Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein INF.6 Datenträgerarchiv

- Einleitung
- Maßnahmen
  - Maßnahmen zum Baustein INF.6 *Datenträgerarchiv*
- Weiterführende Informationen
  - Wissenswertes
  - Quellenverweise

Einleitung

Datenträgerarchive sind abgeschlossene Räumlichkeiten innerhalb einer Institution, in denen Datenträger jeder Art gelagert werden. Hierzu gehören neben Datenträgern, auf denen digitale Informationen abgespeichert sind, grundsätzlich auch Papierdokumente, Filme oder sonstige Medien. Im Rahmen des IT-Grundschutzes werden an die Archivräume hinsichtlich des Brandschutzes keine erhöhten Anforderungen gestellt. Zusätzliche Anforderungen an den Brandschutz können auch durch die Behältnisse, in denen die Datenträger aufbewahrt werden, erfüllt werden.

Bei zentralen Datenträgerarchiven und Datensicherungsarchiven wird generell empfohlen. Datensicherungsschränke zu nutzen, um neben dem Brandschutz den Schutz gegen unbefugten Zugriff und die Durchsetzung von Zugangsberechtigungen zu unterstützen.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins INF.6 *Datenträgerarchiv* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein INF.6 Datenträgerarchiv

INF.6.M1 Handfeuerlöscher (B)

Die meisten Brände entstehen aus kleinen, anfangs noch gut beherrschbaren Brandherden. Der Sofortbekämpfung von Bränden kommt also ein sehr hoher Stellenwert zu.

Diese Sofortbekämpfung ist nur möglich, wenn Handfeuerlöscher in der jeweils geeigneten Brandklasse (siehe [DIN3]) in ausreichender Zahl und Größe (Beratung durch die örtliche Feuerwehr) im Gebäude zur Verfügung stehen. Zudem ist auf dem Instandhaltungsnachweis jedes Löschers regelmäßig zu prüfen, dass die Löscher auch regelmäßig inspiziert und gewartet werden, damit sie im Ernstfall funktionieren.

Wasserlöscher mit Eignung für Brandklasse A bis 1000 V sind durchaus für elektrisch betriebene Geräte geeignet.

Für elektronisch gesteuerte Geräte, z. B. Rechner, sollten vorzugsweise Kohlendioxid-Löscher (Brandklasse B) zur Verfügung stehen. Die Löschwirkung wird erreicht, indem Sauerstoff verdrängt wird, deshalb ist bei Anwendung in engen, schlecht belüfteten Räumen Vorsicht geboten.

Pulverlöscher, die die Brandklassen A (feste Stoffe), B (brennbare Flüssigkeiten) und C (Gase) abdecken, sollten in Bereichen mit elektrischen und elektronischen Geräten nicht eingesetzt werden, weil die Löschschäden in der Regel unverhältnismäßig hoch sind. Es wird daher dringend empfohlen, im direkten Umfeld von Datenträgerarchiven keine Pulverlöscher, sondern ausschließlich geeignete Gaslöscher bereit zu halten. Nur so kann verhindert werden, dass in der Aufregung eines Brandes fälschlicherweise ein Pulverlöscher verwendet wird.

Die Feuerlöscher müssen regelmäßig geprüft und gewartet werden. Die Feuerlöscher müssen so angebracht werden, dass sie im Brandfall leicht erreichbar sind. Die Beschäftigten sollten sich den Standort des nächsten Feuerlöschers einprägen. Die Standorte von Löschern und Hydranten sind durch vorgeschriebene Schilder kenntlich zu machen. Tragbare Feuerlöscher sind zugelassen bis zu einem Gesamtgewicht von 20 kg. Mit den überwiegend eingesetzten Geräten von 6 und 12 kg lassen sich größere Brandherde löschen als von Laien üblicherweise angenommen wird, dies ist allerdings nur bei konsequenter Vorgehensweise gegeben. Bis zur vollständigen Entladung des Löschmittels vergehen nur wenige Sekunden. Daher sind bei entsprechenden Brandschutzübungen die Mitarbeiter in die Benutzung der Handfeuerlöscher einzuweisen und die Bedienung der Löscher auch zu üben.

