Versicherungsverband Österreich

Schutzmaßnahmen

für

Datenzentren

INHALTSVERZEICHNIS

1 ALLGEMEINES

Datenzentren erfordern wegen dieser Bedeutung für die meisten Unternehmen Maßnahmen der Schadenverhütung, die über die gesetzlichen Anforderungen, wie z.B. die des Baurechts, der Gewerbeordnung, der Arbeitnehmer/innen-Schutzbestimmung etc. hinausgehen.

Die Schutzmaßnahmen gelten sowohl für neu zu errichtende als auch bestehende Anlagen. Die Verantwortung des Betreibers des Datenzentrums bleibt hiervon unberührt. Bei der Abwägung möglicher Gefahren und der daraus erwachsenden Risiken ist unter dem Gesichtspunkt der Wirtschaftlichkeit der mögliche Schaden den Aufwendungen zur Schadenvorsorge und -Verhütung gegenüber zu stellen.

Die Festlegung von Maßnahmen orientiert sich immer am Schutzziel. Dabei ist zu definieren,

- gegen welches Ereignis eine Maßnahme schützen soll,
- in welcher Form eine Maßnahme wirken soll und
- in welchem Maße ein Schaden eintreten darf.

Das Schutzkonzept für Datenzentren hat einen entsprechend hohen Stellenwert. Ein adäquates Maß an Sicherheit kann nur durch ein ganzheitliches Konzept erreicht werden. Dabei ist besonderer Wert auf die sinnvolle Verknüpfung von Schutzmaßnahmen zu legen. Ein wesentlicher Bestandteil dieser Maßnahmen ist der Brandschutz; das Versagen, z.B. der Brandschutzmaßnahmen, kann im Schadenfall katastrophale Auswirkungen haben.

2 ANWENDUNGSBEREICH

Datenzentren im Sinne dieser Schutzmaßnahmen sind Rechenzentren und Serverräume sowie zentrale Anlagen der Mess-, Steuer- und Regeltechnik, der Netzwerktechnik und der Kommunikation. Das Merkblatt bezieht sich dabei sowohl auf die Räume als auch auf die technischen Einrichtungen. Sind auf Grund der örtlichen Gegebenheiten die nachfolgend und in der Muster-Checkliste aufgezeigten Schadenverhütungsmaßnahmen nicht vollständig zu realisieren, so ist eine an die Verhältnisse angepasste Auswahl der Maßnahmen zu treffen.

Von Behörden und entsprechenden Institutionen geforderte Sicherheits- und Schadenverhütungsmaßnahmen bleiben von diesen Schutzmaßnahmen unberührt.

Risiken, die sich im Hinblick auf Datenverarbeitung und Datensicherheit (Viren, Hacker etc.) ergeben, sind nicht Gegenstand dieses Merkblatts.

3 GEFAHREN FÜR DATENZENTREN

Der Betrieb eines Datenzentrums ist unterschiedlichen Gefahren ausgesetzt, die zu Schäden an Maschinen und zu Datenverlusten führen können:

3.1 Brand, Rauch, Explosion
3.2 Naturgefahren, Wasser und sonstige Flüssigkeiten
3.3 Einbruch, Diebstahl, Sabotage, Vandalismus
3.4 Fehlerhafte technische Einrichtungen
3.5 Elektrische Störeinflüsse
3.6 Organisatorische Mängel
3.7 Schutz bei Baumaßnahmen

3.1 Brand, Rauch, Explosion

Brandgefahr besteht überall dort, wo brennbare Stoffe, Sauerstoff und eine Zündquelle zusammentreffen. Da Sauerstoff in allen Bereichen vorhanden ist, sind zur Einschätzung des Risikos vor allem das Vorhandensein und die Menge brennbarer Stoffe (Brandlast) sowie potenzielle Zündquellen von Bedeutung. Unnötige Brandlasten in den Aufstellbereichen von Datenzentren begünstigen oft eine schnelle Brandausbreitung. Datenzentren können in mehrere Bereiche eingeteilt werden, die auf Grund der Brandlast bzw. der Brandentstehungsgefahr differenziert zu bewerten sind. Zur Verdeutlichung der Brandgefahren ist eine Übersicht in Tabelle 3.01 wiedergegeben.

