VdS VERLAG

Anlagen der Informationstechnologie (IT-Anlagen)

Merkblatt zur Schadenverhütung

VdS 2007 : 2004-08 (03).

Titelbild: Data Center der is:energy GmbH

Anlagen der Informationstechnologie (IT-Anlagen)

Merkblatt zur Schadenverhütung

Inhalt

1 Vorbemerkungen

1.1 Allgemeines

Gewerbliche und industrielle Betriebe, Hochschulen und Universitäten sowie Einrichtungen der Verwaltung sind in hohem Maße von der ordnungsgemäßen Funktion ihrer Anlagen der Informationstechnologie (IT-Anlagen) abhängig. Ihre besondere Bedeutung liegt im hohen Verfügbarkeitsanspruch und ihrer Schlüsselfunktion für die nachfolgenden Produktions- und Verwaltungsprozesse des Unternehmens. Ausfälle solcher Anlagen stellen eine ernste Bedrohung für das Unternehmen dar. IT-Anlagen erfordern wegen dieser Bedeutung für die meisten Unternehmen Maßnahmen der Schadenverhütung, die über die gesetzlichen Anforderungen wie z.B. die des Baurechts, Arbeitsschutzrechts etc. hinausgehen.

Das vorliegende Merkblatt wurde vom Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV) im Einvernehmen mit dem Bundesverband der Deutschen Industrie e. V. (BDI) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt und konkretisiert die Anforderungen und Maßnahmen zur Schadenverhütung für IT-Anlagen in Betrieben, Hochschulen und Verwaltungen. Es aktualisiert VdS 2007 Elektronische Datenverarbeitungsanlagen (EDVA), Merkblatt zum Brandschutz in Räumen für EDVA.

Das Merkblatt gilt sowohl für neu zu errichtende als auch bestehende Anlagen. Die Verantwortung des Betreibers der IT-Anlagen 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.

Hinweis: Eine Muster-Checkliste im Anhang C enthält (ohne Anspruch auf Vollständigkeit) eine Übersicht und weitere Hinweise zu einzelnen schadenverhütenden Maßnahmen.

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 die IT-Anlagen sollte einen entsprechend hohen Stellenwert erhalten. 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.

1.2 Anwendungsbereich

IT-Anlagen im Sinne dieses Merkblatts sind Rechenzentren und Serverräume sowie zentrale Anlagen der Mess-, Steuer- und Regeltechnik (siehe hierzu auch VdS 2556 Sicherung von verfahrenstechnischen Anlagen mit Mitteln der Prozessleittechnik), 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 Baubehörden, Gewerbeaufsichtsämtern und Berufsgenossenschaften geforderte Sicherheits- und Schadenverhütungsmaßnahmen bleiben von diesem Merkblatt unberührt. Sie sind z.T. in das Merkblatt eingearbeitet.

2 Begriffe und Abkürzungen

BMA	Brandmeldeanlage
Disc-Arrays	Verbund mehrerer Festplatten
EMI	Electro Magnetic Inferences
EMV	Elektromagnetische Verträglichkeit
FLA	Feuerlöschanlage
GSHB	Grundschutzhandbuch
NEA	Netzersatzanlage
NHV	Niederspannungshauptverteilung
RAID-Systeme	Redundant Array of Independent Disk
RLT	Raumlufttechnische Anlagen
RWA	Rauch- und Wärme-Abzugsanlage
USV	Unterbrechungsfreie Stromversorgung
VNB	Versorgungsnetzbetreiber
ZKS	Zutrittskontrollsystem

3 Gefahren in IT-Anlagen

Der Betrieb einer IT-Anlage ist unterschiedlichen Gefahren ausgesetzt, die zu Schäden am Gebäude, an Maschinen und zu Datenverlusten führen können:

- Brand, Rauch, Explosion
- Störung der Energieversorgung
- Überspannung (Blitzschlag, EMV, Oberschwingungen, Transientenströme, u.a.)
- mangelhafter Potenzialausgleich
- Wasser
- Einbruch/Diebstahl, Vandalismus und Sabotage
- Elementarereignisse (Hochwasser, Sturm, Erdbeben etc.)
- fehlerhafte Gebäudeplanung (Auswahl ungeeigneter Räume)
- fehlerhafte technische Einrichtungen
- organisatorische Mängel (ungenügend ausgebildetes Personal)

Risiken, die sich im Hinblick auf Datensicherheit durch Viren, Hacker etc. ergeben, sind nicht Gegenstand dieses Merkblatts.

3.1 Brand

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 IT-Anlagen begünstigen oft eine schnelle Brandausbreitung. IT-Anlagen 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.

3.2 Elementarereignisse

Elementarereignisse wie Sturm, Hagel, Starkregen, (Hochwasser), Rückstau, Schneedruck, Erdbeben können sowohl direkt als auch indirekt auf die IT-Anlage einwirken.

3.3 Wasser und sonstige Flüssigkeiten

Gefahr von Wasserschäden besteht im Zusammenhang mit

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

Bereich	Gefährdung durch	
	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, RLT, Notstromversorgung etc. können zu unzulässiger Erwärmung von Anlagenteilen führen
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

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

Bei IT-Anlagen 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.

3.4 Einbruch, Diebstahl, Sabotage, Vandalismus

IT-Anlagen 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.

3.5 Technische Einrichtungen

Risiken für IT-Anlagen 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 (RLT-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

3.6 Störung der Energieversorgung

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

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

3.7 Elektrische Störeinflüsse

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

- Blitzschlag,
- Schaltvorgänge,
- Spannungsverschiebung (Sternpunktverschiebung) und
- Elektromagnetische Störungen (EMI)
  Hinweis: siehe DIN VDE 0100-444

verursacht werden.

Hervorzuheben sind die Gefahren durch elektromagnetische Störungen. Ströme, die über galvanische Verbindungen oder durch magnetische bzw. kapazitive Einkopplung in nichtaktiven Leitern fließen, stellen eine besondere Gefahr für IT-Anlagen dar. Schäden können verursacht werden durch Ströme auf Schutzleitern, Potenzialausgleichsleitern, Kabelschirmen, Gehäusen elektrischer Betriebsmittel oder fremden leitfähigen Teilen. Dabei können deren Strombelastbarkeit überschritten, elektronische Schaltungen und Bauteile beeinträchtigt oder Isolierungen über- oder durchschlagen werden. Darüber hinaus kann es zur Entzündung von Isolierungen und anderen brennbaren Materialien kommen.

