

IT-Sicherheit

Authority
Klaus Lipinski (Hrsg.)

2. Identitätsprüfung

4. Veröffentlichung von
Zertifikaten und CRLs

Registration
Authority

Zertifikats-
antrag

3. Zertifikats-
ausgabe

5. Abfrage
Zertifikaten
CRLs

Zertifikats-
antrag

DAT@COM

Inhalt

Abhörsicherheit
Anwendungssicherheit
Asset Classification and Control
Bluetooth-Sicherheit
BS 7799
BSI, Bundesamt für Sicherheit in der Informationstechnik
Business Continuity and Disaster Recovery Planning
CC, common criteria
Compliance
Computer and Network Management
Content-Sicherheit
CRAMM, computer risk analysis and management method
Datensicherheit
EAL, evaluation assurance level

Informationssicherheit
Informationssicherheits- Managementsystem
Internet-Sicherheit
ISO 17799
IT-Sicherheit
ITSEC, information technology security evaluation criteria
Netzwerksicherheit
Perimeter-Sicherheit
Personal Security
Persönliche Sicherheitsumgebung
Physical and Environmental Security
PnP-Sicherheit
Security Organization
Security Policy
Sicherheit

Sicherheits-ID
Sicherheitsarchitektur
Sicherheitsdienst
Sicherheitsinfrastruktur
Sicherheitsmanagement
Sicherheitspolitik
Sicherheitsrichtlinie
Sicherheitsstufe
Sicherheitsvereinbarung System Access Control
System Development and Maintenance
TCSEC, trusted computer security
VM, vulnerability management
WAS, web application security
WLAN-Sicherheit
Zentralstelle für die Sicherheit in der Informationstechnik, ZSI

Impressum:

Herausgeber: Klaus Lipinski

IT-Sicherheit V1

Copyright 2007

DATAKOM-Buchverlag GmbH

84378 Dietersburg

Alle Rechte vorbehalten.

Keine Haftung für die angegebenen Informationen.

Produziert von Media-Schmid

www.media-schmid.de

Abhörsicherheit *bug proof* Unter Abhörsicherheit versteht man ganz allgemein die *Sicherheit* gegen unberechtigtes Mithören von Dritten bei der Übertragung zwischen Endteilnehmern. In der Regel handelt es sich um eine Sprachübertragung, die durch das Fernmeldegeheimnis geschützt ist.

Bei der Mobilkommunikation in GSM-Netzen, bei der die Luftschnittstelle offen ist, werden zu diesem Zweck alle Gespräche individuell verschlüsselt. Als Verschlüsselungs-Algorithmus wird ein teilnehmereigener Primzahlen-Algorithmus verwendet, der sich auf der SIM-Karte befindet, aber nicht ausgelesen werden kann.

Anwendungssicherheit *application security* Der Schutz der Anwendungsebene ist ein wesentlicher Aspekt der *IT-Sicherheit*, da die Angriffe über Web-Applikationen erfolgen und nicht unmittelbar erkennbar sind. Die Angriffe reichen von Datendiebstahl über Wirtschaftsspionage und Datenmissbrauch bis hin zu Vandalismus. So können auf dieser Ebene Dateien mit unternehmenskritischen Informationen und schützenswerten Zugriffsberechtigungen entnommen oder E-Commerce auf fremden Accounts missbräuchlich ausgeführt werden.

Application *Security* dient dem präventiven Schutz und kann durch Erkennen von IT-Risiken in die Applikationsebene implementiert werden. Bei der Anwendungssicherheit wird der Inhalt der Datenpakete überprüft und nicht der Header.

Ansatzpunkte liegen in der genutzten Software, in einer möglichen Authentifizierung bei der Anwendung oder durch geeignete Verschlüsselungsmaßnahmen. So kann man beispielsweise Angriffe, die gleichartig ablaufen wie das Cross Site Scripting (XSS), durch Einbau entsprechender Codes abwehren.

Asset Classification and Control “Asset Classification and Control” ist Kapitel 3 des Sicherheitsstandards *BS 7799*. Die in diesem Kapitel definierten Aufgaben umfassen den Schutz von gemeinsamen Vermögenswerten und Informationen. Es handelt sich um die Aktivwerte des Besitzers, die Bestandsaufnahme, die Klassifizierung der Information, die Kennzeichnung und Bearbeitung der Information und nicht veröffentlichte Vereinbarungen.

Bluetooth-Sicherheit Bluetooth kennt drei *Sicherheitsstufen*: die erste Stufe, *Security-Mode 1*, hat keine Sicherheitsmechanismen, die Geräte erkennen sich und können ohne Authentifizierung miteinander kommunizieren. Der *Security-Mode 2* kennt flexible Zugriffe für unterschiedliche Sicherheitsanforderungen. Die Geräte erkennen sich, können aber ohne Authentifizierung keine Verbindung zueinander herstellen. In *Security-Mode 3* werden die Sicherungsprozeduren bereits beim Verbindungsaufbau initialisiert, der mit dem Verbindungsschlüssel ausgeführt wird. Darüber hinaus dient dieser 128 Bit lange Schlüssel zur Generierung des Sitzungsschlüssels oder Link Key mit dem auch die Geräte authentifiziert werden. Beim Link Key kann es sich um einen Kombinationsschlüssel handeln, gewonnen aus der Schlüsselkombination zweier Geräte. Es kann sich aber auch um einen Geräteschlüssel handeln, einem für ein Bluetooth-Gerät festgelegten Schlüssel, um einen temporären Schlüssel, der nur für die aktuelle Sitzung benutzt werden kann, oder um einen Initialisierungs-Schlüssel zum Schutz der Verbindungsparameter bei der Übertragung handeln.

BS 7799 Der British Standard BS 7799 von 1995 führt die offizielle Bezeichnung “Code of Practise for Information *Security* Management” und bildet die Prüfungsgrundlage für die Sicherheit von IT-Systemen. Der britische Standard bildet eine international anerkannte Norm für die Bewertung der Sicherheit von IT-Umgebungen. Aus diesem Standard ist der internationale Standard *ISO 17799* hervorgegangen, der als Referenzdokument für die Erstellung eines *Informationssicherheits-Managementsystems* (ISMS) dient. Das Ziel dieser Norm ist die Einführung eines Prozessansatzes, mit dem ein organisationsbezogenes ISMS entwickelt, umgesetzt, überwacht und verbessert werden kann.

Bei den Zertifizierungen nach BS 7799 steht das gesamte IT-System auf dem Prüfstand und wird auf vorhandenes Risikopotenzial hin untersucht; und nicht einzelne Anwendungen, Subsysteme oder Dateien. Der Schutz sensibler Daten und wichtiger Geschäftsprozesse stehen im Vordergrund.

Wichtige Aspekte des Standards sind die Definition, Spezifikation und Implementierung eines Informationssicherheits-Managementsystems (ISMS), die



Entwicklung organisationsbezogener Normen und Praktiken hinsichtlich der *Informationssicherheit* sowie die Überwachung der Einhaltung von Vereinbarungen an die Informationssicherheit. Der Standard besteht aus zehn Kapiteln, die die Grundlagen für den praktischen Einsatz bilden:

Security Policy,
Security Organization,
Asset Classification and Control,
Personal Security,
Physical and Environmental Security,
Computer and Network Management,
System Access Control,
System Development and Maintenance,
Business Continuity and Disaster Recovery Planning,
Compliance.

ISO 17799, das das Management von Informationssicherheit beschreibt, schafft die

Sicherheitskonzept Voraussetzungen für die Zertifizierung eines ISMS-Systems.

Der Standard BS 7799 besteht aus zwei Teilen:

Teil 1: Leitfaden zum Management von Informationssicherheit,

Teil 2 von 1999: Spezifikation für Managementsysteme der Informationssicherheit.