	Gefährdung durch	
Bereich	**Brandlast**	**Risikofaktoren/Zündquellen**
Doppelböden Hohlraumestriche	Relativ hohe Brandlast durch: ■ Energie und Datenkabel - nicht mehr benötigte Kabel - Kabel mit brennbaren Isolierungen aus halogenhaltigen Kunststoffen schädigen im Falle der Verbrennung durch korrosive Rauchgase ■ Staubablagerungen	■ fehlerhafte Kontakte, lockere Anschlüsse und Klemmverbindungen ■ Kleintiere (Nager) ■ technische Fehler an Klimaanlagen, Notstromversorgung etc. können zu unzulässiger Erwärmung von Anlagenteilen führen ■ Feuergefährliche Arbeiten
IT-Raum	■ Einrichtungsgegenstände (Möbel etc.) ■ Wandverkleidungen und Dämmmaterialien ■ Verbrauchs- und Verpackungsmaterialien (Papier) ■ Staubablagerungen	■ defekte Geräte ■ Fahrlässigkeiten des Personals ■ Feuergefährliche Arbeiten
Technische Einrichtungen (IT-Geräte, Netzverteiler, Klimaschränke, etc.)	■ Kunststoffe ■ Altgeräte ■ Ersatzteile ■ Baugruppen	■ defekte Bauteile ■ überlastete Netzteile ■ fehlende oder falsche Überlastschutzeinrichtungen ■ nicht IT-gerecht ausgeführte Elektroinstallationen ■ Wärmestau
Tabelle 3.01: Beispiele für Brandgefahren		

3.2 Naturgefahren, Wasser und sonstige Flüssigkeiten

Naturgefahren wie Sturm, Hagel, Starkregen, (Hochwasser), Rückstau, Schneedruck, Erdbeben können sowohl direkt als auch indirekt auf die Datenzentren einwirken.

Gefahr von Wasserschäden besteht weiters im Zusammenhang mit

- wasserführenden Leitungen für Versorgung, Entsorgung und Heizung,
- Grundwasser,
- Oberflächenwasser,
- Löschwasser.

Auch ergeben sich Gefahren durch sonstige flüssigkeitsführende Leitungen, wie z.B. Kühlmittelkreisläufe.

Bei Datenzentren muss vor allem in Räumen unter Erdgleiche mit eindringenden Flüssigkeiten, die sich hier sammeln können, gerechnet werden. Gefahr droht sowohl von durchsickerndem Wasser (auch Löschwasser) aus den darüber liegenden Gebäudeteilen als auch durch Rückstau aus der Kanalisation infolge von Starkregen, Hochwasser, sonstige Oberflächenwasser und Verstopfung.

3.3 Einbruch, Diebstahl, Sabotage, Vandalismus

Datenzentren sind wegen der gespeicherten Informationen sowie der materiellen Werte der installierten technischen Einrichtungen und Geräte immer wieder Ziel von Einbrüchen und Diebstählen. Dabei ist zu bedenken, dass Angriffe sowohl von außerhalb des Unternehmens als auch von innerhalb geführt werden können.

3.4 Fehlerhafte technische Einrichtungen

Risiken für Datenzentren entstehen auch durch die vorhandenen technischen Einrichtungen:

- Raumlufttechnische Anlagen durch Einbringen von Schadstoffen, Brandgasen, Rauch und Staub
- Fehlfunktionen und unzureichende Auslegung der Klimaanlage, Raumlufttechnischen Anlage und fehlende oder defekte Überwachung des Klimas in den IT-Räumen
- unzureichende elektrische Installationen und Anlagenteile, z.B. falsch ausgelegte oder fehlende USV (Unterbrechungsfreie Stromversorgung)
- mangelhafte oder fehlende Kompatibilität zwischen den einzelnen IT-Gerätschaften bzw. Geräten der technischen Infrastruktur
- nicht abgestimmte Brandfallsteuerung
- Einbringen von mechanischen Schwingungen

3.5 Elektrische Störeinflüsse

Die ordnungsgemäße Funktion von IT-Anlagen wird durch eine Störung der Energieversorgung gefährdet. Derartige Störungen können verursacht werden durch

- Ausfall des Versorgungsnetzes,
- Schäden in der (internen) Energieverteilungsanlage,
- Spannungsschwankungen.

IT-Anlagen sind durch Überspannungen und elektromagnetische Störungen gefährdet. Diese können durch

- Blitzschlag,
- Schaltvorgänge,
- Elektromagnetische Störungen

verursacht werden.

