|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Rechenzentrum"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300057 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc83654193)

[Dokumentenhistorie 3](#_Toc83654194)

[Inhaltsverzeichnis 4](#_Toc83654195)

[Allgemeine Festlegungen 5](#_Toc83654196)

[Ziel / Zweck 5](#_Toc83654197)

[Geltungsbereich 6](#_Toc83654198)

[Zuständigkeiten 6](#_Toc83654199)

[Genehmigungs- und Änderungsverfahren 6](#_Toc83654200)

[Aufbau des Dokuments 6](#_Toc83654201)

[Sicherheitsrichtlinie „Rechenzentrum bzw. Serverraum" 8](#_Toc83654202)

[Basismaßnahmen 8](#_Toc83654203)

[Allgemeines Gebäude 8](#_Toc83654204)

[Rechenzentrum sowie Serverraum 9](#_Toc83654205)

[Standardmaßnahmen 13](#_Toc83654206)

[Allgemeines Gebäude 13](#_Toc83654207)

[Rechenzentrum sowie Serverraum 14](#_Toc83654208)

[Maßnahmen bei erhöhtem Schutzbedarf 16](#_Toc83654209)

[Allgemeines Gebäude 17](#_Toc83654210)

[Rechenzentrum sowie Serverraum 18](#_Toc83654211)

# Allgemeine Festlegungen

## Ziel / Zweck

Ein Rechenzentrum ist innerhalb der <Institution> wie folgt definiert:

* Wird die IT der <Institution> innerhalb eines Gebäudes oder einer Liegenschaft verteilt in mehreren Bereichen betrieben und sind diese Bereiche untereinander und zu den IT-Benutzern hin durch hauseigene LAN-Verbindungen angeschlossen, ist mindestens der funktional bedeutendste dieser Bereiche als Rechenzentrum zu behandeln. Des Weiteren sind Bereiche, von deren ordnungsgemäßem Betrieb 50 % und mehr Nutzer abhängig sind oder aus denen heraus 50 % und mehr an Diensten und Daten (gemessen an der Gesamtheit der Bereiche) bereitgestellt werden, als Rechenzentrum zu behandeln.
* Hat die <Institution> nur einen zentralen IT-Betriebsbereich, ist dieser gemeinsam mit den erforderlichen Supportbereichen grundsätzlich immer wie ein Rechenzentrum entsprechend dem Schutzbedarf zu behandeln. Unter „IT-Betriebsbereich“ sind Räume zu verstehen, in denen die Hardware aufgebaut ist und betrieben wird, die der Bereitstellung von Diensten und Daten dient. Das Rechenzentrum umfasst neben dem IT-Betriebsbereich alle weiteren technischen Supportbereiche (z. B. Stromversorgung, Kälteversorgung, Löschtechnik, Sicherheitstechnik), die dem bestimmungsgemäßen Betrieb und der Sicherheit dienen.
* Ist die IT der <Institution> an mehreren räumlich voneinander getrennten Standorten angesiedelt und sind diese durch andere als hauseigene LAN-Verbindungen miteinander gekoppelt, ist jeder der Standorte entsprechend separat zu betrachten und zu behandeln.
* Ein IT-Betriebsbereich, in dem für kritische Geschäftsprozesse (Prozesse, deren Störung oder Ausfall zu wesentlichen Beeinträchtigungen der Erledigung primärer Aufgaben führen) erforderliche IT angesiedelt ist, ist immer als Rechenzentrum zu behandeln, unabhängig von Größe.
* IT-Betriebsbereiche, aus denen heraus Dienste oder Dienstleistungen für Dritte erbracht werden, sind immer als Teil eines Rechenzentrums zu betrachten. Dabei ist es unerheblich, ob dies gegen Entgelt erfolgt oder nicht.
* Besteht ein begründetes Interesse, einen IT-Betriebsbereich gemeinsam mit seinem Supportbereich abweichend von den vorgenannten Regelungen als Serverraum zu behandeln, ist dies samt den sich daraus ergebenden Reduzierungen von Sicherheitsanforderungen zu begründen.

Weicht ein Rechenzentrum von dieser Definition ab, wird der betrachtete IT-Betriebsbereich als Serverraum bezeichnet. Diese Definition orientiert sich ausschließlich an der Bedeutung der IT-Struktur für die Aufgabenerfüllung der <Institution> und steht damit im methodischen Einklang mit der DIN EN 50600.

Soll ein Serverraum abgesichert werden, können die Anforderungen dieser Sicherheitsrichtlinie entsprechend reduziert werden. Dies muss jedoch stichhaltig und nachvollziehbar begründet werden und es müssen mindestens die Basis-Anforderungen umgesetzt werden.

Ziel dieser Sicherheitsrichtlinie ist es zu beschreiben, welche Anforderungen zu erfüllen sind, um ein Rechenzentrum aus Sicht der Informationssicherheit optimal zu nutzen. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines INF.1 „Allgemeines Gebäude" und INF.2 „Rechenzentrum“ zurückgegriffen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „Rechenzentrum bzw. Serverraum“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Rechenzentrum bzw. Serverraum"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Allgemeines Gebäude

#### Planung der Gebäudeabsicherung (INF.1.A1)

Das System der Einbruchhemmung muss wie eine Kette wirken und ist nur so gut wie das schwächste Glied. Aus diesem Grunde muss die Einbruchshemmung bereits bei der Gebäudeplanung beginnen. Unter Berücksichtigung der innerhalb des Rechenzentrums betriebenen Services und deren Schutzbedürfnisse (Verfügbarkeit, Vertraulichkeit und Integrität) muss von den Verantwortlichen für die Planung der Gebäudeabsicherung festgelegt werden, wie dieses unter Anwendung der internen und gesetzlichen Vorgaben abzusichern ist.

