

DIE RISIKEN

BEDROHUNGEN FÜR UNTERNEHMENSZENTRALEN



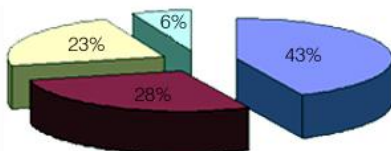
- Feuer
- Diebstahl
- Sabotage
- Feuchtigkeit
- Wassereintritt
- Fremdzutritt
- Staub
- Magnetische Störfelder
- Störungen im Versorgungsnetz
- Überhitzung

Die häufigsten physikalischen Ursachen für den Totalausfall eines Rechenzentrums sind:

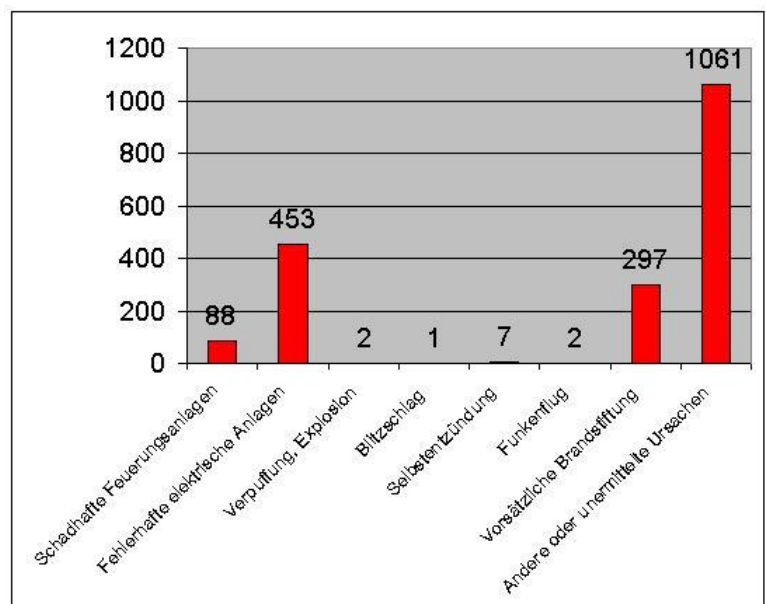
BRAND: KURZSCHLÜSSE (STROMSCHIENEN, ÜBERLASTUNG)
FAHRLÄSSIGKEIT (ZIGARETTE)
SABOTAGE

WASSER SPRINKLERWASSER
ROHRBRUCH
UNWETTER
LÖSCHWASSER NACH BRAND

Wirtschaftliche Auswirkungen von Großbränden



- nehmen den Betrieb nie wieder auf
- sind innerhalb von 3 Jahren aus dem Geschäft
- sind wieder voll betriebsfähig
- fusionieren oder werden verkauft



WISSENSWERTES

Zahlen, Informationen und Fakten, über die sich jeder IT Verantwortliche Gedanken machen sollte.

In einem Rechenzentrum kann man sich weder **Betriebsausfälle**, **Betriebsunterbrechungen**, noch **Hardwaredefekte** und **Datenverluste** leisten. Deshalb müssen sich Betreiber von Rechenzentren Gedanken machen, wie sie ihr Gebäude sichern und drohenden Gefahren standhalten.

Brandschutz in sensiblen EDV-Bereichen ist eine Frage, die sich für immer mehr Unternehmen stellt. Denn Brände haben verheerende Folgen in einem Rechenzentrum: Angefangen bei defekten Geräten, über Systemausfall, (der vermutlich mehrere Tage oder gar Wochen andauert, bis alle Geräte ersetzt und wieder einsatzfähig sind) bis hin zu irreversiblen Datenverlusten. Auf 49% der Firmen hat der Brand eine so große Wirkung, dass sie nicht mehr betriebsfähig sind. 6% davon werden fusioniert oder verkauft. Nur 28% der Firmen können noch drei Jahre nach dem Brand auf dem Markt aktiv sein.

Jeder Server benötigt eine ausreichend dimensionierte **Klimatisierung**, wenn das Rechenzentrum hochverfügbar bleiben soll. Ein richtiges Zusammenspiel zwischen Klimaanlage - Belüftung - Datenrackausführung ist notwendig, um eine sinnvolle Kühlung zu ermöglichen. Am Besten ist dies mit einer überdimensionierten Klimaanlage (die wir meist redundant ausführen) sowie teilweise offenen Serverschränke möglich. Da unsere **Sicherheitszellen** staubdicht sind, ist es möglich alle Serverschränke mit gelochten Türen bzw. Seitenwänden auszustatten und über eine gemeinsame Klimatisierung zu belüften. Lüfter in den Datenschränken entfallen.

