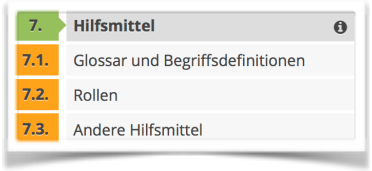
7.1 GLOSSAR UND BEGRIFFSDEFINITIONEN

Ordner Informationssicherheit - Kapitel 7. Hilfsmittel



Erstellt von: Vorname Name

10. Januar 2017

Version: 1.0

MUSTER

7.1 GLOSSAR UND BEGRIFFSDEFINITIONEN

Administrator

Ein Administrator verwaltet und betreut Rechner sowie Computernetze. Er installiert Betriebssysteme und Anwendungsprogramme, richtet neue Benutzerkennungen ein und verteilt die für die Arbeit notwendigen Rechte. Dabei hat er im Allgemeinen weitreichende oder sogar uneingeschränkte Zugriffsrechte auf die betreuten Rechner oder Netze.

Angriff

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Application-Level-Gateway (ALG)

Die Funktionen eines Sicherheitsgateways auf Anwendungsebene werden von den so genannten Application-Level-Gateways (ALG) übernommen. Implizit nehmen ALGs auch Funktionen auf den ISO-/OSI-Schichten 1 bis 3 wahr. ALGs, auch Sicherheitsproxies genannt, unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikationsbeziehung zwischen Client und Server über einen Proxy hinweg nimmt der Proxy die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt der Proxy analog. Sämtliche Kommunikationsbeziehungen zwischen den beiden Rechnern verlaufen in diesem Fall also mittelbar über den Proxy. Diese Kommunikationsform ermöglicht es einem Proxy beispielsweise bestimmte Protokollbefehle zu filtern.

Authentisierung (englisch "authentication")

Authentisierung bezeichnet den Nachweis eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt zu sein. Dies kann unter anderem durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen. Einige Autoren unterscheiden im Deutschen zwischen den Begriffen Authentisierung, Authentifizierung und Authentikation. Mit Authentisierung wird dann die Vorlage eines Nachweises zur Identifikation bezeichnet, mit Authentifizierung die Überprüfung dieses Nachweises. Um den Text verständlich zu halten, verzichtet der IT-Grundschutz auf diese Unterscheidung.

Authentizität

Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er 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-Sicherheitscheck

Der Begriff bezeichnet gemäß IT-Grundschutz die Überprüfung, ob die nach IT-Grundschutz empfohlenen Maßnahmen in einer Organisation bereits umgesetzt sind und welche grundlegenden Sicherheitsmaßnahmen noch fehlen.

Baustein (Rahmenbedingungen)

Der Begriff dient zur Strukturierung von Empfehlungen der IT-Grundschutz-Kataloge. Bausteine sind die Einheiten innerhalb einer Schicht (z. B. IT-Systeme, Netze). Sie beschreiben teils technische Komponenten (wie Verkabelung), teils organisatorische Verfahren (wie Notfallvorsorge-Konzept) und besondere Einsatzformen (wie Häuslicher Arbeitsplatz). In jedem Baustein werden die betrachtete IT-Komponente und die Gefährdungslage beschrieben sowie organisatorische und technische Sicherheitsmaßnahmen empfohlen.

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 dem Besitzer bzw. Benutzer der Informationen 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.

Benutzerkennung (häufig auch Benutzerkonto)

Die Benutzerkennung ist der Name, mit dem sich der Benutzer einem IT-System gegenüber identifiziert. Dies kann der tatsächliche Name sein, ein Pseudonym, eine Abkürzung oder eine Kombination aus Buchstaben und/oder Ziffern.

BIA (Business Impact Analyse)

Eine Business Impact Analyse (Folgeschädenabschätzung) ist eine Analyse zur Ermittlung von potentiellen direkten und indirekten Folgeschäden für eine Institution, die durch das Auftreten eines Notfalls oder einer Krise und Ausfall eines oder mehrerer Geschäftsprozesse verursacht werden.

