
T7	Schalt- und Steuereinrichtungen für den Aggregatbetrieb
T8	Betriebsverhalten im Aggregatbetrieb, Begriffe
T9	Abnahmeprüfung
T10	Stromerzeugungsaggregate kleiner Leistung, Anforderungen und Prüfung
T11	Messung und Beurteilung mechanischer Schwingungen an Stromerzeugungsaggregaten mit Hubkolben-Verbrennungsmotor
T12	Stromerzeugungsaggregate – unterbrechungsfreie Stromversorgung – dynamische USV-Anlagen mit und ohne Hubkolben-Verbrennungsmotor
T13	Stromerzeugungsaggregate – Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren für Sicherheitsstromversorgung in Krankenhäusern und in baulichen Anlagen für Menschenansammlungen
T14	Blockheizkraftwerke (BHKW) mit Hubkolben-Verbrennungsmotoren – Grundlagen, Anforderungen, Komponenten und Ausführungen
T15	Blockheizkraftwerke (BHKW) mit Hubkolben-Verbrennungsmotoren – Prüfungen
ISO 8528	Reciprocating internal combustion engine driven alternating current generating sets.
Bundesimmissionsschutzgesetz	
4. BimSchG	Verordnung zur Durchführung des Verordnung über genehmigungspflichtige Anlagen.
9. BimSchG -	Verordnung zur Durchführung des Grundsätze des Genehmigungsverfahrens
TA	Luft Technische Anleitung zur Reinhaltung der Luft
TA	Lärm Technische Anleitung zum Schutz gegen Lärm
DIN / VDE 0107	Starkstromanlagen in Krankenhäusern und medizinisch genutzten Räumen außerhalb von Krankenhäusern
Beiblatt 1	Auszüge aus bau- und arbeitsschutzrechtlichen Regelungen
Beiblatt 2	Interpretation, Erläuterungen
DIN / VDE 0108	Starkstromanlagen und Sicherheitsstromversorgung in baulichen Anlagen für Menschenansammlungen
Beiblatt 1	Baurechtliche Regelungen

Teil 2	Versammlungsstätten
Teil 3	Geschäftshäuser u. Ausstellungsstätten
Teil 4	Hochhäuser
Teil 5	Gaststätten
Teil 6	Geschlossene Großgaragen
Teil 7	Arbeitsstätten
Teil 8	Fliegende Bauten usw. ...
DIN / VDE 0100 Teil 728	Ersatzstromversorgungsanlagen
EVU	Anschlussbedingungen der EVU
VDEW	Richtlinien Notstromaggregate
VDEW	Parallelbetrieb mit dem Niederspannungsnetz
EltBauVO	Elektrobauverordnung
VDS	Vorschriften des Verbandes der Sachversicherer
WHG	Wasserhaushaltsgesetz
Mineralölsteuergesetz	(Betrieb stationärer Anlagen mit Heizöl)
DIN 31051	Instandhaltung

11 Glossar

19“-Schrank	Rack mit cirka 40 HE, Gesamthöhe cirka 2 Meter Einbaubreite 483 mm, Einbauhöhe wird in Höheneinheiten (HE) gemessen, 1 HE = 44,45 mm
CW	Chilled Water; Klimaanlagen mit Kaltwasser
Datencenter	Serverraum und/oder Rechenzentrum
DX	Direct eXpansion; Klimaanlagen mit Kältemittel
Elektroverteilung	auch NSHV (Niederspannungshauptverteilung) oder PDU (Power Distribution Unit)
Emission	von einem Gerät ausgehende, auf die Umwelt einwirkende Einflüsse
EMV	Elektromagnetische Verträglichkeit
EVU	Energieversorgungsunternehmen
Immission	von der Umwelt ausgehende, auf einen bestimmten Ort einwirkende Einflüsse
IT	Information Technology (früher EDV = elektronische Datenverarbeitung)
Modular	Aufbau eines Systems aus mehreren Modulen (Baugruppen)
NEA	Netzersatzanlage (meist als Notstromdiesel)
Parallelbetrieb	zwei oder mehr Einrichtungen, die gemeinsam die Versorgung von angeschlossenen Verbrauchern durchführen
Präzisionsklimaanlage	Klimaanlage, die sowohl die Temperatur als auch die Luftfeuchtigkeit konstant halten kann. Die Parameter der Luft an den Einlassöffnungen der IT-Geräte sollte zwischen 22 und 27°C und zwischen 40 und 60% rF liegen.
Redundant	mehrfach ausgelegt zur Erhöhung der Verfügbarkeit (Fehlertoleranz)
Skalierbar	Schrittweise an den Bedarf anpassbar
USV	Unterbrechungsfreie Stromversorgung

