

Sicherheit nach den Regeln der Technik für die IT

In diesem Dokument werden die Anforderungen an die technische Infrastruktur für IT/DV-Räume, an die Sicherheitseinrichtungen, und insbesondere an den Brandschutz für einen generellen Überblick zusammengefasst.



Architect of an Open World™

WHITE PAPER

1.	Einleitung	4
1.	Ausgangslage	5
2.	Raumstrukturen.....	6
3.	Bundesamt für Sicherheit in der Informationstechnik	7
4.	Maßnahmenbetrachtungen	10
5.	Brandschutzkonzepte	12
6.	Brand-, Rauchschutz	14
7.	Zutrittskontrolle.....	16
8.	Energieversorgung.....	17
9.	Klimatisierung	19
10.	Gefahrenmeldeanlagen	22
11.	Hinweise	25

Über Bull – Architect of an Open World™

Als einziges europäisches IT-Unternehmen bietet Bull Lösungen für die gesamte IT-Wertschöpfungskette eines Unternehmens. Wir unterstützen weltweit öffentliche und privatwirtschaftliche Kunden dabei, ihre IT-Systeme zu planen, zu optimieren und zu betreiben. Unsere Expertise liegt in der Modernisierung und Entwicklung von Informationssystemen auf Basis offener, flexibler und sicherer Lösungen, die Energie- und Kosteneffizienz in Einklang bringen.

Bull hat eine starke Präsenz in der Industrie, der Finanz- und Telekommunikationsbranche, der Öffentlichen Verwaltung und anderen Branchen. Das Vertriebsnetz von Bull und seinen Geschäftspartnern erstreckt sich weltweit auf über 50 Länder. 2008 erwirtschaftete die Bull-Gruppe mit ca. 8.000 Mitarbeitern einen Umsatz von 1,13 Milliarden Euro. Im Jahr 2009 haben wir im Rahmen des JUROPA-Projekts des Forschungszentrum Jülich einen der schnellsten Supercomputer weltweit geliefert; er belegt Platz 10 der Top500-Liste im Juni 2009.

Die Bull GmbH ist die deutsche Vertriebs- und Service-Niederlassung der Bull-Gruppe mit Hauptsitz in Köln. Nach der Übernahme des Tübinger IT-Dienstleisters für anspruchsvolle Rechnerumgebungen, der science+computing ag, im Jahr 2008 bieten wir nun mit rund 500 Mitarbeitern in Deutschland unseren Kunden ein bundesweit agierendes, flächendeckendes Service-Netzwerk und Dienstleistungen, die auf den Bedarf der Kunden zugeschnitten sind. Schwerpunkte der Geschäftstätigkeit von Bull sind – neben dem Vertrieb von Server- und Speicherlösungen – Data Center Services, Green IT, Virtualisierung, Outtasking, IT-Betriebsunterstützung und High Performance Computing.

Weitere Informationen erhalten Sie unter: <http://www.bull.de>

1. Einleitung

In diesem Dokument werden die Anforderungen an die technische Infrastruktur für IT/DV-Räume, an die Sicherheitseinrichtungen, und insbesondere an den Brandschutz für einen generellen Überblick zusammengefasst.

Bei Nichtbeachtung von Anforderungen „nach den Regeln der Technik“ droht unter Umständen ein Unternehmensschaden aber auch der Wegfall des Versicherungsschutzes im Schadenfall und/oder eine drastische Erhöhung der Versicherungsbeiträge, insbesondere bei Betriebsunterbrechungs-Versicherungen.

Schadensfälle, die die Verfügbarkeit der Unternehmensdaten und/oder der Informationsverarbeitung (IT) bedrohen können, sind unbedingt zu vermeiden und beherrschbar zu gestalten, um die Betriebsprozesse jederzeit sicherzustellen.

Bei der betriebswirtschaftlichen Kostenbetrachtung für die „IT-Verfügbarkeit“ sind die Kosten einer „nicht Verfügbarkeit der IT“ gegenüber zu stellen.

Anfragen - Zusatzinformationen: „Herstellerneutrale Bull-Dienstleistungen“

→ rz-bau@bull → Data Center Services

→ audit@bull → (Security Audit, BS ISO/IEC 17799, 27001, Ready for Certification)

→ alive@bull → (Business Continuity Management)

Hinweis: Bull ist aktiv im BITKOM-Arbeitskreis Betriebssicheres Rechenzentrum & Infrastruktur tätig.

Weitere Informationen: www.bitkom.org/de/publikationen/38337_42509.aspx

2. Ausgangslage

Viele Unternehmen verfügen über Hochverfügbarkeitssysteme, um die Anwendungen und Daten sowie die Verbindungen im und außerhalb des Unternehmens sicher bereitzustellen. Um die Verfügbarkeit zu steigern werden Baugruppen dieser Systeme redundant ausgelegt, Daten gespiegelt und infrastrukturelle Maßnahmen in den Netzwerkkomponenten ergriffen.

Ein Serverraum zum Beispiel dient zur Unterbringung eines oder mehrerer Server sowie server-spezifischer Unterlagen. Darüber hinaus können dort auch Datenträger sowie zusätzliche Hardware, wie etwa Protokolldrucker oder aber auch Infrastruktur wie z.B. Klimatechnik, vorhanden sein.

Im Serverraum ist häufig kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten. Zu beachten ist jedoch, dass im Serverraum aufgrund der Konzentration von IT/Kommunikations-Systemen und Daten ein deutlich höherer Schaden eintreten kann als beispielsweise in einem Büroraum.

Für den Schutz von Serverräumen sind die vielen erforderlichen, entsprechenden baulichen und infrastrukturellen Maßnahmen zur Anwendung und Realisierung zu bringen.

Besondere Beachtung ist dabei folgenden Maßnahmen zu widmen:

- Baulicher Brandschutz, Raumbeschaffenheit
- Vermeidung von Wasserführenden Leitungen und Fenstern
- Branddetektionseinrichtungen, automatische / manuelle Brandbekämpfungseinrichtungen und geeignete Handfeuerlöscher
- mindestens n+1 redundante Klimatisierung
- mindestens n+1 redundante Stromversorgung unterbrechungsfrei mittels Online-USV
- Brandlastarme Energieverteilung mittels Stromschienensystem
- Überspannungsschutz (Innerer Blitzschutz)
- Not-Aus-Schalter
- Raumebelegung unter Berücksichtigung von Brandlasten
- Einbruchmeldeeinrichtungen
- Zutrittskontrolle
- Beaufsichtigung oder Begleitung von Fremdpersonen
- Selbstschließende Sicherheitstüren
- Alarmierungsanlage und Alarmorganisation als zentrale Sammelstelle für alle Vorkommnisse in der technischen Infrastruktur mit deren automatischen Weiterleitung von Informationen und Störungen an Bereitschaftsdienste,

um hier nur die Wesentlichsten aufzuzeigen.

3. Raumstrukturen

Doch sehr oft ist es um die Räumlichkeiten und deren technischer Infrastruktur, in denen diese System untergebracht sind, schlecht bestellt. Viele Serverräume, DataCenter, IT-/DV- und Telephonie-Installationsräume weisen elementare Versäumnisse hinsichtlich des Baukörpers, der Räumlichkeiten als solches, deren infrastrukturelle Ausstattung und insbesondere des vorbeugenden Brandschutzes, der schnellen Brandbekämpfung im Schadensfall und der sonstigen erforderlichen Sicherheitseinrichtungen auf.

Die Versäumnisse beruhen in den meisten Fällen nicht wie zu vermuten nur auf wirtschaftlichen Zwängen, sondern oft einfach - oder gerade deshalb - auf der Komplexität der Materie. Zunehmend reagieren auch die Versicherer auf diese Umstände und fordern zwingend die Anpassung der Sicherheitseinrichtungen und des Brandschutzes an die allgemein anerkannten Regeln der Technik und des Datenschutzes. Bei Nichtbeachtung droht der Wegfall des Versicherungsschutzes und/oder eine drastische Erhöhung der Beiträge. Dabei ist es deutlich aufwändiger, ein bestehendes Umfeld mit den entsprechenden baulichen Maßnahmen an die Sicherheitsansprüche anzupassen, als einen Neubau von vornherein nach den Vorgaben zu planen und zu realisieren.

