Informationssicherheit

Als **Informationssicherheit** bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden *(technischen oder nicht-technischen)* Systemen, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken.

In der Praxis orientiert sich die Informationssicherheit im Rahmen des IT-Sicherheitsmanagements unter anderem an der internationalen ISO/IEC-27000-Reihe. Im deutschsprachigen Raum ist ein Vorgehen nach IT-Grundschutz verbreitet. Im Bereich der Evaluierung und Zertifizierung von IT-Produkten und -systemen findet die Norm ISO/IEC 15408 (Common Criteria) häufig Anwendung.

Inhaltsverzeichnis

[Verbergen]

Begriffsbeschreibungen[Bearbeiten | Quelltext bearbeiten]

Viele der nachfolgenden Begriffe werden je nach Autor und sprachlichem Umfeld unterschiedlich interpretiert.

Für die Abkürzung IT wird die Bezeichnung Informationstechnik synonym zu *Informationstechnologie* benutzt. Die technische Verarbeitung und Übertragung von Informationen steht bei der IT im Vordergrund.

Im Englischen hat der deutsche Begriff der *IT-Sicherheit* zwei verschiedene Ausprägungen. Die Eigenschaft der *Funktionssicherheit* (englisch: *safety*) stellt sicher, dass sich ein System konform zur erwarteten Funktionalität verhält. Es funktioniert so, wie es soll. *Informationssicherheit* (englisch: *security*) bezieht sich auf den Schutz der technischen Verarbeitung von Informationen und ist eine Eigenschaft eines funktionssicheren Systems. Sie soll verhindern, dass nicht-autorisierte Datenmanipulationen möglich sind oder die Preisgabe von Informationen stattfindet.[1]:4 f.

Der Begriff *Informationssicherheit* bezieht sich oft auf eine *globale Informationssicherheit*, bei der die Zahl der möglichen schädlichen Szenarien summarisch reduziert ist *oder* der Aufwand zur Kompromittierung für den Betreiber in einem ungünstigen Verhältnis zum erwarteten Informationsgewinn steht. In dieser Sichtweise ist die Informationssicherheit eine ökonomische Größe, mit der zum Beispiel in Betrieben und Organisationen gerechnet werden muss. Daneben bezieht sich der Begriff auch auf die Sicherheit *unter einem bestimmten Szenarium*. In diesem Sinn liegt Informationssicherheit vor, wenn über einen bereits bekannten Weg kein Angriff auf das System mehr möglich ist. Man spricht von einer binären Größe, weil die Information beim Anwenden dieser speziellen Methode entweder sicher oder nicht sicher sein kann.[2]

Folgende Aspekte sind in dem umfassenden Begriff *Informationssicherheit* (Schutz der verarbeiteten Informationen) enthalten:

IT-Sicherheit[Bearbeiten | Quelltext bearbeiten]

IT-Sicherheit bezeichnet die Sicherheit von soziotechnischen Systemen. IT oder auch ITK-Systeme sind Teil der soziotechnischen Systeme. Zu den Aufgaben der IT-Sicherheit gehört der Schutz von Organisationen (zum Beispiel Unternehmen) und deren Werte gegen Bedrohungen. Zudem soll wirtschaftlicher Schaden verhindert werden.[1]:3-7

In Abgrenzung zu *IT-Sicherheit* umfasst *Informationssicherheit* neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen; ein Beispiel: Die „Prinzipien der

Informationssicherheit“ können auch auf per Hand auf Papier notierte Rezepte eines Restaurants angewendet werden (da Vertraulichkeit, Integrität und Verfügbarkeit der Rezepte für das Restaurant extrem wichtig sein können, selbst wenn dieses Restaurant vollkommen ohne Einsatz irgendeines IT-Systems betrieben wird).

Computersicherheit[Bearbeiten | Quelltext bearbeiten]

Computersicherheit: die Sicherheit eines Computersystems vor Ausfall (man spricht von ungeplanter oder geplanter Ausfallzeit, engl. *downtime*) und Manipulation (Datensicherheit) sowie vor unerlaubtem Zugriff.

Datensicherheit[Bearbeiten | Quelltext bearbeiten]

Datensicherheit ist ein häufig mit dem Datenschutz verknüpfter Begriff, der von diesem zu unterscheiden ist: Datensicherheit hat das *technische* Ziel, Daten jeglicher Art in ausreichendem Maße gegen Verlust, Manipulationen und andere Bedrohungen zu sichern. Hinreichende Datensicherheit ist eine Voraussetzung für einen effektiven Datenschutz. Das BDSG nennt den Begriff der Datensicherheit lediglich in § 9a im Zusammenhang mit dem ebenfalls nicht näher definierten „Datenschutzaudit“.

Datensicherung[Bearbeiten | Quelltext bearbeiten]

→ *Hauptartikel: Datensicherung*

Datensicherung ist ein Synonym für das englischsprachige „Backup“ (dt. *Sicherung*), es war der ursprüngliche gesetzliche Begriff für Datensicherheit.

Datenschutz[Bearbeiten | Quelltext bearbeiten]

→ *Hauptartikel: Datenschutz*

Beim Datenschutz geht es nicht um den Schutz von allgemeinen Daten vor Schäden, sondern um den Schutz personenbezogener Daten vor Missbrauch („Datenschutz ist Personenschutz“). Der Schutz personenbezogener Daten stützt sich auf das Prinzip der informationellen Selbstbestimmung. Diese wurde im BVerfG-Urteil zur Volkszählung festgeschrieben. Geschützt werden muss dabei die Privatsphäre, d. h. Persönlichkeitsdaten bzw. Anonymität müssen gewahrt bleiben. Datenschutz verlangt über die Datensicherheit hinaus den Ausschluss des Zugangs zu Daten mit unberechtigtem Lesen durch unbefugte Dritte. Das deutsche Bundesdatenschutzgesetz (BDSG) beschreibt in § 1 ausschließlich Anforderungen für den Umgang mit personenbezogenen Daten. Das BDSG definiert den Unterschied der Begriffe Datenschutz und Datensicherheit

nicht. Nur wenn geeignete Schutzmaßnahmen getroffen werden, kann man davon ausgehen, dass vertrauliche bzw. personenbezogene Daten nicht in die Hände von Unbefugten gelangen. Hierbei spricht man in der Regel von technischen und organisatorischen Maßnahmen zum Datenschutz, die in der Anlage zum § 9 BDSG und in den Landesdatenschutzgesetzen beschrieben sind.

Motivation und Ziele der Informationssicherheit[Bearbeiten | Quelltext bearbeiten]

Information (oder Daten) sind schützenswerte Güter. Der Zugriff auf diese sollte beschränkt und kontrolliert sein. Nur autorisierte Benutzer oder Programme dürfen auf die Information zugreifen. *Schutzziele* werden zum Erreichen bzw. Einhalten der Informationssicherheit und damit zum Schutz der Daten vor beabsichtigten Angriffen von IT-Systemen definiert:[1]:6-11

- Allgemeine Schutzziele:
- *Vertraulichkeit* (englisch: *confidentiality*): Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden, dies gilt sowohl beim Zugriff auf gespeicherte Daten, wie auch während der Datenübertragung.
- *Integrität* (englisch: *integrity*): Daten dürfen nicht unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein.
- *Verfügbarkeit* (englisch: *availability*): Verhinderung von Systemausfällen; der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein.[1]:7-13
- Weitere Schutzziele der Informationssicherheit:[1]:7-13
- *Authentizität* (englisch: *authenticity*) bezeichnet die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit eines Objekts.[3]
- *Verbindlichkeit/Nichtabstreitbarkeit* (englisch: *non repudiation*): Sie erfordert, dass „kein unzulässiges Abstreiten durchgeführter Handlungen“ möglich ist.[4] Sie ist unter anderem wichtig beim elektronischen Abschluss von Verträgen. Erreichbar ist sie beispielsweise durch elektronische Signaturen.[5]
- *Zurechenbarkeit* (englisch: *accountability*): „Eine durchgeführte Handlung kann einem Kommunikationspartner eindeutig zugeordnet werden.“[4]
- in bestimmtem Kontext (zum Beispiel im Internet) auch *Anonymität*

Jedes noch so gut geplante und umgesetzte IT-System kann Schwachstellen besitzen. Sind bestimmte Angriffe zum Umgehen der vorhandenen Sicherheitsvorkehrungen möglich, ist das System *verwundbar*. Nutzt ein Angreifer eine Schwachstelle oder eine Verwundbarkeit zum Eindringen in ein IT-System, sind die Vertraulichkeit, Datenintegrität und Verfügbarkeit bedroht (englisch: *threat*). Angriffe auf die Schutzziele bedeuten für Unternehmen Angriffe auf reale Unternehmenswerte, im Regelfall das Abgreifen oder Verändern von unternehmensinternen Informationen. Jede mögliche Bedrohung ist ein *Risiko* (englisch: *risk*) für das Unternehmen. Unternehmungen versuchen durch die Verwendung eines Risikomanagements (englisch: *risk management*) die

Wahrscheinlichkeit des Eintretens eines Schadens und die daraus resultierende Schadenshöhe zu bestimmen.[1]:14-17

Nach einer *Risikoanalyse* und *Bewertung* der unternehmensspezifischen IT-Systeme, können entsprechende *Schutzziele* definiert werden. Anschließend folgt die Auswahl von IT-Sicherheitsmaßnahmen für die jeweiligen Geschäftsprozesse eines Unternehmens. Dieser Vorgang zählt zu den Tätigkeiten des IT-Sicherheitsmanagements. Eine genormte Vorgehensweise wird durch das Verwenden von IT-Standards ermöglicht.