3.8 Fehlerhafte Planung/ Organisatorische Mängel

Planungsfehler stellen eine Gefahr für IT-Anlagen dar. Beispiele für Planungsfehler sind:

- unzweckmäßige Auswahl der örtlichen und/ oder baulichen Lage der Gebäude oder innerhalb der Gebäude
- unzweckmäßige Anordnung der Einrichtungen von IT-Anlagen
- mangelhafte Koordination der einzelnen Gewerke und Systeme
- außerachtlassen von Benutzeranforderungen

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

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.

4.1 Brandschutzmaßnahmen

4.1.1 Baulicher Brandschutz

4.1.1.1 Bauliche Trennung
IT-Anlagen sind von angrenzenden Bereichen feuerbeständig und mit nichtbrennbaren Baustoffen (F 90-A nach DIN 4102- 4) abzutrennen.

Trennwände innerhalb der IT-Anlage sollten mindestens feuerhemmend (F 30-A nach DIN 4102-4) 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 nach VdS 2234 Brand- und Komplextrennwände, Merkblatt für die Anordnung und Ausführung, 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.

Hinweis: siehe VdS 2097-4 und -6 Produkte und Anlagen des baulichen Brandschutzes

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.

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 ■ RLT ■ Energie- und Netzversorgung	■ Brandmeldeanlage (BMA) ■ Feuerlöschanlage (FLA) ■ Einbruchmeldeanlage (EMA) ■ Entrauchungsanlage ■ Wandhydranten/Feuerlöscher ■ Blitz- und Überspannungsschutz, EMV ■ USV; Netzersatzanlage ■ Feuchtigkeitssensoren/Tauchpumpen ■ Datensicherung ■ Zutrittskontrollsystem (ZKS) ■ Videoüberwachung	■ Notfallabschaltplan ■ IT-Wiederanlaufplan (Business Continuity and Contingency Planning) ■ Brandschutzordnung ■ Feuerwehrplan ■ Brandschutzplan ■ Rettungswegeplan, Betriebsanweisungen ■ Beschilderung/Kennzeichnung (siehe BGV A8) ■ Unnötige Brandlasten vermeiden ■ Rauchverbot ■ Nahrungsmittelverbot ■ Erlaubnisscheine: – Feuergefährliche Arbeiten – Einweisung von Fremdfirmen ■ Werkschutz ■ Besucherregelung ■ Schulungen ■ Übungen
Dokumentation		

Tabelle 4.01: Schutzmaßnahmen

Quelle: Bruno Hecht, Von zur Mühlen GmbH

Bild 4.01: Kabelschottung

4.1.1.2 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 den IT-Anlagen-Räumen und angrenzenden Bereichen einzusetzen. Entsprechendes gilt für die Einrichtung.

Brandlasten und potenzielle Zündquellen sind in den IT-Anlage-Räumen zu vermeiden (siehe Tabelle 3.01).

4.1.2 Anlagentechnischer Brandschutz

4.1.2.1 Brandmeldeanlagen
Die Räume für die IT-Anlagen, einschließlich der Nebenräume, sind durch eine automatische Brandmeldeanlage (BMA) zu überwachen. Neben den Räumen der IT-Anlage selbst, können das sein:

- Aufstellungsräume der Klimaanlage/RLT-Anlage
- Zu- und Abluftkanäle der Klimaanlage/RLT-Anlage einschließlich Frischluft-Ansaugleitung
- Räume für Strom- und Ersatzstromversorgung
- Datenarchivräume
- Papierlager
- angrenzende sonstige Räume, horizontal wie vertikal

Doppelböden und Räume zwischen abgehängten Decken und Geschossdecken sind in die Überwachung einzubeziehen. Ausgenommen hiervon sind Zwischendecken und Zwischenbodenbereiche, die sämtliche der folgenden Bedingungen erfüllen:

- Die Zwischenräume müssen weniger als 0,8 m hoch sein.
- Es dürfen keine Leitungen für Sicherheitsanlagen, z.B. Sicherheitsbeleuchtung, elektroakustische Anlagen usw. vorhanden sein.
- Die Brandlast muss kleiner als 25 MJ, bezogen auf eine Fläche von 1 m x 1 m, sein.
- Die Umfassungsbauteile (Decke, Boden, Wand) müssen nichtbrennbar sein und die Zwischenbereiche müssen mit nichtbrennbarem Material so unterteilt sein, dass Abschnitte von maximal 10 m Breite und 10 m Länge gebildet werden.

Je nach Schutzziel kann eine Überwachung der oben genannten Bereiche allerdings notwendig sein.

Hinweis: siehe VdS 2095 Richtlinien für automatische Brandmeldeanlagen – Planung und Einbau, insbesondere Anhang C "Datenverarbeitungsanlagen"

Bei der Überwachung von IT-Bereichen kommen in den meisten Fällen Rauchmelder zum Einsatz; die Brandmelder müssen immer für den zu überwachenden Bereich und die zu erwartenden Brandkenngrößen geeignet sein.

Ein gewaltfreier Zutritt bei Brandalarm, z.B. durch ein Schlüsseldepot gemäß VdS 2105 (auch Feuerwehr-Schlüsselkasten genannt), muss gewährleistet sein.

4.1.2.2 Einrichtungsüberwachung
In klimatisierten IT-Bereichen, insbesondere solchen mit belüfteten Einrichtungen elektrischer-, elektronischer Systeme, ist eine Brandfrüherkennung mit den üblichen punktförmigen Rauchmeldern wegen der Zwangsluftführung und der "Verdünnung" der Brandkenngröße erheblich erschwert oder gar unmöglich. Um einen lückenlosen Brandschutz sicherzustellen, sind zusätzlich zur Raumüberwachung alle von einer Klimaanlage zwangsbelüfteten Einrichtungen in den Überwachungsumfang einzubeziehen.

Im Unterschied zur klassischen Brandmelderausstattung, mit der in diesem Fall verlässlich nur eine schon recht fortgeschrittene Brandentwicklung detektiert werden kann, bietet die Einrichtungsüberwachung mit Ansaugbrandmeldern mit hoher Ansprechempfindlichkeit die Möglichkeit einer frühen und örtlich begrenzten Reaktion. Dabei können unterschiedliche Alarmschwellen festgelegt werden, die eine Reihe schadenmindernder Reaktionen auslösen können z.B.:

- Aufmerksamkeit bei einer ständig besetzten Stelle
- kontrolliertes Herunterfahren gefährdeter Systeme
- Spannungsfreischalten der Einrichtung, bei der ein Brand detektiert wurde (Allein dadurch kommt die überwiegende Mehrzahl von Bränden zum Erliegen)
- Brandmeldung mit Alarmweiterleitung
- ggf. Auslösung der Einrichtungsschutzanlage (siehe dazu Abschnitt 4.1.2.3)
- ggf. Auslösung der Raumschutzanlage

Durch diese Vorgehensweise lassen sich die Schadenfolgen hinsichtlich der Anzahl bei einem Brand ausfallender Geräte, der Ausfallzeiten und der Kosten deutlich minimieren.

