IT-Grundschutz – Basis für Informationssicherheit

Warum ist Informationssicherheit wichtig?

Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Die meisten Geschäftsprozesse und Fachaufgaben sind heute in Wirtschaft und Verwaltung ohne IT-Unterstützung längst nicht mehr vorstellbar. Eine zuverlässig funktionierende Informationsverarbeitung ist ebenso wie die zugehörige Technik für die Aufrechterhaltung des Betriebes unerlässlich. Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der sogar existenzbedrohend werden kann. Dabei ist ein vernünftiger Informationsschutz ebenso wie eine Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen. Mit dem IT-Grundschutz bietet das BSI eine praktikable Methode an, um die Informationen einer Institution angemessenen zu schützen. Die Kombination aus den IT-Grundschutz-Vorgehensweisen Basis-, Kern- und Standard-Absicherung sowie dem IT-Grundschutz-Kompendium bieten für unterschiedliche Einsatzumgebungen Sicherheitsanforderungen zum Aufbau eines ISMS und somit für den sicheren Umgang mit Informationen. IT-Grundschutz kann sowohl von kleinen und mittleren (KMU) als auch großen Institutionen zum Aufbau eines Managementsystems für Informationssicherheit eingesetzt werden. Dabei setzt eine erfolgreiche Umsetzung des IT-Grundschutz-Kompendiums jedoch voraus, dass eine Organisationseinheit (IT-Betrieb) etabliert wird, die die interne IT einrichtet, betreibt, überwacht und wartet.

Aufgrund der skizzierten Abhängigkeit steigt bei Sicherheitsvorfällen auch die Gefahr für Institutionen, einen Imageschaden zu erleiden. Die verarbeiteten Daten und Informationen müssen adäquat geschützt, Sicherheitsmaßnahmen sorgfältig geplant, umgesetzt und kontrolliert werden. Hierbei ist es aber wichtig, sich nicht nur auf die Sicherheit von IT-Systemen zu konzentrieren, da Informationssicherheit ganzheitlich betrachtet werden muss. Sie hängt auch stark von infrastrukturellen, organisatorischen und personellen Rahmenbedingungen ab. Die Sicherheit der Betriebsumgebung, die ausreichende Schulung der Mitarbeitenden, die Verlässlichkeit von Dienstleistungen, der richtige Umgang mit zu schützenden Informationen und viele andere wichtige Aspekte dürfen auf keinen Fall vernachlässigt werden.

Mängel im Bereich der Informationssicherheit können zu erheblichen Problemen führen. Die potenziellen Schäden lassen sich verschiedenen Kategorien zuordnen:

- **Verlust der Verfügbarkeit**
  Wenn grundlegende Informationen nicht vorhanden sind, fällt dies meistens schnell auf, vor allem, wenn Aufgaben ohne diese nicht weitergeführt werden können. Funktioniert ein IT-System nicht, können beispielsweise keine Geldtransaktionen durchgeführt werden, Online-Bestellungen sind nicht möglich, Produktionsprozesse stehen still. Auch wenn die Verfügbarkeit von bestimmten Informationen lediglich eingeschränkt ist, können die Geschäftsprozesse bzw. Fachaufgaben einer Institution beeinträchtigt werden.
- **Verlust der Vertraulichkeit von Informationen**
  Jede Person möchte, dass mit seinen oder ihren personenbezogenen Daten vertraulich umgegangen wird, unabhängig davon, ob sie von einer Behörde oder einem Unternehmen verarbeitet werden. Jedes Unternehmen sollte wissen, dass interne, vertrauliche Daten über Umsatz, Marketing, Forschung und Entwicklung die Konkurrenz interessieren. Die ungewollte Offenlegung von Informationen kann in vielen Bereichen schwere Schäden nach sich ziehen.
- **Verlust der Integrität (Korrektheit) von Informationen**
  Gefälschte oder verfälschte Daten können beispielsweise zu Fehlbuchungen, falschen Lieferungen oder fehlerhaften Produkten führen. Auch der Verlust der Authentizität (Echtheit und Überprüfbarkeit) hat, als ein Teilbereich der Integrität, eine hohe Bedeutung. Daten werden beispielsweise einer falschen Person zugeordnet. So können Zahlungsanweisungen oder Bestellungen zu Lasten einer dritten Person verarbeitet werden, ungesicherte digitale Willenserklärungen können falschen Personen zugerechnet werden, die „digitale Identität" wird gefälscht.

Informations- und Kommunikationstechnik spielt in fast allen Bereichen des täglichen Lebens eine bedeutende Rolle, dabei ist das Innovationstempo seit Jahren unverändert hoch. Besonders erwähnenswert sind dabei folgende Entwicklungen:

- **Steigender Vernetzungsgrad**
  Menschen, aber auch IT-Systeme, arbeiten heutzutage nicht mehr isoliert voneinander, sondern immer stärker vernetzt. Dies ermöglicht es, auf gemeinsame Datenbestände zuzugreifen und intensive Formen der Kooperation über geographische, politische oder institutionelle Grenzen hinweg zu nutzen. Damit entsteht nicht nur eine Abhängigkeit von einzelnen IT-Systemen, sondern in starkem Maße auch von Datennetzen. Sicherheitsmängel können dadurch schnell globale Auswirkungen haben.

- **IT-Verbreitung und Durchdringung**
  Immer mehr Bereiche werden durch Informationstechnik unterstützt, häufig ohne, dass dies den Menschen, die diese nutzen, auffällt. Die erforderliche Hardware wird zunehmend kleiner und günstiger, sodass kleine und kleinste IT-Einheiten in alle Bereiche des Alltags integriert werden können. So gibt es beispielsweise Bekleidung mit integrierten Gesundheitssensoren, mit dem Internet vernetzte Glühbirnen sowie IT-gestützte Sensorik in Autos, um automatisch auf veränderte Umgebungsverhältnisse reagieren zu können oder sogar selbstfahrende Fahrzeuge. Die Kommunikation der verschiedenen IT-Komponenten untereinander findet dabei zunehmend drahtlos statt. Alltagsgegenstände werden dadurch über das Internet lokalisierbar und steuerbar.

- **Verschwinden der Netzgrenzen**
  Bis vor Kurzem ließen sich Geschäftsprozesse und Anwendungen eindeutig auf IT-Systeme und Kommunikationsstrecken lokalisieren. Ebenso ließ sich sagen, an welchen Standorten und bei welcher Institution diese angesiedelt waren. Durch die zunehmende Verbreitung von Cloud-Diensten sowie der Kommunikation über das Internet verschwinden diese Grenzen zunehmend.

- **Kürzere Angriffszyklen**
  Die beste Vorbeugung gegen Schadprogramme oder andere Angriffe auf IT-Systeme, Anwendungsprogramme und Protokolle ist, sich frühzeitig über Sicherheitslücken und deren Beseitigung, z. B. durch Einspielen von Patches und Updates, zu informieren. Die Zeitspanne zwischen dem Bekanntwerden einer Sicherheitslücke und den ersten Angriffen in der Breite ist mittlerweile sehr kurz, so dass es immer wichtiger wird, ein gut aufgestelltes Informationssicherheitsmanagement und Warnsystem zu haben.

- **Höhere Interaktivität von Anwendungen**
  Bereits vorhandene Techniken werden immer stärker miteinander kombiniert, um so neue Anwendungs- und Nutzungsmodelle zu erschaffen. Darunter finden sich unterschiedliche Anwendungsbereiche wie soziale Kommunikationsplattformen, Portale für die gemeinsame Nutzung von Informationen, Bildern und Videos oder interaktive Web-Anwendungen. Dies führt aber auch zu einer höheren Verquickung unterschiedlicher Geschäftsprozesse und höherer Komplexität, wodurch die IT-Systeme insgesamt schwieriger abzusichern sind.

- **Verantwortung der Benutzenden**
  Die beste Technik und solide Sicherheitsmaßnahmen können keine ausreichende Informationssicherheit gewährleisten, wenn der Mensch als Akteur nicht angemessen berücksichtigt wird. Dabei geht es vor allem um das verantwortungsvolle Handeln des Einzelnen. Dazu ist es notwendig, aktuelle Informationen über Sicherheitsrisiken und Verhaltensregeln im Umgang mit der IT zu beachten.

IT-Grundschutz: Ziel, Idee und Konzeption

Im IT-Grundschutz-Kompendium werden standardisierte Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen, Gebäude und Räume in IT-Grundschutz-Bausteinen beschrieben. Ziel des IT-Grundschutzes ist es, einen angemessenen Schutz für alle Informationen einer Institution zu erreichen. Die IT-Grundschutz-Methodik zeichnet sich dabei durch einen ganzheitlichen Ansatz aus. Durch die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen wird ein Sicherheitsniveau erreicht, das für den jeweiligen Schutzbedarf angemessen und ausreichend ist, um institutionsrelevante Informationen zu schützen. Darüber hinaus bilden die Anforderungen des IT-Grundschutz-Kompendiums nicht nur eine Basis für hochschutzbedürftige Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen, Gebäude und Räume, sondern erläutern an vielen Stellen, wie ein höheres Sicherheitsniveau erreichbar ist.

Der IT-Grundschutz nutzt das Baukastenprinzip, um den heterogenen Bereich der Informationstechnik einschließlich der Einsatzumgebung besser strukturieren und planen zu können. Die einzelnen Bausteine thematisieren typische Abläufe von Geschäftsprozessen und Bereiche des IT-Einsatzes, wie beispielsweise Notfallmanagement, Client-Server-Netze, bauliche Einrichtungen sowie Kommunikations- und Applikationskomponenten.

Die Bausteine des IT-Grundschutz-Kompendiums bilden den Stand der Technik ab, basierend auf den Erkenntnissen zum Zeitpunkt der Veröffentlichung. Die dort formulierten Anforderungen beschreiben, was generell umzusetzen ist, um mit geeigneten Sicherheitsmaßnahmen den Stand der Technik zu erreichen. Anforderungen und Maßnahmen, die den Stand der Technik abbilden, entsprechen dem, was zum jeweiligen Zeitpunkt einerseits technisch fortschrittlich und andererseits in der Praxis als geeignet erwiesen haben.

Analyseaufwand reduzieren

Die Methodik nach IT-Grundschutz ermöglicht es, Sicherheitskonzepte einfach und arbeitsökonomisch zu erstellen. Bei der traditionellen Risikoanalyse werden zunächst die Bedrohungen und Schwachstellen ermittelt und mit Eintrittswahrscheinlichkeiten bewertet, um dann die geeigneten Sicherheitsmaßnahmen auszuwählen und anschließend das noch verbleibende Restrisiko bewerten zu können. Diese Schritte sind beim IT-Grundschutz bereits für jeden Baustein durchgeführt worden. Es wurden die für typische Einsatzszenarien passenden standardisierten Sicherheitsanforderungen ausgewählt, die dann in Sicherheitsmaßnahmen überführt werden können, die zu den individuellen Rahmenbedingungen passen. Bei der IT-Grundschutz-Methodik reduziert sich die Analyse auf einen Soll-Ist-Vergleich zwischen den im IT-Grundschutz-Kompendium empfohlenen und den bereits umgesetzten Sicherheitsanforderungen. Die noch offenen Anforderungen zeigen die Sicherheitsdefizite auf, die es zu beheben gilt. Erst bei einem höheren Schutzbedarf muss zusätzlich zu den Anforderungen aus den IT-Grundschutz-Bausteinen eine individuelle Risikoanalyse unter Beachtung von Kosten- und Wirksamkeitsaspekten durchgeführt werden. Hierbei reicht es dann aber in der Regel aus, die auf Basis des IT-Grundschutz-Kompendiums ausgewählten Maßnahmen durch entsprechende individuelle, qualitativ höherwertige Maßnahmen zu ergänzen. Eine Vorgehensweise hierzu ist im BSI-Standard 200-3 *Risikoanalyse auf der Basis von IT-Grundschutz* beschrieben.

Auch wenn besondere Komponenten oder Einsatzumgebungen vorliegen, die im IT-Grundschutz-Kompendium nicht hinreichend behandelt werden, bietet das IT-Grundschutz-Kompendium eine wertvolle Arbeitshilfe. Bei der erforderlichen individuellen Risikoanalyse kann der Fokus auf die spezifischen Gefährdungen und Sicherheitsmaßnahmen gelegt werden.

Anforderungen für jedes Sicherheitsbedürfnis

Die im IT-Grundschutz-Kompendium aufgeführten Anforderungen sollten erfüllt werden, um ein angemessenes Sicherheitsniveau zu erreichen. Die Anforderungen sind in Basis- und Standard-Anforderungen sowie Anforderungen für erhöhten Schutzbedarf unterteilt. Die Basis-Anforderungen stellen das Minimum dessen dar, was vernünftigerweise an Sicherheitsvorkehrungen umzusetzen ist. Als Einstieg kann sich die umsetzende Institution auf die Basis-Anforderungen beschränken, um so zeitnah die wirkungsvollsten Anforderungen zu erfüllen. Eine angemessene Sicherheit nach dem Stand der Technik wird allerdings erst mit der Umsetzung der Standard-Anforderungen erreicht. Die exemplarischen Anforderungen für einen erhöhten Schutzbedarf haben sich ebenfalls in der Praxis bewährt und zeigen auf, wie eine Institution sich bei erhöhten Sicherheitsanforderungen zusätzlich absichern kann. Zudem enthalten die Umsetzungshinweise, die ergänzend zu den meisten Bausteinen veröffentlicht werden, Best Practices sowie ergänzende Hinweise, wie die Anforderungen erfüllt werden können. Für eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz müssen für den ausgewählten Geltungsbereich die Basis- und Standard-Anforderungen erfüllt werden. Da die Teilanforderungen mit dem Modalverb MUSS uneingeschränkte Anforderungen sind, die vorrangig erfüllt werden müssen, ist eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz nur möglich, wenn alle diese Teilanforderungen erfüllt sind.

Die IT-Grundschutz-Bausteine und die zugehörigen Umsetzungshinweise werden wie die meisten Informationen rund um IT-Grundschutz in elektronischer Form zur Verfügung gestellt. Die IT-Grundschutz-Texte können daher auch als Grundlage benutzt werden, um Sicherheitskonzepte zu erstellen. Zudem stehen Hilfsmittel und Musterlösungen zur Verfügung, die dabei unterstützen können, die Anforderungen geeignet zu erfüllen.

Da der IT-Grundschutz auch international großen Anklang findet, werden das IT-Grundschutz-Kompendium und weitere Veröffentlichungen auch in englischer Sprache online zur Verfügung gestellt.

