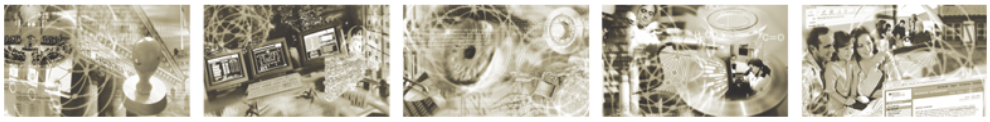
Bundesamt
für Sicherheit in der
Informationstechnik



Band B, Kapitel 11: Infrastruktur

Im Umfeld der Hochverfügbarkeit

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: hochverfügbarkeit@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Die immer stärker werdende Abhängigkeit vieler Organisationen von der Informationstechnik (IT) fordert nachhaltig eine permanente Sicherstellung der Verfügbarkeit kritischer Geschäftsprozesse. Kaum eine Organisation kann sich heutzutage einen Ausfall seiner IT und somit die Einschränkung der Verfügbarkeit seiner Geschäftsprozesse leisten. Nicht zuletzt ist es die stark wachsende Komplexität und Vernetzungsdichte der IT, die höhere Anforderungen an die Verfügbarkeit der IT-Infrastruktur stellt, und somit auch in zunehmendem Maße die Rahmenbedingungen für die kontinuierliche Bereitstellung der Infrastruktur festlegt.

Die Infrastruktur im Sinne dieses Dokuments stellt, als das Fundament für den operativen Betrieb der IT, essenzielle Umgebungsbedingungen und Versorgungsleistungen zur Verfügung. Ein Ausfall einzelner oder mehrerer dieser Versorgungsleistungen der IT, z. B. von Energie oder Klimatisierung kann weitreichende Folgen haben, welche den Ablauf kritischer Geschäftsprozesse stören könnten.

Datennetze, Serverarchitekturen etc. sind nicht Teil dessen, was in diesem Dokument als Infrastruktur betrachtet wird.

Um die Verfügbarkeit von Geschäftsprozessen gewährleisten zu können, muss die Verfügbarkeit der erforderlichen IT-Systeme sichergestellt sein. Ist dies nicht der Fall, können Dienste nicht mehr abgerufen werden. Die möglichen Ursachen für die Funktionsunfähigkeit von Systemen können äußerst vielfältig sein (z. B. Konfigurationsfehler, Sabotage, Software-Unverträglichkeiten, Hardware-Ausfall, Brand oder Diebstahl).

Bedrohungen, die einen direkten Einfluss auf die Verfügbarkeit der Infrastruktur und somit ebenfalls Einfluss auf die Verfügbarkeit unternehmenskritischer Geschäftsprozesse haben, müssen bereits bei der Planung von IT-Strukturen Berücksichtigung finden, um frühzeitig adäquate Gegenmaßnahmen etablieren zu können.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit diesem Hochverfügbarkeitskompendium (HV-Kompendium) einen Überblick über die zurzeit aktuelle Technologie für die Errichtung und den Betrieb hochverfügbarer Infrastrukturen zur Verfügung.

1.1 Ziel

Das vorliegende Dokument widmet sich der Hochverfügbarkeit der Infrastruktur und stellt einen in sich geschlossen Beitrag dar. Es hat zum Ziel, präventive Verfahren und Techniken zu beschreiben, die bei der Planung und Implementierung von hochverfügbaren Infrastrukturen unterstützend wirken. Dabei orientiert sich die Auswahl der Maßnahmen an den Prinzipien der Verfügbarkeit (siehe Beitrag „Prinzipien der Verfügbarkeit“ im HV-Kompendium):

- Fehlertoleranz,
- Redundanz,
- Separation,
- Robustheit,
- Skalierbarkeit,
- Priorisierung,
- Transparenz,

- Virtualisierung,
- Automatismen und
- Autonomie.

Hieraus werden bedarfsorientierte technische Lösungen abgeleitet und beschrieben. Der Vollständigkeit halber sind hier alle Prinzipien der Verfügbarkeit aufgelistet, jedoch finden diese im Kontext der Betrachtungen zur Infrastruktur nicht alle Anwendung.

1.2 Strategien für hohe Verfügbarkeit

Das Bestreben, eine 100-prozentige Verfügbarkeit zu erreichen, ist sowohl technisch nur schwer umsetzbar, als auch wirtschaftlich nicht immer sinnvoll. Strategien für die Realisierung hoher Verfügbarkeit sollten deshalb auch für den Betrachtungsbereich Infrastruktur immer nach erfolgter Analyse der Anforderungen und des Risikos entworfen werden.

Infrastrukturelle Einrichtungen sind nicht Selbstzweck, sondern stellen der IT-Hardware und dem Personal (Nutzern) mittels technischer Einrichtungen definierte Umgebungsbedingungen bereit. Die Nutzer bestimmen die Anforderungen hinsichtlich der Verfügbarkeit (siehe auch Beitrag „Phase S – Überblick“ des HV-Kompendiums). Nur die Kenntnis der Anforderungen, der Bedrohungen und der Risiken ermöglicht wirkungsvolle Strategien in Bezug auf die Infrastruktur. Maßnahmen der baulichen und technischen Infrastruktur können nur dann ihre optimale Wirkung bei gleichzeitiger Wirtschaftlichkeit entwickeln, wenn sie zum frühestmöglichen Zeitpunkt geplant und realisiert werden. Eine spätere Nachrüstung ist in diesem Bereich immer mit deutlichen Mehrkosten und sehr oft verminderter Wirksamkeit der Maßnahmen verbunden.

Eine grundlegende Methode zur Erreichung hoher Verfügbarkeit ist die Vermeidung von „Single Point of Failures (SPoF). Bei SpoFs handelt es sich um Systemkomponenten, deren Ausfall oder Funktionsstörung einen Komplettausfall des Gesamtsystems zur Folge hat. Bei hochverfügbaren Systemen hat sich das mehrfache Vorhandensein funktionsgleicher Systembestandteile (funktionelle Redundanz) etabliert. Redundanzen stellen bei einem Ausfall einer Primärkomponente sicher, dass andere (Sekundär-) Komponenten mit gleicher Funktionalität die Aufgaben übernehmen. Die zugesicherte Verfügbarkeit kann somit in einem höheren Maße gewährleistet werden, als ohne Redundanz. Redundanz ist bei allen Komponenten vorzusehen, die den Erfordernissen der Hochverfügbarkeit genügen müssen.

Wird die Gesamtheit der erforderlichen Infrastruktur als ein System betrachtet und das Prinzip der Redundanz als strategisches Mittel genutzt, so ergeben sich für die Planung von hochverfügbaren Infrastrukturen weit größere Dimensionen, die bis zum Aufbau von Back-up-Rechenzentren führen können.

Ein klassisches Verfahren zur Schaffung von Redundanz ist als N+1-Redundanz bekannt. Dabei wird zu den im Normalbetrieb ausreichenden Systemen (N) ein redundantes (+1) zusätzlich errichtet, das im Fehlerfall des Primärsystems den Betrieb weiterführen kann. Zu „N“ (Anzahl) Systemen existiert also mindestens ein weiteres System. Die N+1.Redundanz hat jedoch eine konstruktive Schwäche. Sollte das Primärsystem ausfallen und die Redundanz den Dienst erbringen, steht in einem zweiten zeitgleichen Fall kein weiters redundantes System zur Verfügung. Für Systeme mit besonders hohen Anforderungen an die Verfügbarkeit ist also ein höherer Grad an Redundanz erforderlich (siehe auch Beitrag „Prinzipien der Verfügbarkeit“ des HV-Kompendiums).

Eine weitere Möglichkeit zur Realisierung einer hochverfügbaren Infrastruktur stellt die Härtung dar, also die Einrichtung einer ausreichend widerstandsfähigen Außenhaut von Sicherheitsbereichen. Nach einer Risikoanalyse und der Identifizierung von Objekten mit hohem Schutzbedarf sind die Widerstandsklassen festzulegen und die entsprechend Maßnahmen auszuwählen, die geeignet sind, potenzielle Angriffe abzuwehren.

Die vorliegende Orientierungshilfe ist unter Beachtung existierender Sicherheitsstandards, Normen und Regelwerken (DIN, ISO, VdS, BSI) verfasst worden und soll dem Leser einen kompakten und allgemein verständlichen Überblick über wichtige Aspekte bei der Planung von hochverfügbaren Infrastrukturen geben.

2 Standort

Die Umsetzung von Maßnahmen für eine hohe Verfügbarkeit beginnt nicht erst innerhalb des Gebäudes, sondern bereits vor den „Toren“. Ob Neubau oder bestehendes Gebäude, die Sicherheitsanforderungen an den Standort sind bereits bei der Konzeption zu berücksichtigen. Für die Auswahl eines Standorts steht vor allem die vollständige der Umsetzbarkeit von Sicherheitsanforderungen im Vordergrund. So werden bei der Planung leider zu häufig solche Gebäude oder Gebäudeteile zum Betrieb hochverfügbarer Infrastrukturen ausgewählt, für die sonst keine andere Verwendung zu finden ist. Die Voraussetzungen hinsichtlich der Sicherheit spielen dabei oftmals eine untergeordnete Rolle. Unzureichende Voraussetzung können, auch nicht durch den Einsatz noch so hochwertiger Sicherheitstechnik, im Nachhinein geheilt werden. Die richtige Wahl des Standortes ist nicht trivial und Versäumnisse im Vorfeld können sich nachhaltig negativ auf die Verfügbarkeit der Infrastruktur auswirken.

So sollte ein im Vorfeld in Auftrag gegebenes geophysikalisches Gutachten Risiken, die von Elementarereignissen ausgehen, identifizieren und bewerten. Standorte, die unmittelbar durch elementare Einflüsse wie Hochwasser, Lawinen, Erdbeben oder Erdrutsch gefährdet sind, sollten vermieden werden. Bodensenkungen und Bergschläge, die infolge aktiven Bergbaus auftreten können, sind ebenso zu berücksichtigen, wie die Nähe zu stillgelegten Zechen.

Auch sind „Brachen“, auf denen früher Fabriken, chemische Betriebe oder Mülldeponien angesiedelt waren, genauer zu begutachten. Es besteht die Wahrscheinlichkeit, auf diesen stillgelegten Bereichen Bodenkontaminationen zu finden. Ferner ist auf Leckagen defekter Abwasserkanäle, Tanklager oder Rohrleitungen zu achten, aus denen schädliche Bodenveränderungen resultieren könnten.

Ebenso wenig ist ein Standort mit Hanglage zu favorisieren. Obwohl dies heutzutage kein nennenswertes Bauproblem darstellt, ist nicht jedes Grundstück für eine Hangbebauung geeignet. Risse in Straßen, die parallel zum Hang verlaufen, deuten oftmals auf Erdbewegung hin. Ein Bodengutachten sollte dem Vorhaben vorausgehen.

Nicht minder bedrohend für die Verfügbarkeit der Infrastruktur erweisen sich in unmittelbarer Nähe befindliche Betriebe, Lagerstätten oder Transportwege mit Gefahrengut sowie Flughäfen, Kraftwerke oder militärische Einrichtungen. Tritt bei einem der genannten „Nachbarn“ ein ernsthafter Zwischenfall auf, können für den Betrieb und somit auch für die Verfügbarkeit der Infrastruktur Sekundärschäden entstehen. In Industriegebieten ist zudem mit einer höheren Emissionsbelastung zu rechnen.

Beachtung sollte ebenfalls die direkte Nähe zu elektromagnetischen Quellen finden. Eine starke Sendeleistung von Sendeanlagen kann zu Störungen empfindlicher Infrastruktur-Systemen führen und somit die Verfügbarkeit einschränken oder sie zum völligen Erliegen bringen.

Eine günstige Verkehrsanbindung des Standorts sollte hilfeleistenden Kräften (Feuerwehr, Polizei) kurze Anfahrtszeiten gewährleisten.

Abschließend ist zu erwähnen, dass für einen sicheren und störungsfreien Betrieb der Infrastruktur auch organisatorische Maßnahmen wie Wartung und die rasche Wiederherstellung von defekten oder gestörten Komponenten erforderlich sind. Werden diese Aufgaben an externe Dienstleister vergeben, sind Aspekte der örtlichen Nähe, Reaktions- und Reparaturzeiten wie auch die Anzahl der Mitarbeiter der Serviceleistenden entscheidend bei der Wahl des Standortes.

3 Perimeterschutz

Die Hauptaufgabe des Perimeterschutzes ist es, Zeit für die Alarmierung und das Eintreffen von Interventionskräften im Fall der Detektion eines unbefugten Geländezutritts zu gewinnen, um das weitere Vordringen eines Angreifers in das Gebäude zu verhindern. Eine Strategie zur Etablierung eines effektiven Perimeterschutzes sollte in der Regel aus Maßnahmen unterschiedlicher Bereiche bestehen. Dazu gehören mechanisch-bauliche, organisatorisch-personelle und elektronische Detektions-Maßnahmen. Entscheidend ist, dass die gewählten Einzelmaßnahmen untereinander abgestimmt sind und sich in ihrem Zusammenwirken Additiv auf die Gesamtzielsetzung auswirken.

Perimeterschutz bedeutet auch Schutz der Infrastruktur und muss bereits bei der Planung berücksichtigt werden.

Während der Planungsphase sind im Rahmen einer Gefährdungsanalyse die Schutzziele und Bedrohungsszenarien zu identifizieren, aus denen später erforderliche Maßnahmen zielgerichtet abgeleitet werden können. Dabei sind Hauptbedrohungen wie Sabotage, Überfall, Diebstahl, Spionage und Vandalismus genauer zu betrachten.

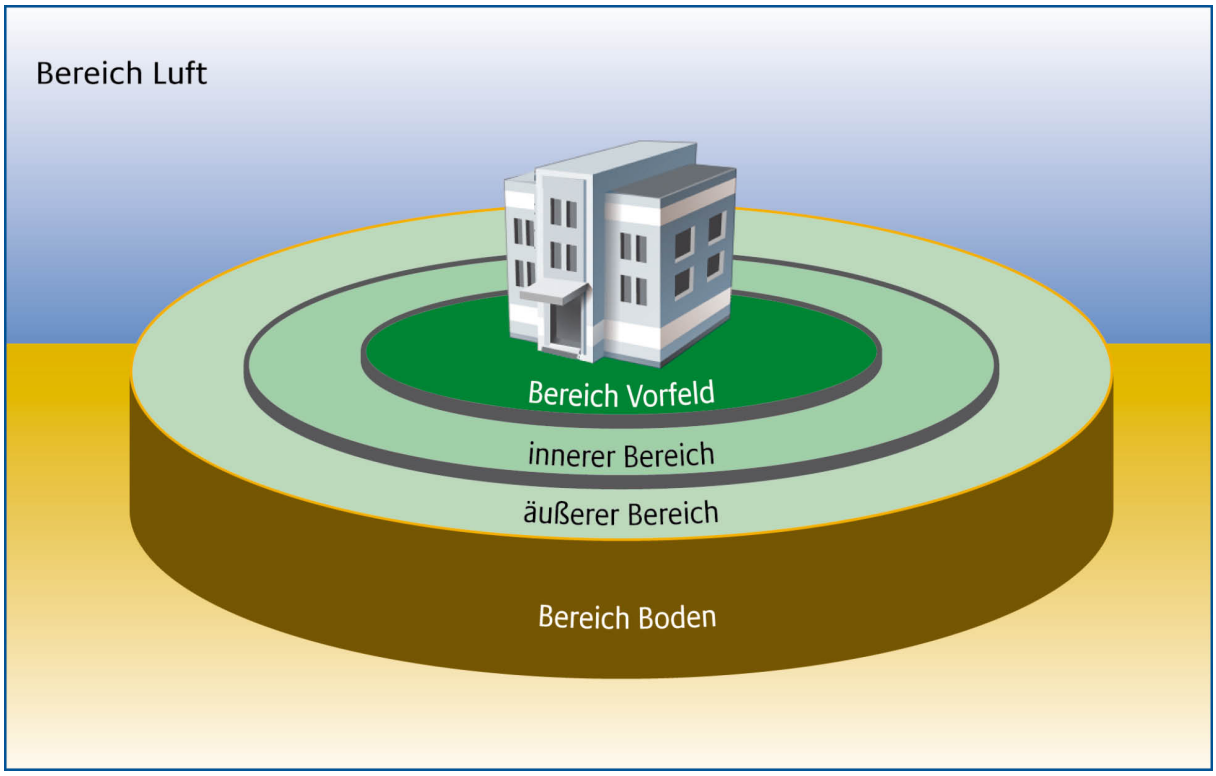


Abbildung 1: Bereiche des Perimeterschutzes

Die Abbildung 1 stellt die verschiedenen Teilbereiche des Umfeldes eines Gebäudes dar. Dazu gehören der weitläufige Bereich des Freigeländes, unterteilt in einen äußeren und inneren Bereich, der Bereich Vorfeld in der unmittelbaren Nähe vor dem Gebäude, der Bereich unterhalb sowie der Bereich oberhalb des Gebäudes. Die Gebäudeaußenhaut stellt nach dem Perimeterschutz weitere Sicherheitsmechanismen zur Verfügung und berücksichtigt ebenfalls vorhandene Gebäudeelemente wie das Dach, Fenster oder die Gebäudezugänge.

3.1 Möglichkeiten des Freilandschutzes

Bei der Gestaltung der Flächen zwischen äußerster Grundstücksgrenze und Gebäude sind die Interessen hinsichtlich der architektonischen Gestaltung und der Etablierung von Sicherheitsmaßnahmen gegenläufig. Der Landschaftsarchitekt ist eher an einer naturnahen Geländeformung und Bepflanzung interessiert, der Sicherheitsplaner indes an freien Sichtverhältnissen bzw. an einer Begrenzungsanlage. Letztendlich stellt auch das Gebäude-Management Anforderungen an die Wartung und Pflege der Flächen. Daher ist schon bei der Planung der Landschafts- und Sicherheitsmaßnahmen eine frühe und enge Zusammenarbeit aller Interessengruppen anzustreben. Dabei ist der Integration von wirkungsvollen Schutzmaßnahmen in die Landschaftsgestaltung der Freiflächen ein hoher Stellenwert einzuräumen.

Grundsätzlich ist die Topologie der Freiflächen auf Gefahrenquellen zu prüfen. Hohe bzw. mittelgroße Bepflanzung wie Bäume, Sträucher oder Büsche sowie Bodenwellen stellen eine Gefahrenquelle dar, die einem Täter als Sichtschutz dienen kann. Mit der Zeit in der Nähe einer errichteten Barriere eventuell entstandenen Erweiterungsbauten (Trafo-, Müllcontainerhäuschen, Garagen etc.), können einem Eindringling als Übersteighilfe dienen.

Die Minimalanforderung an eine mechanische Barriere ist eine eindeutige Kennzeichnung des Grundstückes. Als sichtbares Hindernis soll sie primär eine unbedachte Überschreitung der Grundstücksgrenze verhindern sowie den vermeintlichen Täter abschrecken und ihm das Eindringen in das Gelände erschweren. Abhängig von den gewählten Barrieren kann deren Überwindung Sekunden bis hin zu mehreren Minuten dauern. Je komplexer die gewählten Barrieresysteme gestaltet sind, desto größer ist die Möglichkeit, dass der Täter von seinem Vorhaben absieht.

Die Trennung des äußeren vom inneren Bereich des Freigeländes kann durch bedarfsorientierte Barrieresysteme wie Mauern, Zäune, Stacheldrahthindernisse, Übersteigschutz, Fahrzeugbarrieren sowie der Sicherung von Zufahrten und Toren durch Drehtüren, Drehtore etc. realisiert werden.

Für einen wirksamen Schutz sollten mechanische Barrieren, die primär zur Abwehr von Übergriffen und Erhöhung des Zeitwiderstandes installiert sind, zusätzlich mit elektronischen Detektionssystemen ergänzt werden. Sie werden als reaktive Systeme für die Erkennung, Meldung und Protokollierung von versuchten Übergriffen eingesetzt.

Technische Detektionssysteme bestehen in der Regel aus einem Sensorteil, über den die eigentliche Detektion eines physikalischen Ereignisses aufgenommen wird und einem Auswerteteil, der das Ereignis entweder visuell, akustisch oder kombiniert meldet. Beide Komponenten bilden für sich ein geschlossenes System, das entsprechend den Schutzzielen und den Umfeldbedingungen autark oder durch Unterstützung des Menschen (Wachpersonal) eingesetzt werden kann. Alternativ kann auf einen Einsatz von Detektionssystemen verzichtet und auf einen Wachdienst zurückgegriffen werden. Entscheidend für den Einsatz einer der genannten Detektionssystem-Strategien ist letztendlich die Zielsetzung.

Technische Detektionssysteme sind kostspielig in der Anschaffung und der Wartung, besitzen aber den Vorteil einer permanenten und nahezu vollständigen Überwachung aller Teilbereiche (siehe)). Die unterschiedlichen Gegebenheiten in den Teilbereichen erfordern verschiedene physikalische Detektionsprinzipien, die sich bestimmte physikalische Effekte zunutze machen. Hierzu existieren verschiedene Sensortypen, die für die Detektion im Boden als Bodensensoren oder Boden-Raumsensoren, am Zaun als Zaunsensoren oder Zaun-Raumsensoren, in der freien Fläche als frei stehende Sensorsysteme und im Wasser als Wasserraumsensoren oder Wasser-Barrieresensoren eingesetzt werden.

Jeder Sensortyp reagiert auf unterschiedliche Detektionsart. So erkennen z. B. Bodensensoren Ereignisse, die durch Druckwellen, Schock, Gewicht oder Druck ausgelöst werden. Körperschall und Vibration können sowohl von Boden- als auch Zaunsensoren erfasst werden. Darüber hinaus werden von Zaunsensoren das Zerschneiden von oder ein Kurzschluss in elektrisch geführten Sensorsystemen sowie Unterbrechungen in Lichtwellenleitern erkannt. Die Möglichkeiten der Überwachung des Bereichs oberhalb eines Gebäudes sind begrenzt. Falls der Bedarf einer Luftüberwachung notwendig ist, können Maßnahmen mittels Videosystemen oder Radar realisiert werden.

Freiraumsensoren basieren auf dem Sender-Empfänger Prinzip und benötigen für ihre Installation keine feste Struktur, auf der sie angebracht werden müssen. Sie eignen sich sehr gut für die Überwachung von weitläufigem und schwierigem Gelände und sind für einen Eindringling nicht auf Anhieb zu erkennen. Zum Einsatz kommen Infrarot-, Laser-, Schall- oder Mikrowellen-Sensorsysteme.

Welches der Sensorsysteme zum Einsatz kommt, hängt von den Umgebungsbedingungen, dem zu überwachenden Bereich und den Anforderungen, die das System erfüllen muss, ab.

Zu einem effektiven Detektionssystem gehört ebenfalls eine möglichst intelligente Auswerteeinheit, die in der Lage ist, das durch einen Eindringling verursachte Ereignis von anderen Effekten zu unterscheiden. Sie sollte zwischen dem Ausfall eines Systembauteils oder eines Sensors, der Detektion eines Eindringens und z. B. einem durch Witterungseinflüsse bedingten Fehleralarm unterscheiden und entsprechend reagieren können. Gute Detektionssysteme zeichnen sich dadurch aus, dass ihre Falschmeldungsrate bei ca. einem Fehlalarm pro Monat und Kilometer liegt. Vollkommen falschmeldungsfreie Freilanddetektionssysteme dürften entweder für den Einsatzort ungeeignet, zu unempfindlich eingestellt oder defekt sein.

Die richtige Wahl eines für den angestrebten Zweck geeigneten Detektionssystems sollte sich an seiner Wirksamkeit orientieren und die Gesamtsicherheit erhöhen. Deshalb ist während der Planung eine genaue Analyse des Bedrohungsbildes ebenso notwendig wie die Ermittlung der Bedrohungsarten, die für das zu schützende Objekt (Gelände, Gebäude etc.) infrage kommen könnten. Es ist darauf zu achten, dass das ausgewählte Detektionssystem durch ein kompetentes Fachpersonal installiert, fachgerecht kalibriert und im Rahmen eines Pilotbetriebs umfangreich getestet wird. Nach der Abnahme sollten das administrative Personal eingewiesen und die Mitarbeiter sensibilisiert werden. Eine regelmäßige Wartung der Anlage durch Fachpersonal ist unerlässlich.

3.2 Beleuchtung

Bei der Perimeterbeleuchtung handelt es sich um die Sicherstellung des Gebäudeschutzes durch ergänzende Sicherheitsmaßnahmen mittels Illumination.

