Betriebssicheres Rechenzentrum

Leitfaden

Version Dezember 2013

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:	Christian Herzog Tel.: 030.27576-270 c.herzog@bitkom.org
Copyright:	BITKOM 2013
Redaktion:	Holger Skurk (BITKOM)
Grafik/Layout:	Design Bureau kokliko/ Christine Holzmann /Astrid Scheibe (BITKOM)
Titelbild:	Alejandro Mendoza, istockphoto.com

Betriebssicheres Rechenzentrum

Leitfaden

Version Dezember 2013

BITKOM

Inhaltsverzeichnis

1 Einleitung 7

2 Verfügbarkeit eines Rechenzentrums 8

3 Einfluss von Sicherheitsstandards auf die Gestaltung von Rechenzentren 11
- 3.1 ISO 27001 / ISO 27002:2008 11
- 3.2 ITIL 12
- 3.3 Sarbanes Oxley Act und SAS 70 12
- 3.4 Bewertung der Standards 13

4 Basis der IT-Infrastruktur: Das Rack 14
- 4.1 Serverschrank 14
  - 4.1.1 Standard-Serverschrank (Rack) 14
  - 4.1.2 Sicherer Serverschrank 15
  - 4.1.3 Inventarisierung im Serverschrank 16
- 4.2 Netzwerktechnik 16
- 4.3 Betriebssicheres Rechenzentrum 17

5 Energieversorgung 18
- 5.1 Energieversorgungsunternehmen (EVU) – Stromverteilung und Einspeisung ins Unternehmen 18
  - 5.1.1 Ausgangssituation 18
  - 5.1.2 Funktionsweise der Infrastruktur 18
  - 5.1.3 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten 19
- 5.2 Stromverteilung im Unternehmen 20
  - 5.2.1 Ausgangssituation 20
  - 5.2.2 Funktionsweise der Infrastruktur 20
  - 5.2.3 Intelligente Steckdosenleisten 21
  - 5.2.4 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten 21
  - 5.2.5 Schutzmaßnahmen und Hochverfügbarkeit 21
- 5.3 Unterbrechungsfreie Stromversorgung (USV) 23
  - 5.3.1 Ausgangssituation 23
  - 5.3.2 Technologien von USV-Systemen 23
  - 5.3.3 Funktionsweise 24
  - 5.3.4 Grundsätzlicher Aufbau statischer USV-Anlagen 25
  - 5.3.5 USV-Redundanz 26
  - 5.3.6 Elektronischer Bypass / Handbypass- Serviceumgehung 26
  - 5.3.7 Energiespeicher 27
  - 5.3.8 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten 27
  - 5.3.9 Besonderheiten 28

5.4 Notstrom 29
5.4.1 Stromerzeugungsaggregate für die Ersatzstromversorgung (Notstrom) bei Netzausfall 29
5.4.2 Notstromversorgungen 30
5.4.3 Auslegung der Notstromanlage 30
5.4.4 Empfohlene Notstromversorgung in Abhängigkeit zu den zulässigen Ausfallzeiten 31
5.5 Wartung/Instandhaltung 35
5.5.1 Wartung/Service USV-Anlagen 35
5.5.2 Wartung/Service/Probeläufe Netzersatzanlage 35
5.5.3 Wartung/Prüfung Elektroinstallation 35

6 Klimatisierung 36
6.1 Anforderungen 36
6.1.1 Einhaltung von ITK-Betriebsbedingungen 36
6.1.2 Einzusetzende Klimatechnik 36
6.1.3 Redundanz 37
6.1.4 Energieeffizienz 37
6.1.5 Skalierbarkeit 37
6.1.6 Servicekonzept 37
6.2 Umluftklimatisierung 38
6.2.1 Raumkühlung 38
6.2.2 Reihenkühlung 39
6.2.3 Schrankkühlung 40
6.3 Kälteerzeugung 40
6.3.1 Indirekte Freie Kühlung 41
6.3.2 Direkte Freie Kühlung 42
6.3.3 Klimatisierungssysteme ohne Freie Kühlung 42
6.3.4 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten 43
6.4 Fazit 43

7 Brandschutz 44
7.1 Technischer Brandschutz 44
7.1.1 Funktionsweise der Infrastruktur 44
7.1.2 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten 46
7.2 Baulicher Brandschutz 47
7.2.1 Schutzziele 48
7.2.2 Funktionsweise und Raumanforderungen 48
7.2.3 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten 49
7.3 Vorbeugende und organisatorische Brandschutzmaßnahmen 49

8 Flächenkonzeption und Sicherheitszonen für Rechenzentren 51

9 Verkabelung 53
9.1 Ausgangssituation 53
9.2 Normative Grundlagen 53
9.3 Qualität/Komponenten-/Systemauswahl 53
9.4 Struktur 54
9.5 Redundanz und Sicherheit 55
9.6 Installation 56
9.7 Dokumentation und Beschriftung 57

10 Die Zertifizierung eines betriebssicheren Rechenzentrums 57
10.1 Einführung 58
10.2 Zertifizierungsmöglichkeiten für Rechenzentren 58
10.3 Der Zertifizierungsprozess 59
10.4 Die Vorteile einer Zertifizierung 60
10.5 Die Wahl des richtigen Zertifizierungspartners 60

11 Anhang 61

12 Glossar 63

13 Danksagung 64

Verzeichnis der Abbildungen

Abbildung 1: Häufigkeit von Netzstörungen bezogen auf deren durchschnittliche Dauer 23
Abbildung 2: Redundanzen beim Einsatz von USV-Lösungen 26
Abbildung 3: Netzersatzanlage im Gebäude 33
Abbildung 4: Netzersatzanlage im Container 33
Abbildung 5: Netzüberwachung / Netzumschaltung 34
Abbildung 6: Raumklimatisierung über den Doppelboden mit Kaltgang-/Warmgangbildung 38
Abbildung 7: Raumklimatisierung über den Doppelboden und Einhausung der Kaltgänge 39
Abbildung 8: Klimatisierung mit Klimageräten in den Rackreihen Warmgangeinhausung/Kaltgangeinhausung 40
Abbildung 9: Schrankkühlung mit wassergekühltem Rack 40
Abbildung 10: Indirekte Freie Kühlung 41
Abbildung 11: Direkte Freie Kühlung 41
Abbildung 12: Sicherzeitszonen im Rechenzentrum 52
Abbildung 13: Schematische EN Verkabelungsstruktur nach DIN EN 50173-5 54
Abbildung 14: Bereichsverteilungsverkabelung (Cu und LWLmit Bereichsverteiler (BV) und Server-/Strorageschränken mit Geräteanschluss (GA) 55
Abbildung 15: Hauptverteilungsverkabelung (LWL) mit Hauptverteiler (HV) und Anschluss an die Bereichsverteilungsverkabelung (Cu und LWL) mit Bereichsverteiler (BV) und Server-/Storageschränken mit Geräteanschluss (GA) 55

Verzeichnis der Tabellen

Tabelle 1: Historisches Beispiel für Verfügbarkeitsklassen 8
Tabelle 2: Verfügbarkeitsklassen nach BSI 9
Tabelle 3: EVU Einspeisung 19
Tabelle 4: Übersicht der Leistungsklassen 20
Tabelle 5: Verteilung 22
Tabelle 6: Arten von Netzstörungen und die passenden USV-Lösungen nach EN62040-3 24
Tabelle 7: USV 28
Tabelle 8: Notstrom 31
Tabelle 9: Daueremissionsrichtwerte für Emissionsorte außerhalb von Gebäuden 32
Tabelle 10: Klimatisierung 43
Tabelle 11: Technischer Brandschutz 47
Tabelle 12: Baulicher Brandschutz 49
Tabelle 13: Funktionsbereiche eines Rechenzentrums 52

1 Einleitung

Der BITKOM Arbeitskreis »Betriebssicheres Rechenzentrum« hat diesen Leitfaden mit der Intention entwickelt, die Planung, Ausführung und den Betrieb von IT-Infrastrukturen für unternehmenswichtige Anwendungen in Rechenzentren und anderen IT-Umgebungen übersichtlich und kompetent darzustellen. So ist nicht nur die Auswahl von IT-Geräten zu berücksichtigen, auch das Layout und die Ausführung des Rechenzentrums und der daraus resultierenden Anforderungen an:

- Bauart und Baugröße
- elektrische Leistung
- Wärmeabführung
- Verkabelung
- Sicherheit und Verfügbarkeit
- Flexibilität und Energieeffizienz
- Anschaffungs- und Betriebskosten

sind entscheidende Faktoren.

Der vorliegende Leitfaden bietet eine aktuelle Hilfestellung für die Planung und Implementierung eines Rechenzentrums sowie IT-Umgebungen in mittleren und kleinen Unternehmen. 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 selbst auf der BITKOM-Webseite zum kostenfreien Download zur Verfügung steht.

Die Inhalte der Matrix sind in Auszügen auch in den Unterkapiteln des Leitfadens dargestellt.

Der vorliegende Leitfaden und die Planungshilfe ersetzen allerdings keinesfalls eine fachkundige Beratung und Unterstützung durch erfahrende Berater, Fachplaner und Ingenieurbüros.

2 Verfügbarkeit eines Rechenzentrums

Die fortschreitende Entwicklung und Integration der Informationstechnologie in allen Geschäftsbereichen bedeutet, dass sich heutzutage kein noch so kleines 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.

Bei der Erstellung und Erweiterung oder auch Überprüfung eines IT-Konzeptes ist heute von entscheidender Bedeutung, wie die Erforderlichkeit der 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 (Betriebsstätten wie Tankstellen, Chemiekalienlager etc.) Einfluss auf die Wahrscheinlichkeit eines potentiellen Ausfalls haben können. Weiterhin sollten auch potentielle delikti-sche Angriffe von eigenen oder ehemaligen Mitarbeitern des Unternehmens und externer Personen 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

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 Jahre	mehrere Pfade vorhanden, aber nur eine aktiv, redundante Komponenten Wartung ohne Unterbrechung möglich, 99,982 % Verfügbarkeit
Tier IV	1994	mehrere aktive Strom- u. Kaltwasserverteilungspfade, redundante Komponenten fehlertolerant, 99,995 % Verfügbarkeit

Tabelle 1: Historisches Beispiel für Verfügbarkeitsklassen (nach: Uptime Institute, USA), Quelle: US Uptime Institut: Industry Standards Tier Classification

oder der Abschluss 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 dem BSI HV-Kompendium« 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 in Prozent angegeben und berechnet sich als 1 minus das Verhältnis aus fehlerbedingter Stillstandszeit (= Ausfallzeit) und Gesamtzeit eines Systems.

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%	disaster-tolerant	-	Modellierung nach dem HV-Kompendium. IT-Grundschutz dient weiterhin als Basis für die vorstehenden Bereiche sowie die anderen Schutzwerte Integrität und Vertraulichkeit.

Tabelle 2: Verfügbarkeitsklassen nach BSI

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

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

- 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: s. Tabelle 2, S.9.

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.

Auf der Ebene der physischen Infrastruktur eines Rechenzentrums werden die baulichen Aspekte, die technischen Versorgungssysteme (Elektro/Kälte) und die Sicherheitssysteme (Brandmelde- und Brandlöschanlage, Einbruchmeldeanlage, Zutrittskontrollanlage) auf ihre Eignung und ihren ordnungsgemäßen Einsatz hin überprüft. Eine nationale oder internationale Norm gibt es für diesen Themenkomplex noch nicht. Im deutschsprachigen Raum existieren zurzeit Prüfkataloge unterschiedlicher Zertifizierungsstellen mit einer mehr (wie z. B. der TSI Prüfkatalog vom TÜV) oder minder großen Abdeckung von Anforderungen an die physische Infrastruktur.

Die wichtigsten Normen auf der organisatorischen Ebene wie z. B. 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 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 Planungsphase 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 Risikoerkennungmittels 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 Prozessen 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.

Zur schnellen Übersicht, welche Prozesse im Rechenzentrum vorhanden sind und mit welchen Kennzahlen diese überwacht werden könnten, hat der Arbeitskreis einen Leitfaden »Prozesse und KPI in Rechenzentren« entwickelt, der unter www.bitkom.org/rechenzentren zum Download zur Verfügung steht.

3.3 Sarbanes Oxley Act und SAS 70

Der seit Juli 2002 geltende Sarbanes Oxley Act (SOX) ist ein US-Gesetz zur Verbesserung der Transparenz von Unternehmensberichterstattungen und wurde als Folge der Bilanzskandale von Unternehmen wie Enron oder Worldcom erlassen. Das 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. Aber in der Folge auch für Nicht-US Unternehmen, die jedoch eine an einer amerikanischen Börse notierte Mutter- oder Tochtergesellschaft haben.

Im Rahmen des Sarbanes-Oxley Acts müssen Unternehmensprozesse beschrieben, definiert und interne 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 im Bereich von Rechenzentren nachweislich. Bei Öffentlichen Auftraggebern 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 einzelne Rack. Dabei spricht man im Wesentlichen von Serverracks, Netzwerkracks oder Stromversorgungs- und Stromverteilungsracks.

Da die IT-Systeme in den meisten Unternehmen aus (weltweit) genormten 482,6mm (19")[1]-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, Klimatisierung und Monitoring. 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 z.B. gleiche Brandschutz- und weitere Sicherheitsnormen, denn sie sollen die ITK-Systeme und – noch wichtiger – kritische Unternehmensdaten in ihrem Inneren schützen.

4.1 Serverschrank

4.1.1 Standard-Serverschrank (Rack)

Der moderne Serverschrank, kurz Rack genannt, sollte möglichst variabel aufgebaut sein und sich jederzeit durch flexible Modifikationsmöglichkeiten an zukünftige Anforderungen des IT-Equipments anpassen lassen. Der stufenweise Aufbau , der modulare Ausbau, vom Schrank zur Schrankreihe, vom einzelnen Gang zur ganzen Raumarchitektur, sichert den Wert aktueller Investitionen.

Multifunktionaler Innenausbau, hohe Tragkraft, auf das Rack abgestimmte Klimatisierungskonzepte stellen die herausragenden Anforderungen an Schranksysteme und Racks in Einhausungen dar. Bei der Planung von Racks und deren Aufstellung im Rechenzentrum ist eine ausreichende Entwärmung der Komponenten erforderlich. In einem Rack oder einer Rackreihe ist der für die erforderliche Entwärmung entsprechende Luftvolumenstrom und eine ausreichend niedrige Temperatur (als Temperaturdifferenz zur gewünschten maximalen Betriebstemperatur der Komponenten), welche den Betrieb der Komponenten im gewünschten Temperaturbereich ermöglicht, auszulegen. Die Kontrolle und Regelung der Luftfeuchtigkeit innerhalb eines sicheren Bereiches unterhalb der Taupunktgrenze, ist ebenfalls Voraussetzung für einen störungsfreien Betrieb.