Im Rahmen des IT-Sicherheitsmanagements findet die Auswahl und Umsetzung entsprechender *IT-Sicherheitsstandards* statt. Zu diesem Zweck existieren im Bereich IT-Sicherheitsmanagement verschiedene Standards. Mit Hilfe des *ISO/IEC 27001*- oder des *IT-Grundschutz*-Standards wird mit anerkannten Regeln versucht, die Komplexität soziotechnischer Systeme für den Bereich des IT-Sicherheitsmanagements zu reduzieren und ein geeignetes Maß an Informationssicherheit zu finden.

Bedeutung der Informationssicherheit[Bearbeiten | Quelltext bearbeiten]

Eine Mind-Map der Informationssicherheit

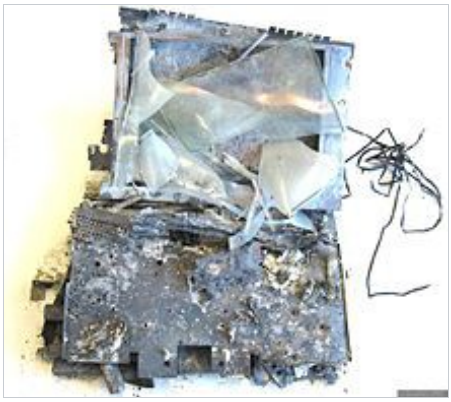
In den frühen Kindertagen des (Personal-)Computers verstand man unter Computersicherheit die Sicherstellung der korrekten Funktionalität von Hardware (Ausfall von zum Beispiel Bandlaufwerken oder anderen mechanischen Bauteilen) und Software (richtige Installation und Wartung von Programmen). Mit der Zeit änderten sich die Anforderungen an die Computer (Internet, Speichermedien); die Aufgaben zur Computersicherheit mussten anders gestaltet werden. Somit bleibt der Begriff der Computersicherheit wandelbar.

Private und öffentliche Unternehmen sind heute in allen Bereichen ihrer Geschäftstätigkeit, Privatpersonen in den meisten Belangen des täglichen Lebens auf IT-Systeme angewiesen. Da neben der Abhängigkeit auch die Risiken für IT-Systeme in Unternehmungen in der Regel größer sind als für Computer und Netzwerke in privaten Haushalten, ist Informationssicherheit überwiegend Aufgabe von Unternehmen.

Entsprechende Verpflichtungen lassen sich im gesamten deutschsprachigen Raum aus den verschiedenen Gesetzen zum Gesellschaftsrecht, Haftungsrecht, Datenschutz, Bankenrecht usw. herleiten. Dort stellt Informationssicherheit einen Baustein des Risikomanagements dar. International spielen Vorschriften wie Basel II und der Sarbanes-Oxley Act eine wichtige Rolle.

Einen Eindruck von der Komplexität und der grundsätzlichen Bedeutung der Informationssicherheit für die Zukunft von Informationsgesellschaften vermittelt die nebenstehende Mind-Map.

Bedrohungen[Bearbeiten | Quelltext bearbeiten]



verbrannter Laptop

Verschiedene Szenarien eines Angriffs lassen sich in der IT-Sicherheit vorstellen. Eine Manipulation der Daten einer Website über eine sogenannte SQL-Injection ist ein Beispiel. Nachfolgend werden einige Angriffe, Ziele sowie Ursachen beschrieben:

Angriffe und Schutz[Bearbeiten | Quelltext bearbeiten]

Unter einem Angriff auf den Datenschutz oder Datensicherheit (repräsentiert durch zum Beispiel ein Computersystem) versteht man jeden Vorgang, dessen Folge oder Ziel ein Verlust des Datenschutzes oder der Datensicherheit ist. Auch technisches Versagen wird in diesem Sinne als Angriff gewertet.

Statistische Sicherheit: Ein System wird dann als sicher bezeichnet, wenn für den Angreifer der Aufwand für das Eindringen in das System höher ist als der daraus resultierende Nutzen. Deshalb ist es wichtig, die Hürden für einen erfolgreichen Einbruch möglichst hoch zu setzen und damit das Risiko zu reduzieren.

Absolute Sicherheit: Ein System ist dann absolut sicher, wenn es jedem denkbaren Angriff widerstehen kann. Die absolute Sicherheit kann nur unter besonderen Bedingungen erreicht werden, die die Arbeitsfähigkeit des Systems oft erheblich einschränken (isolierte Systeme, wenige und hochqualifizierte Zugriffsberechtigte).

Der Mangel an Computersicherheit ist eine vielschichtige Bedrohung, die nur durch eine anspruchsvolle Abwehr beantwortet werden kann. Der Kauf und die Installation einer Software ist kein Ersatz für eine umsichtige Analyse der Risiken, möglicher Verluste, der Abwehr und von Sicherheitsbestimmungen.

Ist einmal die Sicherheit eines Systems verletzt worden, muss es als kompromittiert betrachtet werden, was Maßnahmen zur Verhinderung weiterer Schäden und ggf. zur Datenrettung erfordert.

Effekte oder Ziele[Bearbeiten | Quelltext bearbeiten]

- Technischer Systemausfall
- Systemmissbrauch, durch illegitime Ressourcennutzung, Veränderung von publizierten Inhalten, etc.
- Sabotage
- Spionage
- Betrug und Diebstahl

Ursachen oder Mittel[Bearbeiten | Quelltext bearbeiten]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) klassifiziert die unterschiedlichen Angriffsmethoden und -mittel in:[6]

- Schadsoftware bzw. Malware, zu denen unter anderem Computerviren, Trojaner und Würmer gehören,
- Ransomware, eine besondere Form von Schadsoftware, die den Zugriff auf Daten und Systeme einschränkt und dessen Ressourcen erst gegen Zahlung eines Lösegelds wieder freigibt,
- Social Engineering,
- Advanced Persistent Threats (APT), bei denen der Angreifer sein Ziel sorgfältig aussucht.
- Unerwünscht zugesandte E-Mails (Spam), der wiederum in klassischen Spam, Schadprogramm-Spam und Phishing unterteilt werden,
- Botnetze,
- Distributed Denial of Service (DDoS)-Angriffe,
- Drive-by-Exploits und Exploit-Kits, die Schwachstellen in Browser, Browser-Plugins oder Betriebssystemen ausnutzen,
- Identitätsdiebstahl, wie zum Beispiel Spoofing, Phishing, Pharming oder Vishing,
- Seitenkanalangriffe – also solche Angriffe, die Nebeneffekte (Laufzeitverhalten, Energieverbrauch) beobachten und so Rückschlüsse auf die Daten ziehen; dies findet insbesondere bei Schlüsselmaterial Anwendung.
  Daneben können die oben genannten Effekte auch durch

- physischen Einbruch zum Stehlen sensibler Daten wie Schlüssel oder zum Platzieren von Malware,
- höhere Gewalt, zum Beispiel in Form von Blitzschlag, Feuer, Vulkanausbruch oder Überschwemmung oder
- Fehlbedienung durch Personal oder zugangsberechtigte Personen verursacht werden.

Viren, Würmer, Trojanische Pferde[Bearbeiten | Quelltext bearbeiten]

Während im Firmenumfeld die ganze Themenbreite der Computersicherheit Beachtung findet, verbinden viele Privatanwender mit dem Begriff primär den Schutz vor Viren und Würmern oder Spyware wie Trojanischen Pferden.

Die ersten Computerviren waren noch recht harmlos und dienten lediglich dem Aufzeigen diverser Schwachstellen von Computersystemen. Doch recht bald erkannte man, dass

Viren zu weitaus mehr in der Lage sind. Es begann eine rasante Weiterentwicklung der Schädlinge und der Ausbau ihrer Fähigkeiten – vom simplen Löschen von Dateien über das Ausspionieren von Daten (zum Beispiel von Passwörtern) bis hin zum Öffnen des Rechners für entfernte Benutzer (Backdoor).

Mittlerweile existieren diverse Baukästen im Internet, die neben einer Anleitung auch alle notwendigen Bestandteile für das einfache Programmieren von Viren liefern. Nicht zuletzt schleusen kriminelle Organisationen Viren auf PCs ein, um diese für ihre Zwecke (UBE / UCE, DoS-Angriffe, etc.) zu nutzen. So entstanden bereits riesige Bot-Netze, die auch illegal vermietet werden.

Maßnahmen[Bearbeiten | Quelltext bearbeiten]

Die Maßnahmen müssen im Rahmen der Erstellung eines Sicherheitskonzeptes an den Wert der zu schützenden Unternehmenswerte angepasst werden. Zu viele Maßnahmen bedeuten zu hohe finanzielle, organisatorische oder personelle Aufwände. Akzeptanzprobleme treten auf, wenn die Mitarbeiter nicht genügend in den Prozess der IT-Sicherheit eingebunden werden. Implementiert man zu wenig Maßnahmen, bleiben für Angreifer lohnende Sicherheitslücken offen.