Für den unmittelbar um das Gebäude befindlichen Freiraum (Vorfeld) erscheint es zweckmäßig, diesen, für eine bessere Ausleuchtung und Überwachung, frei von jeglicher Bepflanzung bzw. Ausbauten zu belassen. So gilt analog zur Gestaltung der Freifläche, dass ein nicht einsehbarer Bereich Eindringlingen eine gute Deckung bietet und gleichzeitig patrouillierendes Wachpersonal gefährdet. Üblicherweise wird die Überwachung des Vorfeldes durch eine Videoüberwachung vorgenommen.

Ein richtig geplantes und installiertes Beleuchtungssystem unterstützt den Wachdienst bei seinen Patrouillen und steigert die Effizienz der Videoüberwachung. Dabei erweist sich die Ausrichtung und Anordnung der Beleuchtungselemente weg vom Gebäude als sinnvoll. Der Wachdienst hat

damit die Möglichkeit, sich im Schattenbereich zwischen Gebäude und beleuchteter Fläche aufzuhalten und kann einen Eindringling gut erkennen. Gleichzeitig wird der Eindringling geblendet. Leider kommt es auch immer wieder vor, falls Beleuchtung und Videoüberwachung nicht aufeinander abgestimmt sind, dass durch die waagerecht ausgerichteten Leuchtelemente die Videoüberwachung durch Blendung beeinträchtigt wird. In diesem Fall sollten Mastleuchten das Vorfeld und die inneren Freiflächen sowie das Gebäude mit vertikal am Gebäude angebrachter Beleuchtung ausgeleuchtet werden. Durch die Kombination der im Freigelände und am Gebäude installierten Beleuchtung kann das Wachpersonal die zu überwachenden Bereiche besser einsehen und auf Gefahren schneller reagieren. Gleichzeitig ist der beeinträchtigungsfreie Betrieb der Videoüberwachung gewährleistet. Auf eine auffällige Scheinwerferbeleuchtung, wie sie gerne zu Imagezwecken eingesetzt wird, sollte verzichtet werden, um nicht unter Umständen die Aufmerksamkeit von Angreifern auf das Objekt zu lenken.

3.3 Pförtner- und Wachdienst

Die Kontrolle der Zugänge und Zufahrten zum und im Betriebsgelände ist immer noch eine wichtige Aufgabe, die in der Regel von Menschen bewerkstelligt und durch den Pförtner- und Wachdienst abgedeckt wird.

Der Pförtnerdienst identifiziert und registriert an zentraler Stelle Personen, die Zutritt zum Gelände oder Gebäude wünschen. Die Mitarbeiter der Pforte haben die primäre Aufgabe und Verantwortung, die Zutrittsregelungen, die auch die Besucherregelung beinhaltet, zu kontrollieren und auf deren Durchsetzung zu achten. Die Zutrittsregelungen gelten gleichermaßen für Mitarbeiter wie auch für Besucher. Die Pforte dokumentiert und meldet Verstöße der Zutrittsregelung. Hierzu sind den Mitarbeitern der Pforte klare Handlungsanweisungen auszuhändigen. Die Mitarbeiter der Pforte regeln zusätzlich die Zufahrt und Ausfahrt zum Gelände oder Gebäude. Darüber hinaus müssen diese Mitarbeiter mit den installierten (Gefahren-)Meldeanlagen (Zutritt, Einbruch, Brand, Video etc.) vertraut sein und für die Interpretation von Ereignisdaten wie Alarmen geschult sein.

Zusätzlich können, vorwiegend außerhalb der regulären Betriebszeiten, Kontrollgänge über das Betriebsgelände durch den Wach- oder Streifendienst notwenig sein. Wurde bei der Gestaltung des Perimeterschutzes auf eine technische Detektion verzichtet, sollte der Wachdienst in regelmäßigen Zeitenintervallen, aber zu unterschiedlichen Tageszeiten, das Gelände begehen. Ob dieser permanent vor Ort ist oder erst zu bestimmten Zeiten erscheint, ist von der Überwachungsstrategie und dem Schutzbedarf des zu schützenden Objektes abhängig. Eine permanente Präsenz des Wachdienstes ist jedoch einer gelegentlichen vorzuziehen. Da das Personal ständig vor Ort ist, gibt es keine von außen offenkundigen „Nichtbewachungszeiten“ (parkende Fahrzeuge des Wachdienstes). Bei ständig anwesendem Personal muss ein Angreifer mit unregelmäßigeren Wachrhythmen und zusätzlichen Wachgängen rechnen. Sein Entdeckungsrisiko steigt. Die Wahrscheinlichkeit, dass Ereignisse früher entdeckt werden, ist größer. Bei ortsfestem Personal ist davon auszugehen, dass es die Liegenschaft besser kennt. Streifengänge können so effektiver durchgeführt werden. Es ist dabei auf eine ausreichende Ausstattung des Streifendienstes zur Eigensicherung und Überwachung (Funkgeräte etc.) zu achten.

Der Pförtner- und Wachdienst muss bei der Ausarbeitung eines Gesamtsicherheitskonzeptes berücksichtigt werden. Nicht zuletzt ist auf eine fachgerechte Schulung und Sensibilisierung des Überwachungspersonals zu achten. Bei der Vergabe von Wachdienstleistungen an Externe sollte der beauftragte Dienstleister Erfahrung und Kompetenz nachweisen können. Der genaue Umfang der Dienstleistung muss auf dem Gesamtsicherheitskonzept basieren und ist schriftlich zu vereinbaren.

Ein existierender Pförtner- und Wachdienst wird bei der Ausgestaltung baulich-technischer Maßnahmen gegen unbefugten Zutritt oft in der Weise berücksichtigt, dass diese Maßnahmen etwas schwächer ausgeführt werden. Es ist daher unerlässlich, bei jeder Änderung des Pförtner- und Wachdienstes, die Auswirkungen dieser Änderung auf die Eignung baulich-technischer Maßnahmen zu überprüfen. Es wäre z. B. ein Kardinalfehler, den Pförtner- und Wachdienst aus Kostengründen komplett aufzugeben, ohne (bei unverändertem Schutzbedarf) die baulich-technischer Maßnahmen entsprechend zu ertüchtigen.

4 Gebäudesicherheit

Die Gebäudeinfrastruktur zum Betrieb von IT-Systemen dient der zuverlässigen Bereitstellung der notwendigen technischen, organisatorischen und personellen Ressourcen. Dabei ist jeder Betreiber bestrebt, Schwankungen der Betriebsparameter zu vermeiden und eine konstante Umgebungsbedingung zum Betrieb hochverfügbarer Infrastrukturen zu schaffen.

IT kann nur dann betrieben werden, wenn grundsätzliche Rahmenbedingungen wie das Vorhandensein eines Gebäudes, der Energie- und Kommunikationsanbindungen und geeigneter Räumlichkeiten erfüllt sind. Diese Rahmenbedingungen gilt es, vor Bedrohungen durch Unbefugte oder vor der Einwirkung höherer Gewalt zu schützen.

Eine robuste Gebäudeinfrastruktur muss mehr als nur den Schutz vor „klassischen“ Bedrohungen wie Sabotage und Diebstahl gewährleisten. So sind erhöhte Feinstaubkonzentrationen oder der Ausstoß von Schadstoffen nicht zu vernachlässigende Aspekte bei der Planung der Gebäudesicherheit. Nicht zuletzt muss die Gebäudesicherheit auch Folgen technischer Defekte oder höherer Gewalt wie Brand, Wassereintritt, Überspannung und Explosion abfangen.

4.1 Funktionale Aufteilung

In der Regel werden Funktionsbereiche entsprechend der Ressourcenfunktionalität definiert und anhand ihrer Schutzbedürftigkeit angeordnet. Durch die Trennung in Funktionsbereiche (z. B. Produktion, Administration, Versorgung, Haustechnik) kann der Schutz der Produktivsysteme aufrecht, sowie die erforderlichen Betriebsparameter konstant gehalten werden. Die Funktionstrennung erfolgt grundsätzlich durch Isolation und Separation innerhalb von Sicherheitszonen, um eine gegenseitige Beeinflussung auszuschließen, oder damit sich ein Schaden nicht auf alle Bereiche auswirkt. Die Isolation erfolgt durch Schottung von Räumen oder Bereichen gegenüber Gefahren, die von innen oder außen auf hochverfügbare Infrastrukturen einwirken können. Hier ist die Schottung gegenüber Brand, Rauch, mechanischer Beanspruchung oder unbefugtem Zutritt zu nennen. Die Schottung erfolgt für Räume z. B. durch geeignet dimensionierte Wände, Decken, Türen, Fenster oder Kabeldurchführungen. Die Separation erfolgt durch eine räumliche Aufteilung. So sind technische Anlagen, IT-Systeme oder Bürobereiche durch bauliche Maßnahmen voneinander zu trennen. Die Kontrolle der Separation erfolgt durch Meldeanlagen, wie z. B. einer Zutrittskontrollanlage. Der Schutzbedarf jeder Sicherheitszone bestimmt die umzusetzenden baulichen und technischen Maßnahmen. Sicherheitszonen sollten nach dem klassischen Zwiebelschalenprinzip definiert werden. Die Widerstandsfähigkeit der Sicherheitszonen gegenüber Bedrohungen wird maßgeblich durch deren Lage im Gebäude bestimmt und nimmt zum Inneren des Gebäudes zu.

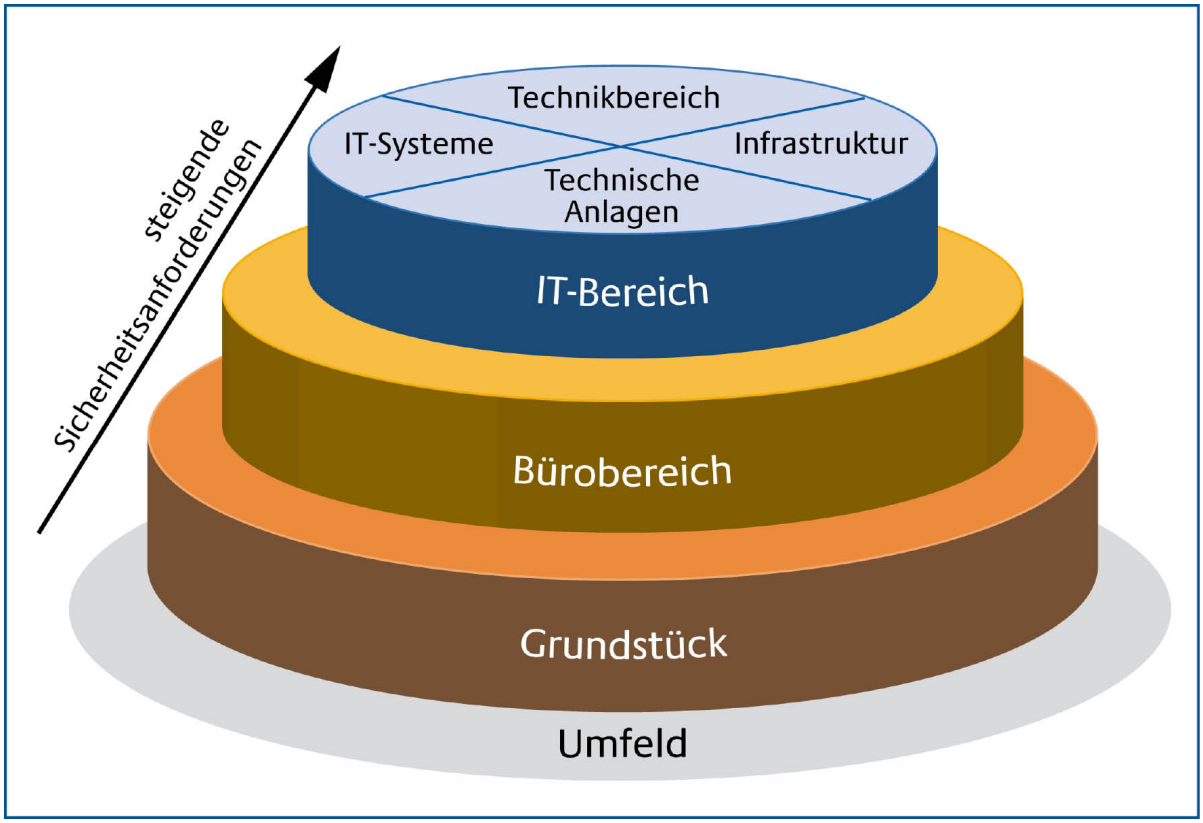


Abbildung 2: Anordnung der Sicherheitszonen

Die Abbildung 2 zeigt schematisch ein Beispiel, wie Sicherheitszonen definiert werden können. Das Umfeld (grau) wird, wie im Kapitel Perimeterschutz beschrieben, durch bauliche Maßnahmen vom Grundstück (dunkelbraun-orangefarbene) an dessen äußerer Grenze getrennt. Über das Grundstück können Büroräume (hellbraun-goldgelb) in öffentlichen Bereichen erreicht werden. Alle nicht öffentlichen und schützenswerten Bereiche (blau) sollten ohne Zutrittskontrollen nicht zu erreichen sein. In diesen Bereichen befinden sich die sicherheitskritischen Systeme der IT und die Überwachungs- sowie Haustechnik, die zum hochverfügbaren Betrieb notwendig sind.

An jedem Zonenübergang sollte eine Zutrittskontrolle zu installieren sein. Dabei ist zu berücksichtigen, dass die Sicherheitsanforderungen von außen nach innen steigenden gleichzeitig aber die Zahl der Berechtigten sinkt. Die Zutrittskontrolle zwischen Umfeld im wesentlichen auf hohen Durchsatz ausgelegt sein. Eine möglichst kleine Zahl von Personen, die trotz fehlender Zutrittsberechtigung eingelassen werden, muss hier hingenommen werden. Zum eigentlichen Sicherheitsbereich hin müssen nur noch wenige Personen, die aber mit hoher Erkennungssicherheit bewältigen muss. Die Erkennungssicherheit muss hier ggf. so hoch gefahren werden, dass selbst Berechtigte im Einzelfall mit einer Abweisung durch das System rechnen müssen.

In Abhängigkeit von den in den Bereichen installierten Systemen sollten in einem Sicherheitskonzept die Zonen definiert und einem Sicherheitsniveau zugeordnet werden. Prinzipiell sind sämtliche Sicherheitszonen durch Separationsmaßnahmen, also durch das Errichtung von Widerständen von Zone zu Zone, voneinander zu trennen.

4.2 Hochbau

Der Hochbau eines Gebäudes sollte einer hochverfügbaren Infrastruktur Schutz vor schädlichen Umwelt- und Elementareinflüssen bieten. Hierzu muss das Gebäude über redundante konstruktive Eigenschaften und technische Einrichtungen verfügen, damit die erforderlichen Rahmenbedingungen zum sicheren Betrieb der IT-Infrastruktur dauerhaft konstant bleiben.

Äußere Einflüsse bedingen den Grad der Stabilität im Inneren des Gebäudes. Klimatische Veränderungen (Wärme, Kälte) muss die Gebäudehaustechnik abfangen und ausgleichen. Sie muss zum Schutz der Versorgungseinrichtungen und der IT-Systeme vor den vielfältigen äußeren Einflüssen (Wasser, Sturm, Erschütterungen, Blitz) vorbeugende Maßnahmen umsetzen.

Das Gebäude bietet mit seiner Außenhaut zudem Schutz gegen das Eindringen Unbefugter. Eine Freiland-Überwachung kann das Eindringen Unbefugter zwar melden und in gewissem Umfang erschweren, keinesfalls aber auf Dauer verhindern. Es muss immer damit gerechnet werden, dass Unbefugte bis an die Gebäudeaußenhaut gelangen und dort in der Lage sind, einen Einbruch zu verüben. Ein Schutz der gesamten Gebäudeaußenhaut oder von Teilbereichen ist somit für hochverfügbare Infrastrukturen zwingend erforderlich. Mechanische Schutzmaßnahmen, auch Härtung genannt, verfolgen den Zweck, durch Stabilität einen Angreifer für eine gewisse Zeit aufzuhalten und damit hilfeleistenden Kräften Zeit zur Intervention zu geben oder den Angreifer zur Aufgabe seines Vorhabens zu bewegen.

Erdgeschoss- und Kellerräume können für einen Angreifer direkt, Obergeschosse ggf. über Steighilfen wie Fluchtbalkone und -treppen, Fassadenbefahrungsanlagen, Regenfallrohre, Blitzableiter, Rankgitter, Anbauten oder Fenstervergitterungen erreichbar sein. Die Außenhauthärtung muss sich daher auf alle für Unbefugte erreichbaren Gebäudeöffnungen (Fenster, Türen, Schächte) erstrecken.

Gefahren wie Brände oder Explosionen in unmittelbarer Nähe des Gebäudes müssen wirksam durch die mechanischen Schutzmaßnahmen des Gebäudes abgewehrt werden. Neben dem Abstand zur Gefahrenquelle als einfachste Maßnahme müssen die Außenwände über eine hohe konstruktive Robustheit und hohen mechanischen Widerstand verfügen. Hierzu werden Materialien in Widerstandsklassen eingeteilt. Verschiedene Normen definieren Widerstandsklassen von Bauelementen in Gebäuden (Wände, Decken, Fenster oder Türen) gegenüber Bränden oder mechanischer Beanspruchung. Für die Errichtung von Gebäuden, in denen hochverfügbare Infrastrukturen betrieben werden, sollten die Widerstandsklassen abhängig vom Schutzbedarf ausgewählt werden.

4.3 Wände und Decken

Eine Musterempfehlung für die zu verwendende Wand- und Deckenkonstruktion oder der zum Ausbau verwendenden Baustoffe kann an dieser Stelle nicht gegeben werden, da die Auswahl sich immer an den individuellen Gegebenheiten vor Ort und den Sicherheitsanforderungen orientieren muss. Grundsätzlich sind hohe Widerstandswerte gegen mechanische und thermische Beanspruchung anzustreben. Hinsichtlich der mechanischen Belastbarkeit über die rein statischen Erfordernisse hinaus definiert die DIN V ENV 1627 bestimmte Wandkonstruktionen für den Einbau Einbruch hemmender Türen. Weiteres dazu siehe unter 5.3.2 Türen.

Neben den klassischen Wänden aus Beton, Mauerwerk oder Gipskarton existieren weitere Wandkonstruktionen, die sich als Speziallösungen etabliert haben. Diese speziellen Ständerwandkonstruktionen mit besonderer Wandverkleidung und -füllung kommen z. B. dann in

Betracht, wenn eine Wand wegen zu geringer Deckentraglast nicht in Mauerwerk oder Beton ausgeführt werden kann. Nicht zu verwechseln sind diese speziellen Lösungen mit den gebräuchlichen Ständerwandkonstruktionen, die üblicherweise in Bürogebäuden zur Abtrennung von Räumen genutzt werden.

Häufig werden Raum in Raum Lösungen, also die Errichtung eines eigenen Raums zur Sicherung von hochverfügbaren Infrastrukturen in einem bestehenden Raum, in Metallkassettenbauweise mit speziellen Wandfüllungen ausgeführt. Diese Konstruktion soll eine einfache Installation mit einer hohen Robustheit gegenüber thermischer und mechanischer Belastung verbinden. Die Gebäudeaußenhaut stellt einen elementaren Schutz zur Verfügung. Sie bündelt alle weiteren Sicherheitsmaßnahmen und stellt sichere Betriebsflächen zur Verfügung. Hierzu ist eine gewisse Robustheit notwendig, die durch die verwendete Konstruktion und die eingesetzten Baustoffe der Gebäudebestandteile bestimmt wird. Die im Betonskelettbau üblicherweise eingesetzten Fassadenelemente bieten in der Regel noch keinen ausreichenden Schutz gegen den Zutritt Unbefugter. Zur Sicherung hochverfügbarer Infrastrukturen sind weitere Schutzmaßnahmen zu treffen, auf die nachfolgend näher eingegangen wird.

5 Gebäudeausbau

Der Ausbau eines Gebäudes bestimmt in hohem Maße die Sicherheit des Bereichs, in dem hochverfügbare IT-Systeme betrieben werden. Der Ausbau der Funktionsbereiche im Inneren eines Gebäudes ist entscheidend für die mechanische Robustheit und den Widerstand gegenüber Gefahren wie Sabotage, Diebstahl sowie Elementarschäden. Nicht immer ist die technisch aufwendige und kostenintensive Sicherung der gesamten Außenhaut eines Gebäudes notwendig. Sind nur bestimmte, klar umrissene Bereiche schutzbedürftig, reicht es gegebenenfalls aus, nur diese an ihren Grenzen zu anderen Bereichen zu schützen. Dabei ist besonders zu beachten, dass es innerhalb eines Gebäudes eine Reihe zusätzlicher, meist versteckter Öffnungen bestehen (z. B. Klima- und Lüftungskanäle, durchgehende Doppelböden, Schächte von Personen-, Lasten- oder Materialaufzügen), die einen Übergang vom ungesicherten zum zu sichernden Bereich ermöglichen. Analog zur Außenhauthärtung sind auch im Innenbereich alle offiziellen und verdeckten Zugänge mit geeigneten Maßnahmen zur Steigerung der Robustheit auszustatten. Diese Maßnahmen beziehen sich im Wesentlichen auf die Bereiche der Decken, Böden, Fenster und Türen.

5.1 Abgehängte Decken

Abgehängte Decken werden zumeist als Installationsraum für die Leitungsführung der Energieversorgung oder Kommunikationstechnik sowie für Komponenten der Gefahrenmeldeanlagen (z. B. Brandmelder) verwendet. Darüber hinaus sie gern als Installationsort der Raumbeleuchtung oder der Versorgungskanäle der Klimatisierungsanlage oder Lüftung verwendet. Daneben bieten abgehängte Decken auch den vermeintlichen Vorteil der Verblendung unansehnlicher Technik. Diesen eher optischen Vorteilen stehen jedoch handfeste Nachteile gegenüber, vor allem, wenn in den Räumen hochverfügbare IT-Systeme betrieben werden. Der Installationsraum der abgehängten Decke bietet den Raum für eine „wuchernde Verkabelung“. Es besteht die Gefahr, dass alte Kabel nicht deinstalliert werden und so irgendwann die Traglast der Kabelpritschen überschritten wird. Zudem bietet die abgehängte Decke Raum für Manipulationen an den Gefahrenmeldeanlagen oder den Detektionskomponenten, wie z. B. Rauchmeldern. Weiterhin können Nachlässigkeiten bei nachträglichen Installationsarbeiten oder der Brandschottung unentdeckt bleiben und die regelmäßige Inspektion der technischen Komponenten durch das Wartungspersonal erschweren. Zudem stellt die abgehängte Decke eine zusätzliche Trümmerlast im Brandfall oder bei Erschütterungen dar. Es sollte daher auf abgehängte Decken gänzlich verzichtet werden.

5.2 Doppelböden, Bodenbeläge

Ein Doppelboden bietet zahlreiche Möglichkeiten zur Installation von Technik und eine optimale Zugänglichkeit. Bei einem Doppelboden handelt es sich um einen aufgeständerten Fußboden ab einer Höhe von ca. 60 cm oberhalb des Rohbodens. Ein Doppelboden besteht aus vorgefertigten Bodenplatten, welche auf entsprechenden Stützen gelagert und eingebaut werden. Ein Doppelboden dient primär der Belüftung des Raums, in denen IT-Systeme betrieben werden. Die Belüftung des Technikraums durch einen Doppelboden stößt jedoch immer häufiger an ihre Grenzen, da die Packungsdichte der IT-Systeme zunimmt und der Doppelboden als Installationsort dient (siehe hierzu auch das Kapitel Klimatisierung).

Da die Bodenelemente einzeln entfernt werden können, bietet ein Doppelboden neben seiner ursprünglichen Hauptaufgabe der Belüftung auch die Möglichkeit der einfachen Verlegung von Leitungen sowie der Installation größerer Technik-Komponenten. Bei ausreichender Höhe können Kabeltrassen geordnet über eine Pritsche geführt werden, wie sie im Wand- oder Deckenbereich üblich sind. Für die Bodenoberfläche steht eine Vielzahl unterschiedlicher Beläge zur Verfügung. Die Qualität des Doppelbodens und des Belags wird durch die Tragfähigkeit, Brandschutz, Schallschutz und den Erdableitwiderstand bestimmt.

Die Vorteile und Freiheiten eines Doppelbodens bei der Nutzung bringen jedoch zugleich die Gefahr der wachsenden Unordnung. Die Notwendigkeit, nicht mehr benötigte Leitungen auszubauen, wird oft ignoriert. Dies und die in Doppelböden häufig anzutreffenden Kabel mit beabsichtigter Überlänge, sogenannte Vorratsschleifen, erhöhen die Brandlast. Zudem besteht die Gefahr, dass der notwendige Luftdurchsatz durch die Installation großvolumiger technischer Komponenten nicht mehr erreicht wird.

