



Kompass der IT-Sicherheitsstandards

Leitfaden und Nachschlagewerk
4. Auflage

■ Impressum

Herausgeber: BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner: Lutz Neugebauer
Tel.: 030.27576-242
l.neugebauer@bitkom.org

Redaktion: Dr. Walter Fumy, Lutz Neugebauer

Verantwortliches
Gremium: AK Sicherheitsmanagement

Redaktionsassistent: Leila Ambrosio

Gestaltung / Layout: Design Bureau kokliko /
Anna Müller-Rosenberger (BITKOM)

Copyright: BITKOM 2009

Stand: August 2009, Version 4.0

DIN
Deutsches Institut der Normung e.V.
Normenausschuss Informationstechnik und
Anwendungen (NIA)
Burggrafenstraße 6
10787 Berlin
Tel.: 030.2601-0
Fax: 030.2601-1231
nia@din.de
www.nia.din.de

Cord Wischhöfer

Normenausschuss Informationstechnik und
Anwendungen (NIA) im DIN, Arbeitsausschuss
NIA-27, IT-Sicherheitsverfahren

Martin Uhlherr

Kompass der IT-Sicherheitsstandards

Leitfaden und Nachschlagewerk

4. Auflage

Inhaltsverzeichnis

1	Einleitung	4
2	Nutzen von Standards	5
3	Arten von Standards, ihre Entwicklung und Mitwirkungsmöglichkeiten	6
	Grundlegende Standards zum IT-Sicherheits- und Risikomanagement	8
4	Kompass der IT-Sicherheitsstandards	11
4.1	Tabelle mit Kompass der IT-Sicherheitsstandards	11
4.2	Beschreibung der IT-Sicherheitsstandards	14
5	Einführung von IT-Sicherheitsstandards im Unternehmen	15
6	Grundlegende Standards zum IT-Sicherheits- und Risikomanagement	17
6.1	Allgemeine Informationssicherheits-Managementsysteme (ISMS)	17
6.4	Sektorspezifische ISMS	21
6.3	Sicherheitsmaßnahmen und Monitoring	24
6.4	Risikomanagement	29
7	Standards mit IT-Sicherheitsaspekten	34
7.1	Cobit	34
7.2	ITIL	35
7.3	IDW PS 330	37
8	Vorschriften	38
8.1	KonTraG	39
8.2	Basel II	39
8.3	SOX	40
8.4	EURO-SOX	40
8.5	BDSG	41
9	Evaluierung von IT-Sicherheit	43
9.1	Common Criteria	43
9.2	Schutzprofile	48
10	Spezielle Sicherheitsfunktionen 1: Normen zu kryptographischen und IT-Sicherheitsverfahren	50
10.1	Verschlüsselung	50
10.2	Digitale Signaturen	52
10.3	Hash-Funktionen und andere Hilfsfunktionen	55
10.4	Authentifizierung	57
10.5	PKI-Dienste	59
10.6	Schlüsselmanagement	60
10.7	Kommunikationsnachweise	61
10.7	Zeitstempeldienste	62
11	Spezielle Sicherheitsfunktionen 2: Physische Sicherheit	64
11.1	BSI Technische Leitlinie (TL) 03400 (vormalig BSI 7500)	64
11.2	Brandschutz	64
11.3	Einbruchshemmung	67
11.4	Gehäuse	68

12	Anhang	70
13	Danksagung	78
14	Fragebogen	79

1 Einleitung

Viele Organisationen (Unternehmen oder Behörden) sind heute von modernen Informations- und Kommunikationstechniken (IuK) abhängig. Die Informationstechnik (IT) dient als Basis für zahlreiche Geschäftsprozesse: Vom Einkauf über die Produktion bis zum Verkauf sowie die komplette Verwaltung. Dank Handys, PDAs und Notebooks können immer mehr Mitarbeiter eines Unternehmens mobil auf das firmeninterne Netz zugreifen. Immer mehr Unternehmen, auch im Mittelstand, sind damit in hohem Maße auf eine funktionierende IT angewiesen.

Nach Angaben des Statistischen Bundesamtes – für das Jahr 2008 – nutzen 97 Prozent aller Unternehmen mit mehr als zehn Mitarbeitern einen Computer. Rund 77 Prozent dieser Unternehmen hatten 2008 ein eigenes Angebot im Internet. 95 Prozent aller Unternehmen in Deutschland nutzten das Internet. Diese prinzipiell positive Entwicklung führt zu einer zunehmenden Abhängigkeit der Organisationen von der Verfügbarkeit der IT, der Integrität (Unversehrtheit) von Daten und Systemen sowie dem Schutz vor unberechtigtem Zugriff auf Daten.

Da eine 100 prozentige Sicherheit nicht erreichbar ist, gilt es, die mit dem Einsatz von IT verbundenen Risiken auf ein Niveau zu bringen, das aus unternehmerischer Sicht vertretbar ist und dauerhaft gehalten werden kann. Um dieses Ziel zu erreichen, ist die Einführung eines IT-Risikomanagements für praktisch jedes Unternehmen notwendig. Standards spielen im Rahmen des IT-Risikomanagements eine wichtige Rolle. Der Einsatz von IT-Sicherheitsstandards im Unternehmen oder in einzelnen Bereichen macht die sicherheitsrelevanten IT-Prozesse des Unternehmens transparent und damit beherrschbar und reduziert somit das Gesamtrisiko.

Großunternehmen haben dies schon lange erkannt und setzen Standards in wachsendem Maße ein. Aber auch mittelständische Unternehmen profitieren von

der Anwendung geeigneter IT-Sicherheitsstandards. Um interessierten Geschäftsführern oder IT-Leitern aus dem Mittelstand einen Überblick zu geben, welche Standards für ihr Unternehmen beziehungsweise oder einzelne Unternehmensbereiche relevant sein könnten, wurde der vorliegende Leitfaden entwickelt.

Das Herzstück des Leitfadens, der Kompass der IT-Sicherheitsstandards, klassifiziert bekannte Standards sowie Standards für spezielle Sicherheitsfunktionen, so dass der Leser diese für sein Unternehmen bewerten und gegebenenfalls als relevant einschätzen kann. Im Kompass sind auch ausgewählte Vorschriften und Gesetze aufgeführt, die im Zusammenhang mit IT-Sicherheit in Medien und Publikationen immer wieder erwähnt werden. Auch diese sind klassifiziert und können so auf ihre Relevanz überprüft werden. Nicht jeder Standard ist für jedes Unternehmen sinnvoll. Nähere Erläuterungen und Informationen zu den aufgeführten Standards und Vorschriften sind in den darauf folgenden Kapiteln zu finden.