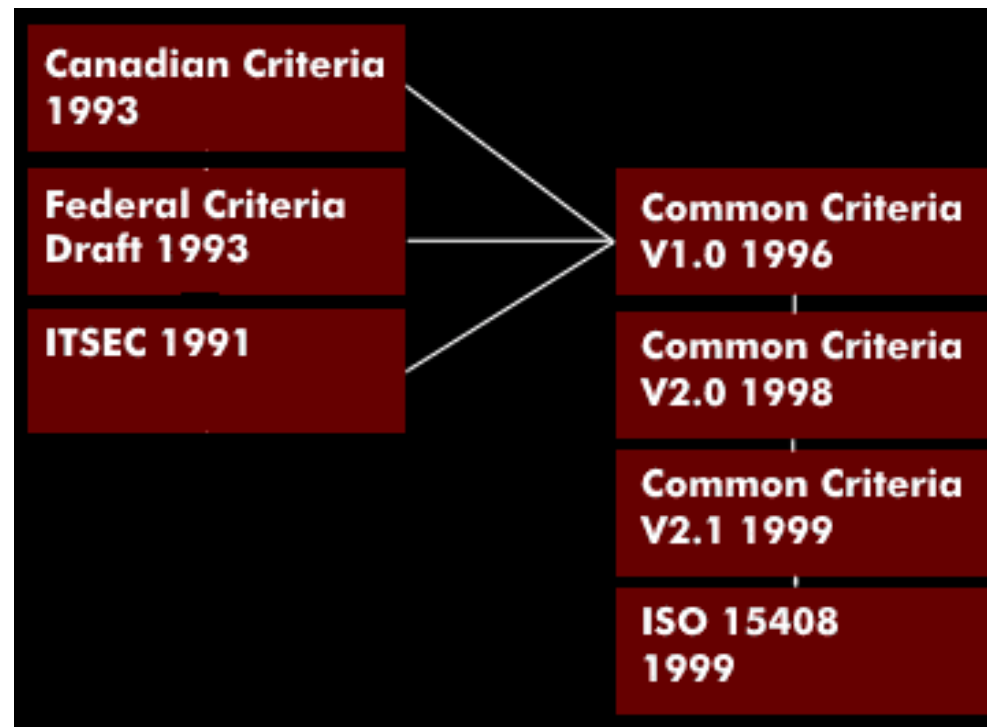
Im Jahre 2002 wurde der zweite Teil an internationale Management-Standards und die OECD-Richtlinien angepasst. Damit können Unternehmen einen Sicherheitsprozess etablieren, der den Sicherheitswert systematisch auf einem zu definierenden Niveau verbessert.

Das von der ISO im Herbst 2005 herausgegebene Regelwerk ISO 27000 beinhaltet die Aspekte von BS 7799 und löst dieses ab.

<http://www.thewindow.to/bs7799/index.htm>

- BSI, Bundesamt für Sicherheit in der Informationstechnik**
GISA, German information security agency
- Das Bundesamt für *Sicherheit* in der Informationstechnik (BSI) wurde 1991 gegründet, um die Entwicklung von Technologien für sichere IT-Netze zu fördern. Schwerpunkte der BSI-Aktivitäten sind der Schutz gegen Computer-Viren, die elektronische Signatur, die *Internet-Sicherheit*, der IT-Grundschutz und das E-Government. Verschiedenen Arbeitsgruppen befassen sich mit der Fortentwicklung des E-Government, der Bereitstellung von Computer-Dienstleistungen für Bundesbehörden sowie der Sicherheit des Internet. Das BSI erstellt Dokumente für die genannten Schwerpunkte, die über das Internet abgerufen werden können.
<http://www.bsi.de>
- Business Continuity and Disaster Recovery Planning**
- “Business Continuity and Disaster Recovery Planning”, Kapitel 9 des Sicherheitsstandards *BS 7799*, dient der Fortführung der Geschäftsplanung und -prozesse.
Das Business Continuity Planning umfasst die Risiko-Analyse, die Planung für die kontinuierliche Fortführung der Geschäftsaktivitäten, die Implementierung von Organisationsstrategien und die Verifizierung der Effizienz. In diesem Konzept werden die fortgeschrittenen Planungen und Vorbereitungen getroffen, die notwendig sind um das Verlustpotential zu identifizieren. Darüber hinaus werden die rentablen Wiederherstellungsstrategien formuliert und implementiert, sowie die Wiederherstellungspläne entwickelt, die die organisatorischen Dienste für den Notfall sichern.
- CC**
common criteria
- “Common Criteria for Information Technology *Security* Evaluation” (CC) ist die Weiterentwicklung von *ITSEC*, der *TCSEC* der USA und der kanadischen CTCPEC. Es handelt sich um weltweit anerkannte Sicherheitsstandards für die Bewertung und Zertifizierung informationstechnischer Systeme.
Die Common-Criteria-Zertifizierung wurde 1998 von den Regierungsstellen in den USA, Kanada, Deutschland, Großbritannien und Frankreich begründet und bereits von mehreren anderen Ländern übernommen. Dabei hat das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) bei der Entwicklung der Common Criteria

Entwicklung der Common Criteria (CC)



eine aktive Rolle übernommen. Die Common Criteria wurden von der NIST veröffentlicht und sind international von der ISO standardisiert. Der Standard ISO 15408 beschreibt die Bewertung der Sicherheitsfunktionen von IT-Produkten. In den Common Criteria werden der Geltungsbereich für die sicherheitsrelevante Evaluierung beschrieben, darüber hinaus die funktionalen Anforderungen in

Zusammenhang mit der Bedrohung und den Sicherheitszielen und die Anforderungen an die Vertrauenswürdigkeit.

Die Klassifizierung der IT-Sicherheitsprüfung im Rahmen der Common Criteria erfolgt in sieben so genannten EAL-Stufen, die auch als Schutzprofile bezeichnet werden. Diese reichen von EAL1 für unzureichendes Vertrauen bis hin zu EAL7 für den formal verifizierten Entwurf und Test des IT-Equipments.

<http://www.bsi.bund.de/cc/>

Compliance Der Begriff Compliance umschreibt ein regelkonformes Verhalten eines Unternehmens in Bezug auf die gesetzlichen und regulativen Bestimmungen. Die Compliance soll sicherstellen, dass die unternehmerischen Risiken erkannt, bewertet und durch die Implementierung technischer Lösungen erfüllt werden.

Die Rechtskonformität betrifft in gleichem Maße die handelsrechtliche und steuerrechtliche Dokumentation von Vorgängen, aber ebenso sicherheitsrelevante Lösungen der elektronischen Kommunikation und vor allem der Archivierung.

Einschlägige Richtlinien für sicherheitstechnische Konformität finden sich in dem *British Standard BS 7799*, dem IT-Grundschutzhandbuch des deutschen

Bundesamtes für *Sicherheit* in der Informationstechnik (BSI/GsHb), in den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) und in den Grundsätzen für ordnungsgemäße DV-gestützte Buchführungssysteme (GoBS).

An weiteren Richtlinien und Gesetzen, die unternehmensspezifische Aspekte berücksichtigen, sind Basel II zu nennen, in denen die Eigenkapitalvorschriften festgelegt sind, die International Financial Reporting Standards (IFRS) für die Rechnungslegungen, das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) mit der die Corporate Governance in deutschen Unternehmen verbessert werden soll und den Sarbanes-Oxley-Act, der bei international tätigen Unternehmen die Bilanztransparenz erhöht.

Computer and Network Management

“Computer & Network Management“ bildet das Kapitel 6 des britischen Sicherheitsstandards *BS 7799* für das Informationssicherheits-Management. Die in diesem Kapitel definierten Ziele sind die Sicherstellung des korrekten und sicheren Betriebs der IT-Anlage, die Systemfehler auf ein Minimum zu reduzieren, die Integrität von Software und Informationen zu schützen und die Integrität und Verfügbarkeit der Informationsverarbeitung und -übertragung zu erhalten. Darüber hinaus sind die Kommunikationsnetze und Infrastruktur zu schützen, Unterbrechungen in der Informationsverarbeitung ebenso wie die Beschädigung von Aktiva und der Verlust, die Änderungen oder der Missbrauch von Informationen, die zwischen verschiedenen Organisationen ausgetauscht werden, zu verhindern.

Content-Sicherheit *content security*

Die *Content-Security* befasst sich mit dem Schutz der Informationen vor allen bekannten Viren, Würmern und Trojanern, sowie mit der Erkennung von neuen Gefahren und die Verhinderung von Spam-Mails. Zur *Content-Security* gehören Sicherheitslösungen für die Abwehr von Hackerangriffen, die über Sicherheitslücken in Netzwerken und Anwendungen Schaden anrichten.