3.6 Organisatorische Mängel

Typische Beispiele für organisatorische Mängel sind:

- unsachgemäßer Betrieb, fehlende oder mangelhafte Instandhaltung der technischen Einrichtungen
- mangelhafte Sauberkeit und Ordnung
- fehlende oder unzureichende Notfallpläne
- fehlendes Konzept für die Durchführung von feuergefährlichen Arbeiten
- kein System zur Kontrolle von Fremdfirmen
- kein Verbot von Rauchen und offenem Licht
- unzureichende Ausbildung des Personals im sicherheitsgerechten Verhalten
- fehlende oder mangelhafte Schulung und Unterweisung des Personals
- Fehlverhalten bei der Brandbekämpfung und in anderen Notfällen
- fehlende Wiederanlaufpläne

3.7 Schutz bei Baumaßnahmen

Bei erforderlichen Umbauten im Datenzentrum oder in der Nähe desselben sind besonders geeignete Schutzmaßnahmen gegen die aus den Baumaßnahmen entstehenden Gefahren zu treffen. Dies gilt insbesondere für:

- Staubentwicklung
- Erschütterungen
- Wassereintritt
- Brandentstehung
- Spannungsschwankungen
- Beeinträchtigungen der Klimatisierung
- Beschädigung der Datenleitungen
- Aufhebung von Sicherheitseinrichtungen und Security-Bereiche
- mechanisch einwirkende Ereignisse

Bei Neuerrichtung von Datenzentren ist auf geeignete Abstände zu Flughäfen und Anflugbahnen zu achten.

4 VORBEUGENDE SCHUTZMASSNAHMEN

Eine wirkungsvolle Schadenverhütung kann nur durch ein auf den jeweiligen Betrieb abgestimmtes Gesamtkonzept erreicht werden, in dem die einzelnen Schutzmaßnahmen optimal kombiniert werden;
siehe hierzu die Auflistung in Tabelle 4.01. Bauliche, anlagentechnische und organisatorische Maßnahmen sind so miteinander abzustimmen, dass angepasst an die jeweilige IT-Anlage die definierten Schutzziele erreicht werden.

Bauliche, gebäudetechnische und planerische Maßnahmen	Anlagentechnische Maßnahmen	Organisatorische Maßnahmen
■ Ausreichende bauliche Trennung gegen Brand, Einbruch und Wassereintritt ■ Schottung von Durchbrüchen gegen Feuer und Rauch ■ Verwendung nichtbrennbarer Baustoffe und Materialien ■ Ausreichende statische Auslegung ■ Rettungswege ■ physische Sicherung ■ Heizungs-, Lüftungs- und Klimaanlagen ■ Raumlufttechnische Anlagen ■ Energie- und Netzversorgung	■ Brandmeldeanlage (BMA) ■ Feuerlöschanlage (FLA) ■ Einbruchmeldeanlage (EMA) ■ Entrauchungsanlage ■ Wandhydranten/Feuerlöscher ■ Blitz- und Überspannungsschutz, Elektromagnetische Verträglichkeit (EMV) ■ Unterbrechungsfreie Stromversorgung (USV); Netzersatzanlage ■ Feuchtigkeitssensoren/ Tauchpumpen ■ Datensicherung ■ Zutrittskontrollsystem (ZKS) ■ Videoüberwachung	■ Notfallabschaltplan ■ IT-Wiederanlaufplan (Business Continuity and Contingency Planning) ■ Brandschutzordnung ■ Feuerwehrplan ■ Brandschutzplan ■ Rettungswegeplan Betriebsanweisungen ■ Beschilderung / Kennzeichnung ■ Unnötige Brandlasten vermeiden ■ Rauchverbot ■ Nahrungsmittelverbot ■ Erlaubnisscheine: - Feuergefährliche Arbeiten - Einweisung von Fremdfirmen ■ Werkschutz ■ Besucherregelung ■ Schulungen ■ Übungen
Dokumentation		

Tabelle 4.01: Schutzmaßnahmen

4.1 Brandschutzmaßnahmen

4.1.1 Baulicher Brandschutz

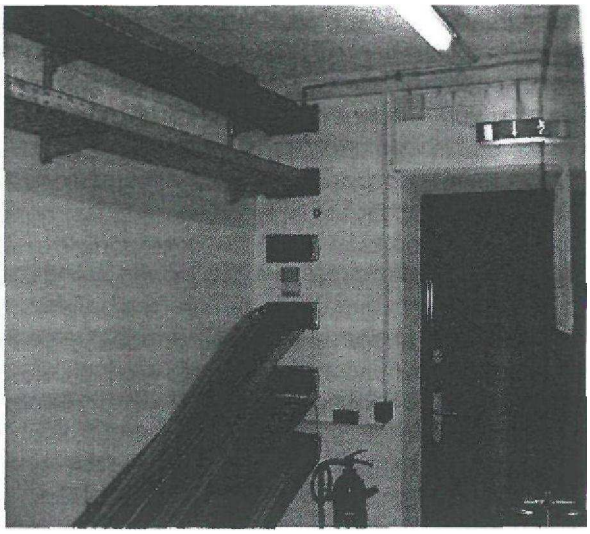
Datenzentren sind von angrenzenden Bereichen feuerbeständig und mit nichtbrennbaren Baustoffen (REI 90/F 90) abzutrennen.

