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.

Bundesamt
für Sicherheit in der
Informationstechnik

INF.2 Rechenzentrum sowie Serverraum

1. Beschreibung

1.1. Einleitung

Heute werden fast alle strategischen und operativen Funktionen und Aufgaben durch Informationstechnik (IT) maßgeblich unterstützt oder sind ohne IT nicht ausführbar. Dadurch steigen die Anforderungen an die Leistungsfähigkeit und Verfügbarkeit der IT-Systeme und deren Anbindung an die Netzumgebung stetig. Um diesem Leistungsbedarf gerecht zu werden, um entsprechende Reserven vorzuhalten und um die IT auch wirtschaftlich betreiben zu können, konzentrieren Institutionen jeglicher Größe ihre IT-Landschaft in Rechenzentren.

Ein Rechenzentrum (RZ) ist wie folgt definiert:

1. Hat eine IT-nutzende Institution nur einen zentralen IT-Betriebsbereich, ist dieser gemeinsam mit den erforderlichen Supportbereichen grundsätzlich immer wie ein RZ 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 RZ umfasst neben dem IT-Betriebsbereich alle weiteren technischen Supportbereiche (z. B. Stromversorgung, Kälteversorgung, Löschtechnik, Sicherheitstechnik), die dem bestimmungsgemäßen Betrieb und der Sicherheit des IT-Betriebsbereichs dienen.
2. 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-Benutzenden hin durch hauseigene LAN-Verbindungen angeschlossen, ist mindestens der funktional bedeutendste dieser Bereiche als RZ zu behandeln. Des Weiteren sind Bereiche, von deren ordnungsgemäßem Betrieb 50 % und mehr IT-Benutzenden abhängig sind oder aus denen heraus 50 % und mehr an Diensten und Daten (gemessen an der Gesamtheit der Bereiche) bereitgestellt werden, als RZ zu behandeln.
3. Ist die IT-nutzende Institution an mehreren räumlich voneinander getrennten Standorten angesiedelt und sind diese durch andere als hauseigene LAN-Verbindungen miteinander gekoppelt, ist jeder der Standorte entsprechend (1) separat zu betrachten und zu behandeln.
4. Ein IT-Betriebsbereich, in dem für kritische Geschäftsprozesse (Prozesse, deren Störung oder Ausfall zu wesentlichen Beeinträchtigungen der Erledigung primärer Aufgaben einer Institution führen) erforderliche IT angesiedelt ist, ist immer als RZ zu behandeln, unabhängig von Größe oder Anteilsregeln aus Nummer (2).

5. IT-Betriebsbereiche, aus denen heraus Dienste oder Dienstleistungen für Dritte erbracht werden, sind immer als Teil eines RZ zu betrachten. Dabei ist es unerheblich, ob dies gegen Entgelt erfolgt oder nicht.
6. 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.

Die Auflistung der sechs Punkte bedeutet nicht, dass alle Punkte gemeinsam erfüllt sein müssen, damit ein Bereich als Rechenzentrum betrachtet wird. Vielmehr werden verschiedene Möglichkeiten beschrieben, wann ein Bereich als RZ anzusehen ist. 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 nutzenden Institution und steht damit im methodischen Einklang mit der DIN EN 50600.

Soll ein Serverraum abgesichert werden, können die Anforderungen dieses Bausteins entsprechend reduziert werden. Dies muss jedoch stichhaltig und nachvollziehbar begründet werden (6) und es müssen mindestens die Basis-Anforderungen umgesetzt werden.

1.2. Zielsetzung

Dieser Baustein richtet sich einerseits an Institutionen, die ein Rechenzentrum betreiben und im Rahmen einer Revision prüfen möchten, ob sie geeignete Sicherheitsmaßnahmen umgesetzt haben. Andererseits kann der Baustein auch dazu benutzt werden, die Sicherheitsmaßnahmen abzuschätzen, die umgesetzt werden müssen, wenn die IT in einem Rechenzentrum zentralisiert werden soll. Das oberste Ziel der in diesem Baustein beschriebenen Anforderungen ist es, den sicheren Betrieb des Rechenzentrums zu gewährleisten.

1.3. Abgrenzung und Modellierung

Der Baustein INF.2 *Rechenzentrum sowie Serverraum* ist auf jedes Rechenzentrum und jeden Serverraum anzuwenden.

Der vorliegende Baustein eignet sich nicht für kleine Informationsverbünde mit z. B. nur einem oder sehr wenigen Servern oder IT-Systemen. Ein Beispiel dafür ist eine kleine Institution mit wenigen IT-Arbeitsplätzen und einem Server, der in einem separaten Raum betrieben wird. In solchen Fällen genügt es oft, den Baustein INF.5 *Raum sowie Schrank für technische Infrastruktur* umzusetzen.

Anforderungen an Gebäude und die Verkabelung im Allgemeinen sind nicht Teil dieses Bausteins. Diese sind in den Bausteinen INF.1 *Allgemeines Gebäude* und INF.12 *Verkabelung* zu finden, die immer auf Räume und Gebäude bzw. die Verkabelung anzuwenden sind.

Um den Baustein überschaubar zu halten, wurde bewusst auf technische Details und planerische Größen verzichtet. Nähere Informationen liefern einschlägige Normen und weitere Veröffentlichungen des BSI.

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.2 *Rechenzentrum sowie Serverraum* von besonderer Bedeutung.

2.1. Fehlerhafte Planung

Wenn ein Rechenzentrum konzipiert und dabei nicht berücksichtigt wird, es gegen elementare Gefährdungen abzusichern, besteht ein sehr hohes Ausfallrisiko. So können z. B. Standortrisiken wie Luftverkehr, Erdbeben oder Hochwasser die Betriebssicherheit und Verfügbarkeit gefährden. Ebenso massiv kann es sich auf den Betrieb eines Rechenzentrums auswirken, wenn durch eine fehlerhafte Konzeptionierung nicht genügend Bandbreite verfügbar ist oder die Energieversorgung am gewählten Standort nicht ausreicht.

2.2. Fehlende oder fehlerhafte Zutrittskontrollen

Fehlen Zutrittskontrollen oder sind diese unzureichend, erhöht sich die Gefahr, dass unberechtigte Personen das Rechenzentrum betreten und dort fahrlässig, z. B. aufgrund mangelnder Fachkenntnisse, oder vorsätzlich Schaden anrichten. Angreifende können so z. B. schützenswerte Daten entwenden, Geräte stehlen oder Server manipulieren. Unzureichende Zutrittskontrollen wirken sich somit auf die Verfügbarkeit, Vertraulichkeit und die Integrität von Daten und IT-Komponenten aus.

2.3. Unzureichende Überwachung

Wird die im Rechenzentrum betriebene IT und Infrastruktur unzureichend überwacht und betreut, können Komponenten unbemerkt ausfallen. Dadurch wird eventuell die Verfügbarkeit und fehlerfreie Funktion des Rechenzentrums stark beeinträchtigt. Ausfälle treten zudem oftmals schleichend ein. Ohne eine aktive Überwachung könnten diese zu spät bemerkt werden. Es ist dann oft nicht mehr möglich, rechtzeitig zu reagieren.

2.4. Unzureichende Klimatisierung im Rechenzentrum

IT-Komponenten benötigen bestimmte Betriebsbedingungen, um zuverlässig zu funktionieren. Auch setzen sie die von ihnen aufgenommene elektrische Leistung in zusätzliche Wärme um. Wenn in einem IT-Betriebsbereich die Temperatur, die Luftfeuchte oder der Schwebestoffanteil nicht innerhalb der von den Geräteherstellenden vorgegebenen Grenzwerte gehalten werden, kann dies dazu führen, dass technische Komponenten nicht mehr richtig funktionieren oder ausfallen.

2.5. Feuer

Feuer ist zwar eine Gefahr, die eher selten eintritt. Entsteht aber tatsächlich ein Brand, hat dieser meist schwerwiegende Auswirkungen. Denn durch Feuer und Rauch können große Schäden entstehen. Während innerhalb des IT-Betriebsbereichs Elektrobrände die häufigste Ursache für Feuer sind, kann ein Feuer außerhalb des IT-Betriebsbereichs und insbesondere in Supportbereichen, wie der Energieversorgung (inklusive NEA und USV) oder der Klimaanlage, zahlreiche weitere Ursachen haben. Haben der IT-Betriebsbereich oder die Supportbereiche sowie andere Nachbarbereiche keinen oder nur einen unzureichenden Brandschutz, kann sich ein Feuer schnell ausbreiten. Zudem könnten außerhalb entstehende Brände auf das Rechenzentrum übergreifen.

2.6. Wasser

Durch undichte Wasserleitungen, Hochwasser, Rohrbruch, defekte Sprinkler- oder Klimaanlagen kann Wasser in das Rechenzentrum eintreten. Hierdurch können Geräte beschädigt werden und nicht mehr funktionieren. Es kann auch ein Kurzschluss ausgelöst werden, durch den einzelne Bereiche des Rechenzentrums ausfallen oder ein Brand entstehen könnte.

2.7. Fehlender oder unzureichender Einbruchschutz

Selbst wenn eine gut funktionierende Zutrittskontrolle eingerichtet ist, können unbefugte Personen in ein Rechenzentrum eindringen, sofern es nicht ausreichend vor Einbrüchen geschützt wird. Täter und Täterinnen könnten so z. B. IT-Komponenten stehlen oder manipulieren und an vertrauliche Informationen gelangen. Auch könnten sie die Geräte zerstören oder das Rechenzentrum insgesamt beschädigen.

2.8. Ausfall der Stromversorgung

Wenn der Strom ausfällt, kann der Betriebsablauf eines Rechenzentrums und damit der Institution erheblich gestört werden. So sind bei einem Stromausfall eventuell die vom Rechenzentrum bereitgestellten IT-Services plötzlich nicht mehr erreichbar. Ebenso können Daten verloren gehen. Zudem ist es möglich, dass durch einen plötzlichen Stromausfall IT-Systeme, TK-Systeme oder Überwachungstechnik beschädigt werden.

2.9. Verschmutzung

Staub und andere Verschmutzungen in einem Rechenzentrum können dazu führen, dass technische Komponenten (z. B. Lüfter) nicht mehr funktionieren. Durch Verschmutzungen verschleißen Geräte früher und fallen häufiger aus.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.2 *Rechenzentrum sowie Serverraum* 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	IT-Betrieb
Weitere Zuständigkeiten	Mitarbeitende, Planende, Datenschutzbeauftragte, Haustechnik, Wartungspersonal

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.2.A1 Festlegung von Anforderungen (B) [Haustechnik, Planende]

Für ein Rechenzentrum MÜSSEN angemessene technische und organisatorische Vorgaben definiert und umgesetzt werden.

Wenn ein Rechenzentrum geplant wird oder geeignete Räumlichkeiten ausgewählt werden, MÜSSEN auch geeignete Sicherheitsmaßnahmen unter Berücksichtigung des Schutzbedarfs der IT-Komponenten (insbesondere der Verfügbarkeit) mit geplant werden.

Ein Rechenzentrum MUSS insgesamt als geschlossener Sicherheitsbereich konzipiert werden. Es MUSS zudem unterschiedliche Sicherheitszonen aufweisen. Dafür MÜSSEN z. B. Verwaltungs-, Logistik-, IT-Betriebs- und Support-Bereiche klar voneinander getrennt werden. Im Falle eines Serverraums SOLLTE geprüft werden, ob unterschiedliche Sicherheitszonen eingerichtet werden können.

INF.2.A2 Bildung von Brandabschnitten (B) [Planende]

Es MÜSSEN geeignete Brand- und Rauchabschnitte für die Räumlichkeiten eines Rechenzentrums festgelegt werden. Die Brand- und Rauchabschnitte MÜSSEN über den baurechtlich vorgeschriebenen Rahmen hinaus auch Schutz für die darin befindlichen technischen Einrichtungen und deren Verfügbarkeit bieten. Es MUSS verhindert werden, dass sich Brand und Rauch ausbreiten. Im Falle eines Serverraums SOLLTE geprüft werden, ob geeignete Brand- und Rauchabschnitte für die Räumlichkeiten umsetzbar sind.

INF.2.A3 Einsatz einer unterbrechungsfreien Stromversorgung (B) [Haustechnik]

Für alle betriebsrelevanten Komponenten des Rechenzentrums MUSS eine unterbrechungsfreie Stromversorgung (USV) installiert werden. Da der Leistungsbedarf von Klimaanlagen oft zu hoch für eine USV ist, MUSS mindestens die Steuerung der Anlagen an die unterbrechungsfreie Stromversorgung angeschlossen werden. Im Falle eines Serverraums SOLLTE je nach Verfügbarkeitsanforderungen der IT-Systeme geprüft werden, ob der Betrieb einer USV notwendig ist.

Die USV MUSS ausreichend dimensioniert sein. Bei relevanten Änderungen an den Verbrauchern MUSS überprüft werden, ob die vorhandenen USV-Systeme noch ausreichend dimensioniert sind.

Bei USV-Systemen mit Batterie als Energiespeicher MUSS die Batterie im erforderlichen Temperaturbereich gehalten werden. Sie SOLLTE dazu vorzugsweise räumlich getrennt von der Leistungselektronik der USV platziert werden. Die USV MUSS regelmäßig gewartet und auf Funktionsfähigkeit getestet werden. Dafür MÜSSEN die vom herstellenden Unternehmen vorgesehenen Wartungsintervalle eingehalten werden.

INF.2.A4 Notabschaltung der Stromversorgung (B) [Haustechnik]

Es MUSS geeignete Möglichkeiten geben, elektrische Verbraucher im Rechenzentrum spannungsfrei zu schalten. Dabei MUSS darauf geachtet werden, ob und wie eine vorhandene USV räumlich und funktional in die Stromversorgung eingebunden ist. Werden klassische Not-Aus-Schalter eingesetzt, MUSS darauf geachtet werden, dass darüber nicht das komplette Rechenzentrum abgeschaltet wird. Die Notabschaltung MUSS sinnvoll parzelliert und zielgerichtet erfolgen. Alle Not-Aus-Schalter MÜSSEN so geschützt sein, dass sie nicht unbeabsichtigt oder unbefugt betätigt werden können.

INF.2.A5 Einhaltung der Lufttemperatur und -feuchtigkeit (B) [Haustechnik]

Es MUSS sichergestellt werden, dass die Lufttemperatur und Luftfeuchtigkeit im IT-Betriebsbereich innerhalb der vorgeschriebenen Grenzwerte liegen. Die tatsächliche Wärmelast in den gekühlten Bereichen MUSS in regelmäßigen Abständen und nach größeren Umbauten überprüft werden.

Eine vorhandene Klimatisierung MUSS regelmäßig gewartet werden. Die Parameter Temperatur und Feuchtigkeit MÜSSEN mindestens so aufgezeichnet werden, dass sich rückwirkend erkennen lässt, ob Grenzwerte überschritten wurden, und dass sie bei der Lokalisierung der Ursache der Abweichung sowie bei der Beseitigung der Ursache unterstützend genutzt werden können.

INF.2.A6 Zutrittskontrolle (B) [Haustechnik]

Der Zutritt zum Rechenzentrum MUSS kontrolliert werden. Zutrittsrechte MÜSSEN gemäß der Vorgaben des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement* vergeben werden. Für im Rechenzentrum tätige Personen MUSS sichergestellt werden, dass diese keinen Zutritt zu IT-Systemen außerhalb ihres Tätigkeitsbereiches erhalten.

Alle Zutrittsmöglichkeiten zum Rechenzentrum MÜSSEN mit Zutrittskontrolleinrichtungen ausgestattet sein. Jeder Zutritt zum Rechenzentrum MUSS von der Zutrittskontrolle individuell erfasst

werden. Im Falle eines Serverraums SOLLTE geprüft werden, ob eine Überwachung aller Zutrittsmöglichkeiten sinnvoll ist.

Es MUSS regelmäßig kontrolliert werden, ob die Regelungen zum Einsatz einer Zutrittskontrolle eingehalten werden.

Die Anforderungen der Institution an ein Zutrittskontrollsystem MÜSSEN in einem Konzept ausreichend detailliert dokumentiert werden.

INF.2.A7 Verschließen und Sichern (B) [Mitarbeitende, Haustechnik]

Alle Türen des Rechenzentrums MÜSSEN stets verschlossen gehalten werden. Fenster MÜSSEN möglichst schon bei der Planung vermieden werden. Falls sie doch vorhanden sind, MÜSSEN sie ebenso wie die Türen stets verschlossen gehalten werden. Türen und Fenster MÜSSEN einen dem Sicherheitsniveau angemessenen Schutz gegen Angriffe und Umgebungseinflüsse bieten. Sie MÜSSEN mit einem Sichtschutz versehen sein. Dabei MUSS beachtet werden, dass die bauliche Ausführung aller raumbildenden Elemente in Bezug auf die erforderliche Schutzwirkung gleichwertig sein muss.

INF.2.A8 Einsatz einer Brandmeldeanlage (B) [Planende]

In einem Rechenzentrum MUSS eine Brandmeldeanlage installiert sein. Diese MUSS alle Flächen überwachen. Alle Meldungen der Brandmeldeanlage MÜSSEN geeignet weitergeleitet werden (siehe dazu auch INF.2.A13 *Planung und Installation von Gefahrenmeldeanlagen*). Die Brandmeldeanlage MUSS regelmäßig gewartet werden. Es MUSS sichergestellt werden, dass in Räumen des Rechenzentrums keine besonderen Brandlasten vorhanden sind.

INF.2.A9 Einsatz einer Lösch- oder Brandvermeidungsanlage (B) [Haustechnik]

In einem Rechenzentrum MUSS entweder eine Lösch- oder Brandvermeidungsanlage nach aktuellem Stand der Technik installiert sein oder durch technische (insbesondere durch eine flächendeckende Brandfrüherkennung, siehe INF.2.A17 *Brandfrüherkennung*) und organisatorische Maßnahmen (geschultes Personal und Reaktionspläne für Meldungen der Brandfrüherkennung) sichergestellt sein, dass unmittelbar (innerhalb von maximal 3 Minuten) auf Meldungen der Brandfrüherkennung mit schadensminimierenden Maßnahmen reagiert wird.

In Serverräumen ohne Lösch- oder Brandvermeidungsanlage MÜSSEN Handfeuerlöscher mit geeigneten Löschmitteln in ausreichender Zahl und Größe vorhanden sein. Es MUSS beachtet werden, dass darüber hinausgehende baurechtliche Anforderungen hinsichtlich der Ausstattung mit Handfeuerlöschern davon unberührt bleiben. Die Feuerlöscher MÜSSEN so angebracht werden, dass sie im Brandfall leicht zu erreichen sind. Jeder Feuerlöscher MUSS regelmäßig geprüft und gewartet werden. Alle Mitarbeitenden, die ein Rechenzentrum oder einen Serverraum betreten dürfen, MÜSSEN in die Benutzung der Handfeuerlöscher eingewiesen werden.

INF.2.A10 Inspektion und Wartung der Infrastruktur (B) [Wartungspersonal, Haustechnik]

Für alle Komponenten der baulich-technischen Infrastruktur MÜSSEN mindestens die vom herstellenden Unternehmen empfohlenen oder durch Normen festgelegten Intervalle und Vorschriften für Inspektion und Wartung eingehalten werden. Inspektionen und Wartungsarbeiten MÜSSEN protokolliert werden. Brandschotten MÜSSEN daraufhin geprüft werden, ob sie unversehrt sind. Die Ergebnisse MÜSSEN dokumentiert werden.

INF.2.A11 Automatische Überwachung der Infrastruktur (B) [Haustechnik]

Alle Einrichtungen der Infrastruktur, wie z. B. Leckageüberwachung, Klima-, Strom- und USV-Anlagen, MÜSSEN automatisch überwacht werden. Erkannte Störungen MÜSSEN schnellstmöglich in geeigneter Weise weitergeleitet und bearbeitet werden.

Im Falle eines Serverraums SOLLTEN IT- und Supportgeräte, die nicht oder nur selten von einer Person bedient werden müssen, mit einer Fernanzeige für Störungen ausgestattet werden. Die verantwortlichen Mitarbeitenden MÜSSEN zeitnah alarmiert werden.

INF.2.A17 Einsatz einer Brandfrüherkennung (B) [Planende, Haustechnik]

Ein Rechenzentrum MUSS mit einer Brandfrüherkennungsanlage ausgestattet werden. Ein Serverraum SOLLTE mit einer Brandfrüherkennungsanlage ausgestattet werden. Die Meldungen der Brandfrüherkennung MÜSSEN an eine ständig besetzte Stelle geleitet werden, die eine Kontrolle und Schutzreaktion innerhalb von maximal 3 Minuten veranlassen kann. Alternativ MUSS eine automatische Schutzreaktion erfolgen. Um ein ausgewogenes Verhältnis zwischen Brandschutz und Verfügbarkeit zu erreichen, MUSS sichergestellt werden, dass sich einander Redundanz gebende Einrichtungen nicht gemeinsam im Wirkungsbereich der gleichen Spannungsfreischaltung befinden.

INF.2.A29 Vermeidung und Überwachung nicht erforderlicher Leitungen (B) [Haustechnik, Planende]

In einem Rechenzentrum DÜRFEN NUR 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. Die Risiken, die von solchen Leitungen ausgehen, MÜSSEN durch geeignete Maßnahmen minimiert werden, z. B. durch Einhausung und Überwachung.

Durch Serverräume dürfen vorgenannte Leitungen geführt werden, ohne zu begründen, warum dies unabwendbar ist, diese MÜSSEN aber genauso behandelt werden, wie für das Rechenzentrum beschrieben.

Meldungen aus der Überwachung der Leitungen MÜSSEN unverzüglich hinsichtlich der Gefährdungsrelevanz geprüft und bewertet werden. Gegenmaßnahmen MÜSSEN entsprechend der erkannten Gefährdungsrelevanz zeitgerecht umgesetzt werden (siehe auch INF.2.A13 *Planung und Installation von Gefahrenmeldeanlagen).*

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.2.A12 Perimeterschutz für das Rechenzentrum (S) [Planende, Haustechnik]

Für Rechenzentren SOLLTE ein Perimeterschutz existieren. Je nach festgelegtem Schutzbedarf für das Rechenzentrum und abhängig vom Gelände SOLLTE der Perimeterschutz aus folgenden 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,
- äußere Personen- und Fahrzeugdetektion,
- Maßnahmen zur Beweissicherung (beispielsweise Videoaufzeichnung) sowie
- automatische Alarmierung.

INF.2.A13 Planung und Installation von Gefahrenmeldeanlagen (S) [Haustechnik]

Basierend auf dem Sicherheitskonzept des Gebäudes SOLLTE geplant werden, welche Gefahrenmeldeanlagen für welche Bereiche des Rechenzentrums benötigt und installiert werden.

Hierüber hinaus SOLLTE festgelegt werden, wie mit Alarmmeldungen umzugehen ist. Das Konzept SOLLTE immer angepasst werden, wenn sich die Nutzung der Gebäudebereiche verändert.

Es SOLLTE eine zum jeweiligen Einsatzzweck passende Gefahrenmeldeanlage (GMA) installiert werden. Die Meldungen der GMA SOLLTEN unter Beachtung der dafür geltenden Technischen Anschlussbedingungen (TAB) auf eine Alarmempfangsstelle aufgeschaltet werden. Die ausgewählte Alarmempfangsstelle MUSS jederzeit erreichbar sein. Sie MUSS technisch sowie personell in der Lage sein, geeignet auf die gemeldete Gefährdung zu reagieren. Der Übertragungsweg zwischen eingesetzter GMA und Alarmempfangsstelle SOLLTE entsprechend den TAB und nach Möglichkeit redundant ausgelegt werden. Alle vorhandenen Übertragungswege MÜSSEN regelmäßig getestet werden.

INF.2.A14 Einsatz einer Netzersatzanlage (S) [Planende, Haustechnik]

Die Energieversorgung eines Rechenzentrums aus dem Netz eines Energieversorgungsunternehmens SOLLTE um eine Netzersatzanlage (NEA) ergänzt werden. Wird eine NEA verwendet, MUSS sie regelmäßig gewartet werden. Bei diesen Wartungen MÜSSEN auch Belastungs- und Funktionstests sowie Testläufe unter Last durchgeführt werden.

Der Betriebsmittelvorrat einer NEA MUSS regelmäßig daraufhin überprüft werden, ob er ausreichend ist. Außerdem MUSS regelmäßig kontrolliert werden, ob die Vorräte noch verwendbar sind, vor allem um die sogenannte Dieselpest zu vermeiden. Nach Möglichkeit SOLLTE statt Diesel-Kraftstoff schwefelarmes Heizöl verwendet werden. Die Tankvorgänge von Brennstoffen MÜSSEN protokolliert werden. Aus dem Protokoll MUSS die Art des Brennstoffs, die genutzten Additive, das Tankdatum und die getankte Menge hervorgehen.

Wenn für einen Serverraum auf den Einsatz einer NEA verzichtet wird, SOLLTE alternativ zur NEA eine USV mit einer dem Schutzbedarf angemessenen Autonomiezeit realisiert werden.

INF.2.A15 Überspannungsschutzeinrichtung (S) [Planende, Haustechnik]

Es SOLLTE auf Basis der aktuell gültigen Norm (DIN EN 62305 Teil 1 bis 4) ein Blitz- und Überspannungsschutzkonzept erstellt werden. Dabei sind die für den ordnungsgemäßen Betrieb des RZ erforderlichen Blitzschutzzonen (LPZ) festzulegen. Für alle für den ordnungsgemäßen Betrieb des RZ und dessen Dienstleistungsbereitstellung erforderlichen Einrichtungen SOLLTE das mindestens die LPZ 2 sein. Alle Einrichtungen des Überspannungsschutzes SOLLTEN gemäß DIN EN 62305-3, Tabelle E.2 ein Mal im Jahr einer Umfassenden Prüfung unterzogen werden.

INF.2.A16 Klimatisierung im Rechenzentrum (S) [Planende]

Es SOLLTE sichergestellt werden, dass im Rechenzentrum geeignete klimatische Bedingungen geschaffen und aufrechterhalten werden. Die Klimatisierung SOLLTE für das Rechenzentrum ausreichend dimensioniert sein. Alle relevanten Werte SOLLTEN ständig überwacht werden. Weicht ein Wert von der Norm ab, SOLLTE automatisch alarmiert werden.

Die Klimaanlagen SOLLTEN in IT-Betriebsbereichen möglichst ausfallsicher sein.

INF.2.A18 ENTFALLEN (S)

Diese Anforderung ist entfallen.

INF.2.A19 Durchführung von Funktionstests der technischen Infrastruktur (S) [Haustechnik]

Die technische Infrastruktur eines Rechenzentrums SOLLTE regelmäßig (zumindest ein- bis zweimal jährlich) sowie nach Systemumbauten und umfangreichen Reparaturen getestet werden. Die Ergebnisse SOLLTEN dokumentiert werden. Besonders ganze Reaktionsketten SOLLTEN einem echten Funktionstest unterzogen werden.

INF.2.A20 ENTFALLEN (S)

Diese Anforderung ist entfallen.

INF.2.A30 Anlagen zur, Löschung oder Vermeidung von Bränden (S) [Haustechnik, Planende]

Ein Rechenzentrum SOLLTE mit einer automatischen Lösch- oder Brandvermeidungsanlage ausgestattet 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.2.A21 Ausweichrechenzentrum (H)

Es SOLLTE ein geografisch separiertes Ausweichrechenzentrum aufgebaut werden. Das Ausweichrechenzentrum SOLLTE so dimensioniert sein, dass alle Prozesse der Institution aufrechterhalten werden können. Auch SOLLTE es ständig einsatzbereit sein. Alle Daten der Institution SOLLTEN regelmäßig ins Ausweichrechenzentrum gespiegelt werden. Der Schwenk auf das Notfallrechenzentrum SOLLTE regelmäßig getestet und geübt werden. Die Übertragungswege in das Ausweichrechenzentrum SOLLTEN geeignet abgesichert und entsprechend redundant ausgelegt sein.

INF.2.A22 Durchführung von Staubschutzmaßnahmen (H) [Haustechnik]

Bei Baumaßnahmen in einem Rechenzentrum SOLLTEN 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.

INF.2.A23 Zweckmäßiger Aufbau der Verkabelung im Rechenzentrum (H) [Haustechnik]

Kabeltrassen in Rechenzentren SOLLTEN sorgfältig geplant und ausgeführt werden. Trassen SOLLTEN hinsichtlich Anordnung und Dimensionierung so ausgelegt sein, dass eine Trennung der Spannungsebenen sowie eine sinnvolle Verteilung von Kabeln auf den Trassen möglich ist und dass auch für zukünftige Bedarfsmehrung ausreichend Platz zur Verfügung steht. Zur optimalen Versorgung von IT-Hardware, die über zwei Netzteile verfügt, SOLLTE ab der Niederspannungshauptverteilung für die IT-Betriebsbereiche eine zweizügige sogenannte A-B-Versorgung aufgebaut werden. Einander Redundanz gebende Leitungen SOLLTEN über getrennte Trassen verlegt werden.

INF.2.A24 Einsatz von Videoüberwachungsanlagen (H) [Datenschutzbeauftragte, Haustechnik, Planende]

Die Zutrittskontrolle und die Einbruchmeldung SOLLTEN durch Videoüberwachungsanlagen ergänzt werden. Eine Videoüberwachung SOLLTE in das gesamte Sicherheitskonzept eingebettet werden. Bei der Planung, Konzeption und eventuellen Auswertung von Videoaufzeichnungen MUSS der Datenschutzbeauftragte immer mit einbezogen werden.

Die für eine Videoüberwachung benötigten zentralen Technikkomponenten SOLLTEN in einer geeigneten Umgebung geschützt aufgestellt werden. Es SOLLTE regelmäßig überprüft werden, ob die Videoüberwachungsanlage korrekt funktioniert und ob die mit dem oder der Datenschutzbeauftragten abgestimmten Blickwinkel eingehalten werden.

INF.2.A25 Redundante Auslegung von unterbrechungsfreien Stromversorgungen (H) [Planende]

USV-Systeme SOLLTEN modular und so aufgebaut sein, dass der Ausfall durch ein redundantes Modul unterbrechungsfrei kompensiert wird. Sofern für die IT-Betriebsbereiche eine zweizügige sogenannte A-B-Versorgung aufgebaut ist, SOLLTE jeder der beiden Strompfade mit einem eigenständigen USV-System ausgestattet sein.

INF.2.A26 Redundante Auslegung von Netzersatzanlagen (H) [Planende]

Netzersatzanlagen SOLLTEN redundant ausgelegt werden. Hinsichtlich der Wartung MÜSSEN auch redundante NEAs entsprechend INF.2.A14 *Einsatz einer Netzersatzanlage* behandelt werden.

INF.2.A27 ENTFALLEN (H)

Diese Anforderung ist entfallen.

INF.2.A28 Einsatz von höherwertigen Gefahrenmeldeanlagen (H) [Planende]

Für Rechenzentrumsbereiche mit erhöhtem Schutzbedarf SOLLTEN ausschließlich Gefahrenmeldeanlagen der VdS-Klasse C (gemäß VDS-Richtlinie 2311) eingesetzt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI stellt unter https://www.bsi.bund.de/dok/RZ-Sicherheit unter anderem Dokumente zu „Rechenzentrums-Definition“, „Standort-Kriterien für Rechenzentren“, „Verfügbarkeitsmaßnahmen für Rechenzentren“, „Redundanz - Modularität - Skalierbarkeit“ und „Brennstofflagerung für Netzersatzanlagen“ zur Verfügung.

Das Deutsche Institut für Normung e. V. (DIN) beschreibt in der Norm „DIN EN 50600-1:2019-08 Informationstechnik - Einrichtungen und Infrastrukturen von Rechenzentren: Teil 1: Allgemeine Konzepte“, allgemeine Prinzipien zur Auslegung von Rechenzentren.

Das Deutsche Institut für Normung e. V. (DIN) behandelt in der Norm „DIN EN 62305-4:2011-10 Blitzschutz: Teil 4: Elektrische und elektronische Systeme in baulichen Anlagen“, das Thema Blitzschutz.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) gibt in seinem Leitfaden „Betriebssicheres Rechenzentrum“, Hilfestellung zu Planung und Aufbau eines Rechenzentrums.

Der Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV) beschreibt in seiner Publikation „Sicherungsleitfaden Perimeter“, Perimetersicherungsmaßnahmen, die als Hilfestellung zur Objektabsicherung herangezogen werden können.

Bundesamt
für Sicherheit in der
Informationstechnik

INF.5 Raum sowie Schrank für technische Infrastruktur

1. Beschreibung

1.1. Einleitung

Ein Raum für technische Infrastruktur enthält technische Komponenten, die nur selten direkt vor Ort bedient werden müssen. Sie sind aber unabdingbar für die Gebäudeinfrastruktur und damit auch für die IT-Infrastruktur. Dabei kann es sich z. B. um Verteiler für die Energieversorgung, Sicherungskästen, Lüftungsanlagen, TK-Anlagenteile, Patchfelder, Switches oder Router handeln. Dieser Raum ist kein ständiger Arbeitsplatz und wird in der Regel nur zur Wartung betreten bzw. geöffnet.

