Bundesamt
für Sicherheit in der
Informationstechnik

INF.1 Allgemeines Gebäude

1. Beschreibung

1.1. Einleitung

Ein Gebäude umschließt alle stationären Arbeitsplätze, die verarbeiteten Informationen sowie die aufgestellte Informationstechnik. Es gewährleistet somit einen Schutz vor äußeren Einflüssen. Daher ist nicht nur das Bauwerk an sich zu betrachten, also Wände, Decken, Böden, Dach, Fenster sowie Türen, sondern auch alle gebäudeweiten Infrastruktur- und Versorgungseinrichtungen wie Strom, Wasser, Gas, Heizung und Kühlung.

Betrachtet wird ein Gebäude, das von einer oder mehreren Organisationseinheiten einer Institution genutzt wird. Diese können unterschiedliche Sicherheitsansprüche haben. Zudem muss in alle Überlegungen einfließen, dass ein Gebäude fast immer auch von institutionsfremden Personen, wie Besuch, Kundschaft oder Liefernden, betreten wird. Wenn ein Gebäude von verschiedenen Parteien genutzt wird, dann müssen Gestaltung und Ausstattung des Gebäudes und das Nutzungskonzept für das Gebäude zueinander passen. Es soll eine optimale Umgebung für die dort tätigen Menschen sichergestellt werden. Unberechtigte sollen dort keinen Zutritt erhalten, wo sie die Sicherheit beeinträchtigen könnten. Die im Gebäude installierte Technik soll zudem sicher und effizient betrieben werden können.

1.2. Zielsetzung

In diesem Baustein wird beschrieben, welche Anforderungen zu erfüllen sind, um ein Gebäude aus Sicht der Informationssicherheit optimal zu schützen. Die sich aus den Anforderungen ergebenden Maßnahmen hängen von der Art und Größe der Institution sowie Art und Größe des Gebäudes ab. Anforderungen aus diesem Baustein können auch auf große Liegenschaften mit mehreren Gebäuden oder auf die Nutzung einzelner Gebäudeteile in Mehrparteienhäusern übertragen werden.

1.3. Abgrenzung und Modellierung

Der Baustein INF.1 *Allgemeines Gebäude* ist für jedes Gebäude einmal anzuwenden.

Dieser Baustein betrachtet technische und nicht-technische Sicherheitsaspekte bei der Planung und Nutzung von typischen Gebäuden für Unternehmen und Behörden. Dabei wird der gesamte Lebenszyklus von Gebäuden aus Sicht der Informationssicherheit betrachtet, beginnend von der Erstellung eines Anforderungskataloges, über die Konzeption, Einrichtung, Nutzung bis hin zu Umbauten oder dem Auszug.

Die Verkabelung in einem Gebäude wird in dem Baustein INF.12 *Verkabelung* gesondert betrachtet, spezielle Räumlichkeiten, wie Serverräume oder Archivräume, in den jeweiligen Bausteinen der Schicht INF *Infrastruktur*.

Der Umgang mit Fremdpersonal ist im Baustein ORP.1 *Organisation* geregelt.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein INF.1 *Allgemeines Gebäude* von besonderer Bedeutung.

2.1. Feuer

Gebäude und Einrichtung können durch ein Feuer schwer beschädigt, Menschen schwer verletzt oder getötet werden. Neben den direkt durch das Feuer verursachten Schäden müssen auch die Folgeschäden betrachtet werden. So dauert die Wiederinbetriebnahme durch Brand beschädigter Bereiche in der Regel Wochen oder gar Monate. Eine sehr große Gefahr bei einem Feuer ist der giftige Brandrauch. Die meisten Personenschäden entstehen daher durch Rauchvergiftungen. Aber auch an Einrichtungen und IT-Systemen kann Brandrauch schwere Schäden anrichten.

Wenn PVC verbrennt, entstehen etwa Chlorgase, die zusammen mit der Luftfeuchtigkeit und dem Löschwasser Salzsäure bilden. Werden die Salzsäuredämpfe über die Klimaanlage verteilt, können auf diese Weise auch Schäden an empfindlichen elektronischen Geräten entstehen, die in einem vom Brandort weit entfernten Teil des Gebäudes stehen.