Trennwände innerhalb der Datenzentren sollten mindestens feuerhemmend (REI 30/F 30) aus nichtbrennbaren Baustoffen ausgeführt werden. Sie sind vom Rohboden bis zur Rohdecke (durch den Doppelboden und die Zwischendecke) auszuführen. IT-Anlagen sind möglichst auf mehrere Räume zu verteilen.

IT-Bereiche dürfen sich nicht im gleichen Brandabschnitt mit Bereichen erhöhtem Risikos befinden. Bei erhöhtem Risiko, z.B. durch unmittelbar angrenzende Fabrikations- oder Lagerräume, sind Wände mit erhöhter mechanischer Festigkeit vorzusehen. Grundsätzlich wird hier eine Beratung mit dem Sachversicherer empfohlen.

Betriebsnotwendige Öffnungen (Türen, Verglasungen, Rohr- und Kabeldurchführungen etc.) sind entsprechend der Feuerwiderstandsklasse der angrenzenden Bauteile auszuführen. Zudem ist die Ausbreitung von Rauch wirksam zu verhindern.

In Dachflächen unmittelbar über der IT-Anlage sollten sich keine Dachdurchdringungen wie Lichtkuppeln oder Dachfenster befinden. Dächer über IT-Anlagen dürfen keine brennbare Eindeckung oder Wärmedämmung aufweisen.



Quelle: Bruno Hecht, Von zur Mühlen GmbH

Bild 4.01: Kabelschottung

Innenausbau/Einrichtung
Für den Innenausbau sind nichtbrennbare Materialien zu verwenden; sofern dieses nicht möglich ist, sind mindestens schwer entflammbare und nicht brennend abtropfende Materialien zu wählen. Es sind möglichst wenig halogenhaltige Kunststoffe in Datenzentren und angrenzenden Bereichen einzusetzen. Entsprechendes gilt für die Einrichtung.

Brandlasten und potenzielle Zündquellen sind in Datenzentren zu vermeiden (siehe Tabelle 3.01).

4.1.2 Anlagentechnischer Brandschutz

4.1.2.1 Brandmeldeanlagen
4.1.2.2 Selbständige Löschanlagen
4.1.2.3 Sauerstoffreduktionsanlagen
4.1.2.4 Natürlich wirkende Rauchabzugsanlagen (NRA) sowie maschinelle Rauchabzüge (MRA), Druckbelüftungsanlagen (DBA)
4.1.2.5 Mittel zur ersten und erweiterten Löschhilfe

4.1.2.1 Brandmeldeanlagen

Die Brandmeldung, Alarmierung, Alarmfallsteuerung, Ansteuerung bzw. Vorsteuerung (Sprinkler) einer Feuerlöschanlage und deren Überwachung erfolgt in der Regel durch eine für diesen Zweck anerkannte Brandmeldeanlage.

4.1.2.2 Selbständige Löschanlagen

- CO2-Feuerlöschanlagen
- Inertgaslöschanlagen
- Anlagen mit chemischen Löschgasen

Für den Einsatz in IT-Bereichen sind Löschmittel wünschenswert, die möglichst rückstandsfrei, nicht korrosiv und elektrisch nicht leitend sein sollten. Dies ist bei Gaslöschanlagen überwiegend der Fall.

4.1.2.3 Sauerstoffreduktionsanlagen

Durch den Einsatz einer Sauerstoffreduktionsanlage (SRA) soll im zu schützenden Bereich durch Absenken des Sauerstoffgehaltes der Umgebungsluft eine offene Brandentstehung verhindert werden.

4.1.2.4 Natürlich wirkende Rauchabzugsanlagen (NRA) sowie maschinelle Rauchabzüge (MRA), Druckbelüftungsanlagen (DBA)

Bei der Neukonzeption von Datenzentren sollte die Installation von Rauchabzugsanlagen, Druckbelüftungsanlagen in die Überlegungen mit einbezogen werden. Ziel ist es, Schädigungen der IT-Geräte durch aggressive Rauchgase und Hitzeeinwirkung zu vermeiden.