Quelle: Theo Gärtner, M+W Zander

Bild 4.02: Einrichtungsüberwachung mit Ansaugbrandmeldern

4.1.2.3 Feuerlöschanlagen

Für den Schutz ganzer IT-Anlagen empfehlen sich selbsttätige, stationäre Feuerlöschanlagen. Dabei kommen grundsätzlich sowohl Gaslöschanlagen als auch Wasserlöschanlagen für die IT-Anlagen einschließlich angrenzender Nebenbereiche, wie Läger, Archive und Büros in Betracht. Diese Feuerlöschanlagen können als Einrichtungs- oder Raumschutzanlagen ausgeführt werden. Einrichtungsschutzanlagen wirken dabei selektiv auf das zu schützende Gerät oder Anlagenteil.

Vor Auslösung einer Feuerlöschanlage sollte die Klimaanlage automatisch abgeschaltet werden.

Wasserlöschanlagen sind üblicherweise Sprinkleranlagen, die vorwiegend dem Gebäude- und Personenschutz dienen und wegen des Restrisikos eines ungewollten Wasseraustritts mit Folgeschäden an empfindlichen Einrichtungen bevorzugt als vorgesteuerte Trockenanlagen (sog. Preaction-Anlagen) ausgeführt werden.

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.

Für den Einsatz in IT-Bereichen, in Kabelböden und dgl. kommen z.B.

- CO_2-Feuerlöschanlagen,
- Inertgaslöschanlagen,
- Anlagen mit chemischen Löschgasen

in Frage.

Jede dieser Löschanlagen hat für diesen speziellen Anwendungszweck Vor- und Nachteile. Daher ist die Art der einzubauenden Löschanlage unter Berücksichtigung des Schutzzieles bereits im Planungsstadium unter der Fachberatung eines kompetenten Planungsbüros oder einer VdS-anerkannten Errichterfirma und der Brandschutzabteilung des Versicherers festzulegen.

Hinweis: Für andere, neue Löschtechniken besteht die Möglichkeit, gemäß VdS 2562 Verfahren für die Anerkennung neuer Löschtechniken, eine VdS-Anerkennung zu erlangen. Voraussetzung hierfür ist der Nachweis der Wirksamkeit und Zuverlässigkeit der neuen Löschtechnik.

Ausgewählte VdS-Richtlinien im Zusammenhang mit Feuerlöschanlagen:

- VdS 2093 CO_2-Feuerlöschanlagen, Planung und Einbau
- VdS 2304 Einrichtungsschutz für elektrische und elektronische Systeme , Richtlinien für Planung und Einbau
- VdS 2380 Planung und Einbau von Löschanlagen mit nicht-verflüssigten Inertgasen
- VdS 2381 Planung und Einbau von Löschanlagen mit halogenierten Kohlenwasserstoffen
- VdS 2496 Richtlinien für die Ansteuerung von Feuerlöschanlagen
- VdS CEA 4001 Planung und Einbau von Sprinkleranlagen

Die Brandmeldung, Alarmierung, Alarmfallsteuerung, Ansteuerung bzw. Vorsteuerung (Sprinkler) einer Feuerlöschanlage und deren Überwachung erfolgt in der Regel durch eine für diesen Zweck anerkannte Brandmeldeanlage gemäß Abschnitt 4.1.2.1.

4.1.2.4 Feuerlöscher
Sowohl in den eigentlichen IT-Anlage-Räumen als auch in den benachbarten Räumen müssen geeignete Feuerlöscher in ausreichender Anzahl vorhanden sein.

Pulverlöscher stellen eine große Gefahr für die IT-Anlage dar und sind weder im IT-Anlagen Raum noch in benachbarten Räumen aufzustellen. Ersatzweise sollten Feuerlöscher mit Wasser, mit Wasser mit Zusätzen bzw. mit Schaum verwendet werden. Für den Einsatz in IT-Anlagen sollten CO_2-Feuerlöscher bevorzugt werden.

Quelle: Theo Gärtner, M+W Zander

Bild 4.03: Mobile CO_2-Feuerlöscher

4.1.2.5 Natürlich wirkende Rauchabzugsanlagen (NRA) sowie maschinelle Rauchabzüge (MRA)

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

Die Einrichtung und Bedienung von Rauchabzugsanlagen ist unter Berücksichtigung der anderen technischen Einrichtungen (z.B. Löschanlagen, Klimaanlage) zu regeln und mit dem für den Brandschutz Zuständigen abzustimmen. Zum Beispiel dürfen Rauch- und Wärmeabzugsanlagen in Räumen, die durch eine Gasanlage geschützt sind, nicht automatisch öffnen; diese und weitere Anforderungen können VdS 2380 Richtlinien für Planung und Einbau von Gaslöschanlagen, entnommen werden.

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 Feuerwiderstandsklassen durchdringen, sind in der entsprechenden Feuerwiderstandsklasse auszuführen.
- Es dürfen für Entrauchungsleitungen nur nichtbrennbare Baustoffe (Klasse A nach DIN 4102) verwendet werden.
- Die Rauchabzugsanlage sollte so ausgelegt werden, dass bereits während des Brandgeschehens Rauch und Heißgase abgeführt werden können.
- Öffnungen ins Freie müssen so geplant werden, dass sie gegen Einwirkungen von außen geschützt sind.

Quelle: Theo Gärtner, M+W Zander

Bild 4.04: Rauchabzug

4.1.3 Organisatorischer Brandschutz

4.1.3.1 Brandschutzordnung
Es ist eine Brandschutzordnung nach DIN 14 096 Teil B aufzustellen und für die IT-Anlage zu spezifizieren. Folgenden 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 nicht zulassen; wenn unvermeidbar, nur mit Erlaubnisschein und entsprechenden Brandschutzvorkehrungen
- 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

Weitere Hinweise hierzu sind im Anhang A "Inhalte einer Brandschutzordnung für IT-Anlagen (Muster)" aufgeführt.

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 einem Brandschutzkonzept niederzulegen. Brandschutzpläne sind ständig auf dem neuesten Stand zu halten. Der Feuerwehrplan ist der zuständigen Feuerwehr zu übergeben.