#### Angepasste Aufteilung der Stromkreise (INF.1.A2)

Es muss regelmäßig überprüft werden, ob die Absicherung und Auslegung der Stromkreise noch den tatsächlichen Bedürfnissen des Rechenzentrumsbetriebes genügen. Bei der Absicherung und Auslegung der Stromkreise muss ebenfalls der voraussichtliche Bedarf für die nächsten zwei Jahre mit einfließen.

#### Einhaltung von Brandschutzvorschriften (INF.1.A3)

Die bestehenden Brandschutzvorschriften sowie die Auflagen der Bauaufsicht müssen von der <Institution> als Betreiber des Rechenzentrums bzw. vom Vermieter des Gebäudes eingehalten werden. Die Fluchtwege müssen vorschriftsmäßig ausgeschildert und freigehalten werden. Bei der Brandschutzplanung sollte die örtliche Feuerwehr hinzugezogen werden. Es muss ein IT-bezogenes Brandschutzkonzept erstellt und umgesetzt werden, dass die fehlenden IT bezogenen Anforderungen aus der Bauordnung zum Brandschutz enthält.

Unnötige Brandlasten müssen vermieden werden.

Es muss eine Brandschutzbeauftragte bzw. einen Brandschutzbeauftragten oder eine mit dem Aufgabengebiet betraute und geschulte Person benannt sein.

Branderkennung in Gebäuden (INF.1.A4)

Das Rechenzentrum muss mit einer ausreichenden Anzahl von Rauchmeldern und einer Brandmeldezentrale (BMZ) ausgestattet sein. Alle Rauchmelder müssen auf der MBZ aufgeschaltet sind. Zusätzlich muss eine Alarmierung bei erkanntem Rauch im Rechenzentrum ausgelöst werden. Die Funktionsfähigkeit aller Rauchmelder bzw. aller Komponenten einer Brandmeldeanlage müssen regelmäßig überprüft werden. Ebenfalls muss regelmäßig kontrolliert werden, dass die Fluchtwege benutzbar und frei von Hindernissen sind, damit das Rechenzentrum in einer Gefahrensituation schnell geräumt werden kann.

Handfeuerlöscher (INF.1.A5)

Zur Sofortbekämpfung von Bränden müssen Handfeuerlöscher in der jeweils geeigneten Brandklasse (DIN EN 3 Tragbare Feuerlöscher) in ausreichender Zahl und Größe im Rechenzentrum zur Verfügung stehen. Die Handfeuerlöscher müssen regelmäßig geprüft und gewartet werden. Die Mitarbeitenden sollten im Rahmen von Brandbekämpfungsschulungen in die Benutzung der Handfeuerlöscher eingewiesen werden.

#### Geschlossene Fenster und Türen (INF.1.A6)

Im Rechenzentrum müssen Fenster und Türen geschlossen werden. Dafür muss eine entsprechende Anweisung erlassen werden. Es muss regelmäßig überprüft werden, ob die Fenster und Türen verschlossen sind. Brand- und Rauchschutztüren dürfen unter Berücksichtigung der Implementierungsart nicht dauerhaft offengehalten werden bzw. müssen bei Erkennung eines Brandes automatisch sich schließen.

#### Zutrittsregelung und -kontrolle (INF.1.A7)

Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen muss geregelt und kontrolliert werden. Die Zahl der zutrittsberechtigten Personen muss für jeden Bereich auf ein Mindestmaß reduziert werden. Weitere Personen dürfen erst Zutritt erhalten, nachdem geprüft wurde, ob dies notwendig ist. Alle erteilten Zutrittsberechtigungen müssen dokumentiert werden. Die Zutrittskontrollmaßnahmen müssen regelmäßig auf ihre Wirksamkeit überprüft werden.

#### Rauchverbot (INF.1.A8)

In den Räumen des Rechenzentrums muss ein striktes Rauchverbot gelten.

### Rechenzentrum sowie Serverraum

#### Festlegung von Anforderungen (INF.2.A1)

Für das Rechenzentrum bzw. einem Verbund aus mehreren Rechenzentren müssen angemessene technische und organisatorische Vorgaben definiert und umgesetzt.

Bei der Planung des Rechenzentrums oder der Auswahl geeigneter Räumlichkeiten muss eine Berücksichtigung potenzieller Gefährdungen durch Umgebungseinflüsse sowie des Sicherheitsniveaus der Geschäftsprozesse, IT-Komponenten (insbesondere Verfügbarkeit) erfolgen. Weiterhin sollten auch Schutzmaßnahmen vor potenziellen internen und externen Angriffen in die Gesamtbetrachtung einfließen.

Ein Rechenzentrum muss insgesamt als geschlossener Sicherheitsbereich konzipiert werden. Zudem müssen unterschiedliche Sicherheitszonen für ein Rechenzentrum geplant werden. Hierfür sollten Verwaltungs-, Logistik-, Technik- und IT-Flächen klar voneinander getrennt werden. Im Falle eines Serverraums sollte geprüft, ob unterschiedliche Sicherheitszonen umsetzbar sind.

Ebenso muss darauf geachtet werden, dass Versorgungsleitungen (z. B. für Wasser, Heizung oder Gas) möglichst nicht in unmittelbarer Nähe von schutzbedürftigen Technikkomponenten verlaufen. Vorhandene Versorgungsleitungen werden zumindest an den kritischen Stellen regelmäßig überprüft, um die Dichtigkeit zu prüfen.