Blackbox-Test

Bei Blackbox-Tests wird das Verhalten von Außentätern simuliert, wobei vorausgesetzt wird, dass der Angreifer keine oder nur oberflächliche Informationen über sein Angriffsziel hat.

Browser

Mit Browser (von "to browse", auf deutsch: schmökern, blättern, umherstreifen) wird Software zum Zugriff auf das World Wide Web bezeichnet. Das Programm interpretiert die ankommenden Daten und stellt sie als Text und Bild auf dem Bildschirm dar. Beispiele: Safari, Firefox, Chrome oder Internet Explorer.

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.

Client

Als Client wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der in einem Netz auf Daten und Programme von Servern zugreift.

Computer-Virus

Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.

Datenschutz

Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. 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".

Datensicherung (englisch "Backup")

Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren. Ordnungsgemäße Datensicherung bedeutet, dass die getroffenen Maßnahmen in Abhängigkeit von der Datensensitivität eine sofortige oder kurzfristige Wiederherstellung des Zustandes von Systemen, Daten, Programmen oder Prozeduren nach erkannter Beeinträchtigung der Verfügbarkeit, Integrität oder Konsistenz aufgrund eines

schadenswirkenden Ereignisses ermöglichen. Die Maßnahmen umfassen dabei mindestens die Herstellung und Erprobung der Rekonstruktionsfähigkeit von Kopien der Software, Daten und Prozeduren in definierten Zyklen und Generationen.

Demilitarisierte Zone (DMZ)

Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird, aber weder zu dem einen, noch zu dem anderen Netz gehört. Sie stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie das eigentlich zu schützende Netz. DMZ werden bei einfachen Sicherheitsgateways üblicherweise an einer dritten Schnittstelle des Paketfilters erzeugt. Besteht das Sicherheitsgateway aus Paketfilter - Application-Level-Gateway - Paketfilter, dient in der Regel eine weitere Schnittstelle des Application-Level-Gateways (ALG) als DMZ-Schnittstelle. Verfügen Paketfilter oder ALG über mehr als drei Schnittstellen, können weitere DMZ gebildet werden.

Digitale Signatur

Eine digitale Signatur ist eine Kontrollinformation, die an eine Nachricht oder Datei angehängt wird, mit der folgende Eigenschaften verbunden sind:

- Anhand einer digitalen Signatur kann eindeutig festgestellt werden, wer diese erzeugt hat,
- und es ist authentisch überprüfbar, ob die Datei, an die die digitale Signatur angehängt wurde, identisch ist mit der Datei, die tatsächlich signiert wurde.

Ergänzende Sicherheitsanalyse

Diese Analyse ist nach IT-Grundschutz erforderlich, wenn Zielobjekte des betrachteten Informationsverbunds einen erhöhten Schutzbedarf haben, nicht geeignet modelliert werden können oder in untypischen Einsatzszenarien betrieben werden. Die Vorgehensweise hierzu ist im BSI-Standard 100-2 "IT-Grundschutz-Vorgehensweise" beschrieben. Die ergänzende Sicherheitsanalyse dient dazu festzustellen, für welche Teile des Informationsverbunds eine Risikoanalyse notwendig ist.

Firewall

Eine Firewall (besser mit Sicherheitsgateway bezeichnet) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln (siehe Sicherheitsgateway).

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. Beispiel: Die Gefahr ist ein Datenverlust. Datenverlust kann unter anderem durch eine defekte Festplatte oder einen Dieb entstehen, der die Festplatte stiehlt. 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 Computer-Viren eine Bedrohung oder eine Gefährdung für Anwender, die im Internet surfen? Nach der oben gegebenen Definition lässt sich feststellen, dass alle Anwender prinzipiell durch Computer-Viren im Internet bedroht sind. Der Anwender, der eine virenverseuchte Datei herunterlädt, wird von dem Computer-Virus gefährdet, wenn sein Computer anfällig für diesen Computer-Viren-Typ ist. Für Anwender mit einem wirksamen Schutzprogramm, einer Konfiguration, die das Funktionieren des Computer-Virus verhindert, oder einem Betriebssystem, das den Virencode nicht ausführen kann, bedeutet das geladene Schadprogramm hingegen keine Gefährdung.