Auch auf ein einfach zu integrierendes Stromverteilungs-System sollte 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 selbst, das sowohl aus dem Versorgungsnetz als auch mit einer unterbrechungsfreien Stromversorgung (USV) gespeist werden kann. Moderne Lösungen bringen hier mehr als 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 sind die Anforderungen an das Belüftungskonzept wie perforierte Türen mit über 80% freier Belüftungsfläche und die konsequente Abschottung 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.

1 Aus Gründen des Sprach- und Leseflusses wird das genormte 482,6mm-System im Folgenden 19"-System genannt. Die ebenfalls im Folgenden anzutreffende Bezeichnung Höheneinheit (HE) entspricht einer Höhe von 44,45mm (1,75").

Beides, Stromabsicherung und Klimatisierung, lassen sich durch in die Infrastruktur integrierbare Sensoren überwachen. Diese Fühler registrieren z.B. die Feuchtigkeit, die Temperatur, aber auch die Leistungsaufnahme der Server. Ein modernes, sensorenbasiertes Überwachungssystem übernimmt möglicherweise auch die Zugangssteuerung und weitere Parameter gleich mit.

Entscheidend für das Gelingen eines systemübergreifenden Monitorings auf Racksebene ist die Einbeziehung der Server und der Infrastrukturen in die Überwachung sowie eine einfach zu handhabende Bus-Verkabelung der Sensoren selbst.

Ein wichtiger Punkt bei allen Rack-Lösungen ist das Thema Stabilität. Durch die hohe Packungsdichte moderner Server-Systeme und Speicherlösungen werden je nach Einsatzfall Server-Racks mit bis zu 1.500 kg Tragkraft benötigt. Dementsprechend müssen auch Geräteböden, Gleitschienen und Snap-In Funktionen für hohe Lasten ausgelegt sein. Bis zu 100 kg pro Boden oder 150 kg für spezielle Aufnahmeschienen können hier zum Tragen kommen.

Die Kabelführung von Strom- und Datenkabeln sollte zur Vermeidung von gegenseitiger Beeinflussung getrennt voneinander erfolgen. Dies gilt besonders bei sehr vielen kupferbasierten Kabeln im Schrank.

4.1.2 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 bei der Standortwahl, 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:

- gleich bleibende Temperatur und Luftfeuchtigkeit durch eine Präzisions-Klimatisierung
- ausreichend sichere Stromversorgung durch unterbrechungsfreie Stromversorgung (USV) und gegebenenfalls zusätzlicher, externer Notstromversorgung
- Schutz gegen Fremdzugriff durch zugriffsgeschützte Verschluss-Systeme, netzwerküberwachten Rackzugang, oder gar die biometrische Datenerfassung
- eine ausreichende Brandvorsorge, -detektion und -reaktion
- die Einbindung der Module bzw. der Architektur in ein zentrales Monitoring- und Management-System.

Gegebenenfalls ist der Doppelboden zu verstärken. Ein weiteres wichtiges Thema sind die Möglichkeiten der Kabeleinführung und der internen Kabelführung. Immer größere Datenmengen bei immer schnelleren Netzen in Verbindung mit einer Verkabelung auf Kupferbasis machen empfindlich für Störeinstrahlung. Strom- und Datenleitungen sollten daher möglichst getrennt voneinander in den sicheren Serverschrank eingeführt werden.Bei der Rackauswahl sollte daher unbedingt auf ausreichende Möglichkeiten der Kabelführung geachtet werden.

Soll eine dreiphasige Stromabsicherung zum Einsatz kommen, besteht die Möglichkeit, die Leistungsaufnahme mittels Motorschutzschaltern zu begrenzen, so dass eine tatsächliche Abnahme von theoretischen 88kW pro Rack verhindert wird. Bei einphasiger Stromabsicherung könnte sich eine Leistungsbegrenzung mittels Messgeräten und Schwellwerten einstellen.

Für Ordnung und Übersicht sorgt eine Strukturierung innerhalb der Verkabelung. Eine hohe Flexibilität innerhalb der Kabelführung und die konsequente Einteilung in Funktionsstränge sind hierfür Voraussetzung.

Freiflächen (ungenutze Höheneinheiten) sollten mittels Blechen verschlossen werden, damit die Kaltluft möglichst nur an den zu kühlenden Komponenten vorbeigeführt wird.

4.1.3 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. Eine korrekte Dokumentation ist 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, oder werden als Datenpaket komplett an ein zentrales Managementsystem übergeben.

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 in 19" ausgeführt 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 Umstecken 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 Änderungen 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 zusammenzuarbeiten, die eine langfristige Verfügbarkeit der Produkte sicherstellen können.

5 Energieversorgung

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 Kraftwerken der EVU, die den Strom aus diversen Primärenergieformen erzeugen. Vom Stromerzeuger wird der Strom mittels Leitungen über Hochspannungsmasten zu den Mittelspannungsstationen transportiert. Von den Mittelspannungsstationen wird der Strom oft über Erdkabel bis zu den Transformatorstationen der verschiedenen Mittelspannungsebenen (10, 20 oder 30 kV) geführt. Transformatorstationen befinden sich oft in größeren Gebäuden sowie am Straßenrand auf speziell dafür eingerichteten Grundstücken.

Große Rechenzentren mit mehreren 1.000 Quadratmetern Rechenzentrumsfläche haben vielfach zwei Einspeisungen auf der Mittelspannungsebene, so dass eine volle Redundanz – also die mehrfache Auslegung zur Erhöhung der Verfügbarkeit - sogar bis zu den Kraftwerken besteht.

Beispiele 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.

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 Fehler)

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

Bei der Stromversorgung sind verschiedene Verkehrswege der Leitungsnetze zu beachten. Es gibt so genannte Stich- und Ringleitungen. Es ist darauf zu achten, dass die Anbindung des Gebäudes über eine Ringleitung erfolgt. Diese ist an mind. zwei Mittelspannungsverteilungen angeschlossen, so dass auch bei einem Ausfall einer Seite die Stromversorgung noch gesichert ist. Die Mittelspannung wird in den Trafostationen auf 400 V herunter transformiert und mittels Kabel oder Stromschienen über die Niederspannungshauptverteilung und Normalnetzverteilung ins Rechenzentrum geleitet. Die Normalnetz-Unterverteilung versorgt auch die unterbrechungsfreien Stromversorgungsanlagen (USV) mit Strom.

5.1.3 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten

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.

Die Kategorie A ist 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 Stromversorgern. 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 USV 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 B bietet ein höheres Sicherheitspotential. Hier erfolgt die Stromversorgung bereits ab der Niederspannungshauptverteilung in redundanter Ausführung mit einer zweiten USV. Fällt ein Versorgungsweg hinter der Niederspannungshauptverteilung aus, wird automatisch über den zweiten, redundanten Weg versorgt. Fällt die Mittelspannungseinspeisung aus, ist die Stromversorgung immer noch über die mobile Netzersatzanlage sichergestellt.

RZ Kategorie	EVU Einspeisung			zulässige RZ Ausfallzeit
	Serverschrank	Serverschrank	Rechenzentrum / Serverraum	
	bis zu 7 kW	ab 7 kW bis zu 40 kW	500 bis zu 2500 Watt/qm	
A	Standard			12 h
B	Redundante Einspeisungen			1 h
C	Redundante Einspeisungen			10 min
D	Redundante Einspeisungen von verschiedenen Umspannwerken			< 1 min

Tabelle 3: aus BITKOM-Matrix »Planungshilfe betriebssicheres Rechenzentrum« – EVU Einspeisung

Bei der Kategorie C kommt zusätzlich zur zweiten USV eine zweite USV-Unterverteilung hinzu. Hierdurch ist bereits eine redundante Versorgung von den USV-Anlagen bis zu den Netzgeräten der Server möglich.

Die Kategorie D 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 dazu fast immer die zweite Kabelzuführung von einer anderen Mittelspannungsstation seitens des jeweiligen Energieversorger 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 Instandhaltung, das heißt, 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 Sicherheitsbeleuchtungsanlagen 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 wiederherstellt.

Alle Elektroverteilungen müssen mit einer Eingangsabsicherung 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:

Phasen	Max. Stromstärke	Max. Leistung
1	16 A	3,6 kW
1	32 A	7,2 kW
3	16 A	11 kW
3	32 A	22 kW

Tabelle 4: Übersicht der Leistungsklassen

Übersicht der Leistungsklassen:
(Weitere Kombinationen mit zwei Phasen sind ebenfalls möglich, sind in Deutschland aber nicht gebräuchlich).

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 Leitungsschutzschalter ausgeführt werden. Der typische Aufbau in einem Schrank erfolgt normalerweise durch zwei getrennte Stromleisten, die einen redundanten Betrieb der IT-Systeme ermöglichen.

Moderne Geräte zur Energieverteilung (PDU) verfügen zusätzlich über Mess- oder Schaltfunktionen sowie einen Netzwerkanschluss für ein erweitertes Energiemanagement. Zusätzlich bieten diverse Modelle noch 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 Stromversorgung an die 19"-Schränke herangeführt werden. Elektroverteilungen gibt es als Wandeinbau- und Aufputzversionen sowie als separate Schränke und als in einen 19"-Schrank integrierte Ausführungen. Oft wird die Stromversorgung im Doppelboden geführt, der aber gleichzeitig auch als Kaltluftführung genutzt wird. Die Luftführung kann dann beeinträchtigt und der Zugang zur Stromversorgung erschwert werden. Alternativ können die 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 Rechenzentrum eingesetzten Steckdosenleisten über unterschiedliche, komfortabel austauschbare 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 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

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 von zwei getrennten 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,

RZ Kategorie	Verteilung			zulässige RZ Ausfallzeit
	Serverschrank	Serverschrank	Rechenzentrum / Serverraum	
	bis zu 7 kW	ab 7 kW bis zu 40 kW	500 bis zu 2500 Watt/qm	
A	Standard, Anbindung der Server über USV- und Normalnetz empfehlenswert			12 h
B	Redundante Ausführung (A und B)			1 h
C	Redundante Ausführung (A und B)			10 min
D	Redundante Ausführung (A und B)			< 1 min

Tabelle 5: aus BITKOM-Matrix »Planungshilfe betriebssicheres Rechenzentrum« – Verteilung

zu denen Datenkabel laufen, als TN-S System[2] ausgeführt sein muss. Ein EMV-gerechter Aufbau des Potentialausgleiches ist zwingend erforderlich. Um einen optimalen Potentialausgleich zu erreichen, ist die getrennte Verwendung eines funktionstechnischen PE (FPE) und eines sicherheitstechnischen PE (PE) sinnvoll. Unbedingt nötig für den sicheren Betrieb ist eine permanente Selbstüberwachung eines »sauberen« TN-S Systems (z. B. mit einer Differenzstrom-Überwachung, RCM) 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.

Auch für den Leitungsschutz müssen alle Elektroverteilungen mit einer Eingangsabsicherung 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 S.20, Tabelle 4: Übersicht der Leistungsklassen). 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.

Beim 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 (RCM) erfüllt die aktuelle Schutzmaßnahmennorm und bietet zusätzlich einen erhöhten Brandschutz, auch ohne Abschaltung durch ein RCD.

2 separate Neutralleiter und Schutzleiter vom Transformator bis zu den Verbrauchsmitteln

5.3 Unterbrechungsfreie Stromversorgung (USV)

5.3.1 Ausgangssituation

Nicht nur ein längerer Komplettausfall, sondern 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 und Datenverluste reduziert.

5.3.2 Technologien von USV-Systemen

Für USV- Systeme werden verschiedene Technologien angewendet. Die am häufigsten eingesetzte ist die der statischen 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 wieder-aufladbaren Batterie. Bei Netzausfall wird die Energie des Speichers über einen statischen Umformer (Wechselrichter) am Ausgang der USV-Anlage für die kritischen Verbraucher bereitgestellt. 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.

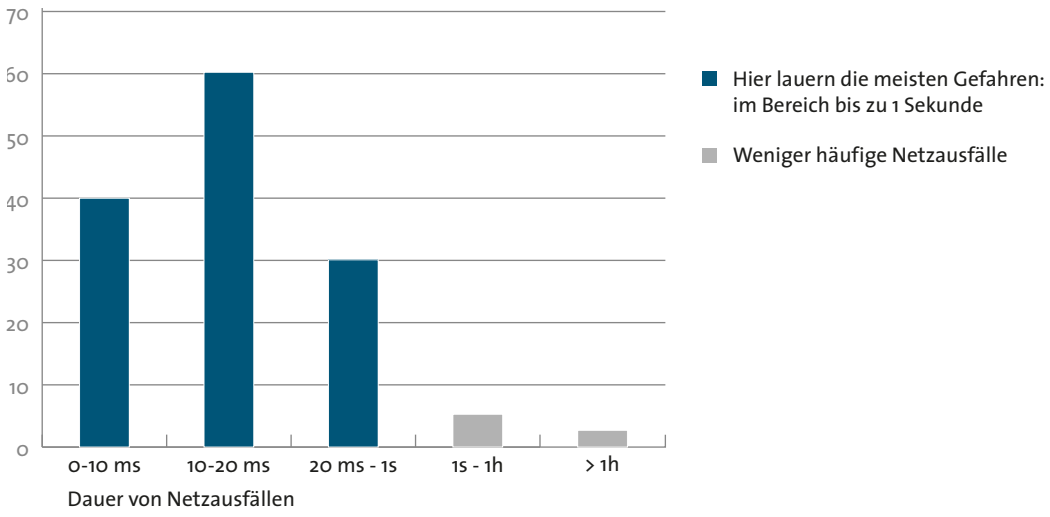

Abbildung 1: Häufigkeit von Netzstörungen bezogen auf deren durchschnittliche Dauer

5.3.3 Funktionsweise

Statische USV-Typen werden in drei Kategorien aufgeteilt. In der europäischen Norm EN62040-3 werden die Klassifizierung und die zugehörigen Bestimmungsmethoden für statische USV-Systeme definiert und beschrieben. Man unterscheidet dabei mehrere Netzstörungsarten (s. Tabelle 6 unten)

Dynamische USV-Anlagen mit und ohne Verbrennungsmotoren 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 parallel schaltbar.

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- Betrieb	-
5. Überspannungen	kontinuierlich			-
6. Spannungsstöße (Surge)	< 4 ms	VFI Voltage + Frequency Independent	Klassifizierung Double Conversion Betrieb (Online) Deltawandler	-
7. Blitzeinwirkungen	sporadisch			Blitz und Über- spannungsschutz IEC 60364-5-534
8. Spannungsverzer- rung (Burst)	periodisch			-
9. Spannungs- oberschwingungen	kontinuierlich			-
10. Frequenzen- schwankungen	sporadisch			-

Tabelle 6: Arten von Netzstörungen und die passenden USV-Lösungen nach EN62040-3 (Ref.: »Unterbrechungsfreie Stromversorgung European Guide«; Hsgr. ZVEI 2004

5.3.4 Grundsätzlicher Aufbau statischer USV-Anlagen

Einzelblockanlagen beinhalten alle für die Funktion der Anlage erforderlichen Komponenten wie

- Gleichrichter
- eigener Batteriezwischenkreis mit Batterie
- Wechselrichter
- elektronischer Bypass
- eventuell Mechanischer Bypass

Diese Anlagen sind als eigenständige Einheit voll funktionsfähig. Die Batterie kann bei kleineren Leistungen und kurzen Überbrückungszeiten in der Anlage integriert sein und bei größeren Leistungen und längerer Überbrückungszeit in externen Batterieschränken oder auf Batteriegestellen untergebracht sein. Die Absicherung der Batterieanlage erfolgt über spezielle DC-Sicherungen oder Leistungsschalter.