Im Anhang sind die Bezüge der behandelten Standards untereinander aufgeführt, dort befinden sich auch Links zu weiteren Informationen.

Noch eine Anmerkung in eigener Sache: Da BITKOM und DIN den Leitfaden weiterentwickeln wollen, sind wir am Feedback des Leser interessiert. Wir würden uns daher freuen, wenn Sie uns den Fragebogen im Anhang zufaxen, damit wir bei der nächsten Version Ihre Anregungen berücksichtigen können.

2 Nutzen von Standards

Der Einsatz von IT in Unternehmen birgt Risiken, die im Rahmen eines IT-Risikomanagements auf ein angemessenes Niveau reduziert werden sollten. Dabei kommt es insbesondere darauf an, die Risiken umfassend zu ermitteln und die Schutzmechanismen aus wirtschaftlichen Gründen nicht aufwendiger zu gestalten, als es das zulässige Risiko verlangt. Die Auswahl und die Anwendung angemessener IT-Sicherheitsstandards ist ein Teil des IT-Sicherheitsmanagements.

Die Etablierung eines umfassenden IT-Sicherheitsmanagements ist eine anspruchsvolle Aufgabe. Hierbei können Planungsfehler entstehen, die zu ineffektiven und vor allem ineffizienten Maßnahmen führen können. Selbst entwickelte Vorgehensweisen sind in der Regel teuer in der Umsetzung und entsprechen erfahrungsgemäß häufig nicht dem Stand der Technik. Hier ist es

sinnvoll, auf bewährte Vorgehensweisen, die in Standards festgehalten sind, zurückzugreifen.

Standards können helfen, die sicherheitsrelevanten IT-Prozesse zum Vorteil des Unternehmens, der Kunden, der eigenen Produkte sowie der Mitarbeiter zu verbessern. Sie bieten Hilfestellung bei der Entwicklung von generischen Maßnahmen auf Management-Ebene bis zu detaillierten technischen Implementierungen an. Sie liefern Methoden für ein leistungsfähiges IT-Sicherheitsmanagement oder definieren die IT-Sicherheit von ausgewiesenen Produkten. Sie können sowohl eigenständig als auch methodisch eingebettet in ein anderes System fortlaufend betrieben werden.

Wesentliche Ziele beim Einsatz von Standards sind in Tabelle 1 zusammengefasst:

Kostensenkung	■ Nutzung vorhandener und praxiserprobter Vorgehensmodelle ■ Methodische Vereinheitlichung und Nachvollziehbarkeit ■ Ressourceneinsparung durch Kontinuität und einheitliche Qualifikation ■ Interoperabilität
Einführung eines angemessenen Sicherheitsniveaus	■ Orientierung am Stand der Technik und Wissenschaft ■ Gewährleistung der Aktualität ■ Verbesserung des Sicherheitsniveaus durch die Notwendigkeit der zyklischen Bewertung
Wettbewerbsvorteile	■ Zertifizierung des Unternehmens sowie von Produkten ■ Nachweisfähigkeit bei öffentlichen und privatwirtschaftlichen Vergabeverfahren ■ Verbesserung des Unternehmensimage ■ Stärkung der Rechtssicherheit

Tabelle 1: Ziele beim Einsatz von Standards

3 Arten von Standards, ihre Entwicklung und Mitwirkungsmöglichkeiten

Weltweit gibt es zahlreiche Gremien, die sich mit der Entwicklung von Sicherheitsstandards und Normen beschäftigen.

Die in diesem Leitfaden aufgeführten und beschriebenen Standards wurden von verschiedenen Gremien nach unterschiedlichen Verfahren entwickelt. In der Regel kann man das verantwortliche Gremium an der Zeichenkette zu Beginn der Kurzbezeichnung des Standards erkennen:

ISO/IEC-Standards

Bei der Mehrzahl handelt es sich um internationale Normen, die unter deutscher Mitwirkung im Subkomitee 27 „IT-Security Techniques“ des Technischen Gemeinschaftskomitees „Information Technology“ der Internationalen Normenorganisationen ISO und IEC, ISO/IEC JTC 1/SC 27 (www.jtc1sc27.din.de), nach einem Konsensverfahren entwickelt und in einer öffentlichen Umfrage bestätigt wurden. Diese Standards sind an der Zeichenkette ISO/IEC gefolgt von der Normennummer zu erkennen (Beispiel: ISO/IEC 27001).

DIN EN-Standards

Bei Standards, die mit der Zeichenkette EN beginnen, handelt es sich um Europäische Normen, die von einer der Europäischen Normenorganisationen CEN, CENELEC oder ETS, ebenfalls nach einem Konsensverfahren mit öffentlicher Umfrage, entwickelt wurden. Beginnt die Zeichenkette mit „DIN“, so handelt es sich um eine deutsche Norm. „DIN EN“ bezeichnet eine Europäische Norm, die in das deutsche Normenwerk übernommen wurde.

Andere Standards

Andere Bezeichnungen (Beispiel: IT-GSHB) deuten auf Standards, die von Konsortien, Interessengruppen oder Behörden nach deren jeweiligen Regeln erarbeitet wurden. Diese Regeln sehen einen gegenüber den Normungsorganisationen eingeschränkten Konsensrahmen vor und legen die Mitwirkungsmöglichkeiten fest.

Die Erarbeitung deutscher Beiträge und Stellungnahmen zu internationalen Normen erfolgt durch das Deutsche Institut der Normung e.V. (DIN), insbesondere durch den Arbeitsausschuss „IT-Sicherheitsverfahren“ des Normenausschusses Informationstechnik NIA-27 (www.nia.din.de/nia27). Die Mitarbeit¹ in den Gremien des DIN ist, bei angemessener Beteiligung an den Kosten der Normungsarbeit, offen für alle interessierten Kreise - unabhängig von der Mitgliedschaft im DIN.

Die internationalen und nationalen Standards werden im zeitlichen Abstand von maximal fünf Jahren einer Revision unterzogen und bei Bedarf überarbeitet. Das Veröffentlichungsdatum gibt jeweils den Abschluss der letzten Überarbeitung an. Bei der Anwendung der Standards ist es sinnvoll, bei einer aktuellen Datenbank (z. B. www.beuth.de, Verlag des DIN) die aktuelle Ausgabe anzufragen. Hier können die Standards auch bezogen werden.