2.2. Blitz

Während eines Gewitters sind Blitzeinschläge die größte Gefahr für Gebäude und Informationstechnik. Blitze erreichen bei Spannungen von mehreren 100.000 Volt Ströme bis zu 200.000 Ampere. Diese enorme elektrische Energie wird innerhalb von 50 bis 100 Mikrosekunden freigesetzt und abgebaut. Ein Blitz mit diesen Werten, der in einem Abstand von etwa zwei Kilometern einschlägt, verursacht auf elektrischen Leitungen im Gebäude immer noch Spannungsspitzen, die zur Zerstörung empfindlicher elektronischer Geräte führen können. Diese indirekten Schäden nehmen zu, je näher am Gebäude der Blitz einschlägt.

Schlägt der Blitz direkt in ein Gebäude ein, können durch die dynamische Energie des Blitzes große Schäden verursacht werden. Dies können zum Beispiel Beschädigungen an Dach und Fassade sowie Schäden durch auftretende Brände oder Überspannungsschäden an elektrischen Geräten sein.

2.3. Wasser

Wasser kann von außen, beispielsweise durch Regen, Hochwasser oder Überschwemmungen, oder von innen, etwa durch defekte wasserführende Leitungen, Schäden an einem Gebäude und seinen Einrichtungen verursachen.

2.4. Elementarschäden und Naturkatastrophen

Je nach Standort ist ein Gebäude den Risiken durch Elementarschäden und Naturkatastrophen unterschiedlich stark ausgesetzt. Ursachen für Naturkatastrophen können seismische, klimatische oder vulkanische Phänomene sein, wie beispielsweise Erdbeben, Hochwasser, Erdrutsche, Tsunamis, Lawinen oder Vulkanausbrüche. Beispiele für extreme meteorologische Phänomene sind Unwetter, Orkane oder Starkregen.

2.5. Umfeld-Gefährdungen

Gebäude können auch durch Ereignisse in der unmittelbaren Umgebung beschädigt werden, beispielsweise wenn giftige Substanzen austreten. Durch Rettungsarbeiten, Straßensperrungen oder Evakuierungen kann es auch möglich sein, dass das Gebäude nur noch eingeschränkt oder nicht mehr genutzt werden kann.

2.6. Unbefugter Zutritt

Wenn Unbefugte in ein Gebäude oder einzelne Räume gelangen, kann dies verschiedene andere Gefährdungen nach sich ziehen. Unbefugte Personen können einerseits durch vorsätzliche Handlungen wie Diebstahl oder Manipulation von Informationen, IT-Systemen oder IT-Komponenten, andererseits aber auch durch unbeabsichtigtes Fehlverhalten, z. B. aufgrund mangelnder Fachkenntnisse, Schäden verursachen.

Dabei können nicht offensichtliche Manipulationen weit höhere Schäden verursachen als direkte Zerstörung. Schon durch das unbefugte Eindringen können Sachschäden entstehen. Fenster und Türen werden gewaltsam geöffnet und dabei beschädigt. Diese zu reparieren oder zu ersetzen, beansprucht in der Regel Zeit und finanzielle Mittel, in der diese ihre Schutzfunktion nicht oder nur eingeschränkt bereitstellen.

2.7. Verstoß gegen Gesetze oder Regelungen

Wird ein Gebäude errichtet, sind viele Gesetze und Vorgaben zu beachten, die beispielsweise den Brandschutz oder andere Aspekte der baulichen Sicherheit betreffen. Wenn gegen diese Gesetze verstoßen wird, fällt dies unter Umständen lange nicht auf, kann aber katastrophale Folgen nach sich ziehen, etwa wenn Brandschotten nicht bestimmungsgemäß eingebaut wurden.

2.8. Unzureichende Brandschottungen

Jedes Gebäude, in dem IT betrieben wird, ist von einer Vielzahl von Kabeln und Leitungen durchzogen, wie beispielsweise Frisch- und Abwasserleitungen, Heizungsrohre oder Leitungen zur Energieversorgung oder Datenübertragung. Es ist dabei unvermeidlich, dass solche Rohr- und Kabeltrassen Brandschutzwände und Geschossdecken queren müssen. Wenn an solchen Stellen keine geeigneten Brandschotten eingebaut sind, können sich darüber unter Umständen Brände und Rauch unkontrolliert ausbreiten.