Management[Bearbeiten | Quelltext bearbeiten]

Informationssicherheit ist grundsätzlich eine Aufgabe der Leitung einer Organisation oder eines Unternehmens und sollte nach einem Top-Down-Ansatz organisiert sein. Insbesondere die Verabschiedung von Informationsschutz- und Sicherheitsrichtlinien (englisch: *Security Policy*) ist Aufgabe des obersten Managements. Weitere Aufgabe des Managements kann die Einführung und der Betrieb eines Informationssicherheitsmanagement-Systems (ISMS) sein. Dieses ist für die operative Umsetzung und Kontrolle der Security Policy zuständig. Durch diese Maßnahmen sollen geeignete Organisations- und Managementstrukturen für den Schutz der Unternehmenswerte geschaffen werden. Weitere Informationen sind im Artikel IT-Sicherheitsmanagement zu finden.

Operative Maßnahmen[Bearbeiten | Quelltext bearbeiten]

Maßnahmen sind unter anderem physische, beziehungsweise räumliche Sicherung von Daten, Zugriffskontrollen, das Aufstellen fehlertoleranter Systeme und Maßnahmen

der Datensicherung und die Verschlüsselung. Wichtige Voraussetzung ist die Sicherheit der verarbeitenden Systeme. Ein effektives Sicherheitskonzept berücksichtigt jedoch neben technischen Maßnahmen auch organisatorische und personelle Maßnahmen.

Zu den Sicherheitsmaßnahmen, die von jedem Verantwortlichen für die Informationssicherheit in Unternehmen, aber vor allem auch von privaten Nutzern von Computern und Netzwerken für die Informationssicherheit getroffen werden können, gehören unter anderem die folgenden Punkte.[7]

Eingeschränkte Benutzerkonten verwenden[Bearbeiten | Quelltext bearbeiten]

Der Systemadministrator darf tiefgehende Änderungen an einem Computer durchführen. Das erfordert entsprechende Kenntnis der Gefahren, und es ist für normale Benutzer alles andere als ratsam, mit den Rechten eines Administrators im Internet zu surfen, Dateienoder E-Mails herunterzuladen. Moderne Betriebssysteme verfügen daher über die Möglichkeit, die Benutzerrechte einzuschränken, so dass zum Beispiel Systemdateien nicht verändert werden können.

Restriktive Konfiguration[Bearbeiten | Quelltext bearbeiten]

Die Verwendung eingeschränkter Benutzerkonten für die tägliche Arbeit verhindert die Kompromittierung des Betriebssystems selbst, der Systemkonfiguration und der (schreibgeschützt) installierten Anwendungs- und System-Programme, bietet aber keinen Schutz gegen Kompromittierung der Benutzerdaten und der Benutzerkonfiguration: unter eingeschränkten Benutzerkonten sind beliebige Programme (dazu zählen auch Shell-Skripts oder Batch-Dateien) ausführbar, obwohl die wenigsten Benutzer diese Möglichkeit überhaupt nutzen.

Da Benutzer typischerweise (nur) die mit dem Betriebssystem gelieferten sowie die von ihrem Administrator installierten Programme verwenden ist es möglich, Benutzern die Rechte zum Ausführen von Dateien nur dort zu gewähren, wo das Betriebssystem und die installierten Programme abgelegt sind (und sie nicht schreiben können), und überall dort zu entziehen, wo sie selbst schreiben können. Schädliche Programme, die beispielsweise von einer infizierten Webseite heruntergeladen und vom Benutzer unbemerkt als sog. „Drive-by-Download“ im Cache des Browsers abgelegt werden, werden damit unschädlich gemacht.

Aktuelle Versionen von Microsoft Windows erlauben die Umsetzung dieser Restriktion mit den sog. „Softwarebeschränkungsrichtlinien“[8][9][10][11][12] alias „SAFER“.

Die Datenausführungsverhinderung[13] aktueller Betriebssysteme wendet dieselbe Restriktion im virtuellen Speicher an.

Software aktuell halten[Bearbeiten | Quelltext bearbeiten]

Für viele Programme werden (regelmäßig) Aktualisierungen angeboten. Diese bieten nicht immer nur eine erweiterte oder verbesserte Funktionalität, sondern beheben häufig auch Sicherheitslücken. Besonders betroffen sind vor allem Programme, die Daten mit dem Internet austauschen, wie zum
Beispiel Betriebssysteme, Browser, Schutzprogramme oder E-Mail-Programme. Die Aktualisierungen sollten so schnell wie möglich auf den entsprechenden Rechnersystemen installiert werden. Viele Programme bieten eine automatische Funktion an, die die Aktualisierung im Hintergrund ohne das Eingreifen des Benutzers bewerkstelligt, indem die neue Software direkt aus dem Internet geladen wird.

Veraltete, unsichere und unbenutzte Software deinstallieren[Bearbeiten | Quelltext bearbeiten]

Software, deren Hersteller die Wartung eingestellt hat, Sogenannte End of Life (EOL) die unsicher ist oder die nicht mehr benutzt wird, müssen deinstalliert werden, um den Schutz zu gewährleisten.

Sicherungskopien erstellen[Bearbeiten | Quelltext bearbeiten]

Von jeder Datei, die wichtig ist, muss mindestens eine Sicherungskopie auf einem separaten Speichermedium angefertigt werden. Hierzu gibt es zum Beispiel Backup-Software, die diese Aufgaben regelmäßig und automatisch erledigt. Im Rahmen von wiederkehrenden Wartungsarbeiten müssen angefertigte Sicherungskopien auf Integrität, Vertraulichkeit und Verfügbarkeit geprüft werden.

Im Unternehmensbereich kommen Backup-Lösungen mit örtlicher Distanz wie beispielsweise durch ein zweites Rechenzentrum mit redundanter Spiegelung sowie Cloud-Lösungen infrage. Diese Lösungen sind oftmals kostspielig. Die Verbesserung der Datensicherheit durch Sicherungskopien ist im Privatbereich weniger kostenintensiv. So können je nach Datenmenge auch kleinere Wechseldatenträger wie DVD oder Blu-ray sowie externe (USB-)Festplatten oder NAS-Systeme zur Sicherung genutzt werden.

Grundsätzlich gilt, dass die Relevanz der Daten für unternehmerische oder private Zwecke über Art und Häufigkeit der Sicherung sowie über die Anzahl der Sicherungskopien entscheiden sollte.

Antiviren-Software verwenden[Bearbeiten | Quelltext bearbeiten]

Wenn Daten aus dem Internet oder von Mailservern heruntergeladen oder von Datenträgern kopiert werden, besteht immer die Möglichkeit, dass sich darunter auch

schädliche Dateien befinden. Zur Vermeidung einer Kompromittierung sollten nur Dateien oder Anhänge geöffnet werden, denen man vertraut oder die von einem sogenannten Antivirenprogramm als unschädlich erkannt werden; allerdings können weder Vertrauen noch Antivirenprogramme vor allen schädlichen Dateien schützen: eine vertrauenswürdige Quelle kann selbst infiziert sein, und Antivirenprogramme können neue sowie unbekannte Schädlinge nicht entdecken. Auch bei dieser Software ist darauf zu achten, dass sie regelmäßig (unter Umständen sogar mehrmals täglich) aktualisiert wird. Antivirenprogramme haben oft selbst schädliche Nebenwirkungen: sie erkennen (regelmäßig) unschädliche Systemdateien irrtümlich als „infiziert“ und beseitigen diese, worauf das Betriebssystem nicht mehr (korrekt) funktioniert oder gar nicht mehr startet. Wie alle Computerprogramme haben sie selbst auch Fehler und Sicherheitslücken, sodass das Computersystem nach ihrer Installation unsicherer sein kann als vorher, bzw. nicht sicherer wird. Zudem wiegen sie den typischen Benutzer durch ihre Werbeaussagen wie „bietet umfassenden Schutz gegen alle Bedrohungen“ in trügerischer Sicherheit und können diesen zu riskanterem Verhalten verleiten. Schadprogramme sind in der Regel auf spezielle und auch oft auf weit verbreitete Betriebssysteme oder häufig genutzte Browser ausgerichtet.

Diversifikation[Bearbeiten | Quelltext bearbeiten]

Eine weitere Maßnahme zur Reduktion der Gefahren besteht in der Diversifizierung von Software, also darin, Software von verschiedenen, auch nicht marktführenden Anbietern zu verwenden. Die Angriffe von Crackern zielen oftmals auf Produkte von großen Anbietern, weil sie bei kriminellen Angriffen damit den größten Gewinn erzielen und ansonsten gegebenenfalls den größten „Ruhm“ erlangen. Insofern kann es ratsam sein, auf Produkte von kleineren und weniger bekannten Unternehmen oder zum Beispiel auf Open-Source-Software zurückzugreifen.

Firewalls verwenden[Bearbeiten | Quelltext bearbeiten]

Für Angriffe, die ohne das aktive Zutun des Nutzers drohen, ist es unerlässlich eine Netzwerk-Firewall oder Personal Firewall zu installieren. Viele unerwünschte Zugriffe auf den Computer und unbeabsichtigte Zugriffe vom eigenen Computer, die vom Benutzer meist gar nicht bemerkt werden, können auf diese Weise verhindert werden. Die Konfiguration einer Firewall ist nicht trivial und erfordert eine gewisse Kenntnis der Vorgänge und Gefahren.

