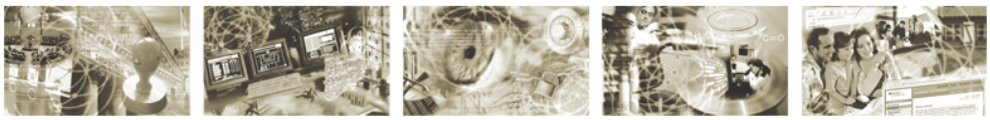
Bundesamt
für Sicherheit in der
Informationstechnik



Band M, Kapitel 11: Infrastruktur

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

Inhaltsverzeichnis

Tabellenverzeichnis

1 Infrastruktur

Die nachfolgenden Maßnahmenkataloge beschreiben Maßnahmen im Sinne von Verfahren und Lösungen für Gebäudeinfrastrukturen im Rahmen der Realisierung hoch verfügbarer IT-Architekturen. Die Zielsetzung der Maßnahmen liegt hierbei in weiten Teilen in der Gewährleistung der Robustheit sowie der weitestgehenden Vermeidung bzw. Reduzierung von Störeinflüssen zur Unterstützung der hoch verfügbar ausgelegten technischen und organisatorischen Funktionskomponenten des HV-Verbundes. Die Strukturierung der Maßnahmen erfolgt in Form von Maßnahmenclustern für die nachfolgenden Subdomänen der HV-Domäne „Infrastruktur“:

- Planung und Organisation
- Gebäude
- Räume
- Türen und Fenster
- Baulicher Brandschutz
- Energieversorgung
- Energieverteilung
- Blitz- und Überspannungsschutz
- Klimatisierung
- Zutrittskontrolle
- Brandmeldung und –Löschung
- Leckage
- Einbruchsmeldung

1.1 Planung und Organisation

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.1</td><td>
Vermeidung von Brandlasten
In IT-Betriebsräumen dürfen grundsätzlich keine „passiven“ Brandlasten wie Möbel, Akten, Papiervorräte, Putzmittel usw. gelagert werden.
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.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Robustheit</td><td>Reifegrad
KPI</td><td>Naturkatastrophen
Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)
CobiT, DS12
GSK M 1.51</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>VM.11.2</td><td colspan="5">Ausweichrechenzentrum (Hot site)
Aufbau und Einsatz eines geografisch separierten Ausweichrechenzentrums. Wenn die Anforderungen sehr hoch sind, muss ein Ausweichrechenzentrum an einem anderen Ort ständig einsatzbereit sein. In diesem Fall werden die gesamten Daten zeitgleich in das Ausweichrechenzentrum gespiegelt.</td></tr>
<tr><td></td><td>Umsetzungsphase</td><td>Prinzip</td><td>Kriterien</td><td>wirkt gegen</td><td>Querverweis</td></tr>
<tr><td></td><td>Planung und Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Redundanz
Separation
Automatismen</td><td>SpoF
Aktivierung
Aktivierungszeit
Automatisierungsgrad
Geographisch
Reifegrad</td><td>Naturkatastrophen
Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Server)
CobiT, DS12</td></tr>
</table>