INF.6.M2 Zutrittsregelung und -kontrolle (B)

Der Zutritt zum schutzbedürftigen Datenträgerarchiv ist zu regeln und zu kontrollieren. Die Maßnahmen reichen dabei von einer einfachen Schlüsselvergabe bis hin zu aufwendigen Identifizierungssystemen mit Personenvereinzelung, wobei auch die Nutzung eines mechanischen Schlüssels nebst Schloss eine Zutrittsregelung darstellt. Für eine Zutrittsregelung und -kontrolle ist es erforderlich, dass der von der Regelung betroffene Bereich eindeutig bestimmt wird. Die Anzahl der zutrittsberechtigten Personen muss sich auf ein Mindestmaß beschränken. Diese Personen müssen gegenseitig ihre Berechtigungen kennen, um Unbefugte als solche erkennen zu können. Die erteilten Zutrittsberechtigungen müssen dokumentiert werden. Die Vergabe von Rechten allein reicht nicht aus, wenn deren Einhaltung bzw. Überschreitung nicht kontrolliert wird. Die Ausgestaltung von Kontrollmechanismen muss nach dem Grundsatz erfolgen, dass einfache und praktikable Lösungen oft ebenso effizient sind wie aufwendige Technik. Beispiele hierfür sind die Sensibilisierung von Berechtigten, Bekanntgabe von Berechtigungsänderungen, sichtbares Tragen von Hausausweisen ergänzt durch die Vergabe von Besucherausweisen, Begleitung von Besuchern, Verhaltensregelungen bei erkannter Berechtigungsüberschreitung und Einschränkungen des ungehinderten Zutritts für nicht Zutrittsberechtigte wie Tür mit Blindknauf, Schloss mit Schlüssel für Berechtigte und Klingel für Besucher.

INF.6.M3 Schutz vor Staub und anderer Verschmutzung (B)

Generell muss sichergestellt werden, dass die Datenträger im Datenträgerarchiv ausreichend vor Staub und Verschmutzung geschützt sind. Hierfür sollten die Datenträger so verpackt werden, dass sie auch über eine lange Lagerzeit keine Schäden durch Staub und Verschmutzung erleiden.

In den meisten Räumlichkeiten von Unternehmen und Behörden ist Rauchen generell verboten, meistens sogar aufgrund gesetzlicher Vorgaben. So verpflichtet in Deutschland die Arbeitsstättenverordnung die meisten Institutionen, den Nichtraucherschutz am Arbeitsplatz zu gewährleisten. Auch in Gebäuden, in denen kein umfassendes Rauchverbot herrscht, muss sichergestellt werden, dass in Räumen mit IT oder Datenträgern (Serverraum, Datenträgerarchiv, aber auch Belegarchiv), in denen Brände oder Verschmutzungen beispielsweise durch Staub zu hohen Schäden führen können, ein Rauchverbot erlassen wird. Dieses Rauchverbot dient gleicherweise dem vorbeugenden Brandschutz wie der Betriebssicherheit von IT mit mechanischen Funktionseinheiten.

Dabei muss sichergestellt werden, dass nicht als Folge eines Rauchverbots im Gebäude der Zutrittsschutz geschwächt wird. Es ist häufig zu beobachten, dass Außentüren in schwer einsehbaren Bereichen ständig offen stehen, weil der Nahbereich der Tür die Raucherzone bildet und die Tür aus Bequemlichkeit während der Arbeitszeiten nie geschlossen wird.

INF.6.M4 Geschlossene Fenster und abgeschlossene Türen (B)

Offene Fenster und Türen bieten Einbrechern ideale Einstiegsmöglichkeiten, die auch während der Betriebszeiten einer Institution genutzt werden können. Fenster und Türen müssen in Zeiten, in denen das Datenträgerarchiv nicht besetzt ist, geschlossen bzw. Türen verschlossen werden. Dadurch wird verhindert, dass Unbefugte Zugriff auf darin befindliche Datenträger erlangen. Das Verschließen des Datenträgerarchivs ist insbesondere dann wichtig, wenn sich dieser im Bereich mit Publikumsverkehr befinden oder der Zutritt nicht durch andere Maßnahmen kontrolliert wird.