Weiterentwicklung des IT-Grundschutz-Kompendiums

Die Inhalte des IT-Grundschutz-Kompendiums sind aufgrund der rasanten Entwicklungen in der Informationstechnik sowie immer kürzer werdender Produktzyklen ständigen Veränderungen ausgesetzt. Struktur und Inhalt des IT-Grundschutz-Kompendiums sind daher danach angelegt, dass einzelne Veröffentlichungen wie Bausteine zügig aktualisiert und neue Themen aufgenommen werden können. Neben dem BSI können auch Anwendende des IT-Grundschutzes ihren Beitrag leisten, indem sie Texte bis hin zu ganzen Bausteinen für den IT-Grundschutz erstellen, Bausteine kommentieren oder neue Themen anregen. Ziel ist es, das IT-Grundschutz-Kompendium auf einem aktuellen Stand zu halten.

Aktuelle Informationen zum IT-Grundschutz liefert der IT-Grundschutz-Newsletter, für den Interessierte sich auf der BSI-Webseite kostenfrei anmelden können. Über den Newsletter werden die Anwendenden auch immer wieder auf Mitwirkungsmöglichkeiten hingewiesen, wie beispielsweise auf Umfragen zu einzelnen aktuellen Themen. Die Rückmeldungen der Anwendenden liefern wertvolle Anregungen und Hinweise für die Weiterentwicklung des IT-Grundschutzes. Die Erfahrungen aus der Alltagspraxis sind sehr wichtig, damit Anforderungen und Empfehlungen stets geprüft und an den aktuellen Bedarf angepasst werden können.

Aufbau des IT-Grundschutz-Kompendiums

Das IT-Grundschutz-Kompendium lässt sich in unterschiedliche Bereiche untergliedern, die zum besseren Verständnis hier kurz erläutert werden:

Einstieg

In diesem einleitenden Teil wird kurz die Idee, Ziel und Struktur des IT-Grundschutz-Kompendiums erläutert. Eine ausführliche Beschreibung der IT-Grundschutz-Methodik ist im BSI-Standard 200-2 nachzulesen.

Hinweise zum Schichtenmodell und zur Modellierung

Um einen komplexen Informationsverbund nach IT-Grundschutz zu modellieren, müssen die passenden Bausteine des IT-Grundschutz-Kompendiums ausgewählt und umgesetzt werden. Um die Auswahl zu erleichtern, sind die Bausteine im IT-Grundschutz-Kompendium zunächst in prozess- und systemorientierte Bausteine aufgeteilt. Prozess-Bausteine gelten in der Regel für sämtliche oder große Teile des Informationsverbunds gleichermaßen, System-Bausteine lassen sich in der Regel auf einzelne Objekte oder Gruppen von Objekten anwenden. Die Prozess- und System-Bausteine bestehen wiederum aus weiteren Teilschichten.

In den Hinweisen zum Schichtenmodell und zur Modellierung wird beschrieben, wann ein einzelner Baustein sinnvollerweise eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist. Außerdem sind die Bausteine danach gekennzeichnet, ob sie vor- oder nachrangig umgesetzt werden sollten.

Beschreibung der Rollen

In den Anforderungen der Bausteine werden die Rollen genannt, die für die jeweilige Umsetzung zuständig sind. Hieraus können die geeigneten Personen für die jeweilige Thematik in der Institution identifiziert werden. Da die Bezeichnungen der im IT-Grundschutz-Kompendium als zuständig genannten Personen oder Rollen nicht in allen Institutionen einheitlich sind, wird für eine leichtere Zuordnung in Kapitel 3 *Rollen* eine kurze Beschreibung der wesentlichen Rollen dargestellt.

Glossar

Im Glossar zum IT-Grundschutz-Kompendium werden die wichtigsten Begriffe rund um Informationssicherheit und IT-Grundschutz erläutert. Ein hierzu ergänzendes Glossar zur Cyber-Sicherheit ist auf den Webseiten des BSI zu finden.

Elementare Gefährdungen

Das BSI hat aus vielen spezifischen Einzelgefährdungen generelle Aspekte herausgearbeitet und in 47 sogenannte elementare Gefährdungen überführt. Diese sind im IT-Grundschutz-Kompendium aufgeführt. Bei der Erstellung der Übersicht der elementaren Gefährdungen wurden die im Folgenden beschriebenen Ziele verfolgt. Elementare Gefährdungen sind

- für die Verwendung bei der Risikoanalyse optimiert,
- produktneutral (immer), technikneutral (möglichst, bestimmte Techniken prägen so stark den Markt, dass sie auch die abstrahierten Gefährdungen beeinflussen),
- kompatibel mit vergleichbaren internationalen Katalogen und Standards und
- nahtlos in den IT-Grundschutz integriert.

IT-Grundschutz-Bausteine

Die Bausteine des IT-Grundschutz-Kompendiums enthalten jeweils eine Beschreibung der betrachteten Komponente, Vorgehensweisen und IT-Systeme, gefolgt von einem kurzen Überblick über spezifische Gefährdungen sowie konkreter Anforderungen, um das Zielobjekt abzusichern.

Aufbau der Bausteine

Die zentrale Rolle des IT-Grundschutz-Kompendiums spielen die einzelnen Bausteine, deren Aufbau jeweils gleich ist. Zunächst wird jeweils das betrachtete Zielobjekt allgemein beschrieben. Die folgende Zielsetzung formuliert, welcher Sicherheitsgewinn mit der Umsetzung des IT-Grundschutz-Bausteins erreicht werden soll. Danach folgt das Kapitel *Abgrenzung und Modellierung*. Hier erfolgt eine Abgrenzung der Aspekte, die nicht im jeweiligen Baustein behandelt werden, sowie Verweise auf andere Bausteine, die diese Aspekte aufgreifen. Neben der Abgrenzung werden in diesem Kapitel auch Modellierungshinweise für den konkreten Baustein aufgeführt.

Im Anschluss werden spezifische Gefährdungen aufgeführt. Sie erheben keinen Anspruch auf Vollständigkeit, liefern aber ein Bild über die Sicherheitsprobleme, die ohne Gegenmaßnahmen beim Einsatz der betrachteten Komponente, Vorgehensweise oder des betrachteten IT-Systems entstehen können. Die Erläuterung der möglichen Risiken kann noch stärker für das Thema sensibilisieren. Bei der Risikoanalyse, die jedem Baustein zugrunde liegt, wurden die spezifischen Gefährdungen aus den elementaren Gefährdungen abgeleitet. Anforderungen, die gegen diese Gefährdungen wirken, sind in der Regel im selben Baustein zu finden, in einigen Fällen sind aber zusätzliche Anforderungen aus anderen Bausteinen zu berücksichtigen.

Auf die spezifischen Gefährdungen folgen in der Bausteinstruktur die Anforderungen. Diese sind in drei Kategorien gegliedert: Basis- und Standard-Anforderungen sowie Anforderungen bei erhöhtem Schutzbedarf. Basis-Anforderungen sind vorrangig umzusetzen, da sie mit geringem Aufwand den größtmöglichen Nutzen erzielen. Gemeinsam mit den Basis-Anforderungen erfüllen die Standard-Anforderungen den Stand der Technik und adressieren den normalen Schutzbedarf. Ergänzend dazu bieten die Bausteine des IT-Grundschutz-Kompendiums Vorschläge für Anforderungen bei erhöhtem Schutzbedarf. Zur Referenzierung sind die Anforderungen bausteinübergreifend eindeutig nummeriert, z. B. SYS.3.4.A2. Über dieses Schema wird zunächst die Schicht (im Beispiel „SYS“) benannt, dann die Nummern der jeweiligen Teilschichten und des Bausteins (im Beispiel „3.4“) und schließlich die Anforderung selbst (im Beispiel „A2“). Gibt es passende Umsetzungshinweise, trägt die dort aufgeführte Maßnahme zu einer Anforderung „A“ die gleiche Nummer mit einem vorangestellten Buchstaben „M“, im Beispiel also „SYS.3.4.M2“.

In jedem Baustein wird beschrieben, wer für dessen Umsetzung zuständig ist. Es ist immer eine grundsätzlich zuständige Rolle benannt. Daneben kann es weitere Rollen geben, die für die Umsetzung von Anforderungen zuständig sind. Diese werden dann jeweils im Titel der Anforderung in eckigen Klammern genannt. Der oder die Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der oder die ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden.

In den Überschriften der Anforderungen werden die Anforderungstitel neben den zu beteiligenden Rollen um ein Kürzel ergänzt, um auch außerhalb des Kontexts des jeweiligen Bausteins direkt ersichtlich zu machen, ob es sich um eine „Basis-Anforderung“ (B), eine „Standard-Anforderung“ (S) oder eine „Anforderung bei erhöhtem Schutzbedarf“ (H) handelt.

Am Ende der Bausteine sind weiterführende Informationen und Verweise aufgeführt. Ergänzt werden die Bausteine zudem in einem Anhang um eine sogenannte Kreuzreferenztabelle, in der den Anforderungen die betreffenden elementaren Gefährdungen zugeordnet werden. Diese Zuordnung kann für eine Risikoanalyse genutzt werden.

Modalverben

In den Bausteinen des IT-Grundschutz-Kompendiums werden die Prüfaspekte in den Anforderungen mit den in Versalien geschriebenen Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert, um die jeweiligen Anforderungen eindeutig zu kennzeichnen. Die Modalverben werden entsprechend den sprachlichen Erfordernissen konjugiert. Bei Verneinungen ist auch eine Trennung der beiden Worte zulässig.

Die hier genutzte Definition basiert auf RFC 2119 (Key words for use in RFCs to Indicate Requirement Levels), Stand 1997 sowie DIN 820-2:2012, Anhang H.

MUSS / DARF NUR:

Dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss (uneingeschränkte Anforderungen, für die keine Risikoübernahme möglich ist).

DARF NICHT / DARF KEIN:

Dieser Ausdruck bedeutet, dass etwas in keinem Fall getan werden darf (uneingeschränktes Verbot).

SOLLTE:

Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.

SOLLTE NICHT / SOLLTE KEIN:

Dieser Ausdruck bedeutet, dass etwas normalerweise nicht getan werden sollte, es aber Gründe gibt, dies doch zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.

Kreuzreferenztabellen

Die Kreuzreferenztabellen werden separat auf den Webseiten des BSI veröffentlicht.

Alle Kreuzreferenztabellen haben einen einheitlichen Aufbau. In der Kopfzeile sind die im dazugehörigen Baustein aufgelisteten elementaren Gefährdungen mit ihren Nummern eingetragen. In der ersten Spalte finden sich entsprechend die Nummern der Anforderungen wieder.

Die übrigen Spalten beschreiben, wie die Anforderungen des Bausteins und die elementaren Gefährdungen konkret zueinander stehen. Ist in einem Feld ein „X“ eingetragen, so bedeutet dies, dass die korrespondierende Anforderung gegen die entsprechende Gefährdung wirksam ist. Dies kann Schäden vorbeugen oder mindern.

Zu beachten ist, dass eine Anforderung nicht automatisch hinfällig wird, wenn alle in der Tabelle zugeordneten Gefährdungen in einem bestimmten Anwendungsfall nicht relevant sind. Ob auf eine Anforderung verzichtet werden kann, muss immer im Einzelfall anhand der vollständigen Sicherheitskonzeption und nicht nur anhand der Kreuzreferenztabelle geprüft und dokumentiert werden.

Überarbeitung von IT-Grundschutz-Bausteinen

Der IT-Grundschutz wird permanent weiterentwickelt. Hierbei wird das IT-Grundschutz-Kompendium nicht nur um Bausteine zu neuen Themen ergänzt, sondern die bestehenden werden regelmäßig überarbeitet, damit die Inhalte dem Stand der Technik entsprechen.

Wenn sich bei einem Baustein einzelne Anforderungen ändern, kann es notwendig sein, dass Institutionen, die den Baustein bereits umgesetzt haben, bestehende Sicherheitskonzepte anpassen müssen. Um diesen Arbeitsschritt zu erleichtern, stellt das BSI jeweils Änderungsdokumente zur Vorjahres-Edition des IT-Grundschutz-Kompendiums bereit. Diese listen alle Änderungen an Bausteinen auf, die über geringfügige sprachliche oder redaktionelle Änderungen hinausgehen. Alle Änderungen sind im Kapitel „Neues im IT-Grundschutz-Kompendium“ zu finden.

Hinweis: Die initial vergebene Nummerierung der einzelnen Anforderungen bleibt bei der Überarbeitung der Bausteine für folgende Editionen bestehen. Hierdurch wird gewährleistet, dass z. B. Sicherheitskonzepte oder IT-Grundschutz-Profile, die auf konkrete Anforderungen verweisen, auch nach einer Aktualisierung des Bausteins weiterhin korrekt referenzieren. Wenn innerhalb eines Bausteins Anforderungen ergänzt, entfernt oder verschoben werden, kann daher keine aufsteigende sowie durchgehende Nummerierung der Anforderungen gewährleistet werden. Besteht beispielsweise ein Baustein in seiner bisherigen Fassung aus fünf Basis- („A1“ bis „A5“) und zehn Standard-Anforderungen („A6“ bis „A15“), die um eine neue Basis-Anforderung ergänzt werden, so erhält diese die Nummer „A16“ und wird am Ende des Kapitels „3.1 Basis-Anforderungen“ zwischen „A5“ und „A6“ platziert.

Umsetzungshinweise

Zu vielen Bausteinen des IT-Grundschutz-Kompendiums gibt es detaillierte Umsetzungshinweise. Diese beschreiben, wie die Anforderungen der Bausteine umgesetzt werden können und erläutern im Detail geeignete Sicherheitsmaßnahmen. Die Maßnahmen können als Grundlage für Sicherheitskonzeptionen verwendet werden, sie sollten aber an die Rahmenbedingungen der jeweiligen Institution angepasst werden.

Die Umsetzungshinweise adressieren jeweils die Personengruppen, die für die Umsetzung der Baustein-Anforderungen zuständig sind, beispielsweise den IT-Betrieb oder die Haustechnik. Die Umsetzungshinweise sind nicht Bestandteil des IT-Grundschutz-Kompendiums, sondern werden als Hilfsmittel zu den Bausteinen veröffentlicht.

Ein Umsetzungshinweis kann Maßnahmen für mehrere Bausteine enthalten, denn in der Regel werden viele Sicherheitsanforderungen bereits durch übergreifende Bausteine abgedeckt. Beispielsweise stellt der Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* eine Anforderung für die Verwendung eines Zugriffsschutzes auf. Diese gilt gleichermaßen für alle Smartphones und Tablets unabhängig vom Betriebssystem. Der Umsetzungshinweis zu SYS.3.2.3 *iOS (for Enterprise)* beschreibt daher konkrete Maßnahmen für iOS, um diese allgemeingültige Anforderung aus SYS.3.2.1 zu erfüllen.

Die Maßnahmen in den Umsetzungshinweisen sind aufsteigend nummeriert, wobei eine eindeutige Zuordnung zwischen den Maßnahmen (gekennzeichnet mit M) und den Anforderungen (gekennzeichnet mit A) besteht. In Umsetzungshinweisen wird nicht nach Anforderungskategorie unterschieden.