Tabelle 1-1: Maßnahmenkatalog Infrastruktur:Planung und Organisation

1.2 Gebäude

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.3</td><td>
Geeignete Standorte für Gebäude
Die Sicherheitsanforderungen an den Standort müssen bereits bei der Konzeption berücksichtigt werden. Für die Auswahl eines Standorts steht vor allem die vollständige Umsetzbarkeit von Sicherheitsanforderungen im Vordergrund. Risiken, die von Elementarereignissen ausgehen, müssen identifizieren und bewerten werden. 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. Standort mit in der Nähe befindlichen Betriebe, Lagerstätten oder Transportwege mit Gefahrengut sowie Flughäfen, Sendeanlagen mit starker Sendeleistung, Kraftwerke oder militärische Einrichtungen sollten vermieden werden. Der Standort sollte über günstige Verkehrsanbindungen für Hilfe leistenden Kräfte (Feuerwehr, Polizei) verfügen.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Naturkatastrophen
Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)
CobiT, DS12
GSK M 1.16</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.4</td><td>
Einrichtung des Perimeterschutzes
Eine Strategie zur Etablierung eines effektiven Perimeterschutzes muss 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.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Sabotage
Manipulation</td><td>HVK (Infrastruktur)
GSK M 1.55</td></tr>
</table>
</td></tr>
<tr><td>VM.11.5</td><td>
Freilandschutz
Die Topologie der Freiflächen muss derart gestaltet werden, dass Sicht versperrende Objekte einem Täter nicht als Sichtschutz dienen können. Die Trennung des äußeren vom inneren Bereich des Freigeländes muss durch bedarfsorientierte Barrieresysteme wie Mauern, Zäune (massiv oder aus Drahtmetall), Stacheldrahthindernisse, Übersteigschutz, Fahrzeugbarrieren sowie der Sicherung von Zufahrten und Toren durch Drehtüren, Drehtore etc. realisiert werden. Zur Abwehr von Übergriffen und Erhöhung des Zeitwiderstandes müssen mechanische Barrieren zusätzlich mit elektronischen Detektionssystemen installiert werden
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Sabotage
Manipulation</td><td>HVK (Infrastruktur)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.6</td><td>
Perimeterbeleuchtung
Unmittelbar um das Gebäude befindlichen Freiräume (Vorfelder) müssen mit geeigneter Illumination versehen werden. Mittels Mastleuchten müssen das Vorfeld und die inneren Freiflächen ausgeleuchtet werden. Das Gebäude muss mit vertikal am Gebäude angebrachter Beleuchtung ausgeleuchtet werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Sabotage
Manipulation</td><td>HVK (Infrastruktur)</td></tr>
</table>
</td></tr>
<tr><td>VM.11.7</td><td>
Pförtner- und Wachdienst
Die Kontrolle der Zugänge und Zufahrten zum und im Betriebsgelände muss durch den Pförtner- und Wachdienst bewerkstelligt und abgedeckt werden. Der Pförtnerdienst identifiziert und registriert an zentraler Stelle Personen, die Zutritt zum Gelände oder Gebäude wünschen. Außerhalb der regulären Betriebszeiten müssen durch den Wach- oder Streifendienst Kontrollgänge über das Betriebsgelände durchgeführt werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)</td></tr>
</table>
</td></tr>
</table>

Nr.	*Maßnahmen*
VM.11.8	**Einrichtung und Anordnung von Funktionsbereichen in Gebäuden**

Funktionsbereiche müssen entsprechend der Ressourcenfunktionalität definiert und anhand ihrer Schutzbedürftigkeit angeordnet werden. Die Funktionstrennung muss durch Isolation und Separation innerhalb von Sicherheitszonen erfolgen. Die Isolation erfolgt durch Schottung von Räumen oder Bereichen gegenüber Gefahren, die von innen oder außen einwirken können. 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. 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 die Errichtung von Widerständen von Zone zu Zone, voneinander zu trennen.

Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
Planung Konzeption Beschaffung Implementierung	Robustheit Separation	Widerstandsklasse Reifegrad	Naturkatastrophen Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur)

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.9</td><td>
Geeigneter Hochbau
Das Gebäude muss über redundante konstruktive Eigenschaften und technische Einrichtungen verfügen, damit die erforderlichen Rahmenbedingungen zum sicheren Betrieb der IT-Infrastruktur dauerhaft konstant bleiben. Das Gebäude muss mit seiner Außenhaut Schutz gegen das Eindringen Unbefugter bieten. Gefahren wie Brände oder Explosionen in unmittelbarer Nähe des Gebäudes müssen wirksam durch die mechanischen Schutzmaßnahmen des Gebäudes abgewehrt werden. Die Außenwände müssen über eine hohe konstruktive Robustheit und hohen mechanischen Widerstand verfügen.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Redundanz
Separation
Robustheit</td><td>SpoF
Widerstandsklasse
HV-Infrastruktur
Reifegrad</td><td>Naturkatastrophen
Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)</td></tr>
</table>
</td></tr>
</table>