Bei der *Content-Security* werden die Daten hinsichtlich ihrer Integrität geprüft; des Weiteren wird geprüft ob sie verschlüsselt gesendet, empfangen und genutzt werden

dürfen. Diese Sicherheitsprüfungen erfolgen nach einem festgelegten Regelwerk, den Policies, mit dem organisatorische und personenspezifische Kenndaten überprüft werden.

Die Maßnahmen für die Content-Security reichen von Anti-Virus-Programmen mit denen der Web-Verkehr und alle E-Mails gescannt werden, über die Abwehr von Hackerangriffen bis hin zu nachgeschalteten Anti-Spam-Filtern, Web-Filtern und E-Mail-Filtern. Wobei die Web-Filterung unerwünschte Webseiten ausfiltert und die E-Mail-Filterung die E-Mails inhaltsabhängig nach Text- und Anhängen durchsucht und entsprechend ausfiltert.

CRAMM *computer risk analysis and management method* CRAMM ist ein bereits 1987 vorgestelltes Software-Paket für das wissenbasierte Risiko-Management, das dem britischen Sicherheitsstandard *BS 7799* entspricht und nach *ISO 17799* zertifiziert ist.

CRAMM basiert auf einer toolgestützten Struktur mit der Geschäftsprozesse modelliert und *Schwachstellen* in IT- und Kommunikationssystemen bewertet werden können. Darüber hinaus kann CRAMM Sicherheitsvorschläge unterbreiten, Notversorgungsmaßnahmen planen, *ISMS* generieren und zu schützende Objekte identifizieren. Mit dem Ergebnis, das als Report ausgegeben werden kann, kann das Management Schwachstellen und Risiken in den IT-gestützten Geschäftsprozessen, in Software und Hardware, Netzwerken, Personal, Gebäude u.a. erfassen, bewerten und beseitigen.

Datensicherheit *data security* Gesetzliche Regelungen und technische Maßnahmen, durch die die unberechtigte Speicherung, Verarbeitung und Weitergabe schutzwürdiger Daten verhindert werden soll. Ziel ist es, die Persönlichkeitsrechte des Menschen vor den Folgen der Erfassung seiner Individualdaten bei der manuellen und automatischen Datenverarbeitung zu schützen. Innerhalb eines Betriebs gehören dazu personelle, organisatorische und revisionstechnische Regelungen, außerdem geräte- und programmtechnische Schutzmechanismen.

Datenschutz, Datenintegrität und Datensicherung bilden die verlässliche

Informationsverarbeitung. In Deutschland ist der Datenschutz durch das "Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung" vom 27.1.1977 im Bundesdatenschutzgesetz (BDSG) verankert. Gewerbliche oder staatliche Computeranwender mit schutzbedürftigen Daten müssen Datenschutzbeauftragte einsetzen.

Darüber hinaus gibt es in Deutschland das Bundesgesetz über den Datenschutzgesetz vom 19.06.1992. Es lautet: "Wer personenbezogene Daten für sich selbst oder im Auftrag für andere elektronisch bearbeitet, muss durch geeignete Maßnahmen den Verlust und den Missbrauch dieser Daten verhindern".

EAL
evaluation assurance level

*Sicherheitslevels nach
ITSEC und
Common Criteria (CC)*

ITSEC	CC	Security Evaluation
0	EAL1	Functional Tested
1	EAL2	Structural Tested
2	EAL3	Methodically tested and proofed
3	EAL4	Methodically developed, tested and proofed
4	EAL5	Semiformal developed and tested
5	EAL6	Semiformal verification of the design
6	EAL7	Formal verification of the design

Die EAL-Stufen kennzeichnen die Vertrauenswürdigkeit in eine Sicherheitsleistung. Im Rahmen der Common Criteria (CC) werden sie für die Bestimmung der Sicherheitsprüfungen verwendet. Es gibt sieben

EAL-Stufen, die mit den Ziffern 1 bis 7 gekennzeichnet sind und mit steigender Ziffer einen höheren Sicherheitsstandard repräsentieren. So bietet die EAL-Stufe EAL1 ein unzureichendes Vertrauen in die IT-Sicherheitsprüfungen, EAL7 hingegen das höchste. Anhand der EAL-Stufen ist eine Vergleichbarkeit der Sicherheitsfunktionalitäten von Programmen und Systemen gegeben. Allerdings sind bei der Bewertung der Sicherheitsleistungen die Schwachstellen, über die Eindringlinge in das oder Attacken auf das System ausgeführt werden können, zu analysieren.

Informationssicherheit
information security

Informationssicherheit ist der Präventivschutz für Persönlichkeits- und Unternehmens-Informationen. Ein solcher Schutz bezieht sich gleichermaßen auf Personen,

Unternehmen, Systeme und Prozesse und wird durch Integrität, Verfügbarkeit, Vertraulichkeit, Verbindlichkeit und Authentizität erzielt. Die Informationssicherheit soll den Verlust, die Manipulation, den unberechtigten Zugriff und die Verfälschung von Daten verhindern. Die Basis für die Informationssicherheit kann durch konzeptionelle, organisatorische und operative Maßnahmen erreicht werden. Dazu gehört die Umsetzung von sicherheitsrelevanten Grundsätzen eines Unternehmens, die so genannte Informationssicherheitspolitik. In dieser sind die Ziele des Unternehmens und die Realisierung festgelegt.

Ein wichtiger Ansatz für die *Sicherheit* von Informationssystemen ist der *British Standard BS 7799* sowie der ISO-Standard 17799 als Implementierungsleitfaden. Diese beiden Sicherheitsstandards werden in den Security-Normen ISO 27000 und 27001 vereint.

Informationssicherheits- Managementsystem *ISMS, information security management system*

Ein Informationssicherheits-Managementsystem (ISMS), das nach dem ISO-Standard 27000, bzw. früher nach *BS 7799* zertifiziert wurde, erfüllt die Voraussetzungen für ein qualifiziertes *Sicherheitsmanagement*. Ein solches ISMS-System, bestehend aus Richtlinien, Maßnahmen und Tools, beherrscht spezifische IT-Risiken und garantiert die geforderte *IT-Sicherheit*.

Bedingt durch die zunehmende Vernetzung von IT- und Kommunikationssystemen werden der Datenschutz und die *Datensicherheit* zu einem wichtigen unternehmerischen Aspekt.

Ein ISMS-System muss in allen Hierarchieebenen eines Unternehmens implementiert sein und von Verantwortlichen betreut werden.

Internet-Sicherheit *Internet security*

Als weltweit größter Netzverbund bietet das Internet Angreifern hinreichende Möglichkeiten, sich unberechtigten Zugriff auf Datenbestände und Ressourcen zu verschaffen, Datenbestände und übertragene Daten zu manipulieren und zu sabotieren. Die technischen Möglichkeiten für das unberechtigte Eindringen in fremde Datenbestände reichen vom Abhören von Passwörtern, über das IP-Spoofing, bei dem sich der Eindringling einer gefälschten IP-Adresse bedient, über das IP-Hijacking, bei

dem der Angreifer eine bestehende IP-Verbindung übernimmt, den Replay-Angriff, bei dem der Angreifer gezielt vorher gesammelte Informationen einsetzt, um dadurch fehlerhafte Transaktionen auszuführen, über das SYN-Flooding, einem gezielten Angriff auf den Server, um diesen durch Überlast von seinen eigentlichen Aufgaben abzulenken, bis hin zum Man-in-the-Middle-Angriff, einer Attacke, bei der die Kommunikation zwischen zwei Partnern abgefangen und manipuliert wird.