Brand- und Rauchschutztüren bieten ebenfalls nur im verschlossenen Zustand den gewünschten Schutz und dürfen deshalb keinesfalls durch Keile oder andere Vorrichtungen dauerhaft offen gehalten werden. Es ist sinnvoll, wenn Pförtner oder Mitarbeiter der Haustechnik regelmäßig überprüfen, ob die Fenster und Türen nach Verlassen der Räume verschlossen wurden.

INF.6.M5 Verwendung von Schutzschränken (S)

Bei zentralen Datenträgerarchiven und Datensicherungsarchiven ist die Nutzung von Schutzschränken empfehlenswert, um den Brandschutz, den Schutz gegen unbefugten Zugriff und die Durchsetzung von Zugangsberechtigungen zu unterstützen.

INF.6.M6 Vermeidung von wasserführenden Leitungen (S)

In Datenträgerarchiven sollten wasserführende Leitungen aller Art vermieden werden. Die einzigen wasserführenden Leitungen sollten, wenn unbedingt erforderlich, Kühlwasserleitungen, Löschwasserleitungen und Heizungsrohre sein. Zuleitungen zu Heizkörpern sollten mit Absperrventilen möglichst außerhalb des Datenträgerarchivs versehen werden. Außerhalb der Heizperiode sind diese Ventile zu schließen.

Sind wasserführende Leitungen unvermeidbar, müssen Vorkehrungen getroffen werden, einen Wasseraustritt möglichst frühzeitig zu erkennen bzw. die negativen Auswirkungen zu minimieren. Als Minimalschutz kann eine Wasserauffangwanne oder -rinne unter der Leitung angebracht werden, deren Ablauf außerhalb des Raumes führt. Günstig ist es, dazu den Flur zu nutzen, da so ein eventueller Leitungsschaden schnell entdeckt werden kann. Zur frühzeitigen Erkennung von Wassereinbrüchen oder undichten Leitungen hat es sich bewährt, Decken hell zu streichen. Mindestens durch Sichtprüfungen müssen die vorhandenen Wasserleitungen regelmäßig auf ihre Dichtigkeit hin überprüft werden.

Es ist zu erwägen, wasserführende Leitung durch Wassermelder zu überwachen. Dafür können besondere Meldekabel unterhalb von Leitungen verlegt werden. Werden diese an eine Wassermeldeanlage angeschlossen, kann darüber schnell und recht genau der Wasseraustritt lokalisiert werden. Eine solche Anlage muss auf eine ständig besetzte Stelle aufgeschaltet werden, um in Verbindung mit entsprechenden Reaktionsplänen und einer aktuellen Dokumentation ein schnelles Eingreifen möglich zu machen. Optional können Wassermelder mit automatisch arbeitenden Magnetventilen eingebaut werden. Diese Magnetventile sind außerhalb des Raumes bzw. Bereiches einzubauen. Damit die Ventile auch bei Stromausfall ihre Schutzfunktion erfüllen, müssen sie im stromlosen Zustand geschlossen sein.

Alle Mitarbeiter im Bereich der IT und der Haustechnik sollten darüber informiert sein, dass im Datenträgerarchiv wasserführende Leitungen problematisch sind und was zu beachten ist. Es sollten Reaktionspläne vorhanden sein, in denen beschrieben ist, welche Maßnahmen bei Wasserleckagen zu ergreifen sind.