Tabelle 1-2: Maßnahmenkatalog Infrastruktur: Gebäude

1.3 Räume

Nr.	*Maßnahmen*				
VM.11.10	**Geeignete Decken und Wände** Decken und Wände in Gebäuden müssen hohe Widerstandswerte gegen mechanische und thermische Beanspruchung aufweisen. Hinsichtlich der mechanischen Belastbarkeit über die rein statischen Erfordernisse hinaus definiert die DIN V ENV 1627 bestimmte Wandkonstruktionen für den Einbau Einbruch hemmender Türen.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen Sabotage Manipulation	HVK (Infrastruktur)
VM.11.11	**Errichtung eines Raumes in einem bestehenden Raum** Es muss eine 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, realisiert werden. Diese Konstruktion verbindet eine einfache Installation mit einer hohen Robustheit gegenüber thermischer und mechanischer Belastung.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen Sabotage Manipulation	HVK (Infrastruktur)

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.12</td><td>
Keine abgehängten Decken verwenden
Alle Komponenten, die im Deckenbereich installiert sind, müssen mit Trägersystemen an der Rohdecke installiert werden und auf abgehängte Decken sollte gänzlich verzichtet werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Naturkatastrophen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)</td></tr>
</table>
</td></tr>
<tr><td>VM.11.13</td><td>
Vorkehrungen für Doppelböden
In Doppelböden sind besondere Sicherheitsvorkehrungen bei der Planung, Installation und vor allem während des Betriebs zu berücksichtigen. Es muss 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.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Sabotage
Manipulation</td><td>HVK (Infrastruktur)</td></tr>
</table>
</td></tr>
</table>

Tabelle 1-3: Maßnahmenkatalog Infrastruktur: Räume

1.4 Türen und Fenster

Nr.	*Maßnahmen*				
VM.11.14	**Einsatz Einbruch hemmende Türen** Zur Trennung von Sicherheits- oder Funktionsbereiche müssen Einbruch hemmende Türen gemäß der Norm DIN V/ EN V1627 einheitlichen Bauteilewiderstandsklassen von RC 1 bis RC6 eingesetzt werden. Darüber hinaus definiert die DIN V ENV 1627 in einer entsprechenden Tabelle für die einzelnen Widerstandklassen der Türen Wandqualitäten nach Dicke und verwenden Baustoffen.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen Sabotage Manipulation	HVK (Infrastruktur) GSK M 1.19
VM.11.15	**Verwendung geeigneter Fenster und Verglasung** Fenster und Verglasung müssen gemäß der Norm DIN V/ EN V1627 einheitlichen Bauteilewiderstandsklassen von RC 1 bis RC6 eingesetzt werden. Die Fenster müssen fest verglast sein, so dass ein Öffnen und damit ein versehentliches Offenstehen verhindert wird.				
	Umsetzungsphase	Prinzip	Kriterien	wirkt gegen	Querverweis
	Planung Konzeption Beschaffung Implementierung	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen Sabotage Manipulation	HVK (Infrastruktur) GSK M 1.19