Rauchabzugsanlagen sollten die folgenden Merkmale aufweisen:

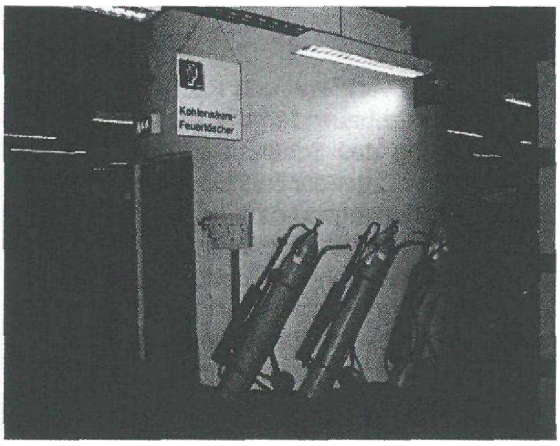
- Eine Entrauchungsanlage sollte speziell für den IT-Bereich geplant und konzipiert werden.
- Entrauchungsleitungen und -klappen, die Decken oder Wände mit definierten Feuerwiderstandsklasse auszuführen.
- Es dürfen für Entrauchungsleitungen nur nichtbrennbare Baustoffe verwendet werden.
- Die Rauchabzugsanlage sollte so ausgelegt werden, dass bereits während des Brandgeschehens Rauch und Heißgabe abgeführt werden können.
- Öffnungen ins Freie müssen so geplant werden, dass sie gegen Einwirkungen von außen geschützt sind.

Druckbelüftungsanlagen sollen das Eindringen von Brandrauch bei Bränden in der Umgebung von IT-Anlagen verhindern.

4.1.2.5 Mittel zur ersten und erweiterten Löschhilfe

Sowohl in den eigentlichen Datenzentren als auch in den benachbarten Räumen müssen geeignete Feuerlöscher in ausreichender Anzahl vorhanden sein.

Für den Einsatz in IT-Anlagen sollten CO2-Feuerlöscher bevorzugt werden. Pulverlöscher stellen eine große Gefahr für die IT-Anlage dar und sind weder im IT-Anlagen-Raum noch in benachbarten Räumen aufzustellen. Ersatzweise könnten Feuerlöscher mit Wasser, mit Wasser mit Zusätzen bzw. mit Schaum verwendet werden.



Quelle: Theo Gärtner, M+W Zander

Bild 4.03: Mobile C02-Feuerlöscher

4.1.3 Organisatorischer Brandschutz

4.1.3.1 Brandschutzausbildung und Brandschutzordnung

Es ist eine Brandschutzorganisation aufzustellen und für die Datenzentren zu spezifizieren und ausdrücklich auf spezielle Datenzentren anzupassen. Folgende Punkte sollten hierbei berücksichtigt werden:

- Brandlasten auf das Notwendigste reduzieren
- Regelungen für das Verhalten im Brandfall aufstellen und Mitarbeiter schulen
- Regelungen für Montage- und Installationsarbeiten treffen
- Feuergefährliche Arbeiten grundsätzlich zu verbieten, Alternativen zu funkenbildenden Arbeiten sind zu bevorzugen
- Außerhalb der Serverräume dürfen Heißarbeiten nur mit Erlaubnisschein und entsprechenden Brandschutzvorkehrungen durchgeführt werden
- Fremdfirmen einweisen und nur unter Aufsicht arbeiten lassen
- Sauberkeit und Ordnung ständig gewährleisten und kontrollieren
- Zündquellen ausschließen
- Rauchverbot; erforderlichenfalls separaten brandschutztechnisch getrennten Raucherbereich vorsehen
- Verbot für private elektrische Geräte

4.1.3.2 Brandschutzkonzept

Alle erforderlichen Schutzmaßnahmen sind mit den Verantwortlichen für Arbeitsschutz und Brandschutz sowie mit der betrieblichen bzw. zuständigen öffentlichen Feuerwehr zu besprechen und in bestehende Brandschutzkonzepte zu integrieren. Brandschutzpläne sind ständig auf dem neuesten Stand zu halten. Der Feuerwehrplan ist der zuständigen Feuerwehr zu übergeben.

4.2 Schutz vor Naturgefahren, Wasser und sonstige Flüssigkeiten

Ein direkter Schutz vor Naturgefahren ist grundsätzlich nicht möglich. Durch entsprechende Auslegung der Gebäudestatik und Aufstellung der Geräte können die durch Naturgefahren verursachten Schäden weitestgehend vermieden, zumindest aber stark begrenzt werden.

Entkoppelung der Anlagen von externen Schwingungen, z.B. durch Erdbeben, sollte bei der Aufstellung von Anlagen berücksichtigt werden.