Sandkästen[Bearbeiten | Quelltext bearbeiten]

„Sandkästen“ (engl. „Sandboxes“) sperren ein potentiell schädliches Programm ein. Im schlimmsten Falle kann das Programm lediglich den Sandkasten zerstören. Beispielsweise gibt es keinen Grund, weshalb ein PDF-Reader auf OpenOffice-Dokumente zugreifen muss. Der Sandkasten wäre in diesem Fall „alle PDF Dokumente und sonst nichts“. Techniken wie AppArmor und SELinux ermöglichen den Bau eines Sandkastens.

Aktive Inhalte deaktivieren[Bearbeiten | Quelltext bearbeiten]

Bei aktiven Inhalten handelt es sich um Funktionalitäten, die die Bedienung eines Computers vereinfachen sollen. Das automatische Öffnen beziehungsweise Ausführen von heruntergeladenen Dateien birgt jedoch die Gefahr, dass diese schädlichen Code ausführen und den Rechner infizieren. Um dies zu vermeiden, sollten aktive Inhalte, wie zum Beispiel ActiveX, Java oder JavaScript, so weit wie möglich deaktiviert werden.

Sensible Daten verschlüsseln[Bearbeiten | Quelltext bearbeiten]

Daten, die nicht in die Hände Dritter geraten sollen, müssen durch geeignete Maßnahmen, wie zum Beispiel GPG oder Device-Encryption-Software verschlüsselt werden (siehe auch Kryptographie). Dies betrifft nicht nur Daten, die zwischen zwei bestimmten Rechnern ausgetauscht werden, sondern auch entsprechende Daten, die sich auf Massenspeichern befinden, und beim Übertragen sensibler Daten, wie zum Beispiel Kreditkartennummern, während des Surfens im Internet (siehe auch HTTPS). Ein Zugriff auf die Inhalte darf nur dann möglich sein, wenn die Beteiligten über den richtigen Schlüssel verfügen. Besonders gefährdet sind unverschlüsselte, kabellose Netze, wie zum Beispiel nicht konfigurierte WLANs, da hierbei Unbefugte unbemerkt Zugriff auf die Daten und sogar die Kontrolle über den ungeschützten Computer erlangen könnten.

Auch für Behörden und Unternehmen ist die Datensicherheit, vor allem in Bezug auf den Datentransport ein äußerst sensibles Thema. Immer wieder erfordern Geschäftsprozesse die mobile Verfügbarkeit von Forschungs-, Finanz-, Kunden- oder Kontodaten. Bei der Datenaufbewahrung und dem Datentransport müssen sich Behörden und Unternehmen auf absolute Sicherheit verlassen können. Gelangen sensible Daten in unbefugte Hände, entsteht meist ein irreparabler Schaden, insbesondere wenn die Daten verbreitet oder missbraucht werden. Um dies zu verhindern und höchste Datensicherheit für den mobilen

Datentransport zu gewährleisten, müssen neben dem Kriterium der Verschlüsselung auch die Kriterien wie Zugriffskontrolle und Erstellung, Speicherung und Zerstörung des kryptographischen Schlüssels beachtet werden. Es ist zu beachten, dass immer alle drei Sicherheitskriterien berücksichtigt werden müssen. Hat eine von diesen Kriterien eine Sicherheitslücke, so wird dadurch die ganze Sicherheitskette gefährdet. Somit können für den sicheren Datentransport nur spezielle externe verschlüsselte Speichermedien genutzt werden.

Die Wahl einer passenden Verschlüsselung entscheidet über die Grundlage zum Erreichen eines höchsten Maßes an Datensicherheit. Für höchste Anforderungen an Datensicherheit empfiehlt das Bundesamt für Sicherheit in der Informationstechnik, die AES Verschlüsselung mit einer Schlüssellänge von 256-Bit im CBC-Modus zu verwenden. Der CBC-Modus sorgt dafür, dass jeder Block mit einem anderen AES-Schlüssel verschlüsselt wird. So werden bei der Verschlüsselung jedes neuen Sektors auch die Informationen von dem vorher verschlüsselten Block miteinbezogen.

Passwörter, persönliche Identifikationsnummern (PIN) und Transaktionsnummern (TAN) sollten nicht unverschlüsselt gespeichert oder übertragen werden.

Protokollierung[Bearbeiten | Quelltext bearbeiten]

Automatisch erstellte Protokolle oder Logdateien können dabei helfen, zu einem späteren Zeitpunkt zu ermitteln, wie es zu Schäden an einem Rechnersystem gekommen ist.

Sichere Entwicklungssysteme und Laufzeitumgebungen verwenden[Bearbeiten | Quelltext bearbeiten]

Für die Generierung und Wartung sicherer Software ist es sehr nützlich, schon bei der Softwareentwicklung strukturiert zu programmieren und leicht überschaubare und erlernbare Werkzeuge zu verwenden, die möglichst enggefasste Sichtbarkeitsregeln und gekapselteProgrammmodule mit eindeutig definierten Schnittstellen erlauben.[14] Durch eingeschränkte Freiheiten bei der Programmierung, wie zum Beispiel die Beschränkung auf einfache Vererbung oder das Verbot von Zirkelbezügen oder kritischen Typumwandlungen, wird in der Regel zugleich das Potential von Programmfehlern eingeschränkt. Dabei ist es auch sinnvoll und hilfreich, bereits getestete Software durch geeignete Maßnahmen wiederzuverwenden, wie zum Beispiel durch die Verwendung von Prozeduren oder objektorientiertenDatenstrukturen. Entwickler von Software, die zum sicheren Datenaustausch zwischen Rechnern eingesetzt wird, müssen moderne Entwicklungssysteme und Programmiersprachen einsetzen, da ältere Systeme häufig Sicherheitslücken haben und nicht über die entsprechende Sicherheitsfunktionalität verfügen. Sichere Software ist nur in entsprechenden, modernen

und sicheren Laufzeitumgebungen lauffähig und sollte mit Entwicklungswerkzeugen (wie zum Beispiel Compilern) erstellt werden, die ein möglichst hohes Maß an inhärenterSicherheit bieten, wie zum Beispiel Modulsicherheit, Typsicherheit oder die Vermeidung von Pufferüberläufen.

Auch bei Geräten, die nicht in einem Rechnernetz beziehungsweise im Internet der Dinge betrieben werden, kann die Informationssicherheit durch geeignete Entwicklungssysteme und Laufzeitumgebungen erhöht werden. Datenverlust durch unzuverlässigen Programmcode (Computerabsturz) kann vorbeugend zum Beispiel durch compilergenerierte Überprüfung von Indizes von Datenfeldern, unzulässigen Zeigern oder nach dem Auftreten von Programmfehlern durch Ausnahmebehandlung in der Laufzeitumgebung vermieden werden. Ferner ist es in objektorientierten Laufzeitumgebungen unerlässlich und auch in anderen Systemen sicherer, eine automatische Speicherbereinigung durchzuführen, damit nicht versehentlich Speicherplatz freigegeben wird.

Manche Entwickler vertrauen auf die Verifikation von Programmcode, um die Korrektheit von Software zu verbessern. Ferner ist es möglich, bereits implementierte Software durch bestimmte Verfahren, wie zum Beispiel die Verwendung von Proof-Carrying Code, erst während der Laufzeit zu überprüfen und deren Ausführung bei der Nichteinhaltung von Sicherheitsrichtlinien zu verhindern.

Sensibilisierung und Befähigung der Mitarbeiter[Bearbeiten | Quelltext bearbeiten]

Ein wichtiger Aspekt in der Umsetzung von Sicherheitsrichtlinien ist die Ansprache der eigenen Mitarbeiter, die Bildung von sogenannter IT-Security-Awareness. Hier fordern die ersten Arbeitsrichter den Nachweis der erfolgten Mitarbeitersensibilisierung für den Fall eines etwaigen Verstoßes gegen die Firmenrichtlinien. Zusätzliche Bedeutung bekommt diese menschliche Seite der Informationssicherheit außerdem, da Industriespionage oder gezielte, wirtschaftlich motivierte Sabotage gegen Unternehmen nicht allein mit technischen Mitteln ausgeführt werden. Um ihren Opfern zu schaden oder Informationen zu stehlen, nutzen die Angreifer beispielsweise Social Engineering, das nur abzuwehren ist, wenn die Mitarbeiter über mögliche Tricks der Angreifer orientiert sind und gelernt haben, mit potenziellen Angriffen umzugehen. Die Mitarbeitersensibilisierung variiert typischerweise von Unternehmen zu Unternehmen von Präsenzveranstaltungen über webbasierte Seminare bis hin zu Sensibilisierungskampagnen.