Tabelle 1-4: Maßnahmenkatalog Infrastruktur: Türen und Fenster

1.5 Baulicher Brandschutz

<table>
<tr><th>Nr.</th><th colspan="5">Maßnahmen</th></tr>
<tr><td rowspan="3">VM.11.16</td><td colspan="5">Einsatz von Brandschutztüren/Rauchschutztüren
Es müssen Brandschutz- oder Rauchschutztüren zum Schutz der Personen und IT-Systeme eingesetzt werden. Brandschutz- oder Rauchschutztüren müssen in vielen Fällen die Funktionen des Einbruchschutzes und des Brandschutzes zum Schutz der IT-Systeme mit dem Personenschutz vereinen. Dazu sind elektrische Systeme einzusetzen, die eine optimale Synthese zwischen den Belangen des Personenschutzes und dem Schutz der IT gegen unberechtigten Zutritt ermöglichen.</td></tr>
<tr><td>Umsetzungsphase</td><td>Prinzip</td><td>Kriterien</td><td>wirkt gegen</td><td>Querverweis</td></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Naturkatastrophen
Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)
GSK M 1.50</td></tr>
</table>

<table>
<tr><th>Nr.</th><th colspan="5">Maßnahmen</th></tr>
<tr><td>VM.11.17</td><td colspan="5">Einrichtung von Brandabschnitten
Ein Gebäude muss in Brandabschnitte aufgeteilt werden. Die Aufteilung von Brandabschnitten orientiert sich im Wesentlichen an der Größe eines Gebäudes und an den Fluchtwegen. Zulässige Größen von Brandabschnitten darf in der Regel 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 laufende Brandabschnitte entsprechend zu sichern. Einzelne Brandabschnitte werden durch Brandschutzkonstruktionen (gemäß DIN 4102) voneinander getrennt.</td></tr>
<tr><td></td><td>Umsetzungsphase</td><td>Prinzip</td><td>Kriterien</td><td>wirkt gegen</td><td>Querverweis</td></tr>
<tr><td></td><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Naturkatastrophen
Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)
GSK M 1.47</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.18</td><td>
Einrichtung einer Brandschottung
Bei der Verlegung von Kabeln durch Brandwände sowie innerhalb von Räumen ist eine geeignete Schottung zwingend erforderlich. 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. 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.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Naturkatastrophen
Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)
GSK M 1.9</td></tr>
</table>
</td></tr>
</table>

Tabelle 1-5: Maßnahmenkatalog Infrastruktur: Baulicher Brandschut

1.6 Energieversorgung

Nr.	*Maßnahmen*				
VM.11.19	**Doppelte Einspeisung der Energieversorgung** Die Verlegung der Anbindung an das EVU in Außentrassen muss mit zwei unabhängigen Kabeln in einer Zwei-Wege-Führung in voneinander getrennten Trassen und an unterschiedlichen Stellen in das Gebäude erfolgen. Die Einspeisungen sollten aus unterschiedlichen Umspannwerken und über räumlich ausreichend weit voneinander entfernt verlegte Trassen erfolgen.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Redundanz Separation	SpoF Aktivierung Aktivierungszeit Automatisierungsgrad Geographisch Reifegrad	Naturkatastrophen Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur)

Nr.	*Maßnahmen*
VM.11.20	**Mittelspannungseinspeisung** Es sollte die Mittelspannungseinspeisung gegenüber einer Niederspannungseinspeisung bevorzugt werden. 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. 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.

Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur)

Nr.	*Maßnahmen*				
VM.11.21	**Autarke Energieversorgung** Einsatz von autarken Energieversorgungseinrichtungen in Form von Blockheizkraftwerken (BHKW). Es 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.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit Autonomie Skalierbarkeit	Widerstandsklasse Systemautonomie Auslastung Skalierungsfaktor Modularisierung Reifegrad	Naturkatastrophen Menschliches Versagen Sabotage Manipulation Technische Ermüdung	HVK (Infrastruktur) CobiT DS4 CobiT DS12

Nr.	*Maßnahmen*				
VM.11.22	**Unterbrechungsfreie Stromversorgung (USV)** Es muss eine unterbrechungsfreie so genannte Voltage and Frequency Independent-Stromversorgung (VFI-USV) mit ausreichender Kapazität installiert werden. 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.				
	Umsetzungsphase	Prinzip	Kriterien	wirkt gegen	Querverweis
	Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Redundanz Automatismen	SpoF Aktivierung Aktivierungszeit Automatisierungsgrad Reifegrad	Naturkatastrophen Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur) GSK M 1.28