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

4.2 Schutz vor Elementarereignissen

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

4.3 Schutz vor Wasser

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

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

befinden. Ist es unvermeidlich den zentralen IT-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 Feuchtemeldern
- in den IT-Anlagen-Räumen 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 folgende Sicherheitsmaßnahmen zu treffen:

- Die Leitungen sind aus nichtrostenden und dem zu erwartenden Druck genügenden Materialien auszuführen. Schweißverbindungen sollten durch geeignete Verfahren auf Rissfreiheit geprüft werden.
- Die Leitungen sind doppelwandig auszuführen (entweder direkt oder durch nachträgliche Ummantelung).
- In der äußeren Ummantelung sind Feuchtemelder zu installieren.
- Die Meldung der Feuchtemelder ist an eine ständig besetzte, entsprechend reaktionsfähige Stelle weiterzuleiten.
- Die durch Feuchtemelder überwachten Wasserleitungen müssen durch außerhalb des IT-Bereichs angeordnete Elektroventile (stromlos geschlossen) absperrbar sein.

4.4 Einbruch- und Sabotageschutz

Der Zutritt Unbefugter zu schützenswerten IT-Anlagen, den Archiven sowie der für den störungsfreien Betrieb erforderlichen peripheren Technik (Energieversorgung, Klimatisierung, etc.) ist in geeigneter, der Bedeutung der IT-Anlagen angepasster Weise zu unterbinden. Daneben ist aber auch der geordnete Zutritt zu den und Zugriff auf die IT-Anlagen durch Befugte sicher zu stellen. Realisiert werden können diese Anforderungen durch Maßnahmen wie:

- mechanischer Einbruchschutz
- Einbruchmeldeanlage
- Zutrittskontrolle
- Passwortschutz

Das sinnvolle Zusammenwirken ist durch die Erstellung und Umsetzung eines Sicherheitskonzeptes zu gewährleisten, das die Möglichkeiten und Grenzen der einzelnen Maßnahmen berücksichtigt und sie sinnvoll miteinander kombiniert. Dieses Konzept sollte mit dem Versicherer abgestimmt werden.

4.4.1 Einbruchschutz

Es ist auf eine anonyme Lage der Räume zu achten. Das Rechenzentrum sollte daher beispielsweise nicht durch Hinweisschilder gekennzeichnet sein. Die IT-Anlagen-Räume sind vor äußeren Angriffen, deren Ziel sowohl die dort befindlichen vertrauliche Daten als auch die hochwertige Hardware sein können, geschützt – abseits öffentlicher oder stark frequentierter innerbetrieblicher Verkehrswege – einzurichten.

Umfassungswände, Fenster und Türen der IT-Anlagen sollen einen angemessen hohen mechanischen Widerstandswert aufweisen.

Hinweis: siehe VdS 2333 Sicherungsrichtlinien für Geschäfte und Betriebe

4.4.2 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 Ausführung der EMA gemäß VdS-Klasse C ist anzustreben. Die Meldungen der EMA sind zu einer ständig besetzten und entsprechend instruierten Stelle weiterzuleiten (Polizei, VdS-anerkanntes Wach- und Sicherheitsunternehmen, Leitzentrale).

Hinweis: siehe VdS 2311 Einbruchmeldeanlagen, Richtlinien für Planung und Einbau

4.4.3 Zutrittskontrolle

Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen ist zu regeln (siehe M 2.6 Vergabe von Zutrittsberechtigungen im IT-GSHB des BSI) und zu kontrollieren. Die Maßnahmen reichen dabei von einer einfachen Schlüsselvergabe bis zum elektronischen Zutrittskontrollsystem (ZKS) z.B. mit Karte und PIN.

Hinweis: Weitere Informationen zur Zutrittskontrolle können dem IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Maßnahme M 2.17 Zutrittsregelung und -kontrolle entnommen werden. Siehe auch VdS 2358 Richtlinien für Zutrittskontrollanlagen, Planung und Einbau.

4.4.4 Passwortschutz

Um den Zugriff Unbefugter auf IT-Systeme und -Anlagen zu unterbinden, ist ein Passwortschutz zu realisieren.

4.5 Technische Einrichtung

4.5.1 Elektrische Installation

Die elektrischen Installationen sind nach den anerkannten Regeln der Elektrotechnik zu errichten und zu unterhalten. Das Installationsnetz im gesamten Gebäude ist gemäß DIN VDE 0100-300 als TN-S-System auszuführen. Um den wesentlichen Vorteil des TN-S-Netzes, eine einzige zentrale Nullung in der Gebäudehauptverteilung, dauerhaft zu gewährleisten, sollte eine permanente Fehlerstromüberwachung mit Meldung der Grenzwertüberschreitung an geeigneter Stelle realisiert werden.

Zur Erhöhung der Ausfallsicherheit kann abhängig vom Schutzbedürfnis eine trassenredundante Verlegung von wichtigen Kabeln und Leitungen realisiert werden.

Hinweis: Um den besonderen Gefahren in Räumen für IT-Anlagen gerecht zu werden, sind Anforderungen und Maßnahmen nach DIN VDE 0100-482 und VdS 2033 Feuergefährdete Betriebsstätten und diesen gleichzustellende Risiken – Richtlinien zur Schadenverhütung anzuwenden. Weiterhin sind die Bestimmungen der DIN VDE 0800 einzuhalten. Grundsätzlich sollten nur halogenfreie Kabel zum Einsatz kommen. Nicht mehr benötigte Kabel müssen entfernt werden.

4.5.1.1 Leuchten
Bei der Auswahl der Leuchten und bei der Errichtung der Beleuchtungsanlagen sind DIN VDE 0100-559, VdS 2005 Elektrische Leuchten sowie VdS 2324 Niedervoltbeleuchtungsanlagen und -systeme zu beachten.

4.5.1.2 Notaus-Schalteinrichtungen
Bei einem Brand können Schäden an den betroffenen IT-Geräten in der Regel verringert werden, wenn rechtzeitig ein Spannungsfreischalten erfolgt. Zur Spannungsfreischaltung durch eine Einrichtungsüberwachung siehe Abschnitt 4.1.2.2. Handbetätigte Notaus-Schalteinrichtungen sind gegen versehentliche Betätigung und Missbrauch zu schützen.

Quelle: Theo Gärtner, M+W Zander

Bild 4.05: Notaus-Schalteinrichtung

Quelle: Bruno Hecht, Von zur Mühlen GmbH

Bild 4.06: Brandschutzklappen-Motorsteuerung

4.5.1.3 Nachrichtentechnik
Eine sichere, kabellose Übertragung von Daten und Kommunikation ist zu ermöglichen.

4.5.2 Klima-/Raumlufttechnische Anlagen

4.5.2.1 Brandschutz
Werden Räume der IT-Anlage klimatisiert, sind hierfür eigene Klimaanlagen/Raumlufttechnische Anlagen (RLT-Anlagen) vorzusehen.

Die Klimaanlage/RLT-Anlage ist nach Möglichkeit in einem feuerbeständig (F90-A nach DIN 4102) 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.