Wenn die zu schützende technische Infrastruktur nicht in einem separaten Raum untergebracht werden kann oder sich der Raum nicht entsprechend der beschriebenen Anforderungen einrichten lässt, kann die technische Infrastruktur auch in einem eigens dafür ausgerüsteten Schrank untergebracht werden. Das kann auch sinnvoll sein, wenn für die Unterbringung der technischen Infrastruktur ein Schrank die wirtschaftlichste Alternative darstellt. Die Anforderungen an den Raum sind dann möglichst wirkungsgleich auf den Schrank und dessen Hülle zu übertragen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, einen Raum oder Schrank für technische Infrastruktur im Sinne der Informationssicherheit baulich, mechanisch und elektronisch zu schützen. Mit einem Raum ist zwar grundsätzlich ein Raum respektive Schrank in einem Gebäude gemeint, es kann sich aber sinngemäß auch um einen Container außerhalb eines Gebäudes oder ein Zelt mit technischer Infrastruktur handeln. Der Schutz sollte derart gestaltet werden, dass die darin befindlichen technischen Komponenten in ihren Funktionen möglichst nicht beeinträchtigt werden können.

Im weiteren Verlauf wird nur noch die Bezeichnung „Raum“ für technische Infrastruktur verwendet. Die Anforderungen des vorliegenden Bausteins sind jedoch auch auf Schränke übertragbar.

1.3. Abgrenzung und Modellierung

Der Baustein INF.5 *Raum sowie Schrank für technische Infrastruktur* ist für Räume anzuwenden, in denen technische Infrastruktur betrieben wird. Der Baustein ist ebenfalls anzuwenden, wenn stationäre Container, im Sinne eines großen Schrankes, betrieben werden.

In der Regel enthalten Räume für technische Infrastruktur ausschließlich technische Komponenten, die typischerweise nicht im Rechenzentrum selbst untergebracht werden (siehe Baustein INF.2 *Rechenzentrum sowie Serverraum*). Im Gegensatz zu Serverräumen enthalten sie nur in begründeten Ausnahmefällen IT-Systeme, die IT-Services erbringen. Eine solche Ausnahme sind kleine Informationsverbünde mit z. B. nur einem oder sehr wenigen Servern oder IT-Systemen. Ein Beispiel dafür ist etwa ein kleines mittelständisches Unternehmen mit wenigen IT-Arbeitsplätzen und einem Server, der in einem separaten Raum betrieben wird. In solchen Fällen genügt es oft, die Anforderungen des vorliegenden Bausteins anstatt des Bausteins INF.2 *Rechenzentrum sowie Serverraum* zu erfüllen. Anforderungen zur Verkabelung werden im Baustein INF.12 *Verkabelung* behandelt.

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.5 *Raum sowie Schrank für technische Infrastruktur* von besonderer Bedeutung.

2.1. Fehlerhafte Planung

Wird ein Raum für technische Infrastruktur fehlerhaft geplant, können mehrere Probleme auftreten. Zum einen kann Wasser eintreten oder die IT-Komponenten können durch Sonneneinstrahlung überhitzen, wenn die Lage des Raumes ungeeignet gewählt wird. Ebenso erhöht eine ungeeignete Lage unter Umständen die Wahrscheinlichkeit, dass dort eingebrochen wird. Auch können Engpässe auftreten, falls die Energieversorgung unzureichend dimensioniert wird. Wurden minderwertige Materialien verbaut, sind die IT-Komponenten oft anfälliger für Ausfälle und Fehlfunktionen. Nicht zuletzt können Regelungen und Vorschriften bereits bei der Planung nicht beachtet und eingehalten werden. Müssen nachträglich unzulässige Abweichungen behoben werden, können unnötig hohe Kosten entstehen.

2.2. Unberechtigter Zutritt

Gibt es keine Zutrittskontrolle oder keinen Einbruchschutz oder sind diese zu schwach, können möglicherweise unberechtigte Personen den Raum für technische Infrastruktur betreten. Sie könnten dort unbeabsichtigt, z. B. aufgrund mangelnder Fachkenntnisse, oder vorsätzlich Schaden anrichten, z. B. indem sie Geräte stehlen, austauschen, manipulieren oder zerstören.

2.3. Unzureichende Lüftung

Wird ein Raum für technische Infrastruktur unzureichend belüftet, kann es passieren, dass der für die verbauten Geräte erlaubte Temperaturbereich nicht eingehalten wird. Als Folge könnten diese Geräte ausfallen oder dauerhaft beschäftigt werden.

2.4. Feuer

Ein Raum für technische Infrastruktur kann durch ein Feuer schwer beschädigt oder ganz zerstört werden, sodass die von ihm abhängigen Geschäftsprozesse oder Fachaufgaben ausfallen. In einem Raum mit Energiekabeln und Stromverbrauchern besteht zum einen die Gefahr von Bränden, etwa wenn Leistungsschutzschalter oder Gerätesicherungen bei zu hohen Strömen nicht auslösen. Zum anderen kann auch Fahrlässigkeit zu Bränden führen, zum Beispiel wenn in dem Raum geraucht wird und Kabel und Geräte aus brennbarem Material Feuer fangen. Darüber hinaus können sich durch Überspannungen oder Überhitzung Funken bilden, die zu einem Brand führen. Ein Brand im Raum für

technische Infrastruktur kann sich zudem auch auf andere Teile des Gebäudes ausbreiten. Umgekehrt kann ein Feuer im Gebäude auch auf den Raum für technische Infrastruktur übergreifen.

2.5. Wasser

Durch eine Überschwemmung innerhalb des Raumes für technische Infrastruktur können sowohl an den dort betriebenen Komponenten als auch am Raum selbst Wasserschäden entstehen. Neben Schäden am Raum können diese Wasserschäden auch zu Kurzschlüssen in elektrischen Geräten führen. Als Folge können Schimmel und Korrosion auftreten. Durch ein Leck in einer Wasserleitung könnte der Raum auch überschwemmt werden. Auch Regenwasser, das bei Starkregen über überlastete Regenwasserkanäle in das Gebäude eindringt, kann zu einer Überschwemmung des Raumes führen.

2.6. Ausfall der Stromversorgung

Fällt die Stromversorgung des Raumes für technische Infrastruktur aus, sind davon meist mehrere elektrisch betriebene Komponenten betroffen. Das kann dazu führen, dass sämtliche damit verbundenen Betriebsabläufe gestoppt werden. Wird die Stromzufuhr plötzlich unterbrochen, kann dies zudem Schäden an den elektrotechnischen Komponenten verursachen, die sich auch dann noch auswirken, wenn die Stromversorgung wiederhergestellt wurde. Nicht zuletzt können auch Folgeschäden auftreten, wenn eine wichtige Komponente nicht einsatzbereit ist, wie z. B. die Lüftung. Erwärmt sich der Raum, können dadurch weitere Geräte beschädigt werden oder sogar ausfallen.

2.7. Blitzschlag und Überspannungen

Neben den Auswirkungen eines direkten Blitzeinschlags können durch die Induktionswirkung indirekter Blitze auch noch einige hundert Meter vom Einschlagsort entfernt Überspannungsspitzen entstehen. Die Induktion wirkt auch in der Nähe der Ableitungen der Blitzschutzanlage. Durch diese induktiven Überspannungsspitzen können unter Umständen Überspannungen auf Kabeltrassen und an elektrotechnischen Geräten innerhalb des Raumes für technische Infrastruktur auftreten, die dazu führen, dass Funktionen gestört werden oder Geräte ganz ausfallen.

2.8. Elektromagnetische Störfelder

Von einer Störquelle, wie z. B. Motoren von Aufzügen, Sendeanlagen oder Ableitungen von Blitzschutzanlagen, können elektromagnetische Felder ausgesendet werden. Diese können möglicherweise Schalter, Regler oder IT-Systeme stören. Diese Störspannung kann dazu führen, dass elektrotechnische Komponenten nicht mehr richtig funktionieren oder sogar ausfallen. Die Geräte innerhalb des Raumes für technische Infrastruktur können sich aber auch gegenseitig stören.

2.9. Elektrostatische Aufladung

Unkontrollierte elektrostatische Entladungen können Geräte mit empfindlichen elektronischen Bauteilen im Raum für technische Infrastruktur beschädigen oder zerstören. Das kann dazu führen, dass die Geräte nicht mehr zuverlässig funktionieren oder komplett ausfallen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.5 *Raum sowie Schrank für technische Infrastruktur* 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	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Mitarbeitende, Planende, IT-Betrieb, Haustechnik, Wartungspersonal

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.5.A1 Planung der Raumabsicherung (B) [Planende]

Für einen Raum für technische Infrastruktur MÜSSEN angemessene technische und organisatorische Vorgaben definiert und umgesetzt werden. Dabei MUSS das für den Raum zu erreichende Schutzniveau berücksichtigt werden. Bei der Planung MÜSSEN sowohl gesetzliche Regelungen und Vorschriften als auch potenzielle Gefährdungen durch Umwelteinflüsse, Einbruch und Sabotage beachtet werden.

INF.5.A2 Lage und Größe des Raumes für technische Infrastruktur (B) [Planende]

Der Raum für technische Infrastruktur DARF KEIN Durchgangsraum sein. Es MUSS sichergestellt sein, dass ausreichend Fläche für Fluchtwege und Arbeitsfläche vorhanden ist.

INF.5.A3 Zutrittsregelung und -kontrolle (B) [Haustechnik, IT-Betrieb]

Der Raum für technische Infrastruktur MUSS gegen unberechtigten Zutritt geschützt werden. Es MUSS geregelt werden, welche Personen für welchen Zeitraum, für welche Bereiche und zu welchem Zweck den Raum betreten dürfen. Dabei MUSS sichergestellt sein, dass keine unnötigen oder zu weitreichenden Zutrittsrechte vergeben werden. Alle Zutritte zum Raum für technische Infrastruktur SOLLTEN von der Zutrittskontrolle individuell erfasst werden.

INF.5.A4 Schutz vor Einbruch (B) [Planende, Haustechnik]

Der Raum MUSS vor Einbruch geschützt werden. Je nach erforderlichem Sicherheitsniveau des Raumes für technische Infrastruktur SOLLTEN geeignete raumbildende Teile wie Wände, Decken und Böden sowie Fenster und Türen mit entsprechenden Widerstandsklassen nach DIN EN 1627 ausgewählt werden.

INF.5.A5 Vermeidung sowie Schutz vor elektromagnetischen Störfeldern (B) [Planende]

Elektromagnetische Felder MÜSSEN in unmittelbarer Nähe zum Raum für technische Infrastruktur vermieden werden. Ein ausreichender Abstand zu großen Maschinen wie z. B. Aufzugsmotoren MUSS eingehalten werden.

INF.5.A6 Minimierung von Brandlasten (B) [Mitarbeitende, Planende]

Brandlasten innerhalb und in der direkten Umgebung des Raumes für technische Infrastruktur MÜSSEN auf ein Minimum reduziert werden. Auf brennbare Materialien für raumbildende Teile MUSS verzichtet werden.

INF.5.A7 Verhinderung von Zweckentfremdung (B) [Mitarbeitende, Planende]

Der Raum für technische Infrastruktur DARF NICHT zweckentfremdet werden, z. B. als Abstellraum oder Putzmittellager.

INF.5.A9 Stromversorgung (B) [Haustechnik]

Das Stromversorgungsnetz, über das der Raum für technische Infrastruktur und die daran angeschlossenen Endgeräte versorgt werden, MUSS als TN-S-System errichtet sein.

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.5.A8 Vermeidung von unkontrollierter elektrostatischer Entladung (S) [Planende]

Im Raum für technische Infrastruktur SOLLTE ein ableitfähiger Fußbodenbelag nach DIN EN 14041 verlegt werden.

INF.5.A10 Einhaltung der Lufttemperatur und -Feuchtigkeit (S) [Haustechnik]

Es SOLLTE sichergestellt werden, dass die Lufttemperatur und Luftfeuchtigkeit im Raum für technische Infrastruktur innerhalb der Grenzen liegen, die in den Datenblättern der darin betriebenen Geräte genannt sind. Dafür SOLLTE eine geeignete raumlufttechnische Anlage eingesetzt werden. Diese SOLLTE ausreichend dimensioniert sein.

INF.5.A11 Vermeidung von Leitungen mit gefährdenden Flüssigkeiten und Gasen (S) [Planende, Haustechnik]

Im Raum für technische Infrastruktur SOLLTE es nur Leitungen geben, die für den Betrieb der Technik im Raum unbedingt erforderlich sind. Leitungen wie Abwasserleitungen, Frischwasserleitungen, Gas- und Heizungsrohre sowie Leitungen für Treibstoff oder Ferndampf SOLLTEN NICHT durch den Raum geführt werden.

INF.5.A12 Schutz vor versehentlicher Beschädigung von Zuleitungen (S) [Planende]

Zuleitungen außerhalb des Raumes für technische Infrastruktur SOLLTEN gegen versehentliche Beschädigung geschützt werden.

INF.5.A13 Schutz vor Schädigung durch Brand und Rauchgase (S) [Planende, Haustechnik]

Unabhängig von den für den Raum geltenden baurechtlichen Brandschutzvorgaben SOLLTEN alle raumbildenden Teile sowie Türen und Fenster gleichwertig rauchdicht sein. Sie SOLLTEN Feuer und Rauch für mindestens 30 Minuten standhalten. Brandlasten im Bereich der Leitungstrassen SOLLTEN vermieden werden.

INF.5.A14 Minimierung von Brandgefahren aus Nachbarbereichen (S) [Planende, Haustechnik]

Der Raum SOLLTE NICHT in unmittelbarer Nähe zu anderen Räumlichkeiten mit brennbaren Materialien liegen, deren Menge über eine bürotypische Nutzung hinaus geht.

INF.5.A15 Blitz- und Überspannungsschutz (S) [Planende, Haustechnik]

Es SOLLTE ein Blitz- und Überspannungsschutzkonzept nach dem Prinzip der energetischen Koordination (siehe DIN EN 62305) erstellt und umgesetzt werden. Der Raum für technische

Infrastruktur SOLLTE mindestens der Blitzschutzzone 2 (LPZ 2) zugeordnet werden. Die Blitz- und Überspannungsschutzeinrichtungen SOLLTEN regelmäßig und anlassbezogen auf ihre Funktion überprüft und, falls erforderlich, ersetzt werden.

INF.5.A16 Einsatz einer unterbrechungsfreien Stromversorgung (S) [Haustechnik]

Es SOLLTE geprüft werden, welche Geräte an eine USV angeschlossen werden sollen. Falls eine USV erforderlich ist, SOLLTE die Stützzeit der USV so ausgelegt sein, dass alle versorgten Komponenten sicher herunterfahren können. Es SOLLTE berücksichtigt werden, dass die Batterien von USV-Anlagen altern.

Bei relevanten Änderungen SOLLTE überprüft werden, ob die vorhandenen USV-Anlagen noch ausreichend dimensioniert sind. Die Batterie der USV SOLLTE im erforderlichen Temperaturbereich gehalten werden.

Die USV SOLLTE regelmäßig gewartet und auf Funktionsfähigkeit getestet werden. Dafür SOLLTEN die vom herstellenden Unternehmen vorgesehenen Wartungsintervalle eingehalten werden.

INF.5.A17 Inspektion und Wartung der Infrastruktur (S) [Haustechnik, IT-Betrieb, Wartungspersonal]

Für alle Komponenten der baulich-technischen Infrastruktur SOLLTEN mindestens die vom herstellenden Unternehmen empfohlenen oder durch Normen festgelegten Intervalle und Vorschriften für Inspektion und Wartung eingehalten werden. Kabel- und Rohrdurchführungen durch brand- und rauchabschnittbegrenzende Wände SOLLTEN daraufhin geprüft werden, ob die Schotten die für den jeweiligen Einsatzzweck erforderliche Zulassung haben und unversehrt sind. Inspektionen und Wartungsarbeiten MÜSSEN geeignet protokolliert 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.5.A18 Lage des Raumes für technische Infrastruktur (H) [Planende]

Der Raum für technische Infrastruktur SOLLTE so im Gebäude angeordnet werden, dass er weder internen noch externen Gefährdungen wie z. B. Regen, Wasser oder Abwasser ausgesetzt ist. In oberirdischen Geschossen SOLLTE darauf geachtet werden, dass der Raum nicht durch Sonneneinstrahlung erwärmt wird. Wird der Raum im obersten Geschoss des Gebäudes untergebracht, SOLLTE sichergestellt werden, dass kein Wasser über das Dach eindringen kann.

INF.5.A19 Redundanz des Raumes für technische Infrastruktur (H) [Planende]

Der Raum SOLLTE redundant ausgelegt werden. Beide Räume SOLLTEN eine eigene Elektrounterverteilung erhalten, die direkt von der Niederspannungshauptverteilung (NSHV) versorgt wird. Beide Räume SOLLTEN unterschiedlichen Brandabschnitten zugeordnet sein und, sofern erforderlich, jeweils über eine eigene raumlufttechnische Anlage verfügen.

INF.5.A20 Erweiterter Schutz vor Einbruch und Sabotage (H) [Planende]

Der Raum SOLLTE fensterlos sein. Sind dennoch Fenster vorhanden, SOLLTEN sie je nach Geschosshöhe gegen Eindringen von außen angemessen gesichert sein. Gibt es neben Fenstern und Türen weitere betriebsnotwendige Öffnungen, wie z. B. Lüftungskanäle, SOLLTEN diese gleichwertig zur Raumhülle geschützt werden.

Es SOLLTEN Einbruchmeldeanlagen nach VdS Klasse C (gemäß VdS-Richtlinie 2311) eingesetzt werden. Alle erforderlichen Türen, Fenster und sonstige geschützte Öffnungen SOLLTEN über die

Einbruchmeldeanlage auf Verschluss, Verriegelung und Durchbruch überwacht werden. Vorhandene Fenster SOLLTEN stets geschlossen sein.

Die Widerstandsklasse von raumbildenden Teilen, Fenstern und Türen SOLLTE dem Sicherheitsbedarf des Raumes angepasst werden. Die Qualität der Schlösser, Schließzylinder und Schutzbeschläge SOLLTE der Widerstandsklasse der Tür entsprechen.

INF.5.A21 ENTFALLEN (H)

Diese Anforderung ist entfallen.

INF.5.A22 Redundante Auslegung der Stromversorgung (H) [Planende]

Die Stromversorgung SOLLTE durchgängig vom Niederspannungshauptverteiler (NSHV) bis zum Verbraucher im Raum für technische Infrastruktur zweizügig sein. Diese Stromversorgungen SOLLTEN sich in getrennten Brandabschnitten befinden. Der NSHV SOLLTE betriebsredundant ausgelegt sein.

INF.5.A23 Netzersatzanlage (H) [Planende, Haustechnik, Wartungspersonal]

Die Energieversorgung der Institution SOLLTE um eine Netzersatzanlage (NEA) ergänzt werden. Der Betriebsmittelvorrat einer NEA SOLLTE regelmäßig kontrolliert werden. Die NEA SOLLTE außerdem regelmäßig gewartet werden. Bei diesen Wartungen SOLLTEN auch Belastungs- und Funktionstests sowie Testläufe unter Last durchgeführt werden.

INF.5.A24 Lüftung und Kühlung (H) [Planende, Haustechnik, Wartungspersonal]

Die Lüftungs- und Kühltechnik SOLLTE betriebsredundant ausgelegt werden. Es SOLLTE sichergestellt werden, dass diese Anlagen regelmäßig gewartet werden.

Bei sehr hohem Schutzbedarf SOLLTE auch eine Wartungsredundanz vorhanden sein.

INF.5.A25 Erhöhter Schutz vor Schädigung durch Brand und Rauchgase (H) [Planende]

Raumbildende Teile sowie Türen, Fenster und Lüftungsklappen SOLLTEN Feuer und Rauch für mindestens 90 Minuten standhalten. Die Zuleitungen SOLLTEN einen Funktionserhalt von mindestens 90 Minuten gewährleisten.

Bei sehr hohem Schutzbedarf SOLLTE die Raumhülle wie ein eigener Brandabschnitt ausgebildet sein. In vorhandenen Lüftungskanälen SOLLTEN Brandschutzklappen eingebaut werden, die über Rauchmelder angesteuert werden. Trassen SOLLTEN bis zum Eintritt in den Raum in getrennten Brandabschnitten geführt werden.

Bei sehr hohem Schutzbedarf SOLLTEN ein Brandfrühesterkennungssystem und eine automatische Löschanlage vorhanden sein. Brand- und Rauchmelder SOLLTEN an die Brandmelderzentrale angeschlossen sein. Das Brandfrühesterkennungssystem und die automatische Löschanlage SOLLTEN an die zweizügige Stromversorgung mit USV und NEA angebunden sein.

INF.5.A26 Überwachung der Energieversorgung (H) [Planende, Haustechnik]

Es SOLLTEN geeignete Überwachungseinrichtungen eingebaut und betrieben werden, die unzulässig hohe Ströme auf dem Schutzleitersystem und damit auf Leitungsschirmen sowie potenziell störende Oberschwingungen erfassen und an geeigneter Stelle zur Nachverfolgung und Behebung anzeigen können.

4. Weiterführende Informationen

4.1. Wissenswertes

Die Deutsche Gesetzliche Unfallversicherung macht in ihrer Vorschrift „DGUV Vorschrift 4 Unfallverhütungsvorschrift, Elektrische Anlagen und Betriebsmittel“ Vorgaben zum richtigen Umgang mit Betriebsmitteln.

Das Deutsche Institut für Normung macht in seiner Norm „DIN EN 14041:2018-05“ Vorgaben zu Bodenbelägen.

Das Deutsche Institut für Normung macht in seiner Norm „DIN EN 1627:2021-11“ Vorgaben zur physischen Sicherheit von Gebäuden und Räumen.

Das Deutsche Institut für Normung macht in seiner Norm „DIN EN 4102:2016-05“ Vorgaben zum Brandverhalten von Baustoffen und Bauteilen.

Die International Electrotechnical Commission macht in ihrem „Merkblatt 62305“ Anmerkungen zu Blitzschutznormen.

Die VdS Schadenverhütung GmbH macht in ihrer „Richtlinie VdS 2311:2021-10“ Vorgaben zum Einsatz von Einbruchmeldeanlagen.

Bundesamt
für Sicherheit in der
Informationstechnik

INF.6 Datenträgerarchiv

1. Beschreibung

1.1. Einleitung

Datenträgerarchive sind abgeschlossene Räumlichkeiten innerhalb einer Institution, in denen Datenträger jeder Art gelagert werden. Dazu gehören neben Datenträgern, auf denen digitale Informationen abgespeichert sind, auch Papierdokumente, Filme oder sonstige Medien.

1.2. Zielsetzung

In diesem Baustein werden die typischen Gefährdungen und Anforderungen bezüglich der Informationssicherheit für ein Datenträgerarchiv beschrieben. Ziel ist der Schutz der Informationen, die sich auf den dort archivierten Datenträgern und weiteren Medien befinden.

1.3. Abgrenzung und Modellierung

Der Baustein INF.6 *Datenträgerarchiv* ist für alle Räume anzuwenden, die als Archiv von Datenträgern genutzt werden.

Dieser Baustein betrachtet technische und nichttechnische Sicherheitsanforderungen für Datenträgerarchive. Empfehlungen zur korrekten Archivierung werden in diesem Baustein nicht behandelt. Hinweise dazu finden sich im Baustein OPS.1.2.2 *Archivierung*.

Im Rahmen des IT-Grundschutzes werden an die Archivräume hinsichtlich des Brandschutzes keine erhöhten Anforderungen gestellt. Zusätzliche Anforderungen an den Brandschutz können aber durch die Behältnisse erfüllt werden, in denen die Datenträger aufbewahrt werden.

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.6 *Datenträgerarchiv* von besonderer Bedeutung.

2.1. Unzulässige Temperatur und Luftfeuchtigkeit

Bei der Lagerung von digitalen Langzeitspeichermedien können Temperaturschwankungen oder zu hohe Luftfeuchtigkeit zu Datenfehlern und reduzierter Speicherdauer führen.

2.2. Fehlende oder unzureichende Regelungen

Wenn Mitarbeitende die Fenster und Türen nach Verlassen des Datenträgerarchivs nicht schließen oder verschließen, können Datenträger oder andere Informationen entwendet werden. Sensible Informationen könnten dann von unberechtigten Personen eingesehen oder weitergegeben werden. Wenn Mitarbeitenden die entsprechenden Regelungen nicht hinreichend bekannt sind, können Sicherheitslücken auftreten. Regelungen lediglich festzulegen ist nicht ausreichend. Sie müssen beachtet werden, damit der Betrieb störungsfrei ist. Viele Probleme entstehen, wenn Regelungen zwar vorhanden, aber nicht bekannt sind.

2.3. Unbefugter Zutritt zu schutzbedürftigen Räumen

Fehlen Zutrittskontrollen oder sind diese unzureichend, können unberechtigte Personen ein Datenträgerarchiv betreten und schützenswerte Informationen einsehen, entwenden oder manipulieren. Dadurch kann die Verfügbarkeit, Vertraulichkeit und Integrität der archivierten Informationen beeinträchtigt werden. Selbst wenn keine unmittelbaren Schäden zu erkennen sind, kann der Betriebsablauf gestört werden.

2.4. Diebstahl

Da viele Datenträger sehr handlich sind, ist es umso leichter, sie unbemerkt in eine Tasche oder unter die Kleidung zu stecken und mitzunehmen. Gibt es keine Kopien von den Informationen, sind die auf den gestohlenen Datenträgern abgespeicherten Informationen verloren. Darüber hinaus könnten die Personen, die Datenträger entwendet haben, vertrauliche Informationen einsehen und offenlegen. Dadurch können weitere Schäden entstehen. Diese wiegen in den meisten Fällen deutlich schwerer als die Kosten von ersatzweise angeschafften Datenträgern.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.6 *Datenträgerarchiv* 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	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Mitarbeitende, Planende, Haustechnik, Brandschutzbeauftragte

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.6.A1 Handfeuerlöscher (B) [Brandschutzbeauftragte]

Im Brandfall MÜSSEN im Datenträgerarchiv geeignete Handfeuerlöscher leicht erreichbar sein. Diese Handfeuerlöscher MÜSSEN regelmäßig inspiziert und gewartet werden. Mitarbeitende, die in der Nähe eines Datenträgerarchivs tätig sind, MÜSSEN in die Benutzung der Handfeuerlöscher eingewiesen werden.

INF.6.A2 Zutrittsregelung und -kontrolle (B) [Haustechnik]

Der Zutritt zum Datenträgerarchiv DARF NUR für befugte Personen möglich sein. Der Zutritt MUSS auf ein Mindestmaß an Mitarbeitenden reduziert sein. Daher MUSS der Zutritt geregelt und kontrolliert werden. Für die Zutrittskontrolle MUSS ein Konzept entwickelt werden. Die darin festgelegten Maßnahmen für die Zutrittskontrolle SOLLTEN regelmäßig daraufhin überprüft werden, ob sie noch wirksam sind. Um es zu erschweren bzw. zu verhindern, dass eine Zutrittskontrolle umgangen wird, MUSS der komplette Raum einen dem Schutzbedarf genügenden mechanischen Widerstand aufweisen, der keinesfalls unter RC2 (gemäß DIN EN 1627) liegen darf.

INF.6.A3 Schutz vor Staub und anderer Verschmutzung (B)

Es MUSS sichergestellt werden, dass die Datenträger im Datenträgerarchiv ausreichend vor Staub und Verschmutzung geschützt sind. Die Anforderungen dafür MÜSSEN bereits in der Planungsphase analysiert werden. Es MUSS in Datenträgerarchiven ein striktes Rauchverbot eingehalten werden.

INF.6.A4 Geschlossene Fenster und abgeschlossene Türen (B) [Mitarbeitende]

In einem Datenträgerarchiv SOLLTEN, wenn möglich, keine Fenster vorhanden sein. Gibt es dennoch Fenster, MÜSSEN diese beim Verlassen des Datenträgerarchivs geschlossen werden. Ebenso MUSS beim Verlassen die Tür verschlossen werden. Auch Brand- und Rauchschutztüren MÜSSEN geschlossen 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.6.A5 Verwendung von Schutzschränken (S) [Mitarbeitende]

Die Datenträger und Medien in Datenträgerarchiven SOLLTEN in geeigneten Schutzschränken gelagert werden.

INF.6.A6 Vermeidung von wasserführenden Leitungen (S) [Haustechnik]

In Datenträgerarchiven SOLLTEN unnötige wasserführende Leitungen generell vermieden werden. Sind dennoch Wasserleitungen durch das Datenträgerarchiv hinweg verlegt, SOLLTEN diese regelmäßig daraufhin überprüft werden, ob sie noch dicht sind. Zudem SOLLTEN Vorkehrungen getroffen werden, um frühzeitig erkennen zu können, ob dort Wasser austritt. Für ein Datenträgerarchiv mit Hochverfügbarkeitsanforderungen SOLLTE es Reaktionspläne geben, die genau vorgeben, wer im Fall eines Lecks informiert werden muss und wie grundsätzlich vorzugehen ist.

INF.6.A7 Einhaltung von klimatischen Bedingungen (S) [Haustechnik]

Es SOLLTE sichergestellt werden, dass die zulässigen Höchst- und Tiefstwerte für Temperatur und Luftfeuchtigkeit sowie der Schwebstoffanteil in der Raumluft im Datenträgerarchiv eingehalten werden. Die Werte von Lufttemperatur und -feuchte SOLLTEN mehrmals im Jahr für die Dauer von einer Woche aufgezeichnet und dokumentiert werden. Dabei festgestellte Abweichungen vom Sollwert

SOLLTEN zeitnah behoben werden. Die eingesetzten Klimageräte SOLLTEN regelmäßig gewartet werden.

INF.6.A8 Sichere Türen und Fenster (S) [Planende]

Sicherungsmaßnahmen wie Fenster, Türen und Wände SOLLTEN bezüglich Einbruch, Brand und Rauch gleichwertig und angemessen sein. Abhängig vom Schutzbedarf SOLLTE eine geeignete Widerstandsklasse gemäß der DIN EN 1627 erfüllt werden. Alle Sicherheitstüren und -fenster SOLLTEN regelmäßig daraufhin überprüft werden, ob sie noch entsprechend funktionieren. Der komplette Raum SOLLTE einen dem Schutzbedarf genügenden mechanischen Widerstand aufweisen, der keinesfalls unter RC3 (gemäß DIN EN 1627) liegt.

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.6.A9 Gefahrenmeldeanlage (H) [Haustechnik]

Es SOLLTE in Datenträgerarchiven eine angemessene Gefahrenmeldeanlage eingerichtet werden. Diese Gefahrenmeldeanlage SOLLTE regelmäßig geprüft und gewartet werden. Es SOLLTE sichergestellt sein, dass diejenigen Personen, die Gefahrenmeldungen empfangen in der Lage sind, auf Alarmmeldungen angemessen zu reagieren.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Deutsche Institut für Normung macht in seiner Norm „DIN EN 1627:2021-11“ Vorgaben zur physischen Sicherheit von Gebäuden und Räumen.

Bundesamt
für Sicherheit in der
Informationstechnik

INF.7 Büroarbeitsplatz

1. Beschreibung

1.1. Einleitung

Ein Büroraum ist der Bereich innerhalb einer Institution, in dem sich ein, eine oder mehrere Mitarbeitende aufhalten, um dort ihre Aufgaben zu erfüllen. In diesem Baustein werden die typischen Gefährdungen und Anforderungen bezüglich der Informationssicherheit für einen Büroraum beschrieben.

1.2. Zielsetzung

Ziel des Bausteins ist der Schutz der Informationen, die in Büroräumen bearbeitet werden.

1.3. Abgrenzung und Modellierung

Der Baustein INF.7 *Büroarbeitsplatz* ist auf jeden Raum im Informationsverbund anzuwenden, der als Büroarbeitsplatz genutzt wird.

Dieser Baustein betrachtet technische und nichttechnische Sicherheitsanforderungen für Büroräume. Empfehlungen, wie die IT-Systeme in diesen Räumen konfiguriert und abgesichert werden können, werden in diesem Baustein nicht behandelt. Hinweise dafür sind unter anderem im Baustein SYS.2.1 *Allgemeiner Client* sowie in den betriebssystemspezifischen Bausteinen zu finden.

Anforderungen an Gebäude im Allgemeinen sind nicht Teil dieses Bausteins. Diese sind im Baustein INF.1 *Allgemeines Gebäude* zu finden, der immer auf Räume und Gebäude anzuwenden ist. Auch auf die Verkabelung von Büroräumen wird nicht eingegangen. Dazu muss der Baustein INF.12 *Verkabelung* betrachtet werden.