#### Bildung von Brandabschnitten (INF.2.A2)

Es müssen entsprechend den örtlichen Gegebenheiten geeignete Brandabschnitte für die Räumlichkeiten eines Rechenzentrums festgelegt werden. Die Anforderungen an die Widerstandsfähigkeit von Brandwand bzw. von Brandabschnitten müssen neben Personen- und Gebäudeschutz auch den Schutz des Inventars und dessen Verfügbarkeit berücksichtigen. Somit sollte verhindert werden, dass sich ein Brand durch Flammen und heiße Rauchgase ausbreitet und eine Blockade von Wärmestrahlung sowie der Ausbreitung von kaltem Rauch erfolgt. Im Falle eines Serverraum muss geprüft werden, ob geeignete Brandabschnitte für die Räumlichkeiten umsetzbar sind.

#### Einsatz einer unterbrechungsfreien Stromversorgung (INF.2.A3)

Für alle geschäftskritischen Komponenten des Rechenzentrums muss eine unterbrechungsfreie Stromversorgung (USV) bereitgestellt und betrieben werden. Da der Leistungsbedarf von Klimatisierungsanlagen oft zu hoch für eine USV ist, sollte mindestens die Steuerung der Anlagen an die unterbrechungsfreie Stromversorgung angeschlossen sein. Im Falle eines Serverraums sollte je nach Verfügbarkeitsanforderungen der IT-Systeme geprüft werden, ob der Betrieb einer USV notwendig ist.

Die USVs müssen ausreichend dimensioniert werden, sodass alle Komponenten bei einem Ausfall der Versorgung so lange mit Strom versorgt sind, dass kein Datenverlust entsteht bzw. ein kontrolliertes Herunterfahren der IT-Systeme ermöglicht wird.

Bei relevanten Änderungen der Infrastruktur muss eine Überprüfung der vorhandenen USV-Systeme erfolgen, ob diese noch ausreichend dimensioniert sind. Bei Verwendung von USVs mit einem Batteriespeicher muss diese im erforderlichen Temperaturbereich gehalten und sollte vorzugsweise in einem separaten Brandabschnitt platziert werden.

Die USV muss regelmäßig gewartet und auf Funktionsfähigkeit getestet werden. Hierbei müssen die vom Hersteller vorgesehenen Wartungsintervalle eingehalten werden. Um die benötigte erforderliche Stützzeit der USV bereitstellt zu können, muss regelmäßig sowie zusätzlich (wenn sich bei den Verbrauchern etwas ändert) eine Ermittlung der tatsächlichen Stützzeit erfolgen.

IT-Geräte die über eine USV versorgt werden, dürfen nicht über geschirmte Leitungen mit weiteren IT-Geräten verbunden sein.

#### Notabschaltung der Stromversorgung (INF.2.A4)

Für den Notfall muss eine geeignete Möglichkeit bereitgestellt werden, das komplette Rechenzentrum spannungsfrei zu schalten. Bei der Etablierung einer Notabschaltung muss sichergestellt werden, dass diese nicht nur die externe Energieversorgung abtrennt, sondern auch die komplette USV-Anlage abschaltet. Hierfür sollte beispielsweise ein Not-Aus-Schalter implementiert werden. Alle Not-Aus-Schalter müssen so geschützt sein, dass sie nicht unbeabsichtigt betätigt werden können.

#### Einhaltung der Lufttemperatur und -feuchtigkeit (INF.2.A5)

Um IT-Systeme entsprechend den Hersteller-Empfehlungen zuverlässig betreiben zu können, muss sichergestellt sein, dass die Lufttemperatur und Luftfeuchtigkeit im IT-Betriebsbereich innerhalb der vorgeschriebenen Grenzen liegen.

Die tatsächliche Wärmelast in den gekühlten Bereichen des Rechenzentrums muss in regelmäßigen Abständen und nach größeren Umbauten durch Berechnung oder Messung überprüft werden.

Vorhandene Klimatisierungseinrichtung müssen regelmäßig gewartet werden. Sollten die beiden Parameter "Temperatur" und "Feuchtigkeit" vom Normwert abweichen, müssen sie über eine repräsentative Dauer hinweg in einem der Situation angepassten Zeitintervall aufgezeichnet werden.

#### Zutrittskontrolle (INF.2.A6)

Für den Schutz gegen unbefugten Zutritt zum Rechenzentrum muss eine Zutrittskontrolle etabliert und betrieben werden. Durch eine auf die jeweiligen Erfordernisse abgestimmte Zutrittsregelung muss für eigene Mitarbeitende und für nur zeitweilig Beschäftigte bzw. Dienstleister sichergestellt sein, dass sie keinen Zutritt zu IT-Systemen außerhalb ihres Tätigkeitsbereiches erhalten.

Zusätzlich muss sichergestellt sein, dass Besucher und Fremdpersonal während aller Arbeiten im Rechenzentrum von der Zutrittskontrolle individuell erfasst sowie in Sicherheitsbereichen ab hohen Schutzbedarf beaufsichtigt werden.

Alle Zutrittsmöglichkeiten zu einem Rechenzentrum müssen überwacht werden. Über die mit Zutrittskontrolleinrichtungen ausgestatteten Zugänge in das Rechenzentrum hinaus darf es keine weiteren Zutrittsmöglichkeiten zum Rechenzentrum geben. Im Falle eines Serverraums muss geprüft werden, ob eine Überwachung aller Zutrittsmöglichkeiten sinnvoll ist.