Generell wird jedoch immer ein Sicherheitsprofil für das Rechenzentrum (RZ) und die IT-Umgebung benötigt. Aus Kostengründen gilt hier: „so viel wie nötig, so wenig wie möglich“. Wir als Berater haben in dieser Dokumentation einen Sicherheitsanspruch in Anlehnung an die Regeln der Technik für unseren Kunden als Betreiber angenommen und aus dieser Annahme und dem daraus resultierenden Schutzziel die erforderlichen Maßnahmen dargestellt. In unseren Projekten werden die Maßnahmen zur Risikominimierung in der Planungsphase mit dem Kunden bzw. mit dem Interessenten abgestimmt. Auch die Nachteile (Grundschutz?) und die neusten Anforderungen – Sicherung von IT und Infrastrukturen nach Stand der Technik – bezogen auf eine bauliche RZ-Lösung werden, wenn erforderlich besprochen.

Die Vorteile für geprüfte und zertifizierte Lösungen werden gegenübergestellt und erklärt.

4. Bundesamt für Sicherheit in der Informationstechnik

Das BSI (Bundesamt für Sicherheit in der Informationstechnik) gibt hier zum „Stand der Technik“ einen 60-Punkte „Maßnahmenkatalog Infrastruktur“ - den wir hier kurz zur Information und der Vollständigkeit halber (siehe www.bsi.de) auflisten möchten:

- 01 Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
- 02 Regelungen für Zutritt zu Verteilern
- 03 Angepasste Aufteilung der Stromkreise
- 04 Blitzschutzeinrichtungen
- 05 Galvanische Trennung von Außenleitungen
- 06 Einhaltung von Brandschutzvorschriften
- 07 Handfeuerlöscher
- 08 Raumbelagung unter Berücksichtigung von Brandlasten
- 09 Brandabschottung von Trassen
- 10 Verwendung von Sicherheitstüren und -fenstern
- 11 Lagepläne der Versorgungsleitungen
- 12 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
- 13 Anordnung schützenswerter Gebäudeteile
- 14 Selbsttätige Entwässerung
- 15 Geschlossene Fenster und Türen
- 16 Geeignete Standortauswahl
- 17 Pförtnerdienst
- 18 Gefahrenmeldeanlage
- 19 Einbruchschutz
- 20 Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht
- 21 Ausreichende Trassendimensionierung
- 22 Materielle Sicherung von Leitungen und Verteilern
- 23 Abgeschlossene Türen
- 24 Vermeidung von wasserführenden Leitungen

- 25 Überspannungsschutz
- 26 Not-Aus-Schalter
- 27 Klimatisierung
- 28 Lokale unterbrechungsfreie Stromversorgung
- 29 Geeignete Aufstellung eines IT-Systems
- 30 Absicherung der Datenträger mit TK-Gebührendaten
- 31 Fernanzeige von Störungen
- 32 Geeignete Aufstellung von Konsole, Geräten mit austauschbaren Datenträgern und Druckern
- 33 Geeignete Aufbewahrung tragbarer PCs bei mobilem Einsatz
- 34 Geeignete Aufbewahrung tragbarer PCs im stationären Einsatz
- 35 Sammelaufbewahrung mehrerer tragbarer PCs
- 36 Sichere Aufbewahrung der Datenträger vor und nach Versand
- 37 Geeignete Aufstellung eines Faxgerätes
- 38 Geeignete Aufstellung eines Modems
- 39 Verhinderung von Ausgleichsströmen auf Schirmungen
- 40 Geeignete Aufstellung von Schutzschranken
- 41 Schutz gegen elektromagnetische Einstrahlung
- 42 Gesicherte Aufstellung von Novell Netware Servern
- 43 Gesicherte Aufstellung von ISDN-Routern
- 44 Geeignete Einrichtung eines häuslichen Arbeitsplatzes
- 45 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
- 46 Einsatz von Diebstahl-Sicherungen
- 47 Eigener Brandabschnitt oder Brandabschnitte
- 48 Brandmeldeanlage
- 49 Technische und organisatorische Vorgaben für das Rechenzentrum
- 50 Rauchschutz
- 51 Brandlastreduzierung
- 52 Redundanzen in der technischen Infrastruktur
- 53 Videoüberwachung
- 54 Brandfrüherkennung / Löschtechnik

- 55 Perimeterschutz
- 56 Sekundär-Energieversorgung
- 57 Aktuelle Infrastruktur- und Baupläne
- 58 Technische und organisatorische Vorgaben für Serverräume
- 59 Geeignete Aufstellung von Archivsystemen
- 60 Geeignete Lagerung von Archivmedien

5. Maßnahmenbetrachtungen

Auf die wichtigsten infrastrukturellen Bereiche wollen wir in diesem Dokument näher eingehen, um unseren Kunden und Interessenten die Einschätzung – „was gehört zum Stand der Technik“ nach der allgemeinen Auffassung näher zu bringen und damit besser in der Lage zu sein, Entscheidungen zu Gunsten oder Verzicht einer Maßnahme zu treffen.

Bei der Betrachtung dieser gesamten Maßnahmen bzw. bei der Erstellung des Sicherheitsprofils und in Folge die Abwägung, welche Maßnahmen aus Kostengründen durchgeführt werden und welche nicht, ist ein wesentlicher Punkt, dass der Betreiber, zum Beispiel beim „Streichen“ einer Maßnahme ein klares Bild von dem verbleibenden Restrisiko hat. Nur damit kann er es realistisch einschätzen und als für ihn, bzw. für sein Unternehmen vertretbar erklären. Denn für das vertretbare Restrisiko übernimmt letztlich immer die Geschäftsleitung die Verantwortung – auch gegenüber dem Gesetzgeber und in Haftungsfragen bei Schadensfällen.

Individuelle Betrachtungen und Einschätzungen die das gesamte Umfeld betreffend, wie negative Einflüsse auf den generellen Standort, wie z.B. Flugverkehr, elektromagnetische Strahlung durch Hochspannungsleistungen, Eisenbahnlinien, Kraftwerke, Betriebe mit hohem Schadstoffausstoß und gefährlichen Stoffen sowie andere Negativeinflussbetrachtungen sind notwendig.

Grundsätzlich sind in IT- und Serverräumen weitgehend nichtbrennbare Baustoffe einzusetzen, die keine oder eine nur geringe Brandlast bilden. Ist das nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, ist zwingend darauf zu achten, dass nur PVC-freie Materialien, die zudem selbstverlöschend sein sollten, zur Anwendung kommen. Diese sind möglichst in feuerbeständigen Kanälen zu führen. PVC ist wegen seines Chloridanteils ungeeignet! Bei PVC-Materialien entsteht im Brandfall hochgiftiges Chlorgas, das sich mit der Luftfeuchte oder z.B. mit Löschwasser zu Salzsäure verbindet. Der Schaden, der durch diese korrosiven Rauchgase entsteht, ist in der Regel um ein Vielfaches höher als der eigentliche Brandschaden. Von der Gefährdung beim Einatmen einmal abgesehen, sind die Schäden an Datenträgern oder der gesamten Hardware meistens irreparabel. Ein Kilogramm PVC kann mehrere tausend Kubikmeter Luft verunreinigen. Mittlerweile bieten Hersteller von passiven Netzwerkkomponenten, Kabelbühnen, Schwach- und Starkstrommaterialien wie auch Schalter, Leerrohre und Installationsgeräte fast durchgängig Produkte auch in halogenfreier Qualität an. Dieses gilt auch für Patch-Kabel und Befestigungsmaterialien.

Häufig lässt sich PVC, auch bei einer bewusster Planung nicht gänzlich verhindern. Deshalb sollte das RZ so geplant sein, dass die Ausbreitung korrosiver Gase im Brandfall erschwert oder verhindert wird. Hierzu eignen sich Feuerschutztüren in entsprechender Qualität, mit gasdichten Eigenschaften. Dadurch wird auch das Eindringen von schädlichen Gasen von außen verhindert, als auch beim automatischen Betrieb einer Gaslöschanlage zur Brandbekämpfung im Raum die Erhaltung der Löschkonzentration gewährleistet. Die Empfehlung ist also immer die Verwendung von rauchgas-dichten Türen.

Für den Brandschutz ist ebenfalls elementar die Betrachtung der Räumlichkeiten, die an die IT-Räume angrenzen. Häufig ist die Situation so, dass Kucheneinrichtungen oder Lagerräume mit ihren erheblichen Brandlasten und Gefährdungspotenzialen direkt an das Rechenzentrum angrenzen.