12 Danksagung

Der vorliegende Leitfaden „Betriebssicheres Rechenzentrum“ entstand in Abstimmung mit dem BITKOM Arbeitskreis „ Rechenzentrum & IT-Infrastruktur“.

Wir bedanken uns ganz herzlich bei allen Mitgliedern des Arbeitskreises für die wertvollen Diskussionen und Anregungen sowie besonders für die Mitwirkung von:

- Silvia Bader, (DEKRA Certification GmbH)
- Harald Becker, (Rosenberger-OSI GmbH & Co. OHG)
- Dr. Gerald Berg, (Rosenberger-OSI GmbH & Co. OHG)
- Klaus Clasen, (Notstromtechnik Clasen GmbH)
- Peter Clauss, (Wagner Group GmbH)
- Aykut Güven, (DEKRA Certification GmbH)
- Frank Hauser, (Server Technology International)
- Dieter Henze, Rittal GmbH & Co. KG)
- Dr. Siegbert Hopf, (Masterguard GmbH)
- Knut Krabbes (QMK IT-Security+Quality)
- Stephan Lang, (Weiss Klimatechnik GmbH)
- Helmut Muhm, (Dipl.-Ing. W. Bender GmbH & Co.KG)
- Hans-Jürgen Niethammer, (Tyco Electronics AMP GmbH)
- Torsten Ped, (Notstromtechnik Clasen GmbH)
- Achim Pfleiderer, (Stulz GmbH)
- Thorsten Punke, (Tyco Electronics AMP GmbH)
- Zeynep Sakalli, (euromicron solutions GmbH)
- Michael Schumacher, (APC Deutschland GmbH)
- Karlheinz Volkert, (Orange Business Germany GmbH)
- Peter Wäsch, SCHÄFER Ausstattungs-Systeme GmbH
- Ralph Wölpert, (Rittal GmbH & Co. KG)

An Version 1 vom November 2006 wirkten mit:

- Helmut Göhl (O2 GmbH),
- Dieter Henze (Rittal GmbH & Co. KG),
- Siegbert Hopf (Masterguard GmbH),
- Peter Koch (Knürr AG),
- Knut Krabbes (QMK IT-Security+Quality)
- Matthias Lohmann (TÜV Secure),
- Ingo Lojewski (Emerson Network Power GmbH),
- Achim Pfleiderer (Stulz GmbH),
- Jörg Richter (I.T.E.N.O.S GmbH),
- Harry Schnabel (Harry Schnabel Consult),
- Michael Schumacher (APC Deutschland GmbH),
- Jürgen Strate (IBM Deutschland GmbH),
- Judith Wagener (Bull GmbH),
- Ralph Wölpert (Lampertz GmbH & Co. KG),
- Eckhard Wolf (AEG Power Supply Systems GmbH),
- Sandra Schulz (Giesecke & Devrient GmbH)

Unseren ganz besonderen Dank richten wir an Harry Schnabel, Vorsitzender des BITKOM Arbeitskreises Rechenzentrum & IT-Infrastruktur.

Informationen zu den Themen, Aktivitäten und Mitgliedern des Arbeitskreises erhalten Sie im Internet unter:
www.bitkom.org/de/wir_ueber_uns/30562.aspx

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.300 Unternehmen, davon 950 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org