Die hohe Dynamik der IT macht es auch im Leitungsnetz immer wieder erforderlich, dass Kabel auch über Brandschotten hinweg nachverlegt werden müssen. In welcher Form dies korrekt erfolgen kann, ist unmittelbar von dem vorhandenen Schott abhängig und kann sehr unterschiedlich sein. Werden Änderungen an einem Brandschott nicht nach den Vorgaben des jeweiligen Unternehmens, das das Schott herstellt, ausgeführt, kann es im Fall eines Brandes versagen. Der Brand könnte sich dann in Bereiche ausweiten, die eigentlich durch das Schott geschützt wären.

2.9. Ausfall der Stromversorgung

Bei einem Stromausfall können ganze Gebäude oder Teile davon unbenutzbar werden. Von der Stromversorgung sind nicht nur die offensichtlichen, direkten Stromverbraucher wie IT oder Beleuchtung abhängig. Auch alle Infrastruktureinrichtungen sind heute direkt oder indirekt vom Strom abhängig, z. B. Aufzüge, Klimatechnik, Gefahrenmeldeanlagen, Sicherheitsschleusen, automatische Türschließanlagen, Sprinkler- oder Telefonnebenstellenanlagen. Selbst die Wasserversorgung ist in Hoch- oder Tiefgeschossen aufgrund der erforderlichen Pumpen auf Strom angewiesen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.1 *Allgemeines Gebäude* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Haustechnik
Weitere Zuständigkeiten	Mitarbeitende, Planende, Errichterfirma, Zentrale Verwaltung, Bauleitung, Haustechnik, Institutionsleitung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

INF.1.A1 Planung der Gebäudeabsicherung (B) [Planende]

Je nach der (geplanten) Nutzung eines Gebäudes und dem Schutzbedarf der dort betriebenen Geschäftsprozesse MUSS festgelegt werden, wie das Gebäude abzusichern ist. Bei einem Gebäude MÜSSEN insbesondere Sicherheitsaspekte zum Schutz von Personen im Gebäude, dem Schutz der Wirtschaftsgüter und der IT beachtet werden, von Brandschutz über Elektrik bis hin zur Zutrittskontrolle. Die Sicherheitsanforderungen aus den verschiedenen Bereichen MÜSSEN aufeinander abgestimmt werden.

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

Es MUSS regelmäßig überprüft werden, ob die Absicherung und Auslegung der Stromkreise noch den tatsächlichen Bedürfnissen genügen.

INF.1.A3 Einhaltung von Brandschutzvorschriften (B)

Die bestehenden Brandschutzvorschriften sowie die Auflagen der Bauaufsicht MÜSSEN eingehalten werden. Die Fluchtwege MÜSSEN vorschriftsmäßig ausgeschildert und freigehalten werden. Es MUSS regelmäßig kontrolliert werden, dass die Fluchtwege benutzbar und frei von Hindernissen sind, damit das Gebäude in einer Gefahrensituation schnell geräumt werden kann. Bei der Brandschutzplanung SOLLTE die örtliche Feuerwehr hinzugezogen werden.

Unnötige Brandlasten MÜSSEN vermieden werden.

Es MUSS eine Brandschutzbeauftragte oder einen Brandschutzbeauftragten oder eine mit dem Aufgabengebiet betraute Person geben. Diese Person MUSS geeignet geschult sein.

INF.1.A4 Branderkennung in Gebäuden (B) [Planende]

Gebäude MÜSSEN entsprechend der Auflagen in der Baugenehmigung und dem Brandschutzkonzept folgend mit einer ausreichenden Anzahl von Rauchmeldern ausgestattet sein. Ist eine lokale Alarmierung am Ort des Melders nicht ausreichend, MÜSSEN alle Melder auf eine Brandmeldezentrale (BMZ) aufgeschaltet werden. Bei Rauchdetektion MUSS eine Alarmierung im Gebäude ausgelöst werden. Es MUSS sichergestellt sein, dass alle im Gebäude anwesenden Personen diese wahrnehmen

können. Die Funktionsfähigkeit aller Rauchmelder sowie aller sonstigen Komponenten einer Brandmeldeanlage (BMA) MUSS regelmäßig überprüft werden.