Der Leistungsbereich von Einzelblockanlagen reicht von ca. 300 VA bis zu ca. 900 kVA.

Modularblockanlagen beinhalten alle Komponenten einer Einzelblockanlage und zusätzlich eine Schnittstelle zur Kommunikation mit einem Modularblock des gleichen Typs.

Jede dieser Anlagen ist als eigenständige Einheit voll funktionsfähig und entspricht der einer Einzelblockanlage. Durch die Schnittstelle zur Kommunikation können Modularblockanlagen zur Bildung einer Redundanz bzw. zur Leistungserhöhung parallel geschaltet werden. Alle erforderlichen Parameter zum synchronen Betrieb der Wechselrichter und des elektronischen Bypasses werden über diese Schnittstelle zwischen den parallel geschalteten Anlagen ausgetauscht. Je nach Hersteller können bis zu 10 Modularblockanlagen parallel geschaltet werden. Bei der Parallelschaltung von Modularblockanlagen zur Leistungserhöhung ist zwingend ein externer mechanischer Bypass sowie ein Kuppelschalter zur Trennung des gesamten USV-Systems von den Verbrauchern erforderlich.

Der Leistungsbereich von Modularblockanlagen reicht – je nach Hersteller – von ca. 10 kVA bis zu ca. 900 kVA.

Sonderlösungen, wie ein zentraler elektronischer Bypass oder eine Zentralbatterie für mehrere USV-Blöcke, werden nicht mehr betrachtet. Diese Sonderlösungen schränken die Redundanz ein und führen zu einem »Single Point of Failure«.

Einschubmodulare USV-Anlagen beinhalten wie Einzelblockanlagen alle für die Funktion erforderlichen Komponenten (siehe oben). Die Funktion gleicht dem des Modularblocksystems. Die einzelnen aktiven Komponenten (Gleich-, Wechselrichter, elektronischer Bypass, als Einheit oder als separate Module, zum Teil auch Batteriesätze,) sind jedoch in Modulbauweise gefertigt und können nach Bedarf ergänzt werden, ohne vorhandene Installationen ändern zu müssen. Die Systemschränke dieser Anlagen sind bereits vorgerüstet auf einen definierten Endausbau. Alle für die möglichen Erweiterungen erforderlichen Schnittstellen sind bereits vorgerüstet und ohne Umbau nutzbar.

Dementsprechend muss die Installation vor und hinter der USV-Anlage auch auf die Leistung des Endausbaus ausgelegt sein.

In der Praxis gibt es zwei Hauptgründe für den Einsatz dieser Anlagen:

Diese Anlagen werden hauptsächlich eingesetzt, um innerhalb eines Systemschrankes eine N+1 Redundanz zu schaffen. Bei Modularblockanlagen kann, um eine Redundanz zu gewährleisten, ein erheblich größeren Platzbedarf und eine größere Investition erforderlich sein.

Beispiele:

- Verbraucherleistung: 64 kW

- Modulare Anlage: 5 x 16 kW = 64 kW + 16 kW = 1 Anlagenschrank

- Modularblockanlage: 2 x 64 kW = 64 kW + 64 kW = 2 Anlagenschränke

- Modularblockanlage: 3 x 32 kW = 64 kW + 32 kW = 3 Anlagenschränke

Häufig wird im Rechenzentrum/Serverraum mit einer geringen Leistung gestartet. Die projektierte Endleistung wird in der Regel erst Jahre nach der Erstinstallation erreicht. Mit einer einschubmodularen Anlage kann ein günstiger Arbeitspunkt (hoher Wirkungsgrad) durch Anpassung auf die Verbraucherleistung gewährleistet werden, ohne die Installation ändern zu müssen oder in Betrieb befindliche Anlagen abzuschalten. Die höheren Kosten für diese Anlagen werden durch die Energieeinsparung in der Regel nach wenigen Jahren ausgeglichen.

Diese Anlagen sind mit Modulgrößen von ca. 4 kVA bis zu 200 kVA verfügbar und können - je nach eingesetzten Modulen - bis 1600 KVA ausgebaut werden. Auch diese Anlagen können teilweise noch parallel geschaltet werden, was bei den meisten Anwendungsfällen jedoch nicht sinnvoll ist. Mit steigender Anzahl von parallel geschalteten Modulen verringert sich die MTBF.

Je nach Hersteller werden unterschiedliche Philosophien vertreten. Einige Hersteller benutzen für alle USV-Module eine zentrale Batterieanlage, andere haben die Möglichkeit, jedes Modul mit einer eigenen, von den anderen Modulen unabhängigen, Batterieanlage zu betreiben. Bei einer Erweiterung einer Zentralbatterieanlage nach mehreren Jahren kann es auf Grund unterschiedlicher Innenwiderstände zu ungleichmäßigen Ladungen / Entladungen und damit zu verkürzten Überbrückungszeiten sowie zu einer verringerten Gebrauchsdauer kommen. Außerdem stellt eine zentrale Batterieanlage einen »Single Point of Failure« dar.

Auch bei dem elektronischen Bypass setzen einige Hersteller auf einen zentralen elektronischen Bypass für alle Module und andere Hersteller auf einen dezentralen Bypass je USV-Modul. Hier verhält es sich ähnlich wie bei der Zentralbatterie. Die Verfügbarkeit wird durch den »Single Point of Failure« verringert.

5.3.5 USV-Redundanz

Folgende Redundanzen werden beim Einsatz von USV-Anlagen angewendet.

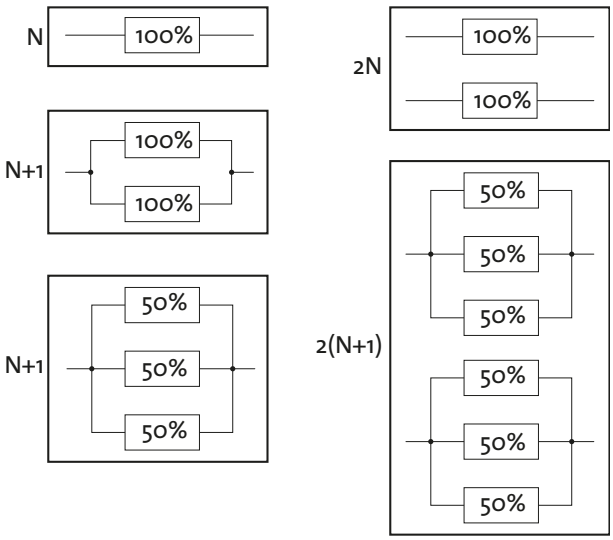

Abbildung 2: Redundanzen beim Einsatz von USV-Lösungen

5.3.6 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.

5.3.7 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 Gebrauchsdauern sind 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.

5.3.8 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 sowie einer 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 Maximalleistungsanforderungen. 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.

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.

5.3.9 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

RZ Kategorie	USV			zulässige RZ Ausfallzeit
	Serverschrank	Serverschrank	Rechenzentrum / Serverraum	
	bis zu 7 kW	ab 7 kW bis zu 40 kW	500 bis zu 2500 Watt/qm	
A	Standard, mind. 10 Minuten Überbrückungszeit (inkl. Ventilation), Minimaldauer abhängig von der kontrollierten Shutdownzeit der Server		Standard, mind. 10 Minuten Überbrückungszeit, Minimaldauer abhängig von der kontrollierten Shutdownzeit der Server	12 h
B	Redundant (N+1), mind. 10 Minuten Überbrückungszeit			1 h
C	Redundant (2N), mind. 10 Minuten Überbrückungszeit			10 min
D	Redundant 2 (N+1), mind. 10 Minuten Überbrückungszeit			< 1 min

Tabelle 7: aus BITKOM-Matrix »Planungshilfe betriebssicheres Rechenzentrum« – 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-practice-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 Standardverträgen schließen die Energieversorgungsunternehmen 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 Unterbrechungsdauer 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 mit einer zu fordernden Lastübernahmezeit im Rechenzentrum zum Einsatz. Die nachfolgenden Ausführungen beziehen sich auf diese Anlagen

5.4.3 Auslegung der Notstromanlage

Für die Auslegung der Aggregatleistung 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 beider 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

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 sichergestellt ist, dass zum entsprechenden Zeitpunkt Leihgeräte überhaupt zur Verfügung stehen.

Raumplanung/Detailplanung für Notstromaggregate

Für die Raumplanung/Detailplanung sind folgende Punkte zu berücksichtigen:

RZ Kategorie	Notstrom			zulässige RZ Ausfallzeit
	Serverschrank	Serverschrank	Rechenzentrum / Serverraum	
	bis zu 7 kW	ab 7 kW bis zu 40 kW	500 bis zu 2500 Watt/qm	
A	optional			12 h
B	Verfügbarkeit in 15 Sekunden, Brennstoffvorrat: 24 Stunden			1 h
C	Redundant, Verfügbarkeit in 15 Sekunden, Brennstoffvorrat: 72 Stunden			10 min
D	Notstromaggregat pro Versorgungspfad, optional redundant, Verfügbarkeit in 15 Sekunden, Brennstoffvorrat mind. 72 Stunden, Betankungsmanagement, optinal Kraftstoffreinigungsanlage			< 1 min

Tabelle 8: aus BITKOM-Matrix »Planungshilfe betriebssicheres Rechenzentrum« - Notstrom

- einzuhaltende Vorschriften (DIN VDE, VDS, WHG, TA Lärm, TA Luft, VAws, TRbF, VDN...)
- grundsätzlicher Aggregataufbau / Aggregatausführung (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 Aggregatraum 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 Emissionsorte 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)

Tabelle 9: Daueremissionsrichtwerte für Emissionsorte außerhalb von Gebäuden

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

Grundsätzlicher Aggregateaufbau/Ausführung

Bei Aggregataufbau /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 Ausführung gibt es Haubenaggregate. Ihr Einsatz erfolgt meistens bei Leistungen von wenigen kVA bis zu einigen hundert kVA. Vorteil liegt in der platzsparenden 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.

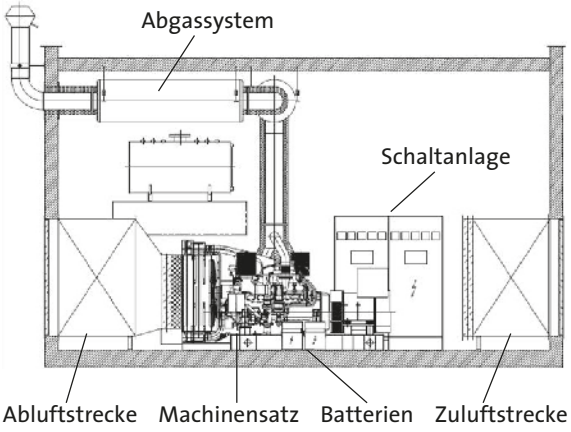

Abbildung 3: Netzersatzanlage im Gebäude

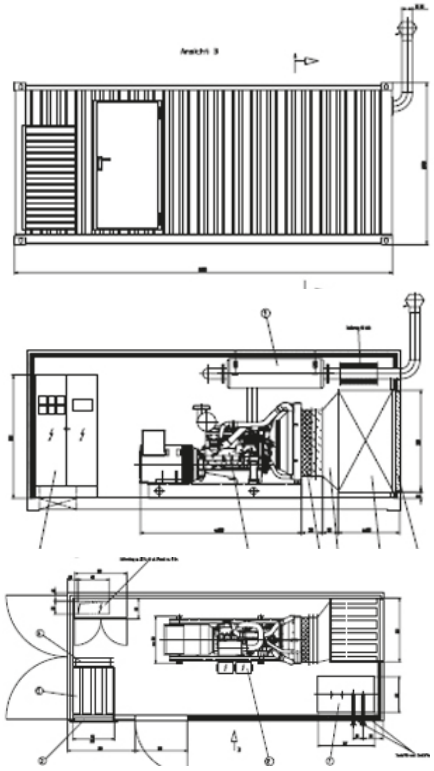

Abbildung 4: Netzersatzanlage im Container

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.

Durch den vermehrten Einsatz von Biokraftstoffen kann es vorkommen, dass Pilze und Mikroorganismen den Kraftstoff in seiner Zusammensetzung verändern und unbrauchbar machen. Ein Totalausfall der Stromversorgung ist nicht unwahrscheinlich. Durch geeignete Kraftstofffiltersysteme können diese Pilze und Mikroorganismen zum größten Teil entfernt werden und es besteht die Möglichkeit, die Qualität des Dieselkraftstoffes über einen längeren Zeitraum stabil zu halten. Positiv auf die Lagerfähigkeit von Kraftstoffen wirkt sich eine gleichmäßig niedrige Temperatur ohne große jahreszeitliche Schwankungen aus, wie sie bei Vorratstankanlagen im Erdreich anzutreffen sind.

Grundsätzlich ist zu beachten, dass nur ein vom Motorhersteller spezifizierter Kraftstoff eingesetzt werden darf. Die meisten Hersteller beziehen sich auf die EN 590. Heizöl erfüllt die Forderung der EN 590 in der Regel nicht.

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.

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.

Auslegung Notstromsteuerung/Schaltanlagen

Jedes Aggregat verfügt mindestens 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:

- 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:

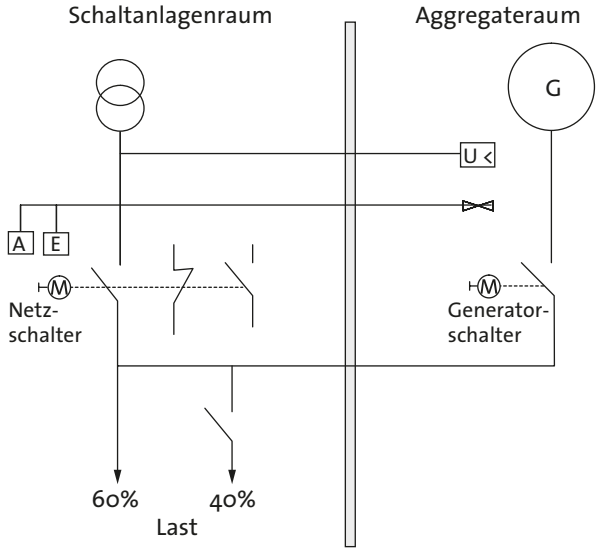

Abbildung 5: Netzüberwachung / Netzumschaltung

5.5 Wartung/Instandhaltung

5.5.1 Wartung/Service USV-Anlagen

Grundvoraussetzung für die Aufrechterhaltung der ordnungsgemäßen Funktion ist die 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. Das 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 deren 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 mindestens 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, der im Notstromfall die zu versorgenden Verbraucher oder das vorhandene Netz mittels Netzparallelbetrieb versorgt. 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 ggf. 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.