ISO 17799 Der im Jahre 2000 verabschiedete internationale Standard ISO 17799 für die *IT-Sicherheit* ist aus dem *British Standard BS 7799* hervorgegangen. Der Standard mit dem Titel “Code of Practice for *Information Security Management*” bietet eine Auswahl an Kontrollmechanismen, die auf Methoden und Verfahren basieren, die sich in der IT-Sicherheit bewährt haben. In dem Standard werden keine konkreten Sicherheitslösungen empfohlen; allerdings sollten Unternehmen und Organisationen aller Branchen die im Standard aufgeführten Richtlinien beachten und umsetzen. Die ISO hat mit ISO 17799 ein formelles Anerkennungs- und Zertifizierungsverfahren für die Einhaltung der Standards eingeführt, wodurch sich die allgemeine Qualität des Standards verbessert hat. Dieser Standard, der den ersten Teil von BS 7799 umfasst, ist weltweit akzeptiert. Im Jahre 2005 wurde ISO 17799 überarbeitet und in der neuen Fassung als ISO 27000 veröffentlicht.

ISO 17799 ist eine Sammlung von Empfehlungen für die IT-Sicherheit, die sich in der Praxis bewährt haben und in allen Hierarchieebenen von Unternehmen, Institutionen und Organisationen eingesetzt werden können. Da die Vielfalt der Sicherheitsaspekte von der Systemumgebung und der Unternehmensorganisation geprägt ist, ist der ISO 17799 ein flexibler Standard, der eigene Interpretationen zulässt.

IT-Sicherheit Die *IT-Sicherheit* tangiert alle Maßnahmen zur Verringerung des Gefährdungspotenzials für IT-Anwendungen und -Systeme. Alle mit dem Gefährdungspotenzial in Zusammenhang stehenden Schutzmaßnahmen, wie die Entwicklung von Sicherheitskonzepten, die Vergabe von Zugriffsberechtigungen und die Implementierung von Sicherheitsstandards, sind Aspekte der IT-Sicherheit. *IT security*

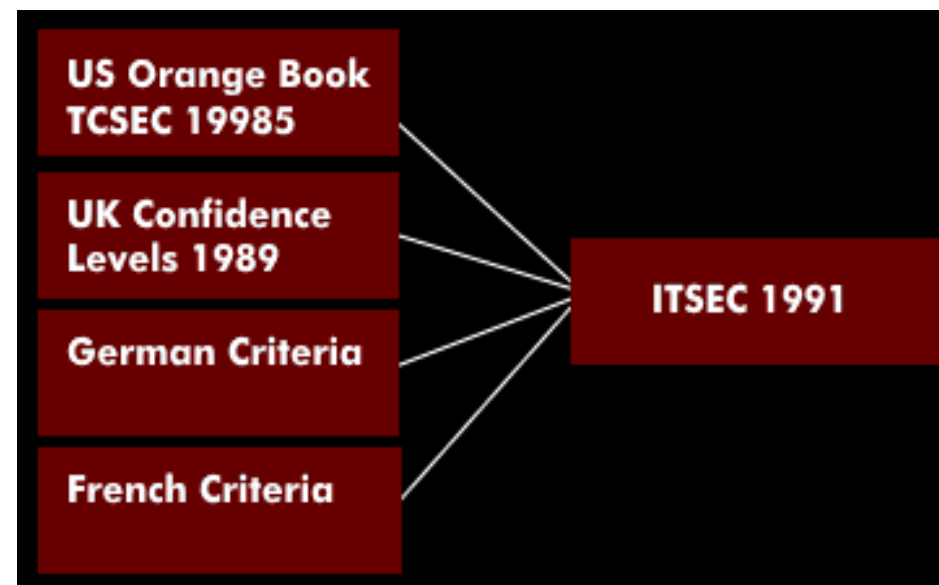
Sicherheit ist die technische Umsetzung der Sicherheitskonzepte unter wirtschaftlichen Aspekten.

Die IT-Sicherheit umfasst alle gefährdeten und daher schützenswerten Einrichtungen, Systeme und Personen. Dazu gehören u.a. Gebäude, Netze, Hardware und Software sowie die an den Systemen Arbeitenden. Ziel der IT-Sicherheit ist es, die Verfügbarkeit von Systemen und Daten sicherzustellen, die Vertraulichkeit zu gewährleisten, damit weder Unbefugte auf Dateien zugreifen können und die Dateien auch bei der Übertragung weiterhin vertraulich bleiben, die Sicherstellung der Authentizität und der Integrität der Daten.

Für die physikalische IT-Sicherheit gibt es mehrere nationale und europäische Standards, so die Definition der Brandabschnitte nach DIN 4102 oder die in den EN-1047-Standards spezifizierten Belastungsgrenzen für Daten und Systeme. Darüber hinaus gibt es Richtlinien und Güteklassen für den Einbruchschutz mit der Beschreibung des Mauerwerks.

ITSEC *information technology security evaluation criteria*

Die Information Technology *Security* Evaluation Criteria (ITSEC) sind europäische Sicherheitsstandards, die der Bewertung und Zertifizierung der Sicherheit von IT-Systemen dienen. ITSEC ist aus verschiedenen europäischen *Sicherheitsrichtlinien*, den UK Confidence Levels, German Criteria, French Criteria und dem US Orange Book *TCSEC* hervorgegangen.



Die Kriterien sind in einem Katalog zusammengefasst und sind nur für den europäischen Raum gültig. Das Vertrauen in die *Sicherheitsstufen* von ITSEC ist in so genannte Evolutionsstufen gegliedert. Es gibt die Stufen E0, was ein unzureichendes Vertrauen widerspiegelt, bis E6 für höchstes Vertrauen. Je höher die Evolutionsstufe, desto fachkundiger sind

Entwicklung der ITSEC

die Eindringlinge. Die Evaluierung beinhaltet die Prüfung und Bewertung der Sicherheitseigenschaften eines IT-Produkts nach den festgelegten Sicherheitskriterien. Die Weiterentwicklung des ITSEC sind die *Common Criteria* for Information Technology Security Evaluation.

Die ITSEC, die 1991 von der EU-Kommission verabschiedet wurde und vom Bundesamt für Sicherheit in der Informationstechnik (*BSI*) angewendet wird, ist das europäische Gegenstück zur amerikanischen TCSEC. Aus beiden wurden die Common Criteria (CC) entwickelt.

Netzwerksicherheit *network security*

Die Netzwerksicherheit ist eine Symbiose aus Richtlinien und Vorschriften, aus Produkten und Diensten. Sie tangiert alle Unternehmensebenen, vom Benutzer über den Administrator bis hin zur Unternehmensführung. Es ist ein Maßnahmenkatalog in Form einer *Security Policy*, die dafür sorgen muss, dass die Zugriffsberechtigung, Autorisierung, Identifikation und Authentifizierung verwaltet werden, dass jede Attacke, jeder unerlaubte Zugriff, jede Art der Sabotage, der Manipulation, des Missbrauchs und der Beeinflussung der Datenbestände und Ressourcen verhindert oder unmittelbar erkannt wird und dass das Einschleusen von Viren, Würmern oder Trojanern, DoS-Attacken oder IP-Spoofing nicht möglich ist. Ausgehend von einem solchen Maßnahmenkatalog können technische Lösungen implementiert werden.

Perimeter-Sicherheit *perimeter security*

Perimeter-Sicherheit betrifft die Sicherheit am Übergang zwischen dem Unternehmensnetz und dem Internet. Für die Perimeter-Sicherheit sind bestimmte Richtlinien definiert, die die IT-Technik des Unternehmens gegen das Gefahrenpotential schützen, das durch Viren, Würmer und Hacker verursacht wird. Zu den in den Richtlinien genannten Möglichkeiten gehören Firewalls, Virens Scanner und Anti-Viren-Software sowie Web-Filtertechniken.

Personal Security

Die *Personal Security* bildet das Kapitel 4 des britischen Sicherheitsstandards *BS 7799* für das Informationssicherheits-Management. Die Ziele dieses Kapitels liegen in

der Reduzierung Risiken, die durch menschliches Versagen verursacht werden können, so durch Diebstahl, Betrug oder Fehlbedienungen von Geräten und Einrichtungen. Es muss sichergestellt werden, dass sich die Benutzer der Bedrohung der *Informationssicherheit* bewusst sind und entsprechend ausgestattet sind um die *Sicherheitspolitik* des Unternehmens in ihre tägliche Arbeit einzubringen.