Aufgrund der beschriebenen Gefahren sind besondere Sicherheitsvorkehrungen bei der Planung, Installation und vor allem während des Betriebs von Doppelböden zu berücksichtigen. Es sollte generell darauf geachtet werden, dass nur absolut notwendige Kabel oder technische Komponenten in einem Doppelboden installiert werden und eine regelmäßige Revision durchgeführt wird. Nicht mehr benötigte Komponenten sind zu entfernen. Brandwände oder solche mit qualifiziertem Einbruchsschutz müssen auch im Doppelbodenbereich bis zum Rohboden ausgeführt werden. Bei Einbau einer automatischen Brandmeldeanlage ist der Doppelboden als separater Bereich, getrennt durch Brandmelder zu überwachen. Markierungen auf dem Boden oder eine Lageplan müssen die Position jedes Melders exakt angeben. Der Doppelboden sollte zusätzlich in die Überwachung durch eine Wassermeldeanlage eingebunden werden.

5.3 Türen, Eigenschaften und Arten

5.3.1 Brandschutztüren/Rauchschutztüren

Als Brandschutztüren werden solche Türen bezeichnet, die selbstschließend und feuerbeständig sind. Brandschutztüren müssen den gleichen Feuerwiderstand oder Funktionserhalt in Minuten aufweisen wie die Decken und die sie umgebende Wand. Brandschutztüren sind immer als System aus allen zugehörigen Bestandteilen anzusehen. Dazu gehören neben dem Türblatt, das Türband und der Rahmen sowie alle weiteren Ein- oder Anbauten wie das Schloss, die Drückergarnitur, ein elektrischer Türöffner etc. Die Brandschutztür entspricht nur dann den Bauvorschriften und erfüllt ihre Schutzfunktion verlässlich, wenn alle Teile in und an der Tür für den jeweiligen Brandschutzwert geprüft und zugelassen sind. Es existieren gemäß der Norm DIN 4102 verschiedene Schutzklassen, auch Feuerwiderstandsklassen genannt. Diese Feuerwiderstandsklassen gelten für selbstschließende Türen oder andere selbstschießende Abschlüsse, um ein Übergreifen eines Feuers in andere Bereiche zu verhindern. Es werden die folgenden Feuerwiderstandsklassen unterschieden, wobei die angegebene Ziffer die Feuerwiderstandsdauer in Minuten bei direkter Beflammung angibt: T30, T60, T90, T120 und T180. In hochverfügbaren Infrastrukturen sollten nur Brandschutztüren ab der Klasse T90 verwendet werden. Die Auswahl von Brandschutztüren muss sich an den Feuerwiderständen sowohl der Umgebung (Wände, Decken, Böden) als auch an den Vorgaben des Fluchtwegsystems oder den behördlichen Vorschriften z. B. der Feuerwehr orientieren.

Häufig wird fälschlicherweise angenommen, dass Brandschutztüren mechanisch so widerstandsfähig sind, dass automatisch auch ein Einbruchschutz besteht. Brandschutz und Einbruchschutz stellen vom Grundsatz her jedoch völlig unterschiedliche Forderungen an die Konstruktion. Eine Brandschutztür muss, um auch unter starker Wärmeeinwirkung nicht zu versagen, ausreichend Spiel nach allen Seiten haben. Eine Einbruchhemmende Tür hingegen sollte so genau und spielfrei wie möglich schließen. Soll der Brandschutz mit der Einbruchhemmung in einer Tür kombiniert werden, so dürfen nur Türen mit einer Zulassung verwendet werden.

Der Rauchschutz ist eine weitere Funktion, die an eine Tür gestellt werden kann. Diese Funktion hat die Aufgabe, die Ausbreitung von Rauch eines entfernten Brandes im Gebäude zu verhindern und dadurch Flucht- und Rettungswege rauchfrei zu halten. Neben einer reinen Rauchschutztür kann auch eine Brandschutztür oder eine einbruchhemmende Tür mit dieser Funktion zusätzlich ausgestattet werden.

Brandschutz- oder Rauchschutztüren müssen Funktionen des Einbruchschutzes und des Brandschutzes zum Schutz der IT-Systeme mit dem Personenschutz vereinen. Auf der einen Seite fordern Bauvorschriften, dass sich Türen im Verlauf von Fluchtwegen von innen leicht und ohne fremde Hilfsmittel öffnen lassen, solange sich Personen im Raum bzw. im Gebäude befinden. Ebenso ist die Feuerwehr daran interessiert, dass Türen den Einsatz nicht behindern und sie schnell und ungehindert vorrücken kann (Rettungsweg). Andererseits sollen diese Türen auch den Zutritt Unbefugter abwehren können. Inzwischen sind elektrische Systeme verfügbar, die eine optimale Synthese zwischen den Belangen des Personenschutzes und dem Schutz der IT gegen unberechtigten Zutritt ermöglichen. Diese Systeme erlauben eine elektronische Steuerung der Türverriegelung oder eine Offenhaltung von Türen durch die Brandmeldeanlage. Sollte ein Alarm ausgelöst werden, so werden Fluchttüren entriegelt oder offen stehende Brand- oder Rauchschutztüren automatisch geschlossen. Es ist darauf zu achten, dass der Zustand der Türen zweifelsfrei erkannt wird und ein Alarm zentral angezeigt wird. Dies ist insbesondere von Bedeutung, wenn die Tür auch den Einbruch in einen Bereich verhindern soll und über eine Einbruchhemmung verfügt.

5.3.2 Einbruchhemmende Türen

Hochverfügbare IT-Systeme müssen gegenüber unberechtigtem Zutritt, Sabotage oder Vandalismus geschützt werden. Türen haben generell die gegensätzliche Aufgabe, Sicherheits- oder Funktionsbereiche voneinander zu trennen aber auch durchlässig zu machen. Die Trennung erfolgt nicht nur gegenüber unberechtigten Externen, sondern ebenfalls gegenüber internen Mitarbeitern, die nur über Zutrittsberechtigungen für einzelne Funktionsbereiche verfügen.

Türen in Sicherheitsbereichen müssen eine hohe Robustheit gegenüber mechanischer Beanspruchung aufweisen und sind daher Einbruch hemmend aufgebaut. Um die Robustheit Einbruch hemmender Türen klassifizieren zu können, werden von der Norm DIN V/ EN V1627 einheitliche Bauteilewiderstandsklassen (WK) von WK 1 bis WK 6 definiert. Diese Widerstandsklassen beziehen sich allgemein auf Abschlüsse, also auf Türen, Fenster oder Rollläden. Bei der Auswahl einer Einbruch hemmenden Tür sind neben der mechanischen Robustheit auch der Einsatzzweck und die Handhabung der Tür von Bedeutung. So ist festzulegen, ob die Einbruchhemmung mit dem Brandschutz zu kombinieren ist oder ob eine einflügelige, zwei- oder mehrflügelige Tür notwendig ist, z. B. wenn sperrige Güter in den Sicherheitsbereich transportiert werden müssen. Weiterhin kann die Funktion der Lösch- und Wasserrückhaltung oder die Schalldämmung sowie die Luftdichtheit für den Einsatzzweck der Tür eine Rolle spielen.

Zu beachten ist ferner, dass mit höherer Widerstandsklasse auch das Gewicht einer Einbruch hemmenden Tür zunimmt. Türen ab WK5 sind beispielsweise aufgrund des Gewichts kaum mehr per Hand zu betätigen, sondern nur noch motorisch, was die Verwendung solcher Türen einschränken kann.

Die Verriegelung einer Tür spielt für die Einbruchhemmung eine weitere wesentliche Rolle. Daher sind der Widerstandsklasse entsprechende Verriegelungssysteme auszuwählen. Hierzu können Zusatzverriegelungssysteme eingesetzt werden, welche die Tür an mehreren Punkten zusätzlich zur Schlossfalle durch das Vorscheiben von Bolzen arretiert. Es ist grundsätzlich darauf zu achten, dass die verbauten Türanbauteile mindestens der gleichen Widerstandsklasse entsprechen wie die Tür selbst. Insbesondere sind hier Schließzylinder, Schutzbeschläge, Schlösser und die Verglasung (wenn vorhanden) zu nennen. Darüber hinaus muss eine Tür für eine dem Einsatzzweck entsprechende Zulassung verfügen.

Eine einbruchhemmende Tür ist natürlich nur in einer geeigneten Wand sinnvoll. Daher definiert die DIN V ENV 1627 in einer entsprechenden Tabelle für die einzelnen Widerstandsklassen der Türen Wandqualitäten nach Dicke und verwenden Baustoffen. So können Wände aus Mauerwerk mit geeignetem Mörtel oder aus gegossenem Stahlbeton einer bestimmten Güte hergestellt werden.

5.4 Fenster und Verglasung

Hinsichtlich des Einbruchschutzes kommt Fenstern die gleiche Bedeutung zu wie Türen. Während Türen in erster Linie das Betreten bzw. Verlassen von Räumen ermöglichen sollen, dienen Fenster primär der Belichtung, sind also verglast. Sinnvollerweise wird daher bei den Anforderungen zwischen Einbruch hemmenden Türen (unverglast) einerseits und Einbruch hemmenden Fenstern andererseits unterschieden. Verglaste Türen, sog. Fenstertüren, sind in diesem Zusammenhang wie einbruchhemmende Fenster zu bewerten. Der Begriff Fenster schließt die Verglasung sowie die Fensterkonstruktion (Rahmen) und alle Fensteranbauteile (z. B. Beschläge) ein. Zudem ist die Art der Verriegelung zu beachten. Insbesondere sollten Fenster umlaufende Verriegelungspunkte aufweisen, wenn eine Öffnung des Fensters vorgesehen ist.

Die Schwachstelle bei Fenstern und Fenstertüren ist durch die Verglasung gegeben. „Normales“ Glas, auch Isolierverglasung, bietet einem Angreifer keinen nennenswerten Widerstand. Erst Verbundglasscheiben können Angriffen in abgestufter Form standhalten oder sie merklich verzögern. Um von einem Durchwurf- oder Durchbruch hemmenden Fenster sprechen zu können, müssen Verglasung und Rahmen eine aufeinander abgestimmte Einheit bilden. Neben der mechanischen Robustheit des Rahmens spielt die Widerstandsklasse der Verglasung dabei eine wichtige Rolle. Es sind Verglasungen unterschiedlicher Güte verfügbar, die sich grob in die Kategorien

- durchwurfhemmende,
- druchbruchhemmende,
- durchschusshemmende und
- sprengwirkungshemmende

Verglasungen einteilen lassen. Die Schutzwirkung von Fenstern ist analog zu Durchbruch hemmenden Türen in Bauteilewiderstandsklassen eingeteilt. Die Widerstandsklassen der Norm EN V /DIN V 1627 für Fenster reichen ebenfalls von WK1 bis WK6.

Neben der mechanischen Robustheit eines Fensters ist auch die Art des Öffnens zu beachten. Es sollte angestrebt werden, nur solche Fenster für das Kippen und vollständige Öffnen zuzulassen, bei denen es für die Art der Raumnutzung unbedingt erforderlich ist. In vielen Bereichen reicht ein Kippen aus und oft können Fenster sogar fest verglast werden (keinerlei Öffnung). Hierdurch wird das versehentliche Offenstehen eines Fensters gänzlich vermieden.

6 Konstruktiver Brandschutz

Der konstruktive Brandschutz umfasst die Gesamtheit aller Maßnahmen, Mittel und Methoden hinsichtlich Bautechnik, Konstruktion, Material, Gestaltung und Funktionsplanung, die erforderlich sind, um einen wirksamen Schutz hochverfügbarer Infrastrukturen vor Bränden zu erreichen. Der bauliche Brandschutz wird vom technischen Brandschutz (Brandmeldeanlage, Löschung) überwacht und kann Fehler bei der Installation des baulichen Brandschutzes nicht mehr korrigieren. Es ist daher für den Betrieb hochverfügbarer IT-Systeme besonderer Wert auf die Qualität der Planung von Brandschutzmaßnahmen sowie auf die fachgerechte Installation und Wartung zu legen.

6.1 Brandabschnitte

Die Aufteilung eines Gebäudes in Brandabschnitte hat den Sinn, Teile des Gebäudes so gegeneinander abzusichern, dass ein Brand in einem Abschnitt nicht oder nur verzögert auf benachbarte Abschnitte übergreifen kann. Die Aufteilung von Brandabschnitten orientiert sich im Wesentlichen an der Größe eines Gebäudes und an den Fluchtwegen. Zulässige Größen von Brandabschnitten sollten eine Fläche von 40 x 40 m nicht überschreiten und nicht mehr als ein Geschoss umfassen. Ausnahmen für die Höhenausdehnung stellen Treppenhäuser, nicht geschottete Steigetrassen und Aufzugsschächte dar. Solche Bereiche sind als senkrecht durch ein Gebäude laufender Brandabschnitt entsprechend zu sichern. Einzelne Brandabschnitte werden durch Brandschutzkonstruktionen (gemäß DIN 4102) voneinander getrennt. Die Feuerwiderstandsklassen für Wände werden z. B. mit F90 angegeben, wobei die Zahl für die Minuten steht, über die hinweg der Widerstandswert erhalten bleibt. Konstruktionen mit anderen Widerstandszeiten tragen entsprechend die Bezeichnung von F30 für 30 bis F180 für 180 Minuten. Andere Buchstaben wie T, I, L, K, S usw. bezeichnen die Widerstandswerte anderer Brandschutzkonstruktionen wie 'Türen, 'I'nstallationskanäle, Lüftungs'L'eitungen, Lüftungs'K'lappen, Kabel'S'chottungen usw. Die baulichen Anforderungen des Brandschutzes an Türen oder Abschlüsse sind in Kapitel 5.3.1 dargelegt.

6.2 Brandlasten

In IT-Betriebsräumen dürfen grundsätzlich keine „passiven“ Brandlasten wie Möbel, Akten, Papiervorräte, Putzmittel usw. gelagert werden. Selbst wenn sich derartige besondere Brandlasten nicht im gleichen Raum, sondern in der näheren Umgebung zentraler Haustechnikeinrichtungen oder gar hochverfügbarer IT-Systeme befinden, können sie eine Brandgefahr darstellen. Im Falle eines Brandes in einem benachbarten Raum kann sich schnell Löschwasser stauen oder Rauch und Brandgase sich rasch im gesamten Brandabschnitt ausbreiten. Netzwerkkomponenten oder andere zentrale IT-Systeme wie Server, Sternkoppler, Verteiler sollten als „aktive“ Brandlasten nicht in begehbaren Steigetrassenräumen untergebracht werden. Ebenso stellen private Elektrogeräte von Mitarbeitern eine Brandlast für den hochverfügbaren Betrieb dar. Der Betrieb privater Elektrogeräte sollte daher generell untersagt werden.

6.3 Brandschottung

Die Schottung von Kabeltrassen verfolgt zwei Ziele:

- Schutz des Bereiches vor Gefahren, die von der Trasse ausgehen können, durch den die Trasse verläuft und
- Schutz der Trasse gegen Brandereignisse innerhalb des Bereiches, durch den sie geführt wird.

Brennende Kabel und Leitungen stellen in mehrfacher Hinsicht eine Gefahr dar: durch Brandausbreitung entlang der Kabel und direkten Übergriff des Brandes auf angrenzende Bereiche, durch die Entstehung von Sekundärbränden durch abtropfendes, brennendes Isoliermaterial, durch die Freisetzung ätzender und toxischer Brandgase sowie durch einen Brand durch Kurzschluss (jedoch unwahrscheinlich). Um diesen Gefahren vorzubeugen, ist es erforderlich, Kabel so gegen ihre Umgebung abzuschotten, dass Folgeschäden vermieden werden. Möglich ist dies u. a. durch die Kabelabschottung in Form eines I-Kanals entsprechend DIN 4102 Teil 11, die Feuerwiderstandsklassen werden mit I30 bis I120 angegeben. Eine andere Möglichkeit besteht durch den Schutz der Daten- und Energieversorgungsleitungen u. a. durch Verlegung der Kabel in einem „E-Kanal“ entsprechend DIN 4102 Teil 12 oder aber durch die Verwendung von Kabeln mit geeignetem Funktionserhalt. Die Funktionserhaltungsklassen werden bei E-Kanälen wie bei Kabeln mit Funktionserhalt mit E30 bis E90 angegeben.

Bei der Verlegung von Kabeln durch Brandwände sowie innerhalb von Räumen ist eine geeignete Schottung zwingend erforderlich, da Kabeltrassen wie beschrieben große Brandlasten darstellen. Dabei ist zwischen drei Schwerpunkten zu unterscheiden:

- die Sicherstellung des Feuerwiderstandswertes einer Brandschutzwand oder Decke bei der Durchführung von Leitungen,
- der Schutz des Bereiches vor Brandschäden, durch den eine Trasse geführt wird, die von der Kabeltrasse ausgeht,
- der Schutz der Trasse gegen Brandereignisse innerhalb des Bereiches, durch den sie geführt wird.

Die Notwendigkeit, Kabeldurchführungen durch eine Brandschutzwand bzw. -decke in geeigneter Weise zu schotten ergibt sich neben der Notwendigkeit des Schutzes hochverfügbarer Infrastrukturen auch aus der jeweiligen Landesbauordnung. Trassen queren Brandabschnittswände sowohl waagerecht im Fußboden, an Decken und als Fensterbankkanäle als auch Geschossdecken senkrecht als Steigetrasse. Bei der Installation und Wartung der Brandschottung muss daher auf eine fachgerechte Ausführung geachtet werden.

Ein Kabelschott muss neben seiner Brandschutzqualität je nach Einsatzfall über weitere Eigenschaften verfügen. Führt das Schott z. B. in eine Tiefgarage, ist zum Schutz von Menschen gegen giftige Gase ein gasdichtes Schott erforderlich. Ist (z. B. in Hochwasserbereichen) mit der Überflutung von Gebäudeteilen zu rechnen, muss das Schott wasserdicht und entsprechend dem zu erwartenden Wasserstand zudem druckfest sein. Eine vielseitig einsetzbare Lösung sind Kabelschotts, die aus vorgeformten Elementen zusammengesetzt und nach Verlegung der Kabel verpresst werden. Bei solchen Systemen ist die Nachverlegung mit vertretbarem Aufwand möglich, ohne dass das Schott seine Schutzfunktion verliert. Die Verwendung von Brandschutzkissen, auch wenn diese zugelassen sind, sollten nur während Installationsarbeiten verwendet werden, da ein mechanisch fester Verbund für den Dauereinsatz sabotagesicher ausgeführt werden muss. Eine weitere flexible Dauerlösung ist der Einsatz von Brandschutzboxen. Diese mit Brandschutzplatten bestückten Metallboxen können schon bei der Rohbauerstellung in die Wand eingemauert bzw. eingegossen aber auch nachträglich eingebaut werden. Im Brandfall quellen die Brandschutzplatten auf und verschließen das Schott zuverlässig. Bei der Auswahl der Brandschottsysteme ist

entsprechend der geplanten Einsatzumgebung auf eine ausreichende Gas-, Wasser- und Druckdichtigkeit zu achten.

7 Elektrische Versorgung

Die elektrische Energieversorgung spielt für die Hochverfügbarkeit einer Infrastruktur eine zentrale Rolle. Die Energieversorgungsunternehmen und die Netzbetreiber sind bemüht, die Versorgungssicherheit auf hohem Niveau zu halten, dennoch muss jederzeit mit Störungen gerechnet werden. Vermehrte Ausfälle zeigen, dass Defekte im öffentlichen Energieversorgungsnetz oder unvorhersehbare Ereignisse im globalen Netzverbund in der Lage sind, weite Teile der Energieversorgung innerhalb Europas lahmzulegen. Durch die Liberalisierung des Strommarktes und dem damit verbundenen Kostendruck ist zukünftig eher mit einer Verschlechterung der Qualität des Stromversorgungsnetzes zu rechnen. Gleichzeitig werden die Anforderungen an die Stromversorgung eher zunehmen. Es ist zum Schutz hochverfügbarer Infrastrukturen also unausweichlich, eigenverantwortlich Maßnahmen zur Erhöhung der Versorgungssicherheit umzusetzen. Es gilt, Strategien zu entwickeln, welche die Anbindung an das öffentliche Energieversorgungsnetz entweder durch die Nutzung alternativer Konzepte ergänzen oder gar durch eine autarke Eigenversorgung ersetzen.

Die elektrischen Geräte, die am internen Energieverteilernetz angeschlossen sind, müssen dauerhaft mit konstanter und störungsfreier Spannung versorgt werden. Ein Großteil der Betriebsstörungen der IT beruht auf Störungen im eigenen Verteilnetz. Neben der Anbindung an die Energieerzeugung spielen daher die Auslegung des internen Energieverteilungsnetzes, die Auswahl hochwertiger Technikkomponenten und die Qualität der Installation zentrale Rollen für die Verfügbarkeit der IT-Systeme. Eine Gefahr stellen Spannungsschwankungen und insbesondere Überspannungen für angeschlossene Geräte dar. Spannungsschwankungen werden entweder durch das öffentliche Energieversorgungsnetz übertragen oder können durch ungeeignete Dimensionierung des internen Verteilernetzes entstehen. Besonders Überspannungen durch Blitzschlag müssen durch wirksame technische Maßnahmen abgeleitet werden. Es sind daher alle Komponenten der Energieversorgung, von der Anbindung bis zum Anschluss der Geräte, über das interne Verteilernetz im Rahmen eines Gesamtkonzepts zu betrachten.

7.1 Möglichkeiten der Energieversorgung

Grundsätzlich stehen zwei verschiedene Arten der primären Energieversorgung zur Verfügung. Zum einen ist die Anbindung an ein oder mehrere Energieversorgungsunternehmen (EVU) über das öffentliche Versorgungsnetz zu nennen und zum anderen besteht die Möglichkeit einer autarken Energieerzeugung am Ort des Bedarfs.

7.1.1 Anbindung an die öffentliche Energieversorgung

Die Energieversorgung besteht grundsätzlich aus der Energieeinspeisung in das Gebäude sowie weiteren technischen Komponenten, wie Außenkabeltrassen, Umsetzungstrafo, Niederspannungshauptverteilung sowie der internen Verkabelung. Bei der doppelten Einspeisung existieren zwei voneinander unabhängige Versorgungsstränge durch ein Energieversorgungsunternehmen.

Die Einspeisungen sollten aus unterschiedlichen Umspannwerken und über räumlich ausreichend weit voneinander entfernt verlegte Trassen erfolgen. Es ist generell bei einer parallelen Energieeinspeisung darauf zu achten, dass die einzelnen Einspeisungsstränge für die gleiche Leistung ausgelegt sind und auf eigene Verteilungen aufgelegt sind, damit eine gegenseitige

Beeinträchtigung vermieden wird. So sind separate Niederspannungshauptverteilungen für jeden Einspeisungsstrang vorzusehen.

Abhängig von der abgenommenen Leistung und der Kapazität des EVU-Netzes erfolgt die Einspeisung direkt mit Niederspannung, also mit 400V/230 V, oder mit Mittelspannung, je nach EVU-Netz zwischen 1 kV und 60 kV. Im zweiten Fall muss ein eigener Transformator zur Umsetzung auf Niederspannung für das interne Netz installieren werden. Es sollte die Mittelspannungseinspeisung gegenüber einer Niederspannungseinspeisung bevorzugt werden, da durch die Transformatoren der Niederspannungsbereich gegen Störungen durch andere Verbraucher im gleichen EVU-Versorgungsbereich entkoppelt und dadurch geschützt wird. Die Transformatoren sind vor unberechtigtem Zutritt und insbesondere vor Brand zu schützen. Transformatoren sind daher, je nach Leistungsfähigkeit, in eigenen Räumen oder in vom Gebäude abgesetzten eigens dafür vorgesehenen Containern zu betreiben. Ein Trafobrand kann durch Überhitzen und Entzünden des im Trafo vorhandenen Kühlöls große Gefahren für das Gebäude selbst oder für die umliegende Bebauung mit sich bringen. Die Betriebsräume von Transformatoren sind daher mit Brandschutzmaßnahmen auszustatten und in die allgemeine Brandüberwachung des Gebäudes einzubeziehen. Die regelmäßige Wartung der Transformatorkomponenten ist ebenso notwendig wie selbstverständlich.