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.23</td><td>
Netzersatzanlage (NEA)
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.
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.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Redundanz</td><td>SpoF
Aktivierung
Aktivierungszeit
Reifegrad</td><td>Naturkatastrophen
Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)
GSK M 1.56</td></tr>
</table>
</td></tr>
</table>

Tabelle 1-6: Maßnahmenkatalog Infrastruktur: Energieversorgung

1.7 Energieverteilung

Nr.	*Maßnahmen*				
VM.11.24	**Niederspannungshauptverteilung (NSHV), Unterverteilungen** Die Verteilung muss 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. 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.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur)

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.25</td><td>
Energieverteilung als TN-S Netz
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.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)</td></tr>
</table>
</td></tr>
<tr><td>VM.11.26</td><td>
Differenzstrom-Überwachung durch Residual Current Monitor (RCM)
Einsatz einer Differenzstrom-Überwachung durch Residual Current Monitor (RCM), die bei Erreichen des Nennfehlerstroms nicht durch sofortiges Abschalten zu reagieren. RCM 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 RCM muss sich auf alle stromführenden Phasen L1, L2, L3 und N sowie separat auf den PE-Leiter erstrecken.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Betrieb
Notfallvorsorge</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)</td></tr>
</table>
</td></tr>
</table>

Nr.	*Maßnahmen*				
VM.11.27	**Regelmäßige Prüfung und fachgerechte Wartung der Verkabelung** Eine regelmäßige Prüfung und fachgerechte Wartung der Verkabelung und aller elektronischen Komponenten ist vorzusehen und kann durch eine ständige technische Überwachung nicht ersetzt werden.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Betrieb Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur)

Nr.	*Maßnahmen*
VM.11.28	**Kabelinstallation** 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.

Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
Planung Konzeption Beschaffung Betrieb Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur)

Nr.	*Maßnahmen*
VM.11.29	**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. Bei der Verlegung von Kabeln im Doppelboden ist 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.

Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur) Fehler: Referenz nicht gefunden

Nr.	*Maßnahmen*				
VM.11.30	**Kabeltrassen** Generell sollten Kabel auf Trassen im offenen Deckenbereich geführt und an der Rohdecke installiert werden. Kabel sind generell zu schützen. 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, müssen Kabeltrassen an Übergängen oder Querungen von verschiedenen Brandabschnitten geschottet werden.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur)

Nr.	*Maßnahmen*				
VM.11.31	**Kabel** Es sollten Kabel in halogenfreier Ausführung gewählt werden und ein Funktionserhalt von mindestens 90 Minuten gegenüber Brand aufweisen.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen	HVK (Infrastruktur) Fehler: Referenz nicht gefunden

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.32</td><td>
Regelmäßige Kontrolle der Kabeltrassennkapazität 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

Kabeltrassen müssen regelmäßig kontrolliert werden. 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 Üb 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.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Naturkatastrophen
Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)</td></tr>
</table>
</td></tr>
</table>

Nr.	*Maßnahmen*				
VM.11.33	**Steigtrassen** Die Verkabelung sollte in durchgängigen, als eigener Brandabschnitt ausgeführten, Steigetrassen installiert werden. 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.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur)

Tabelle 1-7: Maßnahmenkatalog Infrastruktur: Energieverteilung

1.8 Blitz- und Überspannungsschutz

Nr.	*Maßnahmen*				
VM.11.34	**Blitz- und Überspannungskonzept** Ein Blitz- und Überspannungskonzept zur Sicherung von IT-Systemen gemäß DIN EN 62305-1 bis -4 muss von ausgewiesenen Fachleuten erarbeitet und umgesetzt werden. Bereiche, in denen hochverfügbare IT-Systeme betrieben werden, müssen 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.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**