Anwendungsweise des IT-Grundschutz-Kompendiums

Für eine erfolgreiche Etablierung eines ISMS bietet der BSI-Standard 200-2 *IT-Grundschutz-Methodik* gemeinsam mit dem IT-Grundschutz-Kompendium viele Hinweise zu den Vorgehensweisen Basis-, Kern- und Standard-Absicherung sowie praktische Umsetzungshilfen. Hinzu kommen Lösungsansätze für verschiedene, die Informationssicherheit betreffende Aufgabenstellungen, beispielsweise Sicherheitskonzeption, Revision und Zertifizierung. Je nach vorliegender Aufgabenstellung sind dabei unterschiedliche Anwendungsweisen des IT-Grundschutzes zweckmäßig.

Schichtenmodell und Modellierung

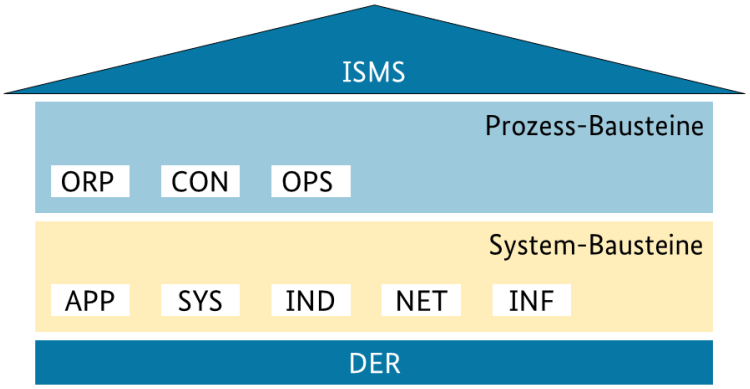
Bei der Umsetzung von IT-Grundschutz muss der betrachtete Informationsverbund mit Hilfe der vorhandenen Bausteine nachgebildet werden, es müssen also die relevanten Sicherheitsanforderungen aus dem IT-Grundschutz-Kompendium zusammengetragen werden. Dafür müssen alle Prozesse, Anwendungen und IT-Systeme erfasst sein, beziehungsweise die Strukturanalyse und in der Regel eine Schutzbedarfsfeststellung vorliegen. Darauf aufbauend wird ein IT-Grundschutz-Modell des Informationsverbunds erstellt, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten IT-Grundschutz-Bausteinen besteht und eine Abbildung zwischen den Bausteinen und den sicherheitsrelevanten Aspekten des Informationsverbunds beinhaltet.

Das erstellte IT-Grundschutz-Modell ist unabhängig davon, ob der Informationsverbund aus bereits im Einsatz befindlichen IT-Systemen besteht oder ob es sich um einen Informationsverbund handelt, der sich erst im Planungsstadium befindet. Das Modell kann daher unterschiedlich verwendet werden:

- Das IT-Grundschutz-Modell eines *bereits realisierten* Informationsverbunds identifiziert über die verwendeten Bausteine die relevanten Sicherheitsanforderungen. Es kann in Form eines Prüfplans benutzt werden, um einen Soll-Ist-Vergleich durchzuführen.
- Das IT-Grundschutz-Modell eines *geplanten* Informationsverbunds stellt hingegen ein Entwicklungskonzept dar. Es beschreibt über die ausgewählten Bausteine, welche Sicherheitsanforderungen bei der Realisierung des Informationsverbunds erfüllt werden müssen.

Typischerweise wird ein im Einsatz befindlicher Informationsverbund sowohl bereits realisierte als auch in Planung befindliche Anteile umfassen. Das resultierende IT-Grundschutz-Modell beinhaltet dann sowohl einen Prüfplan wie auch Anteile eines Entwicklungskonzepts. Alle im Prüfplan bzw. im Entwicklungskonzept vorgesehenen Sicherheitsanforderungen bilden gemeinsam die Basis für die Erstellung des Sicherheitskonzeptes.

Um einen im Allgemeinen komplexen Informationsverbund nach IT-Grundschutz zu modellieren, müssen die passenden Bausteine des IT-Grundschutz-Kompendiums ausgewählt und umgesetzt werden. Um diese Auswahl zu erleichtern, sind die Bausteine im IT-Grundschutz-Kompendium zunächst in Prozess- und System-Bausteine aufgeteilt und diese jeweils in einzelne Schichten untergliedert:



Prozess-Bausteine:

Die Prozess-Bausteine, die in der Regel für sämtliche oder große Teile eines Informationsverbunds gleichermaßen gelten, unterteilen sich in die folgenden Schichten, die wiederum aus weiteren Teilschichten bestehen können.

- Die Schicht ISMS enthält als Grundlage für alle weiteren Aktivitäten im Sicherheitsprozess den Baustein *Sicherheitsmanagement*.
- Die Schicht ORP befasst sich mit organisatorischen und personellen Sicherheitsaspekten. In diese Schicht fallen beispielsweise die Bausteine *Organisation* und *Personal*.
- Die Schicht CON enthält Bausteine, die sich mit Konzepten und Vorgehensweisen befassen. Typische Bausteine der Schicht CON sind unter anderem *Kryptokonzept* und *Datenschutz*.
- Die Schicht OPS umfasst alle Sicherheitsaspekte betrieblicher Art. Insbesondere sind dies die Sicherheitsaspekte des operativen IT-Betriebs, sowohl bei einem Betrieb im Haus, als auch bei einem IT-Betrieb, der in Teilen oder komplett durch Dritte betrieben wird. Ebenso enthält er die Sicherheitsaspekte, die bei einem IT-Betrieb für

Dritte zu beachten sind. Beispiele für die Schicht OPS sind die Bausteine *Schutz vor Schadprogrammen* und *Outsourcing für Kunden.*

- In der Schicht DER finden sich alle Bausteine, die für die Überprüfung der umgesetzten Sicherheitsmaßnahmen, die Detektion von Sicherheitsvorfällen sowie die geeigneten Reaktionen darauf relevant sind. Typische Bausteine der Schicht DER sind *Behandlung von Sicherheitsvorfällen* und *Vorsorge für IT-Forensik*.

Neben den Prozess-Bausteinen beinhaltet das IT-Grundschutz-Kompendium auch System-Bausteine. Diese werden in der Regel auf einzelne Zielobjekte oder Gruppen von Zielobjekten angewendet. Die System-Bausteine unterteilen sich in die folgenden Schichten. Ähnlich wie die Prozess-Bausteine können auch die System-Bausteine aus weiteren Teilschichten bestehen.

System-Bausteine:

- Die Schicht APP beschäftigt sich mit der Absicherung von Anwendungen und Diensten, unter anderem in den Bereichen Kommunikation, Verzeichnisdienste, netzbasierte Dienste sowie Business- und Client-Anwendungen. Typische Bausteine der Schicht APP sind *Allgemeiner E-Mail-Client und -Server*, *Office-Produkte*, *Webserver* und *Relationale Datenbanken*.
- Die Schicht SYS betrifft die einzelnen IT-Systeme des Informationsverbunds, die gegebenenfalls in Gruppen zusammengefasst wurden. Hier werden die Sicherheitsaspekte von Servern, Desktop-Systemen, Mobile Devices und sonstigen IT-Systemen wie Druckern und TK-Anlagen behandelt. Zur Schicht SYS gehören beispielsweise Bausteine zu konkreten Betriebssystemen, *Allgemeine Smartphones und Tablets* sowie *Drucker, Kopierer und Multifunktionsgeräte*.
- Die Schicht IND befasst sich mit Sicherheitsaspekten industrieller IT. In diese Schicht fallen beispielsweise die Bausteine *Prozessleit- und Automatisierungstechnik*, *Allgemeine ICS-Komponente* und *Speicherprogrammierbare Steuerung (SPS)*.
- Die Schicht NET betrachtet die Vernetzungsaspekte, die sich nicht primär auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. Dazu gehören zum Beispiel die Bausteine *Netz-Management*, *Firewall* und *WLAN-Betrieb*.
- Die Schicht INF befasst sich mit den baulich-technischen Gegebenheiten, hier werden Aspekte der infrastrukturellen Sicherheit zusammengeführt. Dies betrifft unter anderem die Bausteine *Allgemeines Gebäude* und *Rechenzentrum*.

Modellierung

Die Modellierung nach IT-Grundschutz besteht darin, für die Bausteine jeder Schicht zu entscheiden, ob und wie sie zur Abbildung des Informationsverbunds herangezogen werden können. Je nach betrachtetem Baustein kann es sich um unterschiedliche Zielobjekte handeln, beispielsweise um Anwendungen, IT-Systeme, Gruppen von Komponenten, Räume und Gebäude.

In den einzelnen Bausteinen ist in Kapitel 1.3 „Abgrenzung und Modellierung" detailliert beschrieben, wann ein Baustein eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist.

Bei der Modellierung eines Informationsverbunds nach IT-Grundschutz kann es Zielobjekte geben, die mit den vorliegenden Bausteinen nicht hinreichend abgebildet werden können. In diesem Fall muss eine Risikoanalyse durchgeführt werden, wie sie in der IT-Grundschutz-Methodik beschrieben ist.

In vielen Teilschichten gibt es allgemeine Bausteine, die grundlegende Aspekte übergreifend für die spezifischen Bausteine beschreiben. Beispielsweise enthält SYS.2.1 *Allgemeiner Client* Anforderungen für *alle* Client-Betriebssysteme, die dann für macOS-, Windows- und Unix/Linux-Clients in den entsprechenden Bausteinen konkretisiert und ergänzt werden. Weitere Beispiele sind APP.2.1 *Allgemeiner Verzeichnisdienst* oder SYS.3.2.1 *Allgemeine Smartphones und Tablets*. Spezifische Bausteine sind stets in Verbindung mit den allgemeinen Bausteinen anzuwenden. Weiterhin stellen allgemeine Bausteine eine gute Grundlage für die Modellierung und Risikoanalyse dar, wenn für ein konkretes Zielobjekt kein spezifischer Baustein existiert.

Die nachfolgende Tabelle gibt einen ersten Überblick, auf welche Zielobjekttypen die Bausteine jeweils anzuwenden sind und in welcher Reihenfolge die Umsetzung der Bausteine erfolgen kann (Erläuterung zu R1, R2 und R3 in Kapitel 2.2 *Bearbeitungsreihenfolge der Bausteine*).

Dabei gibt es Bausteine, die eindeutig zu Zielobjekttypen wie IT-System, Anwendung oder Informationsverbund/übergeordnete Aspekte zuzuordnen sind, d. h. diese Aspekte *ausschließlich* oder *mehrheitlich* behandeln. Einige Bausteine, wie z. B. OPS.1.2.4 *Telearbeit* oder INF.9 *Mobiler Arbeitsplatz*, lassen sich *nicht* eindeutig zu Zielobjekttypen zuordnen, da sie verschiedene Aspekte behandeln. Telearbeit behandelt z. B. Aspekte von IT-Systemen, Kommunikationsverbindungen, Informationsfluss, Datensicherung usw. Diese Bausteine haben somit Auswirkungen auf den gesamten Informationsverbund und werden daher dem Zielobjekttyp „Informationsverbund/übergeordnete Aspekte" zugeordnet.

Die Zuordnung zu den Zielobjekten ist exemplarisch und dient zur besseren Einordnung und einfacherem Verständnis. In der individuellen Umsetzung von IT-Grundschutz bedeutet z. B. eine Zuordnung eines Bausteins zu „Informationsverbund/übergeordnete Aspekte" nicht, dass dieser Zielobjekttyp angelegt werden muss. Vielmehr ist damit gemeint, dass der Baustein Auswirkungen auf den gesamten Informationsverbund und damit gegebenenfalls mehrere Zielobjekte haben kann.

Baustein	Reihenfolge	Anzuwenden auf Zielobjekttyp
ISMS.1 Sicherheitsmanagement	R1	Informationsverbund/übergeordnete Aspekte
ORP.1 Organisation	R1	Informationsverbund/übergeordnete Aspekte
ORP.2 Personal	R1	Informationsverbund/übergeordnete Aspekte
ORP.3 Sensibilisierung und Schulung zur Informationssicherheit	R1	Informationsverbund/übergeordnete Aspekte
ORP.4 Identitäts- und Berechtigungsmanagement	R1	Informationsverbund/übergeordnete Aspekte
ORP.5 Compliance Management (Anforderungsmanagement)	R3	Informationsverbund/übergeordnete Aspekte
CON.1 Kryptokonzept	R3	Informationsverbund/übergeordnete Aspekte
CON.2 Datenschutz	R2	Informationsverbund/übergeordnete Aspekte
CON.3 Datensicherungskonzept	R1	Informationsverbund/übergeordnete Aspekte
CON.6 Löschen und Vernichten	R1	Informationsverbund/übergeordnete Aspekte
CON.7 Informationssicherheit auf Auslandsreisen	R3	Informationsverbund/übergeordnete Aspekte
CON.8 Software-Entwicklung	R3	Informationsverbund/übergeordnete Aspekte
CON.9 Informationsaustausch	R3	Informationsverbund/übergeordnete Aspekte
CON.10 Entwicklung von Webanwendungen	R2	Informationsverbund/übergeordnete Aspekte
CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)	R3	Informationsverbund/übergeordnete Aspekte
OPS.1.1.1 Allgemeiner IT-Betrieb	R1	Informationsverbund/übergeordnete Aspekte
OPS.1.1.2 Ordnungsgemäße IT-Administration	R1	Informationsverbund/übergeordnete Aspekte
OPS.1.1.3 Patch- und Änderungsmanagement	R1	Informationsverbund/übergeordnete Aspekte
OPS.1.1.4 Schutz vor Schadprogrammen	R1	Informationsverbund/übergeordnete Aspekte
OPS.1.1.5 Protokollierung	R1	Informationsverbund/übergeordnete Aspekte
OPS.1.1.6 Software-Tests und -Freigaben	R1	Informationsverbund/übergeordnete Aspekte
OPS.1.1.7 Systemmanagement	R2	Informationsverbund/übergeordnete Aspekte
OPS.1.2.2 Archivierung	R3	Informationsverbund/übergeordnete Aspekte
OPS.1.2.4 Telearbeit	R2	Informationsverbund/übergeordnete Aspekte
OPS.1.2.5 Fernwartung	R3	Informationsverbund/übergeordnete Aspekte
OPS.1.2.6 NTP -Zeitsynchronisation	R2	Anwendung