Die Anbindung an das EVU erfolgt mit Hilfe von Kabeln, die in Außentrassen verlegt sind. Die Verlegung sollte mit zwei unabhängigen Kabeln in einer Zwei-Wege-Führung in voneinander getrennten Trassen und an unterschiedlichen Stellen in das Gebäude erfolgen. Außentrassen lassen sich in unterirdische Erd- und Rohrtrassen unterscheiden. Bei Erdtrassen werden Kabel direkt im Erdreich verlegt, bei Rohrtrassen erfolgt die Kabelverlegung in vorher verlegten Leerrohren und Zugschächten. Erdleitungen bieten durch ihre erschwerte Zugänglichkeit einen besseren Schutz gegen Sabotage als Rohrtrassen. Die Schächte von Rohrtrassen sollten daher in die Überwachung gegen unberechtigtes Öffnen einbezogen werden. Eine erhebliche Gefahr besteht für beide Arten der Verlegung in der versehentlichen Beschädigung durch Erdarbeiten. Eine sorgfältige Trassendokumentation ist daher zwingend vorzusehen. Darüber hinaus lässt sich die Robustheit von Kabeln lediglich durch entsprechende Armierung steigern und eine Manipulation oder unbeabsichtigte Beschädigung erschweren. Grundsätzlich lassen sich Beschädigungen an Kabeln der Energieversorgungsanbindung nicht ausschließen, insbesondere wenn die Zuleitung durch den öffentlichen Bereich führt. Neben einer permanenten Funktionsüberwachung ist daher eine automatisierte Umschaltung auf redundante sekundäre Energieversorgungseinrichtungen vorzusehen, um eine gestörte primäre Energieversorgung zu stützen oder zeitlich zu überbrücken.

7.1.2 Autarke Energieversorgung

Aufgrund der zunehmenden Instabilität des öffentlichen Energieversorgungsnetzes rückt die Autonomie der Energieversorgung für hochverfügbare Infrastrukturen zunehmend in den Mittelpunkt der Betrachtungen. Als Lösungen sind verschiedene Ausführungen und Leistungsstufen von autarken Energieversorgungseinrichtungen in Form Blockheizkraftwerken (BHKW) verfügbar und für den Betrieb hochverfügbarer Infrastrukturen gegenüber der Einspeisung eines EVU zu bevorzugen. Durch die Kraft-Wärme-Kopplung bietet ein BHKW neben der direkten Erzeugung der elektrischen Energie und der Nutzung der dabei entstehenden Wärme den Vorteil eines hohen Wirkungsgrades für den Betrieb. Ein BHKW kann, je nach Leistungsfähigkeit und Auslegung, verschiedene Aufgaben der lokalen Energieversorgung übernehmen. Die Betriebsart eines BHKW kann, je nach Art des lokalen Bedarfs, so ausgelegt werden, dass primär entweder elektrische Energie oder Wärme produziert wird. Ein stromgeführtes BHKW erzeugt im Gegensatz zum

wärmegeführten Betrieb elektrische Energie und Abwärme als Nebenprodukt. Diese Abwärme kann zum Heizen des Gebäudes oder aber mithilfe einer Absorptionskältemaschine zur Unterstützung der Klimatisierungsanlage verwendet werden. Der genaue Einsatzzweck eines BHKW ist daher bei der Planung genau festzulegen.

Bei allen Vorteilen, die der Betrieb eines BHKW bietet, ist jedoch auch hier die Abhängigkeit von der Kraftstoffversorgung gegeben. Es ist daher sicherzustellen, dass für die Anbindung an den Kraftstofflieferanten wirksame Schutzmaßnahmen gegenüber Sabotage oder mechanischer Beschädigung umgesetzt werden. Um eine hochverfügbare autarke Energieversorgung sicherzustellen, muss auch hier das Prinzip der Redundanz greifen. Daher sollte ein BHKW-Verbund, bestehend aus mindestens zwei Anlagen, aufgebaut werden, in dem jede einzelne Anlage in der Lage ist, den gesamten Energiebedarf mit einem Reservefaktor eigenständig bereitzustellen. Zusätzlich ist, wenn es die Art des Kraftstoffs erlaubt, eine ausreichende lokale Bevorratung von Kraftstoff (z. B. Heizöl, Holzpellets) von mehreren Tagen vorzusehen. Zudem ist eine zuverlässige Nachschubversorgung sicherzustellen. Als Betriebsstandort für ein BHKW sollte jeweils ein eigener Raum gewählt werden, der sich in einem anderen Gebäudeteil oder gar anderen Gebäude befindet, als der Technikraum, in dem hochverfügbare IT-Systeme betrieben werden. Der Betriebsraum eines BHKW ist in den baulichen Brandschutz und in die lokale Brandüberwachung einzubeziehen. Der Zutritt zu den Anlagen ist zu kontrollieren und die entsprechenden Betriebsräume in die Überwachung mit einzubeziehen.

7.2 Aufrechterhaltung der Energieversorgung

Jede Art der primären Energieversorgung unterliegt der Gefahr der Unterbrechung durch technisches Versagen, geplante Abschaltungen zu Wartungszwecken oder durch Manipulation. Es ist daher in IT-Strukturen mit hoher und höchster Anforderung an die Verfügbarkeit unerlässlich, weitere Versorgungseinrichtungen zu installieren, die den sicheren Betrieb während solcher Ausfallzeit gewährleisten.

7.2.1 Unterbrechungsfreie Stromversorgung

Eine unterbrechungsfreie Stromversorgung (USV) hat die primäre Aufgabe, für einen begrenzten Zeitraum die konstante Energieversorgung der angeschlossenen Geräte sicherzustellen, wenn die reguläre Energieversorgung Schwankungen unterliegt oder kurzzeitig ganz ausfällt. Stromausfälle über mehrere Stunden oder Tagen kann eine USV-Anlage nicht überbrücken. Sie dient vielmehr der kurzzeitigen Überbrückung von Netzausfällen, Spannungseinbrüchen, Spannungsspitzen oder Überspannungen, aber auch dem Ausgleich von Frequenzschwankungen oder Spannungsverzerrungen.

Die Überbrückungs- oder Stützzeit einer USV ist die Zeit, die erforderlich ist, um eine Netzersatzanlage in Betrieb zu nehmen und auf das interne Verteilernetz umzuschalten. Die hierfür benötigte Zeit und die Last der angeschlossenen hochverfügbaren IT-Systeme bestimmen die Kapazität einer USV-Anlage, wobei ein Sicherheitsfaktor von 1,5 zu veranschlagen ist. Die Stützzeit reicht, je nach Auslegung der Batteriekapazität und angeschlossener Belastung, von mehreren Sekunden bis zu einige Stunden. Eine USV dient ausschließlich der Stützung der IT-Systeme, die für einen hochverfügbaren Betrieb unbedingt notwenig sind. Sie versorgt also nicht die Raumbeleuchtung oder andere Technikkomponenten der Haustechnik (z. B. Klimaanlage) oder IT-Systeme, an die keine Verfügbarkeitsanforderungen gestellt werden. Komponenten der Haustechnik, die für den

Betrieb hochverfügbarer IT-Systeme notwendig sind, sollten in hochverfügbaren Infrastrukturen über eine eigene USV verfügen (siehe auch Kapitel 8.3). Unter Umständen soll durch die USV-Zeit zur Verfügung gestellt werden, um ein kontrolliertes Herunterfahren solcher IT-Systeme zu gewährleisten. Neben der reinen Stützfunktion muss eine USV weitere Funktionen zur Verfügung stellen:

- Auslösen des gezielten Herunterfahrens nicht hochverfügbarer IT-Systeme,
- Anzeige der Betriebszustände,
- Fehleranalyse.

Auf eine Fernwartung der USV sollte wegen vorhandener Manipulationsmöglichkeiten verzichtet werden.

Eine einfache USV besteht aus fünf wesentlichen Baugruppen:

- dem Gleichrichter mit Ladeelektronik,
- Zwischenkreis
- den Stützbatterien als Energiespeicher,
- dem Wechselrichter und
- einem Bypass,

um im Fehlerfall die Versorgung vom „Normalnetz“ auf die USV umzuschalten. Die Ladeelektronik lädt oder erhält den Ladezustand der angeschlossenen Batterien im Normalbetrieb (Netzspannung vorhanden, USV nicht aktiv). Der Wechselrichter erzeugt die Wechselspannung und die Umschalteinheit schaltet im Fehlerfall des Netzes (Netzspannung nicht vorhanden, USV aktiv) die Verbraucher auf die USV um. Die USV erhält die Energie aus den Batterien, die dabei entladen werden. Diese einfache Konstruktion einer USV ist jedoch für den hochverfügbaren Betrieb nicht geeignet, da keinerlei Filterfunktion gegenüber Überspannungen oder Störungen aus dem Energieversorgungsnetz existiert und die Umschaltzeit der USV selbst Störungen für die angeschlossenen IT-Systemen erzeugen kann.

Nur die sogenannte Voltage and Frequency Independent-USV (VFI-USV) eignet sich für den Betrieb in einer hochverfügbaren Infrastruktur. Die VFI-USV, auch bisher „Online-USV“ genannt, ist in ihrer Ausgangsspannung sowohl von der Spannung als auch von der Frequenz der normalen Stromversorgung unabhängig. Die Eingangsspannung aus dem „Normalnetz“ wird gleichgerichtet, zur Ladung und Ladeerhaltung der Batterien und zugleich wieder über den Wechselrichter in die Ausgangsspannung für die Verbraucher umgewandelt. Die gesamte Energieversorgung der angeschlossenen Geräte erfolgt also immer über die USV. Da sowohl im Normal-Betrieb als auch im Betrieb bei Netzausfall die Versorgungsspannung von der USV kommt, besteht für die angeschlossenen Verbraucher keinerlei Unterschied zwischen diesen beiden Betriebszuständen. Im Gegensatz zur weiter oben beschriebenen einfachen Variante existiert keine Umschaltlücke, was den entscheidenden Vorteil der VFI-USV ausmacht. Trotz höherer Kosten und der höheren Belastung des Wechselrichters ist diese Art der USV zu bevorzugen. Eine regelmäßige Wartung der USV ist daher für den zuverlässigen Betrieb unerlässlich.

Die USV trägt mit ihrer Funktion wesentlich zur Verfügbarkeit der IT-Systeme bei. Auch die USV-Anlage ist Gefahren ausgesetzt, die bei der Installation und dem Betrieb zu berücksichtigen sind. So sollte die USV in einem zutrittsgeschützten und möglichst fensterlosen Raum installiert werden, in dem sich sonst keine weiteren technischen Systeme der Haustechnik befinden und in die

Überwachung der Einbruchmeldeanlage einbezogen werden. Es ist zu beachten, dass die Tragfähigkeit des Raumbodens der USV-Auslegung entspricht und für das damit verbundene Gewicht der Batteriebank (Zusammenschaltung mehrerer Batterien) ausreichend dimensioniert ist. Der Raum der USV sollte als eigener Scharfschaltbereich ständig scharf geschaltet und nur für die regelmäßige Wartung temporär aus der Überwachung genommen werden. Der Zutritt sollte nur mithilfe des Vier-Augen-Prinzips erfolgen, bei dem sich mindestens zwei Personen mithilfe ihrer Zutrittskarte nacheinander am Zutrittsterminal der einzigen Zutrittstür identifizieren und authentifizieren. Der Raum der USV sollte feuerhemmend ausgeführt werden und alle Bauteile (Wände, Decken, Böden, Türen etc.) mindestens 90 Minuten Funktionserhalt aufweisen. Der Raum ist in die Brandüberwachung einzubeziehen. Dieser Grundsatz ist auch für die Kabel zur Anbindung an die Niederspannungshauptverteilung und die Kabelführung selbst (z. B. Steigschächte, Kabelkanäle) zu beachten. Darüber hinaus sollte die USV vor eindringendem Wasser geschützt werden. Es wird empfohlen, die USV in die Überwachung durch eine Wassermeldeanlage einzubeziehen und druckbehaftete Wasserleitungen oder Fallrohre der Dachentwässerung zu vermeiden.

7.2.2 Netzersatzanlagen

Energiequellen, die im Falle einer Unterbrechung der Primärversorgung eine Ersatzstromversorgung zur Verfügung stellen, werden als Netzersatzanlagen (NEA) bezeichnet. Die NEA übernimmt als sekundäre Energiequelle eine weitere Sicherungsfunktion, wenn sich die redundant ausgelegte Energiequelle der Primärversorgung (z. B. Blockheizkraftwerk) in der regulären Wartung befindet oder wegen Defekt ausgefallen ist. Hierbei handelt es sich um autarke Notstromaggregate, welche die Stromversorgung durch eigene Generatoren übernehmen. Diese werden in den meisten Fällen von Verbrennungsmotoren angetrieben, die bei einem Ausfall der Primärversorgung automatisch angefahren werden. Die Anlauf- und Umschaltzeit auf das interne Verteilernetz, welche die NEA benötigt, wird von der USV überbrückt. Die Brennstoffversorgung der NEA erfolgt aus einem lokalen Brennstoffvorrat, z. B. Diesel, der in ausreichender Menge und mit gesichertem Nachschub zur Verfügung stehen muss, um auch längere Ausfälle (mehrere Tage) überbrücken zu können. Neben Diesel ist Gas ein weiterer Brennstoff, mit dem eine NEA betrieben werden kann. Es ist dafür Sorge zu tragen, dass eine Sicherung der Versorgungswege existiert. Eine unterbrechungsfreie Versorgung ist jedoch nur durch eine lokale Treibstoffbevorratung sichergestellt. Im Bereich der hohen und sehr hohen Verfügbarkeit sollte der örtlich vorgehaltene Brennstoffvorrat für mindesten 72 Stunden Volllastbetrieb ausreichen. In Einzelfällen können sogar 120 Stunden erforderlich sein.

Der Betrieb einer NEA, gleichgültig auf welcher Technologie diese beruht, lässt sich nicht von dem der USV trennen. Beide Systeme stellen aufeinander abgestimmte Teilkomponenten zur Aufrechterhaltung der Energieversorgung dar. Auch an den Betrieb einer NEA werden Sicherheitsanforderungen gestellt, die sich an denen der USV orientieren (siehe Kapitel 7.2.1). Für den Betrieb der gesamten Sekundärversorgung in einer hochverfügbaren Infrastruktur (bestehend aus NEA und USV), ist es unverzichtbar, Echt-Last-Tests, also Testläufe bis zur maximalen Belastung, durchzuführen, um die Leistungsfähigkeit unter realen Bedingungen zu überprüfen. Darüber hinaus sind die Sicherheitsanforderungen, die an die Zutrittskontrolle, die Einbruchmeldeanlage, an den baulichen und technischen Brandschutz sowie den Wasserschutz gestellt werden, ebenso für den Betrieb einer NEA umzusetzen.

Als zu bevorzugende Lösung zum Betrieb hochverfügbarer IT-Systeme sollte eine Kombination aus jeweils redundanter USV und NEA als Sekundärversorgung vorgesehen werden. Es ist bei der

Dimensionierung der Leistungsfähigkeit von NEA und USV mindestens ein Faktor von 1,5 der maximalen Belastung anzunehmen.

7.3 Stromverteilung und Verkabelung

Die Anbindung an die elektrische Primärversorgung erfolgt direkt in der Hauptverteilung. Bei Versorgung mit Niederspannung (400V/230V) ist die Hauptverteilung identisch mit der Niederspannungshauptverteilung (NSHV) des zu versorgenden Bereichs oder Gebäudes. Bei Versorgung mit Mittelspannung (bis zu mehreren kV) ist der niederspannungsseitige Ausgang des Umspannungstransformators dort angeschlossen. Bei mehreren zu versorgenden Gebäuden oder Bereichen ist der Hauptverteilung eine Liegenschaftshauptverteilung vorgeschaltet.

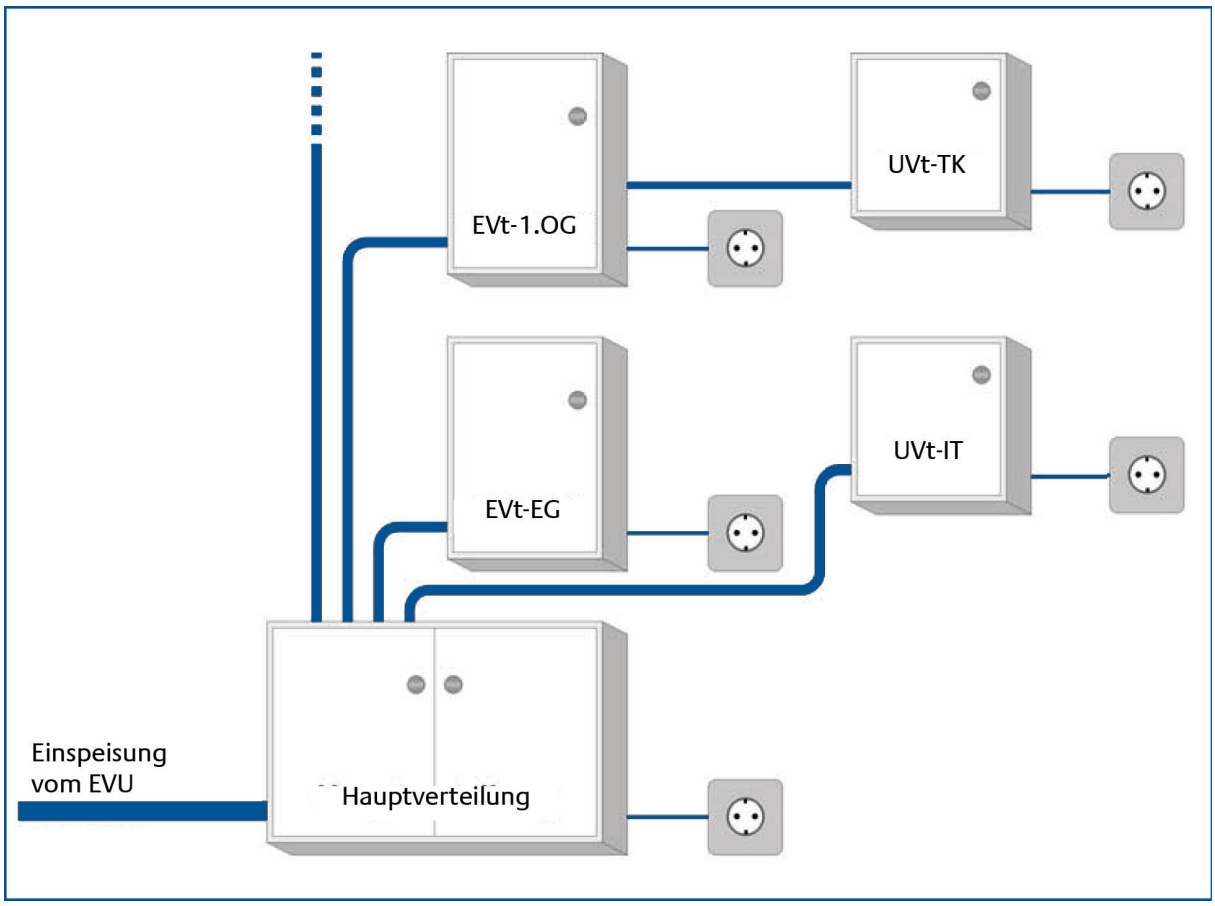


Abbildung 3: Energieverteilung innerhalb eines Gebäudes

Die weitere Energieverteilung erfolgt innerhalb eines Gebäudes standardmäßig, wie in Abbildung 3 dargestellt, ab der Niederspannungshauptverteilung über Etagenverteiler (EVt) und dann für einzelne kleinere Bereiche über Unterverteiler (UVt). Unterverteilungen können jedoch auch direkt an der NSHV angeschlossen sein. Der Anschluss der zu versorgenden Geräte kann aus jeder Verteilung (NSHV, EVt, UVt) erfolgen.

7.3.1 Niederspannungshauptverteilung, Unterverteilungen

Die Verteilung für Bereiche, in denen hochverfügbare IT-Systeme betrieben werden, sollten aus Gründen der Manipulationssicherheit und dem Vermeiden von Störeinflüssen aus anderen Bereichen (z. B. Wartungsarbeiten, Kurzschlüsse, Störspannungen), direkt an der NSHV angeschlossen werden. Die Anbindung der Unterverteilung an die NSHV sollte mit ungeschnittenen Kabeln und in gesicherten Kabelkanälen, Steigschächten oder Stahlpanzerrohren erfolgen. Besonderes Augenmerk ist auf die Standortwahl der NSHV zu legen. Die NSHV sollte in einem Raum installiert werden, in dem keine Rohrleitungen der Wasserversorgung oder Wasserentsorgung verlegt sind, oder in dem sich gar die Anbindung an die zentrale Wasserversorgung des Gebäudes befindet. Weiterhin muss die NSHV oder jede Unterverteilung vor unberechtigtem Zutritt geschützt sein. Die Raumtür ist daher an eine Zutrittskontrollanlage anzuschließen. Der Raum selbst sollte nicht als Lagerraum verwendet werden, damit der Zutritt Unbefugter vermieden und keine zusätzlichen Brandlasten (Putzmittel, Kartons etc.) eingebracht werden. Meist wird die NSHV oder eine Unterverteilung mit weiteren technischen Einrichtungen in einem gemeinsamen Raum innerhalb eines Technikschranks installiert. In diesem Fall sind der Verschluss des Technikschranks und eine Überwachung auf unberechtigtes Öffnen durch eine Einbruchmeldeanlage erforderlich. Der Raum oder der Technikschrank der NSHV oder einer Unterverteilung sind in die Brandüberwachung einzubeziehen.

7.3.2 Netzarten, Trassen und Verkabelung

Die interne Energieverteilung erfolgt durch die im Gebäude oder in einem Bereich installierte Verkabelung von der Niederspannungshauptverteilung über die Unterverteilungen bis zu den angeschlossenen IT-Systemen. Zum Betrieb hochverfügbarer IT-Systeme ist die interne Verkabelung der Energieverteilung als sogenanntes TN-S Netz auszulegen. In einem solchen Netz wird von der Potenzialausgleichschiene der Neutral (N)-Leiter und Protection Earth (PE)-Leiter (oder Schutzleiter) getrennt geführt. In einem TN-S System ist die Summe der Ströme auf den stromführenden Phasen L1, L2 und L3 gleich dem Strom auf dem N-Leiter. Auf dem PE-Leiter fließt kein Strom. Nur ein TN-S-System ist geeignet, die angeschlossenen Geräte vor Ausgleichströmen auf dem Schutzleitersystem und damit auf Schirmungen sicher zu vermeiden. Bei Umbaumaßnahmen oder Erweiterungen der Verkabelung muss gewährleistet sein, dass keine unzulässigen Veränderungen (z. B. Brücken zwischen N und PE) an einem TN-S Netz vorgenommen werden. Im Fall eines Fehlers im Stromnetz, der eine Stromabschaltung erfordert, z. B. durch Kurzschluss in einem Gerät, reicht eine ereignisgesteuerte Abschaltung mit Hilfe von Residual Current Protective Devices (RCD), im Sprachgebrauch auch Fehlerstromschutzschalter oder FI-Schalter genannt, nicht aus, da vorhanden IT-Systeme keine Zeit für eine Umschaltung auf redundante Systeme oder ein reguläres Herunterfahren zur Verfügung steht. Eine Differenzstrom-Überwachung durch Residual Current Monitors (RCM) ist daher notwendig, die, ähnlich wie RCDs arbeiten, jedoch den Vorteil bieten, bei Erreichen des Nennfehlerstroms nicht durch sofortiges Abschalten zu reagieren. RCMs können den Differenzstrom über seine zeitliche Entwicklung hin beobachten und, je nach individueller Einstellung, schon bei Erreichen eines bestimmten Meldefehlerstroms eine Warnmeldung erzeugen, die an zentraler Stelle angezeigt werden sollte. Die Überwachung durch RCMs muss sich auf alle stromführenden Phasen L1, L2, L3 und N sowie separat auf den PE-Leiter erstrecken. Eine regelmäßige Prüfung und fachgerechte Wartung der Verkabelung und aller elektronischen Komponenten ist jedoch weiterhin vorzusehen und kann durch eine ständige technische Überwachung nicht ersetzt werden.

Bei der Kabelinstallation sollte auf eine ungeschnittene, also durchgängige Verkabelung von der Unterverteilung bis zum Gerät selbst oder bis zu einem Technikschrank geachtet werden. Die Kabelverteilung erfolgt von der Trasse im Deckenbereich direkt zum Technikschrank oder über geschlossene an den Wänden installierte Kabelkanäle. Auf ein separiertes eigenes Stromnetz für IT-Systeme und andere Verbraucher ist generell zu verzichten. Eine bessere Alternative hierzu stellt eine bereichsbezogene Absicherung dar. Dabei sollte jeder Bereich, in dem IT-Systeme betrieben werden (Raum, Schränke), über eine separate Absicherung verfügen. Damit werden generelle Überlastungen, wie z. B. bei einer Etagenverteilung, vermieden und deren Folgen, die zu Versorgungsabschaltungen führen können, auf kleine Bereiche begrenzt. Zudem bieten sich Vorteile bei der Installation von Überspannungsschutzeinrichtungen, die gezielter vorgenommen werden können. Auch hier ist darauf zu achten, dass die maximale Stützlast der USV nicht überschritten wird.