Generell sind Datenzentren mit ihren Ver- und Entsorgungseinrichtungen so zu planen, dass sie vor eindringendem Wasser und Wasseraustritt aus Leitungssystemen geschützt sind. Insbesondere sollten zentrale IT-Bereiche sich nicht

- in überschwemmungsgefährdeten Gebieten,
- direkt unter Flachdachbereichen mit Dehnungsfugen oder Einlaufen,
- unter Wasserbehältern

befinden. Ist es unvermeidlich, den zentralen Datenzentren-Bereich dennoch in einem der vorgenannten Bereiche unterzubringen, sind der Situation angepasste Schutzmaßnahmen zu ergreifen. Diese können sein:

- aufgeständerte IT-Installationen (mind. 10 cm hoch)
- Vermeiden von Steckverbindungen (Stromversorgungs- und Datenleitungen) im Doppelboden bzw. direkt auf dem Boden; sofern Steckverbindungen unvermeidbar sind, sollten diese in der Schutzart IP 54 ausgeführt werden
- Wasserschwellen
- Rückstauklappen in den Abwasserleitungen
- Wassermelder
- Pumpensumpf mit automatischer Hebepumpe
- Auffangwannen unter den potenziellen Schwachstellen mit Anschluss an die Gebäudeentwässerung und Feuchtmeldern
- in Datenzentren vorhandene Rohrleitungen (z.B. für Abwasser, Dampf, Frischwasser, Heizung) sind nach Möglichkeit zu entfernen

Sind wasserführende Leitungen systembedingt erforderlich (wassergekühlte Zentraleinheit, Kaltwasserleitungen des Klimasystems), oder aus anderen technischen Gründen unvermeidbar, so sind für derartige Leitungen entsprechende Sicherheitsmaßnahmen zu treffen.

4.3 Einbruch, Diebstahl, Sabotage, Vandalismus

4.3.1 Mechanischer Einbruchschutz

Es ist auf eine anonyme Lage der Räume zu achten. Das Rechenzentrum sollte daher beispielsweise nicht durch Hinweisschilder gekennzeichnet sein.

Umfassungswände, Fenster und Türen der Datenzentren sollen einen angemessen hohen mechanischen Widerstandswert aufweisen.

4.3.2 Einbruchmeldeanlage

Die zu schützenden Räume sind in unbesetzten Zeiten durch eine Einbruchmeldeanlage (EMA) zu überwachen. Alle Türen, Fenster und Öffnungen in der Außenhaut der zu schützenden Räume sind auf Öffnen und Verschluss zu überwachen. Die Meldungen der EMA sind zu einer ständig besetzten und entsprechend instruierten Stelle weiterzuleiten (Polizei, Wach- und Sicherheitsunternehmen, Leitzentrale).

4.3.3 Zutrittskontrolle

Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen ist zu regeln und zu kontrollieren. Der Zutritt sollte nur für autorisierte Personen vorgesehen sein. Die Maßnahmen reichen dabei von einer einfachen Schlüsselvergabe bis zum elektronischen Zutrittskontrollsystem (ZKS) z.B. mit Karte und PIN.

4.4. Fehlerhafte technische Einrichtungen

4.4.1 Elektrische Installation

Die elektrischen Installationen sind nach den anerkannten Regeln der Elektrotechnik zu errichten und zu unterhalten. Dazu gehören auch regelmäßige thermographische Überprüfungen. Eine erhöhte Gefahr stellen Provisorien dar.

4.4.2 Notaus-Schalteinrichtungen

Bei einem Brand können Schäden an den betroffenen IT-Geräten in der Regel verringert werden, wenn rechtzeitig ein Spannungsfreischalten erfolgt. Entsprechende Einrichtungen sind gegen versehentliche Betätigung und Missbrauch zu schützen.

4.4.3 Klima-/Raumlufttechnische Anlagen

Die Klimaanlage/RLT-Anlage ist nach Möglichkeit in einem feuerbeständig abgetrennten Raum unterzubringen. Es sollten vorzugsweise Umluftkühlgeräte zum Einsatz kommen, die außerhalb der IT-Anlage installiert werden. Die Klimaanlage/RLT-Anlage sollte durch eine festmontierte, nicht batteriebetriebene Regelung gesteuert werden.

Ansaugöffnungen für die Außenluft sind so anzuordnen, dass keine Schadstoffe (z.B. Abluft aus anderen Klima- und Lüftungsanlagen) eindringen können. Auch auf den Schutz vor Sabotageakten ist zu achten. Im Einzelfall sollte eine Überwachung der Ansaugöffnung mit Rauchmeldern in Betracht gezogen werden.

4.5 Elektrische Störeinflüsse

Da selbst sehr kurze Umschaltlücken zu Störungen in IT-Systemen führen können, sollte zu deren Überbrückung in jedem Fall an geeigneter Stelle eine unterbrechungsfreie Stromversorgung (USV) realisiert sein.

4.5.1 Schutz der Energieversorgung

Da die Möglichkeit einer zweiten Stromeinspeisung nur selten möglich ist, wird die Installation einer Notstromversorgung empfohlen. Wenn Akkus und Batterien für die Notstromversorgung vorgesehen sind, sollten diese aufgrund der davon ausgehenden Brand- und Explosionsgefahr in einem eigenen gesicherten Bereich aufgestellt werden.