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.7 *Büroarbeitsplatz* von besonderer Bedeutung.

2.1. Unbefugter Zutritt

Fehlen Zutrittskontrollen oder sind diese unzureichend, können unberechtigte Personen einen Büroraum betreten und schützenswerte Daten entwenden, Geräte stehlen oder sie manipulieren. Dadurch kann die Verfügbarkeit, Vertraulichkeit oder Integrität von Geräten und Informationen beeinträchtigt werden. Selbst wenn keine unmittelbaren Schäden erkennbar sind, kann der Betriebsablauf gestört werden. Beispielsweise muss untersucht werden, wie ein solcher Vorfall möglich war, ob Schäden aufgetreten sind oder Manipulationen vorgenommen wurden.

2.2. Beeinträchtigung durch ungünstige Arbeitsbedingungen

Ein nicht nach ergonomischen Gesichtspunkten eingerichteter Büroraum oder ein ungünstiges Arbeitsumfeld sind problematisch. Beides kann dazu führen, dass Mitarbeitende dort nicht ungestört arbeiten oder die verwendete IT nicht oder nicht optimal benutzen können. Störungen können Lärm, starker Kundschaftsverkehr, eine ungünstige Beleuchtung oder eine schlechte Belüftung sein. Dadurch können Arbeitsabläufe und das Potential der Mitarbeitenden eingeschränkt werden. Es können sich bei der Arbeit auch Fehler einschleichen, wodurch die Integrität von Daten vermindert werden kann.

2.3. Manipulationen durch Reinigungs- und Fremdpersonal oder Besuchende

Bei kleineren bzw. kurzen Besprechungen ist es meist effizienter, den Besuch im Büro zu empfangen. Dabei könnte jedoch der Besuch, ebenso wie auch Reinigungs- und Fremdpersonal, auf verschiedene Art und Weise interne Informationen einsehen, Geschäftsprozesse gefährden und IT-Systeme manipulieren. Angefangen von der unsachgemäßen Behandlung der technischen Einrichtungen über den Versuch des „Spielens“ an IT-Systemen bis zum Diebstahl von Unterlagen oder IT-Komponenten ist vieles möglich. So kann beispielsweise vom Reinigungspersonal versehentlich eine Steckverbindung gelöst werden oder Wasser in die IT gelangen. Auch können Unterlagen verlegt oder sogar mit dem Abfall entsorgt werden.

2.4. Manipulation oder Zerstörung von IT, Zubehör, Informationen und Software im Büroraum

Angreifende können aus unterschiedlichen Gründen heraus versuchen, IT-Systeme, Zubehör und andere Datenträger zu manipulieren oder zu zerstören. Die Angriffe sind umso wirkungsvoller, je später sie von Mitarbeitenden oder der Institution selbst entdeckt werden, je umfassender die Kenntnisse der Täter und je tiefgreifender die Folgen für einen Arbeitsvorgang sind. Es könnten etwa unerlaubt schützenswerte Daten der Mitarbeitenden eingesehen werden. Auch könnten Datenträger oder IT-Systeme zerstört werden. Erhebliche Ausfallzeiten und Prozesseinschränkungen könnten die Folge sein.

2.5. Diebstahl

Da IT-Geräte immer handlicher werden, ist es umso leichter, sie unbemerkt in die Tasche zu stecken. Durch den Diebstahl von Datenträgern, IT-Systemen, Zubehör, Software oder Informationen entstehen einerseits Kosten für die Wiederbeschaffung. Aber auch für die Wiederherstellung eines arbeitsfähigen Zustandes sind Ressourcen nötig. Auf der anderen Seite können auch Verluste aufgrund mangelnder Verfügbarkeit entstehen. Darüber hinaus könnte die Person, die die IT-Geräte entwendet hat, vertrauliche Information einsehen und offenlegen. Dadurch können weitere Schäden entstehen. Diese wiegen in vielen Fällen deutlich schwerer als der rein materielle Verlust des IT-Gerätes.

Gestohlen werden neben teuren IT-Systemen häufig auch mobile Endgeräte, die unauffällig und leicht transportiert werden können. Wenn die Büroräume nicht verschlossen, nicht beaufsichtigt oder die IT-

Systeme nicht ausreichend gesichert sind, kann die Technik dementsprechend schnell und unauffällig entwendet werden.

2.6. Fliegende Verkabelung

Je nachdem, wo die Anschlusspunkte der Steckdosen, der Stromversorgung und des Datennetzes im Büroraum liegen, könnten Kabel quer durch den Raum verlegt werden, auch über Verkehrswege hinweg. Solche „fliegenden" Kabel sind nicht nur Stolperfallen, an denen sich Personen verletzen können. Wenn Personen daran hängen bleiben, können auch IT-Geräte beschädigt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.7 *Büroarbeitsplatz* 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	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Mitarbeitende, Zentrale Verwaltung, Haustechnik, Vorgesetzte

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.7.A1 Geeignete Auswahl und Nutzung eines Büroraumes (B) [Vorgesetzte]

Es DÜRFEN NUR geeignete Räume als Büroräume genutzt werden. Die Büroräume MÜSSEN für den Schutzbedarf bzw. das Schutzniveau der dort verarbeiteten Informationen angemessen ausgewählt und ausgestattet sein. Büroräume mit Publikumsverkehr DÜRFEN NICHT in sicherheitsrelevanten Bereichen liegen. Für den Arbeitsplatz und für die Einrichtung eines Büroraumes MUSS die Arbeitsstättenverordnung umgesetzt werden.

INF.7.A2 Geschlossene Fenster und abgeschlossene Türen (B) [Mitarbeitende, Haustechnik]

Wenn Mitarbeitende ihre Büroräume verlassen, SOLLTEN alle Fenster geschlossen werden. Befinden sich vertrauliche Informationen in dem Büroraum, MÜSSEN beim Verlassen die Türen abgeschlossen werden. Dies SOLLTE insbesondere in Bereichen mit Publikumsverkehr beachtet werden. Die entsprechenden Vorgaben SOLLTEN in einer geeigneten Anweisung festgehalten werden. Alle Mitarbeitenden SOLLTEN dazu verpflichtet werden, der Anweisung nachzukommen. Zusätzlich MUSS regelmäßig geprüft werden, ob beim Verlassen des Büroraums die Fenster geschlossen und, wenn notwendig, die Türen abgeschlossen werden. Ebenso MUSS darauf geachtet werden, dass Brand- und Rauchschutztüren tatsächlich geschlossen 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.7.A3 Fliegende Verkabelung (S)

Die Stromanschlüsse und Zugänge zum Datennetz im Büroraum SOLLTEN sich dort befinden, wo die IT-Geräte aufgestellt sind. Verkabelungen, die über den Boden verlaufen, SOLLTEN geeignet abgedeckt werden.

INF.7.A4 ENTFALLEN (S)

Diese Anforderung ist entfallen.

INF.7.A5 Ergonomischer Arbeitsplatz (S) [Zentrale Verwaltung, Vorgesetzte]

Die Arbeitsplätze aller Mitarbeitenden SOLLTEN ergonomisch eingerichtet sein. Vor allem die Bildschirme SOLLTEN so aufgestellt werden, dass ein ergonomisches und ungestörtes Arbeiten möglich ist. Dabei SOLLTE beachtet werden, dass Bildschirme nicht durch Unbefugte eingesehen werden können. Die Bildschirmarbeitsschutzverordnung (BildscharbV) SOLLTE umgesetzt werden. Alle Arbeitsplätze SOLLTEN für eine möglichst fehlerfreie Bedienung der IT individuell verstellbar sein.

INF.7.A6 Aufgeräumter Arbeitsplatz (S) [Mitarbeitende, Vorgesetzte]

Alle Mitarbeitenden SOLLTEN dazu angehalten werden, seinen Arbeitsplatz aufgeräumt zu hinterlassen. Die Mitarbeitenden SOLLTEN dafür sorgen, dass Unbefugte keine vertraulichen Informationen einsehen können. Alle Mitarbeitenden SOLLTEN ihre Arbeitsplätze sorgfältig überprüfen und sicherstellen, dass keine vertraulichen Informationen frei zugänglich sind. Vorgesetzte SOLLTEN Arbeitsplätze sporadisch daraufhin überprüfen, ob dort schutzbedürftige Informationen offen zugreifbar sind.

INF.7.A7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger (S) [Mitarbeitende, Haustechnik]

Die Mitarbeitenden SOLLTEN angewiesen werden, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn sie nicht verwendet werden. Dafür SOLLTEN geeignete Behältnisse in den Büroräumen oder in deren Umfeld aufgestellt 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.7.A8 Einsatz von Diebstahlsicherungen (H) [Mitarbeitende]

Wenn der Zutritt zu den Räumen nicht geeignet beschränkt werden kann, SOLLTEN für alle IT-Systeme Diebstahlsicherungen eingesetzt werden. In Bereichen mit Publikumsverkehr SOLLTEN Diebstahlsicherungen benutzt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

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 und Räumen.

Das Deutsche Institut für Normung macht in seiner Norm „DIN EN 1627:2021-11“ Vorgaben zur physischen Sicherheit von Gebäuden und Räumen.

Das Bundesministerium für Arbeit und Soziales macht in seiner Arbeitsstättenverordnung Vorgaben zum Einrichten und Betreiben von Arbeitsstätten in Bezug auf die Sicherheit und den Schutz der Gesundheit von Beschäftigten.

Bundesamt
für Sicherheit in der
Informationstechnik

INF.8 Häuslicher Arbeitsplatz

1. Beschreibung

1.1. Einleitung

Telearbeitende, freie Mitarbeitende oder Selbstständige arbeiten typischerweise von häuslichen Arbeitsplätzen aus. Im Gegensatz zum Arbeitsplatz im Büro nutzen diese Mitarbeitenden einen Arbeitsplatz in der eigenen Immobilie. Dabei muss ermöglicht werden, dass die berufliche Umgebung hinreichend von der privaten getrennt ist. Wenn Mitarbeitende häusliche Arbeitsplätze dauerhaft benutzen, müssen zudem diverse rechtliche Anforderungen erfüllt sein, beispielsweise müssen die Arbeitsplätze arbeitsmedizinischen und ergonomischen Bestimmungen entsprechen.

Bei einem häuslichen Arbeitsplatz kann nicht die gleiche infrastrukturelle Sicherheit vorausgesetzt werden, wie sie in den Büroräumen einer Institution anzutreffen ist. So ist z. B. der Arbeitsplatz oft auch für Besuch oder Familienangehörige zugänglich. Deshalb müssen Maßnahmen ergriffen werden, mit denen sich ein Sicherheitsniveau erreichen lässt, das mit einem Büroraum vergleichbar ist.

1.2. Zielsetzung

In diesem Baustein wird aufgezeigt, wie sich die Infrastruktur eines häuslichen Arbeitsplatzes sicher aufbauen und betreiben lässt. Kernziel des Bausteins ist der Schutz der Informationen der Institution am häuslichen Arbeitsplatz.

1.3. Abgrenzung und Modellierung

Der Baustein INF.8 *Häuslicher Arbeitsplatz* ist für alle Räume anzuwenden, die als Telearbeitsplatz genutzt werden.

Der Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, um den Gefährdungen für einen häuslichen Arbeitsplatz entgegenwirken zu können. Dabei werden jedoch nur spezifische Anforderungen an die Infrastruktur für einen ortsfesten Arbeitsplatz mit Zugang durch Dritte definiert. Sicherheitsanforderungen für die eingesetzten IT-Systeme, z. B. Clients und Multifunktionsgeräte und insbesondere für die technischen Anteile der Telearbeit, z. B. Kommunikationsverbindungen, sind dagegen nicht Gegenstand des vorliegenden Bausteins. Sie werden im Baustein OPS.1.2.4 *Telearbeit* bzw. in den jeweiligen systemspezifischen Bausteinen beschrieben.

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.8 *Häuslicher Arbeitsplatz* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Regelungen für den häuslichen Arbeitsplatz

Da ein häuslicher Arbeitsplatz außerhalb der Institution liegt, sind die Mitarbeitenden dort weitgehend auf sich allein gestellt. Dadurch können durch fehlende oder unzureichende Regelungen für das häusliche Arbeitsplatzumfeld IT-Probleme mit höheren Ausfallzeiten entstehen. Wenn IT-Probleme nicht per Fernadministration geklärt werden können, muss beispielsweise eine Person vom IT-Betrieb aus der Institution erst zum häuslichen Arbeitsplatz fahren, um dort die Probleme zu beseitigen. Wenn der Umgang mit internen und vertraulichen Informationen am häuslichen Arbeitsplatz nicht nachvollziehbar geregelt ist, könnten Mitarbeitende solche Informationen falsch aufbewahren. Wenn nicht verhindert werden kann, dass Informationen ausgespäht oder modifiziert werden, kann die Vertraulichkeit und Integrität der Informationen gefährdet sein.

2.2. Unbefugter Zutritt zu schutzbedürftigen Räumen des häuslichen Arbeitsplatzes

Räume eines häuslichen Arbeitsplatzes, in denen schutzbedürftige Informationen aufbewahrt und weiterverarbeitet werden oder in denen schutzbedürftige Geräte aufbewahrt oder betrieben werden, werden dadurch zu schutzbedürftigen Räumen. Wenn unbefugte Personen diese Räume unbeaufsichtigt betreten können, ist die Vertraulichkeit, Integrität und Verfügbarkeit dieser Daten und Informationen erheblich gefährdet.

Beispiele:

- Ein Heimarbeitsplatz befindet sich zwar in einem separaten Arbeitszimmer, ist aber nicht konsequent abgeschlossen. Als kleine Kinder kurz unbeaufsichtigt waren, spielten sie in dem nicht verschlossenen Arbeitszimmer. Dabei wurden wichtige Dokumente als Malgrundlage verwendet.
- Als eine Person am häuslichen Arbeitsplatz in eine Projektarbeit vertieft war, traf überraschend Besuch ein. Während die Person in der Küche Kaffee kochte, wollte der Besuch am nicht gesperrten Client schnell etwas im Internet recherchieren und hat diesen dabei versehentlich mit Schadsoftware infiziert.

2.3. Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen am häuslichen Arbeitsplatz

Ein nicht nach ergonomischen Gesichtspunkten eingerichteter häuslicher Arbeitsplatz oder ein ungünstiges Arbeitsumfeld können dazu führen, dass dort nicht ungestört gearbeitet werden kann. Auch die verwendete IT kann möglicherweise nicht oder nicht optimal benutzt werden. Ungünstig auswirken können sich etwa Lärm, Störungen durch Familienmitglieder sowie eine schlechte Beleuchtung oder Belüftung. Dadurch werden Arbeitsabläufe und Potenziale der Mitarbeitenden eingeschränkt. Es könnten sich bei der Arbeit auch Fehler einschleichen. Außerdem kann der Schutz der Integrität von Daten vermindert werden.

2.4. Ungesicherter Akten- und Datenträgertransport

Wenn Dokumente, Datenträger oder Akten zwischen der Institution und dem häuslichen Arbeitsplatz transportiert werden, können diese Daten und Informationen verlorengehen. Auch könnten sie von unbefugten Dritten entwendet, gelesen oder manipuliert werden. Der Akten- und Datenträgertransport kann auf verschiedene Arten unzureichend gesichert sein:

- Werden Unikate transportiert und fehlt ein entsprechendes Backup, können Ziele und Aufgaben nicht wie geplant erreicht werden, wenn das Unikat verlorengeht.
- Fallen unverschlüsselte Datenträger in falsche Hände, kann das zu einem schwerwiegenden Verlust der Vertraulichkeit führen.
- Wenn unterwegs kein ausreichender Zugriffsschutz vorhanden ist, können Akten oder Datenträger unbemerkt kopiert oder manipuliert werden.

2.5. Ungeeignete Entsorgung der Datenträger und Dokumente

Ist es am häuslichen Arbeitsplatz nicht möglich, Datenträger und Dokumente in geeigneter Weise zu entsorgen, könnten sie einfach in den Hausmüll geworfen werden. Hieraus können jedoch wertvolle Informationen gewonnen werden, die sich gezielt für Erpressungsversuche oder zur Wirtschaftsspionage missbrauchen lassen. Die Folgen reichen vom Wissensverlust bis zur Existenzgefährdung der Institution, z. B. wenn dadurch wichtige Aufträge nicht zustande kommen oder geschäftliche Partnerschaften scheitern.

2.6. Manipulation oder Zerstörung von IT, Zubehör, Informationen und Software am häuslichen Arbeitsplatz

IT-Geräte, Zubehör, Informationen und Software, die am häuslichen Arbeitsplatz benutzt werden, können unter Umständen einfacher manipuliert oder zerstört werden als in der Institution. Der häusliche Arbeitsplatz ist oft für Angehörige und Besuch der Familie zugänglich. Auch sind hier die zentralen Schutzmaßnahmen der Institution nicht vorhanden, zum Beispiel Pfortendienste. Wenn IT-Geräte, Zubehör, Informationen oder Software manipuliert oder zerstört werden, sind Mitarbeitende am häuslichen Arbeitsplatz oft nur noch eingeschränkt arbeitsfähig. Des Weiteren müssen womöglich zerstörte IT-Komponenten, Informationen und Softwarelösungen ersetzt werden, was sowohl finanzielle als auch zeitliche Ressourcen erfordert.

2.7. Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz

Der häusliche Arbeitsplatz ist meistens nicht so gut abgesichert wie der Arbeitsplatz in einem Unternehmen oder in einer Behörde. Durch aufwendige Vorkehrungen wie z. B. Sicherheitstüren oder einem Pfortendienst ist dort die Gefahr, dass jemand unbefugt in das Gebäude eindringt, weitaus geringer als bei einem Privathaus. Bei einem Einbruch werden meistens vorrangig Gegenstände gestohlen, die schnell und einfach verkauft werden können. Dabei kann auch dienstliche IT gestohlen werden. Die auf den entwendeten dienstlichen IT-Systemen vorhandenen Informationen besitzen aber oft einen höheren Wert als die IT-Systeme selbst. Dritte könnten versuchen, durch Erpressung oder Weitergabe der Daten an Konkurrenzunternehmen einen höheren Gewinn als durch den Verkauf der Hardware zu erzielen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.8 *Häuslicher Arbeitsplatz* 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	Mitarbeitende
Weitere Zuständigkeiten	Keine

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.8.A1 Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz (B)

Dienstliche Unterlagen und Datenträger MÜSSEN am häuslichen Arbeitsplatz so aufbewahrt werden, dass keine unbefugten Personen darauf zugreifen können. Daher MÜSSEN ausreichend verschließbare Behältnisse (z. B. abschließbare Rollcontainer oder Schränke) vorhanden sein. Alle Mitarbeitenden MÜSSEN ihre Arbeitsplätze aufgeräumt hinterlassen und sicherstellen, dass keine vertraulichen Informationen frei zugänglich sind.

INF.8.A2 Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz (B)

Es MUSS geregelt werden, welche Datenträger und Unterlagen am häuslichen Arbeitsplatz bearbeitet und zwischen der Institution und dem häuslichen Arbeitsplatz hin und her transportiert werden dürfen. Generell MÜSSEN Datenträger und andere Unterlagen sicher transportiert werden. Diese Regelungen MÜSSEN den Mitarbeitenden in geeigneter Weise bekanntgegeben werden.

INF.8.A3 Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz (B)

Den Mitarbeitenden MUSS mitgeteilt werden, welche Regelungen und Maßnahmen zum Einbruchs- und Zutrittsschutz zu beachten sind. So MUSS darauf hingewiesen werden, Fenster zu schließen und Türen abzuschließen, wenn der häusliche Arbeitsplatz nicht besetzt ist.

Es MUSS sichergestellt werden, dass unbefugte Personen zu keiner Zeit den häuslichen Arbeitsplatz betreten und auf dienstliche IT und Unterlagen zugreifen können. Diese Maßnahmen MÜSSEN in sinnvollen zeitlichen Abständen überprüft werden, mindestens aber, wenn sich die häuslichen Verhältnisse ändern.

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.8.A4 Geeignete Einrichtung des häuslichen Arbeitsplatzes (S)

Der häusliche Arbeitsplatz SOLLTE durch eine geeignete Raumaufteilung von den privaten Bereichen der Wohnung getrennt sein. Der häusliche Arbeitsplatz SOLLTE mit Büromöbeln eingerichtet sein, die ergonomischen Anforderungen entsprechen.

Ebenso SOLLTE der häusliche Arbeitsplatz durch geeignete technische Sicherungsmaßnahmen vor Einbrüchen geschützt werden. Die Schutzmaßnahmen SOLLTEN an die örtlichen Gegebenheiten und den vorliegenden Schutzbedarf angepasst sein.

INF.8.A5 Entsorgung von vertraulichen Informationen am häuslichen Arbeitsplatz (S)

Vertrauliche Informationen SOLLTEN sicher entsorgt werden. In einer speziellen Sicherheitsrichtlinie SOLLTE daher geregelt werden, wie schutzbedürftiges Material zu beseitigen ist. Es SOLLTEN die dafür benötigten Entsorgungsmöglichkeiten verfügbar sein.

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.8.A6 Umgang mit dienstlichen Unterlagen bei erhöhtem Schutzbedarf am häuslichen Arbeitsplatz (H)

Wenn Informationen mit erhöhtem Schutzbedarf bearbeitet werden, SOLLTE überlegt werden, von einem häuslichen Arbeitsplatz ganz abzusehen. Anderenfalls SOLLTE der häusliche Arbeitsplatz durch erweiterte, hochwertige technische Sicherungsmaßnahmen geschützt werden.

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 und Räumen.

Das Deutsche Institut für Normung macht in seiner Norm „DIN EN 1627:2011-09“ Vorgaben zur physischen Sicherheit von Gebäuden und Räumen.

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 F-PS Vorgaben zur physischen Sicherheit und Umgebungssicherheit von Gebäuden.

Bundesamt
für Sicherheit in der
Informationstechnik

INF.9 Mobiler Arbeitsplatz

1. Beschreibung

1.1. Einleitung

Eine gute Netzabdeckung sowie leistungsfähige IT-Geräte, wie z. B. Laptops, Smartphones oder Tablets, ermöglichen es Mitarbeitenden, nahezu an jedem Platz bzw. von überall zu arbeiten. Das bedeutet, dass dienstliche Aufgaben häufig nicht mehr nur in den Räumen und Gebäuden der Institution erfüllt werden, sondern an wechselnden Arbeitsplätzen in unterschiedlichen Umgebungen, z. B. in Hotelzimmern, in Zügen oder bei der Kundschaft. Die dabei verarbeiteten Informationen müssen angemessen geschützt werden.

Das mobile Arbeiten verändert einerseits die Dauer, Lage und Verteilung der Arbeitszeiten. Andererseits erhöht es die Anforderungen an die Informationssicherheit, da in Umgebungen mit mobilen Arbeitsplätzen keine sichere IT-Infrastruktur vorausgesetzt werden kann, so wie sie in einer Büroumgebung anzutreffen ist.

1.2. Zielsetzung

Der Baustein beschreibt Sicherheitsanforderungen an mobile Arbeitsplätze. Ziel ist es, für solche Arbeitsplätze eine mit einem Büroraum vergleichbare Sicherheitssituation zu schaffen.

1.3. Abgrenzung und Modellierung

Der Baustein INF.9 *Mobiler Arbeitsplatz* ist für alle Räume anzuwenden, die häufig als mobiler Arbeitsplatz genutzt werden.

Der Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, wenn Mitarbeitende nicht nur innerhalb der Institution arbeiten, sondern auch häufiger an wechselnden Arbeitsplätzen außerhalb.

Der Baustein bildet vor allem die organisatorischen, technischen und personellen Anforderungen an die vollständige oder teilweise mobile Arbeit ab. Um IT-Systeme, Datenträger oder Unterlagen, die beim mobilen Arbeiten genutzt werden, abzusichern, müssen alle relevanten Bausteine wie z. B. SYS.3.1 *Laptops*, SYS.3.2 *Allgemeine Smartphones und Tablets,* SYS.4.5 *Wechseldatenträger*, NET.3.3 *VPN* sowie SYS.2.1 *Allgemeiner Client* gesondert berücksichtigt werden.

Sicherheitsanforderungen an Bildschirmarbeitsplätze außerhalb von Gebäuden der Institution, die von der Institution fest eingerichtet werden (Telearbeitsplätze), sind nicht Gegenstand des vorliegenden Bausteins. Diese werden im Baustein OPS.1.2.4 *Telearbeit* beschrieben. Ebenso wird nicht auf

Sicherheitsanforderungen an die Infrastruktur des Telearbeitsplatzes eingegangen. Dieses Thema wird im Baustein INF.8 *Häuslicher Arbeitsplatz* behandelt.

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.9 *Mobiler Arbeitsplatz* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Regelungen für mobile Arbeitsplätze

Ist das mobile Arbeiten nicht oder nur unzureichend geregelt, können der Institution unter anderem finanzielle Schäden entstehen. Ist beispielsweise nicht geregelt, welche Informationen außerhalb der Institution transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu beachten sind, können vertrauliche Informationen in fremde Hände gelangen. Diese können dann von unbefugten Personen möglicherweise gegen die Institution verwendet werden.

2.2. Beeinträchtigung durch wechselnde Einsatzumgebung

Da mobile Datenträger und Endgeräte in sehr unterschiedlichen Umgebungen eingesetzt werden, sind sie vielen Gefährdungen ausgesetzt. Dazu gehören beispielsweise schädigende Umwelteinflüsse wie z. B. zu hohe oder zu niedrige Temperaturen, Staub oder Feuchtigkeit. Auch Transportschäden können auftreten.

Neben diesen Einflüssen ist auch die Einsatzumgebung mit ihrem unterschiedlichen Sicherheitsniveau zu berücksichtigten. Smartphones, Tablets, Laptops und ähnliche mobile Endgeräte sind nicht nur beweglich, sondern können auch mit anderen IT-Systemen kommunizieren. Dabei können beispielsweise Schadprogramme übertragen oder schützenswerte Informationen kopiert werden. Auch können eventuell Aufgaben nicht mehr erfüllt, Termine mit der Kundschaft nicht wahrgenommen oder IT-Systeme beschädigt werden.

2.3. Manipulation oder Zerstörung von IT-Systemen, Zubehör, Informationen und Software am mobilen Arbeitsplatz

IT-Systeme, Zubehör, Informationen und Software, die mobil genutzt werden, können unter Umständen einfacher manipuliert oder zerstört werden als in der Institution. Der mobile Arbeitsplatz ist oft für Dritte zugänglich. Auch sind hier die zentralen Schutzmaßnahmen der Institution nicht vorhanden, wie z. B. Pfortendienste. Werden IT-Systeme, Zubehör, Informationen oder Software manipuliert oder zerstört, sind die Mitarbeitenden am mobilen Arbeitsplatz oft nur noch eingeschränkt arbeitsfähig. Des Weiteren müssen womöglich zerstörte IT-Komponenten oder Softwarelösungen ersetzt werden, was sowohl finanzielle als auch zeitliche Ressourcen erfordert.

2.4. Verzögerungen durch temporär eingeschränkte Erreichbarkeit

Meist haben die Mitarbeitenden am mobilen Arbeitsplatz keine festen Arbeitszeiten und sind unterwegs auch schwerer zu erreichen. Dadurch kann sich der Informationsfluss deutlich verzögern. Selbst wenn die Informationen per E-Mail übermittelt werden, verkürzt sich nicht zwingend die Reaktionszeit, da nicht sichergestellt werden kann, dass die mobil Mitarbeitenden die E-Mails zeitnah lesen. Die temporär eingeschränkte Erreichbarkeit wirkt sich dabei je nach Situation und Institution unterschiedlich aus, kann aber die Verfügbarkeit von Informationen stark einschränken.

2.5. Ungesicherter Akten- und Datenträgertransport

Wenn Dokumente, Datenträger oder Akten zwischen der Institution und den mobilen Arbeitsplätzen transportiert werden, können diese Informationen und Daten verlorengehen oder auch von unbefugten Personen entwendet, gelesen oder manipuliert werden. Dadurch können der Institution größere finanzielle Schäden entstehen. Der Akten- und Datenträgertransport kann auf verschiedene Arten unzureichend gesichert sein:

- Werden Unikate transportiert und fehlt eine entsprechende Datensicherung, können Ziele und Aufgaben nicht wie geplant erreicht werden, wenn das Unikat verloren geht.
- Fallen unverschlüsselte Datenträger in falsche Hände, kann dies zu einem schwerwiegenden Verlust der Vertraulichkeit führen.
- Ist unterwegs kein ausreichender Zugriffsschutz vorhanden, können Akten oder Datenträger unbemerkt kopiert oder manipuliert werden.

2.6. Ungeeignete Entsorgung der Datenträger und Dokumente

Ist es am mobilen Arbeitsplatz nicht möglich, Datenträger und Dokumente in geeigneter Weise zu entsorgen, wandern diese meist in den Hausmüll. Auch dort, wo unterwegs gearbeitet wird, werfen Mitarbeitende Entwürfe und andere vermeintlich unnütze Dokumente häufig direkt in den nächsten Papierkorb. Oder sie lassen sie einfach liegen, sei es im Hotel oder in der Bahn. Wenn jedoch Datenträger oder Dokumente nicht geeignet entsorgt werden, können Dritte daraus wertvolle Informationen entnehmen, die sich gezielt für Erpressungsversuche oder zur Wirtschaftsspionage missbrauchen lassen. Die Folgen reichen vom Wissensverlust bis zur Existenzgefährdung der Institution, z. B. wenn dadurch wichtige Aufträge nicht zustande kommen oder Partnerschaften scheitern.

2.7. Vertraulichkeitsverlust schützenswerter Informationen

Am mobilen Arbeitsplatz können Dritte einfacher auf vertrauliche Informationen zugreifen, die sich auf Festplatten, auf austauschbaren Speichermedien oder auf Papier befinden, besonders dann, wenn sie dabei professionell agieren. Auch können sie Kommunikationsverbindungen abhören. Werden Informationen unberechtigt gelesen oder preisgegeben, hat das jedoch schwerwiegende Folgen für die gesamte Institution. Unter anderem kann der Verlust der Vertraulichkeit dazu führen, dass die Institution gegen Gesetze verstößt oder dass Wettbewerbsnachteile und finanzielle Schäden entstehen.

2.8. Diebstahl oder Verlust von Datenträgern oder Dokumenten

Der mobile Arbeitsplatz ist nicht so gut abgesichert wie der Arbeitsplatz in einem Unternehmen oder in einer Behörde. Dienstliche IT-Systeme und Dokumente können daher z. B. während einer Bahnfahrt, aus einem Hotelzimmer oder aus externen Konferenzräumen leichter gestohlen werden.

Zudem können mobile IT-Systeme oder IT-Komponenten verloren gehen. Neben dem rein materiellen Schaden durch den unmittelbaren Verlust des mobilen IT-Systems kann zudem ein weiterer finanzieller Schaden entstehen, etwa wenn schützenswerte Daten wie z. B. E-Mails, Notizen von Besprechungen, Adressen oder sonstige Dokumente offengelegt werden. Auch könnte der Ruf der Institution geschädigt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.9 *Mobiler Arbeitsplatz* 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	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Mitarbeitende, IT-Betrieb, Zentrale Verwaltung, Personalabteilung

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.9.A1 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes (B) [IT-Betrieb]

Die Institution MUSS ihren Mitarbeitenden vorschreiben, wie mobile Arbeitsplätze in geeigneter Weise ausgewählt und benutzt werden sollen. Es MÜSSEN Eigenschaften definiert werden, die für einen mobilen Arbeitsplatz wünschenswert sind. Es MÜSSEN aber auch Ausschlusskriterien definiert werden, die gegen einen mobilen Arbeitsplatz sprechen. Mindestens MUSS geregelt werden:

- unter welchen Arbeitsplatzbedingungen schützenswerte Informationen bearbeitet werden dürfen,
- wie sich Mitarbeitende am mobilen Arbeitsplatz vor ungewollter Einsichtnahme Dritter schützen,
- ob eine permanente Netz- und Stromversorgung gegeben sein muss sowie
- welche Arbeitsplatzumgebungen komplett verboten sind.

INF.9.A2 Regelungen für mobile Arbeitsplätze (B) [Personalabteilung]

Für alle Arbeiten unterwegs MUSS geregelt werden, welche Informationen außerhalb der Institution transportiert und bearbeitet werden dürfen. Es MUSS zudem geregelt werden, welche Schutzvorkehrungen dabei zu treffen sind. Dabei MUSS auch geklärt werden, unter welchen Rahmenbedingungen Mitarbeitende mit mobilen IT-Systemen auf interne Informationen ihrer Institution zugreifen dürfen.