**Persönliche
Sicherheitsumgebung**
*PSE, personal security
environment*

In dem Personal *Security* Environment (PSE) sind persönliche sicherheitsrelevante Informationen gespeichert. Das sind alle schützenswerten Informationen eines Benutzers: die kryptografischen Schlüssel, Zertifikate und einige den Benutzer betreffende Kontrollinformationen. Physikalische Träger solcher geheim zu haltenden Sicherheits-Informationen sind Speichermedien wie Disketten, Compact Discs (CD) oder Smartcards. Einige PSE-Informationen können frei zugänglich, wie der Name oder das Zertifikat, andere hingegen können mit PIN oder Passwort geschützt. Die PSE wird u.a. bei der digitalen Signatur angewendet. Eine Schnittstelle für PSEs ist PKCS in der Version PKCS#11.

**Physical and
Environmental Security**

“Physical and Environmental *Security*” bildet das Kapitel 5 des britischen Sicherheitsstandards *BS 7799* für das Informationssicherheits-Management. Die in diesem Kapitel definierten Ziele sollen den unberechtigten Zugriff und die Beeinträchtigung der geschäftlichen Aktivitäten verhindern. Dazu gehören der Verlust und die Beschädigung von Aktivposten sowie die Unterbrechung der Geschäftsaktivitäten, der Diebstahl von Informationen und informationsverarbeitenden Einrichtungen.

PnP-Sicherheit
plug and play security

Plug-and-Play ist ein Schnittstellenkonzept für das konfliktfreie Anschließen von Peripheriegeräten an einen Personal Computer. Das schnelle Erkennen der angeschlossenen Peripheriegeräte bietet aber nicht nur Vorteile, sondern auch diverse Risiken, da durch unberechtigten Zugriff wichtige Daten aus den Personal Computern (PC) kopiert, ebenso aber auch Daten, Viren und Trojaner über die Plug-and-Play-Schnittstelle in das Firmennetz eingespeist werden können. In diesem

Zusammenhang darf die Entwicklung der Mobilspeicher wie dem USB-Stick nicht außer Acht gelassen werden. Dieses Risiko wird durch drahtlose Schnittstellen wie Wireless-USB noch erhöht, da der Anwender häufig nicht erkennen kann, wer mit seinem Computer gerade kommuniziert. Die Betriebssysteme bieten keine Möglichkeit der Schnittstellenkontrolle.

Sicherheitsaspekte von Schnittstellen ist daher ein Thema der Netzwerk- und *IT-Sicherheit*. Bei der Absicherung der Schnittstellen kommt es auf die konsequente Umsetzung der Sicherheitsregeln an. Diese Umsetzung kann durch Sicherheitsmodule vorgenommen werden, die die Nutzung der PnP-Geräte überwachen. Die Echtzeitüberwachung von Schnittstellen und Peripheriegeräten ist ein Punkt bei der Lösung der Schnittstellen-Sicherheitsproblematik, die automatische Geräteerkennung und schnelle Freigabe ein weiterer. Die PnP-Geräte, die eine Zugangsberechtigung haben, werden zentral oder direkt am Arbeitsplatz über Fernzugriff registriert. Die Einstellungen können entweder direkt im Active Directory von Windows oder im NetWare Directory Service (NDS) zentral verwaltet werden.

Security Organization Die *Security Organization* bildet das Kapitel 2 des britischen Sicherheitsstandards *BS 7799* für das *Sicherheitsmanagement*. In diesem Kapitel werden die *Sicherheitsrichtlinien* zur Aufbau- und Ablauforganisation beschrieben. Ein definiertes Ziel ist die Handhabung der *Informationssicherheit* innerhalb des Unternehmens. Dieses Ziel dient der Erhaltung der Sicherheit von informationsverarbeitenden Prozessen und der Sicherheit der Informationen auf die von dritter Seite zugegriffen werden kann. Darüber hinaus dient es zur Erhaltung der *IT-Sicherheit*, beim Outsourcen der Informationsverarbeitung.

Security Policy Die *Security Policy* bildet das Kapitel 1 des britischen Standards *BS 7799* für das *Sicherheitsmanagement*. In diesem Kapitel werden die Richtlinien für das Management und für die Betreuung der *IT-Sicherheit* beschrieben. Darüber hinaus befasst sich RFC 2196 mit der Definition der Security Policy. Generell enthält die Secure Policy die Richtlinien und Vorschriften, die die Personen

beachten müssen, die Zugang zu Datenbeständen, Systemen und Ressourcen haben.

Sicherheit
security Unter Sicherheit sind alle technischen und organisatorischen Maßnahmen zu verstehen die Daten schützen. Dieser Schutz wird bei den Bedienenden realisiert, in Systemen und Computern, bei der Übertragung sowie in Diensten und Anwendungen. Unter Berücksichtigung des möglichen Gefährdungspotentials werden Sicherheitsmechanismen implementiert, die das Eindringen in Systeme, das Abhören der Übertragungswege, die Manipulation, die Sabotage und das Löschen von Datensätzen verhindern soll. Zu den personenbezogenen Schutzmechanismen gehören die Autorisierung und Authentifizierung durch Passwörter oder persönlicher Identifikationsnummer (PIN), biometrische Daten oder Signaturen. Die systembezogenen Sicherheitskriterien gehören zur *IT-Sicherheit* und umfassen technische und organisatorische Maßnahmen. Dazu gehören die Installation eigener *Sicherheitsarchitekturen* mit Firewalls, das *Sicherheitsmanagement* und die Schlüsselverwaltung. Kennzeichnend für die übertragungstechnische Sicherheit, die *Netzwerksicherheit* und die *Internet-Sicherheit*, sind die Verschlüsselungsverfahren und die Datenübertragung mit Sicherheitsprotokollen. Anwendungsorientierte Schutzmaßnahmen haben branchenspezifische Eigenschaften, wie beispielsweise bei geschäftlichen Transaktionen, bei denen digitale Signaturen und Transaktionsnummern die Sicherheit verbessern.

Unter Sicherheit fallen alle Kriterien, die die Integrität, Verfügbarkeit, Vertraulichkeit, Verbindlichkeit und Authentizität betreffen.

Sicherheits-ID
SID, security ID Die Sicherheits-ID identifiziert den Benutzer eindeutig in einem Sicherheitssystem. Solche Sicherheits-IDs können einzelnen Personen oder ganzen Benutzergruppen zugewiesen werden.

Sicherheitsarchitektur
security architecture Die Sicherheitsarchitektur der ISO bildet den zweiten Teil des OSI-Referenzmodells und ist die Basis für die Integration von *Sicherheit* in offenen

Kommunikationssystemen. Die OSI-Sicherheitsarchitektur beschreibt keine bestimmte Technologie, wie Sicherheit in offenen Systemen erreicht wird, sondern sie befasst sich mit den Sicherheitsaspekten in offenen Kommunikationssystemen und definiert die zugehörige Gedanken- und Begriffswelt sowie Richtlinien und Maßnahmen um vorhandene Standards zu verbessern und neue zu entwickeln. Die OSI-Sicherheitsarchitektur stellt die Beziehungen zwischen den *Sicherheitsdiensten* und -mechanismen mit den Schichten des OSI-Referenzmodells her. Die verschiedenen Sicherheitsdienste und -mechanismen sind auf allen sieben Schichten des OSI-Referenzmodells angesiedelt; von der Bitübertragungsschicht bis hin zur Anwendungsschicht.

Sicherheitsdienst
security service

Sicherheitsdienste Sicherheitsmechanismen	Sicherheitsdienste				
	Vertraulichkeit	Datenintegrität	Authentifizierung	Zugriffskontrolle	Unwiderrufbarkeit
Verschlüsselung	X	X			
Digitale Signatur			X		
Zugriffskontrolle				X	
Integritätssicherung		X			X
Datenstromerweiterung	X				
Authentifizierung			X	X	
Leitweglenkungskontrolle	X	X			
Notarisierung			X		X

Sicherheitsdienste und deren -mechanismen

Sicherheitsdienste sollen Angriffe abwehren. Es handelt sich dabei um Technologie-unabhängige Sicherheitsmaßnahmen, die durch ihre Leistungsmerkmale genau definiert sind und in die Schichtenstruktur der *Sicherheitsarchitektur* eingebunden werden. Die fünf primären Sicherheitsdienste Vertraulichkeit, Integrität, Authentifizierung, Zugriffskontrolle und Unwiderrufbarkeit werden durch Sicherheitsmechanismen realisiert. Neben den genannten Sicherheitsdiensten gibt es weitere, die detaillierter sind, wie die Unversehrtheit der Nachricht oder der Kommunikationsnachweis. Jeder Sicherheitsdienst basiert auf einem

oder mehreren Sicherheitsmechanismen.