6 Klimatisierung

6.1 Anforderungen

Die Klimatisierung von ITK-Systemen ist ein wesentliches Kriterium für deren Verfügbarkeit und Betriebssicherheit. Die steigende Integration und Packungsdichte bei Prozessoren und ITK-Systemen verursacht Abwärmemengen, die noch vor wenigen Jahren auf so begrenztem Raum unvorstellbar waren. Dieser Trend wird sich auch zukünftig weiter fortsetzen.

Nachdem über Jahrzehnte eine Kälteleistung von 1 bis 3 kW pro 19"-Schrank ausreichend war, hat sich im vergangenen Jahrzehnt die Wärmelast pro Rack stark erhöht. Moderne IT-Geräte können in einem 19"-Schrank mit 42 Höheneinheiten über 30 kW elektrische Leistung aufnehmen und somit auch über 30 kW Wärme abgeben. Ein weiterer Anstieg ist durch die weiter steigende Leistungsfähigkeit bei sinkender Baugröße absehbar.

Die wichtigste Anforderung an das Klimasystem ist die Funktion »Kühlen«: Jedes Kilowatt (kW) elektrische Leistung, das von ITK-Geräten aufgenommen wird, wird als Wärme wieder freigesetzt. Diese Wärme muss aus dem ITK Equipment, dem Schrank, dem Raum und dem Gebäude abgeführt werden, um die Betriebstemperaturen konstant zu halten. Da praktisch alle derzeit eingesetzte ITK-Systeme luftgekühlt sind, besteht die Aufgabe darin ausreichende Mengen kalter Luft bereitzustellen und die entsprechenden Mengen erwärmter Luft abzuführen. Weitere Funktionen der Klimasysteme sind »Filtern«, »Nachheizen«, »Befeuchten« und »Entfeuchten« der Luft, um die Anforderungen an die Lufttemperaturen und Luftfeuchtigkeit erfüllen zu können

Im Markt sind unterschiedliche Klimatisierungslösungen, je nach Wärmeleistung des ITK Equipments – also der zu erwartenden Abwärme – verfügbar. Nach Messungen und Erfahrungen aus der Praxis lassen sich bis zu etwa 8 kW Verlustleistung in einem Rack oder Gehäuse noch mit der klassischen Doppelbodenklimatisierung beherrschen, wie sie in fast allen Rechenzentren nach wie vor existiert. Der im klassischen EDV Rechenzentrum eingeführte Doppelboden zeigt sich allerdings den heutigen teils extrem hohen Anforderungen zum Teil nicht mehr gewachsen. Für diese hohen Wärmelasten wurde in den vergangenen Jahren die Doppelbodenklimatisierung optimiert und darüber hinaus verschiedene sogenannte High-Density-Klimalösungen entwickelt.

6.1.1 Einhaltung von ITK-Betriebsbedingungen

Die Anforderungen für die Klimatisierung von EDV-Räumen lagen in der Vergangenheit bei einer Raumtemperatur von ca. 21°C ± 1K und etwa 50% ± 5% relative Feuchte (r.F.). Da heute Racks überwiegend entsprechend dem Kaltgang/Warmgang-Prinzip aufgestellt werden, trifft man heute keine Raumtemperaturanforderungen im herkömmlichen Sinne mehr an. Man spricht daher heute nicht mehr von einer Raumtemperatur, sondern von Zuluft- und Abluftbedingungen.

Die für die Klimatisierung wesentlichen Anforderungen betreffen die Zulufttemperatur, die Ablufttemperatur ist für den sicheren Betrieb der ITK-Systeme nicht relevant. Der empfohlene Bereich für Zuluftbedingungen im Kaltgang ist heute sehr weit gefasst und liegt bei 18 bis 27°C Temperatur sowie einer Feuchte zwischen 5,5°C Taupunkt und max. 60% r.F / 15°C Taupunkt (gem. ASHRAE TC9.9 – 2011). Der kurzfristig erlaubte Bereich ist noch wesentlich weiter gefasst.

6.1.2 Einzusetzende Klimatechnik

Die optimalen Bedingungen im Hinblick auf Temperatur und relative Luftfeuchte lassen sich nur mit Umluftklimageräten, sogenannten Präzisionsklimageräten, erreichen. Nur diese Systeme sind auf durchgehenden 24/7-Betrieb ausgelegt und setzen die eingesetzte Energie effizient ein, d.h. in erster Linie für die Kühlung der Rückluft (Temperaturabsenkung = sensible Kühlung). Eine weitere Anforderung an die Klimatechnik stellt der

ganzjährige Betrieb dar. Die Außeneinheiten müssen die Wärme ganzjährig bei den am Standort zu erwartenden Außentemperaturen abführen. Als Auslegungsparameter ist hier die maximal am Standort zu erwartende Außentemperatur anzusetzen.

Im Gegensatz dazu stehen Komfortklimageräte für Wohn- und Büroräume, wie z.B. Split- oder Multisplitklimageräte, die einen großen Teil der eingesetzten Energie permanent für die Entfeuchtung der Umluft einsetzen (Absenkung der Luftfeuchtigkeit = latente Kühlung). Dadurch kommt es zu kritischen Raumbedingungen, aber auch zu erheblich höheren Betriebskosten. Daher ist ein Einsatz in Rechenzentren und ITK Räumen von Komfortklimageräten nicht wirtschaftlich.

6.1.3 Redundanz

Alle technischen Systeme können ausfallen – auch Klimageräte. Aufgrund der zahlreichen elektromechanischen Komponenten in Klimatisierungssystemen ist daher stets mit einer Ausfallwahrscheinlichkeit zu rechnen. Aus diesem Grund werden je nach Verfügbarkeitsanforderung in den meisten Teilsystemen ein oder mehrere zusätzliche, redundante Geräte installiert als nach Wärmelastaufkommen mindestens notwendig sind. Diese Redundanzgeräte stellen bei Ausfällen die Erzeugung der Kälteleistung sicher und realisieren somit die geforderte Verfügbarkeit. Bei einem Geräteausfall ist die volle Redundanz im Klimasystem nicht mehr vorhanden und korrektive Maßnahmen (Reparaturen) müssen umgehend eingeleitet werden, um die Voraussetzungen für sicheren Betrieb wiederherzustellen.

6.1.4 Energieeffizienz

Vor dem Hintergrund der stark steigenden Energiekosten ist bereits in der Planungsphase der Energieeffizienz des Klimatisierungssystems besondere Bedeutung zuzuordnen. Im Rahmen einer Gesamtkostenbetrachtung ist die Summe aus Investitionskosten für die Neuanlage und die zu erwartenden Betriebs- und Wartungskosten über die gesamte Laufzeit zu ermitteln und zu bewerten. Bei einer Laufzeit des Klimasystems von 10 bis 15 Jahren liegen die Energiekosten, die den wesentlichen Teil der Betriebskosten darstellen, in der Regel über den Investitionskosten und stellen somit das wesentliche Entscheidungskriterium dar.

Um die Energiekosten zu minimieren, sind einige Grundprinzipien zu beachten:

- optimierte Betriebsbedingungen (möglichst hohe Temperaturen für die Zuluft und somit auch für den Kaltwasser-/Kühlwasserkreislauf)
- Nutzung von direkter oder indirekter Freier Kühlung
- energieeffiziente Geräte und Komponenten (Lüfter mit EC-Antrieben, leistungsgeregelte Kompressoren mit hohem COP, ...)
- Dimensionierung und möglichst modulare Ausführung der Teilsysteme (Umluftklima, Kälteerzeugung)
- integrierte Regelung aller Teilsysteme, dynamisch der schwankenden ITK-Last automatisch nachregelnd

Mehrkosten bei der Investition werden sich aufgrund der deutlich reduzierten Betriebskosten in einem kurz- bis mittelfristigen Zeitraum amortisieren.

6.1.5 Skalierbarkeit

In vielen Rechenzentren wird der maximale Endausbau der ITK-Systeme erst nach mehreren Jahren erreicht. Daher muss das Klimatisierungssystem entsprechend skalierbar sein, als mitwachsende Lösung aus modularen Einheiten. Weiterhin müssen die Teilsysteme in einem weiten Bereich der schwankenden ITK-Last möglichst stufenlos nachgeregelt werden können. Ein solches Klimasystem kann dann auch in Teillast mit einem guten Wirkungsgrad und hoher Effizienz betrieben werden.

6.1.6 Servicekonzept

In den Klimatisierungssystemen werden zum einen Verschleißteile, wie z.B. Filtermatten, Dampfzylinder

verwendet 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. Aber auch die einschlägigen Verordnungen zum Betrieb von Kälteanlagen sind zu beachten, da der Gesetzgeber dem Anlagenbetreiber turnusgemäße Dichtigkeitsprüfungen und Anlagenlogbücher verbindlich vorschreibt.

Abhängig vom individuellen Verfügbarkeitsanspruch an die Klimatisierung, gibt es abgestimmte Servicevertragsformen. 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 Antrittszeiten vertraglich zu. Auf diesem Wege kann sichergestellt werden, dass korrektive Maßnahmen umgehend durch Fachpersonal eingeleitet werden und die Verfügbarkeit der Anlage schnellstmöglich wieder vollständig hergestellt wird.

6.2 Umluftklimatisierung

Der überwiegende Teil der heute eingesetzten ITK-Systeme ist luftgekühlt, daher muss die Wärmelast zunächst mit dem Medium Luft abgeführt werden. Dies geschieht klassisch mit Umluftklimageräten auf Raumebene. Bei höheren Wärmelasten reicht allerdings der schlechte Wärmeträger Luft auf Raumebene nicht mehr aus. Dann müssen bessere Trägermedien wie z.B. Wasser oder Kältemittel näher an die Wärmelasten herangeführt werden, d.h. bis in die Schrankreihe oder zum Teil sogar bis in den Schrank. Auf diesem Wege ist gewährleistet, dass die hohen Wärmelasten in nächster Nähe an die Klimasysteme übertragen werden und nicht über lange Luftwege transportiert werden müssen.

6.2.1 Raumkühlung

Die Versorgung mit kalter Zuluft und der Abtransport der warmen Abluft erfolgt über Umluftklimageräte, die i. d. R. an den Stirnseiten der Serverräume (im Raum oder außerhalb in einer Klimaspange) platziert werden. Die Zuluft wird über einen Doppelboden im Raum verteilt und die Abluft meist frei im Raum zu den Umluftklimageräten zurückgeführt. In den Umluftklimageräten findet dann der Wärmeübergang auf ein anderes Trägermedium statt (Kühlwasser oder Kältemittel). In der Regel wird dem ITK-Raum ein kleiner Anteil Außenluft zugeführt, zum Luftaustausch und zur Aufrechterhaltung der Luftqualität.

Die Schränke mit den ITK-Systemen werden dabei inzwischen fast durchgängig in der sogenannten

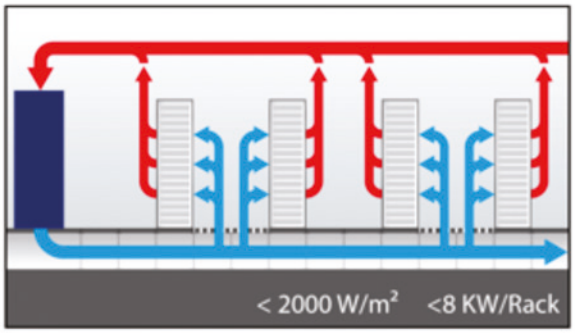

Abbildung 6: Raumklimatisierung über den Doppelboden mit Kaltgang-/Warmgangbildung

Warmgang-Kaltgang-Anordnung aufgestellt, d.h. »Front-to-Front« und »Back-to-Back«. Damit wird verhindert, dass ITK-Systeme in einem Schrank mit warmer Abluft aus einem anderen Schrank versorgt und damit unzureichend klimatisiert werden. Diese Anordnung ist eine wesentliche Voraussetzung für eine effiziente Klimatisierung.

In solchen klassischen Systemen findet allerdings häufig eine mehr oder weniger starke Vermischung von Zu- und Abluft statt. Dadurch erreichen Umluftklimageräte eine Ablufttemperatur, die oft nur wenige Kelvin höher ist als die Zulufttemperatur. Daraus resultieren große Luftvolumenströme für den Abtransport der Wärmelast und die Kühlleistung der Umluftklimageräte wird erheblich reduziert.

Vor einigen Jahren wurden daher Abschottungen (sogenannte Einhausungen) zwischen kalten und warmen Bereichen im Raum eingeführt, die diese Nachteile beheben und einen Luftkurzschluss (Vermischung von Zu- und Abluft) unterbinden.

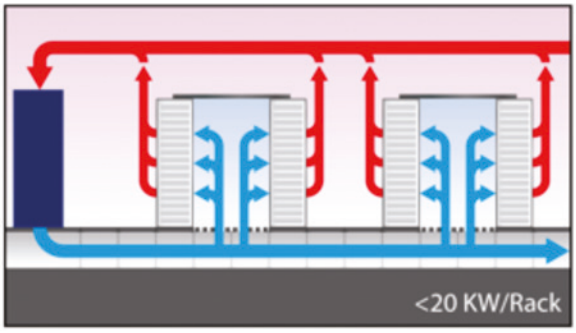

Abbildung 7: Raumklimatisierung über den Doppelboden und Einhausung der Kaltgänge

Diese Abschottungen haben mehrere Vorteile:

- die Temperaturdifferenz zwischen Zu- und Abluft wird stark erhöht, dadurch die Leistungsfähigkeit einer bestehenden Klimatisierungslösung entsprechend verbessert
- die Schränke werden über die gesamte Höhe mit gleicher Zulufttemperatur versorgt, es gibt keine Temperaturschichtung mehr und keine erhöhten Ausfälle von ITK-Systemen in den oberen Schrankbereichen
- die Energieeffizienz der Klimasysteme wird wesentlich verbessert

Eine vollständige Einhausung besteht aus mehreren Komponenten:

- einer vollständigen Abschottung in den Schränken
- einer Einhausung der Gänge, sei es als Kaltgang- oder als Warmgangeinhausung
- einer Abdichtung des Doppelbodens, es sind keine Öffnungen im Warmbereich (Warmgang und unter den Schränken) erlaubt

In dieser Anordnung ist der Luftstrom gewissermaßen gezwungen auf dem Weg vom Doppelboden zurück zum Klimagerät die Wärme aus den ITK Komponenten aufzunehmen.