Lüftungsleitungen (Klimakanäle) sind bei Durchgang durch feuerbeständige Wände und Decken feuerbeständig (L 90 nach DIN 4102) durch die gesamten Räume zu führen oder nach Abschnitt 4.1.1.1 mit bauaufsichtlich zugelassenen Absperrvorrichtungen (z.B. Brandschutzklappen K 90 nach DIN 4102) zu sichern, die zusätzlich rauchdicht und über Rauchmelder gesteuert sind. Brandschutzklappen mit ausschließlich thermischen Auslöseelementen sind für den Einsatz in IT-Anlagen ungeeignet.

Die Lüftungsleitungen (Klimakanäle) und deren Isolierung müssen aus nichtbrennbaren Baustoffen (Klasse A nach DIN 4102) bestehen.

Hinweis: siehe VdS 2298 Brandschutz in Lüftungsanlagen, Merkblatt für den Brandschutz

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.

4.5.2.2 Dimensionierung
Die ordnungsgemäße Funktion von IT-Geräten setzt die Einhaltung von Grenzwerten der Lufttemperatur und Luftfeuchtigkeit voraus. Bei der Festlegung der Grenzwerte reicht es nicht aus, diese hart an den vom Gerätehersteller genannten Grenzwerten zu fahren. Erfahrungswerte aus vielen derartigen Fällen führen zu folgenden Empfehlungen:

- Lufttemperatur im Raum 20-23 °C (in 1,10 m Höhe über dem Doppelboden)
- Relative Luftfeuchte im Raum 45-65 %

Hinweis: Die Temperaturdifferenz zwischen Hin- und Rückluft sollte 8 Kelvin nicht überschreiten. Die Einblasetemperatur (Kaltluft) sollte 18 °C nicht unterschreiten, um einen ausreichenden Abstand zur Taupunkttemperatur zu gewährleisten.

In den Räumen für die IT-Anlagen sollte eine unabhängig von der Klimaanlage/RLT-Anlage arbeitende Überwachungseinrichtung installiert werden, von der die Klimatisierung auf die zulässigen Werte für Temperatur und Feuchtigkeit überwacht wird und die bei Überschreiten der Grenzwerte ein Alarmsignal auslöst und/oder die Klima-/RLT-Anlage und gegebenenfalls auch die IT-Anlage abschaltet. Die Alarmierung ist an eine ständig besetzte Stelle weiterzuleiten.

4.6 Schutz der Energieversorgung

Die Verfügbarkeit von IT-Systemen ist von der Verfügbarkeit der Energie- (Elektrizität, Gas, etc.) und Wasserversorgung abhängig. Dem Schutz der Energie- und Wasserversorgung ist daher mindestens genauso viel Aufmerksamkeit zu widmen, wie dem Schutz der IT-Anlagen.

4.6.1 Ausfall der VNB-Einspeisung

Ein Ausfall der Einspeisung vom Versorgungsnetzbetreiber (VNB) ist zwar relativ selten, kann aber nicht ausgeschlossen werden. Zwei Möglichkeiten gibt es, die Folgen eines solchen Ausfalls zu minimieren:

- durch eine zweite Einspeisung von einem anderen Umspannwerk aus oder
- durch Installation einer Netzersatzanlage (NEA)

In beiden Fällen muss mit einer so genannten Umschaltlücke gerechnet werden, d.h. mit einer kurzfristigen Unterbrechung der Energieversorgung. Dauert diese Umschaltlücke bei einer zweiten Einspeisung nur Bruchteile von Sekunden, muss für den Anlauf einer NEA je nach Ausführung durchaus mit mehreren Sekunden bis in den Minutenbereich gerechnet werden.

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.

Bei zwei getrennten Stromversorgungen sollten auch die Zuleitungen über zwei getrennte Trassen geführt werden.

4.6.2 Störung in der Hausinstallation

Die überwiegende Mehrzahl aller Störungen der Energieversorgung ist “hausgemacht”, Hierbei handelt es sich um Störungen durch Schalthandlungen, defekte Geräte etc. Um die Schadwirkung solcher Störungen zu vermeiden, hat sich der Einbau einer USV in nächster Nähe der wichtigsten IT-Systeme bewährt. Durch eine hochwertige USV werden nicht nur Unterbrechungen abgefangen, sondern auch andere Störungen wie Überspannungen (in gewissen Grenzen), Transienten- und Oberwellenstörungen, etc. Die Verfügbarkeit der USV ist zu überwachen.

In sich geschlossene IT-Anlagen-Bereiche (Rechenzentren, Serverparks etc.) sind über eine separate Zuleitung aus der NHV mit eigener Unterverteilung innerhalb des IT-Bereichs zu versorgen. Die Zuleitung kann bei hohen Anforderungen an die Verfügbarkeit auch als Ring ausgeführt sein. Der gesamte Leitungsweg von der Haupteinspeisung bis zur Unterverteilung im IT-Bereich, mindestens aber alle Verteiler und Schaltschränke sind durch Verschluss gegen den unbefugten Zugriff zu schützen.

Quelle: Theo Gärtner, M+W Zander

Bild 4.07: Batterieanlage

Werden kleine IT-Systeme in normalen Büroräumen betrieben, kann deren Verfügbarkeit am besten durch Beistellung einer lokalen Klein-USV gewährleistet werden. Zudem sollte der betreffende Raum über einen separaten Leitungsschutzschalter, also keinesfalls gemeinsam mit Nachbarräumen, abgesichert werden.

Es ist dafür Sorge zu tragen, dass Schäden durch Oberschwingungsspannungen und -ströme vermieden werden. Für zu treffende Schutzvorkehrungen siehe VdS 2349 Störungsarme Elektroinstallation.

Strom- und Datennetz müssen den Anforderungen des (IT-)Anlagenherstellers entsprechen.

4.7 Blitz- und Überspannungsschutz/ EMV

Für IT-Anlagen ist der Blitzschutz-Potenzialausgleich vorzusehen. Das bedeutet die Ausführung eines lückenlosen Potenzialausgleichs mit Einbeziehung aller aktiven Leiter (siehe DIN V VDE V 0185-3) durch Einbau von Ableitern Typ 1. Zum Schutz gegen Überspannung sind in IT-Anlagen Ableiter Typ 2 und Typ 3 vorzusehen. Dieser Schutz muss alle elektrisch leitenden Verbindungen (Strom-, Daten- und Versorgungsleitungen), insbesondere die Außenverbindungen, erfassen. Inwieweit der gerätenahe Überspannungsschutz (Ableiter Typ 3) noch individuell zu realisieren ist,

hängt davon ab, ob die eingesetzten IT-Geräte schon über diesen verfügen oder nicht.