Vorschriften und Gesetze

Im Themenbereich der IT-Sicherheit spielen verstärkt Vorschriften und Gesetze eine bedeutende Rolle. Aus diesem Grund sind die wichtigsten Vorschriften in dieser Publikation im Kapitel 8 zusammengefasst. Abweichend davon werden in bestimmten Themengebieten die jeweiligen Vorschriften und Gesetze jedoch dem Fachkapitel

1. Anfragen zur Mitarbeit sowie zu den Projekten und Normen können gern an den Ausschuss (siehe Impressum) gestellt werden

direkt zugeordnet. So findet man die gesetzliche Vorgabe des MaRisk im Kapitel Risikomanagement, obwohl es sich hierbei im engeren Sinne nicht um einen Standard, sondern um eine Vorschrift für den Finanzsektor handelt

Alle in dieser Leitlinie behandelten internationalen Standards werden vom NIA-27 für die Anwendung in Deutschland empfohlen.

Angelehnt an die Arbeitsgruppen des NIA-27 erfolgt die Einteilung der Standards in diesem Leitfaden in fünf Bereiche:

- Informationssicherheits-Managementsysteme (siehe Kapitel 6.1)
- Sicherheitsmaßnahmen und Monitoring (siehe Kapitel 6.3)
- Evaluierung von IT-Sicherheit (siehe Kapitel 9)
- Kryptographische und IT-Sicherheitsverfahren (siehe Kapitel 10)
- Physische Sicherheit (siehe Kapitel 11)

Die Einteilung ergibt sich aufgrund der Architekturebene und der Ausrichtung der Standards (siehe Abbildung 1). Hierdurch ist eine gewisse Klassifizierung gegeben.

In der folgenden Tabelle sind die behandelten Standards für die fünf Bereiche aufgeführt. Um die bekanntesten Vorschriften und Standards von anderen Konsortien, Interessengruppen, Behörden mit aufzuführen, sind zwei zusätzliche Bereiche „IT-Standards mit Sicherheitsaspekten“ (siehe Kapitel 7) und „Vorschriften“ (siehe Kapitel 8) eingefügt.

In der linken Tabellenspalte befindet sich die Abkürzunw. oder Zeichenkette, in der rechten Spalte die Namen der Standards auf Englisch und/oder Deutsch. Die Reihenfolge ist identisch mit dem Inhaltsverzeichnis, sodass über diese Tabelle anhand von Begriffen und Namen die Standardw. oder Vorschriften gesucht werden können.

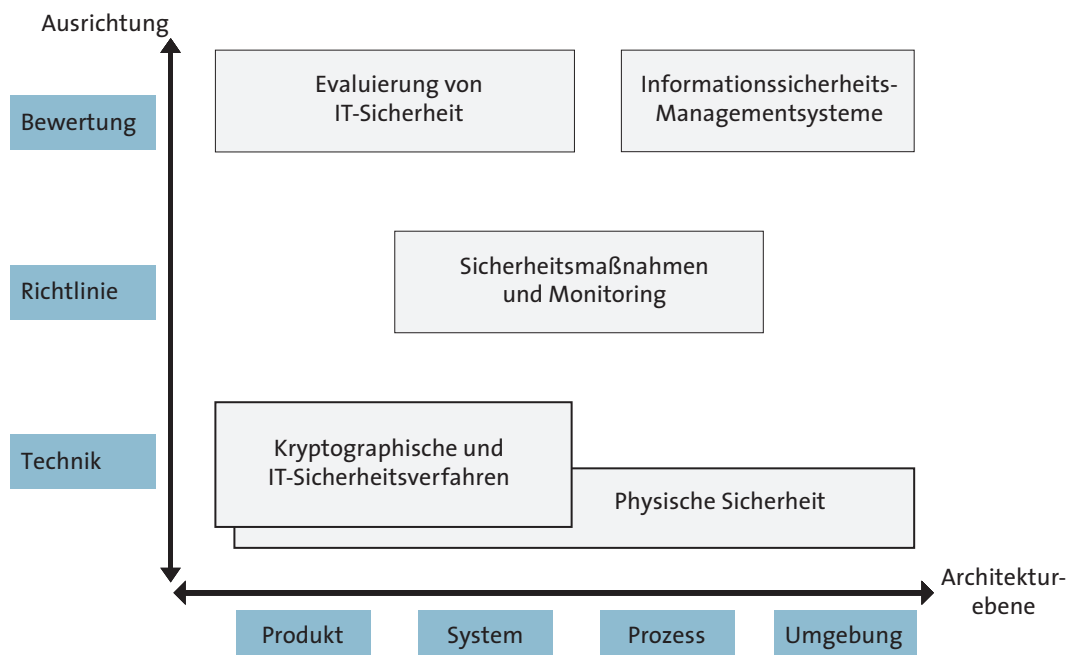


Abbildung 1: Einteilung von Standards in Bereich (angelehnt an Dr. Walter Fumy, Chairman ISO/IEC JTC 1/SC 27)

■ Grundlegende Standards zum IT-Sicherheits- und Risikomanagement

Informationssicherheits-Managementssysteme (ISMS)

■ ISO/IEC 27001	Information security management systems – Requirements Informationssicherheits-Managementssysteme - Anforderungen
■ ISO/IEC 27002	Code of practice for information security management Leitfaden zum Informationssicherheitsmanagement
■ ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems Anforderungen an Stellen, die Auditierung und Zertifizierung von Informationssicherheitsmanagementsystemen bereitstellen.
■ IT-GS	IT-Grundschutz

Sektor-Spezifische ISMS

■ Richtlinie VDI/VDE2182	Informationssicherheit in der industriellen Automatisierung
■ ISO/IEC 27011	Information security management guidelines for telecommunications Informationssicherheitsmanagement-Leitlinien für die Telekommunikation
■ PCI DSS	Payment Card Industry Data Security Standard v 1.2

Sicherheitsmaßnahmen und Monitoring

■ ISO/IEC 18028	IT network security IT Netzwerksicherheit
■ ISO/IEC TR 18044	Information security incident management Management von Sicherheitsvorfällen in der Informationssicherheit

■ ISO/IEC 18043	Selection, deployment and operation of intrusion detection systems (IDS) Auswahl, Einsatz und Betrieb von Systemen zur Erkennung des Eindringens in Netze und Systeme (IDS)
■ ISO/IEC 15816	Security information objects for access control Sicherheitsobjekte für Zugriffskontrolle
■ ISO/IEC 24762	Security techniques - Guidelines for information and communications technology disaster recovery services
■ ISO/IEC 25777	Information and communications technology continuity management. Code of practice

Risikomanagement

■ MaRisk	Mindestanforderungen an das Risikomanagement für Banken
■ ISO/IEC 27005	Information security risk management Informationssicherheits-Risikomanagement