6.2.2 Reihenkühlung

Sobald eine gewisse Wärmedichte im Raum überschritten wird, reicht Luft als Wärmeträgermedium nicht mehr aus, um den Abtransport auf langen Wegen bis zu den Umluftklimageräten zu bewerkstelligen. Die benötigten Luftmengen lassen sich nicht mehr mit einem vertretbaren technischen Aufwand beherrschen. Die notwendige Doppelbodenhöhe für derart hohe Wärmelasten kann in den meisten ITK Räumen baulich nicht realisiert werden.

Daher werden in diesen Fällen Klimageräte in die Schrankreihen/Rackreihen integriert, entweder für die gesamte Wärmelast dimensioniert oder als zusätzliche Geräte zu bestehenden Umluftgeräten. Der Wärmeübergang von Luft auf Wasser oder Kältemittel findet damit näher an den Wärmelasten statt und daher ist es nicht mehr erforderlich die gesamte Kühlluft durch den Doppelboden zu führen.

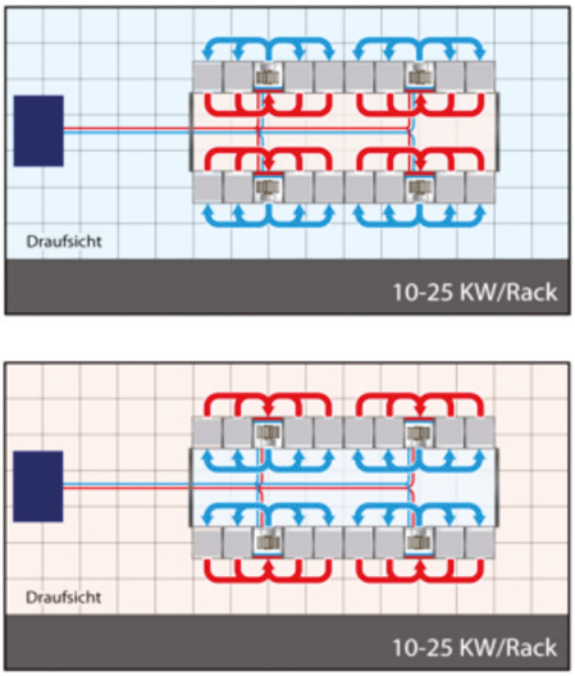

Abbildung 8: Klimatisierung mit Klimageräten in den Rackreihen Warmgangeinhausung/Kaltgangeinhausung

Bei entsprechend ausgeführter Luftführung vor den Serverracks kann die skizzierte Einhausung auch entfallen.

6.2.3 Schrankkühlung

Bei Wärmelasten von mehr als 25 kW pro Rack muss eine direkte Kühlung der Racks vorgenommen werden. Diese direkte Kühlung 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 und mehr 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 dar, auch ohne den Einsatz eines Doppelbodens hohe Wärmelasten sicher abzuführen.

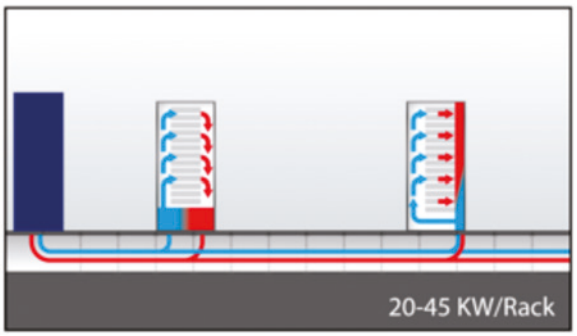

Abbildung 9: Schrankkühlung mit wassergekühltem Rack

6.3 Kälteerzeugung

Umluftklimasysteme unterscheiden sich hinsichtlich Ihres Aufbaus erheblich und das jeweils einzusetzende System muss u.a. den zu erwartenden Wärmelasten, den klimatischen Außenbedingungen und den baulichen Möglichkeiten des ITK Raums Rechnung tragen. In den vorangegangenen Kapiteln ist die zur Verfügungstellung des Luftstroms beschrieben worden, im Weiteren soll nun auf die notwendige Abkühlung des Luftstroms eingegangen werden.

Effiziente Klimatisierungssysteme reduzieren durch den Einsatz der Freien Kühlung die Betriebszeiten der Kälteerzeugung auf ein Minimum und tragen damit erheblich zum energieeffizienten Betrieb der Klimatisierung bei. Die Systeme können in Ausführungen mit Indirekter Freier Kühlung, mit Direkter Freier Kühlung und ohne Freie Kühlung eingeteilt werden.

Indirekte Freie Kühlung

Die Indirekte Freie Kühlung zeichnet sich durch die Trennung der Luftströme im ITK Raum und dem Außenluftvolumenstrom aus. Die Übertragung der Wärmelast erfolgt vom Luftstrom im ITK Raum über das Umluftklimagerät auf einen Wasser/Glykol Wärmeträger, die Wärme wird im außen aufgestellten Rückkühler an die Außenluft übertragen. Die Indirekte Freie Kühlung kommt insbesondere für intolerante Anforderungen an Zulufttemperatur und relativer Zuluftfeuchtigkeit zum Tragen.

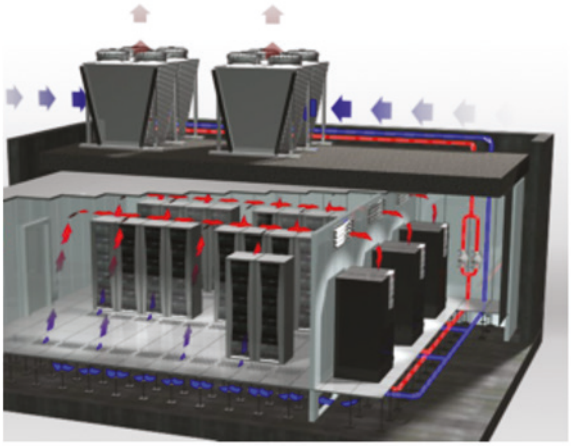

Abbildung 10: Indirekte Freie Kühlung

Direkte Freie Kühlung

Die Direkte Freie Kühlung ist durch die hohen Außenluftvolumenströme in den ITK Raum charakterisiert. Die Wärme wird direkt von der eingeleiteten Außenluft aufgenommen und aus dem ITK Raum abgeführt. Der Wärmeträger Wasser/Glykol ist nicht zwischengeschaltet, daher spricht man bei diesem System von der Direkten Freien Kühlung. Die Direkte Freie Kühlung kommt insbesondere für tolerante Anforderungen an Zulufttemperatur und relativer Zuluftfeuchtigkeit zum Einsatz.

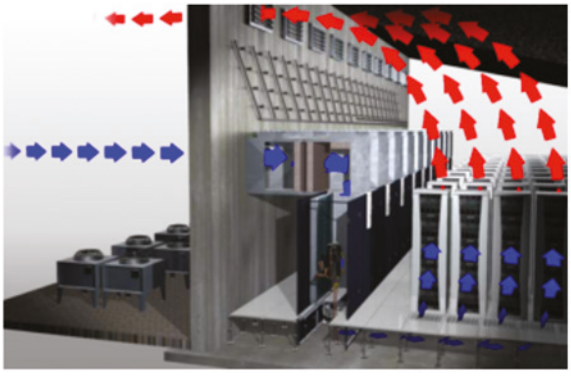

Abbildung 11: Direkte Freie Kühlung

6.3.1 Indirekte Freie Kühlung

Indirekte Freie Kühlung mit Kälteerzeugung in den Umluftklimageräten

Die indirekte freie Kühlung mit Kälteerzeugung in den Umluftklimageräten kommt für Rechenzentren mit einer Wärmelast von bis ca. 500kW zur Anwendung. In den Klimageräten sind Kältekreisläufe verbaut, die bei hohen Außentemperaturen die Kälteerzeugung sicher stellen.

Bei niedrigen Außentemperaturen zirkuliert lediglich ein Wasser/Glykolgemisch zwischen dem Freikühlwärmetauscher im Umluftklimaschrank und dem außen aufgestellten Rückkühlwerk, diese Betriebsweise trägt zu einer erheblichen Betriebsstundenreduzierung der Kälteerzeugung und somit zur Energieeffizienz des Systems bei. Eine höhere Außentemperatur bedingt das Zuschalten des Kältekreislaufes, bei sehr hohen Außentemperaturen wird die energieintensive Kälteerzeugung über Kälteverdichter ausschließlich betrieben.

Mitentscheidend für die Energieeffizienz der Indirekten Freien Kühlung sind die Auslegungsparameter für die Gesamtanlage. Ein höheres zulässiges Temperaturniveau im ITK Raum bedingt längere Betriebszeiten der Freien Kühlung und trägt erheblich zu Energieeffizienz bei. Die Betriebsweise der Freien Kühlung ist über einen möglichst langen Zeitraum sicherzustellen und bis zu einer möglichst hohen Außentemperatur zu realisieren.

Die Kälteerzeugung ist bei diesen Systemen im Umluftklimaschrank integriert und somit im oder in der Nähe des ITK-Raums angeordnet.

Indirekte Freie Kühlung mit Kälteerzeugung über Kaltwassererzeuger

Die Kälteerzeugung ist in 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.

Für die Funktion der Indirekten Freien Kühlung wird auch hier ein zusätzliches Freikühlregister eingesetzt, dies kommt am Kaltwassererzeuger im Außenbereich oder separat als Rückkühler zur Ausführung.

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.

Die weiteren Rahmenbedingungen zur Erzielung der maximalen Energieeffizienz sind unter dem vorangegangenen Punkt 6.3.2.1 beschrieben und gelten auch für die Indirekte Freie Kühlung mit Kälteerzeugung über Kaltwassererzeuger.

Die Kälteerzeugung ist in den i.d.R. außen aufgestellten Kaltwassersätzen integriert. Dieses System findet eher für mittlere bis große ITK Räume Anwendung.

6.3.2 Direkte Freie Kühlung

Die Direkte Freie Kühlung wird seit vielen Jahren für kleinere Telekommunikationseinrichtungen eingesetzt. Die hier verwendeten TK Systeme stellten im Hinblick auf die einzuhaltende Luftfeuchtigkeit keine hohen Anforderungen. Die derzeitigen Toleranzgrenzen für Luftfeuchtigkeit (siehe 6.1.1) ermöglichen den Einsatz der Direkten Freien Kühlung heute auch im Rechenzentrum und somit für größere ITK Räume.

In den Klimageräten sind Kältekreisläufe verbaut, die bei hohen Außentemperaturen die Kälteerzeugung oder bei störenden Umwelteinflüssen die Kälteerzeugung sicherstellen.

Die Außenluft gelangt über eine mehrstufige und großflächig ausgeführte Luftfiltereinheit in den ITK Raum. Die Luft wird vor die ITK Systeme geführt und nimmt die Wärme direkt auf. Die erwärmte Abluft entweicht dem Raum über entsprechende Abluftkanäle. Abhängig von den Entfernungen im Gebäude und den möglichen Luftkanalquerschnitten sind zusätzliche Ventilatoren vorzusehen.

Bei niedrigen Außentemperaturen wird ein Teil der erwärmten Abluft mit der kalten Außenluft gemischt, um die vorgegebenen Zuluftkonditionen einzuhalten. Bei hohen Außentemperaturen schaltet die Anlage in den Umluftbetrieb und die Kälteerzeugung über Kältekreisläufe ist in Funktion.

Die Raumluftfeuchte ist bei diesen Systemen von untergeordneter Rolle und variiert über das Jahr hinweg von ca. min. 15-20 % r.F. bis max. 80-85% r.F. Ein engeres Toleranzfeld für die Feuchte würde zu erheblichen Betriebskosten für die Be- und Entfeuchtung führen.

Auch bei der Direkten Freien Kühlung sind Betriebsbedingungen mitentscheidend für die Energieeffizienz des Systems. Eine möglichst hohe Zulufttemperatur im Kaltgang begünstigt lange Freikühlzeiträume und trägt somit unmittelbar zur Energieeffizienz bei.

6.3.3 Klimatisierungssysteme ohne Freie Kühlung

In Systemen ohne Freikühlungsfunktion ist der Betrieb der energieintensiven Kälteerzeugung über Kältekreisläufe ganzjährig erforderlich. Diese Systeme verursachen deutlich höhere Betriebskosten und kommen insbesondere bei einer Neuanlagenkonzeption nur noch in Ausnahmefällen zum Zuge.

Ferner ist bei kleineren Bestandsanlagen, die in der Vergangenheit teilweise noch mit Komfortklimaanlagen ausgestattet wurden, zu prüfen, ob nicht eine Direkte Freie Kühlung nachgerüstet werden kann.

6.3.4 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten

RZ Kategorie	Klimatisierung			zulässige RZ Ausfallzeit
	Serverschrank	Serverschrank	Rechenzentrum / Serverraum	
	bis zu 7 kW	ab 7 kW bis zu 40 kW	500 bis zu 2500 Watt/qm	
A	Klimatisierung notwendig, Redundanz optional	Klimatisierung notwendig, Redundanz notwendig, USV-Unterstützung	Präzisionskühlung, Redundanz, Kalt-Warmgang-Trennung, ggfs. USV-Unterstützung	12 h
B	Klimatisierung notwendig, Redundanz notwendig	Klimatisierung notwendig, Redundanz notwendig, USV-Unterstützung	Präzisionskühlung, Redundanz, Kalt-Warmgang-Trennung, USV-Unterstützung	1 h
C	Klimatisierung notwendig, Redundanz notwendig, USV-Unterstützung	Klimatisierung notwendig, Redundanz notwendig, USV-Unterstützung	Präzisionskühlung, Geräte und Rohrleitungen redundant, Kalt-Warmgang-Trennung, USV-Unterstützung	10 min
D	Klimatisierung notwendig, komplette Redundanz notwendig, USV-Unterstützung	Klimatisierung notwendig, komplette Redundanz notwendig, USV-Unterstützung	Präzisionskühlung, Geräte und Rohrleitungen redundant, Kalt-Warmgang-Trennung, USV-Unterstützung, Notkühlfunktionen über ein zusätzliches Klimasystem	< 1 min

Tabelle 10: aus BITKOM-Matrix »Planungshilfe betriebssicheres Rechenzentrum« – Klimatisierung

6.4 Fazit

Die technischen Lösungen für eine energieeffiziente und betriebssichere Klimatisierung sind vielfältig und müssen vor dem Hintergrund der ITK Anforderungen, den baulichen Gegebenheiten und wirtschaftlichen Faktoren individuell im Rahmen eines Projektes und einer Fachplanung ausgelotet werden.

Hierin spielen auch die Aspekte der Skalierbarkeit, also des Mitwachsens der Klimasysteme mit den ITK Anforderungen, und die zukünftigen Veränderungen der ITK Systemen eine große Rolle.

Hohe Anforderungen an die Verfügbarkeit der Klimatisierung führen zwangsläufig zu einer aufwendigeren technischen Lösung und zu höheren Investitionskosten, wo hingegen sich höhere Investitionskosten für eine energieeffiziente Klimatisierung auch zukünftig aufgrund der zu erwartenden Energiekostenerhöhung in immer kürzeren Betrachtungszeiträumen amortisieren werden.