Baustein	Reihenfolge	Anzuwenden auf Zielobjekttyp
OPS.2.2 Cloud-Nutzung	R2	Informationsverbund/übergeordnete Aspekte
OPS.2.3 Nutzung von Outsourcing	R2	Informationsverbund/übergeordnete Aspekte
OPS.3.2 Anbieten von Outsourcing	R3	Informationsverbund/übergeordnete Aspekte
DER.1 Detektion von sicherheitsrelevanten Ereignissen	R1	Informationsverbund/übergeordnete Aspekte
DER.2.1 Behandlung von Sicherheitsvorfällen	R1	Informationsverbund/übergeordnete Aspekte
DER.2.2 Vorsorge für die IT-Forensik	R3	Informationsverbund/übergeordnete Aspekte
DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle	R3	Informationsverbund/übergeordnete Aspekte
DER.3.1 Audits und Revisionen	R3	Informationsverbund/übergeordnete Aspekte
DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision	R3	Informationsverbund/übergeordnete Aspekte
DER.4 Notfallmanagement	R3	Informationsverbund/übergeordnete Aspekte
APP.1.1 Office-Produkte	R2	Anwendung
APP.1.2 Webbrowser	R2	Anwendung
APP.1.4 Mobile Anwendungen (Apps)	R2	Anwendung
APP.2.1 Allgemeiner Verzeichnisdienst	R2	Anwendung
APP.2.2 Active Directory Domain Services	R2	Anwendung
APP.2.3 OpenLDAP	R2	Anwendung
APP.3.1 Webanwendungen und Webservices	R2	Anwendung
APP.3.2 Webserver	R2	Anwendung
APP.3.3 Fileserver	R2	Anwendung
APP.3.4 Samba	R2	Anwendung
APP.3.6 DNS-Server	R2	Anwendung
APP.4.2 SAP-ERP-System	R2	Anwendung
APP.4.3 Relationale Datenbanken	R2	Anwendung
APP.4.4 Kubernetes	R2	Anwendung
APP.4.6 SAP ABAP-Programmierung	R2	Anwendung
APP.5.2 Microsoft Exchange und Outlook	R2	Anwendung
APP.5.3 Allgemeiner E-Mail-Client und -Server	R2	Anwendung
APP.5.4 Unified Communications und Collaboration (UCC)	R2	Anwendung
APP.6 Allgemeine Software	R2	Anwendung
APP.7 Entwicklung von Individualsoftware	R3	Informationsverbund/übergeordnete Aspekte
SYS.1.1 Allgemeiner Server	R2	IT-System
SYS.1.2.2 Windows Server 2012	R2	IT-System
SYS.1.2.3 Windows Server	R2	IT-System
SYS.1.3 Server unter Linux und Unix	R2	IT-System
SYS.1.5 Virtualisierung	R2	IT-System
SYS.1.6 Containerisierung	R2	IT-System
SYS.1.7 IBM Z	R2	IT-System
SYS.1.8 Speicherlösungen	R2	IT-System

Baustein	Reihenfolge	Anzuwenden auf Zielobjekttyp
SYS.1.9 Terminalserver	R2	IT-System
SYS.2.1 Allgemeiner Client	R2	IT-System
SYS.2.2.3 Clients unter Windows	R2	IT-System
SYS.2.3 Clients unter Linux und Unix	R2	IT-System
SYS.2.4 Clients unter macOS	R2	IT-System
SYS.2.5 Client-Virtualisierung	R2	IT-System
SYS.2.6 Virtual Desktop Infrastructure	R2	IT-System
SYS.3.1 Laptops	R2	IT-System
SYS.3.2.1 Allgemeine Smartphones und Tablets	R2	IT-System
SYS.3.2.2 Mobile Device Management (MDM)	R2	Informationsverbund/übergeordnete Aspekte
SYS.3.2.3 iOS (for Enterprise)	R2	IT-System
SYS.3.2.4 Android	R2	IT-System
SYS.3.3 Mobiltelefon	R2	IT-System
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	R2	IT-System
SYS.4.3 Eingebettete Systeme	R2	IT-System
SYS.4.4 Allgemeines IoT-Gerät	R2	IT-System
SYS.4.5 Wechseldatenträger	R2	IT-System
NET.1.1 Netzarchitektur und -design	R2	Netz
NET.1.2 Netzmanagement	R2	IT-System
NET.2.1 WLAN-Betrieb	R2	Netz
NET.2.2 WLAN-Nutzung	R2	IT-System
NET.3.1 Router und Switches	R2	IT-System
NET.3.2 Firewall	R2	IT-System
NET.3.3 VPN	R2	IT-System
NET.3.4 Network Access Control	R2	IT-System
NET.4.1 TK-Anlagen	R2	IT-System
NET.4.2 VoIP	R2	Netz
NET.4.3 Faxgeräte und Faxserver	R2	IT-System
IND.1 Prozessleit- und Automatisierungstechnik	R2	Informationsverbund/übergeordnete Aspekte
IND.2.1 Allgemeine ICS-Komponente	R2	IT-System
IND.2.2 Speicherprogrammierbare Steuerung (SPS)	R2	IT-System
IND.2.3 Sensoren und Aktoren	R2	IT-System
IND.2.4 Maschine	R2	IT-System
IND.2.7 Safety Instrumented Systems	R2	IT-System
IND.3.2 Fernwartung im industriellen Umfeld	R2	IT-System
INF.1 Allgemeines Gebäude	R2	Gebäude/Raum
INF.2 Rechenzentrum sowie Serverraum	R2	Gebäude/Raum

Baustein	Reihenfolge	Anzuwenden auf Zielobjekttyp
INF.5 Raum sowie Schrank für technische Infrastruktur	R2	Gebäude/Raum
INF.6 Datenträgerarchiv	R2	Gebäude/Raum
INF.7 Büroarbeitsplatz	R2	Gebäude/Raum
INF.8 Häuslicher Arbeitsplatz	R2	Gebäude/Raum
INF.9 Mobiler Arbeitsplatz	R2	Informationsverbund/übergeordnete Aspekte
INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume	R2	Gebäude/Raum
INF.11 Allgemeines Fahrzeug	R3	Gebäude/Raum
INF.12 Verkabelung	R2	Gebäude/Raum
INF.13 Technisches Gebäudemanagement	R2	Gebäude/Raum
INF.14 Gebäudeautomatisierung	R2	Gebäude/Raum

Bearbeitungsreihenfolge der Bausteine

Um grundlegende Risiken abzudecken und eine ganzheitliche Informationssicherheit aufzubauen, müssen die essenziellen Sicherheitsanforderungen frühzeitig erfüllt und entsprechende Sicherheitsmaßnahmen umgesetzt werden. Daher wird im IT-Grundschutz mit R1, R2 und R3 eine Reihenfolge für die umzusetzenden Bausteine vorgeschlagen (siehe Kapitel 2.1 *Modellierung*).

- R1: Diese Bausteine sollten vorrangig umgesetzt werden, da sie die Grundlage für einen effektiven Sicherheitsprozess bilden.
- R2: Diese Bausteine sollten als nächstes umgesetzt werden, da sie in wesentlichen Teilen des Informationsverbundes für nachhaltige Sicherheit erforderlich sind.
- R3: Diese Bausteine werden zur Erreichung des angestrebten Sicherheitsniveaus ebenfalls benötigt und müssen umgesetzt werden. Es wird empfohlen, diese erst nach den anderen Bausteinen zu betrachten.

Diese Kennzeichnung zeigt eine sinnvolle zeitliche Reihenfolge für die Umsetzung der Anforderungen des jeweiligen Bausteins auf und stellt keine Gewichtung der Bausteine untereinander dar. Grundsätzlich müssen alle für den jeweiligen Informationsverbund relevanten Bausteine des IT-Grundschutz-Kompendiums umgesetzt werden.

Rollen

Auditteam

Das Auditteam besteht aus Auditoren und Auditorinnen sowie Fachleuten, die die Auditteamleitung insbesondere fachlich während eines Audits unterstützen.

Bauleitung

Die Bauleitung ist für die Umsetzung von Baumaßnahmen zuständig.

Benutzende

Die Benutzenden sind die Mitarbeitenden einer Institution, die informationstechnische Systeme im Rahmen der Erledigung ihrer Aufgaben benutzen. IT-Benutzende und Benutzende sind hierbei als Synonyme zu betrachten, da heutzutage nahezu alle Mitarbeitenden eines Unternehmens bzw. einer Behörde informationstechnische Systeme während der Erledigung ihrer Aufgaben verwenden.

Bereichssicherheitsbeauftragte

Die Bereichssicherheitsbeauftragten sind für alle Sicherheitsbelange der Geschäftsprozesse, Anwendungen und IT-Systeme in ihren Bereichen (z. B. Abteilung oder Außenstelle) zuständig. Je nach Größe des zu betreuenden Bereichs kann die Aufgabe der Bereichssicherheitsbeauftragten von Personen übernommen werden, die bereits mit ähnlichen Aufgaben betraut sind.

Beschaffungsstelle

Die Beschaffungsstelle initiiert und überwacht Beschaffungen. Öffentliche Einrichtungen wickeln ihre Beschaffungen nach vorgeschriebenen Verfahren ab. Die Rolle schließt die zuständige Leitung der Organisationseinheit mit ein.

Brandschutzbeauftragte

Brandschutzbeauftragte sind für alle Fragen des Brandschutzes zuständig und stehen dafür als Ansprechperson zur Verfügung. Sie sind unter anderem zuständig für die Erstellung von Brandrisikoanalysen, Aus- und Fortbildung der Beschäftigten, teilweise auch für Wartung und Instandhaltung der Brandschutzeinrichtungen.

Datenschutzbeauftragte

Datenschutzbeauftragte sind von der Behörden- bzw. Unternehmensleitung bestellte Personen, die auf den datenschutzrechtlich korrekten bzw. gesetzeskonformen Umgang mit personenbezogenen Daten im Unternehmen bzw. in der Behörde hinwirken.

Compliance-Beauftragte

Die Compliance-Beauftragten sind dafür zuständig, die für die Institution relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben zu identifizieren und deren Einhaltung zu prüfen.

Entwickelnde

Als Entwickelnde werden im Kontext des IT-Grundschutzes die Personen bezeichnet, die bei der Planung, Entwicklung oder Pflege von Software, Hardware oder ganzen Systemen mitarbeiten. Im IT-Grundschutz werden unter dieser Rolle verschiedene weitere Rollen aus verschiedenen Bereichen zusammengefasst, wie z. B. aus Software-Architektur, Software-Design, Software-Entwicklung, Programmierung und Test. Die Rolle schließt die zuständige Leitung der Organisationseinheit mit ein.

Errichterfirma

Es handelt sich hierbei um ein Unternehmen, das Gewerke oder aber auch Gebäude errichtet.

Fachabteilung

Eine Fachabteilung ist ein Teil einer Behörde bzw. eines Unternehmens, das fachspezifische Aufgaben zu erledigen hat. Bei Bundes- und Landesbehörden ist eine Abteilung die übergeordnete Organisationsform mehrerer Referate, die inhaltlich zusammengehören.

Fachverantwortliche

Fachverantwortliche sind inhaltlich für ein oder mehrere Geschäftsprozesse oder Fachverfahren zuständig. Im IT-Grundschutz werden unter dieser Rolle verschiedene weitere Rollen zusammengefasst. Beispiele hierfür sind Rollen für das Änderungsmanagement oder die Archivverwaltung.

Haustechnik

Haustechnik bezeichnet die Organisationseinheit, die sich um die Einrichtungen der Infrastruktur in einem Gebäude oder in einer Liegenschaft kümmert. Betreute Gewerke können dabei z. B. Elektrotechnik, Melde- und Steuerungstechnik, Sicherungstechnik, IT-Netze (physischer Teil), Heizungs- und Sanitärtechnik oder Aufzüge sein. Die Rolle Haustechnik schließt die zuständige Leitung der Organisationseinheit mit ein.

ICS-Informationssicherheitsbeauftragte

ICS-Informationssicherheitsbeauftragte (oft auch Industrial Security Officer genannt) sind von der Institutionsleitung benannte Personen, die im Auftrag der Leitungsebene dafür sorgen, dass die speziellen Anforderungen im Bereich der industriellen Steuerung abgedeckt sind und die Sicherheitsorganisation aus dem Bereich ICS in das gesamte ISMS der Institution eingebunden ist.

Informationssicherheitsbeauftragte (ISB)

Informationssicherheitsbeauftragte sind von der Institutionsleitung ernannte Personen, die im Auftrag der Leitungsebene die Aufgabe Informationssicherheit koordinieren und innerhalb der Behörde bzw. des Unternehmens vorantreiben.

Institution

Mit dem Begriff Institution werden im IT-Grundschutz Unternehmen, Behörden und sonstige öffentliche oder private Organisationen bezeichnet.

Institutionsleitung

Dies bezeichnet die Leitungsebene der Institution bzw. der betrachteten Organisationseinheit.

IS-Revisionsteam

Das IS-Revisionsteam besteht aus IS-Revisoren und IS-Revisorinnen sowie Fachleuten, die die verantwortliche Leitung für die IS-Revision insbesondere fachlich während der IS-Revision unterstützen.

IT-Betrieb

Als IT-Betrieb wird die Organisationseinheit bezeichnet, die die interne IT einrichtet, betreibt, überwacht und wartet. Die Rolle IT-Betrieb schließt die zuständige Leitung der Organisationseinheit mit ein.

Mitarbeitende

Die Mitarbeitenden sind Teil einer Institution.

Notfallbeauftragte

Notfallbeauftragte steuern alle Aktivitäten rund um das Notfallmanagement. Sie sind für die Erstellung, Umsetzung, Pflege und Betreuung des institutionsweiten Notfallmanagements und der zugehörigen Dokumente, Regelungen und Maßnahmen zuständig. Sie analysieren den Gesamtablauf der Notfallbewältigung nach einem Schadensereignis.

OT-Betrieb (Operational Technology, OT)

Der OT-Betrieb ist für Einrichtung, Betrieb, Überwachung und Wartung der ICS-Systeme zuständig.

OT-Leitung

Die OT-Leitung bezeichnet die Leitung des Bereichs Produktion und Fertigung bzw. die verantwortliche Person für die industriellen Steuerungssysteme (ICS), die von der Institution eingesetzt werden.

Die OT-Leitung ist dafür zuständig, Risiken aus der Informationssicherheit für die Integrität der SIS (Safety Instrumented Systems) zu beurteilen und dem Stand der Technik entsprechende Maßnahmen zu ergreifen. Insbesondere ist die OT-Leitung dafür zuständig, die Belegschaft für die Belange der Informationssicherheit zu schulen.

Personalabteilung

Die Personalabteilung ist unter anderem für folgende Aufgaben zuständig:

- personalwirtschaftliche Grundfragen
- Personalbedarfsplanung
- Personalangelegenheiten der Mitarbeitenden
- soziale Betreuung der Mitarbeitenden
- allgemeine Zusammenarbeit mit der Personalvertretung.

Die Rolle Personalabteilung schließt die zuständige Leitung der Organisationseinheit mit ein.

Planende

Mit dem allgemeinen Begriff Planende werden Rollen zur Planung unterschiedlicher Aspekte zusammengefasst. Gemeint sind also Personen, die für die Planung und Konzeption bestimmter Aufgaben zuständig sind.

Testende

Testende sind Personen, die gemäß einem Testplan nach vorher festgelegten Verfahren und Kriterien eine neue oder veränderte Software bzw. Hardware testen und die Testergebnisse mit den erwarteten Ergebnissen vergleichen.