Standards mit IT-Sicherheitsaspekten

■ Cobit	Control Objectives for Information and Related Technology Kontrollziele für Informations- und verwandte Technologie
■ ITIL	IT Infrastructure Library IT Infrastruktur Verfahrensbibliothek
■ IDW PS 330	Abschlussprüfung bei Einsatz von Informationstechnologie

Vorschriften

■ KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
■ Basel II	-
■ SOX	Sarbanes-Oxley Act

■ EURO-SOX	8. EU-Richtlinie in Anlehnung an Sarbanes-Oxley Act
■ BDSG	Bundesdatenschutzgesetz

Evaluierung von IT-Sicherheit

Common Criteria

■ ISO/IEC 15408 (CC)	Evaluation criteria for IT security (Common Criteria) Evaluationskriterien für IT-Sicherheit
■ ISO/IEC TR 15443	A framework for IT security assurance Rahmenrichtlinien für Sicherung von IT-Sicherheit
■ ISO/IEC 18045	Methodology for IT security evaluation Methodik zur Evaluation von IT-Sicherheit
■ ISO/IEC TR 19791	Security assessment for operational systems Bewertung der Sicherheit von Systemen im Betrieb
■ ISO/IEC 19790 (FIPS 140-2)	Security Requirements for Cryptographic Modules Anforderungen an kryptographische Module
■ ISO/IEC 19792	Security evaluation of biometrics Evaluierung der IT-Sicherheit biometrischer Technologien
■ ISO/IEC 21827 (SSE-CMM)	System Security Engineering – Capability Maturity Model Modell der Ablaufstauglichkeit (auch ISO 21827)
■ ISO/IEC 24759	Test requirements for cryptographic modules Prüfanforderungen für kryptographische Module

Schutzprofile

■ ISO/IEC TR 15446	Guide on the production of protection profiles and security targets Leitfaden zum Erstellen von Schutzprofilen und Sicherheitsvorgaben
--------------------	---

Spezielle Sicherheitsfunktionen 1: Normen zu kryptographischen und IT-Sicherheitsverfahren

Verschlüsselung

■ ISO/IEC 7064	Check character systems Prüfsummensysteme
■ ISO/IEC 18033	Encryption algorithms Verschlüsselungsalgorithmen
■ ISO/IEC 10116	Modes of operation for an n-bit block cipher Betriebsarten für einen n-bit-Blockschlüssel-Algorithmus
■ ISO/IEC 19772	Data encapsulation mechanisms Daten verkapselnde Mechanismen

Digitale Signaturen

■ ISO/IEC 9796	Digital signature schemes giving message recovery Digitaler Unterschriftsmechanismus mit Rückgewinnung der Nachricht
■ ISO/IEC 14888	Digital signatures with appendix Digitale Signaturen mit Anhang
■ ISO/IEC 15946	Cryptographic techniques based on elliptic curves Auf elliptischen Kurven aufbauende kryptographische Techniken

Hash-Funktionen und andere Hilfsfunktionen

■ ISO/IEC 10118	Hash functions Hash-Funktionen
■ ISO/IEC 18031	Random bit generation Erzeugung von Zufallszahlen
■ ISO/IEC 18032	Prime number generation Primzahlerzeugung

Authentifizierung

■ ISO/IEC 9798	Entity authentication Authentisierung von Instanzen
■ ISO/IEC 9797	Message Authentication Codes (MACs) Nachrichten-Authentisierungs-codes (MACs)

PKI-Dienste

■ ISO/IEC 15945	Specification of TTP services to support the application of digital signatures Spezifizierung der Dienste eines vertrauenswürdigen Dritten zur Unterstützung der Anwendung von digitalen Signaturen
■ ISO/IEC TR 14516	Guidelines for the use and management of Trusted Third Party Services Richtlinien für die Nutzung und das Management eines vertrauenswürdigen Dritten

Schlüsselmanagement

■ ISO/IEC 11770	Key management Schlüsselmanagement
-----------------	---------------------------------------

Kommunikationsnachweise

■ ISO/IEC 13888	Non-repudiation Nicht-Abstreitbarkeit
-----------------	--

Zeitstempeldienste

■ ISO/IEC 18014	Time-stamping services Zeitstempeldienste
-----------------	--

Spezielle Sicherheitsfunktionen 2: Physische Sicherheit

■ Technische Leitlinie 03400 (BSI 7500)	Produkte für die materielle Sicherheit
---	--

Brandschutz

■ DIN 4102	Brandverhalten von Baustoffen und Bauteilen
■ DIN 18095	Rauchschutztüren
■ DIN EN 1047	Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand

Einbruchshemmung

■ DIN EN 1143-1	Widerstandsgrad
■ DIN V ENV 1627	Fenster, Türen, Abschlüsse - Einbruchhemmung

Gehäuse

■ DIN EN 60529	Schutzart durch Gehäuse
----------------	-------------------------

Sichere Löschung von Datenträgern

DIN 32757	Vernichtung von Informationsträgern
-----------	-------------------------------------

4 Kompass der IT-Sicherheitsstandards

■ 4.1 Tabelle mit Kompass der IT-Sicherheitsstandards

In der Tabelle 2 ist der „Kompass der IT-Sicherheitsstandards (Version 4.0)“ dargestellt. Er beinhaltet besonders relevante Standards und Vorschriften der IT-Sicherheit für Unternehmen beziehungsweise Unternehmensbereiche.

Um die Relevanz eines Standards/einer Vorschrift für das eigene Unternehmen einschätzen zu können, wurden vier Klassifizierungsbereiche eingeführt:

- Art des Unternehmens
- Rolle innerhalb des Unternehmens
- Merkmal des Standards/der Vorschrift
- Quelle des Standards

Diese vier Klassifizierungsbereiche sind in Eigenschaften weiter unterteilt, deren Relevanz bewertet ist. Bei Art des Unternehmens und Rolle innerhalb des Unternehmens werden die möglichen Zielgruppen als Eigenschaften aufgeführt; bei Merkmal des Standards/der Vorschrift sind die Schwerpunkte als Eigenschaft dargelegt.