INF.6.M7 Einhaltung von klimatischen Bedingungen (S)

Um Datenträger zu lagern bzw. IT-Geräte dauerhaft zuverlässig zu betreiben, muss sichergestellt werden, dass die Umgebungsbedingungen innerhalb der von den Herstellern genannten Grenzen gehalten werden. Der in diesem Zusammenhang stets genutzte Begriff Klimatisierung umfasst die folgenden vier Bereiche der Luftkonditionierung:

- Lufttemperatur
- Luftfeuchtigkeit
- Frischluftanteil
- Schwebstoffbelastung

Neben der Temperatur muss oft auch die Luftfeuchtigkeit innerhalb bestimmter Grenzen gehalten werden, um elektrostatische Aufladungen (bei zu geringer Luftfeuchtigkeit) oder Oxidation und Schimmelbildung (bei zu hoher Luftfeuchtigkeit) zu vermeiden.

Der Schwebstoffgehalt der Luft wird meist schon durch die normalen Filter in Klimaanlagen hinreichend niedrig gehalten. Nur bei besonders stark belasteter Umgebungsluft oder spezieller Hardware ist hier eine weitergehende Filterung erforderlich. Um den erforderlichen Luftdurchsatz zu gewährleisten, müssen die Filter der Klimaanlage regelmäßig kontrolliert und rechtzeitig gewechselt werden.

Die vierte Komponente einer Klimatisierung, die Frischluftbeimischung, ist für den eigentlichen IT-Betrieb und der Archivierung belanglos. In dem Umfang jedoch, in dem die klimatisierten Flächen als Arbeitsplatz ausgewiesen sind, muss entsprechend der einschlägigen Arbeitsstättenverordnungen eine Frischluftbeimischung erfolgen.

INF.6.M8 Sichere Türen und Fenster (S)

Wenn Türen und Fenster einen Übergang zwischen Sicherheitszonen bilden, sollten sie angemessenen Schutz bieten. Eine Außentür muss z. B. vor Einbrüchen schützen, ebenso müssen die erreichbaren Fenster gesichert werden. Im Innenbereich müssen Türen, die die Grenze eines Brandabschnitts bilden, selbst Brandschutzqualität haben, zudem können sie oder auch andere Innentüren eine zweite Linie des Einbruchschutzes bilden.

Sicherheitstüren und -fenster sind in Normen klassifiziert. Aus dem Schutzziel des zu sichernden Bereichs und dem Schutzbedarf der Institution lässt sich eine Auswahl der angemessenen Ausführung von Türen und Fenstern treffen:

- In der Norm DIN EN 1627:2011-09 "Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung" sind die Bauelemente in Widerstandsklassen (RC, engl. Resistance Class) eingeordnet worden (siehe [DIN1627]). Türen gemäß der Klassifizierungen RC1 bis RC4 bieten aufgrund ihrer Stabilität einen höheren Schutz gegen Einbruch (z. B. bei Serverräumen, Räumen mit technische Infrastruktur sowie bei Keller- und Lieferanteneingängen). Die Widerstandsklassen RC5 und RC6 sind in der Regel nur bei sehr speziellen Erfordernissen angemessen und spielen daher beim IT-Grundschutz keine Rolle.
- Selbstschließende feuerhemmende und gegebenenfalls rauchdichte Türen (siehe [DIN4102]) verzögern die Ausbreitung eines Brandes und in der RS-Ausführung auch von Rauch.
- Sie schützen in der Ausführung als selbstschließende Rauchschutztür (siehe [DIN18095-2] die Ausbreitung von Brandrauch. Brandrauch ist so feinkörnig, dass er problemlos durch Druckausgleichs- und Lüftungsöffnungen von Festplatten hindurch kommt. Für die geringen Flughöhen von Festplattenleseköpfen ist er aber immer noch viel zu groß und verursacht dort enorme Schäden.

Es können auch mehrere Schutzeigenschaften in einer Tür kombiniert werden, es gibt beispielsweise rauchdichte Brandschutztüren, die zudem Schutz gegen Einbruch bieten.

Die Sicherungsmaßnahmen aller raumumschließenden Bauelemente müssen gleichwertig sein:

- Bei Verwendung einbruchhemmender Türen ist im Fassadenbereich die Verwendung einbruchhemmender Fenster oder Fassadenelemente (siehe [DIN 1627) zu erwägen.
- Weiterhin ist es z. B. nicht zweckmäßig, eine einbruchhemmende Tür der höchsten Widerstandsklasse in eine Gipskartonwand einzubauen.
- Beim Einbau einer feuerhemmenden oder rauchdichten Tür ist darauf zu achten, dass auch die umgebende Wand gleichwertig feuerhemmend und rauchdicht ist und nicht durch offene Oberlichter oder ungeschottete Kabeldurchführungen ein Bypass besteht.