Gefährdungskataloge

Gefährdungskataloge sind Teil der IT-Grundschutz-Kataloge und enthalten Beschreibungen möglicher Gefährdungen der Informationstechnik. Sie sind in die Schadensursachen höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen gegliedert.

Grundwerte der Informationssicherheit

Der IT-Grundschutz betrachtet die drei Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität. Jedem Anwender steht es natürlich frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies in seinem individuellem Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der Informationssicherheit sind zum Beispiel:

- Authentizität
- Verbindlichkeit
- Zuverlässigkeit
- Nichtabstreitbarkeit

Hintertür (englisch „backdoor")

Hintertüren sind Schadprogramme, die dazu dienen, einen unbefugten Zugang zu einem IT-System offen zu halten, der einen unbemerkten Einbruch in das System ermöglicht und dabei möglichst weitgehende Zugriffsrechte besitzt, beispielsweise um Angriffsspuren zu verstecken.

Informationssicherheit

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Der Begriff "Informationssicherheit" statt IT-Sicherheit ist daher umfassender und wird zunehmend verwendet. Da aber in der Literatur noch überwiegend der Begriff "IT-Sicherheit" zu finden ist, wird er auch in dieser sowie in anderen Publikationen des IT-Grundschutzes weiterhin verwendet, allerdings werden die Texte sukzessive stärker auf die Betrachtung von Informationssicherheit ausgerichtet.

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 Informationssicherheitsmanagement 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. Aus den gleichen Gründen, die oben für die Begriffe "Informationssicherheit" und "IT-Sicherheit" genannt sind, wird im IT-Grundschutz noch häufig der Begriff "IT-Sicherheitsmanagement" verwendet.

Informationstechnik (IT)

Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.

Informationsverbund

Unter einem Informationsverbund (oder auch IT-Verbund) 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.

Institutionen

Mit dem Begriff Institutionen werden in diesem Dokument 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. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

Intranet

Ein Intranet ist ein internes Netz, das sich unter vollständiger Kontrolle des Netzbetreibers (also der jeweiligen Behörde oder des Unternehmens) befindet. Meist werden Zugriffe aus anderen Netzen (wie dem Internet) durch eine Firewall abgesichert.

IS-Management-Team

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

IT-Grundschutz

IT-Grundschutz bezeichnet eine Methodik zum Aufbau eines Sicherheitsmanagementsystems sowie zur Absicherung von Informationsverbünden über Standard-Sicherheitsmaßnahmen. Außerdem wird mit IT-Grundschutz der Zustand bezeichnet, in dem die vom BSI empfohlenen Standard-Sicherheitsmaßnahmen umgesetzt sind, die als Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen, Institutionen mit normalem Schutzbedarf hinreichend absichern.

IT-Grundschutzanalyse

Zu einer IT-Grundschutzanalyse gehören die Modellierung mit der Ermittlung der notwendigen Sicherheitsmaßnahmen und der Basis-Sicherheitscheck, in dem ein Soll-Ist-Vergleich den aktuellen Umsetzungsgrad von Sicherheitsmaßnahmen in einem Unternehmen oder einer Behörde beschreibt.

IT-Sicherheit

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

IT-Sicherheitsbeauftragter

Person mit eigener Fachkompetenz zur Informationssicherheit in einer Stabsstelle eines Unternehmens oder einer Behörde, der für alle Aspekte rund um die Informationssicherheit, Mitwirkung im Sicherheitsprozess und IS-Management-Team zuständig ist, die Leitlinie zur Informationssicherheit, das Sicherheitskonzept und andere Konzepte z. B. für Notfallvorsorge koordinierend erstellt und deren Umsetzung plant und überprüft.
Die Rolle des Verantwortlichen für Informationssicherheit wird je nach Art und Ausrichtung der Institution anders genannt. Häufige Titel sind IT-Sicherheitsbeauftragter oder kurz IT-SiBe, Chief Security Officer (CSO), Chief Information Security Officer (CISO) oder Information Security Manager. Mit dem Titel "Sicherheitsbeauftragter" werden dagegen häufig die Personen bezeichnet, die für Arbeitsschutz, Betriebssicherheit oder Werkschutz zuständig sind.