Weiterhin muss geregelt sein, welche Personenkreise für welchen Zeitraum Zutritt zum Rechenzentrum erhalten. Im Rahmen des Rechenzentrumszutrittskonzeptes muss sichergestellt sein, dass keine unnötigen oder zu weitreichenden Zutrittsrechte vergeben werden. Es muss eine regelmäßige Kontrolle erfolgen, ob die Regelungen zum Einsatz einer Zutrittskontrolle eingehalten werden.

#### Verschließen und Sichern (INF.2.A7)

Alle Türen des Rechenzentrums müssen stets verschlossen gehalten werden. Fenster müssen möglichst schon bei der Planung vermieden werden. Falls Fenster doch vorhanden sind, müssen Fenster wie die Türen stets verschlossen gehalten werden.

Türen und Fenster müssen einen dem Sicherheitsniveau eines Rechenzentrums angemessenen Schutz gegen Angriffsversuche bieten. Die Türen und Fenster müssen entsprechend der geltenden Norm DIN EN 1627:2010-09 ausgelegt werden. Hierbei muss beachtet werden, dass die bauliche Ausführung aller raumbildenden Elemente in Bezug auf die Sicherheit, vor allem hinsichtlich der Sicherheitszonen, gleichwertig sind.

#### Einsatz einer Brandmeldeanlage (INF.2.A8)

In den Räumlichkeiten des Rechenzentrums muss eine Brandmeldeanlage installiert sein. Die Brandmeldeanlage muss alle Flächen überwachen. Alle Meldungen der Brandmeldeanlage müssen geeignet weitergeleitet werden. Die Brandmeldeanlage muss regelmäßig gewartet werden. Es muss sichergestellt werden, dass in Räumen, die im Brandabschnitt des Rechenzentrums liegen, keine besonderen Brandlasten vorhanden sind.

#### Einsatz einer Lösch- oder Brandvermeidungsanlage (INF.2.A9)

In den zentralen Räumlichkeiten des Rechenzentrumsverbundes der <Institution> muss eine Lösch- oder Brandvermeidungsanlage nach aktuellem Stand der Technik etabliert und betrieben werden.

In Serverräumen der <Institution> müssen für die Brandbekämpfung Handfeuerlöscher in ausreichender Zahl und Größe bereitgestellt werden. Die Feuerlöscher müssen so angebracht, dass sie im Brandfall leicht zu erreichen sind.

Jeder Feuerlöscher muss regelmäßig inspiziert und gewartet werden, um die Funktionsfähigkeit im Ernstfall zu gewährleisten. Alle Personen mit Rechenzentrums- oder Serverraumzugang müssen in die Benutzung der Handfeuerlöscher eingewiesen werden.

#### Inspektion und Wartung der Infrastruktur (INF.2.A10)

Für alle Komponenten der technischen Infrastruktur müssen mindestens die empfohlenen oder durch Normen festgelegten Intervalle und Vorschriften für Inspektion und Wartung eingehalten werden. Um nachvollziehen zu können, wann welche Arbeiten durchgeführt wurden, müssen Inspektionen und Wartungsarbeiten protokolliert werden.

Kabel- und Rohrdurchführungen durch Brandwände müssen regelmäßig daraufhin geprüft werden, ob die Schotten normgerecht und unversehrt sind. Die Ergebnisse müssen schriftlich dokumentiert werden.

#### Automatisierte Überwachung der Infrastruktur (INF.2.A11)

Alle Störungsmeldungen der Infrastruktur (bspw. Leckage-Überwachung, Klima-, Strom- und USV-Anlagen) müssen automatisiert überwacht und schnellstmöglich in geeigneter Weise über ein Monitoring-System weitergeleitet werden.

Bei den Serverräumen müssen für IT- und Supportgeräte, die nicht oder nur selten von Personen bedient werden, diese mit Fernanzeigen für Störungen ausgestattet werden. Die verantwortlichen Mitarbeitenden müssen zeitnah über erkannte Störungen alarmiert werden.

#### Brandfrüherkennung (INF.2.A17)

Um Brände in Rechenzentren bereits in einem sehr frühen Stadium erkennen zu können, muss eine Anlage zur Brandfrüherkennung etabliert und betrieben werden.

Um Entstehungsbrände daran zu hindern, dass diese sich weiter ausbreiten können, muss durch die Brandfrüherkennung eine automatische Spannungsfreischaltung erfolgen. Hierbei müssen die Überwachungsbereiche der Brandfrüherkennung sowie die Wirkungsbereiche der Spannungsfreischaltung hinreichend kleinteilig konzipiert werden, um ein ausgewogenes Verhältnis zwischen dem Brandschutz einerseits und der Verfügbarkeit des Rechenzentrums andererseits zu erreichen.

Die Anlage zur Brandfrüherkennung muss dem aktuellen Stand der Technik für Rechenzentren genügen. Die Anlage zur Brandfrüherkennung muss nach den Vorgaben des Herstellers betrieben und regelmäßig gewartet werden.

#### Vermeidung und Überwachung nicht erforderlicher Leitungen (INF.2.A29)

In einem Rechenzentrum dürfen nur solche Leitungen verlegt werden, die der unmittelbaren Versorgung der im Rechenzentrum aufgebauten Technik (in der Regel IT- und gegebenenfalls Kühltechnik) dienen.

Ist es aus baulichen Gründen unabwendbar, Leitungen durch das Rechenzentrum zu führen, um andere Bereiche als die des Rechenzentrums zu versorgen, muss dies einschließlich Begründung dokumentiert werden. Solche Leitungen müssen geeignet eingehaust und überwacht werden. Es sollte beachtet werden, dass durch Serverräume vorgenannte Leitungen geführt werden dürfen, ohne zu begründen, warum dies unabwendbar ist.