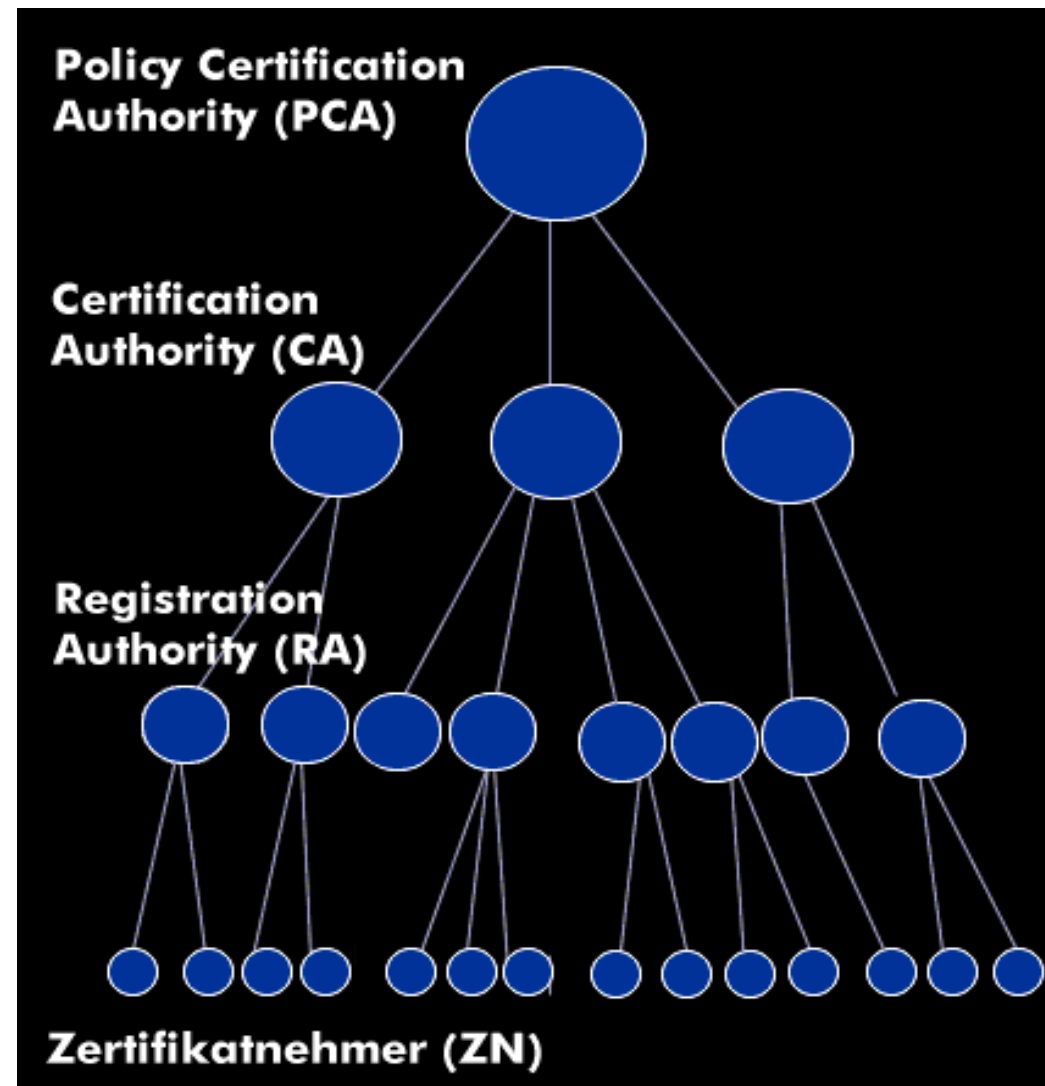
Ein Sicherheitsdienst ist die Vertraulichkeit, mit der sichergestellt wird, dass nur Befugte auf entsprechende Informationen zugreifen können. Sie schützt vor passiven Angriffen und damit vor dem unbefugten Mitlesen von übertragenen Nachrichten und gespeicherten Informationen. Bei den aktiven Angriffen steht die Veränderung der Information und die damit einhergehende Reaktion des Empfängers im Vordergrund. Die Vertraulichkeit basiert auf den Sicherheitsmechanismen Verschlüsselung und Integrität.

Der Sicherheitsdienst Datenintegrität überprüft die Datenunversehrtheit und zeigt an ob Datenströme verändert, manipuliert, modifiziert, gelöscht oder vertauscht wurden. Ein weiterer Sicherheitsdienst ist die Zugriffskontrolle, die durch entsprechende Mechanismen die Möglichkeiten des unberechtigten Zugriffs auf Programme und Daten weitestgehend eingeschränkt. Mit der Vertraulichkeit wird sichergestellt, dass Informationen nur für Befugte zugänglich sind. Die Authentifikation des Kommunikationspartners und des Ursprungs der Nachrichten, der Empfänger- und Urhebernachweis, sind weitere sicherheitsrelevante Dienste.

Sicherheitsinfrastruktur *PKI, public key infrastructure*

Unter einer Public Key Infrastructure (PKI) versteht man eine Umgebung, in der Services zur Verschlüsselung und digitalen Signatur auf Basis von Public-Key-Verfahren bereitgestellt werden. Bei dieser Sicherheitsstruktur wird der öffentliche Schlüssel eines Zertifikatnehmers (ZN) mit den entsprechenden Identifikationsmerkmalen durch eine digitale Signatur von einer Zertifizierungsinstanz (CA) autorisiert.

Die Instanzen der Sicherheitsinfrastruktur sind dabei für das gesamte Schlüssel-Management zuständig. Der Einsatz von PKI bietet eine vertrauenswürdige Netzwerkumgebung, in der Kommunikation vor unberechtigtem Zugriff durch Verschlüsselung geschützt und die Authentizität des Kommunikationspartners durch die digitale Signatur gewährleistet ist. Die verschiedenen Anwendungen der PKI sind kryptografisch geschützt. Dazu gehören E-Mail-Anwendungen, die Sicherung von Desktopsystemen ebenso wie von webbasierten Anwendungen, E-Commerce, die



Strukturierung der PKI

Sicherung von Zugriffskontrollen und die sichere Kommunikation in VPNs.

Die PKI nutzt zwei Schlüssel mit einer typischen Länge von 1024 bis 2048 Bit. Einen privaten, den nur der Besitzer und die Zertifizierungsstelle kennen und der auch nie ausgelesen oder verschickt wird, sowie einen öffentlichen Schlüssel, der dem jeweiligen Geschäftspartner bekannt gemacht werden muss. Die PKI-Architektur besteht aus den Instanzen Policy Certification Authority (PCA), Certification Authority (CA), Registration Authority (RA) und dem Zertifikatnehmer, die

unterschiedliche Aufgaben realisieren. Darüber hinaus umfasst das PKI-Modell mehrere Funktionseinheiten wie das Key Management Center (KMC), die Time Stamping Authority (TSA) und das Key Recovery Center (KRC).

Der ausgezeichnete Teil der PKI wird als Trust Center bezeichnet.

Eine Sicherheitsinfrastruktur muss für den Endbenutzer transparent sein, allerdings sollten die genauen Abläufe des Schlüssel- und Zertifikatmanagements vor dem Benutzer verborgen bleiben. Er sollte aber in der Lage sein, auf einfache Art und Weise die Services zu nutzen.

Sicherheitsmanagement
SM, security management

Das OSI-Sicherheitsmanagement ist einer von fünf Funktionsbereichen des OSI-Managements und hängt mit der Zielspezifikation der Benutzerverwaltung unmittelbar

zusammen. Sicherheitspolitische Aspekte müssen ethische und gesetzliche Komponenten ebenso berücksichtigen wie rechtliche, organisatorische und wirtschaftliche Voraussetzungen. Das Sicherheitsmanagement umfasst den Schutz von Informationen. Dies kann sich auf den Schutz von Objekten, von Diensten und Ressourcen auswirken. Zu den Sicherheitsmaßnahmen gehören u.a. die Authentifizierung, die Passwortverwaltung und die Zugriffsberechtigung auf Netze und LAN-Segmente.