Wasser kann aus verschiedenen Gründe in die Räume eines Rechenzentrums eindringen und damit Schäden an den Geräten anrichten:
Eventuell durch Sprinkleranlagen, auch durch **Löschwasser** der Feuerwehr, **Rohrleitungsbruch**, **Hochwasser**, undichte Dächer und **Undichtigkeiten** in Kühlschläuchen.

Die Hardware eines Rechenzentrums ist anfällig für **technische Störungen**. Vor allem die **Stromversorgung** ist ein kritisches Thema. Es können jedoch auch **Hardwareeschäden** sowie Datenverluste aufgrund von elektromagnetischen Feldern entstehen, die die Datenübertragung empfindlich stören. Etwa 30% aller EDV-Schäden der Computer-, Netzwerk-, Industrie- und Automatisierungsanwendungen werden **durch Störungen im Versorgungsnetz** erzeugt. Die meisten durch **Spannungsspitzen, Überspannungen, Unterspannungen** und **Totalausfälle**.

Rechenzentren sind nicht nur Naturgewalten ausgesetzt und durch Hardwarefehler in ihrem Betrieb eingeschränkt. Sie bieten auch eine Angriffsfläche für **Diebstahl, Sabotage** und **Vandalismus**. Es gibt Maßnahmen, wie man nur Zutrittsbefugten Personen Zutritt zum Gebäude gewähren kann. So kann man Diebstahl, Sabotage und Vandalismus ausschließen.

Österreichisches IT-Sicherheitshandbuch

Teil 2: IT-Sicherheitsmaßnahmen

Version 2.0
September 2001

INF 2.2 Raumbelegung unter Berücksichtigung von Brandlasten

Eine Brandlast entsteht durch alle brennbaren Stoffe, die ins Gebäude eingebracht werden. Sie

ist von der Menge und vom Heizwert der Stoffe abhängig. IT-Geräte und Leitungen stellen

ebenso eine Brandlast dar wie Möbel, Fußbodenbeläge, Gardinen und dergleichen. Bei der Unterbringung von IT-Geräten, Datenträgern etc. sollte eine vorherige Beachtung der

vorhandenen Brandlasten im gleichen Raum und in den benachbarten Räumen erfolgen. So

sollte etwa das Datenträgerarchiv nicht in der Nähe von oder über einem Papierlager oder

Räumen mit erhöhter Brandlast untergebracht sein.

INF 3.7 Schutz gegen elektromagnetische Einstrahlung

Die Funktion informationstechnischer Geräte kann durch die elektromagnetische Strahlung

benachbarter Einrichtungen beeinträchtigt werden. Mögliche Ursachen für solche Störstrahlungen

sind Radarstrahlung, Mobilfunk-, Rundfunk- und Fernsehsender, Richtfunkanlagen, Hochspannungsleitungen, Maschinen, von denen elektromagnetische Störungen ausgehen

können (Schweißgeräte, Anlagen mit starken Elektromotoren, usw.) oder atmosphärische Entladungen.

So weit möglich, sollten solche Störquellen bereits bei der Planung berücksichtigt bzw. ausgeschaltet

werden. Als nachträgliche Maßnahmen bleiben etwa:

- die Verwendung von Schutzschranken mit speziellen Filtern und Türdichtungen oder
- die Abschirmung durch beschichtete Wände.

INF 5.2 Geeignete Aufstellung eines Servers

Unter Servern sind in diesem Zusammenhang etwa Datenbank-, Programm- und Kommunikationsserver, aber auch TK-Anlagen zu verstehen.

Um Vertraulichkeit, Integrität und Verfügbarkeit im Betrieb von Servern sicherzustellen, ist

es zwingend erforderlich, diese in einer gesicherten Umgebung aufzustellen.

Diese kann realisiert werden als:

▫ **Serverraum (vgl. INF 5.6 Serverräume):**

Raum zur Unterbringung von Servern, serverspezifischen Unterlagen, Datenträgern in kleinem Umfang sowie weiterer Hardware (etwa Drucker oder Netzwerkkomponenten). Im Serverraum ist im Allgemeinen kein ständig besetzter Arbeitsplatz eingerichtet, er wird

nur sporadisch und zu kurzfristigen Arbeiten betreten.

▫ **Serverschrank, wenn kein separater Serverraum zur Verfügung steht (vgl. INF 5.7 Beschaffung und Einsatz geeigneter Schutzschränke):**

Serverschränke dienen zur Unterbringung von IT-Geräten und sollen den Inhalt sowohl gegen unbefugten Zugriff als auch gegen die Einwirkung von Feuer oder schädigenden Stoffen (Staub, Gase,...) schützen.

Details zu den technischen und organisatorischen Sicherheitsmaßnahmen bei Serverräumen

und Serverschränken finden sich in *INF 5.6 Serverräume* und *INF 5.7 Beschaffung und Einsatz geeigneter Schutzschränke*.