Meldungen aus der Leitungsüberwachung müssen unverzüglich hinsichtlich der Gefährdungsrelevanz geprüft und bewertet werden. Gegenmaßnahmen müssen entsprechend der erkannten Gefährdungsrelevanz für das Rechenzentrum zeitgerecht umgesetzt werden.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Allgemeines Gebäude

#### Sicherheitskonzept für die Gebäudenutzung (INF.1.A9)

Es muss ein Sicherheitskonzept für die Gebäudenutzung als Rechenzentrum erstellt, regelmäßig auf Aktualität und bei Bedarf aktualisiert werden. Das Sicherheitskonzept für das Gebäude sollte mit dem Gesamt-Sicherheitskonzept der <Institution> abgestimmt und regelmäßig aktualisiert werden.

#### Einhaltung einschlägiger Normen und Vorschriften (INF.1.A10)

Bei der Planung, der Errichtung und dem Umbau des Rechenzentrums sowie beim Einbau von technischen Einrichtungen sollten alle relevanten Normen und Vorschriften berücksichtigt werden.

#### Abgeschlossene Türen (INF.1.A11)

Beschäftigte im Rechenzentrum müssen die Räumlichkeiten abschließen und sollten ihre Arbeitsunterlagen wegschließen, wenn sie den Raum verlassen und der Raum für unberechtigte Personen zugänglich ist. Es sollte sporadisch überprüft werden, ob diese Regelungen umgesetzt werden.

#### Schlüsselverwaltung (INF.1.A12)

Für alle Schlüssel des Rechenzentrums muss ein Schließplan vorliegen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln sollten zentral geregelt werden. Reserveschlüssel sollten vorgehalten und gesichert, aber für Notfälle griffbereit aufbewahrt werden. Nicht ausgegebene Schlüssel sollten sicher aufbewahrt werden. Jede Schlüsselausgabe muss dokumentiert werden.

#### Regelungen für Zutritt zu Verteilern (INF.1.A13)

Der Zutritt zu den Verteilern aller Versorgungseinrichtungen in einem Rechenzentrum muss im Bedarfsfall schnell möglich sein. Der Zutritt zu Verteilern muss auf einen engen Kreis von Berechtigten beschränkt sein.

#### Blitzschutzeinrichtungen (INF.1.A14)

Das Rechenzentrum der <Institution> muss über einen Blitz- und Überspannungsschutz mit den folgenden Anforderungen verfügen:

* Der Blitz- und Überspannungsschutz wird für den direkten Einschlag eines Blitzes sowie für die Einkopplung aufgrund der enormen elektrischen Felder gestaltet.
* Der Blitzschutz teilt sich in den äußeren und inneren Blitzschutz auf und wird nach geltender Norm DIN EN 62305 / VDE 0185 umgesetzt.
* Der äußere Blitzschutz dient im Wesentlichen dem Schutz des Gebäudes. (z. B. Blitzableiter)
* Zum Schutz von IT-Systemen wird ein gestaffelter innerer Blitzschutz, bestehend aus Grobschutz (bis ca. 6000 V), Mittelschutz (bis ca. 2000 V) und Feinschutz realisiert. Der Grobschutz muss blitzstromtragfähig sein.
* Bei der Installation ist auf ein zentrales Potential zu achten, damit die Wirksamkeit der Überspannungsschutzeinrichtungen gegeben ist.
* Für das Rechenzentrum sollten Blitzschutzzonen eingerichtet werden, die sich an den vorhandenen Sicherheitszonen orientieren.

#### Lagepläne der Versorgungsleitungen (INF.1.A15)

Es sollten aktuelle Lagepläne aller Versorgungsleitungen für das Rechenzentrum der <Institution> existieren. Es sollte innerhalb der <Institution> geregelt sein, wer die Lagepläne aller Versorgungsleitungen führt und aktualisiert. Die Pläne sollten so aufbewahrt werden, dass ausschließlich berechtigte Personen darauf zugreifen können, sie aber im Bedarfsfall schnell verfügbar sind.

#### Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile (INF.1.A16)

Lagehinweise auf schutzwürdige Bereiche sollten innerhalb des Rechenzentrums vermieden werden. Schutzwürdige Gebäudebereiche dürfen von außen nicht leicht einsehbar sein.

#### Baulicher Rauchschutz (INF.1.A17)

Der bauliche Rauchschutz sollte nach Installations- und Umbauarbeiten überprüft werden. Es muss regelmäßig überprüft werden, ob die Rauchschutz-Komponenten noch funktionieren.

#### Brandschutzbegehungen (INF.1.A18)

Brandschutzbegehungen müssen mindestens ein- bis zweimal im Jahr stattfinden. Bei Brandschutzbegehungen sollten festgestellte Mängel unverzüglich behoben werden.

#### Frühzeitige Information des Brandschutzbeauftragten (INF.1.A19)

Die Brandschutzbeauftragten sollten über Arbeiten an Leitungstrassen, Fluren, Flucht- und Rettungswegen informiert werden. Die Brandschutzbeauftragten sollten die ordnungsgemäße Ausführung von Brandschutzmaßnahmen kontrollieren.

#### Alarmierungsplan und Brandschutzübungen (INF.1.A20)

Es muss ein Alarmierungsplan für die im Brandfall zu ergreifenden Maßnahmen erstellt werden. Der etablierte Alarmierungsplan sollte periodisch überprüft und bei Bedarf aktualisiert werden. Durch regelmäßige Brandschutzübungen sollten die im Brandfall zu ergreifenden Maßnahmen und der Alarmierungsplan verifiziert und bei Bedarf an aktuelle Erfordernisse angepasst werden.