Die Mitnahme von IT-Komponenten und Datenträgern MUSS klar geregelt werden. So MUSS festgelegt werden, welche IT-Systeme und Datenträger mitgenommen werden dürfen, wer diese mitnehmen darf und welche grundlegenden Sicherheitsanforderungen dabei beachtet werden müssen. Es MUSS zudem protokolliert werden, wann und von wem welche mobilen Endgeräte außer Haus eingesetzt wurden.

Die Benutzenden von mobilen Endgeräten MÜSSEN für den Wert mobiler IT-Systeme und den Wert der darauf gespeicherten Informationen sensibilisiert werden. Sie MÜSSEN über die spezifischen Gefährdungen und Maßnahmen der von ihnen benutzten IT-Systeme aufgeklärt werden. Außerdem MÜSSEN sie darüber informiert werden, welche Art von Informationen auf mobilen IT-Systemen verarbeitet werden darf. Alle Benutzenden MÜSSEN auf die geltenden Regelungen hingewiesen werden, die von ihnen einzuhalten sind. Sie MÜSSEN entsprechend geschult werden

INF.9.A3 Zutritts- und Zugriffsschutz (B) [Zentrale Verwaltung, Mitarbeitende]

Den Mitarbeitenden MUSS bekannt gegeben werden, welche Regelungen und Maßnahmen zum Einbruch- und Zutrittsschutz am mobilen Arbeitsplatz zu beachten sind. Wenn der mobile Arbeitsplatz nicht besetzt ist, MÜSSEN Fenster und Türen abgeschlossen werden. Ist dies nicht möglich, z. B. im Zug, MÜSSEN die Mitarbeitenden alle Unterlagen und IT-Systeme an sicherer Stelle verwahren oder mitführen, wenn sie abwesend sind. Es MUSS sichergestellt werden, dass unbefugte Personen zu keiner Zeit auf dienstliche IT und Unterlagen zugreifen können. Wird der Arbeitsplatz nur kurz verlassen, MÜSSEN die eingesetzten IT-Systeme gesperrt werden, sodass sie nur nach erfolgreicher Authentisierung wieder benutzt werden können.

INF.9.A4 Arbeiten mit fremden IT-Systemen (B) [IT-Betrieb, Mitarbeitende]

Die Institution MUSS regeln, wie Mitarbeitende mit institutionsfremden IT-Systemen arbeiten dürfen. Alle mobilen Mitarbeitenden MÜSSEN über die Gefahren fremder IT-Systeme aufgeklärt werden. Die Regelungen MÜSSEN vorgeben, ob und wie schützenswerte Informationen an fremden IT-Systemen bearbeitet werden dürfen. Sie MÜSSEN zudem festlegen, wie verhindert wird, dass nicht autorisierte Personen die Informationen einsehen können. Wenn Mitarbeitende mit fremden IT-Systemen arbeiten, MUSS grundsätzlich sichergestellt sein, dass alle währenddessen entstandenen temporären Daten gelöscht 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.9.A5 Zeitnahe Verlustmeldung (S) [Mitarbeitende]

Mitarbeitende SOLLTEN ihrer Institution umgehend melden, wenn Informationen, IT-Systeme oder Datenträger verlorengegangen sind oder gestohlen wurden. Dafür SOLLTE es klare Meldewege und Ansprechpartner innerhalb der Institution geben.

INF.9.A6 Entsorgung von vertraulichen Informationen (S) [Mitarbeitende]

Vertrauliche Informationen SOLLTEN auch unterwegs sicher entsorgt werden. Bevor ausgediente oder defekte Datenträger und Dokumente vernichtet werden, MUSS überprüft werden, ob sie sensible Informationen enthalten. Ist dies der Fall, MÜSSEN die Datenträger und Dokumente wieder mit zurücktransportiert werden und auf institutseigenem Wege entsorgt oder vernichtet werden.

INF.9.A7 Rechtliche Rahmenbedingungen für das mobile Arbeiten (S) [Personalabteilung]

Für das mobile Arbeiten SOLLTEN arbeitsrechtliche und arbeitsschutzrechtliche Rahmenbedingungen beachtet und geregelt werden. Alle relevanten Punkte SOLLTEN entweder durch Betriebsvereinbarungen oder durch zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen dem mobilen Mitarbeitenden und der Institution geregelt werden.

INF.9.A8 Sicherheitsrichtlinie für mobile Arbeitsplätze (S) [IT-Betrieb]

Alle relevanten Sicherheitsanforderungen für mobile Arbeitsplätze SOLLTEN in einer für die mobilen Mitarbeitenden verpflichtenden Sicherheitsrichtlinie dokumentiert werden. Sie SOLLTE zudem mit den bereits vorhandenen Sicherheitsrichtlinien der Institution sowie mit allen relevanten Fachabteilungen abgestimmt werden. Die Sicherheitsrichtlinie für mobile Arbeitsplätze SOLLTE regelmäßig aktualisiert werden. Die Mitarbeitenden der Institution SOLLTEN hinsichtlich der aktuellen Sicherheitsrichtlinie sensibilisiert und geschult sein.

INF.9.A9 Verschlüsselung tragbarer IT-Systeme und Datenträger (S) [IT-Betrieb]

Bei tragbaren IT-Systemen und Datenträgern SOLLTE sichergestellt werden, dass diese entsprechend den internen Richtlinien abgesichert sind. Mobile IT-Systeme und Datenträger SOLLTEN dabei verschlüsselt werden. Die kryptografischen Schlüssel SOLLTEN getrennt vom verschlüsselten Gerät aufbewahrt werden.

INF.9.A12 Nutzung eines Bildschirmschutzes (S) [Mitarbeitende]

Wenn IT-Systeme an mobilen Arbeitsplätzen genutzt werden, SOLLTEN die Mitarbeitenden einen Sichtschutz für die Bildschirme der IT-Systeme verwenden.

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.9.A10 Einsatz von Diebstahlsicherungen (H) [Mitarbeitende]

Bietet das verwendete IT-System eine Diebstahlsicherung, SOLLTE sie benutzt werden. Die Diebstahlsicherungen SOLLTEN stets dort eingesetzt werden, wo ein erhöhter Publikumsverkehr herrscht oder die Fluktuation von Benutzenden sehr hoch ist. Dabei SOLLTEN die Mitarbeitenden immer beachten, dass der Schutz der auf den IT-Systemen gespeicherten Informationen meist einen höheren Wert besitzt als die Wiederanschaffungskosten des IT-Systems betragen. Die Beschaffungs- und Einsatzkriterien für Diebstahlsicherungen SOLLTEN an die Prozesse der Institution angepasst und dokumentiert werden.

INF.9.A11 Verbot der Nutzung unsicherer Umgebungen (H) [IT-Betrieb]

Es SOLLTEN Kriterien für die Arbeitsumgebung festgelegt werden, die mindestens erfüllt sein müssen, damit Informationen mit erhöhtem Schutzbedarf mobil bearbeitet werden dürfen. Die Kriterien SOLLTEN mindestens folgende Themenbereiche abdecken:

- Einsicht und Zugriff durch Dritte,
- geschlossene und, falls nötig, abschließbare oder bewachte Räume,
- gesicherte Kommunikationsmöglichkeiten sowie
- eine ausreichende Stromversorgung.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A.11.2 Vorgaben zur Ausrüstung bzw. Ausstattung von mobilen Arbeitsplätzen.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A.6.2.1. Vorgaben zur Erarbeitung einer Richtlinie für mobile Geräte.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel PA2 Vorgaben zum Umgang mit mobilen Endgeräten.

Das National Institute of Standards and Technology (NIST) hat im Rahmen seiner Special Publications die NIST Special Publication 800-46 zu „Remote Access and Bring Your Own Device (BYOD)“ veröffentlicht und macht Vorgaben zum Fernzugriff auf Handware.

Bundesamt
für Sicherheit in der
Informationstechnik

INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume

1. Beschreibung

1.1. Einleitung

In der Regel hat jede Institution einen oder mehrere Räume, in denen Besprechungen, Schulungen oder sonstige Veranstaltungen durchgeführt werden können. Hierfür sind oft speziell ausgestattete Räume vorgesehen. Besprechungs-, Veranstaltungs- und Schulungsräume zeichnen sich im Wesentlichen dadurch aus, dass sie von wechselnden Personen bzw. internen oder externen Personenkreisen in der Regel nur für einen begrenzten Zeitraum genutzt werden. Mitgebrachte IT-Systeme werden dabei häufig gemeinsam mit Geräten der Institution betrieben, wie beispielsweise institutionsfremde Laptops an fest verbauten Beamern. Aus diesen unterschiedlichen Nutzungsszenarien heraus ergibt sich eine besondere Gefährdungslage, die in anderen Räumen der Institution in dieser Weise nicht existiert.

1.2. Zielsetzung

Ziel des Bausteins ist der Schutz von Informationen, die in Besprechungs-, Veranstaltungs- und Schulungsräumen bearbeitet werden, sowie der IT-Systeme, die in diesen Räumen betrieben werden. Außerdem wird der empfohlene Umgang mit externen Personen, die die entsprechende Räume nutzen, behandelt.

1.3. Abgrenzung und Modellierung

Der Baustein INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume* ist auf jeden Besprechungs-, Veranstaltungs- oder Schulungsraum anzuwenden.

Dieser Baustein betrachtet alle technischen und nicht-technischen Sicherheitsaspekte zur Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen. Detaillierte Empfehlungen, wie die IT-Systeme in diesen Räumen konfiguriert und abgesichert werden können, werden nicht in diesem Baustein behandelt. Sie sind in SYS.2.1 *Allgemeiner Client* sowie in den betriebssystemspezifischen System-Bausteinen zu finden. Weitere für Besprechungsräume relevante Sicherheitsaspekte, wie z. B.

für WLANs oder Videokonferenzanlagen, werden in den Bausteinen der Schichten NET.2 *Funknetze* bzw. NET.4 *Telekommunikation* betrachtet. Die Verkabelung in diesen Räumen wird im Baustein INF.12 *Verkabelung* gesondert berücksichtigt. Anforderungen zum Brandschutz sind im Baustein INF.1 *Allgemeines Gebäude* zu finden. Anforderungen zur Beaufsichtigung von Besuch und zum Mitführverbot von Mobiltelefonen sind im Baustein ORP.1 *Organisation* zu finden.

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.10 *Besprechungs-, Veranstaltungs- und Schulungsräume* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Regelungen

Wenn z. B. Mitarbeitende die Fenster und Türen nach Verlassen eines Besprechungs-, Veranstaltungs- oder Schulungsraumes nicht schließen oder vertrauliche Informationen von einem Whiteboard oder Flipchart nicht entfernt werden, können diese Informationen unberechtigt eingesehen werden. Generell sollte den Mitarbeitenden daher entsprechende Regelungen an die Hand gegeben werden, sodass entsprechende Sicherheitslücken nicht auftreten können. Regelungen lediglich festzulegen sichert aber noch nicht, dass sie auch beachtet werden und der Betrieb störungsfrei ist. Viele Probleme entstehen, wenn Regelungen zwar vorhanden, aber den Mitarbeitenden nicht bekannt sind. Oft wissen Mitarbeitende z. B. nicht, dass Fenster und Türen nach Besprechungen verschlossen werden müssen oder wie sie mit den im Besprechungsraum vorhandenen Arbeitsmitteln (z. B. Technik oder Flipchart) umgehen sollen.

2.2. Inkompatibilität zwischen fremder und eigener IT

IT-Systeme werden immer mobiler und zunehmend in unterschiedlichen Umgebungen verwendet. Oft finden Personen Szenarien vor, in denen die eigenen IT-Systeme nicht wie geplant genutzt werden können, da sie nicht mit den fremden IT-Systemen kompatibel sind. Beispielsweise verfügen ältere Geräte nicht über die gleichen Anschlüsse und Stecker wie neuere Geräte. Zudem gibt es Geräte, die nicht ohne passenden Adapter mit anderen Geräten kompatibel sind. Liegt also z. B. ein passender Adapter nicht vor, so kann ein Laptop, der mit allen wichtigen Daten für eine Besprechung vorbereitet wurde, nicht an einen Beamer angeschlossen werden. Darüber hinaus können Versuche, die IT-Systeme dennoch zu verbinden, zu Schäden an den Geräten oder den gespeicherten Daten führen.

2.3. Fliegende Verkabelung

In Besprechungs-, Veranstaltungs- und Schulungsräumen wechseln häufig sowohl Personen als auch die Art, wie die Räume genutzt werden. Dadurch wird mitunter die Geräteausstattung und damit auch die Verkabelung in diesen Räumen permanent geändert. Kabel können somit, je nach Lage der Anschlusspunkte im Raum (Steckdosen der Stromversorgung und des Datennetzes) übergangsweise quer durch den Raum, auch über Verkehrswege hinweg, verlegt werden. Nicht nur Personen werden durch diese Stolperfallen gefährdet, auch IT-Systeme können beschädigt werden, wenn Personen die „fliegenden“ Kabel mit sich reißen.

2.4. Diebstahl

Wenn die in einem Besprechungs-, Veranstaltungs- oder Schulungsraum teils stationär verbauten Datenträger, IT-Systeme, Zubehör, Software oder Daten gestohlen werden, entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes. Andererseits kann der Besprechungs-, Veranstaltungs- oder Schulungsraum aufgrund mangelnder

Verfügbarkeit der Geräte anschließend nur eingeschränkt genutzt werden. Dies verursacht möglicherweise Engpässe bei der Raumbelegung. Darüber hinaus können vertrauliche Informationen gestohlen, missbraucht oder weitergegeben werden.

Gestohlen werden neben teuren IT-Systemen häufig auch mobile Endgeräte, die unauffällig und leicht zu transportieren sind. Sind die Besprechungs-, Veranstaltungs- oder Schulungsräume nicht beaufsichtigt oder die IT-Systeme nicht ausreichend gesichert, kann die Technik dementsprechend schnell und unauffällig entwendet werden. Dies gilt ganz besonders, wenn beispielsweise in Besprechungspausen die Räumlichkeiten nicht verschlossen werden.

2.5. Vertraulichkeitsverlust schützenswerter Informationen

Durch technisches Versagen, Unachtsamkeit, Unwissen und auch durch vorsätzliche Handlungen können vertrauliche Informationen offengelegt werden. Dabei können diese Informationen an unterschiedlichen Stellen vorliegen, z. B. auf Speichermedien innerhalb von IT-Systemen (wie Festplatten), auf austauschbaren Speichermedien (wie USB-Sticks oder optische Medien), in gedruckter Form auf Papier sowie auf Whiteboards oder Flipcharts. Werden Informationen unberechtigt gelesen oder preisgegeben, kann das schwerwiegende Folgen für die Institution haben, beispielsweise Verstöße gegen Gesetze, Wettbewerbsnachteile oder finanzielle Auswirkungen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume* 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	Zentrale Verwaltung
Weitere Zuständigkeiten	Mitarbeitende, IT-Betrieb, Haustechnik

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.10.A1 Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen (B) [Haustechnik, IT-Betrieb]

In den Räumen vorhandene Gerätschaften MÜSSEN angemessen gegen Diebstahl gesichert werden. Zudem MUSS festgelegt werden, wer die in den Räumen dauerhaft vorhandenen IT- und sonstigen Systeme administriert. Es MUSS auch festgelegt werden, ob und unter welchen Bedingungen von externen Personen mitgebrachte IT-Systeme verwenden dürfen. Weiterhin MUSS festgelegt werden, ob und auf welche Netzzugänge und TK-Schnittstellen externen Personen zugreifen dürfen.

INF.10.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

INF.10.A3 Geschlossene Fenster und Türen (B) [Mitarbeitende]

Die Fenster und Türen der Besprechungs-, Veranstaltungs- und Schulungsräume MÜSSEN beim Verlassen verschlossen werden. Bei Räumlichkeiten, in denen sich IT-Systeme oder schützenswerte Informationen befinden, MÜSSEN die Türen beim Verlassen abgeschlossen werden. Zusätzlich MUSS regelmäßig geprüft werden, ob die Fenster und Türen nach Verlassen der Räume verschlossen wurden. Ebenso MUSS darauf geachtet werden, dass Brand- und Rauchschutztüren tatsächlich geschlossen 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.10.A4 Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen (S)

Bei der Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen SOLLTE besonders die Lage der Räume berücksichtigt werden. Insbesondere Räumlichkeiten, die oft zusammen mit oder ausschließlich von externen Personen genutzt werden, SOLLTEN NICHT in Gebäudeteilen liegen, in deren Nähe regelmäßig vertrauliche Informationen besprochen und bearbeitet werden. Es SOLLTE für jeden Raum festgelegt werden, wie vertraulich die Informationen sein dürfen, die dort besprochen oder verarbeitet werden.

INF.10.A5 Fliegende Verkabelung (S)

Die Stromanschlüsse SOLLTEN sich dort befinden, wo Beamer, Laptops oder andere elektronische Geräte aufgestellt werden. Verkabelungen, die über den Boden verlaufen, SOLLTEN geeignet abgedeckt werden.

INF.10.A6 Einrichtung sicherer Netzzugänge (S) [IT-Betrieb]

Es SOLLTE sichergestellt werden, dass mitgebrachte IT-Systeme nicht über das Datennetz mit internen IT-Systemen der Institution verbunden werden können. Auf das LAN der Institution SOLLTEN ausschließlich dafür vorgesehene IT-Systeme zugreifen können. Ein Datennetz für externe Personen SOLLTE vom LAN der Institution getrennt werden. Netzzugänge SOLLTEN so eingerichtet sein, dass verhindert wird, dass Dritte den internen Datenaustausch mitlesen können. Netzanschlüsse in Besprechungs-, Veranstaltungs- oder Schulungsräumen SOLLTEN abgesichert werden. Es SOLLTE verhindert werden, dass IT-Systeme in Besprechungs-, Veranstaltungs- und Schulungsräumen gleichzeitig eine Verbindung zum Intranet und zum Internet aufbauen können.

Außerdem SOLLTE die Stromversorgung aus einer Unterverteilung heraus getrennt von anderen Räumen aufgebaut werden.

INF.10.A7 Sichere Konfiguration von Schulungs- und Präsentationsrechnern (S) [IT-Betrieb]

Dedizierte Schulungs- und Präsentationsrechner SOLLTEN mit einer Minimalkonfiguration versehen werden. Es SOLLTE festgelegt sein, welche Anwendungen auf Schulungs- und Präsentationsrechnern in der jeweiligen Veranstaltung genutzt werden können. Die Schulungs- und Präsentationsrechner SOLLTEN nur an ein separates, vom LAN der Institution getrenntes Datennetz angeschlossen werden.

INF.10.A8 Erstellung eines Nutzungsnachweises für Räume (S)

Je nach Nutzungsart der Besprechungs-, Veranstaltungs- und Schulungsräume SOLLTE ersichtlich sein, wer die Räume zu welchem Zeitpunkt genutzt hat. Für Räumlichkeiten, in denen Schulungen an IT-Systemen oder besonders vertrauliche Besprechungen durchgeführt werden, SOLLTEN ebenfalls Nutzungsnachweise erbracht werden. Es SOLLTE überlegt werden, für Räumlichkeiten, die für jeden Mitarbeitenden zugänglich sind, ebenfalls entsprechende Nutzungsnachweise einzuführen.

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.10.A9 Zurücksetzen von Schulungs- und Präsentationsrechnern (H) [IT-Betrieb]

Es SOLLTE ein Verfahren festgelegt werden, um Schulungs- und Präsentationsrechner nach der Nutzung auf einen vorher definierten Zustand zurückzusetzen. Durch von Benutzenden durchgeführte Änderungen SOLLTEN dabei vollständig entfernt werden.

INF.10.A10 ENTFALLEN (H)

Diese Anforderung ist entfallen.

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 und Räumen.

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 und Räumen.

Das Deutsche Institut für Normung macht in seiner Norm DIN EN 1627-1630:2021-11 Vorgaben zur physischen Sicherheit von Gebäuden und Räumen.

Bundesamt
für Sicherheit in der
Informationstechnik

INF.11 Allgemeines Fahrzeug

1. Beschreibung

1.1. Einleitung

Institutionen nutzen in vielen Situationen die unterschiedlichsten Fahrzeuge im Nah- und Fernbereich. Als Fahrzeug werden im Kontext dieses Bausteins motorisierte Fortbewegungsmittel bezeichnet, die sich in der Regel auf Land- und Luftstraßen, Seewegen sowie Wasserstraßen bewegen und über eine Fahrzeugkabine oder Vergleichbares verfügen. Beispiele hierfür sind PKW, LKW, Flugzeuge oder Schiffe. Im folgenden Text wird nur noch der Oberbegriff Fahrzeug verwendet, außer es ist eine bestimmte Art von Fahrzeug gemeint.

Nahezu alle modernen Fahrzeuge verfügen über integrierte IT-Komponenten, wie zum Beispiel Infotainmentsysteme oder interne Analysesysteme, die im Rahmen der Informationssicherheit ganzheitlich betrachtet werden müssen. Darüber hinaus werden dienstliche Aufgaben häufig nicht nur in den Räumen und Gebäuden einer Institution erledigt, sondern auch innerhalb von Fahrzeugen, die sich an wechselnden Standorten und in verschiedenen Umgebungen befinden können. Ein Fahrzeug ist somit auch eine eigenständige mobile Arbeitsumgebung, die durch die Institution angemessen abgesichert werden muss.

1.2. Zielsetzung

Der Baustein beschreibt spezifische Gefährdungen, die zu beachten sind, wenn Institutionen Fahrzeuge mit IT-Komponenten einsetzen oder Fahrzeuge im Allgemeinen als IT-Arbeitsplätze verwenden. Darauf aufbauend legt der Baustein fest, welche Anforderungen von Fahrzeugnutzenden und -haltenden zu erfüllen sind, um den optimalen Betrieb eines Fahrzeugs aus Sicht der Informationssicherheit zu gewährleisten.

1.3. Abgrenzung und Modellierung

Der Baustein INF.11 *Allgemeines Fahrzeug* ist grundsätzlich auf jedes von der Institution eingesetztes Land-, Luft- und Wasserfahrzeug einmal anzuwenden.

Adressaten des Bausteins sind Benutzende und Betreibende von Fahrzeugen. Autonom fahrende oder ferngesteuerte Fahrzeuge, Schienenfahrzeuge und Raumfahrzeuge sind von diesem Baustein ausgenommen.

Die Art, die Ausstattung, der Einsatzort und das Aufgabenfeld von Fahrzeugen können sich je nach Institution voneinander unterscheiden. In dem Baustein INF.11 *Allgemeines Fahrzeug* werden nur die

typischen Einsatzszenarien von Fahrzeugen berücksichtigt, sodass spezielle Einsatzzwecke, wie etwa Rettungseinsätze von Rettungshubschraubern oder Kampfeinsätze von Militärfahrzeugen, ergänzend individuell betrachtet werden müssen.

Daher wird nicht abschließend auf nachträglich eingebaute, einsatzspezifische IT-Systeme oder fahrzeugspezifische Fachanwendungen eingegangen, wie sie zum Beispiel bei Einsatzfahrzeugen oder Führungsfahrzeugen üblich sind. Die Ausstattung und die damit verbundenen Fachanwendungen dieser Fahrzeuge sind individuell ergänzend zu behandeln.

Außerdem werden die fahrzeugeigenen Netze über Kommunikationsbusse wie CAN, LIN oder Flexray, auch IVN (In-Vehicle-Network) genannt, nicht betrachtet, da diese in der Regel nicht durch die Anwendenden verändert werden.

Um die mitgeführten und nachträglich eingebauten IT-Komponenten abzusichern, müssen alle relevanten Bausteine, wie SYS.3.1 *Laptops*, SYS.3.2 *Allgemeine Smartphones und Tablets*, NET.3.3 *VPN* und die Bausteinschichten NET.4 *Telekommunikation* sowie NET.2 *Funknetze* gesondert berücksichtigt werden.

Darüber hinaus muss, bevor das Fahrzeug entsorgt, bzw. ausgesondert wird, der Baustein CON.6 *Löschen und Vernichten* angewendet werden, damit keine schützenswerten Informationen im Fahrzeug verbleiben.

Dieser Baustein behandelt alle infrastrukturellen Aspekte, sodass INF.9 *Mobiler Arbeitsplatz* nicht zusätzlich zu modellieren ist.

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.11 *Allgemeines Fahrzeug* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Regelungen für Fahrzeuge

Wird nicht oder nur unzureichend geregelt, welche Informationen über die von Fahrzeugen für Benutzende zur Verfügung gestellten Netze wie WLAN oder Bluetooth übertragen und verarbeitet werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind, können vertrauliche Informationen offengelegt werden. Wird nicht hinreichend geregelt, wie diese abzusichern und zu benutzen sind, könnten schützenswerte Informationen wie personenbezogene Daten offengelegt werden.

Wenn Fahrzeuge gestohlen werden oder integrierte IT-Komponenten ausfallen und es hierfür keine Regelungen und festgelegte Abläufe gibt, kann dies gravierende Folgen haben. Es besteht die Gefahr, dass schützenswerte Informationen im Fahrzeug verbleiben und unbefugte Dritte Zugang zu diesen erhalten.

Wenn Fahrzeuge oder die darin verbauten IT-Komponenten unsachgemäß in Betrieb genommen werden, kann dies zu umfangreichen Gefährdungen der Informationssicherheit führen. Es könnten relevante Einstellungen, wie die automatische Synchronisation von Telefonbüchern, falsch konfiguriert sein oder es könnten Funktionstest bei Flugzeugen übersprungen oder unsachgemäß durchgeführt werden. Dies wiederum kann dazu führen, dass die Systeme des Flugzeuges während des Einsatzes nicht wie vorgesehen funktionieren und schlimmstenfalls zu einem Totalverlust des Flugzeugs führen.

Genauso kann aber auch die Funktion der integrierten IT-Komponenten und des gesamten Fahrzeuges gefährdet werden, wenn das Fahrzeug unsachgemäß ausgeschaltet oder temporär außer Betrieb genommen wird. Ein Beispiel hierfür sind Einsatzfahrzeuge. Werden diese für einen längeren Zeitraum ausgeschaltet, so droht aufgrund der umfangreichen Ausstattung, dass sich die Fahrzeugbatterie

vollständig entlädt. Infolgedessen kann das Fahrzeug nicht mehr starten und in den integrierten IT-Komponenten könnten Daten verloren gehen.

2.2. Fehlendes Sicherheitsbewusstsein und Sorglosigkeit beim Umgang mit dem Fahrzeug

Fehlendes Sicherheitsbewusstsein und Sorglosigkeit beim Umgang mit den Fahrzeugen und deren Komponenten stellen eine ernstzunehmende Gefahr dar. Sind Mitarbeitende beispielsweise nicht ausreichend geschult, wie sie mit den Fahrzeugen und den IT-Komponenten umgehen sollen und sind sich der möglichen Risiken nicht bewusst, könnten Fahrzeuge und die darin verbauten IT-Komponenten falsch oder unsorgfältig benutzt werden. So werden zum Beispiel IT-Systeme auf Brücken von Schiffen von unterschiedlichen Personen benutzt. Werden nun wesentliche Einstellungen von einem Benutzenden verändert, ohne die weiteren Benutzenden darüber zu informieren, dann könnten Fehlfunktionen auftreten, die die weiteren Benutzenden nicht nachvollziehen können.

Eine weitere Gefahr kann darin bestehen, dass Fahrzeuge unzuverlässig abgeschlossen werden. Hierdurch könnten unbefugte Dritte einfach die Fahrzeugkabine betreten und alle dort vorhandenen IT-Komponenten und abgelegten Informationen einsehen oder entwenden.

Weiterhin könnten schlecht geschulte Mitarbeitende unangemessen auf Störungen reagieren und durch eine falsche Reaktion die Situation verschlimmern. Wird z. B. bei einer Störung der integrierten IT-Systeme des Fahrzeugs nicht die hierfür zuständige Stelle der Institution kontaktiert, sondern vom Benutzenden versucht, die Störung selbst zu beheben, können hieraus unabsehbare Folgen resultieren. Es könnten beispielsweise relevante Einstellungen für die Sicherheit oder den Datenschutz verändert werden.

2.3. Ungeregelte Datenübertragung an Dritte und unsichere Kommunikationsschnittstellen

Viele moderne Fahrzeuge verfügen nicht nur über die für die Benutzenden relevanten bzw. direkt ersichtlichen drahtlosen Kommunikationsschnittstellen, wie z. B. Bluetooth oder WLAN. Viele interne Systeme des Fahrzeugs kommunizieren direkt über integrierte Mobilfunkschnittstellen mit IT-Systemen der herstellenden Unternehmen, wobei dieser Informationsaustausch von den Anwendenden in der Regel nicht beeinflusst werden kann. Hiermit sind nicht nur gesetzlich vorgeschriebene und für den Anwendenden transparente Systeme wie der eCall gemeint, sondern insbesondere auch solche, die nicht für den Benutzenden direkt ersichtlich sind. Beispielsweise übertragen viele fahrzeugherstellende Unternehmen Daten, um detaillierte Informationen über den Standort und die Kilometerzahl des Fahrzeugs oder über das Verhalten der Fahrzeugführenden zu sammeln. Dadurch könnten umfangreich personenbezogene Daten über die Fahrzeugnutzenden erhoben werden, ohne dass diese darüber Kenntnis haben oder dieser Datenerhebung und -verarbeitung explizit zugestimmt haben.

Eine weitere Gefahr sind unsichere Kommunikationsschnittstellen der Fahrzeuge. Durch mangelnde Schutzmechanismen können so sensible Daten ausgelesen werden. Lässt beispielsweise das Infotainmentsystem eine Bluetooth-Koppelung ohne Sicherheitsmechanismen zu, könnten unbefugte Dritte ihr Smartphone unbemerkt damit koppeln und Adressbücher synchronisieren.

2.4. Unsachgemäße Veränderungen am Fahrzeug

Während herkömmliche PKW sehr selten durch den Fahrzeugbetreibenden verändert werden, müssen Fahrzeuge für spezialisierte Einsatzzwecke sehr häufig noch durch die Betreibenden oder spezialisierten Unternehmen nachträglich angepasst werden. Ein Beispiel hierfür sind Einsatzfahrzeuge oder nachträglich modernisierte oder umfunktionierte Schiffe. Wird in diesen Fällen

ein Fahrzeug unsachgemäß verändert, indem z. B. zusätzliche Kabel ungeeignet verlegt werden, kann dies zu erheblichen Schäden bis hin zum Totalverlust des Fahrzeugs führen.

Auch anderweitige Veränderungen können die Einsatzfähigkeit der Fahrzeuge beeinträchtigen. Wird z. B das Infotainmentsystem manipuliert, um neue bzw. gesperrte Funktionen freizuschalten, könnten die Updates des herstellenden Unternehmens nicht mehr eingespielt und damit verbunden potentielle Sicherheitslücken nicht mehr geschlossen werden.

2.5. Manipulation, unbefugter Zutritt und Diebstahl bei Fahrzeugen

Offen in Fahrzeugen liegende Informationen können häufig von außerhalb der Fahrzeuge eingesehen werden, wenn kein oder nur ein unzureichender Sichtschutz vorhanden ist. Dies kann Begehrlichkeiten wecken, die zu Angriffen führen.

Fahrzeuge werden häufig auf öffentlich zugänglichen Parkplätzen abgestellt oder an Bootsanlegern vertäut, die nicht durch zentrale Schutzmaßnahmen der Institution, wie Sicherheitsdienste oder verschlossene Garagen, geschützt werden. Sie sind somit prinzipiell einem erhöhten Risiko ausgesetzt, von Unbefugten betreten zu werden. Unsichere Schließsysteme können hierbei eine Schwachstelle sein. Zum Beispiel können sogenannte schlüssellose Schließsysteme an Fahrzeugen unter Umständen leicht durch Relay-Angriffe umgangen werden.

Somit können IT-Systeme, Zubehör, Informationen und Software häufig einfacher manipuliert, zerstört oder gestohlen werden, wenn sie in Fahrzeugen statt in Räumlichkeiten der Institution unbeaufsichtigt aufbewahrt werden. Werden IT-Systeme, Zubehör, Informationen oder Software manipuliert oder zerstört, sind die Mitarbeitenden in Fahrzeugen oft nur noch eingeschränkt arbeitsfähig. Die betroffenen IT-Systeme könnten sogar in der Art manipuliert werden, dass z. B. die darauf verarbeiteten Daten durch Schadsoftware an unbefugte Dritte weitergeleitet werden. Des Weiteren müssen womöglich zerstörte IT-Komponenten ersetzt werden, was sowohl finanzielle als auch personelle Ressourcen erfordert.

2.6. Gefahren im Zusammenhang mit Wartung, Reparatur und Updates

Werden Fahrzeuge und die verwendeten IT-Komponenten nicht oder nur unzureichend gewartet und gepflegt oder ihre Funktionsfähigkeit nicht regelmäßig überprüft, kann das dazu führen, dass sie im Bedarfsfall nicht oder nur eingeschränkt einsatzfähig sind.