IT-System

IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Einzelplatz-Computer, Mobiltelefone, Router, Switches und Sicherheitsgateways.

Keylogger

Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern filtern.

Komponenten

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

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.

Mandantenfähigkeit

Als mandantenfähig werden Anwendungen, IT-Systeme oder auch Dienstleistungen bezeichnet, bei denen die Prozesse, Informationen und Anwendungen eines Mandanten strikt von denen anderer Kunden getrennt sind, also keine Zugriffe oder Störungen von dem einen in den anderen Bereich möglich sind und somit auch deren Vertraulichkeit, Integrität oder Verfügbarkeit nicht beeinträchtigt werden kann.

Maßnahmenkataloge

In den IT-Grundschutz-Katalogen werden zu jedem Baustein passende Maßnahmen empfohlen. Diese sind in Katalogen zusammengefasst, die in Infrastruktur, Organisation, Personal, Hardware/Software, Kommunikation und Notfallvorsorge gegliedert sind.

Maximum-Prinzip

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

Modellierung

Bei der Vorgehensweise nach IT-Grundschutz wird bei der Modellierung der betrachtete Informationsverbund eines Unternehmens oder einer Behörde mit Hilfe der Bausteine aus den IT-Grundschutz-Katalogen nachgebildet. Hierzu enthält Kapitel 2.2 der IT-Grundschutz-Kataloge für jeden Baustein 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 einem Absender einer Nachricht unmöglich sein, das Absenden einer bestimmten Nachricht nachträglich zu bestreiten.
- Nichtabstreitbarkeit des Erhalts: Es soll einem Empfänger einer Nachricht unmöglich sein, den Erhalt einer gesendeten Nachricht nachträglich zu bestreiten.

Paketfilter

Paketfilter sind IT-Systeme mit spezieller Software, die den ein- und ausgehenden Datenverkehr in einem Netz anhand spezieller Regeln filtern. Aufgabe eines Paketfilters ist es, Datenpakete anhand der Informationen in den Header-Daten der UDP/IP- bzw. TCP/IP-Schicht (z. B. IP-Adresse und Portnummer) weiterzuleiten oder zu verwerfen. Diese Entscheidung treffen Paketfilter anhand der vom Anwender vorgegebenen Filterregeln. Vielfach bieten die Paketfilter auch eine Möglichkeit zur "Network Address Translation" (NAT), bei der die Absender-Adressen von IP-Paketen durch eine IP-Adresse des Paketfilters ersetzt wird. Dadurch wird die Netzstruktur des zu schützenden Netzes verdeckt.

Patch

Ein Patch (vom englischen "patch", auf deutsch: Flicken) ist ein kleines Programm, das Softwarefehler wie z. B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen behebt.

Penetrationstest

Ein Penetrationstest ist ein gezielter, in der Regel simulierter, Angriffsversuch auf ein IT-System. Er wird als Wirksamkeitsprüfung vorhandener Sicherheitsmaßnahmen eingesetzt.

Privilegierte Berechtigungen

Privilegierte oder administrative Berechtigungen umfassen weitergehende Zugriffsmöglichkeiten auf IT-Systeme oder Software-Komponenten, als für normale Benutzer erforderlich sind. In der Regel werden privilegierte Berechtigungen nur solchen Rollen, Gruppen oder Personen zugewiesen, die überwiegend mit der Administration von Informationstechnik betraut sind. Dazu gehört unter anderem die betriebliche und/ oder sicherheitstechnische Konfiguration.