Der Einsatz von Sicherheitstüren ist hinsichtlich des Brandschutzes über den von der Bauaufsicht und der Feuerwehr vorgeschriebenen Bereich hinaus besonders bei schutzbedürftigen Räumen wie dem Datenträgerarchiv sinnvoll. Bei hochschutzbedürftigen Räumen ist ein ausgewogenes Schutzkonzept zu erstellen, welches den Einbau von Sicherheitstüren und die Gefahrenmeldung und Alarmierung zur Prüfung und Intervention berücksichtigt. Denn hat ein potentieller Angreifer ein ganzes Wochenende Zeit für einen Einbruchsversuch, wird ihn auch eine hochwertige einbruchhemmende Tür nicht von seinem Ziel abhalten, Daten oder Einrichtung zu entwenden oder zu zerstören.

Für die Ausstattung von Rechenzentren sollte für die Türen inklusive deren Einbausituation die Widerstandsklasse RC3 (siehe [DIN 1627]) als Mindestwert angesetzt werden. Lediglich wenn für die Sicherheit ganz besonders günstige Bedingungen vorliegen, insbesondere falls die Interventionszeit hilfeleistender Kräfte kurz ist (maximal 2 Minuten), kann in Ausnahmefällen eine RC2-Tür ausreichen. Liegt die Interventionszeit hilfeleistender Kräfte hingegen bei 5 Minuten und höher, ist sogar eine RC3-Tür als unzureichend anzusehen und es empfiehlt sich der Einbau von RC4-Türen. Sinngemäß gelten die gleiche Überlegungen natürlich auch für alle anderen, die RZ-Hülle bildenden Bauelemente.

Hinweis: Ziel eines Einbruches könnte es auch sein, Daten oder IT-Systeme zu manipulieren. Daher sollten zentrale IT-Systeme nach Einbrüchen auf ihre Integrität überprüft werden.

Es ist dafür zu sorgen, dass Brand- und Rauchschutztüren auch tatsächlich geschlossen und nicht (unzulässigerweise) z. B. durch Keile offen gehalten werden. Alternativ können Türen mit einem automatischen Schließmechanismus, der im Alarmfall aktiviert wird, eingesetzt werden.

Außerdem ist regelmäßig zu prüfen, dass die Sicherheitstüren und -fenster funktionstüchtig sind. Sie müssen in einem ordentlichen mechanischen Zustand sein, sicher öffnen und schließen und überwachende Installationen wie Schließkontakte müssen funktionieren.

INF.6.M9 Gefahrenmeldeanlage (H)

Eine Gefahrenmeldeanlage (GMA) besteht aus einer Vielzahl lokaler Melder, die mit einer Zentrale kommunizieren, über die auch der Alarm ausgelöst wird. Ist eine Gefahrenmeldeanlage für Einbruch, Brand, Wasser oder auch Gas vorhanden und lässt sich diese mit vertretbarem Aufwand entsprechend erweitern, sollten zumindest die Kernbereiche der IT (Serverräume, Datenträgerarchive, Räume für technische Infrastruktur u. ä.) in die Überwachung durch diese Anlage mit eingebunden werden. So lassen sich Gefährdungen wie Feuer, Einbruch, Diebstahl frühzeitig erkennen und Gegenmaßnahmen einleiten. Um dies zu gewährleisten, ist die Weiterleitung der Meldungen an eine ständig besetzte Stelle (Pförtner, Wach- und Sicherheitsdienst, Feuerwehr, etc.) unumgänglich. Dabei muss sichergestellt sein, dass diese Stelle auch in der Lage ist, technisch und personell auf den Alarm zu reagieren. Hierbei sind die Aufschaltrichtlinien der jeweiligen Institutionen und die Anforderungen der "Notruf- und Serviceleitstellen" (siehe [DIN50518]) zu beachten.