Nr.	*Maßnahmen*				
	Planung Konzeption Beschaffung Implementierung Betrieb Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen	HVK (Infrastruktur) CobiT, DS12
VM.11.35	**Überprüfung der Blitz- und Überspannungsschutzmaßnahmen** 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.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Betrieb Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen Menschliches Versagen Fehler in Hard- oder Software	HVK (Infrastruktur) GSK M 1.25

Tabelle 1-8: Maßnahmenkatalog Infrastruktur: Blitz- und Überspannungsschutz

1.9 Klimatisierung

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.36</td><td>
Sicherheitsvorkehrungen für die Klimatisierung
Unabhängig davon, ob die Direktkühlung oder der gehauste Kaltkanal als Klimatisierungsprinzip in hochverfügbaren Infrastrukturen zum Einsatz kommt, muss der Kühlkreislauf immer redundant ausgelegt sein. Die Bedienung der automatischen Klimaregelung darf nur durch berechtigtes und geschultes Personal erfolgen. Auf die Steuerung und Überwachung der Klimatisierungsanlage über eine Fernwartungseinrichtung sollte verzichtet werden. Die Raumlufttemperatur und -feuchtigkeit sollten unabhängig voneinander einstellbar sein. Die von der VDI-Richtlinie 2054 vorgeschriebenen Grenzwerte für die klimatischen Bedingungen der Raumluft in Technikräumen können für einen sicheren und effizienten Betrieb herangezogen werden. Für die Außeneinheit einer Klimatisierungsanlage auf dem Dach oder an der Außenwand eines Gebäudes ist auf eine fachgerechte Montage hinsichtlich des Blitz- und Überspannungsschutzes der Energieversorgung zu achten. Alle Kabel- und Leitungszuführungen der Klimatisierungsanlagen müssen vor Manipulationen und Brand geschützt sowie 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 zum Installationsort der Außeneinheit ist zu kontrollieren und zu überwachen. Ein Erreichen der Außeneinheit der Klimatisierungsanlage mit Hilfe von Steighilfen oder mittels technischer Hilfsmittel der Gebäudetechnik (Servicekran, Leiter, außen liegender Fluchtweg etc.) darf nicht möglich sein.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Betrieb
Notfallvorsorge</td><td>Robustheit
Redundanz
Automatismen</td><td>Widerstandsklasse
SpoF
Aktivierung
Aktivierungszeit
Automatisierungsgrad
Reifegrad</td><td>Naturkatastrophen
Menschliches Versagen
Sabotage
Manipulation
Fehler in Hard- oder Software</td><td>HVK (Infrastruktur)
CobiT, DS12
GSK M 1.27</td></tr>
</table>
</td></tr>
</table>

Tabelle 1-9: Maßnahmenkatalog Infrastruktur: Klimatisierung

1.10 Zutrittskontrolle

Nr.	*Maßnahmen*				
VM.11.37	**Zutrittskontrollsystems (ZKS)** 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).				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung Betrieb	Robustheit	Widerstandsklasse Reifegrad	Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur) CobiT DS12