Die Ausstattung mit technischen Systemen umfasst, neben den IT-Systemen selbst, auch die Überwachungseinrichtungen der Haustechnik (Gebäudeleittechnik), Gefahrenmeldetechnik (z. B. Einbruchmeldeanlage, Brandmeldeanlage, Leckagemeldeanlage) sowie Telekommunikationseinrichtungen. Die Leitungsführung und der Platzbedarf der Kabel dieser Systeme stellen besondere Anforderungen an die Leitungsführung. Leitungsführungssysteme müssen die Verkabelung vor ungewollter mechanischer Beanspruchung, Manipulation oder Brand schützen, gleichzeitig leicht erweiterbar und wartungsfreundlich sein. Auch müssen unterschiedliche Netzarten (Stromnetz, Datennetz, Netz der Gefahrenmeldetechnik) gemeinsam geführt, jedoch soweit trennbar sein, dass gegenseitige Störungen minimiert werden. Die Kabelführungen werden häufig aus ästhetischen Gründen optisch verblendet oder in abgehängten Decken installiert. Dies ist aus den verschiedensten Gründen nicht zu empfehlen, siehe Kapitel 5. Auch die Kabelführung in Doppelböden ist gängige Praxis. Es ist jedoch bei der Verlegung von Kabeln im Doppelboden auf dessen Hauptaufgabe zu achten, nämlich als wesentlicher Bestandteil der Klimatisierungsanlage zur Belüftung eines Raums. Daher sollte auch im Doppelboden auf eine Leitungsführung verzichtet oder mindestens strömungstechnisch nicht behindernd ausgeführt werden.

Generell sollten Kabel auf Trassen im offenen Deckenbereich geführt und an der Rohdecke installiert werden. Kabel sind generell zu schützen, sei es aus Gründen der Betriebssicherheit, zur Sicherheit gegenüber ungewollter Manipulation (z. B. ungenehmigte Erweiterung der Installation) oder Sabotage. Hierzu werden Kabeltrassen zumeist aus Metallführungsschienen hergestellt, die in offener und geschlossener Bauweise angeboten werden. Es sind ausreichend dimensionierte geschlossene Trassenkonstruktionen zu bevorzugen, die zudem eine Überwachung gegenüber unberechtigtem Öffnen durch eine Einbruchmeldeanlage aufweisen. Um dem Brandschutz gerecht zu werden, können Kabeltrassen an Übergängen oder Querungen von verschiedenen Brandabschnitten geschottet werden. Ein Funktionserhalt von mindestens 90 Minuten gegenüber Brand ist vorzusehen. Hierzu ist es, insbesondere bei nachträglicher Verlegung von Kabeln oder deren Entfernung, unerlässlich, die Brandschottung fachgerecht wieder herzustellen. Dies betrifft eine vorhandene Komplettschottung einer Trasse und die Kabeldurchführung durch Wände. Auch die Qualität der Kabel selbst trägt zum Brandschutz bei. So sollten Kabel in halogenfreier Ausführung gewählt werden und ein Funktionserhalt von mindestens 90 Minuten gegenüber Brand aufweisen.

Einen hohen Stellenwert für die Betriebssicherheit nimmt die regelmäßige Kontrolle von Kabeltrassen ein. Dabei steht neben der Kontrolle auf Beschädigungen und der Brandschutz die zumeist wenig beachtete Begrenzung der Trassenkapazität im Vordergrund. Eine bestehende Verkabelung wird rasch erweitert, jedoch das Deinstallieren von nicht mehr benötigten Kabeln oft vergessen. Schnell ist dann die zulässige Trassenkapazität erreicht oder gar überschritten. Nur eine

regelmäßige Kontrolle mit lückenloser Dokumentation und eine konsequente Beschriftung der Kabel kann eine kostspielige Nachinstallation weiterer Trassensysteme verhindern und dazu beitragen, die Übersicht über die Gesamtverkabelung zu behalten.

Die Verkabelung zwischen Etagen in Gebäuden dient entweder der Verbindung von Etagenverteilungen untereinander oder der Verbindung mit der Hauptverteilung. Die Verkabelung sollte in durchgängigen, als eigener Brandabschnitt ausgeführten, Steigetrassen installiert werden. Auch hier sind geeignete Kabelführungssysteme zu wählen, ferner ist die Zugbelastung der Kabel zu berücksichtigen (Einfluss durch Temperaturänderungen und Gebäudebewegungen). Neben der Steigtrasse selbst sind sämtliche Kabeleinführungen in Betriebsräumen feuerfest mit mindestens 90 Minuten Funktionserhalt auszuführen. Weiterhin sollten die Kabel gegenüber unberechtigtem Zutritt geschützt werden. Daher sind vorhandene Wartungsklappen oder -türen ständig verschlossen zu halten und gegenüber unberechtigtem Öffnen zu überwachen. Steigtrassen sind in die Überwachung durch die Brandmeldeanlage einzubeziehen.

7.4 Blitz- und Überspannungsschutz

Der Blitz- und Überspannungsschutz ist ein wesentliches Element zur Aufrechterhaltung der Verfügbarkeit von IT-Systemen. Die Häufigkeit und die Intensität von Blitzen nimmt stetig zu und damit auch die Gefahr der Beschädigungen oder Zerstörung von Gebäuden oder elektrischen Anlagen. Ein wirksamer Blitzschutz muss daher sowohl für den äußeren Bereich als auch für den inneren Bereich eines Gebäudes vorgesehen werden. Die Schutzmaßnahmen dürfen sich aber nicht nur auf den Blitzschutz konzentrieren, sondern müssen ebenfalls Überspannungen berücksichtigen, die in allen Kabelnetzen in einem Gebäude auftreten können. Überspannungen können sowohl durch Blitze entstehen als auch durch Störungen im globalen Verbund der Versorgungsnetze der Energiewirtschaft oder durch elektrostatischen Aufladungen.

Seit 01.10.2006 wurde mit der Norm DIN EN 62305 (entspricht VDE 0185-305) der Blitzschutz auf eine neue normative Grundlage gestellt. Die bisherige Zusammenarbeit mit der Elektrofachplanung (Versorgungs- und Datenleitungen) zur Erstellung eines Blitz- und Überspannungskonzepts reicht dabei nicht mehr aus. Die Wirkung von Blitzen ruft Schäden an Bauwerken oder gar Personen hervor und kann Überspannungen entweder bei direktem Einschlag oder indirekt durch induktive Einkopplung in Kabelnetzwerken bewirken. Um diesen Ereignissen wirksame Maßnahmen gegenüberzustellen, sollte ein Blitz- und Überspannungskonzept zur Sicherung von IT-Systemen gemäß DIN EN 62305-1 bis -4 von ausgewiesenen Fachleuten erarbeitet und umgesetzt werden. Die Norm sieht vier Bestandteile vor:

- Allgemeine Grundsätze:
  Erläuterung der physikalischen und technischen Zusammenhänge von Blitzen.
- Risiko-Management:
  Risikobewertung anhand von zu erwartenden Blitzereignissen sowie den Eigenschaften und Erfordernissen des zu schützenden Gebäudes.
- Schutz von baulichen Anlagen und Personen:
  Äußerer Blitzschutz, um Gebäude und Personen zu schützen.
- Elektrische und elektronische Systeme in baulichen Anlagen:
  Innerer Blitzschutz, um IT-Systeme vor Überspannung zu schützen.

In Abhängigkeit vom ermittelten Risiko muss die Schutzklasse eines Lightning Protection System (LPS) festgelegt werden. Die Schutzklassen I (höchster Schutz) bis IV (geringster Schutz) legen

konkrete bauliche Maßnahmen des inneren und äußeren Blitzschutzes fest, um ein tragbares Restrisiko zu erhalten. Technisch besteht ein LPS aus den folgenden Komponenten:

- Blitzfanganlage,
- Ableitungseinrichtung,
- Erdung,
- Potenzialausgleich,
- Trennungsabstand (Abstand zwischen Blitzschutzeinrichtungen und anderen elektrisch leitenden Bauteilenden).

Das LPS legt den Umfang und die Qualität der Blitzschutzmaßnahmen gemäß der Schutzklasse in einem entsprechenden Maßnahmenkatalog fest. Die Umsetzung dieser Maßnahmen erfolgt in Form von mehreren Blitzschutzzonen, die sich in ihrer Schutzwirkung vom äußeren über den inneren Blitzschutz bis zum Potenzialausgleich addieren. So bündelt die Blitzschutzzone 0, auch Lightning Protection Zone (LPZ) genannt, alle äußeren Schutzmaßnahmen gegen direkten Blitzeinschlag und elektromagnetischer Felder, die indirekt durch Blitzeinschlag entstehen. LPZ 1 bis n bündeln die Schutzmaßnahmen des inneren Blitzschutzes und beschreiben mit steigender Kennziffer zunehmende Schutzeinrichtungen gegenüber Überspannungen innerhalb von Gebäuden.

Jede Schutzmaßnahme muss durch die Installation von Schutzelementen umgesetzt werden. Ein Schutzelement, Surge Protecting Device (SPD) genannt, begrenzt an seinem Ausgang die Energie (Strom, Spannung) so weit, dass alle folgenden Elemente (z. B. Verteilernetz, Geräte) keinen Schaden nehmen. Die Leistungsfähigkeit eines SPD wird in drei verschiedene Typen (1 bis 3) eingeteilt. So ist bei der Auswahl eines bestimmten SPD-Typs ausschlaggebend, welche Belastung am Eingang zu erwarten ist. Der Zusammenhang zwischen LPZ und der Auswahl von SPD-Typen wird Koordination des Überspannungsschutzes genannt und ist in Abbildung 4 verdeutlicht.

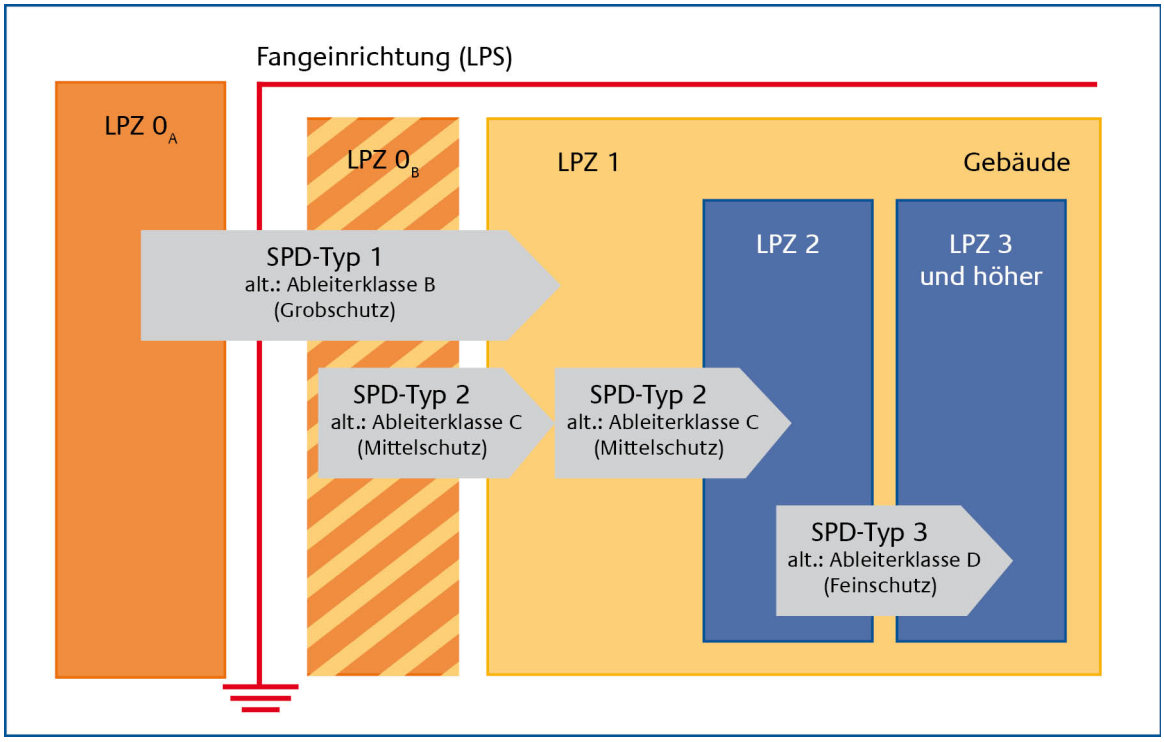


Abbildung 4: Einsatzmöglichkeiten von SPD-Typen in Blitzschutzzonen

Die beiden links rot und rot schraffiert dargestellten Blitzschutzzonen LPZ 0_A und LPZ 0_B repräsentieren den äußeren Blitzschutz. Die beige dargestellte LPZ 1 (das Gebäude) sowie die grün hervorgehobenen LPZ 2 und 3 zeigen den inneren Überspannungsschutz. Alle Maßnahmen einer LPZ bauen von links nach rechts aufeinander auf. Der SPD-Typ 1 ist so robust, dass er in der LPZ 0 bis 1 eingesetzt werden kann und somit Schaden vom SPD-Typ 2 abhält. Dieser wiederum kann von LPZ 0_B bis LPZ 2 eingesetzt werden und schützt den SPD-Typ 3, der lediglich in der LPZ 2 und 3 zum Einsatz kommen kann. Die SPD Typklassifizierungen korrespondieren dabei weitgehend mit den früher verwendeten Ableiterklassen „B“ bis „D“ und den dafür gebräuchlichen Bezeichnungen Grob-, Mittel- und Feinschutz.

Als drittes Element kommt zum äußeren und inneren Blitzschutz der Potenzialausgleich für einen funktionierenden Überspannungsschutz hinzu. Nur wenn alle Schutzeinrichtungen sich auf das gleiche Potenzial beziehen, ist ein optimaler Schutz möglich. Wird dies vernachlässigt, verringert sich die Wirkung von Überspannungsschutzeinrichtungen bis hin zur völligen Unwirksamkeit. Ausgleichsströme zwischen unterschiedlichen Potenzialen können zudem zu Störungen bei der Datenübertragung und zu Beschädigungen von Schnittstellen in IT-Geräten führen.

Bereiche, in denen hochverfügbare IT-Systeme betrieben werden, sollten mindestens als Blitzschutzzone 2 ausgelegt werden. Es sind also alle Maßnahmen der äußeren Blitzschutzzone 0 und der inneren Blitzschutzzonen 1 und 2 umzusetzen. Darüber hinaus muss sich der Überspannungsschutz auf alle Kabelnetze im Gebäude beziehen. Es reicht nicht aus, dies nur für das Stromnetz umzusetzen. Insbesondere sind Netze der Datenkommunikation, Telefonanlage, Kabelnetze der Gefahrenmeldeanlagen, Rohrnetze vorhandener Heizungsinstallationen und Rohrnetze von Versorgungseinrichtungen (Gas- oder Wasserversorgung etc.) in die Überspannungsüberwachung einzubeziehen. Auch sollte eine parallele Kabelverlegung verschiedener Netze vermieden werden, da es zu Spannungsüberkopplungen und dadurch zu Überspannungen auf anderen Leitungen kommen kann. Ein anderer wichtiger Aspekt ist die

konsequente Trennung von Netzen insbesondere dann, wenn getrennte Energieversorgungsnetze existieren. Für Datennetze bietet sich eine galvanische Trennung durch den Einsatz von Lichtwellenleitern (LWL) oder Optokopplern an. Weitere Bedingungen für einen sicheren Betrieb, sind die Verwendung hochwertiger Überspannungsschutzelemente, die ihre Funktionsfähigkeit anzeigen können, sodass diese an einer zentralen Stelle überwacht werden kann sowie die Verwendung eines ableitfähigen und damit antistatischen Bodenbelags mit einem Erdableitwiderstand von $\leq 1 \times 10^8\ \Omega$ (DIN 54346 Klasse 3).

Alle Blitz- und Überspannungsschutzmaßnahmen sind regelmäßig durch Fachpersonal auf ihre Funktionsfähigkeit zu überprüfen und zu warten. Der größte Abstand zwischen den Prüfungen eines Blitzschutzsystem geht aus der DIN 62305-3 Beiblatt 3 hervor und beträgt ja nach Anlagentyp und Gefährdungssituation 1 bis 4 Jahre.

8 Klimatisierung

Die Kühlung ist vielen Fällen Teil der Klimatisierung von IT-Bereichen. Klimatisierung umfasst die Konditionierung der Luft in vielfältiger Weise: Temperatur, Feuchte, Frischluftanteil und Schwebstoffbelastung. In diesem Kompendium werden vornehmlich die Kühlung und die Feuchte betrachtet. Die Frage der Frischluftbeimischung ist keine der Verfügbarkeit von IT, sondern eine der Bereitstellung einer tauglichen Arbeitsumgebung für Personen. Hinsichtlich der Schwebstoffbelastung der Raumluft sind in jedem Fall die Herstellerangaben zu berücksichtigen. Da eigentlich alle derzeit verwendeten Kühlungs- und Klimatisierungssysteme diesen Anforderungen gerecht werden, wird auch dieser Aspekt im Weiteren nicht weiter behandelt.

Im Weiteren sind, wird von Klimatisierung gesprochen, immer nur die beiden Aspekte Temperatur und Luftfeuchte gemeint.

8.1 Anforderungen

Der sichere Betrieb von IT-Systemen erfordert dauerhaft stabile Werte der Umgebungstemperatur und Luftfeuchte, die nur durch hochverfügbare Klimatisierungssysteme garantiert werden können. Werden die von den Herstellern der IT-Systeme vorgeschriebenen Grenzwerte der Betriebsparameter über einen längeren Zeitraum überschritten, drohen Ausfälle und Defekte an den Geräten. Optimale Betriebsbedingungen können aber nur garantiert werden, wenn auch die Klimatisierungsanlage mit ausreichender Redundanz aufgebaut ist. Auch modernste Lösungen garantieren keinen hochverfügbaren Betrieb, wenn Sicherheitsvorkehrungen bei der Installation der Versorgungsleitungen und der Montage technischer Komponenten im Außen- und Innenbereichsbereich vernachlässigt werden. Zudem ist eine regelmäßige Anlagenwartung durch geschultes Personal sowie die Detektion von Defekten unerlässlich. Unabhängig vom gewählten Klimatisierungsprinzip muss das Verhindern von Manipulationen der Anlagenteile oder der Steuerung verhindert werden.

8.2 Klimatisierungsprinzip

Zum hochverfügbaren Betrieb sind die redundante Anlagenauslegung, die zu wählende Kühlstrategie, die Dimensionierung der Kühlleistung und die Erweiterbarkeit der Anlage zu beachten. Besonders auf dem Gebiet der Klimatisierung werden zunehmend bedarfsorientierte und äußerst leistungsfähige Lösungen angeboten.

Betrachtet man die Entwicklung der letzten 10 Jahre, ist ein rasanter Anstieg der pro Quadratmeter abzuführenden Wärme zu verzeichnen. Um 1998 lag die mittlere Wärmelast bei ca. 0,5 kW/m² mit Spitzenwerten noch deutlich unter 1 kW/m². Inzwischen (2008) ist ein Mittelwert von 1,5 kW/m² und Spitzenwerte bei 2,5 kW/m² schon fast die Regel. Trotz „Green IT“ ist ein weiterer Anstieg zu erwarten auf Mittelwerte um 3 kW/m² bei Spitzen bis zu 5 kW/m². In Einzelfällen ist sogar mit noch deutlich höheren Werten zu rechnen. Aus einem mit 40 „Pizzaboxen“ voll bestückten 19“-Schrank müssen bis zu 40 kW abgeführt werden. Je nach Abmessungen des Schrankes liegt die Wärme pro Quadratmeter nur wenig niedriger.

Diese Zahlen machen deutlich, dass man den Kühlungsanforderungen der Zukunft nicht mit den Kühlmechanismen der Vergangenheit begegnen kann, schon gar nicht in Bereichen mit hohen und höchsten Anforderungen an die Verfügbarkeit.

8.2.1 Passive Lüftung

Für die Klimatisierung von IT-Geräten existieren verschiedene Kühlungs- und Lüftungssysteme. Die einfachste Form der Kühlung ist die passive Belüftung. Sie leitet die in den Technikschränken entstandene Warmluft mittels Lüftungsöffnungen in den Raum ab. Zur Unterstützung werden Ventilatoren in den Schränken angebracht, welche die Warmluft besser aus den Schränken abführen können. Passive Kühlung ist nur bei geringer Abwärmeentwicklung (bis wenige 100 W/m²) anwendbar. Neben der begrenzten Kühlleistung funktioniert die passive Kühlung nur, wenn die Außenluft hinreichend kühl ist. Zudem ist die Steuerung passiver Systeme nur sehr begrenzt möglich. Zudem ist es bei dieser Art der Kaltluftzufuhr schwierig, die Schwebstoffbelastung in den zulässigen Grenzen zu halten.

Die passive Kühlung ist für hochverfügbare IT-Systeme nicht geeignet.

8.2.2 Aktive Raumklimatisierung

Das Prinzip des Kühlschranks wird auch für die Klimatisierung von Technikräumen mit einem zu verdampfenden Kältemittel, Kompressor und Kondensator als Wärmetauscher eingesetzt. Kondensator, Verdampfer und Kompressor sind räumlich voneinander getrennte Geräte, die mit Hilfe von Leitungsrohren für das Kältemittel miteinander verbunden sind. Neben dem Prinzip des zu verdampfenden Kältemittels existieren weitere Kühlprinzipien, die auf einem zirkulierenden Wasserkreislauf oder auf der Verwendung anderer Kältemittel (z. B. CO2) basieren.

Das häufigste anzutreffende aktive Prinzip der Klimatisierung ist die klassische Wärmekompensation durch Raumklimatisierung. Vollklimatisierung ist gegeben, wenn durch Zuschaltung von Kühl- oder Heißelementen, Be- oder Entfeuchtern sowie der Beimischung von Frischluft in die Zuluft Betriebsbedingungen in den erforderlichen Grenzen gehalten werden. Die von den Klimageräten erzeugte Kaltluft wird dabei durch den Doppelboden und über Plattenöffnungen in den Technikraum oder direkt in die Technikschränke eingeblasen. Die von den IT-Systemen erzeugte Warmluft wird über das Absaugen der Raumluft den Klimageräten erneut zur Kühlung zugeführt. Klimadecken sollten wegen der im Kapitel 5.1 angeführten Risiken einer abgehängten Decke vermieden werden. Die Anlage befindet sich bei der Vollklimatisierung im Umwälzbetrieb.

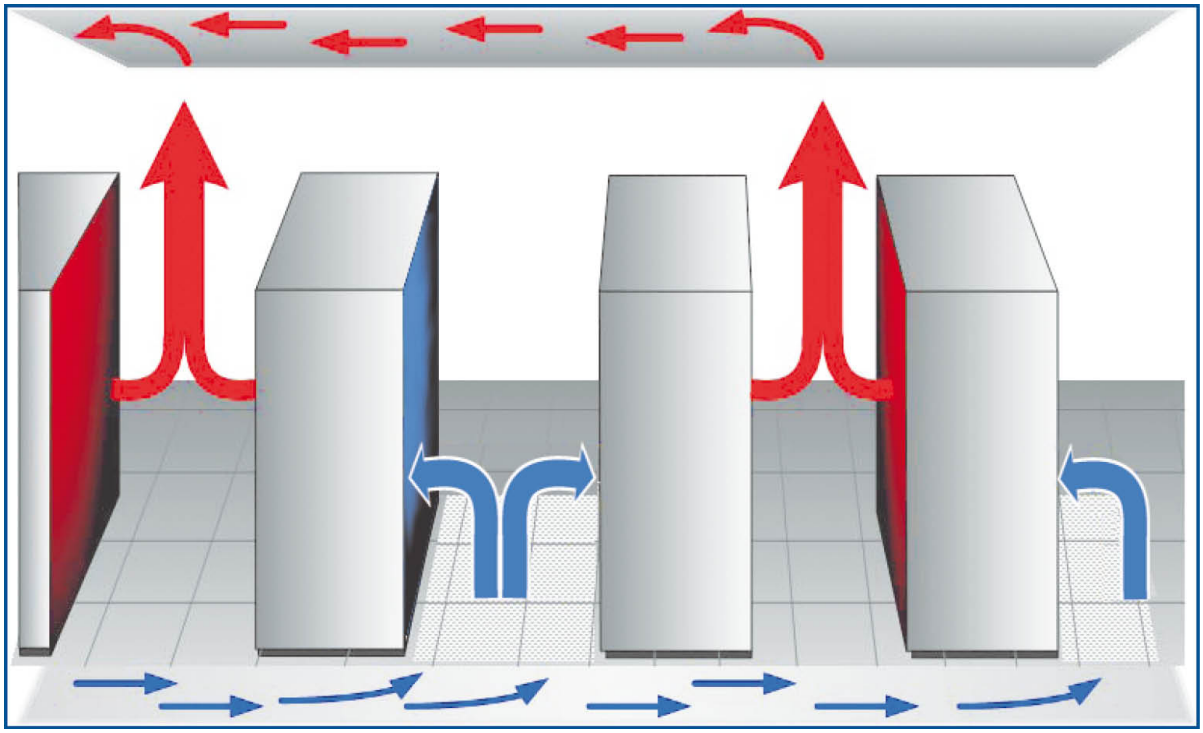


Abbildung 5: Warm- und Kaltluftzonen

Wie in Abbildung 5 dargestellt, saugen zwei jeweils mit der Vorderseite gegenüberstehende Technikschränke die Kühlluft aus der gemeinsamen zentralen Kaltluftzone an. Die Warmluft wird an der Hinterseite jedes Technikschrankes in den Raum abgeführt. Die Rückseite eines Technikschranks bildet so eine eigene Warmluftzone.