Eine große Herausforderung hierbei ist, dass Updates für die in den Fahrzeugen integrierten IT-Systeme nicht unbedingt zu den regelmäßigen Wartungszyklen der Fahrzeuge bereitstehen. Dadurch könnten Updates beispielsweise nur unregelmäßig und verzögert eingespielt werden.

In institutionseigenen Werkstätten können die Fahrzeuge und die verbauten IT-Komponenten in der Regel nicht vollständig gewartet oder repariert werden, weshalb Fahrzeuge häufig an Fremdfirmen übergeben werden. In den Räumlichkeiten der Fremdfirmen sind die Fahrzeuge meist unbeobachtet und Dritte können umfassend auf das Fahrzeug und die verwendeten IT-Komponenten zugreifen. Dadurch besteht ein erhöhtes Risiko, dass die IT-Komponenten missbraucht oder schützenswerte Informationen entwendet werden.

2.7. Gefahren bei der Aussonderung

Werden Fahrzeuge ausgesondert, können diese mit allen verbauten IT-Komponenten oder mit einem Teil davon veräußert werden. Hierdurch können Fremdpersonen auf die IT-Komponenten zugreifen und so auf interne Informationen oder personenbezogene Daten rückschließen, wie zum Beispiel gespeicherte Telefonnummern. Außerdem können institutionseigene Komponenten wie SIM-Karten oder Kryptomodule in den Fahrzeugen verbleiben. Somit würden die nachfolgenden Besitzenden

ungewollt Zugang zu diesen erhalten und könnten beispielsweise Informationen aus diesen Komponenten auslesen (wie z. B. Telefonnummern von der SIM-Karte) und widerrechtlich verwenden.

2.8. Unzulässige Temperatur und Luftfeuchte in Fahrzeugen

Jedes Gerät hat einen Temperaturbereich, innerhalb dessen es ordnungsgemäß funktioniert. Über- oder unterschreitet die Raumtemperatur die Grenzen dieses Bereiches, können Geräte sowie IT-Komponenten ausfallen und der Betrieb kann gestört werden. Ähnliches gilt für die Luftfeuchtigkeit. In Fahrzeugen liegen unterschiedliche Voraussetzungen vor, die genau zu solchen Situationen führen können. So kann der Innenraum von in der Sonne abgestellten Fahrzeugen bis zu 70 Grad erreichen und somit den üblichen Temperaturbereich von z. B. Lithium-Ionen-Akkus überschreiten.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.11 *Allgemeines Fahrzeug* 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	Informationssicherheitsbeauftragte
Weitere Zuständigkeiten	Mitarbeitende, Fachverantwortliche, Datenschutzbeauftragte, Benutzende, Beschaffungsstelle, IT-Betrieb

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.11.A1 Planung und Beschaffung (B) [Fachverantwortliche, Beschaffungsstelle, Datenschutzbeauftragte]

Bevor Fahrzeuge beschafft werden, MUSS der Einsatzzweck geplant werden. Die funktionalen Anforderungen an die Fahrzeuge und insbesondere die Anforderungen an die Informationssicherheit, sowie den Datenschutz der verbauten IT-Komponenten MÜSSEN erhoben werden. Hierbei MÜSSEN folgende Aspekte berücksichtigt werden:

- Einsatzszenarien der Fahrzeuge,
- nähere Einsatzumgebung der Fahrzeuge sowie
- der gesamte Lebenszyklus der Fahrzeuge.

Die Fahrzeuge MÜSSEN außerdem über angemessene Schließsysteme verfügen, sofern die Fahrzeuge nicht durchgehend durch andere Maßnahmen oder Regelungen gesichert werden können. Während der Planung SOLLTE berücksichtigt werden, dass viele Fahrzeuge Daten an die fahrzeugherstellenden Unternehmen und weitere Dritte übermitteln können.

INF.11.A2 Wartung, Inspektion und Updates (B) [Fachverantwortliche, IT-Betrieb]

Die Fahrzeuge und die dazugehörenden IT-Komponenten MÜSSEN nach den Vorgaben des herstellenden Unternehmens gewartet werden. Hierbei MUSS beachtet werden, dass die Intervalle der herkömmlichen Wartung und von Updates der integrierten IT-Komponenten voneinander abweichen können. Es MUSS klar geregelt werden, wer in welcher Umgebung die Updates installieren darf. Auch „Over-the-Air" (OTA) Updates MÜSSEN geregelt eingespielt werden.

Wartungs- und Reparaturarbeiten MÜSSEN von befugtem und qualifiziertem Personal in einer sicheren Umgebung durchgeführt werden. Dabei SOLLTE schon vor der Wartung geklärt werden, wie mit Fremdfirmen umgegangen wird. Werden Fahrzeuge in fremden Institutionen gewartet, SOLLTE geprüft werden, ob alle nicht benötigten, zum Fahrzeug dazugehörigen portablen IT-Systeme entfernt werden.

Werden die Fahrzeuge wieder in den Einsatzbetrieb integriert, MUSS mittels Checkliste geprüft werden, ob alle Beanstandungen und Mängel auch behoben wurden. Es MUSS auch geprüft werden, ob die vorhandenen IT-Komponenten einsatzfähig sind.

INF.11.A3 Regelungen für die Fahrzeugbenutzung (B) [IT-Betrieb, Fachverantwortliche, Benutzende, Datenschutzbeauftragte]

Für alle Tätigkeiten, die sich auf die Sicherheit der in den Fahrzeugen verarbeiteten Informationen auswirken können, MUSS vorher geregelt werden, ob sie in den Fahrzeugen durchgeführt werden dürfen. Hierbei MUSS klar geregelt werden, welche Informationen dabei transportiert und bearbeitet werden dürfen. Ergänzend MUSS festgelegt werden, welche Schutzvorkehrungen dabei zu treffen sind. Dies MUSS für jede Art von Information gelten, auch für Gespräche in den Fahrzeugen. Es MUSS geklärt werden, unter welchen Rahmenbedingungen Mitarbeitende auf welche Art von Informationen ihrer Institution zugreifen dürfen.

Außerdem MUSS geregelt werden, in welchem Umfang Infotainmentsysteme, Anwendungen und sonstige Services der Fahrzeuge genutzt werden dürfen. Des Weiteren MUSS festgelegt werden, wie Schnittstellen abzusichern sind. In bestehende Geschäfts- bzw. Dienstanweisungen MUSS beschrieben werden, wie mitgeführte IT in den Fahrzeugen verwendet und aufbewahrt werden darf.

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.11.A4 Erstellung einer Sicherheitsrichtlinie (S) [Fachverantwortliche, IT-Betrieb]

Alle relevanten Sicherheitsanforderungen für die IT innerhalb der Fahrzeuge SOLLTEN in einer für Mitarbeitende verpflichtenden Sicherheitsrichtlinie dokumentiert werden. Die Richtlinie SOLLTE allen relevanten Mitarbeitenden der Institution bekannt sein und die Grundlage für ihren Umgang mit Fahrzeugen darstellen. In der Richtlinie SOLLTEN die Zuständigkeiten für einzelne Aufgaben klar geregelt sein. Die Sicherheitsrichtlinie SOLLTE regelmäßig überprüft und anlassbezogen aktualisiert werden.

INF.11.A5 Erstellung einer Inventarliste (S)

Für jedes Fahrzeug SOLLTE eine Inventarliste über

- die im Fahrzeug fest verbauten oder zugehörigen IT-Komponenten (z. B. Handfunkgeräte bei Einsatzfahrzeugen),
- die Fachverfahren, die auf den integrierten IT-Komponenten ausgeführt werden,

- Handlungsanweisungen und Betriebsdokumentationen sowie
- die mit dem Infotainmentsystem gekoppelten Mobilgeräte

geführt werden. Die Inventarliste SOLLTE regelmäßig und anlassbezogen aktualisiert werden. Dabei SOLLTE überprüft werden, ob noch alle inventarisierten zum Fahrzeug gehörenden IT-Komponenten vorhanden sind. Zusätzlich SOLLTE anhand der Inventarliste überprüft werden, ob keine mobilen Endgeräte unerlaubt mit dem Infotainmentsystem gekoppelt worden sind.

INF.11.A6 Festlegung von Handlungsanweisungen (S) [Fachverantwortliche, Benutzende]

Für alle wesentlichen Situationen, die die Informationssicherheit von Fahrzeugen betreffen, SOLLTEN Handlungsanweisungen in Form von Checklisten vorliegen. Die Handlungsanweisungen SOLLTEN dabei in die Sicherheitsrichtlinie integriert werden und in geeigneter Form als Checklisten verfügbar sein, während das Fahrzeug benutzt wird. Hierbei SOLLTE auch der Fall berücksichtigt werden, dass das Fahrzeug selbst gestohlen wird. Die Handlungsanweisungen SOLLTEN insbesondere nachfolgende Szenarien behandeln:

- Ausfall von IT-Komponenten der Fahrzeuge,
- Notfallsituationen wie Unfälle,
- unerlaubtes Betreten der Fahrzeuge sowie
- Diebstahl der Fahrzeuge oder darin abgelegter Gegenstände mit Relevanz für die Informationssicherheit.

Die Zuständigkeiten für die einzelnen Aufgaben SOLLTEN in der Checkliste dokumentiert sein. Die Anweisungen SOLLTEN von den Fahrzeugbenutzenden in den entsprechenden Situationen angewendet werden. Anhand der Checkliste SOLLTE dokumentiert werden, wie sie in diesen Situationen vorgegangen sind.

INF.11.A7 Sachgerechter Umgang mit Fahrzeugen und schützenswerten Informationen (S) [Fachverantwortliche, Benutzende]

Die Institution SOLLTE die Handlungsanweisungen zur Fahrzeugbenutzung um Aspekte ergänzen, wann, wie und wo Fahrzeuge sachgerecht abgestellt bzw. angedockt werden dürfen. Hierbei SOLLTE primär die Frage beantwortet werden, welche Umgebungen die Fahrzeuge angemessenen vor unerlaubten Zutritt oder Sachbeschädigung schützen. Des Weiteren SOLLTE hierbei berücksichtigt werden, welche Informationen und IT-Systeme in den Fahrzeugen aufbewahrt werden dürfen. Ausreichende Maßnahmen zum Zutrittsschutz SOLLTEN ergriffen werden.

Die Ladung der Fahrzeuge SOLLTE sicher verstaut werden. Es SOLLTE sichergestellt werden, dass schützenswerte Informationen nicht von außerhalb der Fahrzeuge von Unbefugten eingesehen, mitgehört oder entwendet werden können. Die Mitarbeitenden SOLLTEN mit der grundlegenden Funktionsweise der Fahrzeuge und den betreffenden IT-Komponenten vertraut gemacht werden. Die Mitarbeitenden SOLLTEN auch über die bestehenden Sicherheitsrisiken informiert werden.

INF.11.A8 Schutz vor witterungsbedingten Einflüssen (S) [Benutzende, Fachverantwortliche]

Fahrzeuge und die darin verbauten IT-Komponenten SOLLTEN vor witterungsbedingten Einflüssen ausreichend geschützt werden. Je nach Fahrzeugart, Einsatzort und Einsatzumgebung SOLLTEN zusätzliche Schutzmaßnahmen ergriffen werden. Für kurzfristig auftretende extreme Wettererscheinungen SOLLTEN entsprechende Schutzmaßnahmen getroffen werden.

Diese Schutzmaßnahmen SOLLTEN in den Handlungsanweisungen zur Fahrzeugbenutzung in Form von Checklisten dokumentiert werden.

INF.11.A9 Sicherstellung der Versorgung (S) [Fachverantwortliche]

Bevor Fahrzeuge eingesetzt werden, SOLLTE geplant werden, wie diese mit Betriebsstoffen während des Einsatzes versorgt werden. Die Fahrzeuge SOLLTEN dabei während des Einsatzes immer ausreichend mit Betriebsstoffen versorgt werden.

INF.11.A10 Aussonderung (S) [IT-Betrieb, Fachverantwortliche]

Werden Fahrzeuge ausgesondert, SOLLTEN keine schützenswerten Informationen in den Fahrzeugen verbleiben. Bevor Fahrzeuge endgültig ausgesondert werden, SOLLTE anhand der Inventarliste geprüft werden, ob keine inventarisierten Gegenstände und darüber hinaus relevanten Gegenstände zurückgelassen worden sind.

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.11.A11 Ersatzvorkehrungen bei Ausfällen (H) [Fachverantwortliche]

Für den Fall, dass Fahrzeuge oder Fahrzeugführende ausfallen, SOLLTEN innerhalb der Institution vorbereitende Maßnahmen getroffen werden. Abhängig von der Bedeutung der Fahrzeuge SOLLTEN Ersatzfahrzeuge bereitstehen oder alternativ ein Rahmenvertrag mit einer geeigneten Fremdinstitution geschlossen werden. Zusätzlich dazu SOLLTEN Ersatzfahrzeugführende verfügbar sein.

INF.11.A12 Diebstahlsicherung bzw. Bewachung (H) [Fachverantwortliche, Mitarbeitende]

Eine Alarmanlage SOLLTE vorhanden sein. Bei Bodenfahrzeugen SOLLTE darüber hinaus eine Wegfahrsperre vorhanden sein. Wird das Fahrzeug verlassen, SOLLTEN die Alarmanlage und Wegfahrsperre aktiviert werden. Alternativ SOLLTEN die Fahrzeuge bewacht werden.

INF.11.A13 Schädigende Fremdeinwirkung (H) [Fachverantwortliche]

Je nach Art der Fahrzeuge SOLLTEN geeignete Maßnahmen ergriffen werden, um die Fahrzeuge vor potentieller Fremdeinwirkung in der geplanten Einsatzumgebung zu schützen, wie z. B. störenden Funkstrahlen.

INF.11.A14 Schutz sensibler Informationen vor unbefugtem Zugriff und Kenntnisnahme (H) [IT-Betrieb, Fachverantwortliche]

Fahrzeuge und die dazugehörigen IT-Komponenten SOLLTEN so abgesichert werden, dass sensible Informationen durch Unbefugte nicht ausgelesen bzw. manipuliert oder gelöscht werden können. Hierbei SOLLTEN die vorhandenen Schutzvorkehrungen der herstellenden Unternehmen überprüft und bei Bedarf angepasst werden.

INF.11.A15 Physische Absicherung der Schnittstellen (H) [IT-Betrieb, Fachverantwortliche]

Alle physischen internen und externen Schnittstellen der Fahrzeuge SOLLTEN physisch gegen unbefugte Benutzung und äußere Einflüsse abgesichert werden.

INF.11.A16 Brandlöschanlage (H) [Fachverantwortliche]

Die Fahrzeuge SOLLTEN über eine Brandlöschanlage verfügen, die einen Brand von außen und innen löschen kann. Alternativ SOLLTEN geeignete Mittel zur Brandbekämpfung mitgeführt werden.

INF.11.A17 Netztrennung des In-Vehicle-Network mit einem Sonderfahrzeugnetz über Gateways (H)

Generell SOLLTE die Institution sicherstellen, dass keine Informationen unerlaubt und undefiniert zwischen

- dem In-Vehicle-Network (IVN), das wiederum an die Netze der fahrzeugherstellenden Unternehmen angebunden ist und
- den einsatzspezifischen IT-Komponenten

ausgetauscht werden. Hierzu SOLLTEN Gateways mit standardisierten Protokollen (z. B. nach Standard CiA 447) eingesetzt werden. Die Gateways SOLLTEN dabei vom fahrzeugherstellenden Unternehmen freigegeben sein.

4. Weiterführende Informationen

4.1. Wissenswertes

Der wissenschaftliche Artikel „IT-Sicherheit und Datenschutz im vernetzten Fahrzeug“ des Fraunhofer Instituts (DOI: 10.1007/s11623-015-0434-4) gibt einen generellen Überblick über vernetzte Fahrzeuge, mögliche Anwendungen, die benötigten Daten und die sich daraus ergebenden Bedrohungen.

Der wissenschaftliche Artikel „Security Issues and Vulnerabilities in Connected Car Systems" von der IEEE Konferenz 2015 zeigt auf, welche neuen Bedrohungen durch die Fahrzeugvernetzung entstehen.

Bundesamt
für Sicherheit in der
Informationstechnik

INF.12 Verkabelung

1. Beschreibung

1.1. Einleitung

Die ordnungsgemäße und normgerechte Ausführung der Verkabelung ist Grundlage für einen sicheren IT-Betrieb. Dabei muss grundsätzlich zwischen der elektrotechnischen Verkabelung und der IT-Verkabelung unterschieden werden.

Die elektrotechnische Verkabelung von IT-Systemen und anderen Geräten umfasst alle Kabel und Verteilungen im Gebäude vom Einspeisepunkt des Verteilungsnetzbetreibers (VNB) bis zu den Anschlüssen der Endgeräte.

Die IT-Verkabelung in einer Institution umfasst alle Kommunikationskabel und passiven Komponenten wie Rangier- bzw. Spleißverteiler oder Patchfelder. Sie bildet also die physikalische Grundlage der internen Kommunikationsnetze. Die IT-Verkabelung reicht von den Übergabepunkten aus einem Fremdnetz bis zu den Anschlusspunkten der Netzteilnehmenden. Übergabepunkte sind z. B. der Anschluss eines Telekommunikationsunternehmens oder die DSL-Anbindung eines Internet-Providers.

Trotz dieser Unterscheidung sind die grundlegenden Anforderungen an beide Arten der Verkabelung identisch. Daher sollte die Verkabelung innerhalb einer Institution immer auch als Ganzes betrachtet werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die gesamte elektrotechnische Verkabelung und IT-Verkabelung vor Ausfall, Manipulation und Störung zu schützen.

1.3. Abgrenzung und Modellierung

Der Baustein INF.12 *Verkabelung* ist einmal auf die Verkabelung in Gebäuden und Räumen anzuwenden, zusätzlich zum Baustein INF.1 *Allgemeines Gebäude*. Die Anforderungen des Bausteins sind immer sowohl auf die IT- als auch auf die elektronische Verkabelung anzuwenden.

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.12 *Verkabelung* von besonderer Bedeutung.

2.1. Kabelbrand

Kabelbrände können einen Informationsverbund erheblich schädigen. Ein Kabelbrand verursacht z. B. Kurzschlüsse oder unterbricht Leiter. Infolgedessen fallen auch Schutzeinrichtungen aus. Zudem können bei Kabelbränden, abhängig von den Materialien der Isolierungen, aggressive Gase entstehen.

2.2. Unzureichende Dimensionierung der Verkabelung

Werden Arbeitsplätze, Serverräume oder Rechenzentren geplant, dann werden diese Pläne häufig ausschließlich am aktuellen Bedarf ausgerichtet. Jedoch verlangen zukünftige neue Anforderungen oft auch nach weiteren Kapazitäten des Stromnetzes und der Datenkabel. Dies kann z. B. notwendig werden, sobald zusätzliche Server eingesetzt werden oder sich technische Standards ändern. Die Verkabelung kann aber nur in dem Umfang erweitert werden, den die bereits vorhandenen und verlegten Kabel und Kabeltrassen zulassen.

2.3. Unzureichende Dokumentation der Verkabelung

Wenn die genaue Lage von Kabeln nicht bekannt ist, weil sie unzureichend dokumentiert wurde, dann können diese Kabel bei Bauarbeiten außerhalb oder innerhalb eines Gebäudes beschädigt werden. Eine unzureichende Dokumentation erschwert es auch, Kabel zu prüfen und zu reparieren.

Darüber hinaus kann nicht davon ausgegangen werden, dass alle Kabel in den Installationszonen nach aktuell gültigen Normen installiert sind.

2.4. Unzureichend geschützte Verteiler

Gelegentlich sind Verteilungen des Stromversorgungs- oder Datennetzes unverschlossen in Bereichen installiert, die allgemein zugänglich sind. Unbefugte Personen können solche Verteiler öffnen, manipulieren und so Ausfälle in der Strom- oder Datenversorgung herbeizuführen.

2.5. Leitungsbeschädigungen

Je ungeschützter ein Kabel verlegt ist, desto größer ist die Gefahr, dass es absichtlich oder unabsichtlich beschädigt wird. Beschädigungen verursachen nicht nur direkte Ausfälle von Verbindungen, sondern können auch später zu Störungen führen. Eine beschädigte Isolierung beeinträchtigt unter Umständen erst mit großer zeitlicher Verzögerung die funktionellen Eigenschaften eines Kabels.

2.6. Spannungsschwankungen, Überspannung, Unterspannung

Schwankungen der Versorgungsspannung können in allen Bereichen der Netze entstehen. Extrem kurze und kleine Ereignisse wirken sich kaum oder gar nicht auf IT-Systeme aus. Größere Schwankungen führen jedoch zu Funktionsstörungen. Die angeschlossenen Systeme können beschädigt werden bis hin zu Totalausfällen. Auch zerstörerische Überspannungen können auftreten.

2.7. Verwendung qualitativ unzureichender Steckdosenleisten

Oft reichen die fest installierten Steckdosen für die zu betreibenden Geräte nicht aus. Um dies auszugleichen, werden häufig Steckdosenleisten verwendet. Sind diese Steckdosenleisten jedoch qualitativ unzureichend, dann können sie zur Zündquelle und damit zu einer großen Brandgefahr werden.

In vielen Fällen werden mehrere Steckdosenleisten hintereinander geschaltet, um Steckplätze für alle Geräte bereitzustellen. Bei einer solchen Reihenschaltung besteht die Gefahr der Überlastung. Die Folge kann ein unvollständiger Kurzschluss mit hoher Brandgefahr sein.

2.8. Unzulässige Kabelverbindungen

In manchen Fällen werden zwischen IT-Systemen oder anderen technischen Komponenten Kabelverbindungen hergestellt, die nicht vorgesehen und unzulässig sind. Dies kann Sicherheitsprobleme oder Betriebsstörungen verursachen.

So ermöglichen solche Kabelverbindungen unter Umständen, dass unerlaubt auf Datennetze, IT-Systeme, Informationen oder Anwendungen zugegriffen werden kann. Durch unzulässige Kabelverbindungen können Informationen auch zu falschen Empfangenden übertragen werden. Zudem kann die Verbindung gestört werden.

2.9. Leitungsbeeinträchtigungen

Die elektrische Signalübertragung in Kommunikationskabeln kann durch elektrische und magnetische Felder negativ beeinflusst werden. Eine spezielle Form dieser Leitungsbeeinträchtigung ist Übersprechen. Dabei werden Ströme und Spannungen von benachbarten Leitungen als Störsignale auf das Kommunikationskabel übertragen.

2.10. Abhören und Manipulation von Kabeln

Abhörangriffe auf Datenkabel sind eine Gefahr für die Informationssicherheit, die nicht vernachlässigt werden sollte. Grundsätzlich gibt es keine abhörsicheren Kabel. Die Kabel unterscheiden sich in ihrer Qualität lediglich hinsichtlich des Aufwands, der zum Abhören der Leitung betrieben werden muss. Ob ein Kabel tatsächlich abgehört wird, ist nur mit hohem messtechnischem Aufwand feststellbar.

Daneben stellen bewusste Manipulationen von Kabeln bis hin zu ihrer Zerstörung eine Gefahr für die Institution dar. Fehlfunktionen von Kabeln können in manipulativer Absicht bewusst herbeigeführt werden. Solche Manipulationen verfolgen oftmals das Ziel, den IT-Betrieb zu stören oder die Institution zu schädigen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.12 *Verkabelung* 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	Fachverantwortliche
Weitere Zuständigkeiten	IT-Betrieb, Haustechnik

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.12.A1 Auswahl geeigneter Kabeltypen (B) [IT-Betrieb, Haustechnik]

Bei der Auswahl von Kabeltypen MUSS geprüft werden, welche übertragungstechnischen Eigenschaften notwendig sind. Die einschlägigen Normen und Vorschriften MÜSSEN beachtet werden. Auch die Umgebungsbedingungen im Betrieb und bei der Verlegung MÜSSEN berücksichtigt werden. Hinsichtlich der Umgebungsbedingungen MÜSSEN die folgenden Faktoren beachtet werden:

- Temperaturen,
- Kabelwege,
- Zugkräfte bei der Verlegung,
- die Art der Verlegung sowie
- die Entfernung zwischen den Endpunkten und möglichen Störquellen.

INF.12.A2 Planung der Kabelführung (B) [IT-Betrieb, Haustechnik]

Kabel, Kabelwege und Kabeltrassen MÜSSEN aus funktionaler und aus physikalischer Sicht ausreichend dimensioniert werden. Dabei MÜSSEN künftige Notwendigkeiten eingerechnet werden, z. B. genügend Platz für mögliche technische Erweiterungen in Kabelkanälen und -trassen. Bei der gemeinsamen Führung von IT- und Stromverkabelung in einer Trasse MUSS das Übersprechen zwischen den einzelnen Kabeln verhindert werden. Es MUSS darauf geachtet werden, dass die IT-Verkabelung und die elektrotechnische Verkabelung mit dem normgerechten Trennungsabstand geführt werden. Erkennbare Gefahrenquellen MÜSSEN umgangen werden.

INF.12.A3 Fachgerechte Installation (B) [IT-Betrieb, Haustechnik]

Die Installationsarbeiten der Verkabelung MÜSSEN fachkundig und sorgfältig erfolgen. Bei der Installation MÜSSEN alle relevanten Normen beachtet werden. Die fachgerechte Ausführung der Verkabelung MUSS durch eine fachkundige Person in allen Phasen überprüft werden. Bei Anlieferung des Materials MUSS geprüft werden, ob die richtigen Kabel und Anschlusskomponenten geliefert wurden. Es MUSS darauf geachtet werden, dass die Montage keine Beschädigungen verursacht. Außerdem MÜSSEN die Kabelwege so gewählt werden, dass eine Beschädigung der verlegten Kabel durch die normale Nutzung des Gebäudes ausgeschlossen ist.

INF.12.A4 EMV-taugliche Stromversorgung (B) [Haustechnik]

Die Stromversorgung MUSS EMV (Elektromagnetische Verträglichkeit) -tauglich sein. Dafür MUSS das Stromverteilnetz als TN-S-System aufgebaut sein. Bei Aufbau und Betrieb des Stromverteilnetzes MÜSSEN die in den entsprechenden Normen empfohlenen Trennungsabstände soweit wie möglich eingehalten werden. Vorkehrungen gegen Einstrahlungen von außen, Abstrahlung durch die Stromleitung sowie zur Erkennung von Ausgleichsströmen MÜSSEN getroffen 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.12.A5 Anforderungsanalyse für die Verkabelung (S) [IT-Betrieb, Haustechnik]

Grundsätzlich SOLLTEN die Anforderungen analysiert werden, die Einfluss auf eine zukunftssichere, bedarfsgerechte und wirtschaftliche Ausführung der Verkabelung haben. In dieser Anforderungsanalyse SOLLTE zunächst abgeschätzt werden, wie die kurzfristige Nutzung der

Verkabelung innerhalb der Institution aussieht. Darauf aufbauend SOLLTE die längerfristige Entwicklung der Nutzung abgeschätzt werden. Darüber hinaus MÜSSEN die Schutzziele der Verfügbarkeit, Integrität und Vertraulichkeit bei der Anforderungsanalyse für die Verkabelung mit betrachtet werden.

INF.12.A6 Abnahme der Verkabelung (S) [IT-Betrieb, Haustechnik]

Für die Verkabelung SOLLTE es einen Abnahmeprozess geben. Verkabelungen SOLLTEN immer dann abgenommen werden, wenn alle (gegebenenfalls im Rahmen eines Meilensteins) durchzuführenden Aufgaben abgeschlossen sind. Die Ausführenden SOLLTE hierfür die Aufgaben als abgeschlossen und zur Abnahme bereit gemeldet haben. Außerdem SOLLTEN sich bei den Kontrollen durch die auftraggebende Institution keine inakzeptablen Mängel gezeigt haben. Der Abnahmetermin SOLLTE so gewählt werden, dass die Kontrollen zur Abnahme in ausreichender Zeit vorbereitet werden können. Die auftragnehmende Institution MUSS spätestens zum Abnahmetermin schriftlich belegen, dass sämtliche Normen und Vorschriften eingehalten wurden, die für das Gewerk gelten. Bei der Abnahme MUSS der tatsächliche Umfang der Leistungen überprüft werden. Für das Abnahmeprotokoll SOLLTE eine Checkliste vorbereitet werden. Das Abnahmeprotokoll MUSS von den Teilnehmenden und Verantwortlichen rechtsverbindlich unterzeichnet werden. Das Protokoll MUSS Bestandteil der internen Dokumentation der Verkabelung sein.

INF.12.A7 Überspannungsschutz (S) [Haustechnik]

Jedes elektrisch leitende Netz SOLLTE gegen Überspannungen geschützt werden. Hierfür MUSS ein entsprechendes Überspannungsschutzkonzept erstellt werden, das den gültigen Normen entspricht. Netzersatzanlagen (NEA) und unterbrechungsfreie Stromversorgungen (USV) MÜSSEN in das Überspannungsschutzkonzept aufgenommen werden.

INF.12.A8 Entfernen und Deaktivieren nicht mehr benötigter Kabel (S) [IT-Betrieb, Haustechnik]

Wenn Kabel nicht mehr benötigt werden, SOLLTEN sie fachgerecht und vollständig entfernt werden. Nachdem Kabel entfernt wurden, MÜSSEN die Brandschottungen fachgerecht verschlossen werden.

Kabel, die aktuell nicht mehr benötigt werden, aber mit der vorhandenen Technik sinnvoll als Reserve an Ort und Stelle verbleiben können, SOLLTEN in einem betriebsfähigen Zustand erhalten werden. Solche Kabel MÜSSEN mindestens an den Endpunkten entsprechend gekennzeichnet werden.

Grundsätzlich SOLLTE eine Übersicht über nicht mehr benötigte Kabel aufgestellt werden. Aus der Dokumentation SOLLTE hervorgehen, welche Kabel entfernt oder deaktiviert wurden.

INF.12.A9 Brandschutz in Trassen (S) [Haustechnik]

Trassen SOLLTEN ausreichend dimensioniert werden. Trassen SOLLTEN über eine ausreichende Be- und Entlüftung verfügen.

INF.12.A10 Dokumentation und Kennzeichnung der Verkabelung (S) [IT-Betrieb, Haustechnik]

Eine Institution SOLLTE sicherstellen, dass sie für ihre Verkabelung sowohl über eine interne als auch eine externe Dokumentation verfügt. Die interne Dokumentation MUSS alle Aufzeichnungen zur Installation und zum Betrieb der Verkabelung enthalten. Die interne Dokumentation SOLLTE so umfangreich angefertigt und gepflegt werden, dass der Betrieb und dessen Weiterentwicklung bestmöglich unterstützt werden. Die externe Dokumentation (Beschriftung von Anschlüssen zur Unterstützung des Betriebs) der Verkabelung SOLLTE möglichst neutral gehalten werden.

Jede Veränderung im Netz SOLLTE dokumentiert werden. Eine Interims- oder Arbeitsversion der Dokumentation SOLLTE unmittelbar, d. h. am Tag selbst angepasst werden. Die Stamm-Dokumentation MUSS spätestens 4 Wochen nach Abschluss der jeweiligen Arbeiten aktualisiert sein. Es SOLLTE geprüft werden, ob ein Dokumentenmanagement für die Dokumentation eingesetzt werden kann. Die Dokumentation SOLLTE regelmäßig überprüft und aktualisiert werden. Sämtliche

technischen Einrichtungen, die im Rahmen der Verkabelung dokumentiert sind, MÜSSEN hinsichtlich der Dokumentationstreue spätestens nach 4 Jahren geprüft werden.

INF.12.A11 Neutrale Dokumentation in den Verteilern (S) [IT-Betrieb, Haustechnik]

In jedem Verteiler SOLLTE es eine Dokumentation geben, die den derzeitigen Stand von Rangierungen und Leitungsbelegungen wiedergibt. Die Dokumentation im Verteiler MUSS ein sicheres Schalten ermöglichen.

Die Dokumentation im Verteiler SOLLTE möglichst neutral gehalten werden. In der Dokumentation im Verteiler SOLLTEN nur bestehende und genutzte Verbindungen sowie auflaufende Reservekabel aufgeführt sein. Falls möglich, SOLLTEN keine Hinweise auf die Art gegeben werden, wie Kabel genutzt werden. Es SOLLTEN nur solche Hinweise gegeben werden, die ausdrücklich vorgeschrieben sind. Alle weitergehenden Informationen SOLLTEN in einer Revisionsdokumentation aufgeführt werden.