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.38</td><td>
Funktionen für die Zutrittskontrolle
Für die Zutrittskontrolle in hochverfügbaren Infrastrukturen sollten für besonders schützenswerte Bereiche Funktionen wie:
Zutrittswiederholkontrolle (Anti-Pass-Back), Zwei-Personen-Zutrittskontrolle (Vier-Augen-Prinzip), Mehr-Personen-Anwesenheits-kontrolle (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), umgesetzt werden. Die Einrichtung einer Nötigungs-PIN sollte erwogen werden, wenn die Gefahr von Überfällen besteht. Es ist bei der Planung der Zutrittsberechtigungen für jeden Raum oder Bereich zu entscheiden, wie mechanische Zwangsläufigkeiten umzusetzen sind
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Betrieb</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)
1.10</td></tr>
</table>
</td></tr>
<tr><td>VM.11.39</td><td>
Sicherung der Übergeordnete Zutrittskontrollzentrale (ÜZKZ) und der Bedienungs- und/oder Anzeigeeinheiten (BAE)
Die ÜZKZ und BAE zur Administration müssen in einem zutrittsgeschützten Raum mit der Überwachung durch die Einbruchmeldeanlage installiert sein. Die BAE sollte darüber hinaus mit einem Zugangschutz ausgestattet sein, damit eine Administration der ÜZKZ nur von berechtigtem Personal erfolgen kann.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Betrieb</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)
1.10</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.40</td><td>
Sicherung der Zutrittskontrollzentrale (ZKZ)
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. Die ZKZ muss 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.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Betrieb</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)
1.10</td></tr>
</table>
</td></tr>
<tr><td>VM.11.41</td><td>
Sicherung des Türsteuermoduls
Das Türsteuermodul muss sabotagegeschützt im zutrittskontrollierten und überwachten Bereich installiert sein. Die in den Türen verbauten Motorschlösser oder Türöffner müssen mindestens der Widerstandsklasse der Tür entsprechen. Insbesondere muss auf die sabotagegeschützte Verlegung der Verkabelung sowie der Meldesensoren geachtet werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Betrieb</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.42</td><td>
Identifizierung und Authentifizierung in einem ZKS
Neben der Identifikation über den Besitz eines Tokens muss die zusätzliche Eingabe einer mehrstelligen PIN oder die Abfrage eines biometrischen Merkmals erfolgen. Neben der Identifizierung, also dem Besitz eines Ausweises (Tokens), ist insbesondere für die Kontrolle von hochverfügbaren Infrastrukturen auch die Authentifizierung (Echtheitsprüfung) des Ausweises notwendig.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Betrieb</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Menschliches Versagen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)
1.10</td></tr>
</table>
</td></tr>
<tr><td>VM.11.43</td><td>
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.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Sabotage
Manipulation</td><td>HVK (Infrastruktur)</td></tr>
</table>
</td></tr>
</table>

Tabelle 1-10: Maßnahmenkatalog Infrastruktur: Zutrittskontrolle

1.11 Brandmeldung und Löschung

Nr.	*Maßnahmen*
VM.11.44	**Brandmeldezentrale (BMZ)** Die zentrale Komponente jeder Brandmeldeanlage ist die Brandmeldezentrale. Hier laufen die Meldungen aller Melder zusammen und werden ausgewertet. Aus den Meldungen leitet die BMZ unterschiedliche Reaktionen ab. In erster Linie wird eine Brandmeldung an eine Hilfe leistende Stelle 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 wird 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.

Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen Sabotage Manipulation	HVK (Infrastruktur)

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.45</td><td>
Brandmelder
Die Detektion von Feuer, Schwelbrand oder Rauch erfolgt durch an die BMZ angeschlossenen automatischen Melder.
Die Melder sollten einer regelmäßigen und fachgerechten Wartung unterzogen werden.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Naturkatastrophen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)
1.11</td></tr>
</table>
</td></tr>
<tr><td>VM.11.46</td><td>
Brandfrühesterkennung
Die Detektion von Bränden sollte durch eine 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.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Naturkatastrophen
Sabotage
Manipulation</td><td>HVK (Infrastruktur)
1.11</td></tr>
</table>
</td></tr>
</table>

Nr.	*Maßnahmen*
VM.11.47	**Bereichslöschung** Die Brandbekämpfung muss mittels einer automatischen Löschanlage erfolgen. 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.

Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur)

Nr.	*Maßnahmen*				
VM.11.48	**Objektlöschung** 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.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur)

Tabelle 1-11: Maßnahmenkatalog Infrastruktur: Brandmeldung und Löschung

1.12 Leckage

Nr.	*Maßnahmen*				
VM.11.49	**Leckagevermeidung** In IT-Bereichen sowie in allen Bereichen der Haustechnik, sollte soweit möglich 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.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**

Nr.	*Maßnahmen*				
	Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Naturkatastrophen Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur)
VM.11.50	**Leckagemeldung** Eine Leckagemeldeanlage zum Einsatz in IT-Bereichen besteht aus der zentralen Steuereinheit, der Überwachungseinheit und den Sensoren. Die Leckagemeldezentrale reagiert 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. Neben dem Erkennen von Flüssigkeiten ist die Standortbestimmung einer Leckage eine weitere wichtige Funktion. 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.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Menschliches Versagen Sabotage Manipulation	HVK (Infrastruktur)

Tabelle 1-12: Maßnahmenkatalog Infrastruktur: Leckage

1.13 Einbruchmeldung

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.51</td><td>
Einbruchmeldeanlagen (EMA)
Einbruchmeldeanlagen dienen der Überwachung von Bereichen gegenüber jeglichem Eindringen oder Sabotage, entweder kontinuierlich oder für den Zeitraum, in dem sie scharfgeschaltet sind. 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. Die Detektion eines Eindringens muss 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.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung
Notfallvorsorge</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Sabotage
Manipulation</td><td>HVK (Infrastruktur)
CobiT, DS12</td></tr>
</table>
</td></tr>
<tr><td>VM.11.52</td><td>
Einbruchmeldezentrale (EMZ)
Ereignisse, die von den Meldern einer EMA erfasst werden, laufen in der Einbruchmeldezentrale 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. 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.
</td></tr>
</table>

Nr.	*Maßnahmen*				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Sabotage Manipulation	HVK (Infrastruktur) 1.13
VM.11.53	**Durchbruchüberwachung** Für die Überwachung großer Flächen bieten sich eher mäanderförmig aufgebrachte Alarmdrähte an, die bei Beschädigung bei einem Durchbruchsversuch eine Meldung auszulösen. Für Glasflächen sind verschiedene Arten der Durchbruchüberwachung verfügbar. Verbundsicherheitsglas wird mit Hilfe einer Alarmdrahteinlage oder durch eine transparente Kunststofffolie mit Alarmdrähten überwacht. Bei Einscheibensicherheitsglas ist auf einer vorgespannten Glasschicht eine Leiterbahn als „Alarmspinne“ aufgebrannt.				
	Umsetzungsphase	**Prinzip**	**Kriterien**	**wirkt gegen**	**Querverweis**
	Planung Konzeption Beschaffung Implementierung Notfallvorsorge	Robustheit	Widerstandsklasse Reifegrad	Sabotage Manipulation	HVK (Infrastruktur) 1.13

<table>
<tr><th>Nr.</th><th>Maßnahmen</th></tr>
<tr><td>VM.11.54</td><td>
Überwachung von Verschluss und Verriegelung
Der Verschluss und die Verriegelung alle Öffnungen (Fenster, Türen etc.) müssen überwacht 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.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Sabotage
Manipulation</td><td>HVK (Infrastruktur)
1.13</td></tr>
</table>
</td></tr>
<tr><td>VM.11.55</td><td>
Bewegungsüberwachung
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.
<table>
<tr><th>Umsetzungsphase</th><th>Prinzip</th><th>Kriterien</th><th>wirkt gegen</th><th>Querverweis</th></tr>
<tr><td>Planung
Konzeption
Beschaffung
Implementierung</td><td>Robustheit</td><td>Widerstandsklasse
Reifegrad</td><td>Sabotage
Manipulation</td><td>HVK (Infrastruktur)
1.13</td></tr>
</table>
</td></tr>
</table>

Tabelle 1-13: Maßnahmenkatalog Infrastruktur: Einbruchmeldung