Generell ist zu beachten:

▫ Der Zugang und Zugriff zu Servern darf ausschließlich autorisierten Personen möglich sein.

▫ Eine Vertretungsregelung muss sicherstellen, dass der Zugriff zum Server auch im Vertretungsfall

geregelt möglich ist, und unautorisierte Zugriffe auch in Ausnahmesituationen nicht vorkommen können.

INF 5.3 Geeignete Aufstellung von Netzwerkkomponenten

Netzwerkkomponenten sollten wie Server in einem gesicherten Serverraum oder einem Schutzschrank aufgestellt sein. Die entsprechenden Maßnahmen *INF 5.6 Serverräume* und

INF 5.7 Beschaffung und Einsatz geeigneter Schutzschränke sind zu beachten.

INF 5.6 Serverräume

Ein Serverraum dient zur Unterbringung eines oder mehrerer Server sowie serverspezifischer

Unterlagen. Darüber hinaus können dort auch Datenträger (in kleinerem Umfang) sowie zusätzliche Hardware, wie etwa Protokolldrucker oder Klimatechnik, vorhanden sein.

Im Serverraum ist kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und

zu kurzfristigen Arbeiten betreten. Zu beachten ist jedoch, dass im Serverraum auf Grund der

Konzentration von IT-Geräten und Daten ein deutlich höherer Schaden eintreten kann als beispielsweise

in einem Büroraum.

Für den Schutz von Serverräumen sind die entsprechenden baulichen und infrastrukturellen

Maßnahmen, die im vorliegenden Kapitel 1 beschrieben werden, zur Anwendung zu bringen.

Besondere Beachtung ist dabei folgenden Maßnahmen zu widmen:

- ☐ INF 1.4 Zutrittskontrolle
- ☐ INF 2.2 Raumbelastung unter Berücksichtigung von Brandlasten
- ☐ INF 2.8 Handfeuerlöscher
- ☐ INF 2.11 Rauchverbot
- ☐ INF 3.2 Not-Aus-Schalter
- ☐ INF 3.4 Lokale unterbrechungsfreie Stromversorgung
- ☐ INF 3.6 Überspannungsschutz (Innerer Blitzschutz)
- ☐ INF 4.6 Vermeidung von wasserführenden Leitung
- ☐ INF 6.4 Geschlossene Fenster und Türen
- ☐ INF 6.5 Alarmanlage
- ☐ INF 6.6 Fernanzeige von Störungen
- ☐ INF 6.7 Klimatisierung
- ☐ PER 2.3 Beaufsichtigung oder Begleitung von Fremdpersonen

INF 5.7 Beschaffung und Einsatz geeigneter Schutzschränke

Schutzschränke können ihren Inhalt gegen die Einwirkung von Feuer bzw. gegen unbefugten

Zugriff schützen. Je nach angestrebter Schutzwirkung sind bei der Auswahl geeigneter Schutzschränke folgende Hinweise zu beachten:

· Schutz gegen Feuereinwirkung:

Bei Schutzschränken unterscheidet man bezüglich Schutz gegen Feuereinwirkung die Güteklassen S60 und S120 nach ÖNORM EN 1047-1. In diesen Güteklassen werden die

Schutzschränke darauf geprüft, ob in ihnen bis zu einer Beflammungszeit von 60 bzw. 120

Minuten während eines normierten Testes für die geschützten Datenträger verträgliche Temperaturen erhalten bleiben. Durch Zusätze in der Klassifizierung werden die zu schützenden Datenträger bezeichnet. Die Kürzel bedeuten im Einzelnen:

P = Papier aller Art

D = Datenträger (z.B. Magnetbänder, Filme)

DIS = Disketten, Magnetbandkassetten einschließlich aller anderen Datenträger.
Die Unterschiede zwischen den Klassen liegen in der Isolationsleistung, die bei
DIS-Schränken
am höchsten ist.

Für den IT-Grundschutz sollten bei Schutz gegen Feuer Schutzschränke der Güteklasse
S60 ausreichend sein. Zu beachten bleibt, dass solche Schränke damit Schutz gegen
Feuer
für einen gewissen Zeitraum bieten, so dass Datenträger nicht zerstört werden, jedoch
ist

davon auszugehen, dass im Brandfall der Betrieb eines in einem Serverschrank
untergebrachten Servers nicht aufrechterhalten werden kann.

Bei Schutzschränken, die zum Schutz vor Feuer und Rauch dienen, sollte eine
Vorrichtung

zum automatischen Schließen der Türen im Brandfall vorgesehen werden. Die
Schließung

sollte lokal durch Rauchgasmelder und/oder extern durch ein Signal einer
Brandmeldeanlage

(soweit vorhanden) ausgelöst werden können.