Der Fokus verschiebt sich dabei inzwischen von der reinen Sensibilisierung („Awareness“) hin zur Befähigung („Empowerment“) der Anwender, eigenverantwortlich für mehr Sicherheit im Umgang mit IT-gestützten Informationen zu sorgen.[15] In Unternehmen kommt dabei dem „Information Security Empowerment“ der Führungskräfte besondere Bedeutung zu, da sie Vorbildfunktion für ihre Abteilungsmitarbeiter haben und dafür verantwortlich sind, dass die Sicherheitsrichtlinien ihres Verantwortungsbereiches zu den dortigen Arbeitsabläufen passen – eine wichtige Voraussetzung für die Akzeptanz.[16]

Standards, „Best practices“ und Ausbildung im Überblick[Bearbeiten | Quelltext bearbeiten]

Zur Bewertung und Zertifizierung der *Sicherheit von Computersystemen* existieren internationale Normen. Wichtige Normen in diesem Zusammenhang waren die amerikanischen TCSEC und die europäischen ITSEC-Standards. Beide wurden 1996 von dem neueren Common Criteria-Standard abgelöst. Die Evaluierung und Zertifizierung von IT-Produkten und -systemen erfolgt in Deutschland in der Regel durch das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Die Aufgabe des *IT-Sicherheitsmanagements* ist die systematische Absicherung eines informationsverarbeitenden IT-Verbundes. Gefahren für die Informationssicherheit oder Bedrohungen des Datenschutzes eines Unternehmens oder einer Organisation sollen verhindert oder abgewehrt werden. Die Auswahl und Umsetzung von *IT-Sicherheitsstandards* zählt zu den Aufgaben des IT-Sicherheitsmanagements. Standards des IT-Sicherheitsmanagements sind beispielsweise:

- IT-Grundschutz des BSI
- Die IT-Grundschutz-Kataloge definieren für die verschiedenen Aspekte einer IT-Landschaft konkrete Maßnahmen, die zur Erhaltung der Sicherheit bei niedrigem und mittlerem Schutzbedarf erfüllt werden müssen (Waschzettel). Für Systeme mit hohem Schutzbedarf geben die Grundschutzkataloge ein strukturiertes Vorgehen, um die notwendigen Maßnahmen zu identifizieren. Die Grundschutz-Kataloge sind primär in Deutschland bekannt, liegen allerdings auch englischsprachig vor.
- ISO/IEC 27001: Norm für Informationsicherheitsmanagementsysteme (ISMS)
- ISO/IEC 27002: Leitfaden für das Informationssicherheitsmanagement (vormals ISO/IEC17799:2005)
  Weltweit am stärksten verbreitet ist die ISO/IEC 27001-Norm.

  Weitere Standards sind zu finden im

→ *Hauptartikel: IT-Sicherheitsmanagement*

Neben den Standards zur Informationssicherheit gibt es auch Standards für die Ausbildung von Sicherheitsfachkräften. Als wichtigste sind zu nennen die Zertifizierungen zum Certified Information Security Manager (CISM) und Certified Information Systems Auditor (CISA) der ISACA, die Zertifizierung zum Certified Information Systems Security Professional (CISSP) des International Information Systems Security Certification Consortium (ISC)², die Zertifizierung zum TeleTrusT Information Security Professional (TISP)[17] des TeleTrusT – Bundesverband IT-Sicherheit e. V. sowie die GIAC-Zertifizierungen des SANS Institute. Eine erweiterte Übersicht bietet die Liste der IT-Zertifikate.

Audits und Zertifizierungen[Bearbeiten | Quelltext bearbeiten]

Um ein gewisses Standardmaß an Informationssicherheit zu gewährleisten, ist die regelmäßige Überprüfung von Maßnahmen zur Risikominimierung und -dezimierung Pflicht. Auch hier rücken wieder organisatorische und technische Aspekte in den Vordergrund.

Technische Sicherheit kann zum Beispiel durch Maßnahmen wie regelmäßige Penetrationstests oder vollständige Sicherheitsaudits erreicht werden, um eventuell bestehende Sicherheitsrisiken im Bereich von informationstechnischen Systemen, Applikationen und/oder in der informationstechnischen Infrastruktur zu erkennen und zu beseitigen.

Organisatorische Sicherheit kann durch Audits der entsprechenden Fachabteilungen einer Organisation erreicht und überprüft werden. Beispielsweise können vordefinierte Testschritte beziehungsweise Kontrollpunkte eines Prozesses während eines Audits getestet werden.

Aus Feststellungen der weitreichenden Überprüfungsmethoden lassen sich Maßnahmen zur weiteren Risikominimierung beziehungsweise -dezimierung ableiten. Eine Methodik wie in diesem Absatz beschrieben, ist unmittelbar konform zu Normen wie ISO/IEC 27001, BS 7799 oder gesetzlichen Vorschriften. Hier wird meist eine Nachvollziehbarkeit über Vorgänge der Informationssicherheit unmittelbar eingefordert, indem Unternehmen ein Risikomanagement abverlangt wird.

Umsetzungsbereiche[Bearbeiten | Quelltext bearbeiten]

Zur Sensibilisierung für die Gefahren im Bereich der IT-Sicherheit und um mögliche Gegenmaßnahmen aufzuzeigen, existieren in Deutschland einige Initiativen. Dazu zählen

der Cyber-Sicherheitsrat Deutschland e.V., der Verein Deutschland sicher im Netz und die Allianz für Cyber-Sicherheit.

Privathaushalte[Bearbeiten | Quelltext bearbeiten]

Programmierfehler in fast jeder Software machen es quasi unmöglich, Sicherheit vor jeder Art von Angriffen zu erreichen. Durch den Anschluss von Computern mit sensiblen Daten (zum Beispiel Homebanking, Bearbeitung der Dissertation) an das Internet sind diese Schwachstellen auch von außen nutzbar. Der Standard an IT-Sicherheit in Privathaushalten ist geringer, da kaum ausreichende Maßnahmen zur Absicherung der Infrastruktur (zum Beispiel unterbrechungsfreie Stromversorgung, Einbruchsschutz) ergriffen werden.

Aber auch in anderen Bereichen besteht in privaten Haushalten weiterhin ein Defizit.

Viele private Benutzer haben noch nicht verstanden, dass es wichtig ist, die Konfiguration der genutzten Software an die jeweiligen Bedürfnisse anzupassen. So ist es bei vielen an das Internet angeschlossenen Rechnern nicht nötig, dass auf ihnen Server-Programme laufen. Server-Dienste werden von vielen Betriebssystemen in der Standardinstallation geladen; mit deren Deaktivierung schließt man eine Reihe wichtiger Angriffspunkte.

Sicherheitsaspekte wie zum Beispiel die Einrichtung von Zugriffsbeschränkungen sind vielen Benutzern ebenfalls fremd. Außerdem ist es von Bedeutung, sich über Schwachstellen in der eingesetzten Software zu informieren und regelmäßig Aktualisierungen einzuspielen.

Zur Computersicherheit gehört nicht nur der präventive Einsatz technischer Werkzeuge wie beispielsweise Firewalls, Intrusion-Detection-Systeme etc., sondern auch ein organisatorischer Rahmen in Form durchdachter Grundsätze (Policy, Strategie), die den Menschen als Anwender der Werkzeuge in das System einbezieht. Allzu oft gelingt es Hackern, durch Ausnutzung eines zu schwachen Kennworts oder durch sogenanntes Social Engineering Zugang zu sensiblen Daten zu erlangen.

IT-Sicherheit bei Sparkassen und Banken[Bearbeiten | Quelltext bearbeiten]

Zur Beschleunigung des Prozesses und Hervorhebung der Wichtigkeit haben unter anderem die Ergebnisse von Basel II, die Vorschriften von BaFin und des KWG sowie der einzelnen Verbandsrevisionen der Sparkassen und Banken beigetragen. Verstärkt werden sowohl externe als auch interne Prüfungen auf dieses Thema ausgelegt. Gleichzeitig

entstand ein umfangreiches Dienstleistungsangebot zur Durchführung verschiedener Projekte, die einen IT-Sicherheitsprozesses in Unternehmen etablieren sollen. Anbieter sind sowohl innerhalb der jeweiligen Unternehmensgruppe als auch auf dem externen Markt zu finden. Bei anderen Finanzdienstleistungsinstituten, Versicherungsunternehmen und den Unternehmen des Wertpapierhandels wird das Konzept im Allgemeinen identisch sein, wobei hier zum Beispiel auch andere Gesetze eine Rolle spielen können.

IT-Sicherheit bei anderen Unternehmen[Bearbeiten | Quelltext bearbeiten]

Auch wenn die Gesetzgebungen und Prüfungen in anderen Sektoren der Wirtschaft weniger Vorgaben macht, behält die IT-Sicherheit ihren hohen Stellenwert. Hilfestellungen gewähren die kostenfreien IT-Grundschutz-Kataloge des BSI.

Durch die zunehmende Vernetzung verschiedener Niederlassungen z. B. bei Firmenzukäufen gewinnt eine Absicherung der IT-Systeme größere Bedeutung. Durch die Datenübertragung aus einem internen, geschlossenen Netzwerk über eine externe, öffentliche Verbindung zum anderen Standort existieren risikobehaftete Situationen.

Die Auswirkungen für Unternehmen sind u. a.:

- Verlust von Daten,
- Manipulation von Daten,
- unzuverlässiger Empfang von Daten,
- verspätete Verfügbarkeit von Daten,
- Abkopplung von Systemen für das operative Geschäft,
- unzulässige Verwertung von Daten,
- fehlende Entwicklungsfähigkeit der eingesetzten Systeme.

Aber nicht nur im firmeninternen Datenaustausch liegt die Gefahr, es werden zunehmend Anwendungen direkt zu den Nutzern übertragen, oder aber externe Mitarbeiter oder gar outgesourcte Dienstleistern auf im Unternehmen gespeicherte Daten zuzugreifen und diese zu bearbeiten und zu verwalten. Für deren Zugriffsberechtigung muss eine Authentisierung ebenso erfolgen können, wie eine Dokumentation der getätigten und veränderten Aktionen.