INF.12.A12 Kontrolle elektrotechnischer Anlagen und bestehender Verbindungen (S) [IT-Betrieb, Haustechnik]

Alle elektrischen Anlagen und Betriebsmittel SOLLTEN gemäß DGUV Vorschrift 3, entsprechend den in § 5 Prüfung genannten Durchführungsanweisungen, regelmäßig geprüft werden. Alle Unregelmäßigkeiten, die festgestellt werden, MÜSSEN unverzüglich dokumentiert werden. Festgestellte Unregelmäßigkeiten MÜSSEN unverzüglich den zuständigen Organisationseinheiten gemeldet werden. Die zuständigen Organisationseinheiten MÜSSEN die festgestellten Unregelmäßigkeiten so zeitnah beheben, dass eine Gefährdung von Personen ausgeschlossen werden kann. Die Verfügbarkeit der elektrischen Anlagen und Betriebsmittel MUSS hierbei im erforderlichen Maß sichergestellt sein.

INF.12.A13 Vermeidung elektrischer Zündquellen (S) [Haustechnik]

Die Nutzung privater Elektrogeräte innerhalb einer Institution SOLLTE klar geregelt werden. Alle Elektrogeräte MÜSSEN durch eine Elektrofachkraft geprüft und für sicher befunden werden, bevor sie eingesetzt werden. Die Verwendung von Steckdosenleisten SOLLTE soweit wie möglich vermieden werden. Fehlende Steckdosen SOLLTEN durch eine Elektrofachkraft fachgerecht nachgerüstet 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.12.A14 A-B-Versorgung (H) [Haustechnik]

Es SOLLTE geprüft werden, ob anstelle einer einzügigen Stromversorgung eine zweizügige sogenannte A-B-Versorgung geschaffen werden soll, die wichtige IT-Komponenten und andere Verbraucher versorgt. Dabei SOLLTE die Funktionsfähigkeit der Stromversorgung permanent durch geeignete technische Einrichtungen überwacht werden.

INF.12.A15 Materielle Sicherung der Verkabelung (H) [IT-Betrieb, Haustechnik]

Für alle Räume eines Gebäudes, insbesondere in Räumen mit Publikumsverkehr sowie in unübersichtlichen Bereichen SOLLTE überlegt werden, Kabel und Verteiler gegen unbefugte Zugriffe zu sichern. In jedem Fall SOLLTEN die Zahl und der Umfang derjenigen Stellen möglichst gering gehalten werden, an denen Einrichtungen der Energieversorgung und Zugangspunkte des Datennetzes für Unbefugte zugänglich sind.

INF.12.A16 Nutzung von Schranksystemen (H) [Haustechnik]

Elektrotechnische Anschlüsse und -verteiler SOLLTEN in Schranksystemen aufgestellt oder in diese eingebaut werden. Bei der Dimensionierung der Schranksysteme SOLLTE das erwartete Wachstum für den geplanten Einsatzzeitraum berücksichtigt werden.

INF.12.A17 Redundanzen für die IT-Verkabelung (H) [IT-Betrieb]

Es SOLLTE geprüft werden, ob eine redundante primäre IT-Verkabelung geschaffen werden soll, die über unabhängige Trassen geführt wird. Ebenso SOLLTE geprüft werden, ob die Anschlüsse an IT- oder TK-Provider redundant ausgelegt werden sollen. Bei hohen oder sehr hohen Verfügbarkeitsanforderungen SOLLTE überlegt werden, in den relevanten Gebäuden die Sekundär- und Tertiärverkabelung redundant auszulegen. Dabei SOLLTEN redundant ausgelegte Teile der Sekundärverkabelung in unterschiedlichen Brandabschnitten geführt werden. Wird eine redundante Verkabelung verwendet, SOLLTE deren Funktionsfähigkeit regelmäßig geprüft werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Deutsche Institut für Normung formuliert Vorgaben, die für die Verkabelung relevant sind. Hierbei handelt es sich um folgende Normen:

- DIN 4102, Brandverhalten von Baustoffen und Bauteilen
- DIN IEC 60364, Einrichten von Niederspannungsanlagen
- IEC 62305, Merkblatt: Die Blitzschutz-Normen DIN EN 62305 / VE 01805-305:2006
- IN VDE 0100, Errichten von Niederspannungsanlagen
- DIN VDE 0105-100, Betrieb von elektrischen Anlagen
- DIN 41494, Bauweisen für elektronische Einrichtungen
- DIN EN 50173, Informationstechnik - Anwendungsneutrale Kommunikationskabelanlagen
- DIN EN 50174, Informationstechnik - Installation von Kommunikationsverkabelung
- DIN EN 50310:2017-02, Telekommunikationstechnische Potentialausgleichsanlage für Gebäude und andere Strukturen
- DIN EN 50346:2010-02, Informationstechnik - Installation von Kommunikationsverkabelung - Prüfen installierter Verkabelung
- DIN IEC 60297, Bauweise für elektronische Einrichtungen

Die Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege (BGW) hat in der DGUV Vorschrift 3: „Elektrische Anlagen und Betriebsmittel, Unfallverhütungsvorschrift“ weitere Vorschriften für die elektrotechnische Verkabelung veröffentlicht.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 11801:2002-09 „Informationstechnik - Anwendungsneutrale Standortverkabelung" Vorgaben für die IT-Verkabelung.

Bundesamt
für Sicherheit in der
Informationstechnik

INF.13 Technisches Gebäudemanagement

1. Beschreibung

1.1. Einleitung

Das Gebäudemanagement (GM), auch Facility Management genannt, ist für alle Leistungen zuständig, die in der Planungs- und Nutzungsphase von Gebäuden, Gebäudekomplexen, Liegenschaften oder Liegenschaftsportfolios anfallen. Im Folgenden wird hierfür einheitlich der Begriff Gebäude genutzt. Ausnahmen hiervon werden explizit genannt.

Das GM ist standort- sowie objektbezogen ausgerichtet. Es lässt sich in technisches, infrastrukturelles und kaufmännisches GM untergliedern.

Das technische Gebäudemanagement (TGM) umfasst gemäß DIN 32736 alle Leistungen, die die technische Funktion und Verfügbarkeit eines Gebäudes erhalten. Zu diesen Leistungen gehören unter anderem:

- Betreiben
- Dokumentieren
- Energie- und Umweltmanagement
- Informationsmanagement
- Modernisieren
- Sanieren
- Umbauen
- Verfolgen der technischen Gewährleistung

Wesentliche technische Funktionen eines Gebäudes werden durch die technische Gebäudeausrüstung (TGA) bereitgestellt, die durch das TGM betrieben, gepflegt und weiterentwickelt wird. Die TGA umfasst dabei gemäß VDI 4700 Blatt 1 alle im Bauwerk eingebauten und damit verbundenen technischen und nutzungsspezifischen Einrichtungen sowie technische Einrichtungen in Außenanlagen und Ausstattungen (siehe auch Kapitel 4.1 *Genutzte TGM-spezifische Fachbegriffe*). Falls die TGA automatisiert und gewerkübergreifend betrieben werden soll, wird zusätzliche technische Infrastruktur zur Gebäudeautomation (GA, engl. Building Automation and Control Systems, BACS) eingesetzt. Somit ist die GA ein zentrales Werkzeug des TGM. Ein Gebäude kann durch TGM auch ohne

GA betrieben werden, GA hingegen ist immer durch TGM flankiert. Gewisse Komponenten der GA sind dabei auch der TGA zuzurechnen, wie z. B. echtzeitfähige Industrial Ethernet Switches.

Während die TGA in der Vergangenheit meist unabhängig von der IT und der Prozessleit- und Automatisierungstechnik (Operational Technology, OT) betrieben wurde, werden heute zunehmend Netzübergänge zu diesen Bereichen etabliert. Hinzu kommt, dass Teile der TGA rund um die Uhr genutzt werden. Daher müssen Änderungen oft parallel zur produktiven Nutzung durchgeführt werden.

Auch im TGM müssen die Grundwerte der Informationssicherheit berücksichtigt werden, denn der Verlust von Verfügbarkeit, Vertraulichkeit und Integrität von Systemen kann im TGM weitreichende Auswirkungen bis hin zur Gefährdung von Leib und Leben nach sich ziehen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei Planung, Umsetzung und Betrieb im Rahmen des TGM zu etablieren.

1.3. Abgrenzung und Modellierung

Der Baustein INF.13 *Technisches Gebäudemanagement* ist auf das TGM einer Institution anzuwenden, sobald Gebäude mit TGA geplant, gebaut oder betrieben werden.

Dieser Baustein behandelt das TGM, somit die Aufgaben und Prozesse, die für die Planung und den Betrieb der TGA-Anlagen (siehe Kapitel 4.1 Genutzte TGM-spezifische Fachbegriffe) eines Gebäudes erforderlich sind. Die technische Infrastruktur für den automatisierten Betrieb von Gebäuden wird im Baustein INF.14 *Gebäudeautomation* behandelt. Letzterer muss zusätzlich zum Baustein INF.13 *Technisches Gebäudemanagement* angewendet werden, wenn die zu betreibende TGA automatisiert und anlagenübergreifend gesteuert wird. In diesem Sinne umfasst das TGM auch die Prozesse der GA.

Weiterhin ist es möglich, dass zu den zu verwaltenden Systemen auch solche gehören, die durch Bausteine aus den Schichten IND *Industrielle IT* und SYS *IT-Systeme* modelliert werden, z. B. IND.2.1 *Allgemeine ICS-Komponente* oder auch SYS.4.4 *Allgemeines IoT-Gerät*. Darüber hinaus müssen die für das TGM relevanten Aspekte der Schichten ORP und OPS beachtet werden, insbesondere die Teilschichten OPS.1 *Eigener Betrieb* und OPS.2 *Betrieb von Dritten* sowie die Bausteine ORP.2 *Personal* und ORP.4 *Identitäts- und Berechtigungsmanagement*. Werden für das TGM Cloud-Dienste eingesetzt, muss für die Auswahl dieser Dienste der Baustein OPS.2.2 *Cloud-Nutzung* berücksichtigt werden.

Zur Absicherung von Fernzugängen im TGM sind die Bausteine OPS.1.2.5 *Fernwartung* und IND.3.2 *Fernwartung im industriellen Umfeld* anzuwenden.

Der Baustein INF.13 *Technisches Gebäudemanagement* behandelt nicht die physische Sicherheit von Gebäuden, diese wird in dem Baustein INF.1 *Allgemeines Gebäude* behandelt. Ebenso spielt der Aspekt der Safety in diesem Baustein keine hervorgehobene Rolle, sondern wird im Baustein IND.2.7 *Safety Instrumented Systems* behandelt.

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.13 *Technisches Gebäudemanagement* von besonderer Bedeutung.

2.1. Fehlende Grundlagen für die Planung des TGM

Wenn beim Bau eines Gebäudes die Nachfrageorganisationen (siehe Kapitel 4.1 Genutzte TGM-spezifische Fachbegriffe) noch nicht feststehen, fehlen Kontaktpersonen, Zielsetzung und Bedarfe für

das TGM. Das kann dazu führen, dass das TGM im Betrieb nicht dem tatsächlichen Bedarf entspricht, weil dieser zum Zeitpunkt der Planung und Umsetzung nicht abgefragt werden konnte.

2.2. Mangelnde Dokumentation beim TGM

In das TGM ist häufig eine Vielzahl von Dienstleistenden involviert. Ist die Dokumentation der Zuständigkeiten mit Kontaktpersonen und zugehörigen SLAs unvollständig oder nicht zugänglich, führt dies im Ernstfall, wenn wichtige Systeme ausfallen, zu vermeidbaren Verzögerungen, die gegebenenfalls sogar Personenschaden zur Folge haben können.

Eine fehlende Dokumentation von Sicherheitszertifizierungen der TGA-Anlagen inklusive Terminen für notwendige Erneuerung kann dazu führen, dass abgelaufene Zertifizierungen nicht rechtzeitig erneuert werden. Dadurch kann gegen Gesetze verstoßen werden, je nach TGA-Anlage Gefahr für Leib und Leben entstehen und ein entstandener Schaden nicht über entsprechende Versicherungen abgewickelt werden.

2.3. Kompromittierung der Schnittstellen mit TGM

Das TGM hat technische Schnittstellen zu besonders schützenswerten Bereichen, z. B. Safety Instrumented Systems (SIS), Sicherheitsdienst und Brandmeldeanlagen. Wenn diese Schnittstellen bewusst oder unbewusst durch Fehler im TGM kompromittiert werden, dann kann dies einen Verstoß gegen Gesetze sowie Gefahr für Leib und Leben zur Folge haben.

Wird z. B. bei einem Feueralarm in einem Rechenzentrum die optische oder akustische Warnung außer Kraft gesetzt, können im Raum befindliche Personen diesen nicht rechtzeitig verlassen, bevor der Raum mit Löschgas geflutet wird. Ebenso kann ein vorgetäuschter Feueralarm dazu führen, dass Fluchttüren geöffnet werden und dadurch unberechtigter Zugang erlangt wird oder Türen geschlossen und gegebenenfalls Personen eingeschlossen werden.

2.4. Unzureichendes Monitoring der TGA

Wenn die TGA nur unzureichend durch ein entsprechendes Monitoring überwacht wird, dann werden sicherheitsrelevante Ereignisse, wie z. B. relevante Fehlfunktionen in der TGA, unter Umständen nicht oder zu spät erkannt. Dies kann je nach Ereignis zu weiteren Schäden führen oder Gefahr für Leib und Leben bedeuten.

Wird z. B. der Ausfall der Heizung bei Außentemperaturen im Minusbereich nicht gemeldet, kühlen die Räume erst stark aus, bevor der Ausfall bemerkt wird und eine Behebung eingeleitet werden kann.

2.5. Unzureichendes Rollen- und Berechtigungsmanagement

Wenn das TGM oder einzelne seiner Teile von der restlichen IT der Institution physisch getrennt werden, dann wird in der Regel auch ein dediziertes Identitäts- und Berechtigungsmanagement eingerichtet. Wenn dieses unzureichend konzipiert und umgesetzt wird, dann kann nicht ausgeschlossen werden, dass mehrere Personen dasselbe Konto nutzen oder Berechtigungen von ausgeschiedenen internen oder externen Mitarbeitenden oder Dienstleistenden nicht gelöscht wurden. Als Folge kann auf das TGM unberechtigt zugegriffen werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.13 *Technisches Gebäudemanagement* 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	Planende, IT-Betrieb, 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.13.A1 Beurteilung des Ist-Zustands bei der Übernahme bestehender Gebäude (B)

Bei der Übernahme von bestehenden Gebäuden MÜSSEN die im Gebäude installierten TGA-Anlagen, die Bausubstanz und Einrichtungen sowie vorhandene Dokumentation erfasst und hinsichtlich ihres Zustands (Alter, Supportstatus, Zukunftsfähigkeit, Vollständigkeit der Dokumentation etc.) beurteilt werden.

INF.13.A2 Regelung und Dokumentation von Verantwortlichkeiten und Zuständigkeiten im Gebäude (B) [Institutionsleitung, Planende]

Da es in einem Gebäude meist unterschiedliche Verantwortlichkeiten und Zuständigkeiten für verschiedene Bereiche gibt, MÜSSEN die entsprechenden Rechte, Pflichten, Aufgaben, Kompetenzen und zugehörigen Prozesse geregelt und dokumentiert werden.

Hierbei MÜSSEN auch die organisatorischen Strukturen im Gebäude berücksichtigt und dokumentiert werden. Insbesondere MÜSSEN alle Nachfrage- und betreibenden Organisationen erfasst werden. Wird das TGM durch eine externe Organisation betrieben, MÜSSEN die zugehörigen Rechte, Pflichten, Aufgaben und Kompetenzen gemäß Baustein OPS.2.3 *Nutzung von Outsourcing* vertraglich festgehalten werden.

Weiterhin MÜSSEN die Schnittstellen und Meldewege inklusive Eskalation zwischen allen Beteiligten festgelegt und dokumentiert werden. Auch die Koordination verschiedener betreibender Organisationen MUSS geregelt und dokumentiert werden.

Der Zugriff auf die Dokumentation MUSS geregelt werden. Die gesamte Dokumentation inklusive der zugehörigen Kontaktinformationen MUSS immer aktuell und verfügbar sein.

INF.13.A3 Dokumentation von Gebäudeeinrichtungen (B)

Alle Gebäudeeinrichtungen der TGA inklusive GA MÜSSEN dokumentiert werden. Hierbei MUSS sämtliche, auch schon vorhandene, Dokumentation zusammengeführt, aus dem Blickwinkel des TGM organisiert und um TGM-spezifische Angaben ergänzt werden.

Der Zugriff auf die Dokumentation MUSS geregelt werden. Die gesamte Dokumentation inklusive der zugehörigen Kontaktinformationen MUSS immer aktuell und verfügbar sein.

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.13.A4 Erstellung einer Sicherheitsrichtlinie für TGM (S)

Ausgehend von der allgemeinen Sicherheitsleitlinie der Institution SOLLTE eine übergeordnete Sicherheitsrichtlinie für TGM erstellt sowie nachvollziehbar umgesetzt werden. Aus dieser übergeordneten Sicherheitsrichtlinie SOLLTEN spezifische Sicherheitsrichtlinien für die verschiedenen Themenbereiche des TGM abgeleitet werden. In der Sicherheitsrichtlinie für das TGM SOLLTEN nachvollziehbar Anforderungen und Vorgaben beschrieben werden, wie das TGM umgesetzt wird. Die Sicherheitsrichtlinie SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden, um dem aktuellen Stand der Technik zu entsprechen und auch neueste Erkenntnisse abdecken zu können. Sie SOLLTE allen im Bereich TGM zuständigen Mitarbeitenden bekannt und grundlegend für ihre Arbeit sein.

INF.13.A5 Planung des TGM (S) [Planende]

Das TGM, die zugrundeliegende Infrastruktur und die zugehörigen Prozesse SOLLTEN geeignet geplant werden. Die Planung SOLLTE dabei mindestens eine detaillierte Anforderungsanalyse, eine ausreichende Grobkonzeptionierung und eine Fein- und Umsetzungsplanung umfassen.

Im Rahmen der Anforderungsanalyse SOLLTEN Anforderungen an TGM-Infrastruktur und TGM-Prozesse spezifiziert werden. Dabei SOLLTEN alle wesentlichen Elemente für das TGM berücksichtigt werden. Auch SOLLTE die Sicherheitsrichtlinie für das TGM beachtet werden. Steht die Nachfrageorganisation zum Zeitpunkt der Planung noch nicht fest, SOLLTEN im Rahmen einer universellen Planung zumindest grundlegende Anforderungen erfasst werden, die dem Stand der Technik entsprechen.

Für die Anforderungsspezifikation SOLLTEN auch die Schnittstellen der zu verwaltenden Systeme dokumentiert werden, z. B. um die Kompatibilität von TGM-Lösung und zu verwaltenden Systemen zu gewährleisten.

Außerdem SOLLTEN vor der Beauftragung von Dienstleistenden oder vor der Anschaffung von Hard- oder Software der durch das TGM zu verwaltenden Systeme die Anforderungen des TGM in einem Lastenheft des TGM spezifiziert werden. In diesem Lastenheft SOLLTE auch die Durchführung von Tests berücksichtigt werden (siehe auch INF.13.A22 *Durchführung von Systemtests im TGM*).

Wenn im TGM Funktionen der Künstlichen Intelligenz (KI) eingesetzt werden, SOLLTE bei dem zuständigen herstellenden Unternehmen angefragt werden, ob und wie die Informationssicherheit hier angemessen berücksichtigt wird.

Die Grobkonzeptionierung SOLLTE gemäß INF.13.A6 *Erstellung eines TGM-Konzepts* erfolgen.

In der Fein- und Umsetzungsplanung für das TGM SOLLTEN alle in der Sicherheitsrichtlinie und im TGM-Konzept adressierten Punkte berücksichtigt werden.

INF.13.A6 Erstellung eines TGM-Konzepts (S) [Planende]

Ausgehend von der Sicherheitsrichtlinie für das TGM SOLLTE ein TGM-Konzept erstellt und gepflegt werden. Dabei SOLLTEN mindestens folgende Aspekte bedarfsgerecht berücksichtigt werden:

- Methoden, Techniken und Werkzeuge für das TGM
- Absicherung des Zugangs und der Kommunikation
- Absicherung auf Ebene des Netzes, insbesondere Zuordnung von TGM-Komponenten zu Netzsegmenten
- Umfang des Monitorings und der Alarmierung
- Protokollierung von Ereignissen und administrativen Zugriffen
- Meldeketten bei Störungen und Sicherheitsvorfällen
- benötigte Prozesse für das TGM
- Bereitstellung von TGM-Informationen für andere Betriebsbereiche

- Einbindung des TGM in die Notfallplanung

Das TGM-Konzept SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden, um dem aktuellen Stand der Technik zu entsprechen und auch neue Erkenntnisse abdecken zu können.

Außerdem SOLLTE regelmäßig ein Soll-Ist-Vergleich zwischen den Vorgaben des Konzepts und dem aktuellen Zustand durchgeführt werden. Dabei SOLLTE insbesondere geprüft werden, ob die Systeme gemäß den Vorgaben konfiguriert sind. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert werden. Abweichungen SOLLTEN behoben werden.

INF.13.A7 Erstellung eines Funkfrequenzkatasters (S)

Um Funkfrequenzen weitestgehend störungsfrei nutzen zu können, SOLLTE ein Funkfrequenzkataster erstellt werden, dass die Systeme und Nutzenden des Frequenzspektrums an den Standorten der Institution listet. Dabei SOLLTE bei einer potentiellen Nutzung von Frequenzen durch unterschiedliche Systeme und Nutzende festgelegt werden, wer auf welchen Frequenzen der Primärnutzende ist. Dabei SOLLTE auch eine Abstimmung zwischen IT und TGM erfolgen. Wird in den Gebäuden OT eingesetzt, SOLLTE auch hier eine Abstimmung erfolgen.

Das Funkfrequenzkataster SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden.

INF.13.A8 Erstellung und Pflege eines Inventars für das TGM (S) [Planende]

Für die Dokumentation von Systemen, die durch das TGM verwaltet werden, SOLLTE ein Inventar erstellt und gepflegt werden. Das Inventar SOLLTE vollständig und aktuell gehalten werden. Aus dem Inventar SOLLTEN für alle Systeme Verantwortlichkeiten und Zuständigkeiten ersichtlich sein.

Auch die Elemente der TGM-Infrastruktur selbst SOLLTEN dokumentiert werden.

INF.13.A9 Regelung des Einsatzes von Computer-Aided Facility Management (S) [Planende]

Wird ein Computer-Aided Facility Management-System (CAFM-System) eingesetzt, SOLLTE dieser Einsatz umfassend geplant und konzeptioniert werden. Werden im CAFM Prozesse abgebildet und unterstützt, SOLLTEN entsprechende Rollen und Berechtigungen definiert werden, insbesondere wenn externe Dienstleistende an den Prozessen beteiligt sind.

INF.13.A10 Regelung des Einsatzes von Building Information Modeling (S) [Planende]

Soweit möglich SOLLTE Building Information Modeling (BIM) zur digitalen Modellierung aller relevanten Gebäudedaten eingesetzt werden. Bei der Verwendung von BIM SOLLTE der BIM-Projektabwicklungsplan spezifiziert werden.

Weiterhin SOLLTE die BIM-Architektur umfassend geplant und konzeptioniert werden. Auch für die BIM-Werkzeuge SOLLTE die Informationssicherheit angemessen gewährleistet werden.

INF.13.A11 Angemessene Härtung von Systemen im TGM (S)

Alle Systeme des TGM sowie die Systeme, die durch das TGM betrieben werden, SOLLTEN angemessen gehärtet werden. Die Härtungsmaßnahmen SOLLTEN dokumentiert, regelmäßig und zusätzlich bei Bedarf überprüft und, falls erforderlich, angepasst werden.

Für alle Systeme des TGM sowie die Systeme, die durch das TGM betrieben werden, SOLLTE bei der Beschaffung sichergestellt werden, dass diese angemessen gehärtet werden können und insbesondere sicherheitsrelevante Updates für die geplante Nutzungsdauer bereitgestellt werden.

Systeme, für die keine sicherheitsrelevanten Updates verfügbar sind, SOLLTEN nach Bekanntwerden von Schwachstellen nicht mehr genutzt werden. Wenn dies nicht möglich ist, SOLLTEN die

betroffenen Systeme mit den Mitteln der Netzsegmentierung separiert und die Kommunikation kontrolliert und reglementiert werden.

INF.13.A12 Sichere Konfiguration der TGM-Systeme (S)

Alle Systeme des TGM sowie die Systeme, die durch das TGM betrieben werden, SOLLTEN sicher konfiguriert werden.

Die Konfiguration SOLLTE mindestens vor Inbetriebnahme eines Systems getestet werden. Konfigurationsänderungen während des Produktivbetriebs SOLLTEN vor Aktivierung auf einer Testinstanz getestet oder nur im Vier-Augen-Prinzip durchgeführt werden.

Die Konfiguration von Systemen SOLLTE gesichert werden, um ein schnelles Wiedereinspielen einer fehlerfreien Version zu ermöglichen (Rollback). Rollback-Tests SOLLTEN auf einem Testsystem eingerichtet oder während Wartungsfenstern durchgeführt werden. Die Konfigurationen SOLLTEN zentral gespeichert werden.

Für gleichartige Systeme, inklusive der Geräte der Automations- und Feldebene (siehe Kapitel 4.1 Genutzte TGM-spezifische Fachbegriffe), SOLLTE eine automatisierte Verteilung von Software-Updates und Konfigurationen eingerichtet werden.

Konfigurationsänderungen SOLLTEN allen Beteiligten an Betriebs- und Serviceprozessen (Entstörung, Rufbereitschaft, Wartungen etc.) bekannt gemacht werden, insbesondere

- Änderungen der Zugangsmechanismen oder der Passwörter sowie
- Änderungen an Kommunikations- und Steuerparametern für die eingebundenen Systeme.

Es SOLLTE sichergestellt werden, dass im Störungsfall beispielsweise eine Wartungstechnikerin oder ein Wartungstechniker das System bedienen bzw. parametrieren kann.

Außerdem SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft werden, ob die Systeme gemäß den Vorgaben konfiguriert sind. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert werden. Abweichungen von den Vorgaben SOLLTEN behoben werden.

INF.13.A13 Sichere Anbindung von eingeschränkt vertrauenswürdigen Systemen im TGM (S) [Planende]

Eingeschränkt vertrauenswürdige Systeme, die aus wichtigen betrieblichen Gründen im TGM eingebunden werden müssen, SOLLTEN über ein System angebunden werden, das die Kommunikation mit Hilfe von Firewall-Funktionen kontrolliert und reglementiert. Dieses System SOLLTE in der Verantwortlichkeit des TGM liegen.

INF.13.A14 Berücksichtigung spezieller Rollen und Berechtigungen im TGM (S)

Im Rollen- und Berechtigungskonzept hinsichtlich des TGM SOLLTEN sowohl Nachfrage- als auch betreibende Organisationen der TGM-Systeme und der TGA-Systeme berücksichtigt werden. Dies SOLLTE insbesondere dann sorgfältig geplant werden, wenn das TGM institutionsübergreifend bereitgestellt wird.

INF.13.A15 Schutz vor Schadsoftware im TGM (S)

Können auf einem System keine Virenschutzprogramme gemäß Baustein OPS.1.1.4 *Schutz vor Schadprogrammen* ausgeführt werden, beispielsweise aufgrund von knappen Ressourcen oder aufgrund von Echtzeitanforderungen, SOLLTEN geeignete alternative Schutzverfahren eingesetzt werden.

Jedes externe System und jeder externe Datenträger SOLLTE vor der Verbindung mit einem TGM-System und vor der Datenübertragung auf Schadsoftware geprüft werden.

INF.13.A16 Prozess für Änderungen im TGM (S)

Änderungen SOLLTEN immer angekündigt und mit allen beteiligten Gewerken (siehe Kapitel 4.1 Genutzte TGM-spezifische Fachbegriffe), Nachfrage- und betreibenden Organisationen abgestimmt werden. Außerdem SOLLTEN Regelungen für den Fall getroffen werden, dass ein Rückbau von Änderungen mit fehlerhaftem Ergebnis nicht oder nur mit hohem Aufwand möglich ist. Daher sollten im Änderungsmanagement vor Ausführung der Änderung Tests durchgeführt werden, die auch die Fähigkeit des Rückbaus beinhalten. Für die verschiedenen Typen von Änderungen SOLLTE die jeweilige Testtiefe festgelegt werden. Bei der Einführung neuer Systeme und bei großen Änderungen an bestehenden Systemen SOLLTE eine entsprechend hohe Testtiefe vorgesehen werden (siehe INF.13.A22 *Durchführung von Systemtests im TGM*).

INF.13.A17 Regelung von Wartungs- und Reparaturarbeiten im TGM (S)

Gebäudeeinrichtungen SOLLTEN regelmäßig gewartet werden. Hierfür SOLLTE ein Wartungsplan erstellt werden. Es SOLLTE geregelt sein, welche Sicherheitsaspekte bei Wartungs- und Reparaturarbeiten zu beachten sind. Dabei SOLLTEN auch die Abhängigkeiten der verschiedenen Gewerke berücksichtigt werden. Darüber hinaus SOLLTE festgelegt werden, wer für die Wartung oder Reparatur von Einrichtungen zuständig ist. Durchgeführte Wartungsarbeiten SOLLTEN dokumentiert werden.

Es SOLLTE zu jedem Zeitpunkt gewährleistet werden, dass Wartungs- und Reparaturarbeiten, die durch Dritte ausgeführt werden, kontrolliert, ausschließlich abgestimmt durchgeführt und abgenommen werden. Hierfür SOLLTEN interne Mitarbeitende der Haustechnik bestimmt werden, die solche Wartungs- und Reparaturarbeiten autorisieren, beobachten, gegebenenfalls unterstützen und abnehmen.

INF.13.A18 Proaktive Instandhaltung im TGM (S) [Planende]

Für Systeme, die durch das TGM verwaltet werden, SOLLTE eine angemessene proaktive Instandhaltung durchgeführt werden. Hierfür SOLLTEN die regelmäßigen Wartungsintervalle je System festgelegt werden. Zusätzlich SOLLTE je System abgewogen werden, ob ergänzend zur regelmäßigen Instandhaltung eine vorausschauende Instandhaltung (engl. Predictive Maintenance) genutzt werden kann und in welchem Umfang hierdurch die regelmäßigen Wartungsintervalle verlängert werden können.

INF.13.A19 Konzeptionierung und Durchführung des Monitorings im TGM (S) [Planende]

Es SOLLTE ein Konzept für das Monitoring im TGM erstellt und umgesetzt werden. Darin SOLLTE spezifiziert werden, wie die durch das TGM zu verwaltenden Systeme in ein möglichst einheitliches Monitoring eingebunden werden können und welche Werte überwacht werden sollten. Hierfür SOLLTEN schon bei der Anforderungsanalyse erforderliche Schnittstellen für das Monitoring wichtiger Zustände von Systemen spezifiziert werden, die durch das TGM verwaltet werden. Außerdem SOLLTEN auch die für das TGM genutzten Systeme in das Monitoring eingebunden werden.

Das Konzept SOLLTE regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden, um dem aktuellen Stand der Technik zu entsprechen und auch neueste Erkenntnisse abdecken zu können.

Statusmeldungen und Monitoringdaten SOLLTEN NUR über sichere Kommunikationswege übertragen werden.

INF.13.A20 Regelung des Ereignismanagements im TGM (S) [Planende]

Im TGM auftretende Ereignisse SOLLTEN hinsichtlich ihrer Bedeutung und ihres Einflusses kategorisiert, gefiltert und klassifiziert werden (englisch Event Management). Für die Ereignisse SOLLTEN Schwellwerte definiert werden, die eine automatisierte Einstufung von Ereignissen ermöglichen. Je nach Klassifizierung der Ereignisse SOLLTEN entsprechende Maßnahmen für

Monitoring, Alarmierung und Meldewege (Eskalation) sowie Maßnahmen zur Protokollierung bestimmt werden.

INF.13.A21 Protokollierung im TGM (S)

Ereignisse, die im Ereignismanagement entsprechend klassifiziert wurden, SOLLTEN protokolliert werden. Außerdem SOLLTEN für die Systeme sicherheitsrelevante Ereignisse protokolliert werden.

Alle Konfigurationszugriffe sowie alle manuellen und automatisierten Steuerungszugriffe SOLLTEN protokolliert werden. Abhängig vom Schutzbedarf SOLLTE eine vollumfängliche Protokollierung inklusive Metadaten und Inhalt der Änderungen erfolgen.

Die Protokollierung SOLLTE auf einer zentralen Protokollierungsinstanz zusammengeführt werden.

Protokollierungsdaten SOLLTEN NUR über sichere Kommunikationswege übertragen werden.

Bei sicherheitskritischen Ereignissen SOLLTE automatisch alarmiert werden.