INF.1.A5 Handfeuerlöscher (B)

Zur Sofortbekämpfung von Bränden MÜSSEN Handfeuerlöscher in der jeweils geeigneten Brandklasse (DIN EN 3 Tragbare Feuerlöscher) in ausreichender Zahl und Größe im Gebäude zur Verfügung stehen. Die Handfeuerlöscher MÜSSEN regelmäßig geprüft und gewartet werden. Die Mitarbeitenden SOLLTEN in die Benutzung der Handfeuerlöscher eingewiesen werden. Die Einweisungen SOLLTEN in zweckmäßigen Zeitabständen wiederholt werden.

INF.1.A6 Geschlossene Fenster und Türen (B) [Mitarbeitende]

Fenster und von außen zugängliche Türen, etwa von Balkonen oder Terrassen, MÜSSEN zu Zeiten, in denen ein Raum nicht besetzt ist, geschlossen werden. Räume MÜSSEN verschlossen werden, falls dort vertrauliche Informationen zurückgelassen werden. Dafür MUSS es eine entsprechende Anweisung geben. Alle Mitarbeitenden SOLLTEN dazu verpflichtet werden, der Anweisung nachzukommen. Es MUSS regelmäßig überprüft werden, ob die Fenster und Innen- sowie Außentüren nach Verlassen des Gebäudes verschlossen sind. Brand- und Rauchschutztüren DÜRFEN NUR dann dauerhaft offen gehalten werden, wenn dies durch zugelassene Feststellanlagen erfolgt.

INF.1.A7 Zutrittsregelung und -kontrolle (B) [Zentrale Verwaltung]

Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen MUSS geregelt und kontrolliert werden. Es SOLLTE ein Konzept für die Zutrittskontrolle existieren. Die Zahl der zutrittsberechtigten Personen SOLLTE für jeden Bereich auf ein Mindestmaß reduziert werden. Weitere Personen DÜRFEN erst Zutritt erhalten, nachdem geprüft wurde, ob dies notwendig ist. Alle erteilten Zutrittsberechtigungen SOLLTEN dokumentiert werden. Die Zutrittskontrollmaßnahmen MÜSSEN regelmäßig auf ihre Wirksamkeit überprüft werden.

Zutrittskontrollen SOLLTEN auch während Umzügen soweit wie möglich vorhanden sein.

INF.1.A8 Rauchverbot (B)

Für Räume mit IT oder Datenträgern, in denen Brände oder Verschmutzungen zu hohen Schäden führen können, wie Serverräume, Datenträger- oder Belegarchive, MUSS ein Rauchverbot erlassen werden. Es MUSS regelmäßig kontrolliert werden, dass bei der Einrichtung oder Duldung von Raucherzonen der Zutrittsschutz nicht umgangen wird.

INF.1.A10 Einhaltung einschlägiger Normen und Vorschriften (B) [Errichterfirma, Bauleitung]

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

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

INF.1.A9 Sicherheitskonzept für die Gebäudenutzung (S) [Planende]

Es SOLLTE ein Sicherheitskonzept für die Gebäudenutzung geben. Das Sicherheitskonzept für das Gebäude SOLLTE mit dem Gesamtsicherheitskonzept der Institution abgestimmt sein. Es SOLLTE dokumentiert und regelmäßig aktualisiert werden.

Schützenswerte Räume oder Gebäudeteile SOLLTEN nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein.

Es MUSS ein IT-bezogenes Brandschutzkonzept erstellt und umgesetzt werden.

INF.1.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

INF.1.A12 Schlüsselverwaltung (S)

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

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

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

INF.1.A14 Blitzschutzeinrichtungen (S)

Es SOLLTE eine Blitzschutzanlage nach geltender Norm installiert sein. Es SOLLTE ein umfassendes Blitz- und Überspannungsschutzkonzept vorhanden sein. Die Fangeinrichtungen bei Gebäuden mit umfangreicher IT-Ausstattung SOLLTEN mindestens der Schutzklasse II gemäß DIN EN 62305 Blitzschutz entsprechen. Die Blitzschutzanlage SOLLTE regelmäßig geprüft und gewartet werden.