Auch wenn die Nebenräume keine gefährliche Nutzung aufweisen, sollten sie über Sensoren zur Erfassung und Alarmierung von Wasser- oder Brandschäden verfügen. Generell sollten Rechenzentren und artverwandte Räume grundsätzlich als separate Brandabschnitte konzipiert sein, um die Auswirkungen von Bränden in benachbarten Bereichen zu minimieren. Bei größeren Anlagen empfiehlt es sich sogar, die einzelnen Bereiche wie Serverraum, LAN-Knoten, USV- und Technikräume in weitere Brandabschnitte zu unterteilen, um so die Schadensausweitung bei einem Brand innerhalb des Zentrums in Grenzen zu halten. Große Bedeutung kommt hierbei den vorgeschrie-

benen Brandschottungen zu.

Es lässt sich nicht immer vermeiden, dass Installationen (Elektro- und Schwachstromleitungen, Klimaversorgungsleitungen, Netzwerk- und Glasfaserkabel, usw.) einzelne Brandabschnitte durchqueren. Hierzu sind Durchbrüche durch Brandschutzmauern mit Schottungen bauamtlich erforderlich, die ein zertifizierter Fachbetrieb ausführen muss. Diese Schottungen verhindern ein Ausbreiten von Bränden und Rauchgasen. Sie sollten nur aus hierfür zugelassenem Material bestehen und zudem reversierbar sein, damit der IT-Raum modifizierbar und ausbaubar bleibt.

Wir empfehlen, wo immer technisch möglich, ausschließlich wiederöffnbare, geschraubte und für den jeweiligen Verwendungszweck und Einbau (Mauer, Metallwand, etc.) zugelassene Brandschotte. Diese Brandschotte umhüllen mit ihrem Innenleben jedes einzelne Kabel mit jeweils für dieses Kabel speziell vorhandene Modulbauteil und werden dann verschraubt. Somit ist eine Nachverkabelung ohne großen Aufwand und ohne Sicherheitsrisiko möglich.

Darüber hinaus ist es zweckmäßig, die Leitungen, egal ob im Boden oder an der Decke auf speziellen Trassen zu führen. Das verschafft Überblick und gewährleistet eine sichere Führung. Zudem sollten möglichst wenige Leitungen aus dem RZ heraus führen und ungenutzte Kabel immer entfernt werden, um mehr Übersicht zu erhalten und um möglichst wenig Brandlast zu erzeugen.

Für die Schadensverhütung und Minimierung ist es entscheidend, die Brandlast in den sensiblen Bereichen möglichst gering zu halten. Das heißt, im IT-Raum sollten wenig brennbare Materialien vorhanden sein. Diese setzen bei einem Brand Energie frei, mit der sie erheblich zum Brandverlauf beitragen und ihn sogar entfachen und weiterleiten können. Deshalb haben Kaffeemaschinen, Altgeräte, Verpackungsmaterialien, Druckerpapierlagerungen, Schallschutzverkleidungen aus Schaumstoff, brennbare Flüssigkeiten und Ähnliches in diesem Umfeld nichts zu suchen.

Nicht nur wegen ihrer wirtschaftlichen Bedeutung, sondern auch aufgrund der, trotz aller wie vor genannten Vorkehrungen und möglichen Brandlastreduzierungen, immer noch im Bereich der eigentlichen Installation hohe Brandlasten vorhanden sind, stehen Netznotenpunkte sowie Datenverarbeitungsanlagen im Mittelpunkt der Schutzkonzepte. Diese Anlagen mit ihren umfangreichen elektrischen Installationen bergen stets die Gefahr eines technischen Defekts. Die hohe Kabeldichte in Doppelböden, Kabeltrassen oder Zwischendecken stellt in sich bei stromführenden Kabeln ein weiteres Risiko dar. Deshalb empfehlen wir immer zur Versorgung der elektrischen Energie an die Verbraucher ein Stromschienensystem, welches diese Risiken abermals minimiert. Ein Schwelbrand, der nicht frühzeitig erkannt und gelöscht wird, findet hier ausreichend Nahrung, um sich ungestört weiter auszubreiten.

Erschwerend kommt oft hinzu, dass sich Stromversorgungseinheiten, Schaltschränke und Rechneranlagen an einem Ort bündeln und den Raum zusätzlich aufheizen. Die Liste der typischen Brandursachen ist entsprechend lang: „Defekte Computerplatinen oder Netzteile, lose Klemmverbindungen, überlastete, fehlerhafte oder beschädigte Kabel, defekte Monitore sowie durch Menschen unbemerkt verursachte Brände, wie Phasenüberlast und Unterverteiler in den Rechnerräumen“ – auch ein sträfliches Vergehen, denn hierdurch wird das Brandrisiko erheblich erhöht – daher auch hier wieder unsere Empfehlung zum Stromschienensystem.

Wird ein Brand erst dann erkannt, wenn er sich bereits zum offenen Feuer entwickeln hat, muss der Betreiber von einem Totalschaden der EDV und der gesamten Technik innerhalb dieses Raumes, mit den entsprechenden Folgewirkungen für das oder die verbundenen Unternehmen ausgehen.

6. Brandschutzkonzepte

Aus diesem Grund sind mehrstufige Brandschutzkonzepte entwickelt worden. Die erste Stufe eines Schutzkonzepts beinhaltet die vorschriftsmäßig geforderte konventionelle Überwachung der Bereiche. In IT/DV- und Technikräumen erfolgt dies meist mit punktförmigen Meldern in Doppelboden, Raum und Zwischendecke (wenn vorhanden). Diese Stufe kann in klimatisierten Räumen jedoch bestenfalls einen Personen- und Gebäudeschutz bieten aber die Anlagentechnik nicht wirksam schützen.

Für die zweite Stufe des Brandschutzkonzepts bieten sich hochsensible Rauchansaugsysteme an, die dem zu schützenden Bereich aktiv Luftproben entnehmen und kontinuierlich überprüfen. Um die zuverlässige Überwachung des gesamten Bereiches - Serverschrankreihen, sonstige Systeme innerhalb des Raumes, sowie die Bereiche in Decke und Hohlraumboden, zu gewährleisten - erfolgt der Lufttransport über ein Ansaugrohrsystem. Dem zu überwachenden Bereich werden über das Rohrsystem mit definierten Ansaugöffnungen Luftproben entnommen und der Detektionseinheit zugeführt. Die Rauchkonzentration wird unmittelbar über eine Skala oder Bargraphanzeige angezeigt. Erkennt die Detektionseinheit Rauchpartikel, wird das Erreichen der drei Alarmstufen über LED's angezeigt und über potentialfreie Kontakte an die Brandmeldezentrale weitergeleitet.

Das Rauchansaugsystem verfügt über mehrere abgestufte Alarmpegel (Info-, Vor- und Hauptalarm). Die Verzögerungszeit der einzelnen Alarmschwellen lässt sich zwischen 0 und 60 Sekunden einstellen. Veränderungen der Luftstromwerte, des Rauchpegels oder andere Umgebungsbeeinträchtigungen werden vom Rauchansaugsystem erfasst und zwischengespeichert. Die hohe Sensibilität durch ein optisches Detektionsverfahren mit langlebigen Lichtquellen mit einer Anzeigesensibilität von bis zu 0,005%/m Lichttrübung stellt eine schnelle Detektion sicher.

Die Detektoren haben verglichen mit Punktmeldern eine bis zu 1.000-fach höhere Ansprechsensibilität und können bereits kleinste Ereignisse wie überhitzte Kabel, in der Regel schon bei einer Erwärmung > 600 Celsius, oder Klemmverbindungen sicher detektieren. Um diese geringen Mengen Rauchpartikel frühestmöglich zu erkennen, befinden sich die Sensoren im zentralen Abluftkanal oder vor den Umluftklimageräten. Auf diese Weise erhält der Betreiber sehr früh eine Information über ein Ereignis, das sich meist noch in der Pyrolysephase befindet. Es handelt sich dabei noch nicht um einen Brand, es werden lediglich erste Pyrolyseprodukte, etwa Weichmacher aus Kabelisolierungen, freigesetzt. Die elektrische Funktion der betroffenen Anlagen ist in der Regel noch vollständig gegeben.

Die dritte mögliche Stufe des Sicherheitskonzepts umfasst den Einrichtungsschutz. Das bedeutet, die Detektion erfolgt direkt an den EDV-Anlagen, sodass ein möglicher Brand unverzüglich lokalisierbar ist; zudem sind damit automatische Folgehandlungen möglich. So kann das System in der Frühphase eines Brands gezielt die Stromversorgung der betroffenen Anlagen abschalten und bereits in mehr als 95% aller Fälle die weitere Entwicklung eines Brands sicher verhindern. Hier bietet der Markt je nach Anforderung verschiedenste Systeme an. Das beginnt bei Rauchansaugsystemen über Schranklöschesystemen für einen oder mehrere Serverschränke und geht bis zu Branderkennungssystemen für große Anlagen, die Teil eines Gesamtbrandschutzkonzepts sind.