Legende für die Tabelle

Relevanz

- Hoch
- ⊖ Partiiell
- Niedrig

Kosten

- ▲ Kostenpflichtig
- △ Kostenlos

Sonstiges

- ◆ Zertifizierung (Gütesiegel, Zertifikat, Akkreditierfähiges Verfahren) ist möglich Relevant, wenn Unternehmen an der US Börse notiert ist
- + Angabe woher der Standard kommt

* Ärzte, Apotheken, Krankenhäuser

** Rechtsanwälte, Steuerberater

	Grundlegende Standards zum IT-Sicherheits- und Risikomanagement														Standards mit IT-Sicherheits-aspekten			Vorschriften						
	Informations-sicherheits-Management-systeme (ISMS)				Sektor-Spezifische SMS		Sicherheit-maßnahmen und Monitoring						Risikomanagement		Standards mit IT-Sicherheits-aspekten			Vorschriften						
	ISO/IEC 27001	ISO/IEC 27002	ISO/IEC 27006	IT-GS	Richtlinie VDI/VDE 2182	ISO/IEC 27011	PCIDSS	ISO/IEC 18028	ISO/IEC TR 18044	ISO/IEC 18043	ISO/IEC 15816	ISO/IEC 24762	BS 25777:2008	ISO/IEC 27005	MaRisk / MaRisk VA	Cobit	ITIL	IDW PS 330	KonTraG	Basel II	SOX	EURO-SOX	BDSG	
Art des Unternehmens																								
Banken/Versicherungen	●	●		●			●	⊖	⊖	⊖		⊖	⊖	⊖	●		●	●		●	●	⊖	⊖	●
Behörden/Verwaltungen	●	●		●				⊖		⊖		⊖	⊖	⊖			●	●	●	○	○	○	○	●
Beratung	○	○	⊖	●	○	○	○	⊖	⊖	⊖		⊖	⊖	⊖			●	●	y	○	○	○	○	⊖
HW/SW-Hersteller	⊖	⊖		●	⊖			⊖	⊖	⊖	●	⊖	⊖	⊖			⊖	●	y	○	○	○	○	●
IT-Dienstleister	●	●	⊖	●	⊖	⊖	⊖	⊖	⊖	⊖	●	⊖	⊖	⊖	⊖	⊖	●	●	⊖	⊖	⊖	○	○	●
Gesundheitswesen*	●	●		●				⊖	⊖	⊖		⊖	⊖	⊖			⊖	●	●	○	○	○	○	●
Kanzleien*	●	●		●				⊖	⊖	⊖		⊖	⊖	⊖			⊖	○	●	○	○	○	○	●
Handwerk und Industrie	⊖	⊖		●	●			⊖	⊖	⊖		⊖	⊖	⊖			●	●	●	⊖	⊖	⊖	⊖	●
Dienstleister	⊖	⊖		●				⊖	⊖	⊖	●	⊖	⊖	⊖			●	●	●	⊖	⊖	⊖	⊖	●
internat. Ausrichtung	●	●	●	⊖		●	●	●		●	●	●	●	●			●	●		⊖	⊖	●	●	●
Rolle innerhalb des Unternehmen																								
Management	●	●	○	●	●	●	⊖					⊖		●	●		●	●	⊖	●	●	●	●	●
Revisoren	⊖	⊖	⊖	⊖	⊖	⊖								⊖	●		●	⊖	●	○	○	○	○	●
IT-Sicherheitsbeauftragte	●	●	⊖	●	●	●	●	●	●	●			●	●	●		⊖	●	●	⊖	⊖	⊖	⊖	●
IT-Leitung	●	●	○	●	●	●	●	●	●	●		●	●	●	●		●	●	●	⊖	⊖	⊖	⊖	⊖
Administratoren	⊖	⊖		●	⊖	⊖		⊖	⊖	⊖		●		⊖	⊖			⊖	⊖	○	○	○	○	⊖
Projektmanagement	●	●		⊖	●	●	⊖					⊖	⊖	○	○		⊖	⊖		○	○	○	○	○
Entwicklung	⊖	⊖		⊖	⊖	⊖	⊖				●		⊖	○	○					○				
Merkmale des Standards/ der Vorschrift																								
produktorientiert				⊖							●													
systemorientiert	●	●		●	●	●	⊖	⊖	⊖	⊖		⊖					●		⊖					●
technisch				●			●	●	●	●	●		○					○	⊖					⊖
organisatorisch	●	●	●	●	●	●	●					●	●	●	●		⊖	●	●	●	●	●	●	⊖
strategisch	●	●	●	●	●	●						●	⊖	⊖	⊖		●	●	●	⊖	⊖	⊖	⊖	
konzeptionell	●	●		●	●	●	●				●		●	●	●		●	●	●	○	○	○	○	
operationell				●			●					●		⊖	⊖		●	●	⊖		○	○	○	
Zertifizierung	◆			◆			◆											◆	◆					
Umfang (selten)	34	115	36	2k	14	44	78	166	50	46	20	67	42	55	44	75	1K	30	-	-	66	-	-	
Kosten	▲	▲	▲	△	▲	▲	△	▲	▲	▲	▲	▲	▲	▲	△	△	▲	▲	△	△	△	△	△	
Quelle des Standards																								
Nationale Normungsgorg.					+								+		+									
Europäische Normungsgorg.																								
Internat. Normungsgorg.	+	+	+			+		+	+	+	+	+		+										
Andere nat. Regelwerke				+			+										+	+	+					

Common Criteria und andere Evaluationskriterien										Schutzprofile										Verschlüsselung										Digitale Signaturen										Hash-Funktionen										Authentifizierung										PKI-Dienste										Schlüsselmanagement										Kommunikationsnchw.										Zeitstempeldienste										BSI Technische Leitlinie										Brandschutz										Einbruchshemmung										Gehäuse																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																													
ISO/IEC 15408 (CC)										ISO/IEC 15443										ISO/IEC 18045										ISO/IEC 19791										ISO/IEC 19790 (FIPS 140-2)										ISO/IEC 24759										ISO/IEC 19792										ISO/IEC 21827 (SSE-CMM)										ISO/IEC TR 15446										ISO/IEC 7064										ISO/IEC 18033										ISO/IEC 10116										ISO/IEC 19772										ISO/IEC 9796										ISO/IEC 14888										ISO/IEC 15946										ISO/IEC 10118										ISO/IEC 18031										ISO/IEC 18032										ISO/IEC 9798										ISO/IEC 9797										ISO/IEC 15945										ISO/IEC TR 14516										ISO/IEC 11770										ISO/IEC 13888										ISO/IEC 18014										TL-03400										DIN 4102										DIN 18095										DIN EN 1047										DIN EN 1143-1										DIN V ENV 1627										DIN EN 60539																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																															
●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○										●										○									

■ 4.2 Beschreibung der IT-Sicherheitsstandards

Jeder aufgeführte Standard beziehungsweise jede Norm oder Vorschrift wird in den folgenden Kapiteln kurz beschrieben:

- Die Beschreibung für jeden Standard, jede Vorschrift ist nach einem einheitlichen Schema strukturiert:
 - Inhalt und Anwendungsbereich
 - Methodik (wo sinnvoll)
 - Zertifizierung (wo sinnvoll)
 - Weitere Anmerkungen
 - Bisherige Ausgaben
- Falls ein Abschnitt ohne Inhalte wäre, ist dieser in der Beschreibung nicht aufgeführt. Können zum Beispiel Vorschriften nicht zertifiziert werden, so entfällt bei der Vorschrift „Basel II“ der Abschnitt „Zertifizierung“.
- Sofern es sich um internationale oder europäische Standards handelt, sind der Titel, das Arbeitsgebiet und der Name des Standards (englisch) aufgeführt.