Dieser Thematik folgend entstehen neue Anforderungen an die bestehenden Sicherheitskonzepte. Hinzu kommen die gesetzlichen Vorgaben, die ebenfalls in das IT-Sicherheitskonzept mit integriert werden müssen. Die entsprechenden Gesetze werden

von externen und internen Prüfern kontrolliert. Da keine Methoden definiert worden sind, um diese Ergebnisse zu erreichen, wurden hier für die jeweiligen Bereiche verschiedenen „Best-Practice“-Methoden entwickelt, wie zum Beispiel ITIL, COBIT, ISO oder Basel II.

Hier gilt der Ansatz, ein Unternehmen so zu führen und zu kontrollieren, dass die relevanten und möglichen Risiken abgedeckt sind. Als Standard für die sogenannte IT-Governance sind einmal die zwingenden, sprich Gesetze (HGB, AO, GOB) und Fachgutachten (Sarbanes-Oxley Act, 8. EU-Audit-Richtlinie) und die unterstützenden („Best Practice Methode“) zu sehen.

Das bedeutet diese Risiken zu identifizieren, analysieren und bewerten. Um darauf aufbauend die Erstellung eines ganzheitlichen Sicherheitskonzeptes zu ermöglichen. Das beinhaltet nicht nur die eingesetzten Technologien, sondern auch organisatorische Maßnahmen, wie Zuständigkeiten, Berechtigungen, Kontrollinstanzen oder konzeptionelle Aspekte wie etwa Mindestanforderungen für bestimmte Sicherheitsmerkmale zu definieren.

So werden nun an die EDV besondere Anforderungen gestellt:

1. Verhinderung von Manipulationen
2. Nachweis von Eingriffen
3. Installation von Frühwarnsystemen
4. Interne Kontrollsysteme
   Dabei ist zu beachten, dass die Daten der Automation derart gespeichert werden, dass sie jederzeit lesbar, nachvollziehbar und konsistent sind. Dazu müssen diese Daten vor Manipulation und Löschung geschützt werden. Jegliche Änderung soll ein Versionsmanagement auslösen und die Reporte und Statistiken über die Prozesse und deren Änderungen müssen direkt zentral abrufbar sein.

   Eine Abhilfe können hier hochentwickelte Automatisierungslösungen sein. Dadurch, dass weniger manuelle Eingriffe notwendig sind, werden potentielle Gefahrenquellen ausgeschlossen. Die RZ-Automation umfasst somit folgende Gebiete:

- Risikofaktor Prozessablauf
- Risikofaktor Ressourcen
- Risikofaktor Technologie
- Risikofaktor Zeit

IT-Sicherheit in öffentlichen Einrichtungen und Behörden[Bearbeiten | Quelltext bearbeiten]

In diesem Bereich sind die IT-Grundschutz-Kataloge des BSI Standardwerke. In großem Maße erhalten diese Stellen das zugehörige GSTOOL, welches die Durchführung deutlich vereinfacht, kostenlos.

Gesetzliche Rahmenbedingungen[Bearbeiten | Quelltext bearbeiten]

Corporate Governance kann als Rahmen der IT-Sicherheit gesehen werden. Der Begriff stammt aus dem strategischen Management und bezeichnet einen Prozess zur Steuerung eines privatwirtschaftlichen Unternehmens. Durch Regeln und Kontrollmechanismen wird ein Ausgleich zwischen den verschiedenen Interessengruppen (Stakeholdern) angestrebt. Der Prozess dient dem Erhalt des Unternehmens und unterliegt einer regelmäßigen externen Überprüfung.[18]:32 f.

Gesetze zur Corporate Governance[Bearbeiten | Quelltext bearbeiten]

Mit dem Ziel einer besseren Überwachung der Unternehmensführung (Corporate Governance) und ausländischen Investoren den Zugang zu Informationen über die Unternehmen zu erleichtern (Transparenz), trat im Mai 1998 das *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)* in Kraft. Das Kernthema der weitreichenden Änderungen im Handelsgesetzbuch (HGB) und im Aktiengesetz (AktG) war die Einführung eines Risikofrüherkennungssystems zur Erkennung von bestandsgefährdenden Risiken. Jedes am Kapitalmarkt orientierte Unternehmen musste ein solches System einrichten und Risiken des Unternehmens im Lagebericht des Jahresabschlusses veröffentlichen.[19]:37 f.

Der im Juli 2002 in Kraft getretene Sarbanes-Oxley Act (SOX) hatte das Ziel, verlorengegangenes Vertrauen der Anleger in die veröffentlichten Bilanzdaten von amerikanischen Unternehmen wiederherzustellen. Tochterunternehmen amerikanischer Gesellschaften im Ausland und nichtamerikanische Firmen, die an amerikanischen Börsen gehandelt werden, unterliegen ebenfalls dieser Regelung.[20]:295 f. Das Gesetz schreibt Vorkehrungen im Bereich der IT-Sicherheit wie die Einführung eines ISMS nicht explizit vor. Eine einwandfreie Berichterstattung über die internen Unternehmensdaten ist nur durch zuverlässige IT-Prozesse und einen angemessenen Schutz der verwendeten Daten möglich. Eine Konformität mit dem SOX ist daher nur mit Hilfe von Maßnahmen zur IT-Sicherheit möglich.[20]:295 f.[21]:3 f.

Die europäische Achte Richtlinie 2006/43/EG (auch EuroSOX genannt) entstand in Anlehnung an das amerikanische SOX-Gesetz und trat im Juni 2006 in Kraft. Sie beschreibt die Mindestanforderungen an Unternehmen für ein Risikomanagement und legt die Pflichten der Abschlussprüfer fest.[20]:296

Die deutsche Umsetzung der europäischen EuroSOX erfolgte im Bilanzrechtsmodernisierungsgesetz (BilMoG). Es trat im Mai 2009 in Kraft. Das Gesetz änderte zum Zwecke der Harmonisierung mit Europarecht einige Gesetze wie das HGB und das Aktiengesetz. Unter anderem sind Kapitalgesellschaften wie eine AG oder eine GmbH laut § 289 HGB Abs. 5 aufgefordert, wesentliche Eigenschaften ihres Internen Kontrollsystems (IKS) im Lagebericht des Jahresabschlusses darzulegen.[20]:296

In den europäischen Regelungen *Richtlinie über Eigenkapitalanforderungen (Basel I)* aus dem Jahr 1988 und *Richtlinie für Basissolvenzkapitalanforderungen* aus dem Jahr 1973 (2002 aktualisiert; nachträglich als Solvabilität I bezeichnet) wurden viele einzelne Gesetze unter einem Oberbegriff zusammengefasst.[22] Diese für Kreditinstitute und Versicherungsunternehmen bedeutsamen Regelungen enthielten viele Schwächen. Die neuen Regelungen Basel II für Banken (EU-weit in Kraft seit Januar 2007) und Solvabilität II für Versicherer (in Kraft seit Januar 2016) enthalten modernere Regelungen für ein Risikomanagement.[20]:296 f. Die Nachfolgeregelung Basel III wird seit 2013 eingeführt und soll bis 2019 komplett implementiert sein.

Datenschutzgesetze[Bearbeiten | Quelltext bearbeiten]

Die erste Fassung des Bundesdatenschutzgesetzes (BDSG) mit dem Namen *Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung* wurde am 27. Januar 1977 erlassen (BGBl. I S. 201). Unter dem Eindruck des sogenannten Volkszählungsurteils von 1983 trat durch das *Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes* vom 20. Dezember 1990 am 1. Juni 1991 eine Neufassung des BDSG in Kraft (BGBl. 1990 I S. 2954, 2955). Eine der zahlreichen Änderungen des Gesetzes trat im August 2002 in Kraft. Sie diente der Anpassung des Gesetzes an die EG-Richtlinie 95/46/EG (Datenschutzrichtlinie).[23]

Neben dem BDSG existieren in Deutschland weitere gesetzliche Vorschriften, die die Einführung und das Betreiben eines ISMS erfordern. Dazu zählen das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG).

Der Schutz der Privatsphäre wird in Großbritannien seit 1984 durch den Data Protection Act (DPA) geregelt. Dieser bot in seiner ursprünglichen Version einen minimalen Datenschutz. Die Verarbeitung personenbezogener Daten wurde 1998 durch eine neue Fassung des DPA ersetzt. Diese trat 2000 in Kraft und glich britisches Recht an die EG-Richtlinie 95/46/EG an. In Großbritannien verpflichtete die britische Regierung 2001 alle Ministerien mit dem BS 7799 konform zu werden. Die Implementierung eines ISMS erleichtert es britischen Unternehmen eine Konformität zum DPA nachzuweisen.[24]:135 f.

Die Datenschutz-Grundverordnung setzt die Richtlinie 95/46/EG außer Kraft. Sie trat am 24. Mai 2016 in Kraft und gilt ab 25. Mai 2018 unmittelbar in allen Staaten der Europäischen Union. Die bisherigen nationalen Regelungen wie der englische DPA und das deutsche BDSG werden abgelöst bzw. neu gefasst, um die Regelungsaufträge der Verordnung an den nationalen Gesetzgeber zu erfüllen.

IT-Sicherheitsgesetz[Bearbeiten | Quelltext bearbeiten]

Unter dem Eindruck von Terroranschlägen und aus militärischen Erwägungen tritt in Deutschland und anderen Ländern zunehmend der Schutz kritischer Infrastrukturen vor Cyber-Attacken in den Vordergrund. Hierzu trat am 25. Juli 2015 ein Artikelgesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) in Kraft.[25] Das Gesetz weist dem Bundesamt für Sicherheit in der Informationstechnik die zentrale Rolle beim Schutz kritischer Infrastrukturen in Deutschland zu.