INF.13.A22 Durchführung von Systemtests im TGM (S) [Planende]

Systeme des TGM und Systeme, die durch das TGM verwaltet werden, SOLLTEN vor der Inbetriebnahme und bei großen Systemänderungen hinsichtlich ihrer funktionalen und nicht-funktionalen Anforderungen getestet werden. Dabei SOLLTE auch das Soll- und Ist-Verhalten von Funktionen und Einstellungen geprüft werden. Bei den nicht-funktionalen Anforderungen SOLLTEN auch Anforderungen der Informationssicherheit getestet sowie zusätzlich bei Bedarf auch Lasttests durchgeführt werden. Für die Tests SOLLTE eine Testspezifikation erstellt werden, die eine Beschreibung der Testumgebung, der Testtiefe und der Testfälle inklusive der Kriterien für eine erfolgreiche Testdurchführung enthält. Die Testdurchführung SOLLTE in einem Testbericht dokumentiert werden.

Testspezifikationen SOLLTEN regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden, um dem aktuellen Stand der Technik zu entsprechen und auch neueste Erkenntnisse abdecken zu können.

INF.13.A23 Integration des TGM in das Schwachstellenmanagement (S)

Systeme des TGM und die durch das TGM verwalteten Systeme SOLLTEN fortlaufend hinsichtlich möglicher Schwachstellen überwacht werden.

Hierfür SOLLTEN regelmäßig Informationen über bekanntgewordene Schwachstellen eingeholt und entsprechend berücksichtigt werden. Hierbei SOLLTE auch die Konfiguration der Systeme dahingehend überprüft werden, ob sie bekannt gewordene Schwachstellen begünstigt.

Weiterhin SOLLTE entschieden werden, für welche Systeme regelmäßig oder zumindest bei Inbetriebnahme und bei großen Systemänderungen Schwachstellen-Scans durchgeführt werden. Für Schwachstellen-Scans SOLLTE die Scan-Tiefe festgelegt werden. Außerdem SOLLTE festgelegt werden, ob ein passiver oder ein aktiver Scan durchgeführt wird. In Produktivumgebungen SOLLTEN passive Scans bevorzugt werden. Aktive Scans SOLLTEN in Produktivumgebungen nur durchgeführt werden, wenn sie notwendig sind und Personal hinzugezogen wird, das durch den Scan bedingte, eventuell auftretende Fehler oder Ausfälle beheben kann.

INF.13.A24 Sicherstellung der Kontrolle über die Prozesse bei Cloud-Nutzung für das TGM (S) [Planende]

Werden im TGM Cloud-basierte Dienste genutzt, SOLLTE die Kontrolle über alle TGM-Prozesse im TGM verbleiben. Dies SOLLTE bei Nutzung eines Cloud-Dienstes vertraglich mit dem anbietenden Unternehmen festgelegt 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.13.A25 Aufbau einer Testumgebung für das TGM (H) [Planende]

Bei erhöhtem Schutzbedarf SOLLTE für Systeme des TGM und für Systeme, die durch das TGM verwaltet werden, eine Testumgebung eingerichtet werden, damit Hard- und Software vor der Inbetriebnahme und bei Änderungen getestet und Fehler im produktiven Betrieb reduziert werden können. Außerdem SOLLTEN Regelungen für den Umgang mit Systemen spezifiziert werden, für die keine Testumgebung aufgebaut werden kann.

INF.13.A26 Absicherung von BIM (H) [Planende]

Werden in BIM auch sicherheitskritische Informationen erfasst, SOLLTEN sowohl auf Ebene der BIM-Architektur als auch für Implementierung und Betrieb der BIM-Lösung entsprechende Sicherheits- und Härtungsmaßnahmen vorgesehen werden. Die Absicherung SOLLTE ein verschärftes Rollen- und Berechtigungskonzept sowie weitergehende Schutzmaßnahmen wie Verschlüsselung, Segmentierung und höherwertige Authentisierungsmechanismen, insbesondere eine 2-Faktor-Authentisierung, beinhalten.

INF.13.A27 Einrichtung einer Private Cloud für das TGM (H) [Planende]

Bei erhöhtem Schutzbedarf SOLLTEN Cloud-Dienste zum TGM in einer Private Cloud On-Premises oder einer Private Cloud bei einem vertrauenswürdigen Anbietenden positioniert werden. Der Einsatz einer Public Cloud SOLLTE vermieden werden.

INF.13.A28 Sichere Nutzung von Künstlicher Intelligenz im TGM (H)

Werden bei erhöhtem Schutzbedarf im TGM Funktionen der Künstlichen Intelligenz (KI) genutzt, SOLLTE nur eine KI genutzt werden, die nachweislich sicher ist. Mindestens SOLLTE darauf geachtet werden, dass keine Daten in Netze geleitet werden, die nicht zur eigenen Institution gehören oder nicht vertrauenswürdig sind.

Für Cloud-basierte KI-Dienste SOLLTEN über die Anforderungen des Bausteins OPS.2.2 *Cloud-Nutzung* hinaus auch die Kriterien des AI Cloud Service Compliance Criteria Catalogue (AIC4) des BSI berücksichtigt werden.

INF.13.A29 Integration des TGM in ein SIEM (H) [IT-Betrieb]

Wird ein System für das Security Information and Event Management (SIEM) genutzt, SOLLTEN die Systeme des TGM und soweit möglich auch die durch das TGM verwalteten Systeme entsprechend eingebunden werden, um system- und anwendungsübergreifende sicherheitsrelevante Vorfälle erkennen und analysieren zu können.

INF.13.A30 Durchführung von Penetrationstests im TGM (H)

Um Systeme des TGM und Systeme, die durch das TGM verwaltet werden, entsprechend abzusichern, SOLLTEN bedarfsorientiert Penetrationstests durchgeführt werden. Mindestens SOLLTEN vor der Inbetriebnahme und bei großen Systemänderungen in einer Testumgebung Penetrationstests durchgeführt werden.

Werden im TGM Funktionen der KI genutzt, SOLLTEN diese in die Penetrationstests einbezogen werden.

4. Weiterführende Informationen

4.1. Genutzte TGM-spezifische Fachbegriffe

Automationsebene

Die Automationsebene befindet sich in der Automatisierungspyramide zwischen der Feldebene und der Managementebene. Sie führt die von der Feldebene gelieferten Daten sowie die von der Managementebene übermittelten Vorgaben zusammen. Hier erfolgt die Steuerung und Regelung der TGA-Anlagen, aber auch die Überwachung von Grenzwerten, Schaltzuständen oder Zählerständen.

Building Information Modeling (BIM)

Gemäß VDI 2552 Blatt 2 ist BIM eine Methodik zur Planung, zur Ausführung und zum Betrieb von Bauwerken mit einem kollaborativen Ansatz auf Grundlage eines digitalen Informationsmodells des Bauwerks zur gemeinschaftlichen Nutzung.

Computer-Aided Facility Management (CAFM)

Gemäß VDI 3814 Blatt 2.1 dient CAFM als Werkzeug zur Erfassung, Verarbeitung, Aufbereitung und Archivierung von Daten und Informationen mit dem Ziel, die Leistungsprozesse und Aufgaben in der Betriebsphase eines Gebäudes zu unterstützen.

Feldebene

Die Feldebene stellt die unterste Ebene der Automatisierungspyramide dar und umfasst unterschiedliche Komponenten der GA oder OT. In der Regel werden hier Sensoren und Aktoren betrieben. Sensoren erfassen Informationen (z. B. Bewegung, Helligkeit, Temperatur) und senden diese an die Automationsebene. Aktoren empfangen Steuerinformationen und setzen diese in Schaltsignale um, z. B. für die Beleuchtungs-, Heizungs-, Klima- und Lüftungsanlage.

Gebäude

Der Begriff Gebäude wird im Baustein INF.13 *Technisches Gebäudemanagement* und in den zugehörigen Umsetzungshinweisen synonym für Gebäude, Gebäudekomplex, Liegenschaft und Liegenschaftsportfolio genutzt. Außerdem beschreibt der Begriff Gebäude nicht nur Häuser und Hallen, sondern auch beispielsweise einen Fernsehturm oder eine Bohrinsel.

Gebäudeautomation (englisch Building Automation and Control Systems, BACS)

Die Gebäudeautomation (GA) umfasst gemäß VDI 3814-1 alle Produkte und Dienstleistungen zum zielsetzungsgerichteten Betrieb der Technischen Gebäudeausrüstung.

Gebäudekomplex

Ein Gebäudekomplex ist eine Gruppe von Gebäuden, die baulich miteinander verbunden sind und als Gesamteinheit wahrgenommen werden.

Gewerk

Im Bauwesen umfasst ein Gewerk im Allgemeinen die Arbeiten, die einem in sich geschlossenen Bauleistungsbereich zuzuordnen sind. Es handelt sich um einen Funktionsbereich, der insbesondere verschiedene TGA-Anlagen umfassen kann.

Beispiel: Raumlufttechnische Anlagen (Kostengruppe 430 in DIN 276), wozu etwa Lüftungsanlagen, Klimaanlagen und Kälteanlagen gehören.

Leitstand (englisch Control Center)

Ein Leitstand (auch Bedien- und Beobachtungseinheiten) ist ein technisches Werkzeug zur Visualisierung aktueller Abläufe, Zustände und Situationen von Prozessen, inklusive TGM- und speziell GA-Prozesse.

Liegenschaft

Eine Liegenschaft ist ein Grundstück inklusive seiner Bebauung. Zur Bebauung gehören alle unbeweglichen Sachen, d. h. Gebäude und sonstige Dinge, die nicht ohne Weiteres vom Grundstück entfernt werden können.

Liegenschaftsportfolio

Als Liegenschaftsportfolio wird die Gesamtheit der Liegenschaften im Besitzstand bezeichnet.

Nachfrageorganisation

Eine Nachfrageorganisation ist gemäß DIN EN ISO 41011 eine Organisationseinheit innerhalb oder außerhalb der Institution, die für ihre Erfordernisse autorisiert ist, entsprechende Anforderungen an TGA, GA oder TGM zu stellen und die Kosten zur Erfüllung der Anforderungen zu übernehmen.

Beispiele: Mietparteien innerhalb eines Gebäudes, Eigentümerinnen und Eigentümer eines Gebäudes, Dienstleistende innerhalb einer Institution, z. B. Kantine.

System

Der Begriff System adressiert im Baustein INF.13 *Technisches Gebäudemanagement* und in den zugehörigen Umsetzungshinweisen nicht nur ein IT-System im klassischen Sinn (vergleiche Bausteine der Schicht SYS), sondern umfasst auch alle Komponenten der TGA einschließlich aller Komponenten der Feldebene, wie Sensoren, Aktoren usw.

Technische Gebäudeausrüstung (englisch Building Services, BS)

Die Technische Gebäudeausrüstung (TGA) umfasst gemäß VDI 4700 Blatt 1 alle im Bauwerk eingebauten und damit verbundenen technischen Einrichtungen und nutzungsspezifischen Einrichtungen sowie technische Einrichtungen in Außenanlagen und Ausstattungen. Gewisse Komponenten der Gebäudeautomation sind ebenfalls zur TGA zuzurechnen, z. B. echtzeitfähige Industrial Ethernet Switches.

Technisches Gebäudemanagement (englisch Technical Building Management, TBM)

Das Technische Gebäudemanagement (TGM) beinhaltet gemäß DIN 32736 alle Leistungen, die zum Erhalt der technischen Funktion und Verfügbarkeit eines Gebäudes dienen. Das TGM übernimmt somit für die TGA das Betreiben, Instandhalten, Modernisieren und Dokumentieren der Komponenten und definiert alle notwendigen Prozesse.

TGA-Anlage

Eine Anlage der TGA beschreibt die Gesamtheit aller zur Erfüllung bestimmter Funktionen zusammenwirkenden technischen Komponenten. Beispiele gemäß DIN 276 „Kosten im Bauwesen“ sind Wärmeversorgungsanlagen, Lüftungsanlagen oder Beleuchtungsanlagen.

4.2. Abkürzungen

Abkürzung	Bedeutung
AI	Artificial Intelligence
AIC4	AI Cloud Service Compliance Criteria Catalogue
BACS	Building Automation and Control Systems
BIM	Building Information Modelling
BS	Building Services
CAFM	Computer-Aided Facility Management
DIN	Deutsches Institut für Normung
GA	Gebäudeautomation
GM	Gebäudemanagement
ICS	Industrial Control System
KI	Künstliche Intelligenz
OT	Operational Technology
SIEM	Security Information and Event Management

SIS	Safety Instrumented Systems
SLA	Service Level Agreement
TBM	Technical Building Management
TGA	Technische Gebäude-Ausstattung
TGM	Technisches Gebäude-Management
VDI	Verein Deutscher Ingenieure e.V.

4.3. Wissenswertes

Genannte Normen und Dokumente:

- AI Cloud Service Compliance Criteria Catalogue (AIC4), Bundesamt für Sicherheit in der Informationstechnik, Februar 2021, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/AIC4/AI-Cloud-Service-Compliance-Criteria-Catalogue_AIC4.html
- BSI-CS 108 - Fernwartung im industriellen Umfeld, BSI Veröffentlichung zur Cyber-Sicherheit, Juli 2018, aufrufbar über https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_108.pdf
- DIN 276 - Kosten im Bauwesen, Deutsches Institut für Normung e.V., Dezember 2018, verfügbar im Beuth-Verlag
- DIN 32736 - Gebäudemanagement - Begriffe und Leistungen, Deutsches Institut für Normung, August 2000, verfügbar im Beuth-Verlag
- VDI 4700 Blatt 1 - Begriffe der Bau- und Gebäudetechnik, Verein Deutscher Ingenieure e.V., Oktober 2015, verfügbar im Beuth-Verlag

Bundesamt
für Sicherheit in der
Informationstechnik

INF.14 Gebäudeautomation

1. Beschreibung

1.1. Einleitung

Die Gebäudeautomation (GA, englisch Building Automation and Control Systems, BACS) automatisiert den gewerkübergreifenden Betrieb von Gebäuden ganz oder teilweise und stellt hierfür die technische Infrastruktur zur Verfügung. Wesentliche technische Funktionen eines Gebäudes werden durch die technische Gebäudeausrüstung (TGA) bereitgestellt, die mit den Leistungen des technischen Gebäudemanagements (TGM) betrieben, gepflegt und weiterentwickelt werden. Die GA ist somit ein zentrales Werkzeug des TGM, um für den Gebäudebetrieb die gesetzte Zielrichtung umzusetzen. Sie umfasst alle Produkte und Dienstleistungen zum übergreifenden, automatisierten Betrieb der TGA. Kriterien für die Zielrichtung können Funktionalität, Energieeffizienz und Nachhaltigkeit, Sicherheit, Verfügbarkeit oder Komfort sein. Die GA kann auf Leistungen für Gebäude, Gebäudekomplexe, Liegenschaften oder Liegenschaftsportfolios skaliert werden. Im Folgenden wird hierfür einheitlich der Begriff Gebäude genutzt. Ausnahmen hiervon werden explizit genannt.

Die GA führt unter anderem Automatisierungsaufgaben wie automatisiertes Messen, Steuern und Regeln (MSR) sowie Aufgaben für Monitoring, Service und Diagnose, Optimierung, Bedienung und Management für die TGA eines Gebäudes durch.

Die GA wird innerhalb eines Gebäudes für eine oder gegebenenfalls mehrere Nachfrageorganisationen, beispielsweise Mietparteien, bereitgestellt. Hierfür wird die TGA meist separat für verschiedene GA-Bereiche, beispielsweise für Nachfrageorganisationen oder für Gebäudeteile, gesteuert.

In einem Gebäude kann die GA abhängig von der genutzten TGA durch mehrere parallele GA-Systeme umgesetzt werden. Ein GA-System stellt die technische Realisierung der GA dar und kann auch übergreifend für mehrere Gebäude innerhalb eines Gebäudekomplexes oder einer Liegenschaft genutzt werden. Verschiedene GA-Systeme können kooperieren, aber auch vollständig unabhängig voneinander betrieben werden.

Während die TGA in der Vergangenheit oft nicht übergreifend automatisiert betrieben wurde, werden heute zunehmend GA-Systeme zur übergeordneten, gewerkübergreifenden Steuerung der TGA genutzt. Hierfür werden zunehmend auch Techniken genutzt, die ursprünglich nur in der Informationstechnik (IT) und der industriellen Prozessleit- und Automatisierungstechnik (Operational Technology, OT) verwendet wurden, z. B. eine Kommunikation via Internet und Cloud-Diensten.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei Planung, Realisierung und Betrieb von GA zu etablieren.

1.3. Abgrenzung und Modellierung

Der Baustein INF.14 *Gebäudeautomation* ist auf die GA einer Institution anzuwenden, sobald die TGA in Gebäuden mittels GA gesteuert wird. Der Baustein ist nur auf die Schnittstellen der GA zu den TGA-Anlagen anzuwenden, die TGA-Anlagen mit den anlageninternen Netzen und Netzstrukturen sind nicht im Fokus dieses Bausteins.

Der Baustein INF.14 *Gebäudeautomation* behandelt Systeme und Leistungen, die zu beachten und zu erfüllen sind, wenn die GA, gegebenenfalls bestehend aus mehreren GA-Systemen, geplant, aufgebaut und betrieben wird. Hierbei werden auch spezifische Gegebenheiten behandelt, die für Netze und Netzkomponenten der GA gelten.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Die allgemeinen Anforderungen für GA und TGA, die nicht überwiegenden Aspekte für ein übergreifendes, automatisiertes Messen, Steuern und Regeln thematisieren, werden im Baustein INF.13 *Technisches Gebäudemanagement* behandelt. Dieser ist stets mitzubetrachten.
- Anforderungen an die allgemeine Infrastruktur, insbesondere Gebäude und Räume bzw. Arbeitsplätze, werden in den Bausteinen der Schicht INF *Infrastruktur* behandelt (z. B. Baustein INF.1 *Allgemeines Gebäude*).
- Werden Teile der GA, die für eine Institution erforderlich sind, von einer anderen Institution, z. B. von Dienstleistenden in der Rolle als Gebäudebetreibende (betreibende Organisation), erbracht, so muss für die Bereitstellung und den Betrieb der GA der Baustein OPS.2.3 *Nutzung von Outsourcing* angewendet werden.
- Spezifische Anforderungen an GA-Komponenten, die auch für den Bereich der industriellen IT oder OT genutzt werden können, werden in den Bausteinen der Schicht IND *Industrielle IT* thematisiert (siehe z. B. Baustein IND.2.3 *Sensoren und Aktoren* oder Baustein IND.2.7 *Safety Instrumented Systems*).
- Der Baustein NET.1.1 *Netzarchitektur und -design* behandelt die grundsätzlichen Aspekte für Netze, wie sie neben der Büro-IT auch in der GA und der industriellen IT anwendbar sind. Generelle Anforderungen an die Absicherung von Netzkomponenten behandeln die Bausteine in NET.3 *Netzkomponenten* (z. B. Baustein NET.3.1 *Router und Switches*).
- Außerdem sind alle passenden organisatorischen und technischen Bausteine für Server und Anwendungen anzuwenden. Beispielsweise ist für den Fernzugriff auf die GA-Komponenten der Baustein OPS.1.2.5 *Fernwartung* anzuwenden.
- Erfolgt die Vernetzung von Gebäuden Cloud-basiert, so ist zusätzlich der Baustein OPS.2.2 *Cloud-Nutzung* anzuwenden.

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.14 *Gebäudeautomation* von besonderer Bedeutung.

2.1. Unzureichende Planung der GA

Die GA dient der koordinierten, übergreifenden Steuerung der Anlagen der TGA. Eine unzureichende Planung der GA kann damit zu Sach- oder Vermögensschäden und im schlimmsten Fall zu Personenschäden führen.

Dies kann beispielsweise dann passieren, wenn durch unzureichende Redundanzplanung das zentrale Steuersystem einer Vereinzelungsanlage ausfällt und Personen in einer Schleuse eingeschlossen werden.

Die beschriebene Gefährdungslage verschärft sich in der GA zudem durch die Komplexität der Planung. Hier sind heterogene Gruppen von TGA-Anlagen (Gewerke) sowie eine Vielzahl unterschiedlicher Dienstleistenden und GA-Bereiche zu berücksichtigen.

2.2. Fehlerhafte Integration von TGA-Anlagen in die GA

Die GA steuert die Anlagen der TGA übergreifend. Ist nur eine Anlage fehlerhaft oder unzureichend integriert, kann die Funktionalität der gesamten GA eingeschränkt werden.

Beispielsweise können eingehende Meldungen falsch interpretiert werden oder Meldungen erreichen die GA nicht, so dass die GA falsch oder gar nicht reagiert. Werden beispielsweise die Informationen der Zugangskontrollanlage nicht korrekt oder gar nicht empfangen, können Heizung und Beschattung für die entsprechenden Räume gegebenenfalls nicht angemessen gesteuert werden.

2.3. Nutzung unsicherer Systeme und Protokolle in der GA

In den durch die GA gesteuerten TGA-Anlagen werden häufig Komponenten genutzt, die z. B. aufgrund ihres Alters keine Aktualisierungen mehr erhalten, Schwachstellen aufweisen bzw. nicht mehr dem aktuellen Stand der Technik entsprechen. Dies resultiert oft aus einer unzureichenden Qualität in den Entwicklungs- und Wartungsprozessen der herstellenden Unternehmen oder aus Software, die aufgrund mangelnder Rechen- und Speicherkapazität unsichere Protokolle nutzt.

Darüber hinaus stellen die herstellenden Unternehmen häufig keine Patches bereit, so dass unsichere GA-relevante Komponenten auch über einen sehr langen Zeitraum genutzt werden. Verstärkt wird die Gefährdung dadurch, dass in der GA Zugriffe auch auf solche Komponenten freigeschaltet werden müssen.

2.4. Fehlerhafte Konfiguration der Gebäudeautomation

Je nachdem, welche Bereiche der GA fehlerhaft konfiguriert sind, kann es zu Beeinträchtigungen in Betriebsabläufen, zu nicht erlaubtem physischen Zugang zu geschützten Bereichen, zu Schäden an Systemen bis hin zu Gebäude- und Personenschäden kommen.

Beispiele hierfür sind:

- Fehlerhaft konfigurierte Klimatisierung, die zu Überhitzung und Ausfall von IT-Systemen oder bei entsprechenden Wetterlagen sogar zu Beeinträchtigungen der Gesundheit von Personen führen kann.
- Nicht abgestimmt konfigurierte Systeme der Gebäudetechnik können zu Personen- und Systemschäden führen, wenn beispielsweise Strom- und Löschanlagen nicht koordiniert betrieben werden.
- Ebenso können fehlerhaft konfigurierte Zugangssysteme zu Personenschaden führen, wenn Türen im Notfall nicht geöffnet werden können.

Die Gefährdung ist für die GA besonders relevant, da aus Mangel an Testmöglichkeiten eine fehlerhafte Konfiguration vor Produktivsetzung häufig nicht erkannt werden kann. Dies kann auch bei einem

fehlerhaften Update oder einem fehlerbehafteten Update-Verlauf, der ein System der GA unbrauchbar macht, auftreten.

2.5. Manipulation der Schnittstellen von eigenständigen TGA-Anlagen zur Gebäudeautomation

Manipulierte Schnittstellen zwischen GA-Systemen und gekoppelten TGA-Anlagen können in der GA zu fehlerhaften Reaktionen führen.

Ein Beispiel hierfür ist, dass eine manipulierte Meldung einer Brandmeldeanlage dazu führen kann, dass alle Türen automatisiert geöffnet werden und so unbefugten Personen Zutritt zum Gebäude gewährt wird.

2.6. Unzureichend geschützte Zugänge zur GA

Die GA umfasst eine Vielzahl von Komponenten, die anlagenübergreifende Informationen bereitstellen, austauschen und empfangen, z. B. zur Standortbestimmung von Personal oder zur Raumautomatisierung. Die Geräte kommunizieren über LAN und WLAN, aber auch über sonstige drahtlose Techniken wie beispielsweise Bluetooth.

Sind solche Netzzugänge nicht angemessen geschützt, können hierüber DoS-Angriffe durchgeführt werden. Auch können die Systeme der GA manipuliert oder sabotiert und gegebenenfalls sogar die gesamte IT der Institution erreicht werden. Manipulierte Systeme der GA können dann ein erhöhtes Datenaufkommen bis hin zu einer Überlastung der Netze und Komponenten bedingen. Auch ein Datenabfluss oder das Einspielen von Schadsoftware ist über einen unzureichend geschützten Zugang möglich.

2.7. Unzureichend abgesicherte Bedienelemente der GA

Wenn gut zugängliche Bedienelemente der GA unzureichend abgesichert sind, kann über diese die GA angegriffen werden. Beispiele hierfür sind wandmontierte Bedienelemente oder aber auch Bedienelemente von Pfortenpersonal, mit denen z. B. entfernte Türen oder Tore geöffnet werden können.

Ist der Zugang zu solchen Bedienelementen unzureichend geschützt, z. B. durch fehlende Authentisierung, kann ein unbefugter Zugriff ermöglicht werden.

Ebenfalls können unzureichend geschützte Anschlüsse von Bedienelementen, wie LAN- oder USB-Schnittstellen, einen unbefugten Zugang bieten.

2.8. Unzureichend abgesicherte Mobilfunk-Anschlüsse

Häufig müssen insbesondere in der Feld- und Automatisierungsebene GA-Komponenten genutzt werden, die über eine Mobilfunkschnittstelle mit dem jeweiligen herstellenden Unternehmen oder mit Dienstleistenden wie etwa einem Wetterdienst verbunden sind. Sind diese Schnittstellen und die Kommunikation unzureichend geschützt und dauerhaft aktiv, bieten sie Unbefugten oder bei Angriffen einen Zugriff auf das GA-Netz.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.14 *Gebäudeautomation* 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	Planende, IT-Betrieb

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.14.A1 Planung der Gebäudeautomation (B) [Planende]

Für die von der Gebäudeautomation (GA) gesteuerten Gewerke MUSS festgelegt werden, wie die GA sicher gestaltet werden kann.

Die GA MUSS bereits bei der Planung von Neubau, Umbau, Erweiterung und Sanierung eines Gebäudes berücksichtigt werden. Daher MUSS die GA in den Planungs- und Bauprozessen, auch in Verbindung mit Building Information Modeling (BIM), für alle GA-relevanten Komponenten und TGA-Anlagen berücksichtigt werden.

Im Rahmen der GA-Planung MÜSSEN die einzurichtenden GA-Systeme spezifiziert werden. Es MUSS festgelegt werden, in welchem Umfang TGA-Anlagen über das GA-System automatisiert gesteuert werden sollen.

Die GA SOLLTE so geplant werden, dass zur Kopplung und Integration der TGA-Anlagen möglichst wenig unterschiedliche GA-Systeme sowie Kommunikationsprotokolle und -schnittstellen genutzt werden. Es SOLLTEN sichere und standardisierte Protokolle und Schnittstellen eingesetzt werden. Für eine Entscheidung hinsichtlich der notwendigen Systeme, Protokolle und Schnittstellen SOLLTE die erwartete Funktionalität gegenüber einem gegebenenfalls erhöhten Aufwand für Betriebs- und Informationssicherheit abgewogen werden.

Die Planung SOLLTE dokumentiert, regelmäßig und zusätzlich bei Bedarf aktualisiert und dem Stand der Technik angepasst werden.

Darüber hinaus SOLLTE die Planung regelmäßig und zusätzlich bei Bedarf mit der aktuellen Konfiguration verglichen werden (Soll-Ist-Vergleich).

INF.14.A2 Festlegung eines Inbetriebnahme- und Schnittstellenmanagements für die GA (B)

Aufgrund der Vielzahl von TGA-Anlagen und Komponenten in Gebäuden, die in GA-Systemen angebunden werden, MUSS der Ablauf zur Inbetriebnahme der involvierten TGA-Anlagen und GA-relevanten Komponenten aufeinander abgestimmt und übergreifend festgelegt werden. Dieser Ablauf MUSS koordiniert umgesetzt werden, um ein voll funktionsfähiges Gebäude zu gewährleisten.

Ebenso MÜSSEN klare Schnittstellen zwischen den betreibenden Organisationen der GA und der GA-relevanten Komponenten sowie den betreibenden Organisationen der TGA-Anlagen definiert werden.

Inbetriebnahme- und Schnittstellenmanagement MÜSSEN dokumentiert werden. Sowohl regelmäßig als auch zusätzlich bei Bedarf MÜSSEN die Festlegungen geprüft und gegebenenfalls nachjustiert werden. Insbesondere bei Änderungen innerhalb der GA-Systeme MÜSSEN die Festlegungen angepasst werden.

INF.14.A3 Sichere Anbindung von TGA-Anlagen und GA-Systemen (B)

Für alle TGA-Anlagen, GA-Systeme und GA-relevanten Komponenten MUSS festgelegt werden, ob durch andere TGA-Anlagen, GA-Systeme oder GA-relevante Komponenten Aktionen ausgelöst werden dürfen. Falls eine solche Integration zulässig ist, SOLLTE reglementiert werden, welche automatisierten Aktionen durch welche Informationen eines GA-Systems ausgelöst werden dürfen.

Falls eine TGA-Anlage nicht in ein GA-System integriert werden kann oder darf, diese jedoch an ein GA-System gekoppelt werden soll, MUSS festgelegt werden, welche Informationen der TGA-Anlage an das GA-System gemeldet werden.

Sowohl die Integration von TGA-Anlagen in ein GA-System als auch die rückwirkungsfreie Kopplung von TGA-Anlagen an GA-Systeme MÜSSEN angemessen abgesichert sein. Ebenfalls MUSS die Anbindung von GA-Systemen untereinander angemessen abgesichert werden.

Hierzu MÜSSEN insbesondere die Ablauf- und Funktionsketten innerhalb eines GA-Systems bzw. zwischen GA-Systemen angemessen geplant werden. Hierbei MÜSSEN alle Übergänge zwischen Gewerken und Techniken berücksichtigt werden.

Diese Ablauf- und Funktionsketten MÜSSEN umfassend getestet und bei Fehlverhalten nachjustiert werden.

Die Festlegungen MÜSSEN vollumfänglich dokumentiert werden. Sowohl regelmäßig als auch ergänzend bei Bedarf SOLLTE geprüft werden, ob die Dokumentation noch aktuell ist. Bei Abweichungen MUSS die Ursache für die Abweichungen eruiert und behoben werden.

INF.14.A4 Berücksichtigung von Gefahrenmeldeanlagen in der GA (B) [Planende]

Gefahrenmeldeanlagen inklusive Sicherheitsanlagen MÜSSEN rückwirkungsfrei an GA-Systeme gekoppelt werden. Sie DÜRFEN NICHT in ein GA-System integriert werden.

Für die netztechnische Anbindung MÜSSEN physisch getrennte Netzkomponenten und physisch getrennte Segmente genutzt werden. Werden Funknetze zur Kopplung genutzt, MÜSSEN solche TGA-Anlagen als Primärnutzende für die verwendeten Frequenzbereiche festgelegt werden. Für die Kommunikation über Funknetze SOLLTEN zertifizierte Mechanismen genutzt werden.

INF.14.A5 Dokumentation der GA (B)

Für die GA MUSS die Vielzahl unterschiedlicher Komponenten und Zugänge dokumentiert werden. Die Dokumentation MUSS regelmäßig und bei Änderungen innerhalb der GA geprüft und angepasst werden.

Insbesondere MÜSSEN auch alle deaktivierten physischen Kommunikationsschnittstellen, Protokolle und Zugänge bzw. Zugriffsmöglichkeiten zur GA dokumentiert werden. Darüber hinaus MÜSSEN alle Wechselwirkungen und Abhängigkeiten von GA-relevanten Komponenten sowie von TGA-Anlagen, die in GA-Systeme integriert oder mit GA-Systemen gekoppelt sind, dokumentiert werden. Die verfügbaren und genutzten Sicherheitseigenschaften der verwendeten Protokolle SOLLTEN dokumentiert werden.

Die Dokumentation SOLLTE für alle GA-Systeme übergreifend hinsichtlich Inhalten und deren Datenstrukturen abgestimmt werden.

INF.14.A6 Separierung von Netzen der GA (B) [Planende, IT-Betrieb]

GA-Netze MÜSSEN von Büro-Netzen und sonstigen Netzen der Institution mindestens logisch getrennt werden. Jegliche Kommunikation zwischen GA-Systemen und sonstigen IT-Systemen MUSS kontrolliert und reglementiert werden. Hierfür MÜSSEN an allen Übergängen einer solchen Segmentierung entsprechende Komponenten mit Sicherheitsfunktionen, mindestens mit Firewall-Funktion, vorgesehen werden.