Englische Titel wurden verständnishalber um eine inoffizielle deutsche Übersetzung ergänzt, da nur die in das deutsche Normenwerk übernommenen Dokumente einen offiziellen deutschen Titel tragen. Bei mehrteiligen Standards oder einer Normenreihe wird die Nummer des jeweiligen Teils mit einem Bindestrich nach der Normennummer angefügt.

- Internationale und europäische Standards wurden formal meist nicht in das deutsche Normenwerk übernommen, weil die aufwändige Übersetzung in der Regel keinen entsprechenden Mehrwert für die Anwender schafft. Ist die Übernahme einer internationalen Norm ins deutsche Normenwerk erfolgt oder geplant, so wird dies bei den Erläuterungen im Abschnitt „Weitere Anmerkungen“ ausgewiesen.
- Standards sind von anderen Standards abhängig oder beeinflussen diese. Der Bezug von Standards zu anderen Standards ist im Anhang auf Seite 70 erläutert. Diese Bezüge sind möglichst umfassend angegeben, eine Vollständigkeit kann nicht garantiert werden.

5 Einführung von IT-Sicherheitsstandards im Unternehmen

Die Einführung von Standards im Unternehmen erfolgt in drei generischen Schritten:

■ Auswahl des Standards

In der Regel entscheidet die Geschäftsführung mit Unterstützung des - falls vorhanden - IT-Sicherheitsbeauftragten, IT-Risikobeauftragten und IT-Verantwortlichen den IT-Betrieb vom Unternehmen an einem IT-Sicherheitsstandard auszurichten. Welcher Standard der richtige für ein Unternehmen ist, hängt von einigen Faktoren (siehe Kompass) ab:

- Art des Unternehmens
- Relevanter Unternehmensbereich für die Standardisierung
- Relevante Charakteristika des Standards

■ Einführung

Die Einführung von IT-Sicherheitsstandards im Unternehmen erfolgt nach dem jeweiligen Vorgehensmodell des ausgewählten Standards. Als Beispiel sei hier das Vorgehensmodell nach BSI IT-Grundschutz aufgeführt:

Die Notwendigkeit der einzelnen Schritte des jeweiligen Vorgehensmodells sollten vor der Einführung auf Relevanz geprüft werden. Anschließend sind die ausgewählten Schritte durchzuführen und die Maßnahmen zur Umsetzung des Standards festzulegen. Hierbei ist zu beachten, dass für die Umsetzung des Modells externes Know-how zugezogen beziehungsweise Mitarbeiter entsprechend geschult werden sollten. Die Einführung eines Standards ohne externes oder internes Know-how führt in der Regel zu einem höheren Aufwand bei eventuell schlechterem Ergebnis.

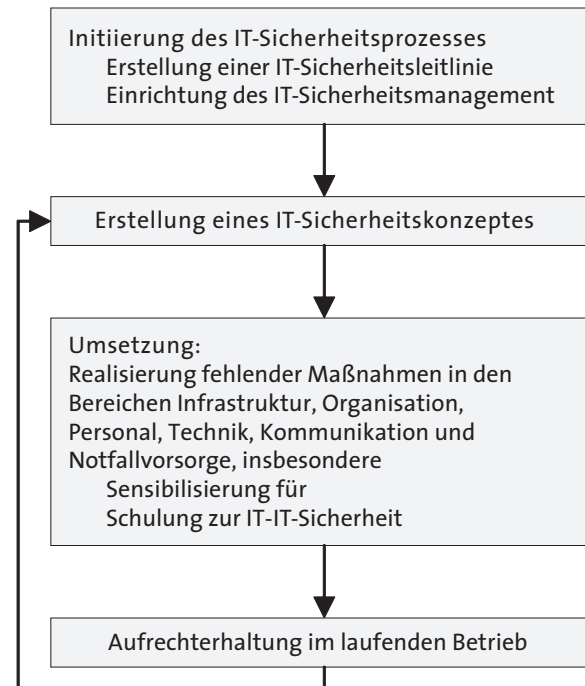


Abbildung 2: Vorgehensmodell nach BSI IT-Grundschutz

■ Betrieb

Nach der Einführung des Standards müssen die getroffenen Maßnahmen (personell, organisatorisch, technisch) in den regulären Betrieb übergehen. Hierfür sind Mitarbeiterschulungen, -information sowie ggf. Prozessanpassungen notwendig. Im Rahmen des regulären IT-Betriebs kann die Einhaltung des Standards durch zwei aufeinander aufbauende Verfahren überprüft und gewährleistet werden:

■ Auditierung

Ein wichtiges Element des Vorgehensmodells ist die Einhaltung und Aktualität der

Sicherheitsmaßnahmen in regelmäßigen Audits von internen oder externen Partnern zu überprüfen. Mit diesem Vorgehen können Unternehmen ihre IT-Sicherheit immer weiter verbessern und sukzessive Sicherheitslücken schließen.

Im Rahmen eines Audits kommt ein externer (zertifizierter) Auditor für einige Tage ins Unternehmen. Anhand der Vorgaben des Standards sowie der Dokumentation des IT-Betriebs wird der Ist-Stand mit dem Soll-Konzept verglichen. Empfehlungen für die Verbesserung der IT-Sicherheit werden ausgesprochen. Diese sollten vom Unternehmen im Nachgang umgesetzt werden.

Eine Auditierung kann den gesamten IT-Betrieb umfassen, sich aber auch nur auf beispielsweise neu eingesetzte Sicherheitskomponenten beschränken (Beispiel: neue Firewall).

■ Zertifizierung

Einige IT-Sicherheitsstandards können als Grundlage für eine Zertifizierung herangezogen werden. Ein Zertifikat ist eine unabhängige Bestätigung dafür, dass

alle (soweit anwendbare) im Standard geforderten Sicherheitsmaßnahmen zum Zeitpunkt der Zertifizierung dokumentiert und tatsächlich umgesetzt sind. Durch die Ausstellung eines Zertifikates, mit dem die Umsetzung des Standards bestätigt wird, kann dies Dritten transparent gemacht werden. Dritte können hierbei Kunden, Banken, Versicherungen oder auch die Öffentlichkeit sein.