7 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 (OVG NRW vom 22.07.2002 - 7 B 508/01) bereits aus dem Jahre 1987 ist auch heute noch nichts hinzuzufügen. Daher ist ein zuverlässiger und wirksamer Brandschutz eine unabdingbare Voraussetzung für den sicheren Betrieb des Rechenzentrums.

Das Löschmittel Wasser allerdings ist im Rechenzentrum in den meisten Fällen fehl am Platz. Die Fachfirmen der Branche bieten heute für jede Bedarfssituation im Rechenzentrum geeignete Brandschutzlösungen an. Bei Neubau oder nachträglicher Absicherung von Rechenzentren ist eine genaue Planung und Auslegung der Anlagen wichtig. Bei Bestandsrechenzentren mit CO_2-Anlagen in bedienten Bereichen sollte umgehend auf alternative, für das Personal sichere, Gaslöschtechnik umgerüstet werden.

7.1 Technischer Brandschutz

Feuer, Rauch und aggressive Rauchgase stellen für Rechenzentren eine latente Gefahr dar. Für die Sicherheit ist eine den Anforderungen entsprechende Branderkennung in Verbindung mit Löschtechnik notwendig. Eine Alternative stellt die Sauerstoffreduzierung (Brandvermeidung) dar.

Ungeeignet für Rechenzentren sind Schaum-, oder Pulverlöschsysteme. Diese bekämpfen zwar erfolgreich einen Brand, zerstören oder schädigen aber gleichzeitig z.B. empfindliche Server oder Netzteile. Unter Umständen wäre dieser Schaden dann höher als der eigentliche Brandschaden. In Rechenzentren sind deshalb automatische Löschanlagen oder Sauerstoffreduzierungsanlagen mit gasförmigen Medien » anerkannter Stand der Technik«.

7.1.1 Funktionsweise der Infrastruktur

Rauchmelder

Für die Branderkennung in Rechenzentren werden hauptsächlich Rauchmelder eingesetzt, die nach dem Streulichtprinzip arbeiten. Die Streuung eines Lichtstrahls an Rauchpartikeln in der optischen Kammer des Rauchmelders 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) Anwendung. Der in früheren Jahren oftmals eingesetzte Ionisationsmelder (I-Melder) ist hingegen fast gänzlich vom europäischen Markt verschwunden.

Ob punktförmige Rauchmelder oder Ansaugrauchmelder (Rauchansaugsystem) besser geeignet sind, hängt vom Einsatzbereich ab. In Bereichen ohne spezielle Detektionsanforderungen, z. B. in Büroräumen, sind in der Regel punktförmige Rauchmelder ausreichend.

In klimatisierten Räumen oder Bereichen mit hohen Decken, erreichen punktförmige Rauchmelder schnell ihre Grenzen. Warmluftpolster oder eine starke Klimaluftströmung verhindert, dass Rauch in ausreichendem Maße schnell genug an die punktförmigen Rauchmelder gelangt. Zur frühzeitigen Branderkennung empfiehlt sich dann die Verwendung von hochsensiblen Ansaugrauchmeldern (Rauchansaugsystemen).

Erfolgt die Ansteuerung der automatischen Löschanlage im Rechenzentrum durch punktförmige Rauchmelder müssen diese zur Vermeidung von Fehlalarmen in sogenannter Zweimelderabhängigkeit installiert werden. Spricht ein punktförmiger Rauchmelder der Raumüberwachung an wird ein interner Alarm ausgelöst und erst wenn zusätzlich ein zweiter punktförmiger Rauchmelder

anspricht erfolgt die Ansteuerung der automatischen Löschanlagen.

Für den Schutz einzelner klimatisierter IT-Einrichtungen innerhalb des Rechenzentrums weist VdS (VdS Schadenverhütung GmbH) darauf hin, dass eine Brandfrüherkennung mit punktförmigen Rauchmeldern mindestens erschwert oder sogar unmöglich ist.

Ein Brand an stromführenden Bauteilen in Schränken kann durch Schmor-, Schwel- und Glimmbrände jederzeit entstehen. Gründe sind z.B. Überlastung von Bauteilen oder defekte Kontakte. Ein Schwelbrand einer Platine führt, wenn er nicht rechtzeitig erkannt wird, zu Verrußung und unter Umständen Korrosion anderer, vom Schwelbrand nicht betroffenen Bauteile. Hinzu kommt, dass in den klimatisierten Schränken die frühzeitige Raucherkennung durch hohe Luftwechselraten der Klimatisierung erschwert ist. Entstehender Rauch wird sofort verdünnt und ist dann von Rauchmeldern in der Entstehungsphase kaum zu detektieren.

Für den Schutz einzelner klimatisierter IT-Einrichtungen innerhalb des Rechenzentrums sind hochsensible Rauchansaugsystemen zuverlässig und bieten die Möglichkeit der frühzeitigen und auf die einzelne IT-Einrichtung begrenzte Maßnahme.

Eine neue Herausforderung für den Brandschutz in Rechenzentren stellen geschlossene Serverschränke dar, die über ein integriertes Kühlsystem verfügen und im Umluftbetrieb arbeiten. Schmor-, Schwel- und Glimmbrände können dann von außen praktisch nicht mehr detektiert werden, da entstehender Rauch nur in sehr kleiner Menge nach außen dringt. Ebenso kann gasförmiges Löschmittel von außen nicht in diese Schränke eindringen.

Für derartige Serverschränke sollten kompakte Branddetektions- und Löschsysteme eingesetzt werden, die z.B. in Form eines 19"-Einschubs integriert werden.

Wie auch bei der Brandfrüherkennung klimatisierter IT-Räume, haben Rauchansaugsysteme zur Überwachung einzelner klimatisierter IT-Einrichtungen Vorteile. Hierbei werden Luftproben z.B. direkt in den IT-Schränken aus dem Luftstrom der Klimatisierung entnommen. Diese Systeme für den integrierten Schutz von IT-Einrichtungen sind heutzutage modular aufgebaut und bieten z.B. Branderkennung und Löschung in einem kompakten 19"-Einschub. Alternativ kann auch eine externe Löscheinheit angesteuert werden.

Löschanlagen

Wirksamkeit und Zuverlässigkeit von Löschanlagen für Rechenzentren werden durch risikogerechte Projektierung und fachgerechte Planung, Ausführung sowie Wartung bestimmt. Löschgase finden bevorzugt Verwendung, denn sie sind elektrisch nicht leitfähig, hinterlassen keine Rückstände und der Betrieb der IT-Einrichtungen kann auch bei ausgelöster Löschanlage aufrecht erhalten werden.

Grundsätzlich muss bei der Planung einer Löschanlage mit gasförmigen Löschmitteln auch eine Raumdruckentlastung berücksichtigt werden, um den entstehenden kurzzeitigen Druckanstieg oder -abfall abzuleiten. Die erforderliche Öffnungsfläche zur Druckentlastung sowie die Raumdichtigkeit im Hinblick auf die Haltezeit der Löschgaskonzentration werden mittels eines Prüfverfahrens (Door-Fan-Prüfmethode) bestimmt. Die minimale Haltezeit der Löschkonzentration sollte mindestens 10 Minuten betragen.

Grundsätzlich werden Gaslöschsysteme für Rechenzentren in Anlagen mit Inertgase und Anlagen mit halogenierten Kohlenwasserstoffen (chemische Löschgase) unterteilt.

Inertgase

Der Löscheffekt der Inertgase beruht auf Reduzierung des Sauerstoffanteils in der Luft.

Die Flutung mit Inertgasen erfolgt innerhalb von 120 Sekunden. Dadurch mischt sich die Raumluft mit dem Inertgas und es entsteht eine sauerstoffarme Atmosphäre. Der Sauerstoffanteil der Raumluft wird dabei so

weit abgesenkt, dass ein Verbrennungsprozess gestoppt wird.

- Argon (Ar)
  Argon gehört zur Gruppe der Edelgase, ist chemisch sehr stabil und geht mit keinem anderen Element eine chemische Verbindung ein. Argon wird kostengünstig aus der Umgebungsluft gewonnen und wird neben der Verwendung als Feuerlöschmittel in vielen anderen technischen Prozessen eingesetzt (z.B. Schutzgas beim Schweißen). Argon ist nicht giftig und schwerer als Luft. Bei einer für die Löschung erforderlichen Argon-Konzentration können Personen durch Sauerstoffmangel gefährdet werden. Deshalb, aber auch wegen der Gefährdung durch Brandgase, werden Räume erst nach Ablauf einer Voralarmzeit mit Argon geflutet, so dass Personen ungefährdet den Bereich verlassen können.

- Stickstoff (N_2)
  Stickstoff ist in der Atmosphäre (mit 78%) enthalten. Es wird wie Argon aus der Umgebungsluft gewonnen und vielfältig verwendet. Es ist ein Inertgas und geht erst bei sehr hohen Temperaturen mit anderen Elementen eine chemische Verbindung ein. Stickstoff ist farb-, geruch- und geschmacklos, nicht giftig und leichter als Luft. Bei einer für die Löschung erforderlichen Stickstoff-Konzentration können Personen durch Sauerstoffmangel gefährdet werden. Deshalb, aber auch wegen der Gefährdung durch Brandgase, werden Räume erst nach Ablauf einer Voralarmzeit mit Stickstoff geflutet, so dass Personen ungefährdet den Bereich verlassen können.

- Chemische Löschgase: HFC227ea, Handelsname z.B. FM-200 und FK-5-1-12, Handelsname Novec 1230
  Die Löschwirkung der chemischen Löschgase beruht auf einer Wärmeabsorption in der Flamme. Vorteil der chemischen Löschgase ist eine hohe Löscheffektivität bei geringer Konzentration. Damit verbunden ist der im Vergleich mit den Inertgasen deutlich geringerer Platzbedarf für die Aufstellung von Löschmittelflaschen. Unter Umständen können die Flaschen, z.B. bei einer Nachrüstung, auch unmittelbar in dem zu schützenden Rechenzentrumsbereich aufgestellt werden. Die Flutungszeit bis zum Erreichen der löschfähigen Konzentration beträgt bei chemischen Gasen nur 10 Sekunden.

Sauerstoffreduzierungsanlagen

Eine Sauerstoffreduzierungsanlage (Brandvermeidungssystem) schafft in einem Rechenzentrum durch Einleiten von Stickstoff eine permanent sauerstoffreduzierte Atmosphäre. Dadurch kann die Entstehung eines offenen Feuers ausgeschlossen werden. Die dauerhafte Sauerstoffreduktion wird durch sehr präzise Steuerungen eines Stickstoffvorrats oder eines Stickstofferzeugers ununterbrochen aufrechterhalten. Bei einem für die Brandvermeidung erforderlichen reduzierten Sauerstoffgehalt bleiben die geschützten Rechenzentrumsbereiche für Personen entsprechend der Information BGI/GUV-I 5162 »Arbeiten in sauerstoffreduzierter Atmosphäre« der Deutschen Gesetzlichen Unfallversicherung begehbar.

7.1.2 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten

Rechenzentren

Liegen die tolerierbaren Ausfallzeiten bei maximal 24 Stunden ist eine sensible Branderkennung im Rechenzentrum ausreichend. Bei höheren Verfügbarkeitsanforderungen an das Rechenzentrum ist zusätzliche eine automatische Löschanlage mit einem gasförmigen Löschmittel oder ein Sauerstoffreduzierungssystem sinnvoll.

Die wesentlichen Merkmale für die Auswahl einer automatischen Löschanlage mit gasförmigen Löschmitteln, einer Sauerstoffreduzierungsanlage oder einer Kombination aus beiden Systemen sind z. B. Anforderungen an die Verfügbarkeit des Rechenzentrums. Je höher der Verfügbarkeitsanspruch umso sinnvoller sind Sauerstoffreduzierungsanlage oder eine innovative Kombination aus Lösch- Sauerstoffreduzierungsanlage.

Bei Löschanlagen mit gasförmigen Löschmitteln, ist aufgrund der bei einer Auslösung entstehenden Überdrücke und ggf. Unterdrücke eine gesicherte Druckentlastung über Druckentlastungskappen erforderlich. 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.

Serverschränke

Eine kompakte, integrierte Einheit mit Branderkennung detektiert eine Brandentstehung bereits in der frühen Phase. Dies schafft einen Zeitvorteil für organisatorische Maßnahmen (z.B. automatische Alarm SMS, Pager etc.) und das Einleiten automatischer Maßnahmen, z.B. «weiches Herunterfahren« der IT-Systeme, Datenauslagerung, selektive Abschaltung oder gezielte Löschung der Netzwerk- und Serverschränke.

Abgeschaltete und stromlose IT-Einheiten gewährleisten im Brandfall die zuverlässigste Alternative gegen ein weiteres Ausbreiten eines Brandes bzw. aggressiver Rauchgase. «Weiches Herunterfahren« bedeutet aber keinesfalls die sofortige Abschaltung der Stromzufuhr. Hierbei wird nach der frühen Branddetektion ein Abschaltmanagement aktiviert, welches die Daten auf nicht geschädigte IT-Einheiten umleitet. Das endgültige Abschalten der Stromzufuhr erfolgt erst nach Abschluss des Datentransfers.

7.2 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

RZ Kategorie	Technischer Brandschutz			zulässige RZ Ausfallzeit
	Serverschrank	Serverschrank	Rechenzentrum / Serverraum	
	bis zu 7 kW	ab 7 kW bis zu 40 kW	500 bis zu 2500 Watt/qm	
A	Überwachungseinheit mit Brandfrüherkennung und Löschtechnik (mit passiver Löschmittelreserve)		Brandmeldeanlage, Überwachungseinheit mit Brandfrüherkennung und eigenständiger Löschtechnik (mit passiver Löschmittelreserve) oder Sauerstoffreduzierungssystem (Brandvermeidungssystem)	12 h
B	Überwachungseinheit mit Brandfrüherkennung und Löschtechnik (mit passiver Löschmittelreserve)		Brandmeldeanlage, Überwachungseinheit mit Brandfrüherkennung und eigenständiger Löschtechnik (mit passiver Löschmittelreserve) oder Sauerstoffreduzierungssystem (Brandvermeidungssystem)	1 h
C	Brandmeldeanlage, Überwachungseinheit mit Brandfrühesterkennung und eigenständiger Löschtechnik (Brandlöschanlage) in redundanter Ausführung oder Sauerstoffreduzierungssystem (Brandvermeidungssystem)			10 min
D	Brandmeldeanlage, Überwachungseinheit mit Brandfrühesterkennung und eigenständiger Löschtechnik (Brandlöschanlage) in redundanter Ausführung oder Sauerstoffreduzierungssystem (Brandvermeidungssystem)			< 1 min

Tabelle 11 aus BITKOM-Matrix »Planungshilfe betriebssicheres Rechenzentrum« – Technischer Brandschutz

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.

7.2.1 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.

7.2.2 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 (z.B. PCV-freie Isolierungen) bildet.