Sollte trotz aller Vorsorge und installierter Technik ein Brand entstehen, müssen entsprechende Sensoren diesen unverzüglich detektieren und einen Alarm absetzen. Das ist bei einer Vielzahl von Anlagen möglich. Manchmal werden dabei jedoch die teilweise erheblichen Strömungsgeschwindigkeiten der Raumklimatisierung unberücksichtigt gelassen. Konventionelle Meldertechnik ist hier schnell überfordert. Abhilfe schaffen Brandmeldesysteme, die auf Lasertechnik basieren und zudem durch eingebaute Ventilatoren aktiv Raumluft ansaugen, sogenannte Rauchansaugsystem zur Brandfrühesterkennung. Damit erreichen sie eine wesentlich höhere Ansprechempfindlichkeit. Gleichzeitig reduziert sich das Risiko von Fehlalarmen. Zusätzlich werden zu dieser Einrichtung konventionelle, optische Rauchmelder und wenn aufgrund der hohen Strö-

mungsgeschwindigkeiten erforderlich noch zusätzliche Klimawächter installiert. In jedem Fall empfehlen wir immer die Errichtung von drei! Brandmeldelinien – eine Linie mit einem oder mehreren Brandfrühest-erkennungssystemen, eine Linie als Schleife 1 und eine weitere Linie als Schleife 2 für die konventionellen Melder.

Darüber hinaus kann ein Unternehmen der Feuerwehr viel Zeitaufwand ersparen, wenn das Feuerwehrbedienfeld und die zugehörigen Laufkarten im Brandfall schnell zugänglich sind. Die örtliche Lage sollte zwingend, bereits im Vorfeld der Bauleistungen mit der Feuerwehr abgestimmt und festgelegt werden.

7. Brand-, Rauchschutz

Hocheffektive Brandlöschanlagen und alternativ Sauerstoffreduktionsanlagen erfordern einen baulichen und finanziellen Einsatz. Gerade im Bereich von IT-Räumen, welche in konventioneller Bauweise errichtet werden, ist die, für den Einsatz derartiger Anlagen erforderliche Rauchgasdichtigkeit meistens nicht gegeben. Hier muss also vorbereitend und noch vor einer Entscheidung für ein derartiges System dies festgestellt werden. Hierfür ermittelt ein "Blower Door Test" exakt die Dichtigkeit des Raumes, sodass ein Fachmann zum einen eine Aussage über die Situation der Rauchgasdichtigkeit machen kann und zum anderen daraus und aus dem Raumvolumen die notwendige Menge des Löschmittels berechnen kann. Zudem erhält der Betreiber mit dem Test eine Aussage über die Qualität der baulichen Brandschutzmaßnahmen im jeweils überprüften Schutzbereich. Ist das Ergebnis über die Rauchgasdichtigkeit negativ, ist dieser Raum meist nur mit hohem Aufwand in diesen Zustand zu versetzen.

Die Lösung durch ein „Raum im Raum System“ oder einer „Outdoor-Lösung“ ist eine sichere Empfehlung, besonders wenn z.B. rauchgasdichte Ausführung und zusätzliche Schutzigenschaften vorhanden sind.

Nach unserer Auffassung ist es mittlerweile unbestritten, dass insbesondere aufgrund von innovativer Löschtechnik, wie z.B. im Falle des Löschmittels NOVEC 1230 eine, sehr schnelle und damit hoch effektive Brandbekämpfung empfehlenswert und sinnvoll ist. Die einsetzbaren Löschgase werden ständig weiterentwickelt.

Hier ist eine Risikoabwägung notwendig, um die Anlage entsprechend den Anforderungen dimensionieren zu können. Die Spanne der verfügbaren Technik reicht von lokalen Systemen für einen Serverschrank bis zu Anlagen, die Räume mit hunderten von Kubikmetern Rauminhalt versorgen. Löschanlagen haben Anforderungen an den Baukörper und erfordern auch weitere technische Einrichtungen. Hier ist es sinnvoll, möglichst in einer frühen Planungsphase zu entscheiden, was in welchen Bereichen eingesetzt werden soll. Im Falle eines Einsatzes von zum Beispiel in einem „Raum im Raum System“ oder „Technikmodulsystem“ sind diese Räume aufgrund ihrer Beschaffenheit und Konstruktion von Haus aus für einen Einsatz von automatischen Löschanlagen vorbereitet.

Für IT/DV-Räume, Rechenzentren und andere, für das Unternehmen überlebenswichtige Räume ist das Schutzziel in der Regel eine größtmögliche Ausfallsicherheit und Verfügbarkeit. Deshalb sollte der Betreiber auf modernste, zuverlässige Technik beim technischen Brandschutz achten und diese aufrecht halten.

Auch dem „Rauchschutz“ kommt eine erhebliche Bedeutung zu.

Rauch stellt bei Bränden die größte Personengefährdung dar. Mehr als 90% der Brandtoten sind durch Raucheinwirkungen (Vergiftungen) leider zu beklagen. Aber auch die IT-Hardware wird durch Rauch erheblich in Mitleidenschaft gezogen. Daher ist auf einen umfassenden Rauchschutz Wert zu legen.

Die folgenden Empfehlungen sollten zum Rauchschutz mindestens berücksichtigt werden:

- Brandschutztüren sollten Rauchschutzqualität aufweisen.
- Rauchschutztüren in Fluren sollten durch Rauchschalter gesteuert werden. Solche Türen können immer offen stehen, da sie bei Rauchdetektion selbsttätig schließen.
- Die Lüftungsanlage bzw. die Klimaanlage sollte eine Entrauchung von IT-Räumen gestatten.

- In Klimakanälen (Zu- und Abluft) sollten Kanalmelder installiert sein.
- In der Frischluftansaugung sollten Melder installiert sein, die automatisch diese sperren, wenn Störgrößen (Rauch) erkannt werden.

Die Funktionsfähigkeit aller Rauchschutz-Komponenten muss regelmäßig überprüft und wie alle notwendigen Überprüfungen und Kontrollen dokumentiert werden.

Hinweis: Alle Mitarbeiter müssen u.a. nachweislich unterrichtet werden, welche Warnsignale die Schutzeinrichtungen haben und wie darauf zu reagieren ist.

8. Zutrittskontrolle

Auch der Schutz gegen unbefugte Zugriffe, Einbruch und Sabotage kann je nach Fall und Sicherheitsstufe sehr unterschiedlich ausfallen. Ein rudimentärer Einbruchschutz und der protokollierte Zutritt in und aus den (IT) Räumlichkeiten ist grundsätzlich unabdingbar. Um späteren Streitigkeiten oder Vorwürfen aus dem Weg zu gehen, empfehlen wir, das Schutzziel mit (unserer) beratenden Unterstützung in enger Abstimmung mit dem Datenschutzbeauftragten und dem Versicherer zu definieren. Im Bereich der Protokollierung und Aufzeichnung ist die Hinzuziehung der Arbeitnehmervertreter (Betriebsrat) ebenfalls bereits im Vorfeld empfehlenswert.

Je nach Aufgabenteilung ergibt sich die Einteilung in die verschiedensten VdS-Klassen (VdS: Verband der Sachversicherer) und somit eine Eingrenzung der möglichen Produkte. Aus Servicegründen empfiehlt es sich, die Brandmeldeanlage, die Einbruchmeldeanlage und das Zutrittskontrollsystem von einem Hersteller und Anbieter zu wählen, der alles aus einer Hand liefern und warten kann.

Hiermit werden vor allem Kommunikations-, Schnittstellen- und Alarmweiterleitungsprobleme vermieden. Wir empfehlen professionellen Produkten, welche in Soft- und Hardware aufeinander abgestimmt sind. Probleme durch fremde Technikkomponenten sind damit weitgehend ausgeschlossen – sowohl im Tagesbetrieb wie auch im Notfall ein entscheidendes Kriterium.

Außerdem ermöglicht dies nicht nur mehr Effizienz schon bei der Installation und Inbetriebnahme, sondern auch bei Wartungs- und Reparaturarbeiten. Insbesondere auch im Notfall kann beispielsweise über unsere Organisation (nach vertraglicher Regelung) sofort unterstützend eingegriffen werden.