Es sollte ein Konzept für die Gefahrenerkennung, Weiterleitung und Alarmierung für die verschiedenen Gebäudebereiche erstellt werden. Dieses muss an Veränderungen bei der Nutzung angepasst werden. Eine Gefahrenmeldeanlage ist ein komplexes Gesamtsystem, das dem Gebäude und dem Risiko entsprechend geplant und installiert werden muss. Planung, Installation und Wartung einer Gefahrenmeldeanlage sollte daher durch Experten durchgeführt werden. Falls diese nicht im eigenen Haus vorhanden sind, sollte auf

externe Unterstützung zurückgegriffen werden. So gibt es beispielsweise eine Vielzahl unterschiedlicher Meldesysteme, die entsprechend der Sicherheitsanforderungen und der Umgebung ausgewählt werden müssen. Zur Einbruchserkennung können z. B. Bewegungsmelder, Glasbruchsensoren, Öffnungskontakte, Videokameras u. a. eingesetzt werden.

Die Melder können untereinander auf verschiedene Arten vernetzt werden. In Abhängigkeit von Art und Größe der zu schützenden Bereiche und der geltenden Richtlinien müssen passende Systeme ausgewählt und installiert werden. Bei der Planung oder Erweiterung einer GMA sollte darauf geachtet werden, dass die Trassen für die Vernetzung ausreichend dimensioniert sein müssen und möglichst wenig Änderungen an der Trassenbelegung vorgenommen werden sollten.

Um die Schutzwirkung der GMA aufrechtzuerhalten, ist eine regelmäßige Wartung und Funktionsprüfung (siehe [DIN0833-2]) vorzusehen.

Ist keine GMA vorhanden oder lässt sich die vorhandene nicht nutzen, kommen als Minimallösung lokale Gefahrenmelder in Betracht. Diese arbeiten völlig selbständig, ohne Anschluss an eine Zentrale. Die Alarmierung erfolgt vor Ort oder mittels einer einfachen Zweidrahtleitung (eventuell Telefonleitung) an anderer Stelle.

Wenn keine zentrale GMA vorhanden ist, sind dort lokale Gefahrenmelder zu installieren. Bei der Verwendung lokaler Gefahrenmelder für die Früherkennung muss dafür gesorgt werden, dass ein Alarm auch außerhalb der betroffenen Räume wahrgenommen wird. Die Meldung kann über verschiedene Wege erfolgen und sollte an eine Stelle weitergeleitet werden, die rund um die Uhr besetzt ist. Beispielsweise gibt es Lösungen, die über die TK-Anlage oder Funk Mitarbeiter über ein Mobiltelefon alarmieren können.

Vor der Planung einer GMA muss ein konsistentes Schutzkonzept für das betrachtete Gebäude erarbeitet werden. Bei der Planung von Gefahrenmeldeanlagen für private bzw. gewerbliche Objekte sollte mit dem Sachversicherer geklärt werden, ob eine Minderung der Versicherungsprämie, insbesondere für die Einbruch-Diebstahlversicherung in Frage kommt.

3. Weiterführende Informationen

3.1. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2. Quellenverweise

[DIN0833-1] DIN VDE 0833-1: 2014-10: Gefahrenmeldeanlagen für Brand, Einbruch und Überfall: Teil 1: Allgemeine Festlegungen, Oktober 2014

[DIN0833-2] DIN VDE 0833-2:2017-10: Gefahrenmeldeanlagen für Brand, Einbruch und Überfall: Teil 2: Festlegungen für Brandmeldeanlagen, Oktober 2017

[DIN1627] DIN EN 1627:2011-09 Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchshemmung - Anforderung und Klassifizierung: September 2011

[DIN18095-2] DIN 18095-2:1991-03: Türen, Rauchschutztüren: Begriffe und Anforderungen

[DIN3] DIN EN 3 Tragbare Feuerlöscher

[DIN4102] DIN 4102 Brandverhalten von Baustoffen und Bauteilen