INF.1.A15 Lagepläne der Versorgungsleitungen (S)

Es SOLLTEN aktuelle Lagepläne aller Versorgungsleitungen existieren. Es SOLLTE 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.

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

Lagehinweise auf schutzwürdige Bereiche SOLLTEN vermieden werden. Schutzwürdige Gebäudebereiche SOLLTEN von außen nicht leicht einsehbar sein.

INF.1.A17 Baulicher Rauchschutz (S) [Planende]

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

INF.1.A18 Brandschutzbegehungen (S)

Brandschutzbegehungen SOLLTEN regelmäßig, d. h. mindestens ein- bis zweimal im Jahr, stattfinden. Bei Brandschutzbegehungen festgestellte Mängel SOLLTEN unverzüglich behoben werden.

INF.1.A19 Information des oder der Brandschutzbeauftragten (S)

Der oder die Brandschutzbeauftragte SOLLTE über Arbeiten an Leitungstrassen, Fluren, Flucht- und Rettungswegen informiert werden. Diese Person SOLLTE die ordnungsgemäße Ausführung von Brandschutzmaßnahmen kontrollieren.

INF.1.A20 Alarmierungsplan und Brandschutzübungen (S)

Es SOLLTE ein Alarmierungsplan für die im Brandfall zu ergreifenden Maßnahmen erstellt werden. Der Alarmierungsplan SOLLTE in regelmäßigen Abständen überprüft und aktualisiert werden. Brandschutzübungen SOLLTEN regelmäßig durchgeführt werden.

INF.1.A27 Einbruchschutz (S)

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. Er SOLLTE regelmäßig durch eine fachkundige Person begutachtet werden. Die Regelungen zum Einbruchschutz SOLLTEN den Mitarbeitenden bekannt sein.

INF.1.A36 Regelmäßige Aktualisierungen der Dokumentation (S)

Die Dokumentation eines Gebäudes, z. B. Baupläne, Trassenpläne, Strangschemata, Fluchtwegpläne und Feuerwehrlaufkarten, SOLLTE immer auf dem aktuellen Stand gehalten werden. Es SOLLTE mindestens einmal innerhalb von drei Jahren überprüft werden, ob alle relevanten Pläne noch aktuell und korrekt sind. Über Änderungen SOLLTEN die Mitarbeitenden informiert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

INF.1.A21 ENTFALLEN (H)

Diese Anforderung ist entfallen.

INF.1.A22 Sichere Türen und Fenster (H)

Türen und Fenster SOLLTEN anhand der Schutzziele des zu sichernden Bereichs und des Schutzbedarfs der Institution in der passenden Klassifizierung nach den einschlägigen Normen ausgewählt werden. Alle raumumschließenden Sicherungsmaßnahmen durch Fenster, Türen und Wände SOLLTEN in Bezug auf Einbruch, Brand und Rauch gleichwertig und angemessen sein. Es SOLLTE regelmäßig überprüft werden, dass die Sicherheitstüren und -fenster funktionstüchtig sind.

INF.1.A23 Bildung von Sicherheitszonen (H) [Planende]

Räume ähnlichen Schutzbedarfs SOLLTEN in Zonen zusammengefasst werden, um vergleichbare Risiken einheitlich behandeln und Kosten für erforderliche Sicherheitsmaßnahmen reduzieren zu können.

INF.1.A24 Selbsttätige Entwässerung (H)

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.

INF.1.A25 Geeignete Standortauswahl (H) [Institutionsleitung]

Bei Planung und Auswahl des Gebäudestandortes SOLLTE geprüft werden, welche Umfeldbedingungen Einfluss auf die Informationssicherheit haben könnten. Es SOLLTE eine Übersicht über standortbedingte Gefährdungen geben. Diesen Gefährdungen SOLLTE mit zusätzlichen kompensierenden Maßnahmen entgegengewirkt werden.