Der Aufwand für die Zertifizierung ist abhängig vom Unternehmen und dem Zertifizierungsziel. Hierbei kann jedoch von einem externen Aufwand von einigen Tagen bis einigen Wochen ausgegangen werden. Der interne Aufwand kann deutlich höher sein, je nach Vorbereitungsstand des Unternehmens. Eine generelle Aussage kann nicht getroffen werden.

Bei der Auswahl des Zertifizierers ist zu beachten, dass einige Standards einen akkreditierten Zertifizierer fordern.

6 Grundlegende Standards zum IT-Sicherheits- und Risikomanagement

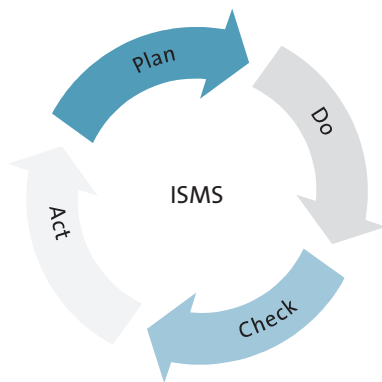


Abbildung 3: Regelkreislauf des ISMS

Die folgenden Standards bieten Richtlinien für einzelne Aspekte des IT-Sicherheits- und Risikomanagements an. Hierzu gehört: Sicherheitsstrategien und Sicherheitsleitlinien von Organisationen festzulegen, Risiken der IT-Sicherheit zu bewerten, Sicherheitsziele zu ermitteln und Sicherheitsanforderungen abzuleiten, geeignete Gegenmaßnahmen (unter anderem auch Grundschutzmaßnahmen) auszuwählen und deren dauerhafte Umsetzung sicherzustellen. Dies alles erfolgt in der Regel im Rahmen des IT-Sicherheits- oder IT-Risikomanagements², welches das systematische Erkennen, Bewerten, Steuern und Überwachen von IT-Sicherheitsrisiken umfasst. Diese Aktivitäten werden im Allgemeinen auch als Regelkreislauf dargestellt und setzen sich aus den Elementen „Plan, Do, Check, Act“ (Englisch für Planen, Durchführen, Überprüfen und Verbessern) zusammen, dem so genannten PDCA-Modell, das die Grundlage eines Informationssicherheits-Managementsystems (ISMS) bildet.

■ 6.1 Allgemeine Informationssicherheits-Managementsysteme (ISMS)

Der bedeutendste Standard für ein Informationssicherheits-Managementsystem ist die Norm ISO/IEC 27001. Sie beschreibt die grundlegenden Anforderungen an das ISMS in einer Organisation (Unternehmen oder Behörde).

Weitere Standards aus der ISO/IEC 27000er-Familie ergänzen ISO/IEC 27001. So wird in ISO/IEC 27000:2009 die Terminologie, in ISO/IEC 27002 (zuvor ISO/IEC 17799) werden einzelne Maßnahmen erläutert. Darüber hinaus werden in ISO/IEC 27006 die Anforderungen an Stellen beschrieben, die ein ISMS auditieren oder zertifizieren. Eine Reihe weiterer Standards in der 27000er-Reihe befindet sich zurzeit in der Erstellung.

Das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene IT-Grundschriftshandbuch erläutert ebenfalls die Anforderungen an ein ISMS und ist mit ISO/IEC 27001 kompatibel.

ISO/IEC 27001

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Information security management systems - Requirements Informationssicherheitsmanagementsysteme – Anforderungen

2. Siehe dazu auch BITKOM-Leitfaden „Leitfaden IT-Risiko- und Chancenmanagement für kleine und mittlere Unternehmen“, www.bitkom.org/de/publikationen/38337_39864.aspx

Inhalt und Anwendungsbereich

Die ISO/IEC 27001 ist aus dem Teil 2 des britischen Standards BS 7799-2 hervorgegangen. Erklärtes Ziel des Standards ist es, die Anforderungen an ein ISMS im Rahmen eines Prozess-Ansatzes darzustellen.

Das Dokument beinhaltet Anforderungen an ein ISMS, das mittelbar zur Informationssicherheit beiträgt. Da das Dokument sehr generisch gehalten ist, um auf alle Organisationen unabhängig von Typ, Größe und Geschäftsfeld anwendbar zu sein, haben diese Anforderungen einen niedrigen technischen Detaillierungsgrad, wobei die Anforderungen an die Prozesse wohl definiert sind. Aufbauend auf der Norm können nationale Zertifizierungsschemata definiert werden.

Methodik

Das Dokument basiert auf dem PDCA-Modell, das im Kontext eines ISMS angewandt wird. Ein ISMS erlaubt es, ermittelte Risiken durch geeignete, in die Organisationsprozesse eingebettete Kontrollmechanismen zu reduzieren, zu verlagern oder anders zu kontrollieren. Hierbei sind die Geschäftsziele und die resultierenden Sicherheitsanforderungen als Input sowie "gemanagte" Informationssicherheit als Output anzusehen. Die transformierenden Systemprozesse sind das Aufbauen, das Umsetzen und Betreiben, das Überprüfen sowie das Aufrechterhalten und Verbessern. Ergänzend treten die Verantwortung des Managements und das Management-Review hinzu.

Als Managementstandard richtet sich das Dokument an die Geschäftsleitung und den IT-Sicherheitsbeauftragten weniger an die Umsetzungsverantwortlichen, Techniker oder Administratoren.

Zertifizierung

Der Grad der Umsetzung des Informationssicherheits-Managementsystems kann von internen oder externen Parteien (Auditoren) kontrolliert werden.

Bis Mitte Juli 2006 konnte noch eine Zertifizierung nach BS 7799-2:2002 erfolgen, die Zertifikate konnten sowohl nach BS 7799-2 als auch nach ISO/IEC 27001 ausgestellt werden. Seit Mitte Juli 2006 kann nur noch nach ISO/IEC 27001 zertifiziert werden. Das Umschreiben der Zertifikate - ausgestellt nach BS7799-2:2002 - lief im Juli 2007 ab. Alle anderen Zertifikate verlieren dann ihre Gültigkeit.

Es ist auch möglich, nur Teilbereiche eines Unternehmens zertifizieren zu lassen. Die Zertifizierung erfolgt durch akkreditierte Unternehmen, sogenannte Zertifizierungsstellen. Eine aktuelle Liste der akkreditierten Stellen, auch für andere Zertifizierungen, kann bei der TGA - Trägergemeinschaft für Akkreditierung GmbH (www.tga-gmbh.de) abgerufen werden.