Hierzu wurde das BSI-Gesetz um Sicherheitsanforderungen an sogenannte „Kritische Infrastrukturen“ ergänzt. Dies sind Einrichtungen, Anlagen oder Teile davon, die

- den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
- von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. In einer zugehörigen Verordnung KRITIS-Verordnung (BSI-KritisV[26]) wird geklärt, welche Einrichtungen, Anlagen oder Teile davon konkret unter die Vorgaben des IT-Sicherheitsgesetzes fallen.
  Kritische Infrastrukturen müssen branchenspezifische Mindeststandards erfüllen, wozu insbesondere die Einführung eines ISMS zählt. Weiterhin müssen sie relevante Vorfälle, die die IT-Sicherheit betreffen, an das BSI melden.

  Durch das IT-Sicherheitsgesetz wurden außerdem weitere Gesetze wie z. B. das Energiewirtschaftsgesetz geändert. Durch die Änderung des Energiewirtschaftsgesetz werden sämtliche Strom- und Gasnetzbetreiber verpflichtet, den IT-Sicherheitskatalog der Bundesnetzagentur umzusetzen und ein ISMS einzuführen.[27]

Strafrechtliche Aspekte[Bearbeiten | Quelltext bearbeiten]

Dieser Artikel oder Absatz stellt die Situation in Deutschland dar. Hilf mit, die Situation in anderen Staaten zu schildern.

Jegliches rechtswidrige Verändern, Löschen, Unterdrücken oder Unbrauchbar-Machen fremder Daten erfüllt den Tatbestand nach § 303a StGB (Datenveränderung). In besonders schweren Fällen ist dies auch nach § 303b I Nr. 1 StGB („Computersabotage“) strafbar und wird mit Haftstrafe von bis zu fünf Jahren oder Geldstrafe bestraft. Die Durchführung von DDOS-Attacken stellt seit 2007 ebenfalls eine Computersabotage dar, gleiches gilt für jegliche Handlungen, die zur Beschädigung eines Informationssystems führen, das für einen anderen von wesentlicher Bedeutung ist.

Das Ausspähen von Daten (§ 202a StGB), also die Erlangung des Zugangs zu fremden Daten, die hiergegen besonders geschützt sind, wird mit Haftstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. Das Abfangen fremder Daten in Netzen oder aus elektromagnetischen Abstrahlungen ist seit 2007 ebenfalls strafbar, anders als bei § 202a StGB kommt es hier nicht auf eine besondere Zugangssicherung an. Das sich Verschaffen, Erstellen, Verbreiten, Öffentlich-Zugänglichmachen etc. von sog. „Hackertools“ steht ebenfalls seit 2007 unter Strafe, wenn damit eine Straftat vorbereitet wird (§ 202c StGB).

Daten sind nach § 202a Abs. 2 in Verbindung mit Abs. 1 aber nur vor dem Ausspähen geschützt, wenn sie „besonders gesichert“ sind, um ein Ausufern des Tatbestandes zu vermeiden. Das heißt, erst wenn der Nutzer seine Daten technisch schützt, genießt er

auch den strafrechtlichen Schutz. Die frühere Debatte, ob das „Hacken“ ohne Abruf von Daten strafbar sei, ist hinfällig, seit der Wortlaut der Norm 2007 derart geändert wurde, dass Strafbarkeit bereits mit Erlangung des Zugangs zu Daten einsetzt. Weiter ist umstritten, ob die Verschlüsselung zur besonderen Sicherung zählt. Sie ist zwar sehr effektiv, aber es wird argumentiert, die Daten seien ja nicht gesichert, sondern lägen nur in „unverständlicher“ bzw. schlicht „anderer“ Form vor.

Als Computerbetrug wird nach § 263 a StGB mit Geldstrafe oder Freiheitsstrafe bis zu fünf Jahren bestraft, wenn Datenverarbeitungsvorgänge zur Erlangung von Vermögensvorteilen manipuliert werden. Schon das Erstellen, Verschaffen, Anbieten, Verwahren oder Überlassen dafür geeigneter Computerprogramme ist strafbar.

Zitate[Bearbeiten | Quelltext bearbeiten]

> „Ich glaube, dass es zunehmend wahrscheinlicher wird, dass wir bis 2017 einige katastrophale Systemfehler erleben. Noch wahrscheinlicher, wir werden von einem fürchterlichen Systemausfall betroffen sein, weil irgendein kritisches System mit einem nicht-kritischen verbunden war, das mit dem Internet verbunden wurde, damit irgendjemand an MySpace herankommt – und dieses Hilfssystem wird von Malware infiziert.“
>
> – Marcus J. Ranum, IT-Sicherheitsexperte[28]: zitiert nach Niels Boeing[29]

Siehe auch[Bearbeiten | Quelltext bearbeiten]

- Big Data
- Cyberkrieg
- Europäische Agentur für Netz- und Informationssicherheit
- Internetkriminalität, IT-Sicherheitsverfahren
- Need-to-know-Prinzip
- TeleTrusT

Literatur[Bearbeiten | Quelltext bearbeiten]

Dieser Artikel oder Abschnitt bedarf einer Überarbeitung. *Näheres ist auf der Diskussionsseite angegeben.* Hilf mit, ihn zu verbessern, und entferne anschließend diese

Markierung.

- IBM X-Force Threat Reports (*zweimal jährlich erscheinende Berichte zur IT- und Internetsicherheit, PDF-Downloads möglich – vgl.* Anja Schütz, Florian Kalenda: IBMs X-Report: „Im Internet kann man niemandem mehr trauen“. ZDNet.de, 27. August 2009)
- *Fokus: IT-Sicherheit*. In: *Technology Review*, Nr. 7/2009 (12 S. Sonderteil)
- Clay Wilson: *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. (PDF; 260 kB; 43 S.) Congressional Research Service, Update 29. Januar 2008
- *IT-Sicherheitsmanagement und IT-Grundschutz BSI-Standards zur IT-Sicherheit*. Bundesamt für Sicherheit in der Informationstechnik. In: *Bundesanzeiger*, 2005, ISBN 3-89817-547-2
- Steffen Wendzel, Johannes Plötner: *Praxisbuch Netzwerksicherheit*. Galileo Computing, 2007, ISBN 978-3-89842-828-6
- Ralf Röhrig, Gerald Spyra: *Information Security Management – Praxishandbuch für Aufbau, Zertifizierung und Betrieb*. Vierteljährliche Aktualisierung, TÜV Media GmbH, ISBN 978-3-8249-0711-3
- Claudia Eckert: *IT-Sicherheit. Konzepte – Verfahren – Protokolle*. 7., überarbeitete und erweiterte Auflage, Oldenbourg, München, 2012, ISBN 978-3-486-70687-1
- ENISA Quarterly on *Secure Software* (PDF; 2 MB)
- Gabriela Hoppe, Andreas Prieß: *Sicherheit von Informationssystemen. Gefahren, Maßnahmen und Management im IT-Bereich*. Verlag Neue Wirtschafts-Briefe 2003, ISBN 3-482-52571-4
- Heinrich Kersten, Klaus-Dieter Wolfenstetter: *Handbuch der Informations- und Kommunikationssicherheit* Fachverlag Deutscher Wirtschaftsdienst GmbH & Co. KG, Köln, 2000, ISBN 3-87156-403-6
- Stefan Kleinermann: *Schlüsselelemente der IT-Sicherheit aus Sicht des IT-Sachverständigen* proliteratur 2005, ISBN 3-86611-138-X
- Hans-Peter Königs: *IT-Risiko-Management mit System*. Vieweg 2005, ISBN 3-528-05875-7 (Ausführliche Rezension)
- Michael Mörike: *IT-Sicherheit*. dpunkt 2004, ISBN 3-89864-290-9
- Michael Mörike, Stephanie Teufel: *Kosten und Nutzen IT-Sicherheit*. dpunkt 2006, ISBN 3-89864-380-8