Feuer breitet sich auch schnell und unkontrollierbar über entflammbare (oder gar brennbare) Rohre aus, die an Decken und Wänden geführt sind. Schutz bieten Rohrabschottungen oder feuerfeste Funktionserhaltlösungen als feuerbeständige und rauchgasdichte Barrieren.

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 unbedingt einer europäisch 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. Diese aktuelle Europa-Norm für die bauliche Rechenzentrums-Infrastruktur legt sowohl die Stärke als auch die Zeitdauer von genau definierten Belastungen fest. Der Anwender hat damit über

RZ Kategorie	Baulicher Brandschutz			zulässige RZ Ausfallzeit
	Serverschrank	Serverschrank	Rechenzentrum / Serverraum	
	bis zu 7 kW	ab 7 kW bis zu 40 kW	500 bis zu 2500 Watt/qm	
A	Wände, Böden, Decke, Feuerwiderstandsklasse mind. F90, Schutz gegen Rauchgas und Spritzwasser, mind. T90-Türen, Kabelschotts in gleicher Schutzwertigkeit	Wände, Böden, Decke, Feuerwiderstandsklasse mind. F90, Schutz gegen Rauchgas und Wasser für 30 min, mind. T90-Türen, Kabelschotts in gleicher Schutzwertigkeit		12 h
B	Systemprüfung des baulichen Brandschutzes Wände, Böden, Decke, Türen: nach Europanorm EN 1047-2, Kabelschotts in gleicher Schutzwertigkeit, Schutz gegen Rauchgas und Spritzwasser für 60 min	Systemprüfung des baulichen Brandschutzes Wände, Böden, Decke, Türen: nach Europanorm EN 1047-2, Kabelschotts in gleicher Schutzwertigkeit, Schutz gegen Rauchgas und Spritzwasser für 60 min		1 h
C	Systemprüfung des baulichen Brandschutzes Wände, Böden, Decke, Türen: nach Europanorm EN 1047-2, Kabelschotts in gleicher Schutzwertigkeit, Schutz gegen Rauchgas und Spritzwasser für 60 min	Systemprüfung des baulichen Brandschutzes Wände, Böden, Decke, Türen: nach Europanorm EN 1047-2, Kabelschotts in gleicher Schutzwertigkeit, Schutz gegen Rauchgas und Spritzwasser für 60 min		10 min
D	Systemprüfung des baulichen Brandschutzes Wände, Böden, Decke, Türen: nach Europanorm EN 1047-2, Kabelschotts in gleicher Schutzwertigkeit, Schutz gegen Rauchgas und Spritzwasser für 60 min			< 1 min

Tabelle 12: aus BITKOM-Matrix »Planungshilfe betriebssicheres Rechenzentrum« – Baulicher Brandschutz

das vom VDMA erteilte ECB-S Zertifikat die Sicherheit, dass sein gesamtes System und nicht nur eine einzelne Wand oder die Tür feuerbeständig ist.

7.2.3 Empfohlene Ausstattung bei unterschiedlichen Ausfallzeiten

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

7.3 Vorbeugende und organisatorische Brandschutzmaßnahmen

Der vorbeugende Brandschutz in der Bundesrepublik Deutschland liegt im internationalen Vergleich auf hohem Niveau. Trotz des mittlerweile erreichten Sicherheitsstandards zeigen die Erfahrungen der letzten Jahre, dass das menschliche Verhalten im Brandfall über Eintritt,

Auswirkung und Ausmaß eines Brandes entscheidet (Human Factor).

Vorbeugende und organisatorische Brandschutzmaßnahmen werden häufig vernachlässigt. Dabei können bei richtigen Verhalten der Beteiligten und durch eine optimierte Brandschutzorganisation die Auswirkungen eines Brandes gravierend begrenzt werden.

Wird eine betriebliche Brandschutzorganisation etabliert, ist sie Führungsaufgabe und soll die Motivation der Mitarbeiter fördern, sich aktiv an der Brandverhütung zu beteiligen. Bei dem Aufbau der Brandschutzorganisation müssen den Mitarbeitern die brandschutztechnischen Zusammenhänge aufgezeigt und erklärt werden. Die organisatorischen Regelungen zum Brandschutz sollten in die betrieblichen Abläufe integriert werden. Nur motivierte, informierte und eingebundene Mitarbeiter können einen aktiven Beitrag zur Minimierung des Brandrisikos leisten.

Die organisatorischen Brandschutzmaßnahmen ergänzen bei bestehenden Gebäuden und Anlagen die bereits vorhandenen, vorbeugenden baulichen und anlagentechnischen Brandschutzmaßnahmen.

Bei einem Neubau dient der organisatorische Brandschutz dazu, bereits in der Planungsphase das bauliche und anlagentechnische Schutzkonzept mitzugestalten.

Nachfolgendes sollte bei der Planung und dem Betrieb von Rechenzentren berücksichtigt werden:

- Notfallabschaltplan
- IT-Wiederanlaufplan
- Brandschutzordnung
- Feuerwehrplan
- Brandschutzplan
- Rettungswegeplan, Betriebsanweisungen
- Beschilderung / Kennzeichnung
- Vermeidung unnötiger Brandlasten
- Rauchverbot
- Nahrungsmittelverbot
- Erlaubnisscheine:
  - Feuergefährliche Arbeiten
  - Einweisung von Fremdfirmen
- Werkschutz
- Besucherregelung
- Schulungen

Bei allen Planungen sind nicht nur die aktuellen Gegebenheiten, sondern auch die absehbaren zukünftigen Entwicklungen zu berücksichtigen.

8 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. Entscheidende Rollen 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 in Tabelle 13 auf S. 52 einteilen.

Anordnung der Sicherheitszonen

Stellt man die unterschiedlichen Sicherheitszonen schematisch dar, ergibt sich beispielhaft das in Abbildung 12 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.

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 13: Funktionsbereiche eines Rechenzentrums

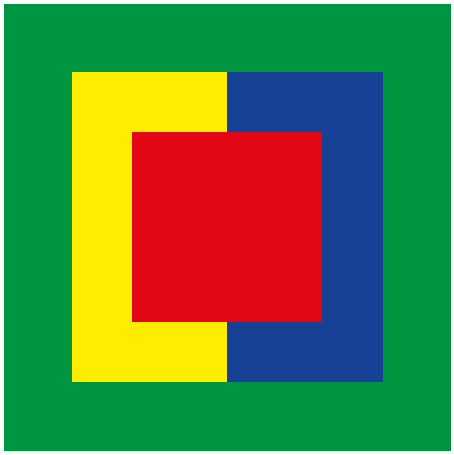

Abbildung 12: Sicherzeitszonen im Rechenzentrum

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.

9 Verkabelung

9.1 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.

Die 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.

9.2 Normative Grundlagen

Eine dem aktuellen Stand der Technik entsprechende Verkabelung nach DIN EN 50173-5 (VDE 0800-173-5) ist durch die Forderung nach bzw. die Festschreibung einer strukturierten, anwendungsneutralen IT-Verkabelung charakterisiert. Diese Norm spricht 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 (VDE 0800-174) beschrieben. Wesentliche Inhalte sind z.B. der Qualitätsplan, Sicherheitsabstände, die Abstände von Kupfer-IT-Verkabelungen zu anderen elektrischen Quellen zur Vermeidung von elektromagnetischen Störungen sowie die Dokumentation und Abnahme des gesamten Rechenzentrums. Für den Potentialausgleich in Gebäuden mit informationstechnischen Anlagen ist DIN EN 50310 (VDE 0800-2-310) einzuhalten.

9.3 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 bei

- Kabeldesign bei Kupfer und LWL
- Bandbreiten bei Kupfersystemen und LWL-Kabeln
- 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 DIN EN 50173-5 (VDE 0800-173-5) wird mindestens eine Kupferverkabelung der Klasse EA 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.

9.4 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.

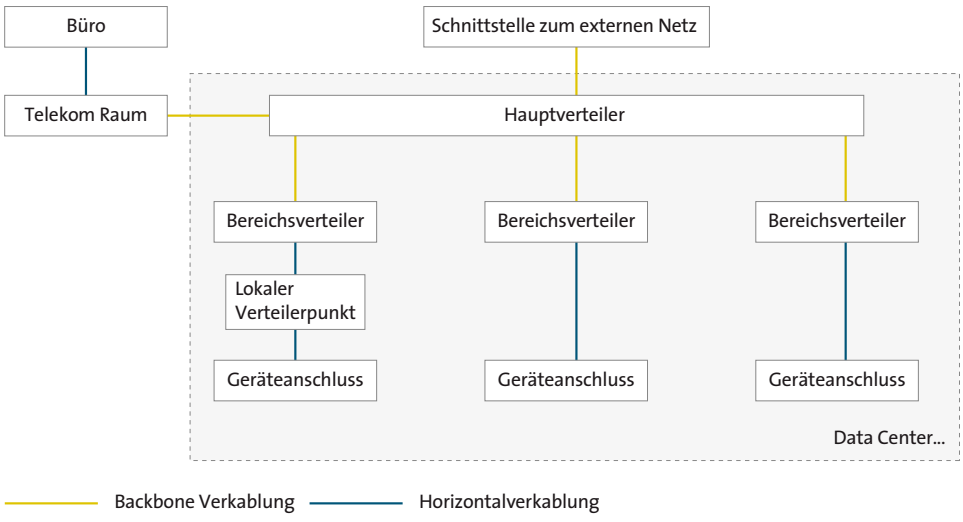

Abbildung 13: Schematische EN Verkabelungsstruktur nach DIN EN 50173-5

In DIN EN 50173-5 (VDE 0800-173-5) [bzw. ISO/IEC 24764] wird diese festinstallierte Geräteverkabelung in die Segmente Bereichs-Hauptverteilungs- und Bereichsverteilungsverkabelung, an deren Ende die GA (Geräteanschluss) genannte Schnittstelle liegt, aufgeteilt. Die aktiven Geräte werden durch möglichst kurze, gerätespezifische Anschlusskabel über die GA-Schnittstelle an die dadurch »geräteneutrale« Bereichsverteilungsverkabelung 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 Bereichsverteilungsverkabelung eingreifen oder diese rückbauen zu müssen.

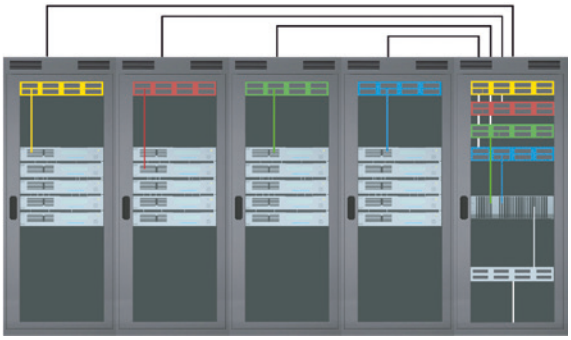

Abbildung 14: Bereichsverteilungsverkabelung (Cu und LWLmit Bereichsverteiler (BV) und Server-/Strorageschränken mit Geräteanschluss (GA)

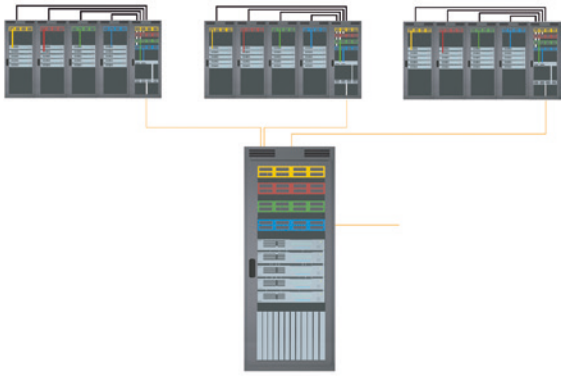

Abbildung 15: Hauptverteilungsverkabelung (LWL) mit Hauptverteiler (HV) und Anschluss an die Bereichsverteilungsverkabelung (Cu und LWL) mit Bereichsverteiler (BV) und Server-/Storageschränken mit Geräteanschluss (GA)

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 Bereichsverteilungsverkabelung sollte, wo erforderlich, in Kupfer und LWL ausgeführt werden, damit verschiedene Geräte angeschlossen werden können. Die Hauptverteilungsverkabelung 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 50173-5 (bzw. ISO/IEC 24764) benennen entsprechende Stecksysteme.

9.5 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-Verkabelungsplattform 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 fiber«), oder eigene LWL-Kabelstrecken von immenser Wichtigkeit für die Betriebssicherheit und Verfügbarkeit und ist wie die rechenzentrumsinterne IT-Verkabelung redundant auszulegen.

9.6 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 »4.1.2 Sicherer Serverschrank« ist aus Verkabelungssicht zu empfehlen, mind. 800 mm breite Schranksysteme einzusetzen. Sie ermöglichen die Installation eines gesamtheitlichen Kabelmanagements in vertikaler und horizontaler Ausrichtung. Die Schranktiefe ergibt sich in der Regel durch die zu installierenden passiven und aktiven 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. DIN EN 50174-2 (VDE 0800-174-2) enthält hierzu detaillierte Anforderungen und Empfehlungen.

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.

9.7 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. Wesentliche Anforderungen an die sogen. Systemverwaltung und Dokumentation nennt DIN EN 50174-1 (VDE 0800-174-1). 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.

10 Die Zertifizierung eines betriebssicheren Rechenzentrums

10.1 Einführung

Das betriebssichere Rechenzentrum vereint auf der Infrastrukturebene unterschiedliche Ingenieursdisziplinen, wie z. B. Elektrotechnik, Mechanik, Bauingenieurwesen, Brandschutz, Sicherheitstechnik, etc. Auf der Ebene der IT-Technik kommen nahezu alle Facetten der Informatik zum Einsatz und auf der organisatorischen Ebene finden sich diverse Managementmethoden zur Überwachung und Steuerung der Prozesse.

Bei der Fragestellung der Sicherheit eines Rechenzentrums im Sinne der Verfügbarkeit, Vertraulichkeit und Integrität der Daten, haben sich Zertifizierungsverfahren auf Basis von Normen und Prüfkatalogen auf folgenden drei Bereichen etabliert:

- physische Infrastruktur
- Informationstechnik
- organisatorische Abläufe

Die Zertifizierung ist ein Vorgang, bei dem ein unparteiischer Dritter aufzeigt, dass angemessenes Vertrauen besteht, dass ein Produkt, ein System, eine Dienstleistung oder ein Prozess in Übereinstimmung mit einer bestimmten nationalen und/oder internationalen Norm oder einem normativen Dokument steht. Der Begriff »Norm« wird in der DIN EN 45020 wie folgt beschrieben: Ein Dokument, das mit Konsens erstellt und von einer anerkannten Institution angenommen wurde und das für die allgemeine und wiederkehrende Anwendung, Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt.