Bei der dargestellten Raumklimatisierung ist eine Erhöhung der Kühlleistung nur mithilfe eines höheren Luftdurchsatzes durch Steigerung der Strömungsgeschwindigkeit zu erreichen. Ungünstige Bedingungen im Betriebsraum, ein zu niedriger sowie mit der Installation von Technikkomponenten überfrachteter Doppelboden können die maximale Kühlleistung verringern und rasch zu einer zu warmen Umgebung führen.

Eine solche zwar schon etwas geführte aber im Wesentlichen noch immer freie Kühlung dürfte bis in den Bereich um 2 kW/m² noch ausreichend funktionieren. Bei höheren Werten der Abwärme pro Quadratmeter, also schon in absehbarer Zukunft, sind wesentlich effizientere Lösungen erforderlich, wie sie die Kaltgang Einhausung und die Direktkühlung darstellen.

8.2.3 Kaltgang Einhausung und Direktkühlung

Auch bei der fachgerechten Aufstellung der Technikschränke ist eine völlige Separation von Warm- und Kaltluftzonen praktisch nicht möglich. Durch Verwirbelungen ist immer mit einer Vermischung der Zonen zu rechnen und damit mit einem reduzierten Wirkungsgrad. Diesen Nachteil kann eine Klimatisierungsanlage mithilfe eines isoliert geführten, also vom Raum abgeschotteten Kaltluftstroms beheben, Kaltgang Einhausung genannt.

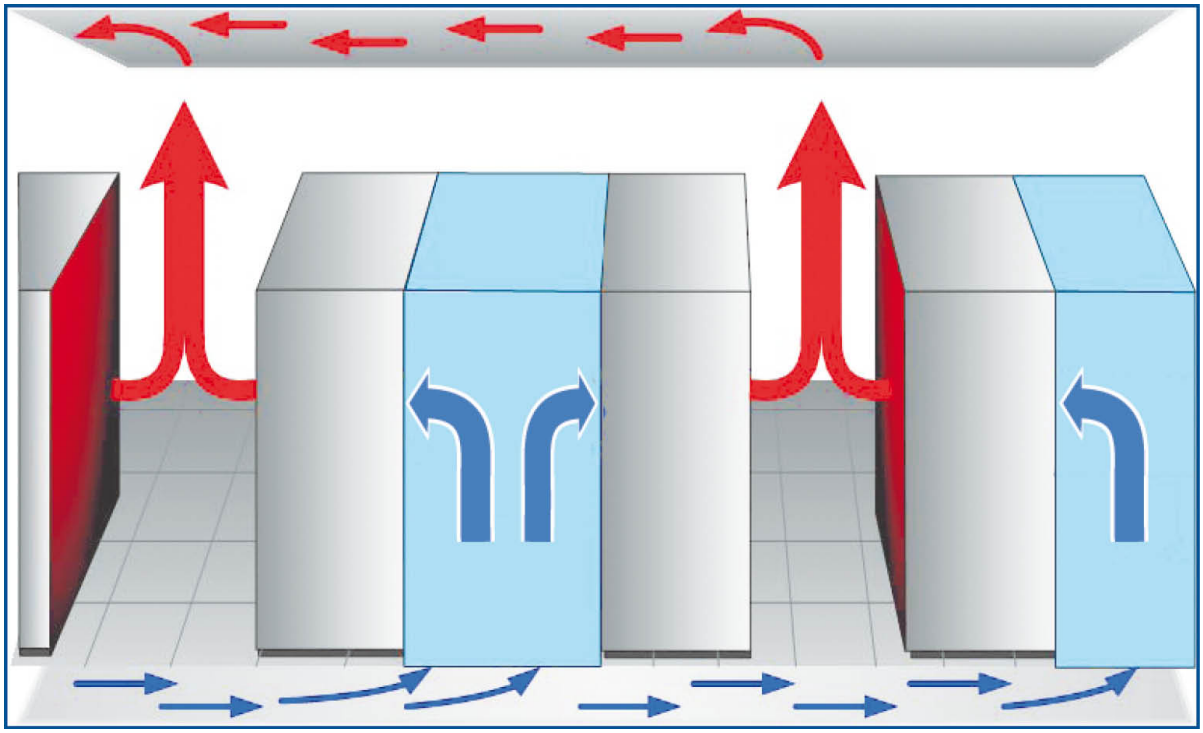


Abbildung 6: Kaltgang-Einhausung

Bei der Kaltgang-Einhausung wird anstatt einer ungezielten und freien Einblasung von Kaltluft über den Doppelboden in den Raum eine isolierte und damit gezielte Kaltlufteinführung über den eingehausten Kaltgang direkt zu den IT-Systemen geführt. Wie in Abbildung 6 dargestellt, wird der Technikschrank mit Hilfe eigener Öffnungen im Doppelboden über die gesamte Höhe mit Kühlluft versorgt. Die gekühlte Luft wird dabei mit gleichmäßig verteiltem Druck direkt in den Technikschrank eingeblasen, wobei die Abwärme aus dem Technikschrank in den Raum abgegeben wird. Das Abführen der Abwärme erfolgt wie bei der klassischen Raumkühlung über das Absaugen der Raumluft. Der Wirkungsgrad und einer solchen Klimatisierungsanlage ist höher als bei der herkömmlichen Raumkühlung und stellt damit eine höhere Kühlleistung zur Verfügung.

Eine ebenfalls effiziente Möglichkeit zur Kühlung hochverfügbarer IT-Systeme ist durch den Einsatz einer bedarfsgerechten Klimatisierung in Form einer Direktkühlung gegeben. Die bedarfsgerechte Klimatisierung einzelner Technikschränke gemäß dem tatsächlichen Kühlbedarf bietet ebenfalls eine deutlich höhere Effizienz gegenüber der klassischen Raumkühlung. Die Kühlung erfolgt durch direkt in den Technikschränken installierte Wärmetauscher. Der Vorteil einer Direktkühlung liegt in der bedarfsorientierten Steuerung der Kühlleistung für IT-Systeme in jedem Technikschrank. Hierdurch wird die Kühlung des gesamten Technikraums vermieden. Die Direktkühlung erfordert den Anschluss jedes zu kühlenden Technikschranks an ein Rohrleitungssystem, über das ein Kältemittel im Kühlkreislauf zirkuliert. Hier sind besondere Sicherheitsmaßnahmen in Bezug auf die Detektion von austretendem Kältemittel zu treffen.

Unbeschadet der zusätzlichen Risiken durch Kühlmittel im eigentlichen IT-Bereich wird die Direktkühlung die Lösung der Zukunft sein. Nur sie ist in der Lage, Wärmelasten sogar bis über 50 kW pro Schrank anzuführen.

8.3 Aufbau und Betrieb

Unabhängig davon, ob die Direktkühlung oder der gehauste Kaltkanal als Klimatisierungsprinzip in hochverfügbaren Infrastrukturen zum Einsatz kommt, sollte der Kühlkreislauf immer redundant ausgelegt sein, um die Klimatisierung auch bei Ausfall eines Kreislaufs aufrechtzuerhalten. Es sind darüber hinaus weitere Sicherheitsvorkehrungen zu treffen, die für alle Klimatisierungsprinzipien gelten. Der Regelung der Parameter einer Klimatisierungsanlage, speziell der Temperatur und Luftfeuchte, kommt eine hohe Bedeutung für die Sicherheit des Betriebs zu. Die Bedienung der automatischen Klimaregelung sollte nur durch berechtigtes und geschultes Personal erfolgen. Auf die Steuerung und Überwachung der Klimatisierungsanlage über eine Fernwartungseinrichtung sollte aufgrund von Manipulationsmöglichkeiten gänzlich verzichtet werden. Die Raumlufttemperatur und -feuchtigkeit sollten unabhängig voneinander einstellbar sein. Die VDI-Richtlinie 2054 „Raumlufttechnische Anlagen für Datenverarbeitung“ kann mit den darin genannten Grenzwerten (Temperatur: 20°C bis 28°C, Luftfeuchte: 30 % bis 68 % r. F.) für die klimatischen Bedingungen der Raumluft in Technikräumen für einen sicheren und effizienten Betrieb herangezogen werden.

Bei der Installation der Außeneinheit einer Klimatisierungsanlage auf dem Dach oder an der Außenwand eines Gebäudes ist auf eine fachgerechte Ausführung des Blitz- und Überspannungsschutzes zu achten. Alle Kabel- und Leitungszuführungen der Klimatisierungsanlagen müssen vor Manipulationen und Brand geschützt durch eigene, geschlossene oder verschließbare Bereiche (Steigschächte, Kabelkanäle, Stahlpanzerrohre) geführt werden. Eine Überwachung dieser Bereiche auf Manipulation und Brand sollte separat erfolgen, eine Alarmierung ist zentral anzuzeigen. Der Zutritt zur Außeneinheit ist zu kontrollieren und zu überwachen. Ein Erreichen der Außeneinheit der Klimatisierungsanlage mit Hilfe von Steighilfen oder mittels technischer Hilfsmittel der Gebäudetechnik (außen liegender Fluchtweg etc.) darf nicht möglich sein.

9 Meldeanlagen

Die Funktionalitäten von Meldeanlagen ähneln in gewisser Weiser denen von Gefahrenmeldeanlagen, dienen jedoch überwiegend der Erfassung und Steuerung von Betriebszuständen oder Betriebsparametern. Eine strikte Trennung der beiden Kategorien Gefahrenmeldeanlagen und Meldeanlagen ist nicht möglich, wird aber innerhalb dieses Dokuments unter dem primären Gesichtspunkt der Erfassung, Übertragung und Anzeige von Betriebszuständen und der Reaktion darauf verstanden. Dies trifft für Zutrittskontroll- wie auch für Videokontrollanlagen zu. Diese dienen in erster Linie der Durchsetzung von organisatorisch vorgegebenen Zwangsläufigkeiten, die mit Hilfe technischer Anlagen durchgesetzt und kontrolliert werden sollen. Eine Zutrittskontrollanlage (ZKA) erfasst und protokolliert Türzustände und gewährt oder verweigert Zutritte gemäß den im System hinterlegten Berechtigungsprofilen. Erst ein unzulässiger Betriebszustand, z. B. eine Türoffenzeitüberschreitung, führt zu einer Meldung, die ein Alarm darstellen kann. Die Definition gilt auch für die Videokontrollanlagen. Hier werden optische Bildaufnahmen aufgezeichnet, verarbeitet, angezeigt und gespeichert, welche unter Umständen auf eine Gefahr hindeuten, wenn unerwartete Ereignisse erkannt werden.

9.1 Zutrittskontrolle

Für die Durchsetzung von Zutrittsregelungen in hochverfügbaren Infrastrukturen reicht ein mechanisches Schließsystem, das auf Schlüsseln basiert, nicht aus. Hierzu sind die Installation und der Betrieb eines sicheren Zutrittskontrollsystems (ZKS) mit allen erforderlichen baulichen, apparativen und organisatorischen Details notwendig. Ein ZKS besteht gemäß der Norm DIN V VDE 0830-8-1 neben den baulichen und organisatorischen Komponenten technisch aus einer Zutrittskontrollanlage (ZKA). Eine ZKA besteht grundsätzlich aus den technischen Komponenten

- Übergeordnete Zutrittskontroll-Zentrale (ÜZKZ),
- Bedienungs- und/oder Anzeigeeinheiten (BAE),
- Zutrittskontrollzentrale (ZKZ),
- Zutrittskontrollstellglied und
- an den Türen angebrachten Identifikationsmerkmal-Erfassungseinheiten (z. B. Chipkartenleser).

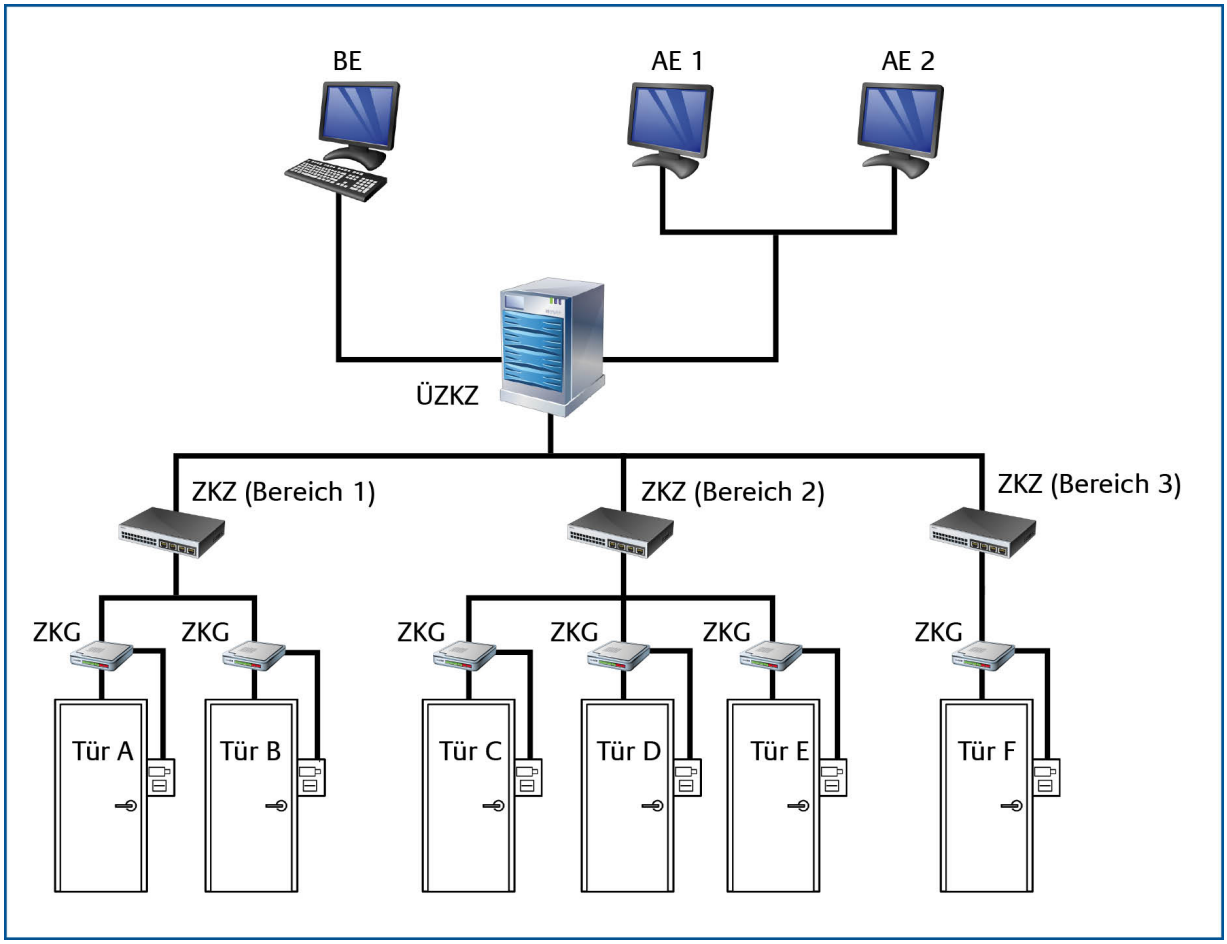


Abbildung 7: Beispiel eines ZKA-Aufbaus

In der Abbildung 7 ist eine ZKA beispielhaft schematisch dargestellt. An der ÜZKZ ist eine Bedienungseinheit als Administrationszugang angeschlossen. Die beiden Anzeigeeinheiten dienen der Beobachtung von Ereignis- oder Alarmdaten an verschiedenen ständig besetzten Stellen. Die ÜZKZ verteilt die über die BE eingegebenen Zutrittsberechtigungsdaten an verschiedene ZKAen für die Zutrittskontrolle dreier getrennter Sicherheitsbereiche mit insgesamt sechs Türen (Türen A bis F). Alle Türen verfügen über ein eigenes Zutrittskontrollstellglied (ZKG), an dem die Türzustandssensoren und Motorschlösser (beide nicht dargestellt) angeschlossen sind. Jedes ZKG meldet den Türzustand zur ZKZ und steuert die Freigabe der Tür für einen gewährten Zutritt. Die Ansteuerung erfolgt durch die ZKZ nur nach erfolgreicher Identifizierung und Authentifizierung eines Ausweises oder einer Person. Die Identifikationsmerkmal-Erfassungseinheit (Terminal) an jeder Tür wird über das lokale Zutrittskontrollglied an die ZKA angebunden. Eine direkte Anbindung eines Terminals an die ZKZ ist ebenfalls denkbar. Die Kommunikation des Terminals erfolgt jedoch immer gesichert direkt mit der ZKZ.

9.1.1 Übergeordnete Zutrittskontrollzentrale

Die ÜZKZ ist die zentrale Steuereinheit in einer ZKA. Die ÜZKZ steuert die Maßnahmen der Zutrittskontrolle, um organisatorische Festlegungen umzusetzen. In ihr sind in einer Datenbank die Zutrittsberechtigungsdaten in Raumzonen (Raum oder Bereich) und Zeitzonen (Zeitintervall der Berechtigung) gespeichert, innerhalb derer ein Zutritt für Personen gewährt oder verweigert wird.

Die Festlegung weiterer Funktionen und die Umsetzung der Zutrittsorganisation für Personal oder Besucher erfolgt ebenfalls in der ÜZKZ. So kann individuell festgelegt werden, in welchem Raum z. B. eine Zutrittswiederholkontrolle (Anti-Pass-Back) oder eine Zwei-Personen-Zutrittskontrolle (Vier-Augen-Prinzip) durchgeführt werden soll. Beim Anti-Pass-Back Verfahren wird kein weiterer Zutritt in einen anderen Raum gestattet, wenn nicht vorher eine Ausbuchung aus der bereits betretenen Raumzone erfolgt ist. Das Vier-Augen-Prinzip fordert mindestens zwei zutrittsberechtigte Personen, die sich nacheinander innerhalb einer festgelegten Zeit in eine Raumzone einbuchen müssen. Für die Zutrittskontrolle in hochverfügbaren Infrastrukturen sollten für besonders schützenswerte Bereiche die genannten Funktionen umgesetzt werden. Weitere Kontrollmöglichkeiten bieten die Mehr-Personen-Anwesenheitskontrolle (ein Zutrittsberechtigter darf sich nicht allein in einem Raum befinden) oder die Raumzonenwechselkontrolle (ein Zutritt in eine benachbarte Raumzone kann nur erfolgen, wenn in der davor liegenden Zone eine Einbuchung erfolgte). Die Einrichtung einer Nötigungs-PIN sollte erwogen werden, wenn die Gefahr von Überfällen besteht. Mit der Eingabe einer festgelegten PIN durch einen zur Türöffnung genötigten Mitarbeiter wird das Überwachungspersonal über die Nötigung informiert und kann Gegenmaßnahmen einleiten. Es ist bei der Planung der Zutrittsberechtigungen für jeden Raum oder Bereich zu entscheiden, wie mechanische Zwangsläufigkeiten umzusetzen sind. Manche Regelungen lassen sich nur durch die Installation von zusätzlichen Einrichtungen, z. B. einer Personenvereinzelungsschleuse, umsetzten, um die Anwesenheit in und die Ausbuchung aus einer Raumzone für das ZKS zweifelsfrei festzustellen.

Die ÜZKZ und die BAE zur Administration müssen selbst in einem zutrittsgeschützten Raum mit der Überwachung durch die Einbruchmeldeanlage installiert sein. Die BAE sollte darüber hinaus mit einem Zugangsschutz ausgestattet sein, damit eine Administration der ÜZKZ nur von berechtigtem Personal erfolgen kann.

9.1.2 Zutrittskontrollzentrale

Die Zutrittskontrollzentrale (ZKZ) steuert die lokale Zutrittskontrolle in den ihr zugeordneten Bereichen. Die ZKZ ist in lokaler Nähe zu den zu steuernden Türen installiert. An einer ZKZ sind die mechanischen und elektromechanischen Zutrittskontrollstellglieder oder die Terminals zur Identifikationsmerkmalerfassung (z. B. biometrischer Sensor, Chipkatzenleser) der Türen angeschlossen. In der ZKZ werden alle an sie übertragenen Identifikationsmerkmale mit den hinterlegten Zutrittsberechtigungsdaten verglichen und bei vorliegender Berechtigung eine Öffnung durch Ansteuerung der Zutrittskontrollstellglieder der angeschlossenen Türöffner oder Motorschlösser veranlasst. Dabei wird der Zutritt protokolliert und gespeichert sowie an die ÜZKZ übertragen. Eine ZKZ sollte autark, also ohne Kontakt zur ÜZKZ, funktionsfähig sein und muss über eine eigene unabhängige Stromversorgung verfügen. Die Konfiguration und Steuerung der ZKZ sollte ausschließlich über die ÜZKZ erfolgen. Da alle benötigten Zutrittsberechtigungsdaten lokal gespeichert sind, muss die ZKZ selbst in dem zu kontrollierenden Bereich sabotagegeschützt installiert sein. Das Gehäuse der ZKZ sollte zusätzlich gegenüber unberechtigtem Öffnen überwacht werden. Die Kommunikation zwischen der ÜZKZ und den lokalen ZKZen erfolgt mit Hilfe von Protokollen entweder über ein vorhandenes LAN/WAN oder eine eigene Verkabelung. In allen Fällen ist wegen der Vertraulichkeit der Zugangsberechtigungs- und Ereignisdaten eine gesicherte (verschlüsselte) Kommunikation dringend zu empfehlen.

Neue Entwicklungen zeigen, dass die Integrationsdichte auch im Bereich der Zutrittskontrollsysteme weiter fortschreitet. So verzichten vermehrt Systeme auf eine eigenständige ZKZ und integrieren deren Funktionalitäten in die Zutrittskontrollstellglieder zu einem Controller,

der direkt mit der ÜZKZ über Protokolle (z. B. IP-basiert) kommuniziert und zusätzlich in der Lage ist, die Türsteuerung zu übernehmen. Jedoch ist auch hier darauf zu achten, dass die Kommunikation zwischen Controller und ÜZKZ gesichert ist.

9.1.3 Türsteuerung und -Überwachung

Die Türsteuerung erfolgt direkt von einem Zutrittskontrollstellglied oder Türsteuermodul. Das Türsteuermodul versorgt die in der Tür eingebauten Türöffner, Motorschlösser oder andere elektromechanischen Einrichtung mit Spannung zur Betätigung. Über das Türsteuermodul werden ebenfalls Türzustände (offen, geschlossen, verriegelt etc.) durch in oder an der Tür montierte Meldesensoren (z. B. Magnet- oder Riegelkontakte) erfasst und deren Zustand an die ZKZ signalisiert. Unter Umständen sind das Türsteuermodul auch die an den Türen vorhandenen Identifikationserfassungsterminals angeschlossen. Das Türsteuermodul hat in einem ZKS eine zentrale Sicherheitsfunktion, da es den Türzustand direkt beeinflusst. Es muss daher immer sabotagegeschützt im zutrittskontrollierten und überwachten Bereich installiert sein. Die in den Türen eingebauten Motorschlösser oder Türöffner müssen mindestens der Widerstandsklasse der Tür entsprechen. Bei der Verkabelung ist darauf zu achten, dass eine Manipulation von außen nicht möglich ist.