Vorgesetzte

Als Vorgesetzte werden die Mitarbeitenden einer Institution bezeichnet, die gegenüber anderen, ihnen zugeordneten Mitarbeitenden weisungsbefugt sind.

Wartungspersonal

Beim Wartungspersonal handelt es sich um Mitarbeitende von Dienstleistenden, die mit der Wartung von technischen Systemen (z. B. ICS- oder IT-Systeme) im Informationsverbund beauftragt wurden. Hierbei ist es in der Regel notwendig, dass das Wartungspersonal Zugriff auf die betroffenen Systeme erhält.

Zentrale Verwaltung

Die Rolle bezeichnet die Organisationseinheit, die den allgemeinen Betrieb regelt und überwacht sowie alle Verwaltungsdienstleistungen plant, organisiert und durchführt. Die Rolle Zentrale Verwaltung schließt die zuständige Leitung der Organisationseinheit mit ein.

Glossar

In diesem Glossar werden die wichtigsten Begriffe rund um Informationssicherheit und IT-Grundschutz erläutert. Ein hierzu ergänzendes Glossar zur Cyber-Sicherheit ist auf den Webseiten des BSI unter https://www.bsi.bund.de/cyberglossar zu finden.

Anforderung bei erhöhtem Schutzbedarf

Siehe Sicherheitsanforderung.

Angriff

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einer dritten Person zu schädigen. Ein Angriff kann auch im Auftrag von Dritten, die sich Vorteile verschaffen wollen, erfolgen.

Assets

Als Assets werden Bestände von Objekten bezeichnet, die für einen bestimmten Zweck, besonders zur Erreichung von Geschäftszielen, benötigt werden. Der englische Begriff „asset" wird häufig mit „Wert" übersetzt. Wert ist allerdings im Deutschen ein mit vielen Bedeutungen belegter Begriff, von der gesellschaftlichen Bedeutung, die einer Sache zukommt, bis hin zur inneren Qualität eines Objekts. Im IT-Grundschutz wird der Begriff „Assets" in der Bedeutung von „werthaltigen bzw. wertvollen Zielobjekten" verwendet.

Authentisierung (englisch „authentication")

Authentisierung bezeichnet den Nachweis oder die Überprüfung der Authentizität. Die Authentisierung einer Identität kann u.a. durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z. B. durch kryptographische Signaturen.

Authentizität

Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass eine Kommunikationsstelle tatsächlich diejenige ist, der sie vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

Autorisierung

Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist.

Basis-Absicherung

Die Basis-Absicherung ermöglicht es, als Einstieg in den IT-Grundschutz zunächst eine breite, grundlegende Erst-Absicherung über alle Geschäftsprozesse bzw. Fachverfahren einer Institution vorzunehmen.

Basis-Anforderung

Siehe Sicherheitsanforderung.

Bausteine

Das IT-Grundschutz-Kompendium enthält für unterschiedliche Vorgehensweisen, Komponenten und IT-Systeme Erläuterungen zur Gefährdungslage, Sicherheitsanforderungen und weiterführende Informationen, die jeweils in einem Baustein zusammengefasst sind. Das IT-Grundschutz-Kompendium ist aufgrund der Baustein-Struktur modular aufgebaut und legt einen Fokus auf die Darstellung der wesentlichen Sicherheitsanforderungen in den Bausteinen. Die grundlegende Struktur des IT-Grundschutz-Kompendiums unterteilt die Bausteine in prozess- und systemorientierte Bausteine, zudem sind sie nach Themen in ein Schichtenmodell einsortiert.

Beauftragte für IT-Sicherheit

Personen mit Fachkompetenz zur IT-Sicherheit, die in großen Institutionen für Aspekte rund um die IT-Sicherheit zuständig sind, in enger Abstimmung mit dem IT-Betrieb. Der oder die Informationssicherheitsbeauftragte (ISB) gestaltet das Informationssicherheitsmanagement und erstellt die generellen Sicherheitsziele und -vorgaben, ein Be-

auftragter oder eine Beauftragte für die IT-Sicherheit sorgt dafür, dass diese technisch umgesetzt werden. Diese für die IT-Sicherheit zuständigen Personen sind somit typischerweise im IT-Betrieb tätig, während der oder die ISB unmittelbar der Leitungsebene zuarbeitet.

Bedrohung (englisch „threat")

Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch der Person, die die Informationen besitzt oder benutzt, ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.

BIA (Business Impact Analyse)

Eine Business Impact Analyse (Folgeschädenabschätzung) ist eine Analyse zur Ermittlung von potenziellen direkten und indirekten Folgeschäden für eine Institution, die durch das Auftreten eines Notfalls oder einer Krise und Ausfall eines oder mehrerer Geschäftsprozesse verursacht werden. Es ist ein Verfahren, um kritische Ressourcen und Wiederanlaufanforderungen sowie die Auswirkungen von ungeplanten Geschäftsunterbrechungen zu identifizieren.

Business Continuity Management

Business Continuity Management (BCM) bezeichnet alle organisatorischen, technischen und personellen Maßnahmen, die zur Fortführung des Kerngeschäfts einer Behörde oder eines Unternehmens nach Eintritt eines Notfalls bzw. eines Sicherheitsvorfalls dienen. Weiterhin unterstützt BCM die sukzessive Fortführung der Geschäftsprozesse bei länger anhaltenden Ausfällen oder Störungen.

Cyber-Sicherheit

Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Häufig wird bei der Betrachtung von Cyber-Sicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt.

Datenschutz

Datenschutz soll einzelne Personen davor schützen, dass diese durch den Umgang mit ihren personenbezogenen Daten in ihren Persönlichkeitsrechten beeinträchtigt werden. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).

Für den Begriff „Datenschutz" existieren zwei englische Übersetzungen: Dabei bezeichnet „Data Protection" den Datenschutz als Rechtsbegriff. „Privacy" zielt dagegen auf die gesellschaftliche Lebensweise ab (Schutz der Privatsphäre) und wird überwiegend im amerikanischen Sprachumfeld und mittlerweile auch im EU-Raum vermehrt genutzt.

Datenschutz-Management

Mit Datenschutz-Management werden die Prozesse bezeichnet, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen.

Datensicherheit

Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein modernerer Begriff dafür ist „Informationssicherheit".

Fachaufgabe

Fachaufgaben sind Aufgaben, die aus der Zweckbestimmung einer Institution bzw. deren Auftrag folgen. Als Fachaufgaben werden im IT-Grundschutz Geschäftsprozesse in Behörden bezeichnet.

Gefahr

„Gefahr" wird oft als übergeordneter Begriff gesehen, wohingegen unter „Gefährdung" eine genauer beschriebene Gefahr (räumlich und zeitlich nach Art, Größe und Richtung bestimmt) verstanden wird. Die Gefahr ist beispielsweise ein Datenverlust. Datenverlust kann unter anderem durch eine defekte Festplatte oder Personen entstehen, der die Festplatte stehlen. Die Gefährdungen sind dann „defekter Datenträger" und „Diebstahl von Datenträgern". Diese Unterscheidung wird aber in der Literatur nicht durchgängig gemacht und ist eher von akademischer Bedeutung, so dass es sinnvoll ist, „Gefahr" und „Gefährdung" als gleichbedeutend aufzufassen.

Gefährdung (englisch „applied threat")

Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.

Sind beispielsweise Schadprogramme eine Bedrohung oder eine Gefährdung für Personen, die im Internet surfen? Nach der oben gegebenen Definition lässt sich feststellen, dass alle Anwendenden prinzipiell durch Schadprogramme im Internet bedroht sind. Die Person, die eine mit Schadprogrammen infizierte Datei herunterlädt, wird von dem Schadprogramm gefährdet, wenn das IT-System anfällig für diesen Typ des Schadprogramms ist. Für Anwendende mit einem wirksamen Virenschutz, einer Konfiguration, die das Funktionieren des Schadprogramms verhindert, oder einem Betriebssystem, das den Code des Schadprogramms nicht ausführen kann, bedeutet das geladene Schadprogramm hingegen keine Gefährdung.

Geschäftsprozess

Ein Geschäftsprozess ist eine Menge logisch verknüpfter Einzeltätigkeiten (Aufgaben, Arbeitsabläufe), die ausgeführt werden, um ein bestimmtes geschäftliches oder betriebliches Ziel zu erreichen.

Grundwerte der Informationssicherheit

Der IT-Grundschutz betrachtet die drei Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität.

Jedem Anwendenden des IT-Grundschutzes steht es natürlich frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies in seinem oder ihrem individuellen Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der Informationssicherheit sind zum Beispiel Authentizität, Verbindlichkeit, Zuverlässigkeit und Nichtabstreitbarkeit.

Industrial Control System (ICS)

ICS ist ein Oberbegriff für Automatisierungslösungen zur Steuerung technischer Prozesse.

Ein industrielles Steuerungssystem (Industrial Control System, ICS, IACS) ist eine integrierte Hard- und Software-Lösung zur Automatisierung, dazu gehören Sensoren, Aktoren und deren Vernetzung, sowie Verfahren zur Auswertung und Steuerung von vorwiegend industriellen Prozessen. Durch kontinuierliches Messen und Steuern werden Abläufe für den Betrieb von Maschinen automatisiert.

Informationssicherheit

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in IT-Systemen oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwendende ziehen in ihre Betrachtungen weitere Grundwerte mit ein.

Informationssicherheitsbeauftragte (ISB)

Der oder die Informationssicherheitsbeauftragte (kurz ISB oder seltener IS-Beauftragte) ist für die operative Erfüllung der Aufgabe „Informationssicherheit" zuständig. Andere Bezeichnungen sind CISO (Chief Information Security Officer) oder Informationssicherheitsmanager oder -managerin (ISM). Die Rolle des oder der ISB sollte von einer Person mit eigener Fachkompetenz zur Informationssicherheit in einer Stabsstelle eines Unternehmens oder einer Behörde wahrgenommen werden.

Informationssicherheitsmanagement (IS-Management)

Die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informations-

sicherheitsmanagement bezeichnet. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

Informationssicherheitsmanagement-Team (IS-Management-Team)

In größeren Institutionen ist es sinnvoll, ein IS-Management-Team (häufig auch IT-Sicherheitsmanagement-Team) aufzubauen, das den oder die ISB unterstützt, beispielsweise indem es übergreifende Maßnahmen in der Gesamtorganisation koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt.

Informationssicherheitsrevision (IS-Revision)

Informationssicherheitsrevision (IS-Revision) ist ein Bestandteil eines jeden erfolgreichen Informationssicherheitsmanagements. Nur durch die regelmäßige Überprüfung der etablierten Sicherheitsmaßnahmen und des Informationssicherheits-Prozesses können Aussagen über deren wirksame Umsetzung, Aktualität, Vollständigkeit und Angemessenheit und damit über den aktuellen Zustand der Informationssicherheit getroffen werden. Die IS-Revision ist somit ein Werkzeug zum Feststellen, Erreichen und Aufrechterhalten eines angemessenen Sicherheitsniveaus in einer Institution.

Informationsverbund

Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

Infrastruktur

Beim IT-Grundschutz werden unter Infrastruktur die für die Informationsverarbeitung und die IT genutzten Gebäude, Räume, Energieversorgung, Klimatisierung und die Verkabelung verstanden. Die IT-Systeme und Netzkoppelelemente gehören nicht dazu.

Institution

Mit dem Begriff Institution werden im IT-Grundschutz Unternehmen, Behörden und sonstige öffentliche oder private Organisationen bezeichnet.

Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf „Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf „Informationen" angewendet. Der Begriff „Information" wird dabei für „Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autorenschaft oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zur verfassenden Person verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

IT-Grundschutz-Check

Der Begriff bezeichnet im IT-Grundschutz die Überprüfung, ob die nach IT-Grundschutz empfohlenen Anforderungen in einer Institution bereits erfüllt sind und welche grundlegenden Sicherheitsanforderungen noch fehlen (früher: Basis-Sicherheitscheck).

IT-Grundschutz-Kompendium

Die Bausteine des IT-Grundschutzes sind im IT-Grundschutz-Kompendium zusammengefasst. Es stellt den Nachfolger der bis zur 15. Ergänzungslieferung verfügbaren IT-Grundschutz-Kataloge dar.

IT-System

IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls.

Kern-Absicherung

Im Fokus der Kern-Absicherung stehen zunächst die besonders gefährdeten Geschäftsprozesse und Assets.

Komponenten

Eine Komponente ist in der Softwarearchitektur eine eigenständig einsetzbare Einheit mit Schnittstellen nach außen, die mit anderen Komponenten verbunden werden kann. Sie ist sowohl fachlich als auch technisch unabhängig und besitzt eine gewisse Größe (im Sinne eines wirtschaftlichen Wertes).

Als Komponenten werden im IT-Grundschutz technische Zielobjekte (siehe dort) oder Teile von Zielobjekten bezeichnet.

Kronjuwelen

Als Kronjuwelen werden solche Assets bezeichnet, deren Diebstahl, Zerstörung oder Kompromittierung einen existenzbedrohenden Schaden für die Institution bedeuten würde.

Kumulationseffekt

Der Kumulationseffekt beschreibt, dass sich der Schutzbedarf eines IT-Systems erhöhen kann, wenn durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann. Ein Auslöser kann auch sein, dass mehrere IT-Anwendungen bzw. eine Vielzahl sensitiver Informationen auf einem IT-System verarbeitet werden, so dass durch Kumulation von Schäden der Gesamtschaden höher sein kann.

Leitlinie zur Informationssicherheit

Die Leitlinie ist ein zentrales Dokument für die Informationssicherheit einer Institution. In ihr wird beschrieben, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll. Sie beinhaltet die von der Institution angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Sicherheitsleitlinie beschreibt damit auch über die Sicherheitsziele das angestrebte Sicherheitsniveau in einer Behörde oder einem Unternehmen.

Maximumprinzip

Nach dem Maximumprinzip bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines Geschäftsprozesses, einer Anwendung bzw. eines IT-Systems.

Modellierung

Bei den Vorgehensweisen nach IT-Grundschutz wird bei der Modellierung der betrachtete Informationsverbund eines Unternehmens oder einer Behörde mit Hilfe der Bausteine aus dem IT-Grundschutz-Kompendium nachgebildet. Hierzu enthalten die Bausteine des IT-Grundschutz-Kompendiums im Kapitel „Abgrenzung und Modellierung" einen Hinweis, auf welche Zielobjekte er anzuwenden ist und welche Voraussetzungen dabei gegebenenfalls zu beachten sind.

Netzplan

Ein Netzplan ist eine graphische Übersicht über die Komponenten eines Netzes und ihrer Verbindungen.

Nichtabstreitbarkeit (englisch „non repudiation")

Hierbei liegt der Schwerpunkt auf der Nachweisbarkeit gegenüber Dritten. Ziel ist es zu gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es wird unterschieden zwischen

- Nichtabstreitbarkeit der Herkunft: Es soll einer absendenden Stelle (Person oder IT-System) einer Nachricht unmöglich sein, das Absenden einer bestimmten Nachricht nachträglich zu bestreiten.
- Nichtabstreitbarkeit des Erhalts: Es soll einer empfangenden Stelle (Person oder IT-System) einer Nachricht unmöglich sein, den Erhalt einer gesendeten Nachricht nachträglich zu bestreiten.