Sicherheitsbetrachtungen müssen unter der Prämisse geplant werden, dass Informationen einen Wert darstellen, der quantifiziert und qualifiziert werden kann. Die Datenbasis des OSI-Sicherheitsmanagements bildet die *Security Management Information Base (SMIB)*. Die *OSI-Sicherheitsarchitektur* kennt drei Management-Kategorien: System Security Management, Security Services Management und Security Mechanismen Management.

Die Abwicklung des Sicherheitsmanagements zwischen den Endsystemen erfolgt über Sicherheitsprotokolle. Dabei müssen die Sicherheitsprotokolle und die übertragenen Management-Informationen geschützt werden.

Sicherheitspolitik *security policies*

In der Sicherheitspolitik werden die Regeln und Verfahrensweisen festgelegt, nach denen die Datenübermittlung, -verarbeitung und -speicherung erfolgen. Sie berücksichtigt personelle, technische, organisatorische und rechtliche Einflussfaktoren.

Bei den personellen Einflussfaktoren geht es um das Bedienpersonal, der Zuverlässigkeit, Sensibilität und Vertrauenswürdigkeit. Es geht um die Antworten auf Fragen wie "Wer darf auf welche Daten zugreifen?" oder "Wer ist für die Sicherheitspolitik verantwortlich?"

Die technischen Einflussfaktoren sind geprägt durch die vorhandenen Computer, die Art und Sensibilität der Daten und der Software, aber auch durch räumliche Gegebenheiten, die Art der eingesetzten Übertragungsmedien und -techniken, sowie die Anzahl der Prozesse usw. Bei der Technik stellen sich Fragen hinsichtlich der Daten, der Art der Vermittlung oder der Verkehrsbeziehungen. So beispielsweise:

“Welche Verkehrsbeziehungen sind erlaubt?” oder “Auf welcher Schicht werden die *Sicherheitsdienste* installiert?”.

Bei den organisatorischen Einflussfaktoren handelt es sich um solche, die sich mit den Arbeitsabläufen der Benutzer beschäftigen. Bei diesen Einflussfaktoren geht es um die vielen sicherheitsrelevanten Aspekte, wie “An wen werden Alarme gemeldet?” oder “Welche Maßnahmen sind zu treffen, damit die Sicherheitspolitik eingehalten wird?”.

Darüber hinaus muss sich die Sicherheitspolitik auch nach den Gesetzen und rechtlichen Vereinbarungen richten. Zu nennen sind das Bundesdatenschutzgesetz (BDSG), Signaturgesetz (SigG), Teledienstschutzgesetz (TDDSG) und andere. Letztlich geht es auch um die Rechtsverbindlichkeit der Informationen, um deren Urhebernachweis oder Kommunikationsnachweis.

Sicherheitsrichtlinie *security directive*

Sicherheitsrichtlinien sind unternehmensspezifische Regeln in denen die Ziele für alle sicherheitsrelevanten Arbeitsgebiete festgelegt sind.

In Unternehmen definieren die Sicherheitsrichtlinien die Regeln, die die Mitarbeiter, die an der Ausarbeitung der Richtlinien beteiligt sein sollten, in ihrem Arbeitsgebiet beachten müssen. Zu den wichtigsten Interessengruppen in einem Unternehmen gehören die Sicherheits- und Netzwerkadministration, Arbeitnehmervertreter, Vertreter der Nutzergruppen und der Geschäftsführung. Die ausgearbeiteten Sicherheitsrichtlinien sollten von den Nutzern umgesetzt und akzeptiert werden, sie sollten die *Sicherheit* des Netzwerks und der Systeme gewährleisten und die Rechte und Pflichten der Nutzer, der Administration und der Geschäftsführung klar regeln. Bestandteile der Sicherheitsrichtlinien umfassen die Beschaffung der Software, Computer- und Netzwerktechnik und die darin realisierten Sicherheitsstandards, die Zugriffsberechtigungen und alle Maßnahmen die dem Datenverlust und der Abwehr von Angriffen dienen, die Betriebs- und Wartungsrichtlinien und das Reporting, um nur einige zu nennen.

In die Sicherheitsrichtlinien fließen die nationalen und internationalen Sicherheitsstandards für die Bewertung und Zertifizierung von IT-Systemen ein. Dazu

gehören die europäischen *Information Technology Security Evaluation Criteria* (ITSEC), die amerikanischen *Trusted Computer Security* (TCSEC) und die *Common Criteria* for Information Technology Security Evaluation (CC). Außerdem befasst sich Kapitel 1 des britischen Standards *BS 7799* für das *Sicherheitsmanagement* mit den Sicherheitsrichtlinien für das Management und für die Betreuung der *IT-Sicherheit*.

Sicherheitsstufe
SIL, safety integrity level

Der Safety Integrity Level (SIL) ist ein Verfahren zur Ermittlung des potentiellen Risikos von Personen, Systemen, Geräten und Prozessen im Falle einer Fehlfunktion. Die Basis für die Spezifikationen, den Entwurf und Betrieb von sicherheitstechnischen Systemen (SIS) bildet der IEC-Standard 61508.

IEC 61508 bietet ein kohärentes Framework in dem alle früheren Sicherheitsregularien berücksichtigt sind. Dazu gehören die in Deutschland bekannten Sicherheitsnormen DIN/VDE 19250, DIN/VDE 19251 und DIN/VDE 801. Der 61508-Standard definiert die *Sicherheit* in Abhängigkeit vom Grad der Beschädigung und der Wahrscheinlichkeit, die eine bestimmte Anwendung hinsichtlich einer risikorelevanten Situation hat. 61508 hat eine eigene Risikobewertung mit der die Sicherheits-Integritätslevel (SIL) für die Geräte und Systeme mit Sicherheitsaufgaben ermittelt werden. Der IEC-Standard kennt die vier SIL-Level SIL1 bis SIL4, die als Sicherheitsausführungen von elektrischen und elektronischen Geräten definiert sind. Im SIL-Wert drückt sich die spezifizierte Sicherheitsfunktion im Fehlerfall aus: Mit welcher Wahrscheinlichkeit

SIL-Level	PFD	Verfügbarkeit	1/PFD
4	10exp-5 ...	> 99,99%	10exp5 ...
	10exp-4		10exp4
3	10exp-4 ...	99,90% ...	10exp4 ...
	10exp-3		10exp3
2	10exp-3 ...	99,00% ...	10exp3 ...
	10exp-2		10exp2
1	10exp-2 ...	90,00% ...	10exp2 ...
	10exp-1		10exp1

PFD, probability to fail on demand

arbeitet das System im angeforderten Fehlerfall (PFD). Bei einem SIL-Level von 1 ist die Gefahr oder das wirtschaftliche Risiko relativ gering und die Verfügbarkeit des der sicherheitstechnischen Systeme mit 90 % oder 10 % Fehlerwahrscheinlichkeit akzeptabel.

SIL-Level des IEC-Standards 61508

Das Risikopotential wird in technischen Einrichtungen, verfahrenstechnischen Anlagen, in der Automotive-Technik, in Maschinen, Aufzügen, programmierbaren Steuerungen, IT-Anlagen und -Systemen bestimmt.

Sicherheitsvereinbarung *SA, security association*

Security Associations (SA) sind Sicherheitsvereinbarungen, die zwei mittels IPSec miteinander kommunizierende Instanzen vor der Kommunikation untereinander austauschen. SAs werden für den Authentication Header (AH) und den Encapsulated Security Payload (ESP) jeweils individuell getroffen. Sie gelten für die unidirektionale Kommunikation, also nur für eine Übertragungsrichtung. Da eine Kommunikation bidirektional erfolgt, sind mindestens zwei SAs für die Übertragung erforderlich.