In jedem Fall ist ein umfassendes Überspannungsschutzkonzept durch einen geeigneten Fachplaner, z.B. einem VdS-anerkannten EMV- Sachkundigen, zu erstellen.

Sofern Störungen durch elektromagnetische Felder, wie sie beispielsweise von Mobiltelefonen oder anderen Funkgeräten ausgehen, auftreten können, sind geeignete Maßnahmen festzulegen (z.B. Verbot von Mobiltelefonen).

Im Gebäude, in dem sich die IT-Anlagen befinden, ist ein konsequenter Potenzialausgleich durchzuführen. Die Schirmungen aller Datenleitungen, der Schutzleiter der Stromversorgung, Fundamenterder, Stahlskelette, metallische Fassadenverkleidungen, Versorgungsleitungen für Wasser, Heizung u.s.w. sind in den Potenzialausgleich zu integrieren. Der Erdungswiderstand soll gemäß DIN VDE 0185-100 klein sein.

Die Richtlinien zur Schadenverhütung VdS 2010 Risikoorientierter Blitz- und Überspannungsschutz, VdS 2031 Blitz- und Überspannungsschutz, VdS 2569 Überspannungsschutz für Elektronische Datenverarbeitungsanlagen, sowie VdS 2349 Störungsarme Elektroinstallationen, sind zu beachten.

4.8 Organisation

Technische Maßnahmen zum Schutz der IT-Anlagen können ohne einen adäquaten organisatorischen und personellen Unterbau ihre Wirkung nicht entfalten (z.B. die Alarmierung einer ständig besetzten hilfeleistenden Stelle oder die Besucherregelung). Organisatorische und planerische Maßnahmen sind im Folgenden erläutert. Bei allen Planungen sind nicht nur die aktuellen Gegebenheiten, sondern auch die absehbaren zukünftigen Entwicklungen zu berücksichtigen.

4.8.1 Personal/Schulung

Grundvoraussetzung für den ordnungsgemäßen und sicheren Betrieb der IT-Anlage ist es, dass alle damit befassten Personen von der Notwendigkeit aller ergriffenen Maßnahmen überzeugt sind, also diese akzeptieren und leben. Dieser Zustand ist durch geeignete, wiederholte Schulungs- und Motivationsveranstaltungen zu erreichen und zu erhalten.

Das für Betrieb und Sicherheit der IT-Anlage zuständige Personal ist mit großer Sorgfalt auszuwählen. Das Hauptaugenmerk sollte auf

- hohe Motivation,
- besonders gutes Fachwissen und
- große Loyalität

gelegt werden.

Hinweis: Ausführliche Informationen rund um das Thema Personal und IT-Sicherheit sind im IT-GSHB des BSI, Baustein 3.2 Personal und Maßnahmekatalog M 3 – Personal zu finden.

4.8.2 Regelwerke

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

4.8.3 Datensicherung

Entsprechend den betrieblichen Erfordernissen ist eine regelmäßige Datensicherung, mindestens nach dem Drei-Generationen-Prinzip vorzunehmen. Dabei kann, je nach Datenvolumen und Verfügbarkeitsanforderung die inkrementelle Sicherung für die kurzen Sicherungszeiträume mit der Vollsicherung für Wochen- und Monatssicherungen kombiniert werden.

Hinweis: Weitere Informationen zum Thema Datensicherung sind in M 6.13 Erstellung eines Datensicherungsplans, M 6.32 Regelmäßige Datensicherung im IT-GSHB des BSI zu finden.

4.8.4 Sichere Aufbewahrung von Datenträgern

Sicherungsdatenträger sowie alle nicht im laufenden Betrieb erforderlichen sonstigen Datenträger sind gegen Brand und unbefugten Zugriff ge-

schützt zu verwahren. Dies kann entweder in einem separaten Datenschutzarchiv in einem anderen Komplex geschehen oder im Falle kurzzeitiger Lagerung durch Unterbringung der Datenträger in einem Datensicherungsschrank, mindestens der Güteklasse S 120 DIS nach VDMA-Einheitsblatt 24 991. Sinngemäß ist bei einer aktiven Datenspiegelung (Disc-Arrays, RAID-Systeme) zu verfahren.

4.8.5 Dokumentation

Die Dokumentation aller technischer Einrichtungen, besonders die von Einrichtungen der IT-Sicherheit, stellt die Grundlage sowohl für den ordnungsgemäßen Betrieb als auch für eine rasche Fehlerbehebung dar. Sie ist – soweit dort geregelt – **DIN-gerecht** auszuführen und ständig aktuell zu halten.

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

Folgende Unterlagen sollen in der Dokumentation enthalten sein (ohne Anspruch auf Vollständigkeit oder Ausschließlichkeit!):

- Gebäudepläne
  - Lageplan (Betriebsgelände)
  - alle Architekten- und Ausführungspläne
  - Grundriss/Geschossplan/Raumbelegungsplan
  - Plan der flüssigkeitsführenden Systeme in/über den IT-Anlage-Bereichen
  - Wasser-Rückhaltekonzept
- Elektropläne zu
  - Energieversorgung
  - Überspannungsschutz
  - Potentialausgleich
  - Blitzschutz
  - sowie Stromlaufpläne
- Brandschutzkonzept
  - Brandschutzplan/Brandschutzordnung
- Netzpläne
  - Energie und Daten
  - Pläne aller Trassen (Energie und Daten)
  - Datenflussschema
  - Spezifikationen der Datenleitungen
- Sicherheitstechnik
  - Einbruchmeldeanlage
  - Brandmeldeanlage
  - Zutrittskontrollsystem
- Notfallplanung
  - Notruflisten
  - Lieferanten-Listen

Alle vorhandenen Einrichtungen und Installationen sowie die zur Schadenverhütung durchgeführten Maßnahmen sind zu dokumentieren. Die Dokumentation ist bei Erweiterungen und Umbauten entsprechend zu ergänzen bzw. anzupassen.

Es ist dringend geboten, derartige Unterlagen bereits bei der Planung der IT-Anlagen zu erstellen.

Anhang A – Hinweise zur Erstellung einer Brandschutzordnung für IT-Anlagen

A.1 Brandlasten

Die Mengen an brennbaren Materialien sind auf ein Minimum zu beschränken.

Unterlagen in Papierform sind auf das unbedingt notwendige Maß zu beschränken und in den Rechnerräumen in Blechschränken aufzubewahren.

Brennbare Flüssigkeiten sollten nach Möglichkeit durch nichtbrennbare Ersatzstoffe ausgetauscht werden. Sie sind in unzerbrechlichen, auslaufgeschützten Gefäßen aufzubewahren.