Risiko

Risiko wird häufig definiert als die Kombination (also dem Produkt) aus der Häufigkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Der Schaden wird häufig als Differenz zwischen einem geplanten und ungeplanten Ergebnis dargestellt. Risiko ist eine spezielle Form der Unsicherheit oder besser Unwägbarkeit.

In der ISO wird Risiko auch als das Ergebnis von Unwägbarkeiten auf Zielobjekte definiert. In diesem Sinne wird daher auch von Konsequenzen statt von Schaden gesprochen, wenn Ereignisse anders eintreten als erwartet. Hierbei kann eine Konsequenz negativ (Schaden) oder positiv (Chance) sein. Die obige Definition hat sich allerdings als gängiger in der Praxis durchgesetzt.

Im Unterschied zu „Gefährdung" umfasst der Begriff „Risiko" bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.

Risikoanalyse

Als Risikoanalyse wird der komplette Prozess bezeichnet, um Risiken zu beurteilen (identifizieren, einschätzen und bewerten) sowie zu behandeln. Risikoanalyse bezeichnet nach den einschlägigen ISO-Normen ISO 31000 und ISO 27005 nur einen Schritt im Rahmen der Risikobeurteilung, die aus den folgenden Schritten besteht:

- Identifikation von Risiken (Risk Identification)
- Analyse von Risiken (Risk Analysis)
- Evaluation oder Bewertung von Risiken (Risk Evaluation)

Im deutschen Sprachgebrauch hat sich allerdings der Begriff Risikoanalyse für den kompletten Prozess der Risikobeurteilung und Risikobehandlung etabliert. Daher wird auch in den Dokumenten zum IT-Grundschutz weiter der Begriff Risikoanalyse für den umfassenden Prozess benutzt.

Risikoappetit (auch Risikoneigung oder Risikobereitschaft)

Risikoappetit bezeichnet die durch kulturelle, interne, externe oder wirtschaftliche Einflüsse entstandene Neigung einer Institution, wie sie Risiken bewertet und mit ihnen umgeht.

Risikobehandlungsplan

Die vollständige Erfüllung der im IT-Grundschutz geforderten Basis- und Standard-Anforderungen und gegebenenfalls die Anforderungen bei erhöhtem Schutzbedarf ist ein hoher Anspruch an jede Institution. In der Praxis lassen sich nicht alle Anforderungen erfüllen, sei es, dass Umstände vorliegen, die eine Erfüllung nicht sinnvoll erscheinen lassen (Neubeschaffung von Informationstechnik, Umzugspläne oder Ähnliches) oder dass eine Anforderung aus organisatorischen oder technischen Rahmenbedingungen nicht möglich ist (IT-System oder Anwendung werden nicht eingesetzt oder Ähnliches). Bestehende Defizite bei der Umsetzung von Sicherheitsmaßnahmen, die aus den Sicherheitsanforderungen resultieren und die damit verbundenen Risiken müssen in Form eines Managementberichtes dokumentiert werden, einschließlich einer Umsetzungsplanung für die weitere Behandlung der bestehenden Risiken. Der Risikobehandlungsplan sollte eine Beschreibung der geplanten Ressourcen und zeitliche Vorgaben enthalten. Er wird durch Unterschrift der Institutionsleitung genehmigt.

Die einzelnen Anforderungen aus dem Risikobehandlungsplan sollten mindestens einmal pro Jahr überprüft werden. Eine dauerhafte und unbefristete Übernahme von Risiken durch die Institutionsleitung muss vermieden werden, da sich im Bereich der Informationssicherheit die Risiken in kurzer Zeit verändern können. Eine unbefristete Übernahme von Risiken birgt die Gefahr, dass diese Risiken nur zu einem Stichtag geprüft und bewertet werden und eine erneute Betrachtung ausgeschlossen bleibt.

Risikomanagement

Als Risikomanagement werden alle Aktivitäten mit Bezug auf die strategische und operative Behandlung von Risiken bezeichnet, also alle Tätigkeiten, um Risiken für eine Institution zu identifizieren, zu steuern und zu kontrollieren.

Das strategische Risikomanagement beschreibt die wesentlichen Rahmenbedingungen, wie die Behandlung von Risiken innerhalb einer Institution, die Kultur zum Umgang mit Risiken und die Methodik ausgestaltet sind. Diese Grundsätze für die Behandlung von Risiken innerhalb eines ISMS müssen mit den Rahmenbedingungen des organisationsweiten Risikomanagements übereinstimmen bzw. aufeinander abgestimmt sein.

Die Rahmenbedingungen des operativen Risikomanagements umfassen den Regelprozess aus

- Identifikation von Risiken,
- Einschätzung und Bewertung von Risiken,
- Behandlung von Risiken,

- Überwachung von Risiken und
- Risikokommunikation.

Schaden / Konsequenz

Eine Abweichung von einem erwarteten Ergebnis führt zu einer Konsequenz (häufig „Schaden" genannt). Hierbei kann es sich grundsätzlich um eine positive oder negative Abweichung handeln.

Eine positive Konsequenz beziehungsweise positiver Schaden im Sinne der Chancen- und Risikoanalyse wird auch als Chance bezeichnet. Meistens werden in der Risikoanalyse jedoch die negativen Konsequenzen, also die Schäden, betrachtet.

Das Ausmaß eines Schadens wird als Schadenshöhe definiert und kann als bezifferbar oder nicht direkt bezifferbar betitelt werden. Die bezifferbaren Schäden können in der Regel mit direkten Aufwänden (z. B. finanzieller Art) dargestellt werden. Zu den nicht direkt bezifferbaren Schäden gehören z. B. Imageschäden oder Opportunitätskosten. Bei diesen lässt sich die tatsächliche Schadenshöhe häufig nur vermuten oder schätzen. Alle Angaben werden in der Regel aufgrund von Erfahrungs- oder Branchenwerten in Kategorien klassifiziert.

Schutzbedarf

Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

Schutzbedarfsfeststellung

Bei der Schutzbedarfsfeststellung wird der Schutzbedarf der Geschäftsprozesse, der verarbeiteten Informationen, der IT-Systeme, Räume und Kommunikationsverbindungen bestimmt. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung der Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität oder Verfügbarkeit) entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien „normal", „hoch" und „sehr hoch".

Schwachstelle (englisch „vulnerability")

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

Sicherheitsanforderung

Als Sicherheitsanforderung werden Anforderungen für den organisatorischen, personellen, infrastrukturellen und technischen Bereich bezeichnet, deren Erfüllung zur Erhöhung der Informationssicherheit notwendig ist bzw. dazu beiträgt. Eine Sicherheitsanforderung beschreibt also, was getan werden muss, um ein bestimmtes Niveau bezüglich der Informationssicherheit zu erreichen. Wie die Anforderungen im konkreten Fall erfüllt werden können, ist in entsprechenden Sicherheitsmaßnahmen beschrieben (siehe dort). Im englischen Sprachraum wird für Sicherheitsanforderungen häufig der Begriff „control" verwendet.

Der IT-Grundschutz unterscheidet zwischen Basis-Anforderungen, Standard-Anforderungen und Anforderungen bei erhöhtem Schutzbedarf. Basis-Anforderungen sind fundamental und vorrangig umzusetzen, sofern nicht gravierende Gründe dagegen sprechen. Standard-Anforderungen sind für den normalen Schutzbedarf grundsätzlich umzusetzen, sofern sie nicht durch mindestens gleichwertige Alternativen oder die bewusste Akzeptanz des Restrisikos ersetzt werden. Anforderungen bei erhöhtem Schutzbedarf sind exemplarische Vorschläge, was bei entsprechendem Schutzbedarf zur Absicherung sinnvoll umzusetzen ist.

Sicherheitskonzept

Ein Sicherheitskonzept dient zur Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Sicherheitsmaßnahme muss sich letztlich darauf zurückführen lassen.

Sicherheitskonzeption

Die Sicherheitskonzeption ist eine der zentralen Aufgaben des Informationssicherheitsmanagements. Aufbauend auf den Ergebnissen von Strukturanalyse und Schutzbedarfsfeststellung werden hier die erforderlichen Sicherheitsmaßnahmen identifiziert und im Sicherheitskonzept dokumentiert.

Sicherheitsmaßnahme

Mit Sicherheitsmaßnahme (kurz Maßnahme) werden alle Aktionen bezeichnet, die dazu dienen, um Sicherheitsrisiken zu steuern und um diesen entgegenzuwirken. Dies schließt sowohl organisatorische, als auch personelle, technische oder infrastrukturelle Sicherheitsmaßnahmen ein. Sicherheitsmaßnahmen dienen zur Erfüllung von Sicherheitsanforderungen (siehe dort). Als englische Übersetzung wurde „safeguard", „security measure" oder „measure" gewählt.

Sicherheitsrichtlinie (englisch „Security Policy")

In einer Sicherheitsrichtlinie werden Schutzziele und allgemeine Sicherheitsanforderungen im Sinne offizieller Vorgaben eines Unternehmens oder einer Behörde formuliert. Detaillierte Sicherheitsmaßnahmen sind in einem umfangreicheren Sicherheitskonzept enthalten.

Standard-Absicherung

Die Standard-Absicherung entspricht im Wesentlichen der klassischen IT-Grundschutz-Vorgehensweise des BSI-Standards 100-2. Mit der Standard-Absicherung kann der oder die ISB die Assets und Prozesse einer Institution sowohl umfassend als auch in der Tiefe absichern.

Standard-Anforderung

Siehe Sicherheitsanforderung.

Starke Authentisierung

Starke Authentisierung bezeichnet die Kombination von zwei oder mehr Authentisierungstechniken, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte. Daher wird dies auch häufig als Zwei- oder Mehr-Faktor-Authentisierung bezeichnet.

Strukturanalyse

In einer Strukturanalyse werden die erforderlichen Informationen über den ausgewählten Informationsverbund, die Geschäftsprozesse, Anwendungen, IT-Systeme, Netze, Räume, Gebäude und Verbindungen erfasst und so aufbereitet, dass sie die weiteren Schritte gemäß IT-Grundschutz unterstützen.

Verbindlichkeit

Unter Verbindlichkeit werden die Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendenden stets wie vorgesehen genutzt werden können.

Verteilungseffekt

Der Verteilungseffekt kann sich auf den Schutzbedarf relativierend auswirken, wenn zwar eine Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der Anwendung ausgeführt werden.

Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Wert (englisch „asset“)

Werte sind alles, was wichtig für eine Institution ist (Vermögen, Wissen, Gegenstände, Gesundheit).

Zertifikat

Der Begriff Zertifikat wird in der Informationssicherheit in verschiedenen Bereichen mit unterschiedlichen Bedeutungen verwendet. Zu unterscheiden sind vor allem:

- ISO 27001-Zertifikate: Der ISO-Standard 27001 „Information technology – Security techniques – Information security management systems requirements specification“ ermöglicht eine Zertifizierung des Informationssicherheitsmanagements.
- ISO 27001-Zertifikate auf der Basis von IT-Grundschutz: Damit kann dokumentiert werden, dass für den betrachteten Informationsverbund alle relevanten Sicherheitsanforderungen gemäß IT-Grundschutz realisiert wurden. Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist eine Überprüfung durch einen vom BSI zertifizierten ISO 27001-IT-Grundschutz-Auditor. Zu den Aufgaben eines ISO 27001-IT-Grundschutz-Auditors gehören eine Sichtung der von der Institution erstellten Referenzdokumente, die Durchführung einer Vor-Ort-Prüfung und die Erstellung eines Audit-Reports. Die Zertifizierungsstelle BSI stellt aufgrund des Audit-Reports fest, ob die notwendigen Sicherheitsanforderungen umgesetzt sind, erteilt im positiven Falle ein Zertifikat und veröffentlicht es auf Wunsch des Antragstellers.
- Schlüsselzertifikat: Ein Schlüsselzertifikat ist eine elektronische Bescheinigung, mit der Signaturprüfschlüssel einer Person zugeordnet werden. Bei digitalen Signaturen wird ein Zertifikat als Bestätigung einer vertrauenswürdigen dritten Partei benötigt, um nachzuweisen, dass die zur Erzeugung der Digitalen Signatur eingesetzten kryptographischen Schlüssel wirklich zu dem Unterzeichnenden gehören.
- Zertifikate für IT-Produktsicherheit: Zertifiziert wird nach international anerkannten Sicherheitskriterien, wie z. B. den Common Criteria (ISO/IEC 15408). Auf dieser Basis können Produkte unterschiedlichster Art evaluiert werden. Eine wesentliche Voraussetzung ist jedoch, dass die am Ende des Verfahrens im Zertifikat zu bestätigenden Sicherheitseigenschaften im Zusammenhang mit der Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität stehen.

Ein digitales Zertifikat ist ein Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Ein digitales Zertifikat ermöglicht unter anderem die Verwendung elektronischer Signaturen.

Zielobjekt

Zielobjekte sind Teile des Informationsverbunds, denen im Rahmen der Modellierung ein oder mehrere Bausteine aus dem IT-Grundschutz-Kompendium zugeordnet werden können. Zielobjekte können dabei physische Objekte sein, z. B. IT-Systeme. Häufig sind Zielobjekte jedoch logische Objekte, wie beispielsweise Organisationseinheiten, Anwendungen oder der gesamte Informationsverbund.

Zugang

Mit Zugang wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet. Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen wie IT-Systeme oder System-Komponenten und Netze zu nutzen.

Zugriff

Mit Zugriff wird die Nutzung von Informationen oder Daten bezeichnet. Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen, zu nutzen oder Transaktionen auszuführen.

Zutritt

Mit Zutritt wird das Betreten von abgegrenzten Bereichen wie z. B. Räumen oder geschützten Arealen in einem Gelände bezeichnet. Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, also beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes.

Elementare Gefährdungen

G 0.1 Feuer

Feuer können schwere Schäden an Menschen, Gebäuden und deren Einrichtung verursachen. Neben direkten durch Feuer verursachten Schäden lassen sich Folgeschäden aufzeigen, die insbesondere für die Informationstechnik in ihrer Schadenswirkung ein katastrophales Ausmaß erreichen können. Löschwasserschäden treten beispielsweise nicht nur an der Brandstelle auf. Sie können auch in tiefer liegenden Gebäudeteilen entstehen. Bei der Verbrennung von PVC entstehen Chlorgase, die zusammen mit der Luftfeuchtigkeit und dem Löschwasser Salzsäure bilden. Werden die Salzsäuredämpfe über die Klimaanlage verteilt, können auf diese Weise Schäden an empfindlichen elektronischen Geräten entstehen, die in einem vom Brandort weit entfernten Teil des Gebäudes stehen. Aber auch „normaler" Brandrauch kann auf diesem Weg beschädigend auf die IT-Einrichtung einwirken.