4.5.2 Blitz- und Überspannungsschutz

Für IT-Anlagen ist der Blitzschutz-Potenzialausgleich vorzusehen. In jedem Fall ist ein umfassendes Überspannungsschutzkonzept durch einen geeigneten Fachplaner zu erstellen.

4.6 Organisatorische Mängel

Wesentliche Grundlage für die IT-Sicherheit sind klare Regelungen darüber, wer was zu tun hat, bzw. wer was keinesfalls tun darf. Es sind daher entsprechende Regelwerke zu erstellen, zu pflegen und den Betroffenen zur Kenntnis zu geben. Es sollten z.B. Aussagen getroffen werden bezüglich:

- Ansprechpartner, Zuständigkeiten, Administrationsorganisation (inkl. Organigramm des Unternehmens)
- Darstellung der Aufgaben der IT-Anlage
- allen der IT-Sicherheit dienenden Regelungen
  - Zutrittsberechtigungen (inkl. Besucherregelung)
  - Datensicherungskonzept
  - Maßnahmen bei Störungen oder besonderen Zwischenfällen (Incident-Handling)
- sonstigen Sicherheitskonzepten
  - Datenschutz
  - Brandschutz
  - physische Sicherung
- Katastrophenschutz/Notfallpläne

5. HINWEISE

Auf folgende Richtlinien und Normen in der jeweils geltenden Fassung wird ausdrücklich verwiesen:

TRVB 104 Brandgefahren beim Schweißen, Schneiden, Löten und anderen Feuerarbeiten // Brandschutzvorkehrungen (S. 10)

TRVB 107 Brandschutzgutachten // Brandschutzkonzept (S. 10)

TRVB 117 Betrieblicher Brandschutz – Ausbildung // Ausbildung (S. 9)

TRVB 119 Betriebsbrandschutz – Organisation // Brandschutzordnung (S. 9)

TRVB 120 Betriebsbrandschutz – Eigenkontrolle // Brandschutzordnung (S. 9)

TRVB 123 Automatische Brandmeldeanlagen // Brandmeldeanlagen (S. 8)

TRVB 124 Erste und Erweiterte Löschhilfe // Mittel zur ersten und erweiterten Löschhilfe (S. 9)

TRVB 128 Steigleitungen und Wandhydranten // Mittel zur ersten und erweiterten Löschhilfe (S. 9)

TRVB 140 CO2-Löschanlagen // CO2-Feuerlöschanlagen (S. 9)

TRVB 152 Automatische Löschanlagen - Gasförmige Sonderlöschmittel // Inertgas (S. 8)

TRVB 155 Sauerstoffreduzieranlagen (SRA) // Sauerstoffreduktionsanlagen (S. 8)

Die technischen Richtlinien vorbeugender Brandschutz (TRVBs) können bei den Landesbrandverhütungsstellen oder beim Bundesfeuerwehrverband bezogen werden.

DIN 41Q2 Brandverhalten von Baustoffen und Bauteilen EN 13501

- Teil 1: Baustoffe; Begriffe, Anforderungen und Prüfungen
- Teil 2: Bauteile; Begriffe, Anforderungen und Prüfungen
- Teil 4: Zusammenstellung und Anwendung klassifizierter Baustoffe, Bauteile und Sonderbauteile
- Teil 5: Feuerschutzabschlüsse; Abschlüsse in Fahrschachtwänden und gegen Feuerwiderstandsfähige Verglasungen, Begriffe, Anforderungen und Prüfungen
- Teil 6: Lüftungsleitungen; Begriffe, Anforderungen und Prüfungen
- Teil 12: Funktionserhalt von elektrischen Kabelanlagen, Anforderungen und Prüfungen

DIN 14 096 Brandschutzordnung, Teil B: Regeln für das Erstellen des Teils B (für Personen ohne besondere Brandschutzaufgaben)

DIN EN 356 Glas im Bauwesen - Sicherheitssonderverglasung, Prüfverfahren und Klasseneinteilung des Widerstandes gegen manuellen Angriff

DIN EN 1063 Glas im Bauwesen - Sicherheitssonderverglasung - Prüfverfahren und Klasseneinteilung für den Widerstand gegen Beschuss

DIN EN 61 355 Klassifikation und Kennzeichnung von Dokumenten für Anlagen, Systeme und Einrichtungen

DIN V ENV 1627 Einbruchhemmung, Anforderungen und Klassifizierung

DIN V VDE V 0185-3 Blitzschutz, Schutz von baulichen Anlagen und Personen

DIN VDE 0100 Bestimmungen für das Errichten von Starkstromanlagen mit Netzspannungen bis 1000 V