Ein weiterer Vorteil ist die Begrenzung des Zutritts von betriebsfremden Personen. Um die Gefahr durch unvermeidbare Zugriffe von Fremdpersonal zu verringern, sollte das Zutrittskontrollsystem über mehrere Raum-/Zeitzone verfügen. So ist sichergestellt, dass einzelnen Personen- und Personengruppen der Zutritt nur in den hierfür festgelegten Zeiten und zu den definierten Bereichen möglich ist. Der Zutritt zum Kern des IT-Raum, wie auch zu den hierzu gehörenden Infrastrukturräumen sollte generell auf einen kleinen und definierten Personenkreis beschränkt sein und betriebsfremden nie ohne Aufsicht möglich sein.

Prozess-Beispiel:

- Risiken ⇔ Planungen ⇔ Maßnahmen ⇔ Regelungen ⇔ Anweisungen ⇔ Kontrollen.

9. Energieversorgung

Ein nächster strategischer Punkt ist die Absicherung der Energieversorgung.

Je nach Qualität und Ausbau des Versorgungsnetzes des Energieversorgungsunternehmens und des eigenen Stromleitungsnetzes, abhängig vom Umfeld (andere Stromverbraucher) und von der geographischen Lage, können durch Induktion oder Blitzschlag Überspannungsspitzen im Stromversorgungsnetz entstehen. Überspannungsschutzmaßnahmen dienen zur Reduzierung möglicher Schäden an IT-Systemen in Netzen durch direkten Blitzeinschlag, Einkopplungen und Schaltvorgängen.

Auch über andere elektrisch leitende Außenanbindungen wie Telefon-, Wasser- oder Gasleitungen können Überspannungen in ein Gebäude und die dort betriebene IT gelangen. Darüber hinaus können Überspannungen auch auf interne Leitungen eingekoppelt werden.

Ein komplettes Überspannungsschutzkonzept berücksichtigt alle externen und internen elektrisch leitenden Verbindungen und baut sich in drei Stufen auf, die sich im Wesentlichen an den Bemessungsstoßspannungen für die Überspannungskategorien gemäß DIN VDE 0110/IEC Publikation 664 orientieren:

- Der Grobschutz in der Gebäudeeinspeisung ist in der Lage Überspannungen abzufangen, wie sie durch direkten Blitzeinschlag entstehen und sie auf Werte kleiner als 6.000 V zu begrenzen. Bei vorhandenem äußeren Blitzschutz muss der Grobschutz blitzstromfähig sein, da mit Strömen im 100 kA-Bereich zu rechnen ist.
- Der Mittelschutz in den Etagenverteilern begrenzt die verbleibenden Überspannungen auf ca. 1.500 V und ist darauf angewiesen, dass die von ihm abzufangenden Überspannungen 6.000 V nicht überschreiten.
- Der Feinschutz an den jeweiligen Steckdosen und den Steckverbindungen aller anderen Leitungen reduziert die verbleibenden Überspannungen auf das von den angeschlossenen Geräten verkraftbare Maß. Die Hersteller elektrischer und elektronischer Geräte sind in den meisten Ländern verpflichtet, ihre Geräte mit einem für den sicheren Betrieb erforderlichen Feinschutz auszustatten.

In Deutschland ist dies durch das Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) geregelt.

Die Schutzwirkung jeder Stufe baut auf der vorherigen auf. Der Verzicht auf eine Stufe macht den gesamten Überspannungsschutz nahezu unwirksam.

Ist der gebäudeweite Aufbau eines Überspannungsschutzes nicht möglich, so kann man zumindest wichtige Teile der IT (Server etc.) mit einer entsprechenden Schutzzone umgeben. Netze mit einer Vielzahl angeschlossener Geräte können, um einen möglichen Schaden klein zu halten, durch Optokoppler oder Überspannungsableiter in kleine, gegeneinander geschützte Bereiche aufgeteilt werden. Dabei müssen geschützte und nicht geschützte Bereiche bis zurück zu der Schutzeinrichtung, bei der die Teilung erfolgt, konsequent getrennt werden. Die Zuleitungen müssen mit ausreichendem Abstand geführt werden, eine gemeinsame Verlegung in einem Kabelkanal würde die Schutzwirkung aufheben. Überspannungsschutzeinrichtungen sollten periodisch und nach bekannten Ereignissen geprüft und ggf. ersetzt werden. Insbesondere bei Neugestaltung eines Schutzkonzeptes für Überspannung sind Auslegung und Funktionsweise bestehender USV (unterbrechungsfreier Stromversorgung) und NEA (Netzersatzanlage) zu berücksichtigen.

Neben dem Überspannungsschutz im Versorgungsnetz müssen in Serverräumen und den Kerneinheiten eines Rechenzentrums Maßnahmen gegen elektrostatische Aufladung getroffen werden. Der Durchgangswiderstand der Bodenbeläge in solchen Räumen muss zwischen 10 und 100

Megaohm liegen. Die Einstufung nach DIN-Vorschrift 4102-1 muss mindestens "B1 - schwer entflammbar" erreichen. Dies gilt auch für einen Doppelboden oder einen Installationsboden.

Zwei Grundvoraussetzungen sind unabhängig von Umfang und Ausbau des Überspannungsschutzes zu beachten:

- Die Leitungslänge zwischen dem Feinschutz und zu schützenden Geräten sollte 20m nicht überschreiten. Falls doch, ist ein erneuter Feinschutz zwischenzuschalten. Verfügt ein Gerät über einen Feinschutz im Eingang, entfällt die 20m Begrenzung.
- Für einen funktionierenden Überspannungsschutz ist ein umfassender Potentialausgleich aller in den Überspannungsschutz einbezogenen elektrischen Betriebsmittel erforderlich! Die Mehrzahl der Schäden an IT-Geräten durch Überspannungen ist auf nicht konsequent umgesetzten Potentialausgleich zurückzuführen.

Eine sichere Energie- und Klimaversorgung ist für die Systeme ebenfalls unverzichtbar.

Deshalb sollten die zentralen Komponenten der Energieversorgung wie Einspeisung oder Trafos redundant ausgelegt werden. Bei einem Stromausfall stellt im Idealfall das Notstromaggregat die Versorgung sicher. Eine, oder mehrer zwischengeschaltete Online-USV-Anlagen überbrücken hierbei den Zeitraum vom Ausfall bis zur Lastübernahme des Dieselaggregats (je nach Typ und Last etwa acht Sekunden) oder einer Brennstoffzelle. Bei der Installation von USV-Anlagen, welche im Notfall von einem Notstromaggregat versorgt werden, ist zu beachten, dass die Synchronisation aller Anlagen unterbrechungsfrei und automatisch erfolgt. Das Notstromaggregat muss aufgrund der Beschaffenheit der Online-USV-Anlagen so geplant sein, dass es im Einsatzfall den mindestens 1,8 fachen Leistungsstrom der USV-Anlage(n) als Anlaufstrom liefern kann. Bei der Planung, Realisierung und Wartung der Netzersatzanlage sind umfangreiche Gesichtspunkte, Anforderungsabhängig zu beachten.

Die USV-Anlage muss so installiert sein, dass sie eine galvanische Trennung in allen Leitungsverbindungen sicherstellt. Dies ist unbedingt erforderlich, um z.B. einen Ausfall der USV-Anlage aufgrund eines Blitzschlages zu vermeiden. Hier muss ein entsprechender Trenntrafo in Wechselrichterzugang der USV-Anlage integriert sein. Ein automatischer und ein manueller Bypass sorgen im Wartungsfalle oder bei einem Anlagendefekt unterbrechungsfrei auf das Zurückschalten auf das Normalnetz. Darüber hinaus gewährleistet die USV im normalen Betrieb eine reine, sinusförmige Stromversorgung und filtert die Störungen aus dem eingehenden Netz des Energieversorgers. Die zur USV gehörige Batterieanlage muss mindestens so dimensioniert sein, dass in einem Notfall von mindestens 10 Minuten überbrückt werden kann und danach soviel Batteriekapazität vorhanden ist, dass alle an der USV angeschlossenen Komponenten noch ordentlich heruntergefahren werden. In der Regel geschieht dies dann automatisch über die vom USV-Hersteller mitgelieferten Shutdown-Software, in welcher die Parameter individuell für den jeweiligen Bedarf gesetzt werden können.