Wird die GA für einen Gebäudekomplex oder eine Liegenschaft zentral eingerichtet, so MUSS die gebäudeübergreifende GA-Kommunikation über LAN-, WLAN-, WAN-, Funknetz- oder Internet-Verbindungen auch auf Ebene des Netzes separiert 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.14.A7 Festlegung einer Sicherheitsrichtlinie für die GA (S)

Ausgehend von der allgemeinen Sicherheitsleitlinie der Institution und der übergreifenden Sicherheitsrichtlinie für das TGM SOLLTEN die Sicherheitsanforderungen an die GA, d. h. für alle GA-Systeme, in einer GA-Sicherheitsrichtlinie konkretisiert werden. Diese Richtlinie SOLLTE allen Personen, die an Planung, Beschaffung, Implementierung und Betrieb der GA-Systeme beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Die Inhalte und die Umsetzung der geforderten Richtlinieninhalte SOLLTEN regelmäßig überprüft, gegebenenfalls angepasst und die Ergebnisse der Prüfung nachvollziehbar dokumentiert werden.

In der Sicherheitsrichtlinie SOLLTEN auch die Vorgaben an Entwicklung und Test für den Einsatz von GA-Systemen spezifiziert werden.

INF.14.A8 Anforderungsspezifikation für GA-Systeme (S)

Ausgehend von der GA-Sicherheitsrichtlinie SOLLTE für die GA eine übergreifende und für jedes GA-System eine eigene Anforderungsspezifikation erstellt werden. Aus den Anforderungen SOLLTEN sich alle wesentlichen Elemente für Architektur und Design des jeweiligen GA-Systems und der Kopplung von GA-Systemen ableiten lassen.

Die Anforderungsspezifikation SOLLTE dokumentiert sowie regelmäßig und zusätzlich bei Bedarf dem Stand der Technik angepasst werden. Darüber hinaus SOLLTE regelmäßig die Umsetzung der Anforderungen geprüft werden.

Es SOLLTEN in der GA ausschließlich Komponenten eingesetzt werden, die eine Authentisierung mindestens über einen änderbaren Anmeldenamen und ein änderbares Passwort bereitstellen.

INF.14.A9 Entwicklung eines GA-Konzepts (S)

Ausgehend von der GA-Sicherheitsrichtlinie und den Anforderungsspezifikationen SOLLTE für die GA ein übergreifendes GA-Konzept entwickelt werden. Hieraus abgeleitet SOLLTEN für alle GA-Systeme detaillierte Konzepte entwickelt werden. In den Konzepten SOLLTEN mindestens folgende Punkte angemessen berücksichtigt werden:

- alle in das jeweilige GA-System integrierten TGA-Anlagen
- alle mit dem jeweiligen GA-System gekoppelten TGA-Anlagen
- alle GA-relevanten Komponenten mit den jeweiligen Kommunikationsverbindungen

Die Konzepte SOLLTEN alle technischen und organisatorischen Vorgaben beschreiben. Die erstellten Konzepte SOLLTEN regelmäßig geprüft und gegebenenfalls aktualisiert werden.

INF.14.A10 Bildung von unabhängigen GA-Bereichen (S) [Planende]

In der GA SOLLTEN GA-Bereiche derart geplant und umgesetzt werden, dass Abhängigkeiten zwischen den GA-Bereichen minimiert werden und GA-Bereiche unabhängig gesteuert werden können. Eine Störung in einem GA-Bereich SOLLTE keine oder nur geringe Auswirkungen auf andere GA-Bereiche haben.

Insbesondere SOLLTEN die Gebäude innerhalb eines Gebäudekomplexes oder einer Liegenschaft separat steuerbar sein.

Die eingerichteten GA-Bereiche SOLLTEN auch im GA-Managementsystem entsprechend sichtbar sein.

INF.14.A11 Absicherung von frei zugänglichen Ports und Zugängen der GA (S) [Planende]

Der Anschluss von Komponenten, speziell von unautorisierten, unbekannten Komponenten und Fremdgeräten, SOLLTE insbesondere an frei zugänglichen Ethernet-Ports, USB-Ports und anderen Schnittstellen der GA kontrolliert und eingeschränkt werden.

Der Anschluss einer unautorisierten oder unbekannten Komponente SOLLTE in die Ereignisprotokollierung aufgenommen werden. Eine direkte IP-basierte Kommunikation von solchen Komponenten mit Systemen der GA SOLLTE unterbunden werden (siehe INF.14.A13 *Netzsegementierung in der GA*).

Für frei zugängliche LAN- oder WLAN-Zugänge SOLLTE eine Netzzugangskontrolle gemäß IEEE 802.1X oder vergleichbare Sicherheitsmechanismen eingesetzt werden. Hiermit SOLLTEN unzureichend authentisierte und autorisierte Komponenten in getrennten Netzsegmenten positioniert werden.

Frei zugängliche Schnittstellen für temporäre Wartungszwecke, wie beispielsweise USB-Ports an GA-Komponenten, SOLLTEN nur bei Bedarf aktiviert werden.

INF.14.A12 Nutzung sicherer Übertragungsprotokolle für die GA (S)

Für Konfiguration, Wartung und Steuerung von GA-relevanten Komponenten, die auf Ethernet und IP basieren, SOLLTEN sichere Protokolle eingesetzt werden, falls nicht über vertrauenswürdige Netzsegmente kommuniziert wird.

Außerhalb vertrauenswürdiger Netzsegmente SOLLTE die Kommunikation über Ethernet und IP zwischen GA-Systemen verschlüsselt erfolgen. Die Verschlüsselung SOLLTE mit den jeweils aktuellen Verschlüsselungsmechanismen durchgeführt werden.

INF.14.A13 Netzsegmentierung in der GA (S) [Planende]

Innerhalb des GA-Netzes SOLLTE eine Netzsegmentierung umgesetzt werden, die bedarfsgerecht einzelne GA-Systeme, einzelne TGA-Anlagen oder einzelne Gruppen von TGA-Anlagen innerhalb eines GA-Systems voneinander trennt.

Für die Übergänge zwischen den Segmenten SOLLTEN entsprechende Regeln definiert und zur Umsetzung Komponenten mit Sicherheitsfunktionen, mindestens zustandsbehaftete Paketfilter, genutzt werden.

INF.14.A14 Nutzung eines GA-geeigneten Zugriffsschutzes (S)

Für die GA SOLLTE ein Identitäts- und Berechtigungsmanagement gemäß Baustein ORP.4 *Identitäts und Berechtigungsmanagement* genutzt werden, das die Anforderungen der GA angemessen umsetzt. Hierfür SOLLTE bedarfsabhängig eine GA-eigene Authentisierungslösung oder eine geeignete Replikation einer zentralen Authentisierungslösung der Institution realisiert werden. In die Authentisierungslösung SOLLTEN soweit möglich alle GA-relevanten Komponenten eingebunden werden.

Betreibende der GA-Systeme, Betreibende der TGA-Anlagen und auch Nachfrageorganisationen SOLLTEN im Rollen- und Berechtigungskonzept hinsichtlich der GA angemessen berücksichtigt werden. Dies SOLLTE insbesondere dann sorgfältig geplant und abgestimmt werden, wenn die GA institutionsübergreifend bereitgestellt wird.

Alle GA-relevanten Komponenten, inklusive der Komponenten der Feldebene und Bedienelemente, SOLLTEN geeignete Funktionen zur Absicherung von Zugriffen umsetzen können. Komponenten, die keinen Zugriffsschutz bieten oder für die vom herstellenden Unternehmen vorgegebenen Zugangsparameter nicht änderbar sind, SOLLTEN NICHT genutzt werden.

INF.14.A15 Absicherung von GA-spezifischen Netzen (S)

Sind in GA-spezifischen Netzen wie z. B. BACnet Sicherheitsmechanismen der Kommunikation verfügbar, SOLLTEN diese genutzt werden. Mindestens SOLLTEN Mechanismen zur Authentisierung und Verschlüsselung genutzt werden.

Für GA-spezifische Netze, die keine angemessenen Sicherheitsmechanismen realisieren können, SOLLTE erwogen werden, diese auf ein GA-spezifisches Netz mit angemessenen Sicherheitsmechanismen umzustellen.

Grundsätzlich SOLLTE die Kommunikation mit GA-spezifischen Netzen durch Koppelelemente mit Sicherheitsfunktionen kontrolliert und gegebenenfalls reglementiert werden.

INF.14.A16 Absicherung von drahtloser Kommunikation in GA-Netzen (S) [Planende]

In GA-Netzen, die auf einer drahtlosen Kommunikation wie z. B. EnOcean basieren, SOLLTEN die Sicherheitsmechanismen der jeweiligen Funktechnik zur Absicherung der Kommunikation genutzt werden. Insbesondere SOLLTEN eine angemessene Authentisierung und eine Verschlüsselung auf der Luftschnittstelle umgesetzt werden. Ist dies für die entsprechenden Endgeräte nicht möglich, SOLLTE für diese Endgeräte die Kommunikation am Übergang in kabelgebundene Netze kontrolliert werden, z. B. durch eine Komponente mit Firewall-Funktion.

Darüber hinaus SOLLTEN mögliche Störungen für die Ausbreitung der Funkwellen, beispielsweise durch Abschattungen, bei der Planung der GA-Netze berücksichtigt werden.

INF.14.A17 Absicherung von Mobilfunkkommunikation in GA-Netzen (S) [Planende]

Wird im Rahmen der GA Mobilfunk eingesetzt, SOLLTEN für solche GA-Netze die Sicherheitsmechanismen der jeweiligen Mobilfunknetze genutzt werden.

Werden öffentliche Mobilfunknetze wie 5G oder Sigfox in der GA verwendet, SOLLTE eine unkontrollierte direkte IP-basierte Kommunikation mit GA-relevanten Komponenten unterbunden werden.

GA-Komponenten SOLLTEN nur dann mit einem dedizierten Anschluss an ein öffentliches Mobilfunknetz ausgestattet werden, falls dieser für deren Betrieb essenziell ist. Hierfür SOLLTE geprüft und festgelegt werden, für welche GA-Komponenten ein Anschluss an öffentliche Mobilfunknetze notwendig ist.

Sofern im öffentlichen Mobilfunknetz keine Trennung der GA-Netze möglich ist, wie z. B. bei 5G mit Slicing, SOLLTE im Kommunikationspfad eine Entkopplung der IP-Kommunikation durch ein Application Layer Gateway (ALG) stattfinden.

Falls Mobilfunktechniken in der GA als Bestandteil der öffentlichen Mobilfunkinfrastruktur eines Mobilfunkunternehmens eingesetzt werden, SOLLTEN mit den Mitteln der entsprechenden Mobilfunktechnik ein oder mehrere virtuelle Mobilfunknetze realisiert werden, die ausschließlich der GA zur Verfügung stehen.

Falls in der GA mit Hilfe von Mobilfunktechniken wie LTE und 5G autarke private Mobilfunknetze lokal auf dem Campus eingerichtet werden, SOLLTE der Übergang zwischen diesen Mobilfunknetzen und den sonstigen Netzen durch ein Koppelelement mit Firewall-Funktion abgesichert werden. Auch für private Mobilfunknetze SOLLTE eine Segmentierung in mehrere virtuelle Mobilfunknetze umgesetzt werden.

INF.14.A18 Sichere Anbindung von GA-externen Systemen (S)

Die Kommunikation von GA-Systemen mit GA-externen Systemen SOLLTE ausschließlich über definierte Schnittstellen und mit definierten IT-Systemen möglich sein. Die Kommunikation SOLLTE authentisiert und verschlüsselt werden.

Die möglichen Schnittstellen zu GA-externen Systemen SOLLTEN auf das notwendige Maß beschränkt werden.

INF.14.A19 Nutzung dedizierter Adressbereiche für GA-Netze (S) [Planende]

Für die GA SOLLTEN dedizierte Adressbereiche genutzt werden, die sich insbesondere von den Adressbereichen der Büro-IT und der OT unterscheiden. Für diese Adressbereiche SOLLTE festgelegt werden, aus welchen Bereichen statische Adressen vergeben werden und welche GA-relevanten Komponenten statische Adressen erhalten.

Falls an die GA angebundene Netzbereiche wie TGA-Anlagen identische Adressbereiche nutzen (Replizieren von Anlagenkonfigurationen), MÜSSEN diese in getrennten Segmenten positioniert werden, um Adresskonflikte zu unterbinden. In diesem Fall MUSS die segmentübergreifende Kommunikation durch entsprechende Mechanismen abgesichert werden, beispielsweise durch den Einsatz eines ALG oder von Network Address Translation (NAT).

INF.14.A20 Vermeidung von Broadcast-Kommunikation in GA-Netzen (S) [Planende]

In GA-Netzen SOLLTE die Broadcast-Last auf OSI Layer 2 oder OSI Layer 3 für unbeteiligte Systeme und Komponenten minimiert werden, um eine Überlastung zu vermeiden. Hierzu SOLLTE die Kommunikation auf gruppenspezifische Multicasts umgestellt oder in der Planung der Segmentierung entsprechend berücksichtigt werden.

INF.14.A21 Anzeigen der Gültigkeit von Informationen in GA-Systemen (S)

Ein GA-System SOLLTE visualisieren, ob die angezeigten Informationen bezüglich Zeit, Ort, Wert, Zustand oder Ereignis auf planmäßig erhaltenen Informationen basieren. Informationen, die simulierte oder „eingefrorene“ Werte anzeigen, SOLLTEN abhängig vom Schutzbedarf der TGA-Anlagen erkennbar sein oder einen Alarm auslösen.

INF.14.A22 Sicherstellung von autark funktionierenden GA-Systemen und TGA-Anlagen (S) [Planende]

Innerhalb eines GA-Systems SOLLTE sichergestellt werden, dass TGA-Anlagen gemäß ihrem Schutzbedarf auch unabhängig von der Anbindung an das GA-System autark funktionieren. Insbesondere SOLLTEN GA-Systeme so konfiguriert werden, dass keine betriebsverhindernden Abhängigkeiten zum TGM, zu anderen GA-Systemen oder TGA-Anlagen bestehen. Eine TGA-Anlage SOLLTE auch bei Ausfall der Verbindung zur GA für einen bestimmten Zeitraum gemäß dem jeweiligen Schutzbedarf betriebsfähig bleiben und ihre Funktion wahrnehmen.

INF.14.A23 Einsatz von physisch robusten Komponenten für die GA (S) [Planende]

Abhängig von den Einsatzbedingungen der Komponenten in der GA SOLLTEN entsprechend physisch robuste Komponenten eingesetzt werden, die besonders auch für harsche Umgebungsbedingungen vorgesehen bzw. ausgewiesen sind. Sind angemessen robuste Komponenten nicht verfügbar, SOLLTEN entsprechende Kompensationsmaßnahmen ergriffen werden.

INF.14.A24 Zeitsynchronisation für die GA (S)

Alle in einem GA-System angebundenen Komponenten und TGA-Anlagen SOLLTEN eine synchrone Uhrzeit nutzen, um ein automatisiertes Messen, Steuern und Regeln zu gewährleisten (siehe auch Baustein OPS.1.2.6 *NTP-Zeitsynchronisation*). Auch GA-Systeme, die miteinander verbunden sind, SOLLTEN eine synchrone Uhrzeit nutzen. Erstreckt sich die GA über Gebäudekomplexe oder Liegenschaften, SOLLTE die Zeitsynchronisation für alle Gebäude gewährleistet werden.

Falls innerhalb eines GA-Systems eine Kommunikation mit Echtzeit-Anforderungen erforderlich ist, SOLLTE für die Zeitsynchronisation PTP oder ein vergleichbarer Mechanismus anstelle von NTP genutzt werden.

INF.14.A25 Dediziertes Monitoring in der GA (S)

Für alle Komponenten, die für die GA betriebsrelevant sind, SOLLTE ein geeignetes Monitoringkonzept erstellt und umgesetzt werden. Hierbei SOLLTEN die Verfügbarkeit sowie bedeutsame Parameter der GA-relevanten Komponenten laufend überwacht werden. Fehlerzustände sowie die Überschreitung definierter Grenzwerte SOLLTEN automatisch an die betreibende Organisation gemeldet werden.

Es SOLLTEN durch die GA mindestens Alarme ausgelöst werden, wenn TGA-Anlagen ausfallen oder wichtige Funktionen zum automatisierten Steuern und Regeln nicht verfügbar sind. Zudem SOLLTE festgelegt werden, für welche besonders sicherheitsrelevanten Ereignisse und für welche weiteren Ereignisse automatische Alarmmeldungen generiert werden.

Statusmeldungen und Monitoringdaten SOLLTEN NUR über sichere Kommunikationswege übertragen werden.

INF.14.A26 Protokollierung in der GA (S)

Ergänzend zum Baustein OPS.1.1.5 *Protokollierung* SOLLTEN Statusänderungen an GA-relevanten Komponenten und sicherheitsrelevante Ereignisse protokolliert werden. Zusätzlich SOLLTEN alle schreibenden Konfigurationszugriffe auf TGA-Anlagen und gegebenenfalls GA-relevante Komponenten sowie alle manuellen und automatisierten Änderungen der Zustände von diesen protokolliert werden.

Es SOLLTE festgelegt werden, welche Protokollierungsdaten auf einer zentralen Protokollierungsinstanz zusammengeführt werden.

Protokollierungsdaten SOLLTEN NUR über sichere Kommunikationswege übertragen werden.

INF.14.A27 Berücksichtigung von Wechselwirkungen zwischen Komponenten der GA in der Notfallplanung (S)

Es SOLLTE initial und in regelmäßigen Abständen nachvollziehbar analysiert werden, wie sich die GA und die abgeleiteten Planungen und Konzepte auf die Notfallplanung auswirken. Insbesondere SOLLTE festgelegt werden, wie bei einem Ausfall von TGA-Anlagen oder GA-relevanten Komponenten durch technischen Defekt oder Angriff die Wechselwirkungen auf andere TGA-Anlagen, GA-relevante Systeme und TGM minimiert werden können. Im Rahmen der Notfallplanung SOLLTE auch festgelegt werden, welches Wartungspersonal für die betroffenen TGA-Anlagen und GA-relevanten Systeme zuständig ist und über welche Meldewege dieses erreicht werden kann. Außerdem SOLLTE festgelegt werden, welche Berechtigungen das Wartungspersonal zur Behebung von Notfällen hat.

Es SOLLTE in der Notfallplanung auch spezifiziert werden, wie bei Ausfall der GA-Systeme ein gegebenenfalls erforderlicher Notbetrieb von TGA-Anlagen sichergestellt wird. Dabei SOLLTE für alle TGA-Anlagen und GA-Systeme inklusive aller GA-relevanten Komponenten eine Wiederanlaufreihenfolge festgelegt und in den entsprechenden Wiederanlaufplänen dokumentiert 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.14.A28 Physische Trennung der GA (H) [Planende]

Bei erhöhtem Schutzbedarf SOLLTEN GA-Netze als physisch getrennte Zonen gemäß Baustein NET.1.1 *Netzarchitektur und -design* realisiert werden.

Abhängig vom Schutzbedarf SOLLTE für die Anbindung beispielsweise an externe Clouds ein dedizierter, restriktiv reglementierter Internet-Zugang bereitgestellt werden.

Ebenfalls SOLLTEN, abhängig vom Schutzbedarf der GA-Systeme, Anbindungen an nicht vertrauenswürdige Netze, gegebenenfalls auch Anbindungen an institutionseigene Büro- oder OT-Netze, unterbunden werden.

INF.14.A29 Trennung einzelner TGA-Anlagen (H)

Um einzelne TGA-Anlagen mit erhöhtem Schutzbedarf innerhalb eines GA-Systems abzusichern, SOLLTEN solche TGA-Anlagen in separaten Netzsegmenten positioniert werden. Zur Kontrolle der Kommunikation SOLLTEN Firewall-Funktionen unmittelbar vor dem Anlagennetz positioniert werden.

INF.14.A30 Bereitstellung eines GA-eigenen Zeitservers zur Zeitsynchronisation (H)

Bei erhöhtem Schutzbedarf SOLLTE für die GA oder auch für einzelne GA-Systeme ein eigener GA-Zeitserver bereitgestellt werden, der direkt mit einer Atom- oder Funkuhr (Stratum 0) gekoppelt ist und an den gegebenenfalls weitere nachgelagerte GA-Zeitserver angebunden werden.

4. Weiterführende Informationen

4.1. Genutzte GA-spezifische Fachbegriffe

Anlagenautomation (englisch System Automation and Control, SAC)

Die Anlagenautomation (AA) ist ein Teil eines GA-Systems und realisiert die Automation zum energieeffizienten, wirtschaftlichen und sicheren Betrieb von Anlagen der TGA. Die Anlagenautomation steuert über Aktoren die TGA-Anlage und dessen Zustandsgrößen. Diese werden wiederum durch die Sensoren der TGA-Anlage erfasst.

Bedien- und Beobachtungseinheiten (englisch Control and Display Device, CDD)

Gemäß DIN EN ISO 16484-2 umfasst der Begriff Bedien- und Beobachtungseinheiten (auch Leitstand oder Leitwarte genannt) die Summe der Einrichtungen für die Benutzenden, die als Schnittstelle zu den Bedien- und Managementfunktionen eines GA-Systems fungiert.

GA-Bereich (englisch BACS Area)

Ein GA-Bereich umfasst einen oder mehrere Räume ähnlicher Nutzung, die horizontal, vertikal oder gemischt verteilt sein können und mehrere GA-Segmente umfasst.

Beispiele: ein Flur, eine Etage, ein Gebäudeflügel, eine Produktionshalle.

GA-Management (englisch Management Building Automation and Control Systems, M-BACS)

Das GA-Management (GA-M), auch als Gebäudeleittechnik bezeichnet, übernimmt als Bestandteil eines GA-Systems Aufgaben zur Informationsverarbeitung für das Management der GA, beispielhaft Funktionen für ein übergeordnetes Energiemanagement, Wartungsmanagement, Störmanagement aber auch Raumbuchungsmanagement.

GA-Segment (englisch BACS Segment)

Ein GA-Segment bezeichnet die kleinste betrachtete räumliche Einheit, für die GA-Funktionen anwendbar sind. Ein GA-Segment ist nicht zu verwechseln mit einem Netzsegment, das über Sicherheitselemente vom restlichen Netz separiert wird.

GA-spezifische Netze (englisch BACS-specific Networks)

Ein GA-spezifisches Netz beschreibt ein Netz, das eine Verkabelung nutzt, die meist nicht auf Ethernet-Techniken basiert, z. B. KNX-Bussystem, oder das spezifische Protokolle nutzt, die nicht auf IP und Ethernet gemäß IEEE 802.3 basiert, z. B. BACnet. Spezifische Protokolle können aufgrund von Anforderungen an eine Echtzeitkommunikation oder an einen reduzierten Protokollumfang erforderlich werden.

GA-System (englisch Building Automation and Control System, BACS)

Ein GA-System stellt gemäß VDI 3814-1 die technische Realisierung der GA dar und umfasst die folgenden Teile:

- GA-Management
- Anlagenautomation
- Raumautomation

Anlagenautomation und Raumautomation bestehen analog zur Operational Technology (OT) aus den (funktionalen) Ebenen Automationsebene (z. B. Anlagensteuerungen) und Feldebene (z. B. Aktoren und Sensoren).

Gebäudeautomation (englisch Building Automation and Control Systems, BACS)

Die Gebäudeautomation (GA) umfasst gemäß VDI 3814-1 alle Produkte und Dienstleistungen zum zielsetzungsgerichteten automatisierten Betrieb der Technischen Gebäudeausrüstung (TGA).

Gefahrenmeldeanlage (englisch Alarm System)

Gefahrenmeldeanlagen (GMA) sind TGA-Anlagen, die Gefahren wie Einbruch, Feuer und Rauch erkennen und melden können. Sie erfassen Gefahren durch Interaktion mit Sensoren oder Bedieneinheiten und erzeugen Gefahrenmeldungen, die an eine zentrale Komponente gesendet werden.

Gewerk

Im Bauwesen umfasst ein Gewerk im Allgemeinen die Arbeiten, die einem in sich geschlossenen Bauleistungsbereich zuzuordnen sind. Es handelt sich um einen Funktionsbereich, der insbesondere verschiedene TGA-Anlagen umfassen kann.

Beispiel: Raumlufttechnische Anlagen (Kostengruppe 430 in DIN 276), wozu etwa Lüftungsanlagen, Klimaanlagen und Kälteanlagen gehören.

Integration von Systemen oder Anlagen

Eine Integration von Systemen oder Anlagen bedeutet gemäß VDI 3814, dass integrierte Systeme oder Anlagen Informationen mit dem GA-Management austauschen und sich hierdurch gegenseitig beeinflussen können.

Eine Systemintegration im Rahmen der GA ist abzugrenzen von eingebetteten Systemen (englisch Embedded Systems). Diese sind intelligente Elemente, die in andere Systeme eingebettet sind und weitestgehend unsichtbar Überwachungs-, Steuerungs-, Verarbeitungs- oder Regelfunktionen innerhalb des einbindenden Systems übernehmen.

Kopplung von Systemen oder Anlagen

Eine Kopplung von Systemen und Anlagen bedeutet gemäß VDI 3814-2-2, dass die gekoppelten Systeme (Brandmeldeanlage oder Einbruchsmeldeanlage) ihre Informationen zur GA schicken, ohne dadurch ihre Autarkie einzuschränken oder zu verlieren. Eine System- oder Anlagenkopplung ist somit grundsätzlich rückwirkungsfrei.

Beispiele: Brandmeldeanlage oder Einbruchsmeldeanlage.

Leitstand (englisch Control Center)

Ein Leitstand (siehe auch Bedien- und Beobachtungseinheiten) ist ein technisches Werkzeug zur Visualisierung aktueller Abläufe, Zustände und Situationen von GA-Prozessen.

Liegenschaft (englisch Property)

Eine Liegenschaft umfasst gemäß VDI 3814-1 ein oder mehrere, meist lokal benachbarte Gebäude.

Lokale Vorrangbedienung (englisch Local Override, LOR)

Eine lokale Vorrangbedienung (LVB, früher auch Notbedieneinrichtung genannt) stellt gemäß VDI 3814-1 die Schnittstelle zu GA-relevanten Komponenten, die ein eingeschränktes Betreiben unabhängig von Automationseinrichtungen mit vorrangigem Anzeigen, Schalten und/oder Stellen ermöglicht. Ein Beispiel ist der manuelle vorrangige Betrieb von Ventilatoren.

Nachfrageorganisation

Eine Nachfrageorganisation ist gemäß DIN EN ISO 41011 eine Organisationseinheit innerhalb oder außerhalb der Institution, die für ihre Erfordernisse autorisiert ist, entsprechende Anforderungen an TGA, GA oder TGM zu stellen und die Kosten zur Erfüllung der Anforderungen zu übernehmen.

Beispiele: Mietparteien innerhalb eines Gebäudes, Eigentümerinnen und Eigentümer eines Gebäudes, Dienstleistende innerhalb einer Institution, z. B. Kantine

Raumautomation (englisch Room Automation and Controls, RAC)

Die Raumautomation (RA) ist Bestandteil eines GA-Systems und realisiert alle Aufgaben einer anlagenübergreifenden Automation im betrachteten Raum, z. B. die Bedienung der im Raum installierten Technik.

Rückwirkungsfreiheit

Eine rückwirkungsfreie Anbindung einer TGA-Anlage an die GA bedeutet, dass die TGA-Anlage zwar Informationen an die GA liefert, von dieser jedoch auf Basis dieser Informationen nicht beeinflusst werden kann. Die Anlage bleibt weiterhin autark.

Technische Gebäudeausrüstung (englisch Building Services, BS)

Die Technische Gebäudeausrüstung (TGA) umfasst gemäß VDI 4700 Blatt 1 alle im Gebäude eingebauten und damit verbundenen technischen Einrichtungen und nutzungsspezifischen Einrichtungen sowie technische Einrichtungen in Außenanlagen und Ausstattungen. Gewisse Komponenten der GA sind ebenfalls zur TGA zuzurechnen, z. B. echtzeitfähige Industrial Ethernet Switches.

Technisches Gebäudemanagement (englisch Technical Building Management, TBM)

Das Technische Gebäudemanagement (TGM) beinhaltet gemäß DIN 32736 alle Leistungen, die zum Erhalt der technischen Funktion und Verfügbarkeit eines Gebäudes dienen. Das TGM übernimmt somit für die TGA das Betreiben, Instandhalten, Modernisieren und Dokumentieren der Komponenten und definiert alle notwendigen Prozesse.

TGA-Anlage

Eine Anlage der TGA beschreibt die Gesamtheit aller zur Erfüllung bestimmter Funktionen zusammenwirkenden technischen Komponenten. Beispiele gemäß DIN 276 „Kosten im Bauwesen“ sind Wärmeversorgungsanlagen, Lüftungsanlagen oder Beleuchtungsanlagen. Anlagen werden in der GA in ein GA-System integriert oder mit GA-Systemen gekoppelt.

4.2. Abkürzungen

Abkürzung	Bedeutung
5G	5. Generation des Mobilfunks
AA	Anlagenautomation
ALG	Application Layer Gateway
BACS	Building Automation and Control Systems
BIM	Building Information Modelling
DIN	Deutsches Institut für Normung
DoS	Denial of Service
EN	Europäische Norm
GA	Gebäudeautomation
GMA	Gefahrenmeldeanlagen

IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	Internationale Organisation für Normung
KNX	Konnex(-Bus)
LAN	Local Area Network
LTE	Long Term Evolution
MSR	Messen, Steuern, Regeln
NAT	Network Address Translation
NTP	Network Time Protocol
OSI	Open Systems Interconnection
OT	Operational Technology
PTP	Precision Time Protocol
RA	Raumautomation
SLA	Service Level Agreement
TGA	Technische Gebäude-Ausstattung
TGM	Technisches Gebäude-Management
VDI	Verein Deutscher Ingenieure e.V.
VDMA	Verband Deutscher Maschinen- und Anlagenbau
WAN	Wide Area Network
WLAN	Wireless Local Area Network

4.3. Wissenswertes

Genannten Normen und Dokumente:

DIN EN ISO 16484 - Systeme der Gebäudeautomation (GA)

- DIN EN ISO 16484-1 - Systeme der Gebäudeautomation (GA), Teil 1: Projektplanung und -ausführung, DIN/EN/ISO, März 2011, verfügbar im Beuth-Verlag
- DIN EN ISO 16484-2 - Systeme der Gebäudeautomation (GA), Teil 2: Hardware, DIN/EN/ISO, Oktober 2004, verfügbar im Beuth-Verlag
- DIN EN ISO 16484-3 - Systeme der Gebäudeautomation (GA), Teil 3: Funktionen, DIN/EN/ISO, Dezember 2005, verfügbar im Beuth-Verlag
- DIN EN ISO 16484-5 - Systeme der Gebäudeautomation (GA), Teil 5: Datenkommunikationsprotokoll (BACnet), DIN/EN/ISO, Dezember 2017, verfügbar im Beuth-Verlag

DIN 32736 - Gebäudemanagement - Begriffe und Leistungen, Deutsches Institut für Normung, August 2000, verfügbar im Beuth-Verlag

DIN EN ISO 41011 - Facility Management - Begriffe, DIN/EN/ISO, April 2019, verfügbar im Beuth-Verlag

DIN 276 - Kosten im Bauwesen, Deutsches Institut für Normung e.V., Dezember 2018, verfügbar im Beuth-Verlag

VDI 4700 Blatt 1 - Begriffe der Bau- und Gebäudetechnik, Verein Deutscher Ingenieure e.V., Oktober 2015, verfügbar im Beuth-Verlag

VDI 3814 - Gebäudeautomation (GA)

- VDI 3814 Blatt 1 - Gebäudeautomation (GA) - Grundlagen, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 2.1 - Gebäudeautomation (GA) - Planung - Bedarfsplanung, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag

- VDI 3814 Blatt 2.2 - Gebäudeautomation (GA) - Planung - Planungsinhalte, Systemintegration und Schnittstellen, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 2.3 - Gebäudeautomation (GA) - Planung - Bedienkonzept und Benutzeroberflächen, Verein Deutscher Ingenieure e.V., September 2019, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 3.1 - Gebäudeautomation (GA) - Planung - GA-Funktionen - Automationsfunktionen, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 4.1 - Gebäudeautomation (GA) - Methoden und Arbeitsmittel für Planung, Ausführung und Übergabe - Kennzeichnung, Adressierung und Listen, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 4.2 - Gebäudeautomation (GA) - Methoden und Arbeitsmittel für Planung, Ausführung und Übergabe - Bedarfsplanung, Planungsinhalte und Systemintegration, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 4.3 - Gebäudeautomation (GA) - Methoden und Arbeitsmittel für Planung, Ausführung und Übergabe - GA-Automationsschema, GA-Funktionsliste, GA-Funktionsbeschreibung, Verein Deutscher Ingenieure e.V., November 2020, Entwurf, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 6 - Gebäudeautomation (GA) - Qualifizierung, Rollen und Kompetenzen, Verein Deutscher Ingenieure e.V., April 2020, Entwurf, verfügbar im Beuth-Verlag

VDMA 24774 - IT-Sicherheit in der Gebäudeautomation, VDMA e. V., Februar 2021, verfügbar im Beuth-Verlag