- Teil 300: Bestimmungen allgemeiner Merkmale
- Teil 444: Schutz gegen elektromagnetische Störungen (EMI) in Anlagen von Gebäuden
- Teil 482: Brandschutz bei besonderen Risiken und Gefahren
- Teil 559: Leuchten und Beleuchtungsanlagen

DIN VDE 0185-100 Blitzschutz baulicher Anlagen, Allgemeine Grundsätze

DIN VDE 0660 Normenreihe Niederspannungsschaltgeräte

DIN VDE 0712 Bestimmungen für Entladungslampenzubehör mit Nennspannung bis 1000 V

DIN VDE 0800 Informationstechnik

- Teil 1: Allgemeine Begriffe, Anforderungen und Prüfungen für die Sicherheit der Anlagen und Geräte
- Teil 174-2: Installation von Verkabelungsanlagen (entspricht EN 50174-2)
- Teil 2-310: Anwendung von Maßnahmen für Potenzialausgleich und Erdung in Gebäuden mit Einrichtungen der Informationstechnik (entspricht EN 50310)
- Teil 10: Fernmeldetechnik Übergangsfestlegungen für Errichtung und Betrieb der Anlagen

VDI 2054 Raumlufttechnische Anlagen für Datenverarbeitung

VDMA24 991 Prüfbedingungen für das Brandverhalten von Stahlschränken und sonstigen Behältern

VdS-Publikationen

VdS 2000 Brandschutz im Betrieb, Leitfaden für den Brandschutz

VdS 2001 Regeln für die Ausrüstung von Arbeitsstätten mit Feuerlöschern

VdS 2005 Leuchten, Richtlinien zur Schadenverhütung

VdS 2009 Brandschutzmanagement, Leitfaden für die Verantwortlichen im Betrieb und Unternehmen

VdS 2010 Risikoorientierter Blitz- und Überspannungsschutz, Richtlinien zur Schadenverhütung

VdS 2005 Kabel- und Leitungsanlagen, Richtlinien zur Schadenverhütung

VdS 2031 Blitz- und Überspannungsschutz in elektrischen Anlagen, Richtlinien zur Schadenverhütung

VdS 2033 Feuergefährdete Betriebsstätten und diesen gleichzustellende Risiken, Richtlinien zur Schadenverhütung

VdS 2036 Erlaubnisschein für feuergefährliche Arbeiten (Muster)

VdS 2093 C02-Feuerlöschanlagen, Planung und Einbau

VdS 2095 Brandmeldeanlagen, Richtlinien für Planung und Einbau

VdS 2097-4-6 Produkte und Anlagen des baulichen Brandschutzes

VdS 2105 Richtlinien für mechanische Sicherungseinrichtungen, Schlüsseldepots (SD), Anforderungen an Anlagenteile, Planung und Einbau

VdS 2163 Richtlinien für mechanische Sicherungstechnik, Einbruchhemmende Verglasung, Anforderungen und Prüfmethoden

VdS 2234 Brand- und Komplextrennwände, Merkblatt für die Anordnung und Ausführung

VdS 2298 Brandschutz in Lüftungsanlagen, Merkblatt für den Brandschutz

VdS 2304 Einrichtungsschutz für elektrische und elektronische Geräte

VdS 2311 Einbruchmeldeanlagen, Richtlinien für Planung und Einbau

VdS 2324 Niedervoltbeleuchtungsanlagen und - Systeme, Richtlinien zur Schadenverhütung

VdS 2333 Sicherungsrichtlinien für Geschäfte und Betriebe

VdS 2349 Störungsarme Elektroinstallationen, Richtlinien zur Schadenverhütung

VdS 2358 Richtlinien für Zutrittskontrollanlagen, Planung und Einbau

VdS 2380 Planung und Einbau von Löschanlagen mit nicht-verflüssigten Inertgasen (Argon, Stickstoff, Inergen)

VdS 2381 Planung und Einbau von Löschanlagen mit halogenierten Kohlenwasserstoffen

VdS 2496 Richtlinien für die Ansteuerung von Feuerlöschanlagen

VdS 2534 Richtlinien für mechanische Sicherungseinrichtungen, Einbruchhemmende Fassadenelemente, Anforderungen und Prüfmethoden

VdS 2556 Sicherung von verfahrenstechnischen Anlagen mit Mitteln der Prozessleittechnik

VdS 2562 Verfahren für die Anerkennung neuer Löschtechniken

VdS 2569 Überspannungsschutz für elektronische Datenverarbeitungsanlagen, Richtlinien zur Schadenverhütung

VdS CEA 4001 Planung und Einbau von Sprinkleranlagen

VdS Schadenverhütung Verlag
Amsterdamer Str. 174, 50735 Köln
Internet: www.vds.de