Proxy

Ein Proxy ist eine Art Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.

Qualifizierungsstufe

Die IT-Grundschutz-Methodik sieht drei Qualifizierungsstufen vor: "A" für die IT-Grundschutz-Einstiegsstufe, "B" für die IT-Grundschutz-Aufbaustufe, "C" für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz. Mit "Z" werden Maßnahmen bezeichnet, die Ergänzungen darstellen, die vor allem bei höheren Sicherheitsanforderungen hilfreich sein können. Mit "W" gekennzeichnete Maßnahmen dienen ausschließlich der Vermittlung von Grundlagen und Kenntnissen, die für das Verständnis und die Umsetzung der anderen Maßnahmen hilfreich sind.

Revision

Revision ist die systematische Überprüfung der Eignung und Einhaltung vorgegebener (Sicherheits-)Richtlinien. Die Revision sollte unabhängig und neutral sein.

Risiko

Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab. Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens. Im Unterschied zu "Gefährdung" umfasst der Begriff "Risiko" bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.

Risikoanalyse (englisch "Risk Assessment / Analysis")

Mit einer Risikoanalyse wird untersucht, welche schädigenden Ereignisse eintreten können, wie wahrscheinlich das Eintreten eines schädigenden Ereignisses ist und welche negativen Folgen der Schaden hätte.

Rootkit

Ein Rootkit ist ein Schadprogramm, das manipulierte Versionen von Systemprogrammen enthält. Unter Unix sind dies typischerweise Programme wie login, ps, who, netstat etc. Die manipulierten Systemprogramme sollen es einem Angreifer ermöglichen, zu verbergen, dass er sich erfolgreich einen Zugriff mit Administratorenrechten verschafft hat, so dass er diesen Zugang später erneut benutzen kann.

Schadfunktion

Mit Schadfunktion wird eine vom Anwender ungewünschte Funktion bezeichnet, die die Informationssicherheit unbeabsichtigt oder bewusst gesteuert gefährden kann.

Schadprogramm / Schadsoftware / Malware

Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Malware ist ein Kunstwort, abgeleitet aus "Malicious software" und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computer-Viren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte

Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

Schutzbedarf

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

Schutzbedarfsdefinitionen

Dies sind auf die jeweils betrachtete Institution angepasste Kriterien, anhand derer entschieden werden kann, welche Schutzbedarfskategorie auf eine IT-Komponente anzuwenden ist.

Schutzbedarfsfeststellung

Bei der Schutzbedarfsfeststellung wird der Schutzbedarf der Geschäftsprozesse, der verarbeiteten Informationen und der IT-Komponenten 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.

Server

Als Server wird Soft- oder Hardware bezeichnet, die bestimmte Dienste anderen (nämlich Clients) anbietet. Typischerweise wird damit ein Rechner bezeichnet, der seine Hardware- und Software-Ressourcen in einem Netz anderen Rechnern zugänglich macht. Beispiele sind Applikations-, Daten-, Web- oder E-Mail-Server. Zu häufiger Verwirrung führen X-Server, da ein X-Server-Prozess typischerweise auf einem Arbeitsplatzrechner, also einem Client in einem Server-Client-Netz, läuft.

Sicherheitsgateway

Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardware-technischen Komponenten. Es gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer Sicherheitsrichtlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden.

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 Erstellung einer 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. Synonym werden auch die Begriffe Sicherheitsvorkehrung oder Schutzmaßnahme benutzt. Als englische Übersetzung wurde "safeguard", "security measure" oder "measure" gewählt. Im englischen Sprachraum wird neben "safeguard" außerdem häufig der Begriff "control" verwendet.

Sicherheitspolitik

Hierbei handelt es sich um eine falsche Übersetzung des englischen Begriffs "Security Policy", siehe Sicherheitsrichtlinie.

Sicherheitsrichtlinie (englisch "Security Policy")

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

Spyware

Als Spyware werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig nur als lästig, es sollte aber nicht übersehen werden, dass durch Spyware auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden können.