Die Lagerung von IT-Geräten in der Verpackung ist innerhalb der IT-Räume nicht zulässig.

A.2 Verhalten im Brandfall

Die Regeln für die Brandverhütung und das Verhalten im Brandfall sind in dem Teil der Brandschutzordnung, der für die IT-Anlage gilt, niedergelegt.

Der für die IT-Anlagen zuständige Vorgesetzte sollte Anweisungen über besondere Maßnahmen im Brandfall erteilen und seine Mitarbeiter vor Aufnahme des Arbeitsverhältnisses sowie regelmäßig darüber informieren.

Ein Schwerpunkt betrieblicher Brandschutzmaßnahmen liegt in der Unterweisung der Mitarbeiter, im Verhalten bei Ausbruch eines Brandes. Sie müssen in der sicheren Handhabung der vorhandenen Löschgeräte, als auch in den durchzuführenden Maßnahmen wie Abschaltungen, Sicherungsmaßnahmen, Brandmeldung etc. geschult werden. Diese Schulungen sind regelmäßig jährlich für alle, bzw. bei Neueinstellungen vorzunehmen. Die Unterweisung ist zu dokumentieren.

A.3 Montage und Installationsarbeiten

Bei Installationsarbeiten sowie während der Montage der Informationstechnik als auch nach der Fertigstellung muss auf Ordnung und Sauberkeit, Vermeiden von Ansammlungen brennbarer Stoffe, Einhaltung des Rauchverbots und Ausschluss von anderen Zündmöglichkeiten geachtet werden.

A.4 Feuergefährliche Arbeiten

Feuergefährliche Arbeiten sind grundsätzlich zu verbieten. Sind in Ausnahmefällen jedoch solche Arbeiten nicht zu vermeiden, sind besondere Schutzvorkehrungen zu treffen. Feuergefährliche Arbeiten müssen schriftlich genehmigt werden. Im Erlaubnisschein für feuergefährliche Arbeiten (siehe VdS 2036, Muster für einen “Erlaubnisschein für feuergefährliche Arbeiten”) sind die durchzuführenden Schutzmaßnahmen festzulegen und die Verantwortlichen zu benennen.

A.5 Fremdfirmen

Arbeitsmaßnahmen durch Fremdfirmen können mit besonderen Brandgefahren für einen Betrieb verbunden sein. Deshalb sind neben den einschlägigen Sicherheitsvorschriften und Richtlinien ggf. weitere schriftliche Verhaltensregeln (Sicherheitsanweisungen) erforderlich. Wichtig ist, dass die Mitarbeiter von Fremdfirmen über die betrieblichen Besonderheiten belehrt werden. Fremdfirmen sollten bei der Auftragserteilung schriftlich verpflichtet werden, die Sicherheitsvorschriften des Betriebes, z.B. die Brandschutzordnung einzuhalten. Die Repräsentanten der Firmen vor Ort sind verantwortlich, ihre Mitarbeiter über die im jeweiligen Betrieb notwendigen Schutzmaßnahmen zu unterweisen.

A.6 Sauberkeit und Ordnung

In der gesamten IT-Anlage ist besonders auf Sauberkeit und Ordnung zu achten. Abfälle sind spätesten bei Schichtende aus den Räumen der IT-Anlage zu entfernen und ordnungsgemäß zu entsorgen.

Es sind geschlossene nichtbrennbare Abfallbehälter mit selbstschließendem Deckel aufzustellen. Wenn möglich sollte das außerhalb der Räume der IT-Anlage geschehen oder in einem brandschutztechnisch abgetrennten Bereich.

A.7 Zündquellen

Im Rechenzentrum muss ein absolut striktes Verbot von Feuer und offenem Licht gelten. Das schließt selbstverständlich ein Rauchverbot ein, sollte aber trotzdem gesondert betont werden. Dieses Verbot muss auf seine Einhaltung kontrolliert, Verstöße müssen geahndet werden.

Bei Bedarf ist ein eigener, feuerbeständig abgetrennter Raucher- bzw. Pausenbereich einzurichten.

A.8 Private elektrische Geräte

Aus brandschutztechnischen Gründen sollte der Gebrauch privater elektrischer Geräte in den Räume der IT-Anlage grundsätzlich nicht erlaubt werden. In schriftlich zu genehmigenden Ausnahmefällen sollten diese Geräte zuvor einer Sicherheitsüberprüfung unterzogen und in die regelmäßig wiederkehrende Überprüfung aller Geräte mit einbezogen werden.

Anhang B – Zutrittskontrolle, Hinweise zur Ausführung/Umsetzung

Für eine Zutrittsregelung und -kontrolle ist es erforderlich, dass

- der von der Regelung betroffene Bereich eindeutig bestimmt wird,
- die Zahl der zutrittsberechtigten Personen auf ein Mindestmaß reduziert wird; diese Personen sollen gegenseitig ihre Berechtigung kennen, um Unberechtigte als solche erkennen zu können,
- der Zutritt anderer Personen (Besucher) erst nach vorheriger Prüfung der Notwendigkeit erfolgt,
- erteilte Zutrittsberechtigungen dokumentiert werden.

Um ein kontrolliertes Verlassen des IT-Bereiches sicherzustellen, ist dabei ebenfalls die Betätigung des Kartenlesers vorzuschreiben.

Die Einhaltung bzw. Überschreitung von Rechten ist nach dem Grundsatz zu kontrollieren, dass einfache und praktikable Lösungen oft ebenso effizient sind wie aufwendige Technik:

- Information und Sensibilisierung der Berechtigten
- Bekanntgabe von Berechtigungsänderungen
- sichtbares Tragen von Hausausweisen, ggf. Vergabe von Besucherausweisen
- Begleitung von Besuchern
- Verhaltensregelungen bei erkannter Berechtigungsüberschreitung
- Einschränkung des ungehinderten Zutritts für nicht Zutrittsberechtigte (z.B. Tür mit Blindknauf, Schloss für Berechtigte mit Schlüssel, Klingel mit (Video-)Gegensprechanlage für Besucher)

Moderne ZKS bieten die Möglichkeit, eine Vielzahl von Meldungen über Betriebszustände, Bedienung und Fehlbedienung zu erzeugen. Die Meldungen lassen sich grob in drei Kategorien fassen:

- Alarmmeldungen
- Störmeldungen
- statistische Meldungen

Auf Alarmmeldung soll umgehend mit aller Konsequenz reagiert werden. Es ist daher ratsam, die Zahl der zu einer Alarmmeldung führenden Ereignisse so gering wie möglich zu halten. Hierzu gehören vornehmlich die Verwendung einer wegen Verlust oder Diebstahl gesperrten Zutrittsberechtigung und der unberechtigte Zugriff auf Einrichtungen des ZKS.