Wenn keine Norm existiert, hängt die Akzeptanz des Zertifikats besonders von dem normativen Dokument ab, inwieweit es aus der Feder von Sachverständigen stammt, es einen Konsens anderer Fachgruppen zu den Vorgaben gibt und welche Verbreitung die Vorgaben im Markt haben. Ein weiterer Faktor der Akzeptanz ist der Zertifizierungspartner. Er sollte auf dem Prüfgebiet den Sachverstand aufbieten können, die Zertifizierungsprozesse definiert und zugänglich gemacht haben und eine Akkreditierung als Zertifizierungsstelle aufweisen.

Aufgrund der Komplexität des »Systems Rechenzentrum« gibt es unterschiedliche Ansätze für eine Zertifizierung, die Teilbereiche oder ausgewählte Eigenschaften eines Rechenzentrums prüfen und bestätigen. Zu den unterschiedlichen Normen wird auf den Punkt 3 dieser Broschüre verwiesen.

10.2 Zertifizierungsmöglichkeiten für Rechenzentren

Auf der Ebene der physischen Infrastruktur eines Rechenzentrums werden die baulichen Aspekte, die technischen Versorgungssysteme (Elektro/Kälte) und die Sicherheitssysteme (Brandmelde- und Brandlöschanlage, Einbruchmeldeanlage, Zutrittskontrollanlage) auf ihre Eignung und ihren ordnungsgemäßen Einsatz hin überprüft. Als Industriestandard für die Zertifizierung der Rechenzentrumsinfrastruktur hat sich der speziell darauf abgestimmte TSI-Prüfkatalog vom TÜV etabliert. Die Reihe der Europäischen Normen EN 50600 (teilweise noch in Entwicklung) legt Anforderungen für die technische Infrastruktur von Rechenzentren und der darin betriebenen Anlagen fest. Es wird erwartet, dass der TSI-Katalog in Zukunft diese Anforderungen abdecken wird.

Auf der Ebene der Informationstechnik findet eine Zertifizierung in der Regel im Produktumfeld statt und somit bei den Herstellern von IT-Systemen (Hardware und Software). Hier hat sich seit Ende der 1990er Jahre die ISO15408 – auch bekannt als Common

Criteria – etabliert. Diese internationale Norm definiert umfangreiche Anforderungen an die Sicherheitsfunktionen und –mechanismen und macht Vorgaben an die Untersuchungsmethodik.

Auf der Ebene der organisatorischen Abläufe gibt es eine Reihe von Zertifizierungsmöglichkeiten. Es handelt sich hierbei um die Zertifizierung des Sicherheitsmanagementsystems (ISO27001 - ISMS) oder der Bewertung typischer Rechenzentrumsbetriebsprozesse (ISO20000 – ITIL) oder eine Überprüfung der Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs (BS25999 – Business Continuity). Auch Wirtschaftsprüferorganisationen bieten auf Basis eigener Anforderungskataloge wie z. B. SAS70 oder IDW951 Prüfleistungen an. Das Arbeitsergebnis und die Vorgehensweise haben einen etwas anderen Stellenwert, da kein Zertifikat vergeben wird und in der Regel das Vier-Augen-Prinzip (Prüfinstitution und Zertifizierungsstelle) nicht zur Anwendung kommt.

10.3 Der Zertifizierungsprozess

Ist das Rechenzentrum in Betrieb und sind die technischen Konzepte und/oder die organisatorischen Abläufe und Regelungen dokumentiert und im Unternehmen wirksam eingeführt, kann es durch ein unabhängiges, neutrales und zur Zertifizierung berechtigtes (akkreditiertes) Unternehmen zertifiziert werden. Die Institution prüft zunächst die Dokumentation und danach das System vor Ort. Der Prüfer (Auditor) verfügt über die erforderlichen Qualifikationen und Berufserfahrung. Ein positives Ergebnis führt zu einem Zertifikat, welches in der Regel 2-3 Jahre gültig ist.

Der Ablauf einer Zertifizierung vollzieht sich nach einem festen Muster, wobei es leichte Variationen in Abhängigkeit von dem Prüfprogramm gibt.

Der Wahl der Zertifizierungsstelle 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 Zertifizierungsstelle die erforderliche Dokumentation zur Verfügung zu stellen. Alternativ kann unter Umständen die 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 vorliegen. Es wird ermittelt, ob das Zertifizierungsaudit zum geplanten Termin mit Aussicht auf Erfolg durchgeführt werden kann.

Die Untersuchung im Rahmen des Voraudits beinhaltet eine Sichtung und erste Bewertung der Unterlagen. Grundsätzlich beinhaltet das Voraudit eine stichprobenartige Prüfung und erhebt keinen Anspruch auf Vollständigkeit.

Das Zertifizierungsverfahren

Die Auditoren überprüfen beim Zertifizierungsaudit, ob die dokumentierten technischen Konzepte bzw. die Verfahren und Abläufe den Anforderungen des zugrundeliegenden Regelwerkes erfüllen und ob die technischen Installationen und die im Unternehmen definierten Prozesse und Vereinbarungen mit der Dokumentation übereinstimmen. Das Verfahren ist in der Regel dreistufig, beginnend mit dem Durcharbeiten der bereitgestellten Unterlagen und erster Begutachtung in Bezug auf das Regelwerk, gefolgt von der Überprüfung vor Ort in Form eines Audits und Sichtung der technischen Realisierungen und abschließend mit dem eigentlichen Zertifizierungsprozess, bei dem das in einem Bewertungsbericht festgehaltene Ergebnis der Zertifizierungsstelle vorgelegt wird.

Auf dieser Grundlage entscheidet das Zertifizierungsgremium der Zertifizierungsstelle, ob ein Zertifikat erteilt wird.

Das Überwachungsaudit

Während der Gültigkeitsdauer des Zertifikates können abhängig vom Zertifizierungsverfahren jährliche Überwachungsaudits stattfinden.

Inhalte der Überwachungsaudits ist die stichprobenartige Überprüfung ob:

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

Wurden die Überwachungsaudits erfolgreich abgeschlossen, findet bei den Zertifizierungen nach zwei oder drei Jahren in einem neuen Verfahren die erneute vollständige Überprüfung statt, bzw. bei den TSI-Zertifizierungen im Wesentlichen die Überprüfung von Änderungen seit der letzten Zertifizierung.

Die Rezertifizierung

Bei den Managementsystemen wird nach drei Jahren eine Rezertifizierung vorgenommen. Bei den TSI-Zertifizierungen erfolgt kein Überwachungsaudit, dafür wird eine Rezertifizierung bereits nach zwei Jahren durchgeführt.

10.4 Die Vorteile einer Zertifizierung

Das Zertifikat ist ein neutraler Nachweis über die Einhaltung der Prüfanforderungen (Norm/Industriestandard) und kann folgende Vorteile bieten:

- Neukundengewinnung als Türöffner für neue Märkte
- Stärkung der Wettbewerbsfähigkeit
- Schwachstellen beseitigen (Fehlervermeidung)
- Stärkung des Vertrauens interessierter Parteien in die Wirksamkeit und Effizienz der Organisation
- Verbesserung des Rankings und der Kreditwürdigkeit
- Reduktion des Aufwands für den Nachweis der Qualitätsfähigkeit
- Internationale Anerkennung und Akzeptanz
- Möglichkeiten der Einordnung der Verfügbarkeitseigenschaften eines Rechenzentrums
- Nachweis, ein Rechenzentrum nach Stand der Technik zu betreiben
- Nachweis für überwachende Institutionen

10.5 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.

Unter Umständen kann auch 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 akkreditierten Zertifizierungsstellen auf ähnlich hohem Niveau, da die Zulassung der Auditoren seitens der Zertifizierungsstellen vorgegeben und von dem Akkreditierer überwacht wird. Dennoch sollte beachtet werden, dass je nach Themenfokus (physische Infrastruktur, Informationstechnik, organisatorische Abläufe) unterschiedliche Zertifizierungsverfahren mit unterschiedlicher Prüftiefe zur Anwendung kommen und sich hier auch Unterschiede bei der Auditorenzusammenstellung zeigen.

Daher kann keine allgemeingültige Aussage zum richtigen Zertifizierungspartner gemacht werden. Richtig gewählt ist ein Zertifizierungspartner, wenn er die mit der Zertifizierung verfolgten Ziele bestmöglich unterstützt und den richtigen Anwendungsbereich (physisch, informationstechnisch, organisatorisch) abdeckt. Insofern können auch die Referenzen der Zertifizierungsstelle wie auch ihre Akkreditierung und Anerkennung durch Dritte ein wichtiger Anhaltspunkt sein.

Auf den Internetseiten der Akkreditierer können für bestimmte Normen zugelassene Prüfgesellschaften abgefragt werden, siehe hierzu www.dakks.de.

11 Anhang

Auswahl wichtiger Vorschriften und Regelwerke:

T1	Allgemeine Begriffe
T2	Leistungsauslegung und Leistungsschilder
T3	Betriebsgrenzwerte für das Motor-, Generator- und Aggregatverhalten
T4	Drehzahlregelung 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-Verbrennungs-motoren 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

Bundesimmissionsschutzgesetz:

4.	Verordnung zur Durchführung des BimSchG, Verordnung über genehmigungspflichtige Anlagen
9.	Verordnung zur Durchführung des BimSchG, Grundsätze des Genehmigungsverfahrens
TA	Luft Technische Anleitung zur Reinhaltung der Luft
TA	Lärm Technische Anleitung zum Schutz gegen Lärm
BS ISO 8528-1: 2006-02-10	Titel (deutsch): Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren – Anwendung, Bemessungen und Ausführungen
ISO 8528-2: 2006-02-10	Titel (deutsch): Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren – Motoren
BS ISO 8528-3: 2006-02-10	Titel (deutsch): Wechsel-Stromerzeugungsaggregate mit Antrieb durch Hubkolben-Verbrennungsmotoren-Wechselstrom-Generatoren für Stromerzeugungsaggregate
BS ISO 8528-4: 2006-02-03	Titel (deutsch): Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren – Steuer- und Schalteinrichtungen

BS ISO 8528-5: 2013-04-30	Titel (englisch): Reciprocating internal combustion engine driven alternating current generating sets. Generating sets
BS ISO 8528-6: 2006-02-03	Titel (deutsch): Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren – Prüfverfahren
DIN ISO 8528-7: 1997-11	Titel (deutsch): Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren – Teil 7: Technische Festlegung für Auslegung und Ausführungen (ISO 8528-7:1994)
DIN 6280-13: 1994-12	Titel (deutsch): Stromerzeugungsaggregate - Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren – Teil 13: Für Sicherheitsstromversorgung in Krankenhäusern und in baulichen Anlagen für Menschenansammlungen
DIN EN 50173-5 (VDE 0800-173-5)	Informationstechnik – Anwendungsneutrale Kommunikationskabelanlagen – Teil 5: Rechenzentren
DIN EN 50174-1 (VDE 0800-174-1)	Informationstechnik – Installation von Kommunikationsverkabelung – Teil 1: Installationsspezifikation und Qualitätssicherung, Informationstechnik
DIN EN 50174-2 (VDE 0800-174-2)	Informationstechnik – Installation von Kommunikationsverkabelung – Teil 2: Installationsplanung und Installationspraktiken in Gebäuden
DIN EN 50310 (VDE 0800-2-310)	Anwendung von Maßnahmen für Erdung und Potentialausgleich in Gebäuden mit Einrichtungen der Informationstechnik
DIN EN 50600-1 (VDE 0801-1)	Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 1: Allgemeine Konzepte
E DIN EN 50600-2-1 (VDE 0801-2-1)	Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2: Gebäudekonstruktion
E DIN EN 50600-2-2 (VDE 0801-2-2)	Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren – Teil 2-2: Stromversorgung
DIN VDE 0100-551 (VDE 0551)	Errichten von Niederspannungsanlagen – Teil 5-55: Auswahl und Errichtung elektrischer Betriebsmittel – Andere Betriebsmittel – Abschnitt 551: Niederspannungsstromerzeugungseinrichtungen
DIN VDE 0100-560 (VDE 0560)	Errichten von Niederspannungsanlagen – Teil 5-56: Auswahl und Errichtung elektrischer Betriebsmittel – Einrichtungen für Sicherheitszwecke
DIN VDE 0100-710 (VDE 0710)	Errichten von Niederspannungsanlagen – Anforderungen für Betriebsstätten, Räume und Anlagen besonderer Art – Teil 710: Medizinisch genutzte Räume
DIN VDE 0100-718 (VDE 0718)	Errichten von Niederspannungsanlagen – Anforderungen für Betriebsstätten, Räume und Anlagen besonderer Art – Teil 718: Bauliche Anlagen für Menschenansammlungen
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

12 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 sollten 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

13 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:

- 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
- Joachim Faulhaber
  TÜV Informationstechnik GmbH
- Helmut Göhl
  O2 GmbH
- Christian Leu
  Minimax GmbH & Co. KG
- Matthias Lohmann
  TÜV Secure
- Wilhelm Lorz
  Atos IT-Solutions and Services GmbH
- Helmut Muhm
  Dipl.-Ing. W. Bender GmbH & Co.KG
- Torsten Ped
  Notstromtechnik Clasen GmbH
- Achim Pfleiderer,
  Stulz GmbH
- Dr. Jörg Richter
  I.T.E.N.O.S GmbH
- Harry Schnabel
  Schnabel Consult GmbH
- Christian Schneider
  Siemens AG
- Michael Schumacher
  Schneider Electric GmbH
- Peter Wäsch
  SCHÄFER Ausstattungs-Systeme GmbH
- Thomas H. Wegmann
  DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE
- Manfred Willnecker
  Emerson Network Power Systems EMEA
- Ralph Wölpert
  Rittal GmbH & Co. KG
- Ingo Zimmermann
  AXA

An früheren Versionen wirkten weiterhin mit:

- Silvia Bader
  DEKRA certification GmbH
- Aykut Güven
  DEKRA certification GmbH
- Frank Hauser
  Server Technology International
- Dieter Henze
  Rittal GmbH & Co. KG
- Dr. Siegbert Hopf
  Masterguard GmbH
- Peter Koch
  Emerson Network Power Systems EMEA
- Knut Krabbes
  QMK IT-Security+Quality
- Stephan Lang
  Weiss Klimatechnik GmbH
- Ingo Lojewski
  Emerson Network Power GmbH
- Hans-Jürgen Niethammer
  Tyco Electronics AMP GmbH
- Thorsten Punke
  Tyco Electronics AMP GmbH
- Zeynep Sakalli
  euromicron solutions GmbH
- Dr. Sandra Schulz
  Giesecke & Devrient GmbH
- Jürgen Strate
  IBM Deutschland GmbH
- Karlheinz Volkert
  Orange Business Germany GmbH
- Judith Wagener
  Bull GmbH
- Eckhard Wolf
  AEG Power Supply Systems GmbH

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

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

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 2.000 Unternehmen, davon über 1.200 Direktmitglieder mit etwa 140 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu gehören fast alle Global Player sowie 800 leistungsstarke Mittelständler und zahlreiche gründergeführte, kreative Unternehmen. Mitglieder sind Anbieter von Software und IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien und der Netzwirtschaft. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik 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