Standardsoftware

Unter Standardsoftware wird Software (Programme, Programm-Module, Tools etc.) verstanden, die für die Bedürfnisse einer Mehrzahl von Kunden am Markt und nicht speziell vom Auftragnehmer für den Auftraggeber entwickelt wurde, einschließlich der zugehörigen Dokumentation. Sie zeichnet sich außerdem dadurch aus, dass sie vom Anwender selbst installiert werden soll und dass nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist.

Starke Authentisierung

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

Strukturanalyse

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

Trojanisches Pferd

Ein Trojanisches Pferd, oft auch (fälschlicherweise) kurz Trojaner genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

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 Anwendern stets wie vorgesehen genutzt werden können.

Verschlüsselung

Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartextes aus dem Geheimtext - wird Entschlüsselung genannt.

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 laufen.

Vertraulichkeit

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

VLAN

Virtuelle lokale Netze (Virtual LANs, VLANs) werden zur logischen Strukturierung von Netzen verwendet. Dabei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, indem funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz verbunden werden.

VPN

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme

kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner sicher authentisiert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind. Der Begriff VPN wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls.

Wert (englisch "asset")

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

WLAN (englisch "WiFi")

Mit WLAN werden drahtlose Netze bezeichnet, die auf der als IEEE 802.11 bezeichneten Gruppe von Standards basieren, die vom Institute of Electrical and Electronics Engineers (IEEE) spezifiziert wurden. Es gibt verschlüsselte und unverschlüsselte WLAN.

Wurm

Bei (Computer-, Internet-, E-Mail-)Würmern handelt es sich um Schadsoftware, ähnlich einem Virus, die sich selbst reproduziert und sich durch Ausnutzung der Kommunikationsschnittstellen selbstständig verbreitet.

Zertifikat

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

- IT-Grundschutz-Zertifikat: Damit kann dokumentiert werden, dass für den betrachteten Informationsverbund alle relevanten Sicherheitsmaßnahmen gemäß IT-Grundschutz-Vorgehensweise realisiert wurden. Dieses Zertifizierungsverfahren wurde durch die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz (siehe unten) abgelöst.

- 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: Seit Anfang 2006 können ISO 27001-Zertifikate auf der Basis von IT-Grundschutz beim BSI beantragt werden. Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist eine Überprüfung durch einen vom BSI zertifizierten ISO 27001-Grundschutz-Auditor. Zu den Aufgaben eines ISO 27001-Grundschutz-Auditors gehört 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 Sicherheitsmaßnahmen umgesetzt sind, erteilt im positiven Falle ein Zertifikat und veröffentlicht es.

- Zertifikat (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.

- Zertifikat (IT-Sicherheitszertifikat, CC-Zertifikat): Zertifiziert wird nach international anerkannten Sicherheitskriterien, wie z. B. den Common Criteria (ISO/IEC 15408). Auf dieser Basis können Produkte und Systeme 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.

- Zertifikat von Schutzprofilen (Profil-Zertifikate): Mit Schutzprofilen wird bei den Common Criteria Anwendergruppen und Herstellern die Möglichkeit gegeben, produktklassentypische und dienstleistungsspezifische Sicherheitsanforderungen festzulegen. Die Berücksichtigung von Schutzprofilen bei der Produktentwicklung erleichtert deren Evaluierung und führt zu Produkten, die in besonderem Maße den anwenderspezifischen Anforderungen entsprechen. Auch Schutzprofile können evaluiert und zertifiziert werden.

Zielobjekt

Zielobjekte sind Teile des Informationsverbunds, denen im Rahmen der Modellierung ein oder mehrere Bausteine aus den IT-Grundschutz-Katalogen zugeordnet werden können. Zielobjekte können dabei physische Objekte sein, wie beispielsweise Netze oder 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 bzw. System-Komponenten und Netze zu nutzen.

Zugriff

Mit Zugriff wird die Nutzung von Informationen bzw. 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.