- Ulrich Moser: *Information Security. Sicherheitskonzepte für Unternehmen.* BPX.ch ICT-Fachverlag, Rheinfelden 2005, ISBN 3-905413-38-8
- Klaus-Rainer Müller: *IT-Sicherheit mit System*. 3. Auflage. Vieweg, 2008, ISBN 3-8348-0368-5
- Hartmut Pohl, Gerhard Weck: *Einführung in die Informationssicherheit*. Oldenbourg 1993, ISBN 3-486-22036-5
- Christoph Ruland: *Informationssicherheit in Datennetzen* VMI Buch AG, Bonn 1993, ISBN 3-89238-081-3
- Jürg Schneider: *Informationssicherheit in der IT und persönliche Haftung der Verwaltungsräte*. Bibliothek zur Zeitschrift für Schweizerisches Recht, Beiheft 48, Helbing Lichtenhahn Verlag, Basel 2008, ISBN 978-3-7190-2802-2
- Bruce Schneier: *Angewandte Kryptographie*. Pearson Studium, ISBN 978-3-8273-7228-4
- Bruce Schneier: *Beyond Fear*. Springer, ISBN 0-387-02620-7
- Bruce Schneier: *Secrets & Lies: IT-Sicherheit in einer vernetzten Welt*. dpunkt Verlag, 2004, ISBN 3-89864-302-6
- Markus Schumacher: *Hacker Contest*. Xpert.press, ISBN 3-540-41164-X
- Clifford Stoll: *Kuckucksei: Die Jagd auf die deutschen Hacker, die das Pentagon knackten*. Fischer Taschenbücher, ISBN 3-596-13984-8
- Görtz, Stolp: *Informationssicherheit im Unternehmen. Sicherheitskonzepte und -lösungen in der Praxis* Addison-Wesley 1999, ISBN 3-8273-1426-7
- Johannes Wiele: *Die Mitarbeiter als Firewall: Wie Sicherheitsbewusstsein entsteht. Über interne Awareness-Kampagnen bei SAP und Cisco*. In: *LANline*, 7/2005, S. 56, ISSN 0942-4172
- Gerd Wolfram: *Bürokommunikation und Informationssicherheit.* Vieweg, Wiesbaden 1986, ISBN 3-528-03604-4
- Allgemeine IT-Sicherheits Broschüre für Konsumenten (PDF; 1,7 MB)
- *Hacker's Guide*. Markt und Technik, ISBN 3-8272-6522-3
- *Hacking Intern*. Data Becker, ISBN 3-8158-2284-X
- *Sicherheitskultur im Unternehmen*. (PDF) Securitymanager.de Handbuch. Umfangreiche Artikelsammlung zur Informationssicherheit, Sicherheitskultur und Security Awareness
- *Maßnahmenkatalog und Best Practices für die Sicherheit von Webanwendungen*. (PDF) BSI, August 2006

- Andreas Pfitzmann: Scriptum *Sicherheit in Rechnernetzen: Mehrseitige Sicherheit in verteilten und durch verteilte Systeme* (PDF)
- *Hakin9 – Hard Core IT Security Magazin* ist ein Magazin, das zweimonatlich erscheint; es dokumentiert jeweils immer die neuesten Sicherheitsprobleme bzw. Lösungen.
- Michael Helisch, Dietmar Pokoyski, Kathrin Prantner: *Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung.* Vieweg+Teubner Verlag, 2009, ISBN 3-8348-0668-4

Weblinks[Bearbeiten | Quelltext bearbeiten]

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- BMWi: Task Force „IT-Sicherheit in der Wirtschaft“
- Seiten-Check der Initiative-S der Task Force „IT-Sicherheit in der Wirtschaft“ Service des eco Verband der Internetwirtschaft e.V gefördert durch das Bundesministerium für Wirtschaft und Technologie (BMWi)
- Deutschland sicher im Netz e. V.
- *A Users' Guide: How to raise information security awareness* (DE). Bundesamt für Sicherheit in der Informationstechnik, Juni 2006, ENISA (mit PDF *Leitfaden für die Praxis: Wege zu mehr Bewusstsein für Informationssicherheit*; 2 MB)
- DIN NIA-01-27 IT-Sicherheitsverfahren
- Christian Hawellek: *Die strafrechtliche Relevanz von IT-Sicherheitsaudits – Wege zur Rechtssicherheit vor dem Hintergrund des neuen Computerstrafrechts*. (PDF; 734 kB)
- Ken Thompson: *Reflections on Trusting Trust*. (PDF; 220 kB; englisch) Exzellenter Artikel über Softwaresicherheit und deren Untergrabung, etwa durch Trojaner.

Einzelnachweise[Bearbeiten | Quelltext bearbeiten]

1. ↑ *Hochspringen nach:a b c d e f* Claudia Eckert: *IT-Sicherheit. Konzepte – Verfahren – Protokolle.* 7., überarbeitete und erweiterte Auflage. Oldenbourg, 2012, ISBN 978-3-486-70687-1
2. *Hochspringen*↑ Einfache Darstellung der Informationssicherheit
3. *Hochspringen*↑ R. Shirey: RFC 4949, Internet Security Glossary, Version 2. IETF. S. 29. Abgerufen im 10. November 2011: „The property of being genuine and able to be verified and be trusted.“

4. ↑ *Hochspringen nach:a b* Carsten Bormann et al.: *Vorlesungsfolien 0.* In: *Vorlesung Informationssicherheit 1, SS 2005, Uni Bremen.* 16. April 2005, abgerufen am 30. August 2008 (PDF; 718 kB). Folie 25.
5. *Hochspringen*↑ Claudia Eckert: *Vorlesung IT-Sicherheit, WS 2002/2003, TU Darmstadt.* Vorlesungsfolien Kap. 2, Folie 17. TU Darmstadt FG Sicherheit in der Informationstechnik, 20. Oktober 2004, S. 26, archiviert vom Original am 3. Dezember 2013; abgerufen am 19. November 2010 (PDF; 6,8 MB). **Info:** Der Archivlink wurde automatisch eingesetzt und noch nicht geprüft. Bitte prüfe den Link gemäß Anleitung und entferne dann diesen Hinweis.
6. *Hochspringen*↑ Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Die Lage der IT-Sicherheit in Deutschland 2016*. Oktober 2016.
7. *Hochspringen*↑ Vergleiche auch ENISA Quarterly Vol. 2, No. 3, Oct 2006, ENISA, abgerufen am 29. Mai 2012
8. *Hochspringen*↑ Beschreibung der Softwarebeschränkungsrichtlinien in Windows XP, abgerufen am 9. August 2013.
9. *Hochspringen*↑ So wird's gemacht: Verwendung von Richtlinien für Softwareeinschränkung in Windows Server 2003, abgerufen am 9. August 2013.
10. *Hochspringen*↑ Using Software Restriction Policies to Protect Against Unauthorized Software, abgerufen am 9. August 2013.
11. *Hochspringen*↑ Using Software Restriction Policies to Protect Against Unauthorized Software, abgerufen am 9. August 2013.
12. *Hochspringen*↑ How Software Restriction Policies Work, abgerufen am 9. August 2013.
13. *Hochspringen*↑ Detaillierte Beschreibung der Funktion „Datenausführungsverhinderung" in Windows XP Service Pack 2, Windows XP Tablet PC Edition 2005 und Windows Server 2003, abgerufen am 9. August 2013.
14. *Hochspringen*↑ ENISA Quarterly, Q4 2007, vol. 3, no. 4, ENISA, abgerufen am 29. Mai 2012
15. *Hochspringen*↑ Urs E. Gattiker: *Why information security awareness initiatives have failed and will continue to do so*. (PDF; 279 kB) Präsentation auf der govcert.nl 2007 conference.
16. *Hochspringen*↑ Axel Tietz, Johannes Wiele: *Awareness ist nur ein Anfang*. In: *Informationsdienst IT-Grundschutz*, Nr. 5/6, Mai 2009, S. 28–30, (ISSN 1862-4375)
17. *Hochspringen*↑ Frank van der Beek: *Wie lehrt man IT-Sicherheit am Besten? Eine empirische Studie* (PDF; 2,4 MB). S. 17.

18. *Hochspringen*↑ Michael Falk: *IT-Compliance in der Corporate Governance: Anforderungen und Umsetzung.* Wiesbaden, Gabler Verlag, 2012, ISBN 3-8349-3988-9
19. *Hochspringen*↑ Thomas A. Martin: *Grundzüge des Risikomanagements nach KonTraG: Das Risikomanagementsystem zur Krisenfrüherkennung nach § 91 Abs. 2 AktG.* München, Oldenbourg, 2002. ISBN 978-3-486-25876-9
20. ↑ *Hochspringen nach:a b c d e* J. Hofmann, W. Schmidt: *Masterkurs IT-Management: Grundlagen, Umsetzung und erfolgreiche Praxis für Studenten und Praktiker.* 2., akt. und erw. Auflage. Vieweg+Teubner, 2010, ISBN 978-3-8348-0842-4.
21. *Hochspringen*↑ Heinrich Kersten, Jürgen Reuter, Klaus-Werner Schröder, Klaus-Dieter Wolfenstetter: *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung.* 4., akt. u. erw. Auflage. Springer, Wiesbaden 2013, ISBN 978-3-658-01723-1.
22. *Hochspringen*↑ Erste Richtlinie 73/239/EWG des Rates vom 24. Juli 1973 zur Koordinierung der Rechts- und Verwaltungsvorschriften betreffend die Aufnahme und Ausübung der Tätigkeit der Direktversicherung (mit Ausnahme der Lebensversicherung), abgerufen am 9. Januar 2014
23. *Hochspringen*↑ Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 22. Mai 2001 (BGBl. I S. 904)
24. *Hochspringen*↑ M.J. Kenning: *Security Management Standard: ISO 17799/BS 7799.* In: *BT Technology Journal*, 19, 2001, Nr. 3, S. 132–136.
25. *Hochspringen*↑ Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17. Juli 2015 (BGBl. I S. 1324)
26. *Hochspringen*↑ Bundesministerium der Justiz und Verbraucherschutz: *KritisV.* 22. April 2016, abgerufen am 22. Juli 2016.
27. *Hochspringen*↑ Bundesnetzagentur: *IT-Sicherheitskatalog.* Abgerufen am 22. Juli 2016 (PDF).
28. *Hochspringen*↑ Marcus J. Ranum (Website)
29. *Hochspringen*↑ Niels Boeing: Blitz und Donner in der Matrix („Technology Review“, deutsche Ausgabe, 25. Januar 2008)