Ein Brand entsteht nicht nur durch den fahrlässigen Umgang mit Feuer (z. B. durch unbeaufsichtigte offene Flammen, Schweiß- und Lötarbeiten), sondern auch durch unsachgemäße Benutzung elektrischer Einrichtungen (z. B. unbeaufsichtigte Kaffeemaschine, Überlastung von Mehrfachsteckdosen). Technische Defekte an elektrischen Geräten können ebenfalls zu einem Brand führen.

Die Ausbreitung eines Brandes kann unter anderem begünstigt werden durch:

- Aufhalten von Brandabschnittstüren durch Keile,
- unsachgemäße Lagerung brennbarer Materialien (z. B. Altpapier),
- Nichtbeachtung der einschlägigen Normen und Vorschriften zur Brandvermeidung,
- fehlende Brandmeldeeinrichtungen (z. B. Rauchmelder),
- fehlende oder nicht einsatzbereite Handfeuerlöscher oder automatische Löscheinrichtungen (z. B. Gaslöschanlagen),
- mangelhaften vorbeugenden Brandschutz (z. B. Fehlen von Brandabschottungen auf Kabeltrassen oder Verwendung ungeeigneter Dämmmaterialien zur Wärme- und Schallisolierung).

Beispiele:

- Anfang der 90er Jahre erlitt im Frankfurter Raum ein Großrechenzentrum einen katastrophalen Brandschaden, der zu einem kompletten Ausfall führte.
- Immer wieder kommt es vor, dass elektrische Kleingeräte, wie z. B. Kaffeemaschinen oder Tischleuchten, unsachgemäß installiert oder aufgestellt sind und dadurch Brände verursachen.

G 0.2 Ungünstige klimatische Bedingungen

Ungünstige klimatische Bedingungen wie Hitze, Frost oder hohe Luftfeuchtigkeit können zu Schäden verschiedenster Art führen, beispielsweise zu Fehlfunktionen in technischen Komponenten oder zur Beschädigung von Speichermedien. Häufige Schwankungen der klimatischen Bedingungen verstärken diesen Effekt. Ungünstige klimatische Bedingungen können auch dazu führen, dass Menschen nicht mehr arbeiten können oder sogar verletzt oder getötet werden.

Jeder Mensch und jedes technische Gerät hat einen Temperaturbereich, innerhalb dessen seine normale Arbeitsweise bzw. ordnungsgemäße Funktion gewährleistet ist. Überschreitet die Umgebungstemperatur die Grenzen dieses Bereiches nach oben oder unten, kann es zu Arbeitsausfällen, Betriebsstörungen oder zu Geräteausfällen kommen.

Zu Lüftungszwecken werden oft unerlaubt Fenster von Serverräumen geöffnet. In der Übergangszeit (Frühjahr, Herbst) kann das bei großen Temperaturschwankungen dazu führen, dass durch starke Abkühlung die zulässige Luftfeuchte überschritten wird.

Beispiele:

- Bei hochsommerlichen Temperaturen und unzureichender Kühlung kann es bei IT-Geräten zu temperaturbedingten Ausfällen kommen.
- Zu viel Staub in IT-Systemen kann zu einem Hitzestau führen.
- Durch zu hohe Temperaturen können magnetische Datenträger entmagnetisiert werden.

G 0.3 Wasser

Durch Wasser kann die Integrität und Verfügbarkeit von Informationen beeinträchtigt werden, die auf analogen und digitalen Datenträgern gespeichert sind. Auch Informationen im Arbeitsspeicher von IT-Systemen sind gefährdet. Der unkontrollierte Eintritt von Wasser in Gebäude oder Räume kann beispielsweise bedingt sein durch:

- Störungen in der Wasser-Versorgung oder Abwasser-Entsorgung,
- Defekte der Heizungsanlage,
- Defekte an Klimaanlagen mit Wasseranschluss,
- Defekte in Sprinkleranlagen,
- Löschwasser bei der Brandbekämpfung und
- Wassersabotage z. B. durch Öffnen der Wasserhähne und Verstopfen der Abflüsse.

Unabhängig davon, auf welche Weise Wasser in Gebäude oder Räume gelangt, besteht die Gefahr, dass Versorgungseinrichtungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden (Kurzschluss, mechanische Beschädigung, Rost etc.). Besonders wenn zentrale Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) in Kellerräumen ohne selbsttätige Entwässerung untergebracht sind, kann eindringendes Wasser sehr hohe Schäden verursachen.

Probleme können außerdem durch Frost entstehen. Beispielsweise können Rohre in frostgefährdeten Bereichen undicht werden, wenn darin Wasser bei anhaltendem Frost stillsteht. Auch eine vorhandene Wärmedämmung wird mit der Zeit vom Frost überwunden.

Beispiel:

- In einem Serverraum verlief eine Wasserleitung unterhalb der Decke, die mit Gipskartonelementen verkleidet war. Als eine Verbindung der Wasserleitung undicht wurde, wurde dies nicht rechtzeitig erkannt. Das austretende Wasser sammelte sich zunächst an der tiefsten Stelle der Verkleidung, bevor es dort austrat und im darunter angebrachten Stromverteiler einen Kurzschluss verursachte. Dies führte dazu, dass bis zur endgültigen Reparatur sowohl die Wasser- als auch die Stromversorgung des betroffenen Gebäudeteils komplett abgeschaltet werden musste.

G 0.4 Verschmutzung, Staub, Korrosion

Viele IT-Geräte enthalten neben der Elektronik auch mechanisch arbeitende Komponenten, wie z. B. bei Fest- und Wechselplatten, DVD-Laufwerken, Druckern, Scannern etc., aber auch Lüftern von Prozessoren und Netzteilen. Mit steigenden Anforderungen an die Qualität und die Schnelligkeit müssen diese Geräte immer präziser arbeiten. Bereits geringfügige Verunreinigungen können zu einer Störung eines Gerätes führen. Staub und Verschmutzungen können beispielsweise durch folgende Tätigkeiten in größerem Maße entstehen:

- Arbeiten an Wänden, Doppelböden oder anderen Gebäudeteilen,
- Umrüstungsarbeiten an der Hardware bzw.
- Entpackungsaktionen von Geräten (z. B. aufwirbelndes Styropor).

Vorhandene Sicherheitsschaltungen in den Geräten führen meist zu einem rechtzeitigen Abschalten. Das hält zwar den direkten Schaden am Gerät, die Instandsetzungskosten und die Ausfallzeiten klein, führt aber dazu, dass das betroffene Gerät nicht verfügbar ist.

Die Geräte und die Infrastruktur können außerdem durch Korrosion angegriffen werden. Dies kann sich nicht nur auf die IT, sondern sogar auf die Sicherheit von Gebäuden negativ auswirken.

Durch Korrosion können auch indirekt weitere Gefährdungen entstehen. So kann beispielsweise Wasser aus korrodierten Stellen austreten (siehe G 0.3 Wasser).

Insgesamt können Verschmutzung, Staub oder Korrosion somit zu Ausfällen oder Beschädigungen von IT-Komponenten und Versorgungseinrichtungen führen. Als Folge kann die ordnungsgemäße Informationsverarbeitung beeinträchtigt werden.

Beispiele:

- Bei der Aufstellung eines Servers in einem Medienraum, zusammen mit einem Kopierer und einem Faxgerät, traten nacheinander die Lähmung des Prozessor-Lüfters und des Netzteil-Lüfters aufgrund der hohen Staubbelastung des Raumes auf. Der Ausfall des Prozessor-Lüfters führte zu sporadischen Server-Abstürzen. Der Ausfall des Netzteil-Lüfters führte schließlich zu einer Überhitzung des Netzteils mit der Folge eines Kurzschlusses, was schließlich einen Totalausfall des Servers nach sich zog.
- Um eine Wandtafel in einem Büro aufzuhängen, wurden von der Haustechnik Löcher in die Wand gebohrt. Die Mitarbeitenden hatten hierzu ihr Büro für kurze Zeit verlassen. Nach Rückkehr an den Arbeitsplatz funktionierte ein PC nicht mehr. Ursache hierfür war Bohrstaub, der durch die Lüftungsschlitze in das PC-Netzteil eingedrungen war.

G 0.5 Naturkatastrophen

Unter Naturkatastrophen werden natürliche Veränderungen verstanden, die verheerende Auswirkungen auf Menschen und Infrastrukturen haben. Ursachen für eine Naturkatastrophe können seismische, klimatische oder vulkanische Phänomene sein, wie beispielsweise Erdbeben, Hochwasser, Erdrutsche, Tsunamis, Lawinen und Vulkanausbrüche. Beispiele für extreme meteorologische Phänomene sind Unwetter, Orkane oder Zyklone. Je nach Standort der Institution ist diese den Risiken durch die verschiedenen Arten von Naturkatastrophen unterschiedlich stark ausgesetzt.

Beispiele:

- Für Rechenzentren in Hochwasser-gefährdeten Gebieten besteht oft in besonderem Maße die Gefahr, dass unkontrolliert Wasser in das Gebäude eindringt (Überschwemmungen oder Anstieg des Grundwasserspiegels).
- Die Häufigkeit von Erdbeben und somit auch das damit verbundene Risiko hängen stark von der geografischen Lage ab.

Unabhängig von der Art der Naturkatastrophe besteht auch in nicht unmittelbar betroffenen Gebieten die Gefahr, dass Versorgungseinrichtungen, Kommunikationsverbindungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden. Besonders der Ausfall zentraler Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) kann sehr hohe Schäden nach sich ziehen. Betriebs- und Service-Personal kann aufgrund von großflächig eingerichteten Sperrbereichen der Zutritt zur Infrastruktur verwehrt werden.

Beispiele:

- Viele Gewerbebetriebe, auch große Unternehmen, tragen der Hochwassergefährdung nicht hinreichend Rechnung. So wurde ein Unternehmen bereits mehrere Male durch Hochwasserschäden am Rechenzentrum „überrascht". Das Rechenzentrum schwamm im wahrsten Sinne des Wortes innerhalb von 14 Monaten zum zweiten Mal davon. Der entstandene Schaden belief sich auf mehrere hunderttausend Euro und ist von keiner Versicherung gedeckt.
- Ein IT-System wird an einem Standort untergebracht, dessen geografische Lage für vulkanische Aktivität bekannt ist (zeitweilig aussetzendes Phänomen, bei dem die Emissionsphasen mit zum Teil langen Ruhephasen abwechseln).

G 0.6 Katastrophen im Umfeld

Eine Behörde bzw. ein Unternehmen kann Schaden nehmen, wenn sich im Umfeld ein schwerer Unglücksfall ereignet, zum Beispiel ein Brand, eine Explosion, die Freisetzung giftiger Substanzen oder das Austreten gefährlicher Strahlung. Gefahr besteht dabei nicht nur durch das Ereignis selbst, sondern auch durch die häufig daraus resultierenden Aktivitäten, beispielsweise Sperrungen oder Rettungsmaßnahmen.

Die Liegenschaften einer Institution können verschiedenen Gefährdungen aus dem Umfeld ausgesetzt sein, unter anderem durch Verkehr (Straßen, Schiene, Luft, Wasser), Nachbarbetriebe oder Wohngebiete.

Vorbeugungs- oder Rettungsmaßnahmen können die Liegenschaften dabei direkt betreffen. Solche Maßnahmen können auch dazu führen, dass Mitarbeitende ihre Arbeitsplätze nicht erreichen können oder Personal evakuiert werden muss. Durch die Komplexität der Haustechnik und der IT-Einrichtungen kann es aber auch zu indirekten Problemen kommen.

Beispiel:

- Bei einem Brand in einem chemischen Betrieb in unmittelbarer Nähe eines Rechenzentrums (ca. 1000 m Luftlinie) entstand eine mächtige Rauchwolke. Das Rechenzentrum besaß eine Klima- und Lüftungsanlage, die über keine Außenluftüberwachung verfügte. Nur durch die Aufmerksamkeit eines Mitarbeitenden (der Unfall geschah während der Arbeitszeit), der die Entstehung und Ausbreitung verfolgte, konnte die Außenluftzufuhr rechtzeitig manuell abgeschaltet werden.

G 0.7 Großereignisse im Umfeld

Großveranstaltungen aller Art können zu Behinderungen des ordnungsgemäßen Betriebs einer Behörde bzw. eines Unternehmens führen. Hierzu gehören unter anderem Straßenfeste, Konzerte, Sportveranstaltungen, Arbeitskämpfe oder Demonstrationen. Ausschreitungen im Zusammenhang mit solchen Veranstaltungen können zusätzliche Auswirkungen, wie die Einschüchterung von Mitarbeitenden bis hin zur Gewaltanwendung gegen das Personal oder das Gebäude, nach sich ziehen.

Beispiele:

- Während der heißen Sommermonate fand eine Demonstration in der Nähe eines Rechenzentrums statt. Die Situation eskalierte und es kam zu Gewalttätigkeiten. In einer Nebenstraße stand noch ein Fenster des Rechenzentrumsbereiches auf, durch das ein Demonstrant eindrang und die Gelegenheit nutzte, Hardware mit wichtigen Daten zu entwenden.
- Beim Aufbau einer Großkirmes wurde aus Versehen eine Stromleitung gekappt. Dies führte in einem hierdurch versorgten Rechenzentrum zu einem Ausfall, der jedoch durch die vorhandene Netzersatzanlage abgefangen werden konnte.

G 0.8 Ausfall oder Störung der Stromversorgung

Trotz hoher Versorgungssicherheit kommt es immer wieder zu Unterbrechungen der Stromversorgung seitens der Verteilungsnetzbetreiber (VNB) bzw. Energieversorgungsunternehmen (EVU). Die größte Zahl dieser Störungen ist mit Zeiten unter einer Sekunde so kurz, dass der Mensch sie nicht bemerkt. Aber schon Unterbrechungen von mehr als 10 ms sind geeignet, den IT-Betrieb zu stören. Neben Störungen im Versorgungsnetz können jedoch auch Abschaltungen bei nicht angekündigten Arbeiten oder Kabelbeschädigungen bei Tiefbauarbeiten dazu führen, dass die Stromversorgung ausfällt.

Von der Stromversorgung sind nicht nur die offensichtlichen, direkten Stromverbraucher (PC, Beleuchtung usw.) abhängig. Viele Infrastruktur-Einrichtungen sind heute vom Strom abhängig, z. B. Aufzüge, Klimatechnik, Gefahrenmeldeanlagen, Sicherheitsschleusen, automatische Türschließanlagen und Sprinkleranlagen. Selbst die Wasserversorgung in Hochhäusern ist wegen der zur Druck-Erzeugung in den oberen Etagen erforderlichen Pumpen stromabhängig. Bei längeren Stromausfällen kann der Ausfall der Infrastruktur-Einrichtungen dazu führen, dass keinerlei Tätigkeiten mehr in den betroffenen Räumlichkeiten durchgeführt werden können.