Idealerweise erfolgt dann die Energieverteilung aus der USV über eine Verteilung nach der USV direkt in den IT-Raum und dort über ein Stromschienensystem, mit einem oder mehreren Schienen. Am Schienensystem selbst wird dann die Energie zu jedem Rack über einen Abgangskasten, separat abgesichert gebracht. Hierdurch kann auch sehr einfach eine komplett redundante Versorgung bis hin zum Netzteil realisiert werden. Auch Nachinstallationen sind einfach und erfordern keine Umbauten in irgendwelchen Elektroverteiltern. Durch den Einsatz von diesen Schienensystemen werden ebenfalls wieder Brandlasten durch Stromkabel eingespart.

Generell ist zu beachten, dass innerhalb dieser IT/DV- bzw. Serverräume eine Notabschalteinrichtung nach VDE 0800 zu installieren ist. Bei Betätigung der Notabschalteinrichtung muss die gesamte Energieversorgung für die Rechnersysteme und für die anderen vorhandenen Anlagen aus dem Serverraum abgeschaltet werden. Die Energieversorgung für die Beleuchtung sollte dabei erhalten bleiben. Die Notabschaltvorrichtungen sind gemäß VDE 0800 gegen unbeabsichtigtes Betätigen zu sichern und zu kennzeichnen.

10. Klimatisierung

Die Klimatechnik für DV/IT-Räume, wie auch die betriebsabhängigen Räume mit der jeweiligen technischen Infrastruktur, müssen nach Stand der Technik immer mit einer, mindestens n +1 redundanten Klimatechnik ausgestattet sein.

Das BSI gibt hier folgende Mindestanforderungen vor:

□ Um den zulässigen Betriebstemperaturbereich von IT-Systemen zu gewährleisten, reicht der normale Luft- und Wärmeaustausch eines Raumes in der Regel nicht aus, sodass der Einbau einer Klimatisierung erforderlich wird. Deren Aufgabe ist es, die Raumtemperatur innerhalb der von der IT vorgegebenen Toleranzgrenzen zu halten. Werden darüber hinaus Forderungen an die Luftfeuchtigkeit gestellt, um beispielsweise elektrostatische Aufladungen zu vermeiden, kann ein Klimagerät durch Be- und Entfeuchtung auch diese erfüllen. Dazu muss das Klimagerät allerdings an eine Wasserleitung angeschlossen werden. Die Vermeidung von wasserführenden Leitungen ist jedoch generell zu beachten, wenn aber nicht möglich, sind Risiko-Minimierungsmaßnahmen zu ergreifen.

- Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige, fachgerechte Wartung der Klimatisierungseinrichtung unabdingbar. Eine zusätzliche Überwachungseinrichtung für die ordnungsgemäße Klimatisierung ist zu empfehlen, insbesondere bei Vollklimatisierung.
- Da bei einem Ausfall der Klimatisierung unter Umständen viele (insbesondere wichtige) IT-Systeme abgeschaltet werden müssen, muss diese auf eine hohe Verfügbarkeit ausgelegt sein. Die Leistungsreserve muss deshalb entsprechend dimensioniert werden, außerdem sollte sie einfach erweiterbar sein. Die Klimatisierung sollte bei der Notfallplanung mit berücksichtigt werden.
- Für einen Serverraum oder ein Rechenzentrum ist zur Bestimmung der nötigen Kühlleistung eine exakte Wärmelastberechnung durchzuführen. Eine Frischluft-Beimischung ist dann erforderlich, wenn der oder die klimatisierten Räume ständig mit Personal besetzt ist.
- Ebenso ist - durch mehrere Messungen zu verschiedenen Tageszeiten - zu bestimmen, ob eine Luftbefeuchtung oder -entfeuchtung in den Räumen erforderlich ist. Hier sind auch die Herstellervorgaben für die IT-Komponenten und Datenträger unbedingt zu beachten.
- Wärmetauscher und Rückkühlwerke sollten möglichst nicht direkt in einem Serverraum oder Rechenzentrum aufgestellt sein, um zu verhindern, dass Schäden an der Klimaanlage weitere Beeinträchtigungen verursachen, z. B. durch austretende Kühlflüssigkeit oder Kurzschlüsse.
- Die Rückkühlwerke der Klimaanlage sind bei Aufstellung im Freien gegen direkten Blitzeinschlag zu schützen. Insbesondere in Hochsicherheitsbereichen sollten die Rückkühlwerke nicht für jedermann zugänglich sein und gegebenenfalls gegen Sabotage materiell geschützt werden.

Im Idealfall - auch nach einer Empfehlung des BSI (Trennung von grober und feiner Technik) - soll die Installation außerhalb des DV/IT-Raumes erfolgen.

In diesem Fall erfolgt die Einblasung der aufbereiteten Luft über vollautomatische und wartungsfreie Brandschutzklappen in den Außenwänden direkt in den Bereich des Doppelbodens innerhalb des DV/IT-Raumes. Innerhalb dieses Doppelbodens wird die Luft (mit dem vorher errechneten Luftdruck) verteilt. Die Kühlung der System erfolgt aus dem Doppelboden über spezielle Lüftungslatten und / oder Auslässe. Diese Auslässe müssen ebenfalls wieder für den jeweiligen Anwendungsfall berechnet sein.

In der Regel wird für die Kühlleistung ohne Redundanz 1kW pro Quadratmeter Fläche geplant. Ausnahmen sind hier die hochkonzentrierten Hochleistungsserver wie z.B. Blade's, welche pro Gerät derzeit bis zu 3,7kW Abwärme produzieren. Beim Einsatz solcher Systeme sind spezielle Kühlracks erforderlich, da bei der Installationen von mehreren dieser Server in einem Rack sehr schnell ein Kühlbedarf bis zu 20kW entsteht.

Eine derartige Leistung ist mit konventioneller Kälte-/Lufttechnik nicht mehr (Herstellieranforderung) zu erreichen. Für diese Anforderungen haben wir spezielle Kühlrack-Lösungen. Hier können Leistungen individuell für jedes Rack redundant konfiguriert werden, bis zu einer Gesamtleistung von derzeit => 22kW sensibler Kälte - pro 19-Zoll Rack.

Die Redundanz stellt weitgehend sicher, dass beim Ausfall einer Klimaanlage, sei es durch Wartung oder Defekt, immer eine Anlage mit vergleichbarer Leistung sofort und unterbrechungsfrei einspringt. Damit das auch funktioniert, werden die Anlagen wechselweise betrieben. Das bedeutet, dass immer eine Anlage z.B. für eine Woche auf „standby“ ist, dann im Wechsel in der nächsten Woche wieder eine andere Anlage, usw..

Zur Umsetzung dieser Anforderungen gibt es mehrere Lösungsansätze. Entweder Anlagen mit Kaltwassersatz gespeist, welcher über außen installierte Cooler aufbereitet wird. Hier ist auch die Realisierung einer Kosten einsparenden, freien Kühlung möglich. Oder aber Anlagen als Präzisions-Splitanlagen in Form von Direktverdampferanlagen. Diese Anlagen arbeiten mit chemischem Kühlmittel, derzeit zugelassen R407C. Hier wird die Kühlflüssigkeit mit hohem Druck ebenfalls zu einem Außengerät mit Kondensator befördert, wo diese Kühlflüssigkeit wieder rückgekühlt wird. Diese Anlagen eignen sich insbesondere bei kleineren Kälteleistungen. Von einfachen Splitgeräten, insbesondere als Deckenunterbaugeräte installiert, wird in einem professionellen DV/IT-Umfeld abgeraten.

Generelle Grundanforderungen an eine Klimatechnik nach Stand der Technik:

Alle Geräte sollten Anschlussfertig und betriebsbereit sein. In der Regel sollten Schrankklimageräte in kompakter modularer Bauform mit minimaler Aufstellungsfläche bei guter Zugänglichkeit zu allen Einbauteilen nur von vorne, mit hoher Wirtschaftlichkeit und niedrigem Schallpegel zum Einsatz kommen. Die Geräte müssen nach Konstruktion, Herstellung und Qualitätskontrolle der EG-Norm EN29000 entsprechen und müssen die in die europäische Normung eingegangenen VDE-Normen sowie die Sicherheitsvorschriften nach UVV und VBG erfüllen.

Idealerweise ist vom Hersteller jedes Gerät gemäß dem Qualitätssicherungssystem ISO9001-2000 während der Produktion, nach Fertigstellung und vor der Auslieferung geprüft und getestet. Ein entsprechendes Qualitätssicherungszertifikat sollte dann jedem Gerät beigelegt sein. Alle Geräte müssen das CE- Zeichen tragen und somit den europäischen Sicherheitsvorschriften entsprechen.