### Rechenzentrum sowie Serverraum

#### Entwurf und Umsetzung eines Perimeter-Schutzes für das Rechenzentrum (INF.2.A12)

Die Sicherheitsmaßnahmen zum Perimeter-Schutz sollten gleichwertig mit denen des Sicherheitskonzeptes für das Gebäude und Umfeld sein. Je nach festgelegten Schutzbedarf für das Rechenzentrum und abhängig vom Gelände sollte der Perimeter-Schutz ausfolgenden Komponenten bestehen:

* Äußere Umschließung oder Umfriedung,
* Sicherungsmaßnahmen gegen unbeabsichtigtes Überschreiten einer Grundstücksgrenze,
* Sicherungsmaßnahmen gegen beabsichtigtes gewaltloses Überwinden der Grundstücksgrenze,
* Sicherungsmaßnahmen gegen beabsichtigtes gewaltsames Überwinden der Grundstücksgrenze,
* Freiland-Sicherungsmaßnahmen sowie
* Äußere Personen- und Fahrzeugidentifikation.

#### Planung und Installation von Gefahrenmeldeanlagen (INF.2.A13)

Es muss ein konsistentes Schutzkonzept für das jeweilige Gebäude erarbeitet werden. Erst im Anschluss sollte geplant werden, welche Gefahrenmeldeanlagen für welche Gebäudebereiche des Rechenzentrums benötigt, installiert und betrieben werden und wie mit Alarmmeldungen umzugehen ist. Das Sicherheitsmaßnahmen müssen immer angepasst werden, wenn sich die Nutzung der Gebäudebereiche verändert.

Es sollte eine für den Betrieb eines Rechenzentrums angemessene Gefahrenmeldeanlage etabliert und betrieben werden. Die Meldungen der Gefahrenmeldeanlage sind unter Beachtung der dafür geltenden technischen Anschlussbedingungen auf eine Alarmempfangsstelle aufzuschalten. Die ausgewählte Alarmempfangsstelle sollte jederzeit erreichbar und technisch sowie personell in der Lage sein, geeignet auf die gemeldete Gefährdung zu reagieren. Der Übertragungsweg zwischen eingesetzter Gefahrenmeldeanlage und hilfeleistender Stelle sollte redundant ausgelegt werden. Sofern eine Gefahrenmeldeanlage eingesetzt wird, sind alle vorhandenen Übertragungswege regelmäßig zu testen.

#### Einsatz einer Netzersatzanlage (INF.2.A14)

Die Energieversorgung aus dem Stromnetz eines Energieversorgers sollte um eine Netzersatzanlage ergänzt werden. Beim Einsatz einer Netzersatzanlage sollte der Betriebsmittelvorrat regelmäßig kontrolliert und dokumentiert werden.

Um die Schutzwirkung einer Netzersatzanlage aufrechtzuerhalten, muss diese regelmäßig gewartet werden. Im Rahmen der Wartung der Netzersatzanlage sollten auch Belastungs- und Funktionstests sowie Testläufe unter Last durchzuführen.

#### Überspannungsschutzeinrichtung (INF.2.A15)

Es muss auf Basis der aktuell gültigen Norm ein Konzept für den Blitz- und Überspannungsschutz unter Beachtung der energetischen Koordination erstellt und etabliert werden (siehe DIN EN 62305-4). Die energetische Koordination der Einrichtungen für den Überspannungsschutz sollte in einem Konzept dokumentiert und abgenommen werden.

Die Einrichtungen des Blitz- und Überspannungsschutzes sollte periodisch und nach bekannten Ereignissen geprüft und falls erforderlich ersetzt werden. Unabhängig von Umfang und Ausbau des Überspannungsschutzes sollte berücksichtigt werden, dass ein umfassender und durchgängiger Potenzialausgleich aller in den Überspannungsschutz einbezogenen elektrischen Betriebsmittel erforderlich ist. Bei Nachinstallationen muss darauf geachtet werden, dass der Potenzialausgleich mitgeführt wird.

#### Klimatisierung im Rechenzentrum (INF.2.A16)

Es muss sichergestellt werden, dass im Rechenzentrum geeignete klimatische Bedingungen geschaffen und aufrechterhalten werden. Dies betrifft die Lufttemperatur und Luftfeuchtigkeit sowie den Frischluftanteil und die Schwebstoffbelastung. Die Klimatisierung für das Rechenzentrum sollte unter Berücksichtigung der ermittelten Wärmelast ausreichend für den ererbten Schutzbedarf genügend dimensioniert werden. Alle relevanten Werte für eine ausreichende Klimatisierung des Rechenzentrums müssen ständig überwacht werden. Insofern ein überwachter Wert von der Norm abweicht, sollte eine automatische Alarmierung an die verantwortlichen für den Betrieb der Klimaanlagen stattfinden.

Die Klimaanlagen des Rechenzentrums sollten durch redundant ausgelegte Komponenten ausfallsicher betrieben werden.

#### Durchführung von Funktionstests der technischen Infrastruktur (INF.2.A19)

Die technische Infrastruktur eines Rechenzentrums sollte regelmäßig (zumindest ein- bis zweimal jährlich) sowie nach Systemumbauten und umfangreichen Reparaturen getestet werden. Die Ergebnisse der Überprüfung der technischen Infrastruktur des Rechenzentrums muss dokumentiert werden. Im Rahmen von echten Funktionstest bspw. unter zur Hilfenahme der Methodiken des Chaos Engineering sollten ganze Reaktionsketten einbezogen und getestet werden.