9.1.4 Identifizierung und Authentifizierung

Die Identifikation von berechtigten Personen gegenüber dem im ZKS gespeicherten Profil der Zutrittsberechtigungsdaten erfolgt mit Hilfe eines Identifikationsmerkmailträgers, oder besser bekannt als Token oder Ausweis in Form z. B. einer Chipkarte (kontaktiertet, kontaktlos) oder über individuelle biometrische Merkmale. Neben der Identifizierung, also dem Besitz eines Ausweises, ist insbesondere für die Kontrolle von hochverfügbaren Infrastrukturen auch die Authentifizierung (Echtheitsprüfung) des Ausweises von Bedeutung, um unerlaubte Kopien erkennen zu können. Neben dem „Besitz“ ist auch das „Wissen“ eines zusätzlichen Geheimnisses für die Zutrittskontrolle in hochverfügbaren Infrastrukturen von Bedeutung. So sollte neben der Identifikation über den Besitz eines Tokens die zusätzliche Eingabe einer mehrstelligen PIN oder die Abfrage eines biometrischen Merkmals erfolgen.

Der Ausweis sowie das Hintergrundsystem müssen in der Lage sein, gesichert zu kommunizieren und eine Fälschungserkennung aufweisen. Es sind verschiedene Betriebssysteme und Hardwareplattformen für Token verfügbar, die über eine Sicherheitszertifizierung verfügen. Solche Systeme sind beim Einsatz in hochverfügbaren Infrastrukturen zu bevorzugen.

Zutrittskontrollsysteme auf Basis biometrischer Merkmale erfassen als Identifikationsmerkmal individuelle körperliche Merkmale des Menschen. Dies bietet den Vorteil, dass das Identifikationsmittel nicht verloren gehen kann oder wie eine PIN vergessen werden kann. Verschiedene Merkmale des Menschen werden für eine Identifizierung genutzt. Gängige Verfahren nutzen

- die menschliche Iris,
- den Fingerabdruck,
- die Geometrie der Hände,
- das optische Abbild des Gesichts oder

– die Stimmerkennung.

Je nach Art des biometrischen Verfahrens zur Identifizierung und der verwendeten Sensortechnologie kann die Überbindungssicherheit sehr schlecht oder auch sehr hoch sein. So spielt die Einsatzumgebung eine wesentliche Rolle für die Wahl eines geeigneten Verfahrens. Falls eine visuelle oder per Videokontrollanlage überwachte Stelle zur Erfassung biometrischer Merkmale existiert, kann eine niedrigere Fälschungssicherheit akzeptiert werden, als wenn ein Erfassungsterminal nicht beobachtet wird. In Bezug auf Fehlerraten ist ein gut geplantes auf Biometrie basierendes ZKS in der Lage, ähnliche Fehlerraten wie die herkömmlicher Systeme zu erreichen. Für beide Systemarten gilt der Grundsatz einer sorgfältigen Auswahl der grundlegenden Technikkomponenten insbesondere bei der Identifikationsmerkmalerfassung und der Definition organisatorischer Verfahren. In jedem Fall sind bei der Planung eines ZKS die betrieblichen Arbeitnehmervertretungen einzubeziehen, um Transparenz zu schaffen. Die oft angeführte schlechte Benutzerakzeptanz sollte im Umfeld des Betriebs hochverfügbarer Infrastrukturen kein Einwand gegenüber der Verwendung biometrischer Verfahren für die Zutrittskontrolle sein.

Bei der Planung eines ZKS in hochverfügbaren Infrastrukturen sollte geprüft werden, ob die Verbindung aus Ausweis mit Authentifizierungsfunktion (Echtheitsprüfung des Ausweises) und die zusätzliche Erfassung eines biometrischen Merkmals (Echtheitsprüfung der Person) eine praktikable und praxisgerechte Kombination darstellt.

9.2 Videokontrolle

Videokontrollanlagen ergänzen die Schutzfunktionen der Zutrittskontrolle und der Einbruchmeldung. Sie dienen der visuellen Überwachung von Außen- und Innenbereichen, Objekten oder Personen mit Hilfe von Videokameras, Monitoren oder Aufzeichnungsgeräten. Ein zu einem Closed Circuit Television (CCTV) zusammengefasstes geschlossenes System besteht aus einer Vielzahl von Komponenten. Ein herkömmliches CCTV-System, welches auf Analogtechnik basiert, besteht aus den analogen Videokameras, einer sogenannten Kreuzschiene oder Videomultiplexer, die das analoge Bild zu verschiedenen Überwachungsmonitoren über Koaxialkabel oder Fiberoptikkabel überträgt und verteilt. Zur Bildaufzeichnung bei nicht ständig beobachteten Monitoren oder für die Nachvollziehbarkeit von Ereignissen dient in solchen Systemen ein Langzeitvideorekorder oder ein IT-gestütztes System, welches das analoge Bild kontinuierlich aufzeichnet. Die Beleuchtung des Überwachungsobjekts bei nicht ausreichenden Lichtverhältnissen erfolgt meist durch Infrarotscheinwerfer.

Die jeweiligen Komponenten einer Videokontrollanlage müssen einzeln vor Sabotage oder Umwelteinflüssen geschützt werden. Der mechanische Schutz von Außenkameras erfolgt durch ein Wetterschutzgehäuse, welches die Kameras vor äußeren Einflüssen (z. B. Feuchtigkeit, Staub etc.) schützt. Die Kameras selbst müssen sabotagegeschützt (nicht direkt erreichbar) montiert sein und einen Verdrehschutz oder weitere Sabotageschutzmechanismen aufweisen. Die Monitore, Aufzeichnungsgeräte und vor allem die Aufzeichnungsmedien sind vor unberechtigtem Zugriff zu schützen. Hierzu sollten die Aufzeichnungsgeräte in einem vor unberechtigtem Zutritt geschützten Raum installiert werden. Die Beobachtungsmonitore befinden sich an einer ständig besetzten Stelle (z. B. Pförtner). Für die Anlagenverkabelung gelten die gleichen Sicherheitsvorkehrungen wie für die Verkabelung der Energieversorgung und/oder des LAN/WAN. Eine vorhandene Außenverkabelung muss besonders vor mechanischer Beschädigung oder Manipulation geschützt werden. Hierzu können spezielle Kabelschutzsysteme oder überwachte Kabelkanäle dienen. Auch für das Kabelnetzwerk der Videoüberwachungsanlage ist der Blitz- und Überspannungsschutz umzusetzen.

Vermehrt kommen moderne digitale Videoüberwachungssysteme zum Einsatz. Die Signale der Videokameras werden direkt digitalisiert und sind an ein vorhandenes (meist IP basiertes) LAN/WAN angeschlossen. Ein digitales Videoüberwachungssystem besteht aus einer Vielzahl von Komponenten, die zu einem Videomanagementsystem zusammengefasst werden können. Es handelt sich hierbei um ein Rechner-gestütztes System mit spezieller Software, welche die Übertragung, Verwaltung und Speicherung der digitalen Videobilder kontrolliert und Schnittstellen zu vorhandenen Sicherheitsleitsystemen bereitstellt. Solche Systeme lassen sich leicht erweitern, da auf eine vorhandene LAN-Verkabelung als Kommunikationsverbindung zurückgegriffen werden kann. Vor allem bei weit auseinanderliegenden Kameras bietet sich hierdurch ein Vorteil, weil das Videosignal nicht durch analoge Verstärker für weite Übertragungsstrecken aufbereitet werden muss und die Aufzeichnung ohne eine Analog/Digital-Wandlung erfolgen kann. Auch analoge Kameras können über Video-Server an ein digitales Videokontrollsystem angeschlossen werden. Damit ist ein Mischbetrieb zwischen analogen und digitalen Videokameras möglich. Die Signale werden dann ebenfalls über das vorhandene LAN/WAN übertragen. Insbesondere für digitale Systeme, die mit „Video Over IP“ arbeiten, sind neben der Bereitstellung ausreichender Bandbreite für die Bildübertragung Sicherheitsmaßnahmen umzusetzen, die auch in der Informationstechnik zum Einsatz kommen.

10 Gefahrenmeldeanlagen

Gefahrenmeldeanlagen dienen gemäß der Norm DIN VDE 0833 dem zuverlässigen Erkennen und Melden von Gefahren für Personen und Sachen. Über die Definition der Norm hinaus werden unter dem Begriff Gefahrenmeldeanlage (GMA) folgende Anlagentypen zusammengefasst:

- Brandmeldeanlage (BMA),
- Leckagemeldeanlage (LMA),
- Einbruchmeldeanlage (EMA),
- Überfallmeldeanlagen (ÜMA),
- und die Übertragungsanlage (ÜAG),

welche der Aufnahme und Übertragung von Meldungen an eine zentrale Stelle dient. Die ÜAG ist zumeist integraler Bestandteil der einzelnen Anlagentypen und wird daher nicht gesondert betrachtet.

Über die Definition der Norm hinaus können jedoch weitere Gefahren für einen Sicherheitsbereich auftreten. So sind z. B. das Eindringen von Wasser und die Detektion von Überspannungen weitere ernst zu nehmende Gefahren für den hochverfügbaren IT-Betrieb. Moderne GMA-Systeme wachsen zunehmend mit der Gebäudeleittechnik oder der Zutrittskontrolle zu umfangreichen Gebäudemanagementsystemen zusammen, vor allem bei der Weiterleitung und zentralen Anzeige von Ereignissen oder der gemeinsamen Nutzung von Übertragungswegen. Auch werden Anlagenteile gemeinsam genutzt, wie die Verwendung von Terminals der Zutrittskontrolle zur Scharf- und Unscharfschaltung der EMA. Trotz dieser Entwicklung muss jede Komponente einer GMA für sich betrachtet und anlagentypische Sicherheitsanforderungen für die Installation und den Betrieb berücksichtigt werden. Insbesondere ist bei der gemeinsamen Nutzung von Datenkommunikationseinrichtungen (z. B. ein IP basiertes Netzwerk) auf die Umsetzung von Schutzfunktionen der IT-Sicherheit in Bezug auf die Identifizierung und Authentifizierung sowie eine gesicherte (verschlüsselte) Datenübertragung zu achten. Es ist also bei der Erstellung eines IT-Sicherheitskonzepts nicht nur die Kommunikation von hochverfügbaren IT-Systemen zu berücksichtigen, sondern ebenfalls die Kommunikation der Gefahrenmeldeanlagen.

10.1 Brandmeldeanlagen und Löschung

Der technische Brandschutz ergänzt den baulichen Brandschutz, den ein Gebäude oder der Ausbau (Türen, Wände, Bodenbeläge etc.) durch bauteilabhängige Widerstände gegenüber thermischer Belastung zur Verfügung stellt. Folglich steht gleichwertig neben dem baulichen der technische Brandschutz. Er umfasst die Gesamtheit aller Brandschutzmaßnahmen, die durch Nutzung spezieller Anlagen und technischer Mittel sowohl vorbeugend (Detektion) als auch abwehrend (automatische Löschung) wirken. Fehler beim baulichen Brandschutz können nicht durch die Installation eines noch so umfangreichen technischen Brandschutzes beseitigt werden. Nur das sinnvolle Zusammenwirken von baulichem und technischem Brandschutz stellt einen optimalen Schutz gegen Brände und deren Folgen dar. Während der Arbeitszeit kann ein Brand von Mitarbeitern erkannt werden. Außerhalb der Arbeitszeit ist dies nicht möglich. Um einen Schaden durch Brand so gering wie möglich zu halten, ist es daher notwendig, den Brand so früh wie möglich zu erkennen und automatisch zu bekämpfen. Hierzu stehen moderne Brandmeldeanlagen

und Löschsysteme zur Verfügung, die grundsätzlich über eine VdS-Anerkennung verfügen sowie einer regelmäßigen und fachkundigen Wartung unterliegen müssen.

10.1.1 Brandmeldezentrale

Die zentrale Komponente jeder Brandmeldeanlage ist die Brandmeldezentrale (BMZ). Hier laufen die Meldungen aller Melder zusammen und werden ausgewertet. Aus den Meldungen leitet die BMZ unterschiedliche Reaktionen ab. In erster Linie wird natürlich eine Brandmeldung an eine hilfeleistende Stelle, meist direkt die Feuerwehr, abgesetzt. Darüber hinaus steuert die BMZ-Alarmierungseinrichtungen (akustisch, optisch), das Abschalten der Klimatisierungsanlage, das Schließen von Feuer- und Rauschschutztüren sowie das Öffnen von Rauch- und Wärmeabzügen sowie die Aktivierung der Löschanlagen. Die Verknüpfung der BMZ mit sicherheitstechnischen IT-Einrichtungen, wie dem geregelten Herunterfahren nicht hochverfügbarer IT-Systeme oder die Umschaltung auf hochverfügbare redundante Systeme wird dringend empfohlen. Die Brandmeldezentrale sollte an einer zentral gelegenen und ständig besetzten Stelle (z. B. Sicherheitswarte) installiert werden. Der Zutritt zur BMZ muss kontrolliert sein, um Sabotage oder Fehlbedienungen auszuschließen.

10.1.2 Brandmelder

Die Detektion von Feuer, Schwelbrand oder Rauch erfolgt durch an die BMZ angeschlossenen automatischen Melder. Folgende Melderarten sind verfügbar:

- Optische Rauchmelder oder Ionisationsrauchmelder erkennen die bei der Verbrennung entstehenden Rauchgase,
- Wärmedifferenzmelder und Wärmemaximalmelder dienen zur Erkennung eines besonders schnellen oder hohen Temperaturanstieges,
- Flammenmelder erkennen die charakteristischen Strahlungseigenschaften einer offenen Flamme (spektrale Zusammensetzung und Flackerverhalten).

Alle genannten Melderarten gelten als technisch ausgereift. Die Auswahl eines geeigneten Melders oder die Kombination aus den Melderarten hängt jedoch immer vom Einsatzort, also von der Art des zu erwartenden Rauchs ab. Hier spielen die im zu überwachenden Bereich verwendeten Baustoffe eine wichtige Rolle und die bei Brand zu erwartende Art der Verbrennung sowie die entstehenden Rauchgase. Bei allen Melderarten muss immer mit einer Veränderung des Detektionsverhaltens auf Grund von Alterung und Verschmutzung gerechnet werden. Auch wenn moderne Melder in der Lage sind, ihre Alarmschwelle in bestimmten Grenzen nachzuführen und Störungen durch Selbstüberwachung anzuzeigen, sind Melder nur dann in der Lage, ihre Aufgabe zu erfüllen, wenn diese einer regelmäßigen und fachgerechten Wartung unterzogen werden.

10.1.3 Brandüberwachung

Die Detektion von Bränden erfolgt meist über eine Raumüberwachung. Dies ist jedoch nur für Bereiche zu empfehlen, in denen keine hochverfügbaren IT-Systeme betrieben werden. Die Überwachung eines Raumes erfolgt mit Hilfe von an der Decke installierten Brandmeldern. Ebenso werden Doppelböden in die Brandüberwachung mit Hilfe von Brandmeldern einbezogen. Die

häufigste Brandart in Bereichen, in den IT-Systeme betrieben werden, ist der Schwelbrand. Hierbei ist kaum ein Temperaturanstieg zu bemerken, aber eine stärkere Rauchgasentwicklung im Umfeld des Brandes. Die in der Brandentstehungsphase noch geringe Rauchgasmenge wird durch die Gehäuselüftung eines Rechners nur zu einem Teil nach außen transportiert und dort bei vorhandener Klimaanlage mit der Raumluft verwirbelt. Die Rauchgas-Konzentration an der Decke bleibt lange weit unter der Detektionsschwelle des Melders. Die Luftabsaugung der Klimaanlage sorgt zusätzlich dafür, dass eine ausreichende Rauchgas-Konzentration weiter verzögert oder gar verhindert wird. Zusammen mit der Errichtervorschrift, dass erst zwei Melder auslösen müssen, bevor der Alarm an die Feuerwehr weitergeleitet werden darf (Zwei-Linien-Abhängigkeit) und bevor eine automatische Löschung erfolgt, führt dies dazu, dass besonders in vollklimatisierten Räumen meist jeder Löscheinsatz zu spät kommt.

Die Detektion von Bränden sollte in Bereichen, in den IT-Systeme betrieben werden, durch eine sogenannte Brandfrühesterkennung erfolgen. Dabei wird die Abluft einzelner IT-Geräte (Rechner, Drucker, USV, Klimaanlage etc.) durch ein Rauchansaugsystem (RAS) einem empfindlichen Rauchmelder zugeleitet und von diesem ausgewertet. Systeme, welche die Luft direkt aus dem Gerät ansaugen, reagieren deutlich früher als solche, die die Luft aus der Raumluft entnehmen. Entsprechend der Rauchgaskonzentration werden durch das System unterschiedliche Maßnahmen ausgelöst. Diese reichen von der Information eines Anlagen-Betreuers über die Energieabschaltung des betroffenen Gerätes und automatischen Umschaltung auf ein redundantes System, bis hin zum Feueralarm und ggf. einer Löschung des betroffenen Gerätes.

10.1.4 Löschung

Es existieren verschiedene Arten der Löschung von Bränden. Nur einige hiervon eignen sich zum Einsatz in Räumen, in denen IT-Systeme betrieben werden. Die Handlöschung mit Hilfe von Handfeuerlöschern (Pulver, Wasser, CO2) ist für sicherheitsbedürftige Bereiche nicht geeignet, da ein Brand wegen der Entstehung korrosiver Brandgase möglichst früh erkannt und bekämpft werden muss. Die meisten Brände sind kurz nach der Entstehung nicht mehr durch Handlöschung beherrschbar. Handfeuerlöscher sollten jedoch in Bürobereichen gut erreichbar installiert sein und die Mitarbeiter sollten mit dem Umgang vertraut sein. Die Brandbekämpfung bei größeren Bränden oder außerhalb der Arbeitszeit muss der Feuerwehr oder einer automatischen Löschanlage überlassen werden.

Die Feuerwehr kann einen Schaden nur dann optimal begrenzen, wenn der Einsatzfall gut vorbereitet wurde, die Zufahrten zum Gebäude sowie die Einsatzwege im Gebäude frei sind und der Anfahrtsweg kurz genug ist. Da die Feuerwehren keine Rücksicht auf IT-Sicherheitsanforderungen nehmen, ist eine Löschung durch die Feuerwehr meist gleichbedeutend mit einer Zerstörung der Infrastruktur, da hier neben den Schäden durch Brand zusätzlich mit massiven Schäden durch Löschwasser gerechnet werden muss. Fast immer ist mit einer umfangreichen und lang andauernden Sanierung des Bereichs zu rechnen, der den sicheren Betrieb von IT unmöglich macht. Es muss daher ein Löschsystem ausgewählt werden, welches Brände wirksam löscht, die Löschung lokal begrenzt und eine Löschung den IT-Betrieb nicht nachhaltig stört. Zusätzlich sind weitere Sicherheitsmaßnahmen umzusetzen, um Brände möglichst kurz nach ihrer Entstehung zu löschen. Allein durch die Energieabschaltung von elektronischen Geräten kann die Wahrscheinlichkeit größerer Schäden deutlich reduziert werden. Ergänzend dazu kann nur eine automatische Löschanlage die Anforderungen an eine effiziente Löschung erfüllen. Eine Löschanlage, die einen begrenzten Bereich löscht, besteht aus einer Löschsteuerzentrale, einer Signalisierungseinheit und den Löschmittelbehältern, die meist in Batterien zu mehreren Behältern außerhalb des zu

löschenden Bereichs installiert sind. Die Löschsteuerzentrale löst bei der Detektion eines Brandes die Löschung eines Bereichs mit vorhergehender akustischer und optischer Signalisierung verzögert aus. Wichtig dabei ist der Einsatz des geeigneten Löschmittels. Wasser, Löschschaum und Löschpulver sind wegen der Folgeschäden an den IT-Systemen nicht geeignet. Hier muss auf Löschgase zurückgegriffen werden.

Das bei einer Löschung ausströmende Gas verdrängt entweder den zur Verbrennung notwendigen Sauerstoff oder hemmt die Flammbildung chemisch. Dazu werden Gasgemische wie CO2 oder Inergen (bestehend aus Stickstoff, Argon und CO2) eingesetzt, aber auch Gase in reiner Form wie Stickstoff oder das Edelgas Argon. Das äußerst wirkungsvolle und für den Menschen als ungefährlich geltende Gas Halon ist wegen seiner Ozon-Schädigenden Wirkung verboten. Alle erlaubten Verdrängungsgase sind auf Grund ihrer Wirkungsweise (Sauerstoffverdrängung) in den benötigten Löschgaskonzentrationen (ca. 35 - 50%) prinzipiell für Menschen gefährlich. Sie dürfen daher nur mit einer Zeitverzögerung, während deren die Personen den Raum verlassen können, eingesetzt werden. Um eine Löschwirkung zu erzielen, muss das aus einer Löschanlage in einen Brandbereich einströmende Löschgas einen Volumenanteil von ca. 8% erreichen. Die Erhöhung des Volumenanteils zu Beginn der Raumlöschung ist mit einer starken Druckerhöhung im Brandbereich verbunden. Alle Brandschutzkonstruktionen (z. B. Türen, Wände, Brandschutzklappen) müssen so konstruiert und angeordnet sein, dass sie diesem zusätzlichen Druck standhalten können. Nach erfolgter Löschung müssen Lösch- und Rauchgase aus dem gefluteten Bereich erst entfernt werden (Absaugung, Lüftung etc.), bevor Personen den Bereich wieder betreten dürfen.

Eine Alternative zur Raumlöschung ist die Verwendung einer lokal begrenzt wirkenden Objektlöschanlage. Solche Systeme verwenden, ähnlich wie eine Raumlöschanlage, Gase, um den Verbrennungsprozess zu beenden. Objektlöschanlagen werden in oder auf Technikschränken installiert, in denen die IT-Systeme betrieben werden. Das Löschgas befindet sich in einem lokalen Vorratsbehälter. Erfolgt die Detektion eines Brandes, so wird der Technikschrank gasdicht durch installierte Schottsysteme verschlossen, die Geräte spannungsfrei geschaltet und die Löschung ausgelöst. Das Auslösen wird optisch und akustisch angezeigt und als Alarmmeldung an eine ständig besetzte Stelle weitergeleitet. Ein wesentlicher Vorteil ist dabei, dass die Löschung lokal auf wenige IT-Systeme begrenzt ist und keine Evakuierung des gesamten Raumes erfolgen muss. Zudem kann sogar Löschgas wie CO2 verwendet werden, das effizient wirkt, aber für eine Raumlöschung wegen der Gefährlichkeit für Menschen und der damit verbundenen Installation umfangreicher technischer Schutzmaßnahmen nicht mehr zum Einsatz kommt. Der Einsatz von Objektlöschanlagen erfordert zudem speziell ausgestattete Technikschränke und ist mit einem höheren Installationsaufwand verbunden, da jeder zu löschende Technikschrank ausgerüstet werden muss. Der Aufwand relativiert sich jedoch, wenn man die Kosten für eine Füllung der Gasbatterie einer Raumlöschanlage nach Auslösung, die Evakuierung des Personals eines Bereichs und den entstehenden Nutzungsausfall betrachtet. Die Auswahl der Löschmethode (Raumlöschung oder Objektlöschung) ist vom zu löschenden System abhängig. So kann eine leistungsstarke USV, eine NEA oder eine Klimatisierungsanlage nicht mit einer Objektlöschung ausgerüstet werden.

10.2 Leckagemeldeanlagen

Beim Schutz von IT-Systemen und Komponenten der Haustechnik müssen neben der Leckage von Flüssigkeiten wie Frisch- und Abwasser Kühlmittel, Öle oder Hydraulikflüssigkeit aus Leitungen oder Anlagen betrachtet werden. In IT-Bereichen sowie in allen Bereichen der Haustechnik sollte auf druckbehaftete Leitungen verzichtet werden. Hochverfügbare IT-Bereiche sollten nicht unter Regenwassereinläufen oder Dehnungsfugen oder generell unter Flachdächern installiert werden.

Auch Kellerbereiche sind für die Raumwahl zum Betrieb hochverfügbarer Infrastrukturen meist nicht geeignet. Sowohl Rückstau aus der Abwasserentsorgung, als auch ein hoher Grundwasserspiegel sind als Gefahren zu beachten.

Eine ernste Gefahr in Bereichen, in denen hochverfügbare IT-Systeme betrieben werden, geht von Flüssigkeiten aus, die aus dem Außenbereich eindringen oder aus Lecks von Rohrleitungen (z. B. Wasser- oder Treibstoffversorgung) oder technischen Anlagen (z. B. Klimatisierungsanlagen) austreten. Falls eine Leckage nicht erkannt wird, können Flüssigkeiten den Betrieb durch Kurzschluss, Korrosion oder Kontaminierung unterbrechen. Ein ganzheitlicher Leckageschutz muss daher, ähnlich wie beim Brandschutz, aus konstruktiven und technischen Maßnahmen bestehen. Die technische Überwachung ist nur in der Lage, den Eintritt von Flüssigkeiten anzuzeigen, verhindern kann sie ihn nicht. Eine Leckagemeldeanlage zum Einsatz in IT-Bereichen besteht aus der zentralen Steuereinheit, der Überwachungseinheit und den Sensoren. Die Leckagemeldezentrale reagiert ähnlich wie andere Zentraleinheiten von Gefahrenmeldeanlagen auf die Signale der Überwachungseinheit und leitet einen Alarm an eine ständig besetzte Stelle.