Neben Ausfällen können auch andere Störungen der Stromversorgung den Betrieb beeinträchtigen. Überspannung kann beispielsweise zu Fehlfunktionen oder sogar zu Beschädigungen von elektrischen Geräten führen.

Zu beachten ist außerdem, dass durch Ausfälle oder Störungen der Stromversorgung in der Nachbarschaft unter Umständen auch die eigenen Geschäftsprozesse betroffen sein können, beispielsweise wenn Zufahrtswege blockiert werden.

Beispiele:

- Durch einen Fehler in der USV eines Rechenzentrums schaltete diese nach einem kurzen Stromausfall nicht auf Normalbetrieb zurück. Nach Entladung der Batterien (nach etwa 40 Minuten) fielen alle Rechner im betroffenen Server-Saal aus.
- Anfang 2001 gab es über 40 Tage einen Strom-Notstand in Kalifornien. Die Stromversorgungslage war dort so angespannt, dass die Kalifornische Netzüberwachungsbehörde rotierende Stromabschaltungen anordnete. Von diesen Stromabschaltungen, die bis zu 90 Minuten andauerten, waren nicht nur Haushalte, sondern auch die High-Tech-Industrie betroffen. Weil mit dem Stromausfall auch Alarmanlagen und Überwachungskameras ausgeschaltet wurden, hielten die energieversorgenden Unternehmen ihre Abschaltpläne geheim.
- Im November 2005 waren nach heftigen Schneefällen in Niedersachsen und Nordrhein-Westfalen viele Gemeinden tagelang ohne Stromversorgung, weil viele Hochspannungsmasten unter der Schnee- und Eislast umgestürzt waren. Die Wiederherstellung der Stromversorgung dauerte einige Tage.

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

Für viele Geschäftsprozesse werden heutzutage zumindest zeitweise intakte Kommunikationsverbindungen benötigt, sei es über Telefon, Fax, E-Mail oder andere Dienste über Nah- oder Weitverkehrsnetze. Fallen einige oder mehrere dieser Kommunikationsverbindungen über einen längeren Zeitraum aus, kann dies beispielsweise dazu führen, dass

- Geschäftsprozesse nicht mehr weiterbearbeitet werden können, weil benötigte Informationen nicht abgerufen werden können,
- die Kundschaft die Institution nicht mehr für Rückfragen erreichen kann,
- Aufträge nicht abgegeben oder beendet werden können.

Werden auf IT-Systemen, die über Weitverkehrsnetze verbunden sind, zeitkritische Anwendungen betrieben, sind die durch einen Netzausfall möglichen Schäden und Folgeschäden entsprechend hoch, wenn keine Ausweichmöglichkeiten (z. B. Anbindung an ein zweites Kommunikationsnetz) vorhanden sind.

Zu ähnlichen Problemen kann es kommen, wenn die benötigten Kommunikationsnetze gestört sind, ohne jedoch vollständig auszufallen. Kommunikationsverbindungen können beispielsweise eine erhöhte Fehlerrate oder andere Qualitätsmängel aufweisen. Falsche Betriebsparameter können ebenfalls zu Beeinträchtigungen führen.

Beispiele:

- Das Internet ist heute für viele Institutionen zu einem unverzichtbaren Kommunikationsmedium geworden, unter anderem zum Abruf wichtiger Informationen, zur Außendarstellung sowie zur Kommunikation mit der Kundschaft und sonstigen Personen. Unternehmen, die sich auf Internet-basierte Dienstleistungen spezialisiert haben, sind natürlich in besonderem Maße von einer funktionierenden Internet-Anbindung abhängig.
- Im Zuge der Konvergenz der Netze werden Sprach- und Datendienste häufig über die gleichen technischen Komponenten transportiert (z. B. VoIP). Dadurch steigt jedoch die Gefahr, dass bei einer Störung der Kommunikationstechnik die Sprachdienste und die Datendienste gleichzeitig ausfallen.

G 0.10 Ausfall oder Störung von Versorgungsnetzen

Es gibt in einem Gebäude eine Vielzahl von Netzen, die der grundlegenden Ver- und Entsorgung und somit als Basis für alle Geschäftsprozesse einer Institution einschließlich der IT dienen. Beispiele für solche Versorgungsnetze sind:

- Strom,
- Telefon,
- Kühlung,
- Heizung bzw. Lüftung,
- Wasser und Abwasser,
- Löschwasserspeisungen,
- Gas,
- Melde- und Steueranlagen (z. B. für Einbruch, Brand, Hausleittechnik) und
- Sprechanlagen.

Der Ausfall oder die Störung eines Versorgungsnetzes kann unter anderem dazu führen, dass Menschen nicht mehr im Gebäude arbeiten können oder dass der IT-Betrieb und somit die Informationsverarbeitung beeinträchtigt wird.

Die Netze sind in unterschiedlich starker Weise voneinander abhängig, so dass sich Betriebsstörungen in jedem einzelnen Netz auch auf andere auswirken können.

Beispiele:

- Ein Ausfall von Heizung oder Lüftung kann zur Folge haben, dass alle Mitarbeitenden die betroffenen Gebäude verlassen müssen. Dies kann unter Umständen hohe Schäden nach sich ziehen.
- Der Ausfall der Stromversorgung wirkt nicht nur auf die IT direkt, sondern auch auf alle anderen Netze, die mit elektrisch betriebener Steuer- und Regeltechnik ausgestattet sind. Selbst in Abwasserleitungen sind unter Umständen elektrische Hebepumpen vorhanden.
- Der Ausfall der Wasserversorgung beeinträchtigt eventuell die Funktion von Klimaanlagen.

G 0.11 Ausfall oder Störung von Dienstleistungsunternehmen

Kaum eine Institution arbeitet heute noch ohne Outsourcing-Anbietende, Dienstleistungs- oder Zulieferunternehmen. Wenn Organisationseinheiten von Dienstleistungsunternehmen abhängig sind, kann durch Ausfälle externer Dienstleistungen die Aufgabenbewältigung beeinträchtigt werden. Der teilweise oder vollständige Ausfall von Outsourcing-Dienstleistenden oder Zulieferunternehmen kann sich erheblich auf die betriebliche Kontinuität auswirken, insbesondere bei kritischen Geschäftsprozessen. Es gibt verschiedene Ursachen für solche Ausfälle, beispielsweise Insolvenz, einseitige Kündigung des Vertrags durch die Dienstleistungs- oder Zulieferunternehmen, betriebliche Probleme beispielsweise durch Naturgewalten oder Personalausfall. Probleme können auch entstehen, wenn die von den Dienstleistungsunternehmen erbrachten Leistungen nicht den Qualitätsanforderungen der Auftraggebenden entsprechen.

Zu beachten ist außerdem, dass Dienstleistungsunternehmen ebenfalls häufig auf Subunternehmen zurückgreifen, um ihre Leistungen gegenüber den Auftraggebenden zu erbringen. Störungen, Qualitätsmängel und Ausfälle seitens der Subunternehmen können dadurch indirekt zu Beeinträchtigungen bei den Auftraggebenden führen.

Auch durch Ausfälle von IT-Systemen bei den Dienstleistungsunternehmen oder der Kommunikationsanbindungen zu diesen können Geschäftsprozesse bei den Auftraggebenden beeinträchtigt werden.

Eine gegebenenfalls notwendige Rückholung ausgelagerter Prozesse kann stark erschwert sein, beispielsweise weil die ausgelagerten Verfahren nicht hinreichend dokumentiert sind oder weil die bisherigen Dienstleistungsunternehmen die Rückholung nicht unterstützen.

Beispiele:

- Ein Unternehmen hat seine Server in einem Rechenzentrum eines externen Dienstleistungsunternehmens installiert. Nach einem Brand in diesem Rechenzentrum war die Finanzabteilung des Unternehmens nicht mehr handlungsfähig. Es entstanden erhebliche finanzielle Verluste für das Unternehmen.
- Die Just-in-Time-Produktion eines Unternehmens war von der Zulieferung von Betriebsmitteln externer Dienstleistungsunternehmen abhängig. Nachdem ein LKW durch einen Defekt beim Dienstleistungsunternehmen ausfiel, verzögerte sich die Lieferung dringend benötigter Teile drastisch. Ein großer Teil der Kundschaft konnte dadurch nicht fristgerecht beliefert werden.
- Ein Bankinstitut wickelte alle Geldtransporte mit einem Werttransportunternehmen ab. Das Werttransportunternehmen meldete überraschend Konkurs an. Die Vereinbarung und Tourenplanung mit einem neuen Werttransportunternehmen dauerte mehrere Tage. Als Folge kam es zu erheblichen Problemen und Zeitverzögerungen bei der Geldversorgung und -entsorgung der Bankfilialen.

G 0.12 Elektromagnetische Störstrahlung

Informationstechnik setzt sich heute zu einem großen Teil aus elektronischen Komponenten zusammen. Zwar wird zunehmend auch optische Übertragungstechnik eingesetzt, dennoch enthalten beispielsweise Computer, Netzkoppelelemente und Speichersysteme in der Regel sehr viele elektronische Bauteile. Durch elektromagnetische Störstrahlung, die auf solche Bauteile einwirkt, können elektronische Geräte in ihrer Funktion beeinträchtigt oder sogar beschädigt werden. Als Folge kann es unter anderem zu Ausfällen, Störungen, falschen Verarbeitungsergebnissen oder Kommunikationsfehlern kommen.

Auch drahtlose Kommunikation kann durch elektromagnetische Störstrahlung beeinträchtigt werden. Hierzu reicht unter Umständen eine ausreichend starke Störung der verwendeten Frequenzbänder.

Weiterhin können Informationen, die auf bestimmten Arten von Datenträgern gespeichert sind, durch elektromagnetische Störstrahlung gelöscht oder verfälscht werden. Dies betrifft insbesondere magnetisierbare Datenträger (Festplatten, Magnetbänder etc.) und Halbleiter-Speicher. Auch eine Beschädigung solcher Datenträger durch elektromagnetische Störstrahlung ist möglich.

Es gibt viele unterschiedliche Quellen elektromagnetischer Felder oder Strahlung, zum Beispiel Funknetze wie WLAN, Bluetooth, GSM, UMTS etc., Dauermagnete und kosmische Strahlung. Außerdem strahlt jedes elektrische Gerät mehr oder weniger starke elektromagnetische Wellen ab, die sich unter anderem durch die Luft und entlang metallischer Leiter (z. B. Kabel, Klimakanäle, Heizungsrohre etc.) ausbreiten können.

In Deutschland enthält das Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG) Regelungen zu diesem Thema.

G 0.13 Abfangen kompromittierender Strahlung

Elektrische Geräte strahlen elektromagnetische Wellen ab. Bei Geräten, die Informationen verarbeiten (z. B. Computer, Bildschirme, Netzkoppelelemente, Drucker), kann diese Strahlung auch die gerade verarbeiteten Informationen mit sich führen. Derartige informationstragende Abstrahlung wird bloßstellende oder kompromittierende Abstrahlung genannt. Angreifende, die sich beispielsweise in einem Nachbarhaus oder in einem in der Nähe abgestellten Fahrzeug befinden, können versuchen, diese Abstrahlung zu empfangen und daraus die verarbeiteten Informationen zu rekonstruieren. Die Vertraulichkeit der Informationen ist damit in Frage gestellt. Eine mögliche Zielsetzung eines solchen Angriffes ist Industriespionage.

Die Grenzwerte des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG) reichen im Allgemeinen nicht aus, um das Abfangen der bloßstellenden Abstrahlung zu verhindern. Falls dieses Risiko nicht akzeptiert werden kann, müssen deshalb in aller Regel zusätzliche Schutzmaßnahmen getroffen werden.

Bloßstellende Abstrahlung ist nicht auf elektromagnetische Wellen beschränkt. Auch aus Schallwellen, zum Beispiel bei Druckern oder Tastaturen, können unter Umständen nützliche Informationen gewonnen werden.

Zu beachten ist außerdem, dass bloßstellende Abstrahlung in bestimmten Fällen auch durch äußere Manipulation von Geräten verursacht oder verstärkt werden kann. Wird zum Beispiel ein Gerät mit elektromagnetischen Wellen bestrahlt, kann es passieren, dass die reflektierten Wellen vertrauliche Informationen mit sich führen.

G 0.14 Ausspähen von Informationen (Spionage)

Mit Spionage werden Angriffe bezeichnet, die das Ziel haben, Informationen über Unternehmen, Personen, Produkte oder andere Zielobjekte zu sammeln, auszuwerten und aufzubereiten. Die aufbereiteten Informationen können dann beispielsweise eingesetzt werden, um einem anderen Unternehmen bestimmte Wettbewerbsvorteile zu verschaffen, Personen zu erpressen oder ein Produkt nachbauen zu können.

Neben einer Vielzahl technisch komplexer Angriffe gibt es oft auch viel einfachere Methoden, um an wertvolle Informationen zu kommen, beispielsweise indem Informationen aus mehreren öffentlich zugänglichen Quellen zusammengeführt werden, die einzeln unverfänglich aussehen, aber in anderen Zusammenhängen kompromittierend sein können. Da vertrauliche Daten häufig nicht ausreichend geschützt werden, können diese oft auf optischem, akustischem oder elektronischem Weg ausgespäht werden.

Beispiele:

- Viele IT-Systeme sind durch Identifikations- und Authentisierungsmechanismen gegen eine unberechtigte Nutzung geschützt, z. B. in Form von Kontoname- und Passwort-Prüfung. Wenn das Passwort allerdings unverschlüsselt über die Leitung geschickt wird, ist unter Umständen möglich, dieses auszulesen.
- Um Geld an einem Geldausgabeautomaten abheben zu können, muss die korrekte PIN für die verwendete ec- oder Kreditkarte eingegeben werden. Leider ist der Sichtschutz an diesen Geräten häufig unzureichend, so dass Angreifende der Kundschaft bei der Eingabe der PIN ohne Mühe über die Schulter schauen können. Wenn Angreifende hinterher die Karte stehlen, können sie damit das Konto plündern.
- Um Zugriffsrechte auf einem PC zu erhalten oder diesen anderweitig zu manipulieren, können Angreifende den Benutzenden ein Trojanisches Pferd schicken, das sie als vorgeblich nützliches Programm einer E-Mail beigefügt haben. Neben unmittelbaren Schäden können über Trojanische Pferde vielfältige Informationen nicht nur über den einzelnen Rechner, sondern auch über das lokale Netz ausgespäht werden. Insbesondere verfolgen viele Trojanische Pferde das Ziel, Passwörter oder andere Zugangsdaten auszuspähen.
- In vielen Büros sind die Arbeitsplätze akustisch nicht gut gegeneinander abgeschirmt. Dadurch können andere Mitarbeitende und auch Besuchende eventuell Gespräche mithören und dabei Kenntnis von Informationen erlangen, die nicht für sie bestimmt oder sogar vertraulich sind.