#### Regelmäßige Aktualisierungen der Infrastruktur- und Baupläne (INF.2.A20)

Baupläne, Trassenpläne, Strangschemata, Fluchtwegpläne, Feuerwehrlaufkarten usw. sollten nach jeder Umbaumaßnahme umgehend aktualisiert werden. Die Aktualisierung der Dokumentation sollte ebenfalls erfolgen, wenn die Infrastruktur oder die Sicherheitstechnik des Rechenzentrums erweitert wurden. Es muss mindestens einmal innerhalb von drei Jahren überprüft werden, ob alle relevanten Pläne noch aktuell und korrekt sind.

Die Mitarbeitenden sollten regelmäßig über Aktualisierungen der Infrastruktur- und Baupläne informiert werden.

#### Anlagen zur Erkennung, Löschung oder Vermeidung von Bränden (INF.2.A30)

Das Rechenzentrum sollte mit einer automatischen Lösch- oder Brandvermeidungsanlage zusätzlich zu den Basis-Anforderung der Brandfrüherkennung ausgestattet sein. Ein Serverraum sollte mit einer Anlage zur Brandfrüherkennung ausgestattet werden.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Allgemeines Gebäude

#### Unabhängige elektrische Versorgungsstränge (INF.1.A21 - A)

Die IT-Systeme im Rechenzentrum sollten über zwei voneinander unabhängige Versorgungsstränge gespeist werden.

#### Sichere Türen und Fenster (INF.1.A22 - A)

Das System der Einbruchhemmung sollte wie eine Kette wirken und ist nur so gut wie das schwächste Glied. Aus diesem Grunde muss die Einbruchshemmung bereits bei der Gebäudeplanung beginnen. Der Zutritt zum Rechenzentrum sollte über einen Haupteingang erfolgen, der in den Geschäftszeiten mit einem Empfangsdienst besetzt sein sollte. An kleineren Standorten kann auf den Empfangsdienst verzichtet werden, wenn die nachfolgenden Regelungen eingehalten werden.

* Der Außenbereich eines Rechenzentrums wird vom Innenbereich mit einer auch dauerhaft verschließbaren Tür abgeschottet.
* Die Tür und etwaige Fenster in den leicht zugänglichen Etagen des Rechenzentrums werden entsprechend der geltenden Normen (DIN EN 1627:2010-09) ausgelegt und verfügt über eine hohe bis sehr hohe Widerstandsklasse. Hieraus ableitend muss in der Kette der zu durchquerenden Türen, um in die Räumlichkeiten des Rechenzentrums und an die IT-System zu gelangen mindestens ein 20-minütiger Einbruchswiderstand realisiert werden.
* Ein Zutritt von Personen erfolgt nur nach erfolgreicher Zutrittskontrolle (personalisierte Zugangskarten).
* Jeder Mitarbeitende des Rechenzentrums ist zur Einhaltung und Überwachung dieser Richtlinie zu verpflichten.

#### Bildung von Sicherheitszonen (INF.1.A23 - A)

Räume ähnlichen Schutzbedarfs sollten in Sicherheitszonen zusammengefasst werden, um vergleichbare Risiken einheitlich behandeln und Kosten für erforderliche Sicherheitsmaßnahmen reduzieren zu können. Es muss ein Sicherheitszonenkonzept für Gebäude und Grundstück entwickelt und dokumentiert werden.

#### Selbsttätige Entwässerung (INF.1.A24 - A)

Alle von Wasser gefährdeten Bereiche sollten mit einer selbsttätigen Entwässerung ausgestattet sein. Es sollte regelmäßig geprüft werden, ob die aktiven und passiven Entwässerungseinrichtungen noch funktionieren.

#### Geeignete Standortauswahl (INF.1.A25 - A)

Wird ein Rechenzentrumsstandort geplant oder ausgewählt, muss geprüft werden, welche Bedingungen aus dem Umfeld Einfluss auf die Informationssicherheit haben könnten. Es sollte eine Übersicht über standortbedingte Gefährdungen geben. Diesen Gefährdungen müssen mit zusätzlichen kompensierenden Maßnahmen entgegengewirkt werden.

#### Pförtner- oder Sicherheitsdienst (INF.1.A26 - A)

Die Aufgaben des Pförtner- bzw. Sicherheitsdienstes sollten klar dokumentiert sein. Die Pförtner sollten alle Personenbewegungen an der Pforte und an allen anderen Eingängen beobachten bzw. kontrollieren. Alle Mitarbeiter und Besucher des Rechenzentrums sollten sich bei den Pförtnern ausweisen können. Besucher sollten zu den Besuchten begleitet bzw. an der Pforte abgeholt werden. Die Pförtner sollten über die etablierten Prozesse rechtzeitig darüber informiert werden, wenn sich Zutrittsberechtigungen ändern.

#### Einbruchschutz (INF.1.A27 - A)

Es sollten ausreichende und den örtlichen Gegebenheiten angepasste Maßnahmen zum Einbruchschutz umgesetzt werden. Bei der Planung, der Umsetzung und im Betrieb sollte beim Einbruchschutz darauf geachtet werden, dass er gleichwertig und durchgängig ist. Hieraus ableitend muss in der Kette der zu durchquerenden Türen, um in die Räumlichkeiten des Rechenzentrums und an die IT-System zu gelangen mindestens ein 20-minütiger Einbruchswiderstand realisiert werden.