Security Associations sind die grundlegende individuelle Basis jeder IPSec-Verbindung. Sie definieren exakt, wie der Host oder das Security Gateway eine Verbindung zur Zielkomponente aufbauen und erhalten muss. Eine SA ist stets einzigartig und wird durch drei wesentliche Komponenten beschrieben: Den Security Parameter Index (SPI) die IP-Zieladresse und den Security Protocol Identifier.

System Access Control

Die System Access Control bildet das Kapitel 7 des britischen Sicherheitsstandards *BS 7799* für das Informationssicherheits-Management. Dieses Kapitel beschreibt die Zugriffskontrolle zu Systemen und Informationen. Als definierte Ziele sollen die Informationssysteme vor nichtautorisiertem Zugriff geschützt werden; Aktivitäten in dieser Richtung sollen entdeckt und erfasst werden. Darüber hinaus soll der Schutz der netzwerkbasierten Services sichergestellt werden auch unter Berücksichtigung des Mobile Computing.

System Development and Maintenance

“System Development and Maintenance” bildet das Kapitel 8 des britischen Sicherheitsstandards *BS 7799* für das Informationssicherheits-Management. Dieses Kapitel beschreibt die Sicherstellung der *Sicherheit* bei der Weiterentwicklung des Systems.

Es gilt Verluste, Änderungen oder Missbrauch von Benutzerdaten zu verhindern, die

Sicherheit des Systems zu gewährleisten, die Vertraulichkeit, Authentizität und Integrität der Informationen zu schützen, IT-Projekte und Support-Aktivitäten in Bezug auf die Sicherheit zu garantieren und die Sicherheit von Daten und Programmen zu erhalten.

- TCSEC** *trusted computer security* Die *Trusted Computer Security* (TCSEC) ist ein Kriterienkatalog für die Sicherheit von IT-Systemen. Der von der amerikanischen NCSC entwickelte und vom US-amerikanischen Verteidigungsministerium 1985 herausgegebene Kriterienkatalog dient US-Firmen zur Bewertung von sicherheitsrelevanten Maßnahmen. Aufbauend auf dem in den 80er Jahren definierten TCSEC wurden diverse Maßnahmenkataloge für verschiedene Länder und die Nato entwickelt. International werden die *Common Criteria* (CC) verwendet, die aus den *ITSEC* und den TCSEC entwickelt wurden.
- VM** *vulnerability management* Das Vulnerability Management (VM) befasst sich mit den sicherheitsrelevanten Schwachstellen in IT-Systemen. Mit dem VM-Management sollen Prozesse und Techniken erarbeitet werden, mit denen zur Steigerung der *IT-Sicherheit* eine Sicherheitskonfiguration in Unternehmen eingeführt und verwaltet werden kann. Das Vulnerability Management umfasst die Schwachstellenanalyse unter Berücksichtigung der in den Standards *BS 7799* resp. *ISO 17799* detailliert beschriebenen Faktoren Mensch, Maschine, Umgebung und Daten. Darüber hinaus spielt beim VM-Management das Common Vulnerability Scoring System (CVSS), mit dem ein Rating- Index erstellt wird, eine wesentliche Rolle.
- WAS** *web application security*
Web-Applikationssicherheit *Web Application Security* (WAS) schützt Web-Anwendungen und Webservices vor Angriffen, die über das HTTP-Protokoll erfolgen. Ziel dieser Angriffe ist es, in den Rechner einzudringen oder die Web-Aktivitäten zu blockieren. Ein Beispiel für diese Attacken ist das Cross Site Scripting (XSS). Die Web-Applikationssicherheit umfasst diverse netzwerktechnische, technologische und anwendungsspezifische Aspekte, die weit über die Programmierung und Konfiguration hinausgehen. Aus diesem Grund hat sich für die Umsetzung der Web-

Das Sechs-Ebenen-Modell für die Web Application Security (WAS)

	Ebene	Inhalt
6	Vorschriften und Bestimmungen	Einhealtung gesetzlicher Regelungen und unternehmensspezifischer Vorgaben
5	Semantik	Schutz vor Täuschung und Betrug
4	Logik	Absicherung von Prozessen und Workflows als Ganzes
3	Implementierung	Vermeiden von Programmierfehlern, die zu Schwachstellen führen
2	Technologie	Richtige Wahl und sicherer Einsatz von Technologie
1	System	Absicherung der auf der Systemplattform eingesetzten Software
0	Netzwerk & Host	Absicherung von Host und Netzwerk

Applikationssicherheit ein Modell aus sechs Ebenen bewährt, in dem alle Aspekte berücksichtigt werden. Erst wenn alle Ebenen dieses Modells betrachtet wurden, gilt eine Web-Anwendung als hinreichend sicher. Da die Sicherheitsmechanismen der Firewalls auf der

Netzwerk- und Transportschicht stattfinden, können bei Einhaltung der Zugangskriterien die Angriffe auch auf der Anwendungsebene erfolgen. Dies soll die Web Application Security verhindern. Das WAS-Konzept setzt daher auf der Anwendungsschicht Web Application Firewalls, auch Web Shields genannt, ein. Die Web Shields untersuchen potenzielle Hackeraktivitäten auf Sicherheitslöcher in der Server-Software. Sie sind an bestimmten Mustern im Footprint zu erkennen oder sie profitieren von einer fehlerhaften Programmierung. Werden solche Attacken entdeckt, sperrt der Web Application Firewall den Zugriff und verhindert damit, dass die *Sicherheit* der Website unterlaufen wird.

Im Gegensatz zu den Web Shields sind die ebenfalls in die Web-Sicherheit eingebundenen XML-Firewalls auf Webservices spezialisiert.

WLAN-Sicherheit
WLAN security

Der von der Arbeitsgruppe 802.11i für WLANs definierte Sicherheitsstandard hatte einige Lücken und wurde daher vollkommen überarbeitet und neu definiert. Mit der Neudefinition sind herstellerübergreifende WLAN-Sicherheitslösungen in allen Netzkonfigurationen möglich, unabhängig von den eingesetzten Produkten.

Generell bezieht sich die *WLAN-Sicherheit* als Teil des WLAN-Managements auf den Zugangsschutz der Teilnehmer durch Authentifizierung und den Schutz vor der Einwahl in unberechtigte Access Points (AP). Darüber hinaus müssen die Sicherheitslösungen sicherstellen, dass Unberechtigte die über Funk empfangenen Datenströme nicht auswerten können. Da sich der Empfang von Funksignalen in einer entsprechenden Entfernung nicht verhindern lässt, müssen geeignete Maßnahmen in Form von Verschlüsselung eingesetzt werden, damit die verschlüsselten Datenpakete nicht entschlüsselt und ausgewertet werden können. Des Weiteren muss die WLAN-Sicherheit auch die Manipulation von Datenströmen erkennen und verhindern können. Dies kann mittels zyklischer Blockprüfung (CRC) erfolgen.

Der Schlüsselaustausch über das WLAN ist ein weiterer Punkt, der besonders bei symmetrischer Verschlüsselung, bei der Sender und Empfänger mit gleichem Schlüssel arbeiten, Probleme aufwirft. Daher arbeiten WLANs häufig beim Schlüsselaustausch mit asymmetrischer Verschlüsselung und in der Übertragung mit symmetrischer Verschlüsselung. In diesem Zusammenhang ist das WEP-Protokoll zu nennen, das in 802.11 definiert wurde.

Da das WEP-Protokoll einige Schwächen hat, werden neben diesem Sicherheitsprotokoll mit statischen Schlüsseln weitere mit dynamischer Schlüsselvergabe eingesetzt. So das EAP-Protokoll und das von der WiFi-Allianz definierte WiFi Protected Access (WPA).

802.11i hat ein ausgefeiltes Sicherheitskonzept mit einer umfassenden Schlüsselhierarchie, die neben einem Master Key (MK), Pairwise Master Key (PMK), Pairwise Transient Key (PTK) sowie weitere daraus abgeleitete Schlüssel kennt.

Zentralstelle für die Sicherheit in der Informationstechnik, ZSI

Von der deutschen Bundesregierung ins Leben gerufene, neutrale Institution, die Sicherheitskriterien für Rechnersysteme entwickelt, Systeme prüft und bewertet sowie Zertifikate an Systemhersteller und -anwender vergibt.