In der Regel besteht das Gerätegehäuse aus Stahlprofilen und abgekanteten Profilblechen, die zu einer verwindungssteifen Einheit verschraubt werden. Die Ausführung des Gehäuses sollte im Idealfall komplett doppelschalig erfolgen. Die doppelschalige Geräterückwand kann fest mit der Gehäusestruktur verschraubt sein, die Seitenpaneele jedoch sollten aus zwei unabhängigen Schalen bestehen, wobei die innere Schale einen tragenden Bestandteil des Gehäuses darstellt und die als Verkleidung dienende Außenschale abnehmbar ausgeführt sein sollte. Das Frontpaneel sollte als eine einseitig in Scharnieren gelagerte Fronttür ausgeführt sein und problemlos die freie Zugänglichkeit zu allen Einbauteilen ermöglichen. Idealerweise lässt sie sich durch einen Schnellverschluss leicht öffnen und schließen. In der Regel ist ein Bedienteil in die Tür eingesetzt mit dem Display der Mikroprozessorregelung des Gerätes. Eine hinter der Fronttür angebrachte zusätzliche Abschottung des luftführenden Bereiches durch Servicepaneele sollte die Doppelschaligkeit auch im Frontbereich des Gerätes gewährleisten. Die Wartung und Bedienung der Schaltanlage sowie Servicearbeiten am Kältekreis müssen bei laufendem Gerät möglich sein. Das Gehäuse und die Paneele sollten aus galvanisch verzinktem Stahlblech gefertigt und mit einer Epoxydharzpulverbeschichtung einbrennlackiert sein. Die Verschraubungen der Einzelteile sollten mit nicht rostenden Schrauben ausgeführt sein. Das Gehäuse und die Paneele müssen thermisch

und akustisch mit einer ausreichend starken Mineralwolle isoliert sein und mindestens der Klasse 0 gemäß ISO 11822 - entspricht Brandklasse A1 entsprechen.

Die saugseitig angeordneten Trockenschichtfilter sollen der Filtergüte G4 gemäß Standard CEN-EN779 (= Filtergüte EU4 gemäß Standard EU4/5) entsprechen und aus einem Glasfaserfiltermedium bestehen.

Die Filter sollten unbedingt ein hohes Staubrückhaltevermögen bei einem geringen Luftwiderstand aufweisen und leicht zu wechseln sein. Eine zuverlässige Filterüberwachung muss installiert sein. Dies kann z.B. mit Hilfe eines Differenzdruckschalters erfolgen, welcher bei Überschreiten des eingestellten Differenzdruckes eine akustische und optische Warnmeldung ausgibt.

Die Steuerung und Regelung aller modernen Geräte erfolgt heute immer durch eine Mikroprozessoregelung, die dem Anwender alle wichtigen Informationen bietet. Im Display wie auch über z.B. „SNMP“-Kopplung werden alle Gerätefunktionen, Warn-, Alarm- und Statusmeldungen sofort ausgegeben. Ein zusätzliches Bedien- oder Tastenfeld dient zur leichten Bedienung sowie zur direkten Programmierung. Zur Sicherheit gegen unbefugte Bedienung ist die Veränderung der Sollwerte sowie der Systemkonfiguration (Parameter) über verschiedene Passwörter zu schützen. Alarmmeldungen hoher und niedriger Priorität müssen am Gerät jeweils optisch und akustisch, gleichzeitig über „SNMP“-Kopplung via Netzwerk und alternativ über potentialfreie Kontakte als einzelne Zustands-, Betriebs- und Sammelstörmeldung zur externen Verarbeitung gemeldet werden können.

Die Regelung der Temperatur und Feuchte erfolgt gemäß des eingestellten Temperatursollwerte und der Toleranzen. Als Regelfühler sollte ein kombinierter Temperatur-/ Feuchtfühler eingesetzt werden und im Lieferumfang enthalten sein.

Beim Einsatz von mehreren Anlagen muss eine Software zur Geräte-Kommunikation ebenfalls im Lieferumfang enthalten sein. Dadurch muss ein effektiver Netzwerkbetrieb für alle eingesetzten Klimageräte möglich sein. Die Verbindung der Geräte untereinander sollte durch eine Standard-BUS-Verbindung hergestellt werden und die Adressierung der einzelnen Geräte innerhalb des Netzwerkes ausgeführt werden können. Die Gesamtlänge der Busverbindungen sollte dabei mindestens bis zu 300m betragen.

Eine vollautomatische Einstellung muss dafür sorgen, dass die aktiven Geräte nach den Durchschnittswerten aller aktiven Sensoren geregelt werden, und eine zeit- und störungsabhängige Umschaltung der Geräte realisierbar ist – gerade wichtig für die Redundanzsteuerung. Die Anzahl der aktiven und der stand by Geräte innerhalb einer vernetzten Gerätegruppe muss frei wählbar sein. Weiterhin soll eine Kaskaden-Schaltung möglich sein, wobei die Zuschaltkriterien der Geräte frei wählbar sein sollen. Diese Steuerung muss über einen ausreichenden Funktionsumfang im Bereich Regelung, Event- Historie und Kommunikation verfügen und wesentlich auch bei Totalausfall von angeschlossenen Geräten uneingeschränkt deren Funktion sicherstellen.

Der immer zu Anlage gehörende, luftgekühlte Kondensator ist leistungsmäßig auf das Klimagerät abgestimmt. Der Wärmetauscherblock sollte aus Aluminiumlamellen und nahtlos gezogenem Kupferrohr bestehen. Das gesamte Gehäuse inklusive seiner Einbauten muss absolut witterungsbeständig ausgeführt sein. Da die Vergangenheit gezeigt hat, dass auch in unseren Regionen im Sommer Temperaturen von über 350 Celsius erreicht werden, muss diese Anlage so ausgelegt sein, dass sie ihre Leistung bis zu einer Außentemperatur von 400 Celsius erbringen kann. Weitere Informationen zum Thema Klimatisierung werden auf Anfrage zur Verfügung gestellt.

Für die Raumtemperatur von IT/DV-Räumen hat sich eine ständig konstante Temperatur von 220 Celsius mit einer Schwankungsbandbreite von maximal 20C nach oben und 20C nach unten bewährt. Für Räume mit USV- und Batterieanlagen sind 180 Celsius als konstante Temperatur erforderlich, da dies die Lebensdauer der Batterien erheblich positiv beeinflusst.

11. Gefahrenmeldeanlagen

Wichtig ist es auch, alle diese technischen Anlagen zur Aufrechterhaltung dieser komplexen Infrastruktur mit einer Leittechnik oder mindestens einer Gefahrenmeldeanlage permanent zu überwachen, um im Schadensfall schnell reagieren zu können.

Eine Gefahrenmeldeanlage (GMA) besteht aus einer Vielzahl lokaler Melder, die mit einer Zentrale kommunizieren, über die auch der Alarm ausgelöst wird. Ist im Betriebsgebäude bereits eine Gefahrenmeldeanlage für Einbruch, Brand, Wasser oder auch Gas vorhanden, lässt sich diese meistens mit vertretbarem Aufwand entsprechend erweitern. Es sollten zumindest die Kernbereiche der IT (Serverräume, Datenträgerarchive, Räume für technische Infrastruktur u. ä.), wie auch alle für die Versorgung der IT-Räume erforderlichen Infrastrukturanlagen in die Überwachung durch diese Anlage mit eingebunden werden. In der Regel ist es jedoch zu empfehlen, den Teil der GMA für den Bereich der IT/DV-Räume sowie deren Anlagen für die technische Infrastruktur als eigenständige Unteranlage auszuführen. So lassen sich Gefährdungen wie Feuer, Einbruch, Diebstahl frühzeitig erkennen und Gegenmaßnahmen einleiten. Um dies zu gewährleisten, ist die Weiterleitung der Meldungen an eine ständig besetzte Stelle (Pförtner, Wach- und Sicherheitsdienst, Feuerwehr, Bereitschaftsdienst, etc.) unumgänglich. Dabei muss sichergestellt sein, dass diese Stelle auch in der Lage ist (technisch und personell) auf den Alarm zu reagieren. Hierbei sind die Aufschaltrichtlinien der jeweiligen Institutionen zu beachten.