Der Einbruchswiderstand sollte regelmäßig durch fachkundige Personen begutachtet und dokumentiert werden.

#### Klimatisierung durch raumlufttechnische Anlagen (INF.1.A28 - A)

In Rechenzentren sollte die Luftversorgung durch raumlufttechnische Anlagen (RLT-Anlagen) sichergestellt werden. Die RLT-Anlagen sollten auf die tatsächliche Nutzung und Wärmelast des Rechenzentrums ausgelegt und regelmäßig gewartet werden.

#### Organisatorische Vorgaben für die Gebäudereinigung (INF.1.A29 - CI)

Es muss kontrolliert werden, ob die Verantwortlichen Mitarbeiter für die Reinigung bzw. die Mitarbeiter der beauftragten Reinigungsfirma die ausgegebenen Zutrittsmittel (bspw. RFID-Karten, Schlüssel bzw. Ausweise) vertragsgemäß verwenden. Die Reinigungskräfte sollten über den Umgang mit der IT ausreichend informiert sein. Reinigungskräfte müssen in besonders sensitiven Bereichen des Rechenzentrums bei der Arbeit beaufsichtigt werden.

### Rechenzentrum sowie Serverraum

#### Ausweichrechenzentrum (INF.2.A21 - A)

Zur Erfüllung der hohen und sehr hohen Verfügbarkeitsanforderungen der Prozesse der <Institution> müssen geografisch separierte Ausweichrechenzentren etabliert und eingesetzt werden. Die Ausweichrechenzentren müssen so dimensioniert sein, dass alle geschäftskritischen Prozesse der <Institution> aufrechterhalten werden können. Die Ausweichrechenzentren müssen ständig einsatzbereit sein. Alle erforderlichen Daten müssen regelmäßig in die Ausweichrechenzentren gespiegelt.

#### Durchführung von Staubschutzmaßnahmen (INF.2.A22 - A)

Wenn ein bestehendes Rechenzentrum erweitert wird, müssen geeignete Staubschutzmaßnahmen definiert, geplant und umgesetzt werden. Personen, die selbst nicht an den Baumaßnahmen beteiligt sind, sollten in ausreichend engen Zeitabständen kontrollieren, ob die Staubschutzmaßnahmen ordnungsgemäß funktionieren und die Regelungen zum Staubschutz eingehalten werden.

#### Sicher strukturierte Verkabelung im Rechenzentrum (INF.2.A23 - A)

Kabeltrassen innerhalb des Rechenzentrums müssen sorgfältig geplant und ausgeführt. Alle Kabel sollten vor ungewollten mechanischen Beanspruchungen, Manipulationen, Abhörversuchen oder Bränden geschützt werden. Für unterschiedliche Netzarten, z. B. Datennetz, Netz für Gefahrenmeldeanlagen und Stromnetz, werden getrennte Kabel benutzt. Werden Kabel für verschiedene Netze gemeinsam geführt, muss sichergestellt sein, dass gegenseitige Störungen minimiert werden. Zudem sollte eine redundante Kanten- und Trassen-disjunkte Führung angestrebt.

#### Einsatz von Videoüberwachungsanlagen (INF.2.A24 - A)

Die Zutrittskontrolle und die Einbruchmeldung sollten durch Videoüberwachungsanlagen ergänzt. Hierzu müssen die für Videoüberwachungsanlagen sinnvollen Flächen identifiziert werden.

Eine geplante Videoüberwachung muss konsistent in das gesamte Sicherheitskonzept der <Institution> eingebettet. Bei der Planung, Konzeption und eventuellen Auswertung von Videoaufzeichnungen muss immer der Datenschutz und die Personalvertretung mit einbezogen.

Die für eine Videoüberwachung benötigten zentralen Technikkomponenten müssen in einer geeigneten Umgebung aufgestellt und geschützt werden. Es muss regelmäßig überprüft, ob die Videoüberwachungsanlage korrekt funktioniert und dem vereinbarten Zweck genügt.

#### Redundante Auslegung von unterbrechungsfreien Stromversorgungen (INF.2.A25 - A)

Um die Verfügbarkeit eines Rechenzentrums sicherzustellen, sollten die USV-Anlagen redundant ausgelegt werden. Nach einem Stromausfall sollten alle für den ordnungsgemäßen Betrieb des Rechenzentrums erforderlichen Komponenten so lange mit Strom versorgt, bis eine alternative Stromquelle angeschlossen werden kann.

#### Redundante Auslegung von Netzersatzanlagen (INF.2.A26 - A)

Bei sehr hohen Schutzbedarf sollten Netzersatzanlagen redundant ausgelegt. Es muss sichergestellt, dass alle Netzersatzanlagen regelmäßig gewartet werden.

#### Durchführung von Alarmierungs- und Brandschutzübungen (INF.2.A27 - A)

Es sollten regelmäßige Alarmierungs- und Brandschutzübungen unter Berücksichtigung eines Rechenzentrumsbetriebes durchgeführt werden. Diese basieren auf einem Alarmierungsplan, in dem die zu ergreifenden Maßnahmen dokumentiert sind. Es muss regelmäßig geprüft, ob die Maßnahmen noch korrekt, aktuell und praktikabel sind.

#### Einsatz von höherwertigen Gefahrenmeldeanlagen (INF.2.A28 - A)

Für Rechenzentrumsbereiche mit sehr hohen Schutzbedarf sollten durch die <Institution> ausschließlich Gefahrenmeldeanlagen der VdS-Klasse C (gemäß VDS-Richtlinie 2311) eingesetzt werden.