Störmeldungen zeigen Ereignisse und Betriebszustände an, die, wenn sie erst in absehbarer Zeit, nicht aber sofort, zu einer relevanten Verminderung der Sicherheit führen. Störmeldungen sind ihrer Bedeutung entsprechend abgestuft anzuzeigen. So sollten Versuche eigentlich Berechtigter außerhalb ihrer räumlichen oder zeitlichen Berechtigung Zutritt zu erlangen nur angezeigt werden, wenn sich solche Versuche bei bestimmten Türen oder Personen häufen. Das erfolglose Zutrittbegehren selbst führt schließlich zu keiner direkten Beeinträchtigung der Sicherheit.

Statistische Meldungen bieten Informationen, die regelmäßig oder aus besonderen Anlass nachträglich abgerufen werden können. Sie werden nicht selbsttätig angezeigt.

Anhang C – Checkliste

Nachfolgend ist als Muster eine Checkliste für Stichpunktkontrollen dargestellt.

	Ja	Nein	Nicht zutreffend
Bauliche Gegebenheiten			
Bei einstöckigen Gebäuden bzw. Räumen direkt unter der Bedachung: Oberflächenschutz in Ordnung (z.B. Bekiesung noch flächendeckend, Dacheinläufe frei von Verstopfung)?			
Es sind keine Undichtigkeiten an flüssigkeitsführenden Leitungen und keine Flüssigkeitsspuren erkennbar			
Wassermelder sind funktionsbereit			
Ordnung und Sauberkeit/Organisation			
Die Flure sind frei von Möbeln und sonstigen Gegenständen			
Abfall und Verpackungsreste werden regelmäßig beseitigt			
Das Rauchverbot wird eingehalten; in Raucherzonen befinden sich geeignete Aschenbecher			
Brandschutzübungen wurden durchgeführt			
Es befinden sich keine privaten Elektrogeräte in den IT-Räumen			
Lager			
Die vorgeschriebenen Lagerhöhen sind eingehalten			
Gänge zwischen den Regalen sind frei zugänglich			
Der Abstand zwischen Lagergut und Lampen, Heizgeräten etc. ist ausreichend			
Brennbare Flüssigkeiten sind in Sicherheitsbehältern gelagert			
Elektrische Anlage/Blitz- und Überspannungsschutz			
Elektrische Verteiler, Schaltanlagen, Batterieladestationen sind im Umkreis von 2,5 m frei von Brandlast			
Es sind nur zugelassene Geräte in Betrieb			
Vorgeschriebene Prüfungen der Blitz- und Überspannungsschutzanlage wurden durchgeführt			
Brand- und Rauchschutztüren			
Die Türen sind funktionstüchtig (einwandfreier Schließmechanismus, nicht unterkeilt etc.)			
Türen sind frei zugänglich (nicht versperrt, z.B. durch Lagergüter)			
Öffnungen in Brandabschnittswänden und Decken			
Sind alle Kabel- und Rohrdurchführungen mit zugelassenen Schottungen abgedichtet?			
Sind Durchführungen im Baustellenbereich provisorisch abgedichtet?			
Handlöschausrüstung			
Alle Feuerlöscher und Wandhydranten sind frei zugänglich			
Handfeuerlöscher befinden sich am vorgesehenen Ort und tragen eine gültige Prüfplakette			

	Ja	Nein	Nicht zutreffend
Feuergefährliche Arbeiten			
Das Erlaubnisscheinverfahren für feuergefährliche Arbeiten wurde immer angewendet			
Brandmelde- und Feuerlöschanlagen			
Wurden die regelmäßigen Wartungs- und Inspektionsarbeiten durchgeführt?			
Die Anlagen sind funktionstüchtig; es sind keine Melder abgeschaltet			
Alarmierung/Notrufe			
Das Notruftelefon funktioniert			
Das elektro-akustische Notfallwarnsystem ist einsatzbereit			
Notrufe können über vorhandene Sprechanlagen (z.B. in Fahrstühlen) abgesetzt werden			
Notfallorganisation			
Notruflisten und Notfallpläne sind aktuell			
Notfallanweisungen für Empfang und Werkschutz/Sicherheitsunternehmen sind aktuell			
Sicherheitseinrichtungen			
Zutrittsrechte sind dokumentiert. Es bestehen keine unnötigen Zutrittsrechte. Zutrittsrechte werden regelmäßig überprüft			
Nach Arbeiten durch externe Kräfte wurden offengelegte Passwörter ersetzt			
Die zum geschützten Bereich ausgegebenen Schlüssel sind dokumentiert, Reserveschlüssel werden sicher verwahrt und es ist kein Verlust bekannt			

Durchgeführt am:_____

Unterschrift:_____

Weitergeleitet am:_____

Hinweis: Detaillierte Checklisten sind in VdS 2000 Brandschutz im Betrieb aufgeführt.

Anhang D – Literatur/Quellen

D.1 Gesetze und Verordnungen, behördliche Richtlinien und Empfehlungen

IT Grundschutzhandbuch des BSI
Bundesamt für Sicherheit in der Informationstechnik
www.bsi.de

Bundesanzeiger Verlagsges.mbH, Köln
Postfach 100534, 50455 Köln
Internet: www.bundesanzeiger.de

BGR 133 Ausrüstung von Arbeitsstätten mit Feuerlöschern

BGV A8 Sicherheits- und Gesundheitsschutzkennzeichnung am Arbeitsplatz

Carl Heymanns Verlag KG
Luxemburger Str. 449, 50939 Köln
Internet: www.heymanns.com

D.2 Normen

DIN 4102 Brandverhalten von Baustoffen und Bauteilen
- 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 Feuer widerstandsfähige 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

Beuth Verlag GmbH
Burggrafenstraße 6
10787 Berlin
Internet: www.beuth.de

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

VDE-Verlag GmbH Berlin – Offenbach
Bismarkstr. 33, 10625 Berlin
Internet: www.vde-verlag.de
oder
Beuth Verlag GmbH
Burggrafenstraße 6
10787 Berlin
Internet: www.beuth.de

VDI 2054 Raumlufttechnische Anlagen für Datenverarbeitung

VDMA 24 991 Prüfbedingungen für das Brandverhalten von Stahlschränken und sonstigen Behältern

Beuth Verlag GmbH
Burggrafenstraße 6
10787 Berlin
Internet: www.beuth.de

D.3 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 2025 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 CO_2-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

Herausgeber: Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV)

Verlag: VdS Schadenverhütung GmbH • Amsterdamer Str. 174 • D-50735 Köln
Telefon: (0221) 77 66 - 0 • Fax: (0221) 77 66 - 341