Die GMA ist ein komplexes Gesamtsystem, das entsprechend (Gebäude- / Risiko-Situation) geplant und fachgerecht installiert werden muss. Lösungen, wie Einbruchmelde-, Brandmelde-, Wassermelde-, Störmelde- und Raumüberwachungseinrichtungen sind zu berücksichtigen. Da es beispielsweise eine Vielzahl unterschiedlicher Meldesysteme gibt, müssen diese den Sicherheitsanforderungen entsprechend ausgewählt werden. Zur Einbruchserkennung können z.B. Bewegungsmelder, Glasbruchsensoren, Öffnungskontakte, Videokameras bis hin zu Meldetapeten eingesetzt werden.

Die Melder können untereinander auf verschiedene Arten vernetzt werden. In Abhängigkeit von Art und Größe der zu schützenden Bereiche und der geltenden Richtlinien müssen passende Systeme ausgewählt und installiert werden. Bei der Planung oder Erweiterung einer GMA sollte darauf geachtet werden, dass die Trassen für die Vernetzung ausreichend dimensioniert ist/wird. Um die Schutzwirkung der GMA aufrechtzuerhalten, ist eine regelmäßige Wartung und Funktionsprüfung (DIN VDE 0833 Teil 1-3) vorzusehen.

Ist keine GMA vorhanden oder lässt sich die Vorhandene nicht nutzen, kommen als Minimallösung lokale Gefahrenmelder (VdS) in Betracht. Diese arbeiten völlig selbständig, ohne Anschluss an eine Zentrale. Die Alarmierung erfolgt vor Ort oder mittels einer einfachen Zweidrahtleitung (evtl. Telefonleitung) an eine anderer Stelle.

Für den Betrieb eines Rechenzentrums muss eine GMA zur Brand- und Einbruchdetektion installiert sein. Weitere Detektionsbereiche können nach Lage des Standorts und dessen Infrastruktur sinnvoll sein.

Die Räume wie Serverraum, Datenträgerarchiv haben einen erhöhten Schutzbedarf. Wenn keine zentrale GMA vorhanden ist, sind dort lokale Gefahrenmelder zu installieren. Bei der Verwendung lokaler Gefahrenmelder für die Früherkennung muss dafür gesorgt werden, dass ein Alarm auch außerhalb der betroffenen Räume wahrgenommen wird. Die Meldung kann über verschiedene Wege erfolgen und sollte an eine Stelle weitergeleitet werden, die rund um die Uhr besetzt ist. Beispielsweise gibt es Lösungen, die über die TK-Anlage oder Funk Mitarbeiter über ein Mobiltelefon alarmieren können.

Hinweis: Werden Gefahren-, Alarmierungs- und Störmeldeanlagen für private bzw. gewerbliche Objekte eingesetzt, sollte mit dem Sachversicherer geklärt werden, ob eine Minderung der Versicherungsprämie, insbesondere für die Einbruch-Diebstahlversicherung in Frage kommt.

Wesentliche Beachtung gilt auch nach der Installation der Wartung. Diese ist für alle technischen Einrichtung mindestens in den Intervallen durchzuführen, wie sie vom Hersteller und Gesetzgeber vorgeschrieben sind.

Ein abschließendes Augenmerk muss auch auf das direkte Umfeld des Gebäudes, in dem sich die IT/DV-Räume und Räume mit der technischen Infrastruktur befinden, gelegt werden.

Falls das Gebäude oder Rechenzentrum innerhalb eines Grundstücks liegt, auf dem zusätzliche Sicherheitseinrichtungen installiert werden können, sollten Maßnahmen ergriffen werden, um von außen wirkende Gefährdungen vom Rechenzentrum abzuhalten.

Insbesondere kann hier die erste Stufe einer Zutritts- und vor allem Zufahrtsregelung geschaffen werden. Je nach Schutzbedarf und topologischen Gegebenheiten kann ein Perimeterschutz aus folgenden Komponenten bestehen:

- Äußere Umschließung oder Umfriedung, z. B. Zaunanlage, Mauerwerk und Zaunüberwachung

Dies bietet:

- Schutz gegen unbeabsichtigtes Überschreiten einer Grundstücksgrenze,
- Schutz gegen beabsichtigtes gewaltloses Überwinden der Grundstücksgrenze sowie
- Schutz gegen beabsichtigtes gewaltsames Überwinden der Grundstücksgrenze.
- Freiland-Sicherungsmaßnahmen, z.B. Geländegestaltung, Zufahrtssperren, Beleuchtung des Geländes und des Gebäudes, Bewachungsunternehmen, Videoüberwachung und Detektionssensorik auf dem Gelände.

Dies bietet Schutz gegen unbemerkten Zutritt eines Eindringlings für die Fläche zwischen Umfriedung und Gebäude.

- Äußere Personen- und Fahrzeugidentifikation, z. B. Videogegensprechanlage, Personen- bzw.
- Fahrzeugschleuse, Tür- bzw. Toröffnung und Zutrittskontrollenheiten.

Dies bietet Schutz gegen erkennbar (visuell, akustisch oder sensorisch) unberechtigte Zutrittsversuche als erste Stufe des Zutrittskontrollkonzeptes. Diese Aufgabe kann durch einen Pförtnerdienst unterstützt werden.

Bevor Maßnahmen aus dem Bereich Perimeterschutz realisiert werden, muss in jedem Fall ein stimmiges Schutzkonzept erarbeitet werden, das die oben genannten Aspekte und den Gebäudeschutz umfasst. Anderenfalls besteht die Gefahr, dass vergleichsweise teure Sicherheitsmaßnahmen umgesetzt werden, beispielsweise aufwändige Zaunanlagen und ausgefeilte Gelände-Videoüberwachung, die in keinem Verhältnis zur Gebäudesicherung stehen und daher nicht angemessen sind.

Das Schutzkonzept sollte darauf ausgerichtet sein, mit den zur Verfügung stehenden Ressourcen möglichst wirksame Schutzmaßnahmen aufzubauen. Dies betrifft besonders den Bereich Perimeterschutz. Die hier ergriffenen Maßnahmen sollten die Gesamtsicherheit erhöhen und nicht nur das Image einer "Hochsicherheitskulisse" vermitteln, da sich qualifizierte Angreifer allein durch den Anblick von hohen Zäunen und Videoüberwachung kaum von ihrem Vorsatz abbringen lassen.

Beispiel: Wenn ein Angreifer zwei Minuten benötigt, um den Weg über den Zaun bis zum Gebäude zu nehmen und anschließend nur eine halbe Minute für das Eindringen ins Gebäude, stimmt die Relation nicht. Dies gilt um so mehr, wenn das Eintreffen von Einsatzkräften der örtlichen Polizei nach Alarmierung durch ein privates Bewachungsunternehmen beispielsweise acht

Minuten dauert. In dieser Zeit könnte ein Einbrecher schon wieder nach vollbrachter Tat das Gelände verlassen haben. Er wäre zwar bemerkt und auf Videomaterial aufgenommen worden, bei geeigneter Maskierung jedoch kaum zu identifizieren.

In unserem Konzept können wir auch entsprechende Komponenten z.B. für eine Videoüberwachung berücksichtigen. Diese Anlage könnte für einen Perimeterschutz erweitert werden.

12. Hinweise

Alle aufgeführten Informationen erheben keinen Anspruch auf Vollständigkeit. Haftungsansprüche können hieraus nicht abgeleitet werden. Diese spiegeln jedoch weitgehend die Empfehlungen, sowie Vorgaben des BSI zum „Stand der Technik“ wieder. Die Beschreibung der Komponenten wurden teilweise von den jeweiligen Partnern, Lieferanten und Herstellern zur Verfügung gestellt. Gesetze, Vorschriften und auch die vom Gewerbeamt und den Berufsgenossenschaften geforderten Sicherheits- und Schadenverhütungsmaßnahmen werden hier nicht oder nur begrenzt behandelt.



Architect of an Open World™

Deutschland:

Bull GmbH
Von-der-Wettern-Str. 27
51149 Köln
Tel +49 2203 305-0
Fax +49 2203 305-1818
info@bull.de
www.bull.de

Österreich:

Bull GmbH
Lemböckgasse 49
1230 Wien
Tel.: +43 (0)1-891 36-0
Fax: +43 (0)1-891 36-3317
info@bull.at
www.bull.at

Schweiz:

Bull (Schweiz) AG
Wallisellerstraße 116
8152 Opfikon
Tel.: +41 (0)43 455 80 90
Fax: +41(0)43 455 80 99
info@bull.ch
www.bull.ch