Eine wirksame Überwachung muss sich sowohl auf die Flächen in den Betriebsräumen (Wände, Decke, Boden) als auch auf Objekte erstrecken, von denen eine Gefahr ausgehen kann, wie z. B. die Rohrleitungssysteme einer Klimatisierungsanlage. Daher reicht es nicht aus, nur den Rohboden zu überwachen. Eine Anlage ist so auszulegen, dass sie alle örtlich relevanten Flüssigkeiten erkennen kann. Die Detektion erfolgt zumeist mit Hilfe von Sensorkabeln, die in geeigneter Weise auf den zu überwachende Flächen oder Objekten angebracht werden. Die Sensoren nutzen für die Detektion von Flüssigkeiten den Effekt der Veränderung der Leitfähigkeit bei Berührung mit (leitfähigen) Flüssigkeiten. Die dadurch erzeugte Widerstandsänderung wird von der Überwachungs- und Steuereinheit erkannt und als Alarm weitergeleitet. Neben dem Erkennen von Flüssigkeiten ist die Standortbestimmung einer Leckage eine weitere wichtige Funktion. Besonders bei der Flüssigkeits-detektion ist das Erkennen der „Quelle“ umso wichtiger, weil diese an einer ganz anderen Stelle liegen kann als der Ort der Detektion. Besonders bei großen Flächen vergeht sonst viel Zeit für die Suche.

Die Anlagenzentrale sowie die Überwachungseinheiten müssen sabotagegeschützt installiert werden. Ebenso müssen Störungen, wie z. B. Sensordefekte, selbstständig erkannt werden und zu einer Störmeldung führen. Überlegungen zur Umsetzung weiterer Sicherheitsmaßnahmen, wie ein automatisches Schließen von Rohrleitungen von Versorgungsnetzen (Wasser, Heizöl etc.) oder das kontrollierte Herunterfahren (oder Umschalten) und Abschalten der Energieversorgung von Geräten, bei denen eine Leckage erkannt wird, sollten in die Planungen einer Leckageanlage einfließen.

10.3 Einbruchmeldeanlage/Überfallmeldeanlage

Einbruchmeldeanlagen (EMA) dienen der Überwachung von Bereichen gegenüber jeglichem Eindringen oder Sabotage, entweder kontinuierlich oder für den Zeitraum, in dem sie scharf geschaltet sind. Hierzu lassen sich zu überwachende Bereiche entweder einzeln oder gruppenweise in Scharfschaltbereiche einteilen. Jeder „Scharfschaltebereich“ kann für sich über geeignete Funktionseinheiten scharf oder unscharf geschaltet werden, z. B. über in einer Tür eingebaute Blockschlösser oder über elektronische Terminals. Der Einsatzzweck einer Einbruchmeldeanlage ist nicht die Verhinderung eines unberechtigten Eindringens, sondern dessen zuverlässige Detektion, die Weiterleitung und die Anzeige des Alarms an eine ständig besetzte Stelle. Eine EMA dient nur dem Zweck des Zeitgewinns bis zum Eingreifen durch Hilfe leistende Kräfte (z. B. Wachdienst, Polizei). Es muss sichergestellt sein, dass während der Zeit, die ein Einbrecher benötigt um ins

Gebäude einzudringen, der Einbruchsversuch so früh entdeckt wird, dass ein rechtzeitiges Eingreifen möglich ist. Eine robuste Ausstattung des Perimeterschutzes oder eines Gebäudes kann einen Einbruch nur verzögern, aber nicht verhindern. Selbst wenn alle Maßnahmen umgesetzt werden, können diese einen qualifizierten Einbrecher nicht länger als eine Stunde aufhalten, wenn er ungestört bleibt. Daher muss die Detektion eines Eindringens zuverlässig und umfassend erfolgen. Die EMA muss weiterhin sabotagegeschützt aufgebaut und mit einer ausfallsicheren Stromversorgung ausgestattet sein. Eine weitere wichtige Rolle spielt die zuverlässige Weiterleitung des Alarms und die Alarmanzeige. Die Norm DIN EN 50131 (DIN VDE 0830) beschreibt den fachgerechten Aufbau und formuliert Sicherheitsanforderungen an eine EMA. Demnach besteht eine EMA besteht grundsätzlich aus

- der Einbruchmeldezentrale,
- den Meldern,
- den Signalgebern,
- den Übertragungsanlagen,
- und der Energieversorgung.

Einbruchmeldeanlagen können in verschiedene Sicherheitsklassen gruppiert werden, die unterschiedliche Sicherheitsanforderungen an die Komponenten einer EMA stellen (z. B. Ausfallsicherheit, Überwindungssicherheit, Störanfälligkeit). Die VdS Schadenverhütung GmbH (VdS)definiert hierzu die folgenden Klassen:

- Einbruchmeldeanlagen der Klasse A verfügen über einen einfachen Schutz gegen Überwindungsversuche im scharfen sowie im unscharfen Zustand; die Melder verfügen über eine mittlere Ansprechempfindlichkeit.
- Einbruchmeldeanlagen der Klasse B verfügen über einen mittleren Schutz gegen Überwindungsversuche im scharfen sowie im unscharfen Zustand; die Melder verfügen über eine mittlere Ansprechempfindlichkeit.
- Einbruchmeldeanlagen der Klasse C verfügen über einen erhöhten Schutz gegen Überwindungsversuche im scharfen sowie im unscharfen Zustand; die Melder verfügen über eine erhöhte Ansprechempfindlichkeit. Eine weitgehende Überwachung der sicherheitsrelevanten Funktionen ist vorhanden.

Für die Überwachung von Bereichen mit hochverfügbaren IT-Systemen sind grundsätzlich Komponenten auszuwählen, die der VdS-Klasse C genügen und damit über eine gültige Zulassung verfügen. Darüber hinaus muss eine EMA in regelmäßigen Abständen gewartet und Personen bestimmt und geschult werden, welche die EMA scharf schalten sowie die Alarm- und Störmeldungen zurückstellen dürfen.

Die Überfallmeldeanlage (ÜMA) ist eine besondere Ausprägung der Gefahrenmeldeanlage und dient dem Melden eines Überfalls mit Hilfe eines auszulösenden verborgen angebrachten Überfallschalters. Überfallmeldeanlagen werden in Sicherheitsbereichen mit Publikumsverkehr, z. B Banken oder Geschäften, installiert. In hochverfügbaren Infrastrukturen kommen diese Anlagen allenfalls im Pförtnerbereich zum Einsatz und werden hier nicht näher betrachtet. Als weiterführende Literatur sei auf die Norm DIN VDE 0833 verwiesen.

10.3.1 Einbruchmeldezentrale

Ereignisse, die von den Meldern einer EMA erfasst werden, laufen in der Einbruchmeldezentrale (EMZ) auf. Diese Zentrale erfasst und wertet die Signale der Melder aus und generiert im Falle eines unbefugten Eindringens daraus eine Alarmmeldung, die über eine Schnittstelle weitergeleitet wird. Zu den weiteren Aufgaben gehören neben dem Erfassen und Verarbeiten auch die Protokollierung von Ereignissen und die Signalisierungen von Betriebsstörungen. Die EMZ als zentrale Komponente einer EMA muss ebenfalls sabotagegeschützt aufgebaut und in einem eigenen Scharfschaltbereich installiert werden. Neben der hohen Qualität der Melder zur Detektion von Ereignissen und einer sabotagesicheren Verkabelung aller Komponenten ist eine kontinuierliche Energieversorgung von entscheidender Bedeutung für einen zuverlässigen Betrieb. Hierzu ist die EMA an die redundant ausgelegte Energieversorgung eines Sicherheitsbereichs anzuschließen und darüber hinaus mit einer eigenen ausfallsicheren Stromversorgung (z. B. eigener USV) lokal auszustatten. Die Bedienung, also u. a. die Berechtigungseingaben, die Alarmquittierung, das Löschen von Alarmen oder Ereignisdaten muss ebenfalls über die EMZ möglich sein, jedoch nur nach vorheriger Identifizierung und Authentifizierung durch eine berechtigte Person.

10.3.2 Durchbruchüberwachung

Die Durchbruchüberwachung kann mit verschiedenen Melderarten erfolgen. Die bekannteste Methode basiert auf der Verwendung passiver Körperschallmelder. Diese Melder arbeiten nach dem Mikrofonprinzip und reagieren auf die charakteristischen Schallwellen, wie sie durch Angriffe mit Hammer und Meißel oder Bohrmaschine erzeugt werden. Trotz des Vorteils einer einfachen Überwachung großer Flächen überwiegt der Nachteil einer geringen Sicherheit gegenüber Fehlalarmen, die durch Geräusche aus angrenzenden Bereichen entstehen können. Auf den Einsatz von Körperschallmeldern sollte in hochverfügbaren Infrastrukturen daher verzichtet werden. Für die Überwachung großer Flächen bieten sich eher mäanderförmig aufgebrachte sogenannte Alarmdrähte an, die bei Beschädigung bei einem Durchbruchsversuch eine Meldung auszulösen. Der Alarmdraht muss durch eine vorgesetzte Schutzschicht (Metallplatte o. ä.) vor versehentlicher Beschädigung geschützt werden.

Für Glasflächen stehen verschiedene Arten der Durchbruchüberwachung zur Verfügung.

Am bekanntesten sind aktiv oder passiv arbeitende Glasbruchmelder. Aus zwei Gründen kommen sie für den Einsatz zu Schutz hochverfügbarer IT-Bereiche keinesfalls in Betracht. Zum einen sind sie relativ leicht zu überwinden und zum anderen werden sie immer innen auf einer Glasfläche montiert. Damit erkennen sie einen Angriff erst, wenn die weiter außen liegenden Schichten einer durchbruchhemmenden Verglasung überwunden sind, also viel zu spät.

Unabhängig von der Glasart kann eine Scheibe mit Hilfe einer Alarmdrahteinlage oder durch eine transparente Kunststofffolie mit Alarmdrähten überwacht werden. Wegen der sichtbaren Drähte wird die Variante aber ungern eingesetzt. Zum einen leidet der optische Eindruck der Verglasung. Zum anderen gibt es Möglichkeiten, Alarmdrähte so zu manipulieren, dass ein Durchbruch durch die Verglasung möglich wird.

Das derzeit einzig sinnvoll verwendbare Mittel einer Flächenüberwachung von Glas ist eine Fläche aus Einscheibensicherheitsglas (ESG) mit „Alarmspinne“. Einscheibensicherheitsglas wird bei der Herstellung so behandelt, dass es bei der kleinsten Verletzung über seine gesamte Fläche in tausende kleine Stücke zerspringt, man sagt, das Glas ist „vorgespannt“. Auf dieser ESG-Scheibe

wird innen eine mäanderförmige Leiterbahn aufgebracht, die beim Zerspringen der ESG-Scheibe ebenfalls zerstör wird und damit eine Meldung auslöst.

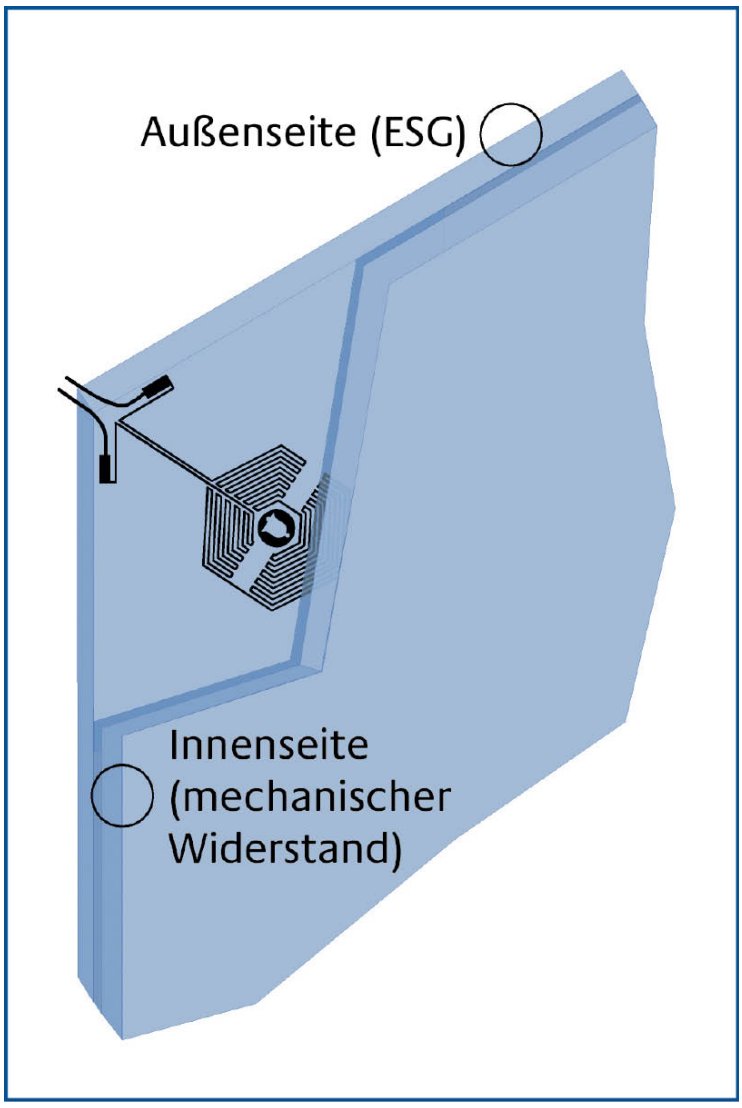


Abbildung 8: Aufbau einer Glasscheibe mit Alarmspinne

Die weiteren Schichten einer durchbruchhemmenden Verglasung folgen nach innen hin. Somit wird die Meldung sofort zu Beginn eines Angriffs ausgelöst und der komplette mechanische Widerstand kommt erst danach zum Tragen.

10.3.3 Überwachung von Verschluss und Verriegelung

Alle zu überwachende Öffnungen (Fenster, Türen etc.) müssen geschlossen und verriegelt sein. Geschlossene aber nicht verriegelte Türen und Fenster können von außen leicht geöffnet werden. Die Überwachung des Verschlusses erfolgt durch sabotagegeschützt angebrachte Magnetkontakte. Um die tatsächliche Verriegelung zu überwachen, wird bei Türschlössern im Schließblech ein mechanischer Schalter eingebaut, der durch den Riegel der Tür betätigt wird (Riegelkontakt). Bei Fenstern wird durch einen weiteren Kontakt die Verriegelungsstellung des Riegelwerkes oder des

Fenstergriffes überwacht. Moderne Riegelwerke bieten die Möglichkeit, Verschluss und Verriegelung gemeinsam mit einem Magnetkontakt zu überwachen.

10.3.4 Überwachung auf Bewegung

Die Bewegungsüberwachung erkennt Bewegungen von Personen innerhalb eines überwachten Bereiches. Der Einsatz von Bewegungsmeldern als Infrarot- oder Ultraschallmelder bietet sich für die Vorfeldüberwachung an. Hierbei wird das Vorfeld eines zu schützenden Bereichs auf unberechtigtes Eindringen überwacht und nicht das Innere des zu schützenden Bereichs selbst. Die für die Sicherheit zuständigen Kräfte erhalten nur so eine frühzeitige Alarmmeldung und können ein weiteres Eindringen verhindern.

Bei Dualmeldern ist innerhalb eines Meldergehäuses die Sensortechnik eines Infrarot- und eines Ultraschallmelders gemeinsam untergebracht. Durch die Kombination beider Techniken ist es möglich, die Meldesicherheit zu erhöhen oder die Falschmeldungsrate zu vermindern. Zudem verfügt ein Dualmelder über eine hohe Überwindungssicherheit, da ein Überwindungsversuch des einen Sensors vom anderen detektiert werden kann.

11 Zusammenfassung

Bei der Konzipierung von hochverfügbaren Infrastrukturen ist darauf zu achten, dass vor Beginn der Maßnahmenumsetzung ein individuelles und bedarfsorientiertes Gesamtkonzept erstellt wird. Die in diesem Dokument beschriebenen Strategien, Prinzipien und Maßnahmen zur Erreichung einer Hochverfügbarkeit dienen als Wegweiser bei der Planung. Der Erfolg zur Realisierung einer hochverfügbaren Infrastruktur hängt im Wesentlichen von einer ganzheitlichen Betrachtung der gegebenen Rahmenbedingungen ab.

Die wesentlichen Aspekte, die dabei zu beachten sind, ergeben sich aus den einzelnen Kapiteln und werden im Folgenden als Empfehlungen zusammengefasst.

Bei der Standortwahl wird empfohlen, Gebiete zu favorisieren die eine stabile geographische Lage aufweisen. Stabil bedeutet in diesem Zusammenhang die Meidung von Standorten von denen durch Elementareinflüsse (Flüsse, Bodensenkungen, Erosionen, Sturm, Blitz, starke Regenfälle etc.) Gefahren ausgehen könnten. Der Standort sollte zudem über eine optimale Infrastrukturanbindung verfügen. Zum Schutz vor Sabotage sollte der Standort sich in einer geschützten Lage befinden, die einem Angreifer kaum die Möglichkeit bietet, bei seinem Sabotageversuch unentdeckt zu bleiben. Auch wird empfohlen, die Umgebung (Nachbarbetriebe, technische Einrichtungen, Funktionsflächen) auf ihr Gefahrenpotential hin zu begutachten. Ein gut gewählter Standort erleichtert im weiteren Verlauf auch die Planung des Perimeterschutzes.

Ist der Standort gewählt und Risiken soweit wie möglich vermieden worden, sollte der unmittelbare Schutz des Perimeters geplant werden. Ziel des Perimeterschutzes ist es, Einbruchsversuche zu detektieren, zu melden und Angreifer so lange wie möglich vom Gebäude fernzuhalten. Hier wird empfohlen, das Umfeld genau zu analysieren, um das Angriffs- und Bedrohungspotential identifizieren zu können. Jedoch kann ein Perimeterschutz ein Vordringen bis an und ein Eindringen in das Gebäude nicht gänzlich verhindern. Ist der Eindringling im Gebäude gilt es, seine weiteren Übergriffe einzudämmen. Hauptaugenmerk hinsichtlich der Gebäudesicherheit sollte daher auf die Definition von Sicherheitszonen und den räumlichen Aufbau innerhalb des Gebäudes gelegt werden. Ein in sich schlüssiges und gut durchdachtes Konzept bei der Festlegung der Sicherheitszonen und der räumlichen Trennung von „kritischen“ und „unkritischen“ Bereichen im Innern des Gebäudes erhöht den Schutz vor äußeren und inneren Bedrohungen. Letztendlich bestimmt der Grad der Schutzbedürftigkeit der zu schützenden Objekte die räumliche Trennung und damit die erforderlichen Maßnahmen. Auch sind die Anforderungen an Außen- und Innenwände sowie Decken anhand des Bedrohungspotentials (Penetration, Feuer, Wasser) und der Schutzbedürftigkeit der in den Räumen befindlichen Komponenten festzulegen und in der Planung des Gebäudeausbaues zu berücksichtigen.

Bevor Maßnahmen zum wirksamen baulichen Brandschutz getroffen werden, wird empfohlen, eine ausführliche Beratung durch die örtliche Feuerwehr in Anspruch zu nehmen. Alle technischen Einrichtungen, die dem baulichen Brandschutz dienen sollen, z. B. Kabelschotts oder Türen im Zuge von Flucht- und Rettungswegen, bedürfen entweder einer Zulassung oder eines Eignungsnachweises.

Stabilität und Permanenz sind die wichtigsten Kriterien, die bei der elektrischen Versorgung beachtet werden sollten. Denn ohne deren Berücksichtigung ist es nicht einmal ansatzweise möglich, eine hochverfügbare Infrastruktur zu betreiben und somit die Verfügbarkeit von kritischen IT-Diensten zu garantieren. Dabei spielt die permanente Einspeisung der benötigten elektrischen Energie eine wichtige Rolle. Es wird eine doppelte Einspeisung empfohlen, die von zwei voneinander unabhängigen Versorgungssträngen erfolgt, die den Strom aus unterschiedlichen

Umspannwerken und über räumlich ausreichend weit voneinander entfernt verlegte Trassen beziehen. Die Stränge müssen die gleiche Leistung aufweisen und auf eigene Verteiler aufgelegt sein. Somit können gegenseitige Beeinträchtigungen vermieden werden. Um die Abhängigkeit von der Stromversorgung durch die EVU weiter zu minimieren, wäre eine Kombination aus externer und autarker Versorgung strategisch günstig. Bricht die externe Stromversorgung weg, weil z. B. Strommasten beschädigt sind und ist absehbar, dass die Versorgung in einem angemessenen Zeitraum nicht wieder zur Verfügung steht, kann dann durch autarke Ressourcen der Betrieb gewährleistet werden. Hierzu kann eine Kombination aus jeweils redundanter USV und NEA als Sekundärversorgung vorgesehen werden. Ein konsequenter Schritt in Richtung Unabhängigkeit vom öffentlichen Energieversorgungsnetz stellt die Errichtung einer autarken eigenen Versorgung mit elektrischer Energie z. B. mit Hilfe von Blockheizkraftwerken dar. Auch diese Anlagen müssen redundant aufgebaut sein, um Ausfälle durch technische Defekte oder Wartungsarbeiten zu vermeiden.

Als ein weiterer wichtiger Aspekt in einem Hochverfügbarkeits-Umfeld ist die Sicherstellung dauerhaft stabiler Werte der Umgebungstemperatur und Luftfeuchte, die mittels moderner Klimatisierungsanlagen realisiert werden kann. Für hochverfügbare Infrastrukturen empfehlen sich Klimasysteme nach den Prinzipien des eingehausten Kaltgangs oder der Direktkühlung. Die Gewährleistung der Umgebungsbedingungen bedeutet auch den Schutz der technischen Anlagen und sensiblen Bereiche vor unberechtigtem Zutritt. Hierbei wird ein rein mechanisches Schließsystem den erhöhten Sicherheitsanforderungen in einem Hochverfügbarkeits-Umfeld nicht gerecht. Es wird empfohlen, zur Durchsetzung der Zutrittskontrolle ein Zutrittskontrollsystem zu installieren. Die Identifikation Zutrittsberechtigter sollte mittels eines Tokens, beispielsweise in Form einer Chipkarte oder durch die Abfrage eines biometrischen Merkmales erfolgen. Bei Nutzung einer Token-basierenden Zutrittskontrolle lässt sich als weiteres Sicherheitsmerkmal die zusätzliche Abfrage einer PIN implementieren. Ergänzend zum Zutrittskontrollsystem sollte in einem Hochverfügbarkeits-Umfeld zur weiteren Überwachung schützenswerter Innen- und Außen-Bereiche Videokontrollanlagen installiert werden.

Bei der Gesamtbetrachtung der Maßnahmen zur Etablierung einer hochverfügbaren Infrastruktur ist neben deren Umsetzung zur Abwehr von Gefahren auch die Detektion und Meldung erforderlich. Hier gilt es, verlässliche Systeme zu installieren, um frühzeitig Gefahren, die durch Brände, Leckagen, Einbruch, Überfall oder Überspannung hervorgerufen werden, zu erkennen und zu melden, damit Gegenmaßnahmen schnellstmöglich eingeleitet werden können. Meldesysteme sind dort anzubringen, wo die körperliche Unversehrtheit und die Verfügbarkeit kritischer Systeme durch Auslösen eines Schadensereignisses stark gefährdet sind. Die Systeme sind nach ihrer Zielausrichtung (Detektion von Wasser, Feuer, Einbruch) durch qualifiziertes Personal zu installieren. Dies gilt auch für die Durchführung der regelmäßigen Wartung und Überwachung der Systeme. Bei der Installation der Systeme ist vor allem darauf zu achten, dass die Systeme einer angemessenen Sicherheitsklassifizierung entsprechen und keine Angriffspunkte für eine Sabotage oder Manipulation bieten. Auch sind die Meldesysteme mit redundanten Energiequellen auszustatten, damit die Betriebssicherheit garantiert werden kann.

Anhang: Verzeichnisse

Abkürzungsverzeichnis

Ein komplettes Verzeichnis hierzu findet sich im Band AH, Kapitel 5

Glossar

Ein komplettes Verzeichnis hierzu findet sich im Band AH, Kapitel 6

Literaturverzeichnis

Ein komplettes Verzeichnis hierzu findet sich im Band AH, Kapitel 7