INF.1.A26 Pforten- oder Sicherheitsdienst (H)

Die Aufgaben des Pforten- oder Sicherheitsdienstes SOLLTEN klar dokumentiert sein. Der Pfortendienst SOLLTE alle Personenbewegungen an der Pforte und an allen anderen Eingängen beobachten und, je nach Sicherheitskonzept, kontrollieren. Alle Mitarbeitenden und Besuchenden SOLLTEN sich bei dem Pfortendienst ausweisen können. Besuchende SOLLTEN zu den Besuchten begleitet oder an der Pforte abgeholt werden. Der Pfortendienst SOLLTE rechtzeitig darüber informiert werden, wenn sich Zutrittsberechtigungen ändern.

INF.1.A28 ENTFALLEN (H)

Diese Anforderung ist entfallen.

INF.1.A29 ENTFALLEN (H)

Diese Anforderung ist entfallen.

INF.1.A30 Auswahl eines geeigneten Gebäudes (H)

Bei der Auswahl eines geeigneten Gebäudes SOLLTE geprüft werden, ob alle für die spätere Nutzung relevanten Sicherheitsanforderungen umgesetzt werden können. Für jedes Gebäude SOLLTEN im Vorfeld die vorhandenen Gefährdungen und die erforderlichen Schäden vorbeugenden oder reduzierenden Maßnahmen dokumentiert werden.

INF.1.A31 Auszug aus Gebäuden (H) [Zentrale Verwaltung]

Im Vorfeld des Auszugs SOLLTE ein Bestandsverzeichnis aller für die Informationssicherheit für den Umzug relevanten Objekte wie Hardware, Software, Datenträger, Ordner oder Schriftstücke erstellt werden. Nach dem Auszug SOLLTEN alle Räume nach zurückgelassenen Dingen durchsucht werden.

INF.1.A32 Brandschott-Kataster (H)

Es SOLLTE ein Brandschott-Kataster geführt werden. In diesem SOLLTEN alle Arten von Schotten individuell aufgenommen werden. Nach Arbeiten an Brandschotten SOLLTEN die Änderungen im Kataster spätestens nach vier Wochen eingetragen werden.

INF.1.A33 ENTFALLEN (H)

Diese Anforderung ist entfallen.

INF.1.A34 Gefahrenmeldeanlage (H)

Es SOLLTE eine den Räumlichkeiten und den Risiken angemessene Gefahrenmeldeanlage geben. Die Gefahrenmeldeanlage SOLLTE regelmäßig geprüft und gewartet werden. Es MUSS sichergestellt werden, dass diejenigen, die Gefahrenmeldungen empfangen in der Lage sind, technisch und personell angemessen auf den Alarm zu reagieren.

INF.1.A35 Perimeterschutz (H) [Planende, Haustechnik]

Abhängig vom Schutzbedarf des Gebäudes und abhängig vom Gelände SOLLTE dieses über einen Perimeterschutz verfügen. Hierbei SOLLTEN mindestens folgende Komponenten auf ihren Nutzen und ihre Umsetzbarkeit hin betrachtet werden:

- äußere Umschließung oder Umfriedung,
- Sicherungsmaßnahmen gegen unbeabsichtigtes Überschreiten einer Grundstücksgrenze,
- Sicherungsmaßnahmen gegen beabsichtigtes gewaltloses Überwinden der Grundstücksgrenze,
- Maßnahmen zur Erschwerung des beabsichtigten gewaltsamen Überwindens der Grundstücksgrenze,
- Freigelände-Sicherungsmaßnahmen,
- Personen- und Fahrzeugdetektion,
- Maßnahmen zur Beweissicherung (beispielsweise Videoaufzeichnung) sowie
- automatische Alarmierung.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A.11 Vorgaben zur physischen Sicherheit und Umgebungssicherheit von Gebäuden.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel CF19 Vorgaben zur physischen Sicherheit und Umgebungssicherheit von Gebäuden.

Das National Institute of Standards and Technology (NIST) hat im Rahmen seiner Special Publications die NIST Special Publication 800-53 zu „Assessing Security and Privacy Controls for Federal Information Systems and Organizations“ veröffentlicht und macht im Appendix C (Table C-11) Vorgaben zur physischen Sicherheit und Umgebungssicherheit von Gebäuden.