Weitere Anmerkungen

Wegen der engen methodischen Anlehnung an die ISO 9000 (Qualitätsmanagement) und die ISO 14000 (Umweltmanagement) kann die ISO/IEC 27001 als ein Qualitätsstandard für Managementsysteme bezüglich Informationssicherheit angesehen werden.

Die ISO/IEC 27001:2005 wurde als DIN ISO/IEC 27001 ins Deutsche Normenwerk übernommen.

Bisherige Ausgaben

- ISO/IEC 27001:2005
- ISO/IEC 27002 (zuvor 17799)

ISO/IEC 27002 (zuvor 17799)

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Code of practice for information security management Leitfaden zum Informationssicherheitsmanagement

Inhalt und Anwendungsbereich

Die ISO/IEC 27002 ist aus dem Teil 1 des britischen Standards BS 7799-1 hervorgegangen.

Grundsätzlich ist dieser Standard dort anzuwenden, wo ein Schutzbedarf für Informationen besteht. Ziel des Dokuments ist es, Informationssicherheit als Gesamtaufgabe darzustellen, da es "guidelines and general principles for [...] information security management in an organization" enthält. In den Prozess der Informationssicherheit sind alle Bereiche der Organisation einzubeziehen, da alle an der Erhebung, Verarbeitung, Speicherung, Löschung von Informationen beteiligt sind. Der Anwendungsbereich ist somit ohne einen konkreten Bezug zu den Anforderungen in einer Organisation nicht abgrenzbar. Das Dokument richtet sich an IT-Sicherheitsbeauftragte.

Methodik

Der Standard legt Richtlinien und allgemeine Prinzipien für das Initiieren, Umsetzen, Aufrechterhalten und Verbessern des Informationssicherheitsmanagements in einer Organisation fest.

Das Sicherheitsmanagement wird thematisch angewendet auf:

- Risikoeinschätzung und –behandlung (risk assessment and treatment)
- Sicherheitsleitlinie (security policy)
- Organisation der Informationssicherheit (organizing information security)
- Management von organisationseigenen Werten (asset management)
- Personalsicherheit (human resources security)
- Physische und umgebungsbezogene Sicherheit (physical and environmental security)
- Betriebs- und Kommunikationsmanagement (communications and operations management)
- Zugangskontrolle (access control)
- Beschaffung, Entwicklung und Wartung von Informationssystemen (information systems acquisition, development and maintenance)

- Umgang mit Informationssicherheitsvorfällen (information security incident management)
- Sicherstellung des Geschäftsbetriebs (business continuity management)
- Einhaltung von Vorgaben (compliance)

Aufgrund der Bestrebungen, alle Standards, die ISMS betreffen, als ISO/IEC 27000er-Reihe zusammenzuführen, wurde ISO/IEC 17799 im Jahr 2007 in ISO/IEC 27002:2005 umbenannt.

Die ISO/IEC 27002:2005 wurde als DIN ISO/IEC 27002:2009 ins Deutsche Normenwerk übernommen.

Bisherige Ausgaben

- ISO/IEC 17799:2000
- ISO/IEC 17799:2005 (2. Ausgabe)
- ISO/IEC 27002:2005 (textgleich mit ISO/IEC 17799:2005)

ISO/IEC 27006

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Requirements for bodies providing audit and certification of information security management systems Anforderungen an Stellen, die Auditierung und Zertifizierung von Informationssicherheitsmanagementsystemen bereitstellen.

Inhalt und Anwendungsbereich

Die ISO/IEC 27006 ist aus dem Leitfaden EA-7/03 der European Accreditation Foundation hervorgegangen. Sie basiert auf der DIN EN ISO/IEC 17021 („Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren“) und ergänzt diese um die ISMS-spezifischen Anforderungen. Grundsätzlich ist dieser Standard dort anzuwenden, wo die Anforderungen an Zertifizierungs- und Auditierungsstellen von ISMS gemäß DIN ISO/IEC 27001 definiert werden. Primär dient

er somit der Akkreditierung von Zertifizierungsstellen, kann aber auch im Rahmen von „peer assessments“ oder zur Etablierung von Auditprozessen herangezogen werden. Ziel des Dokuments ist es, harmonisierte Anforderungen an alle Zertifizierungsstellen zu formulieren und diesen einen Leitfaden zur Umsetzung bereitzustellen, beispielsweise für Aspekte wie die Dauer von Audits.

Methodik

Der Standard legt Anforderungen und allgemeine Prinzipien für die Kompetenz von Auditoren und deren Überwachung, die Anforderungen an Zertifizierungsstellen (Beispiel: Ressourcen, rechtliche Stellung, Umgang mit Beschwerden) sowie den Auditierungs- und Zertifizierungsprozess fest. Er übernimmt dabei die Anforderungen der DIN EN ISO/IEC 17021 (die daher parallel zu beachten ist) und verfeinert sie für die Auditierung und Zertifizierung von ISMS gemäß ISO/IEC 27001.

Bisherige Ausgaben

- ISO/IEC 27006:2007

IT-Grundschutz

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als nachgeordnete Behörde des Bundesministeriums des Innern, bietet bereits seit 1994 das IT-Grundschutzhandbuch (IT-GSHB) an, welches detailliert IT-Sicherheitsmaßnahmen aus verschiedenen Bereichen (Technik, Organisation, Infrastruktur und Personal) sowie Anforderungen an das IT-Sicherheitsmanagement beschreibt. Damit auch der internationale Standard für Informationssicherheits-Managementsysteme abdeckt werden kann, wurde das Vorgehen nach IT-Grundschutz im Jahr 2006 an die ISO/IEC 27001 angepasst. Es ist vollständig kompatibel zur ISO/IEC 27001 und berücksichtigt weiterhin die Empfehlungen der ISO/IEC 27002. Die empfohlene Vorgehensweise bei der Umsetzung von IT-Grundschutz wird nun in so genannten BSI-Standards beschrieben, wobei Bausteine,

Gefährdungen und Sicherheitsmaßnahmen aus dem IT-Grundschutzhandbuch weiterhin in den IT-Grundschutz-Katalogen verfügbar sind:

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit [BSI1]
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise [BSI2]
- BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz [BSI3]
- IT-Grundschutz-Kataloge [GS-KAT]

Darüber hinaus werden eine Schulung (Web-Kurs) für einen kompakten Einstieg in die Materie und ein Leitfaden mit einem allgemein verständlichen Überblick über wichtige IT-Sicherheitsmaßnahmen angeboten. Zur Unterstützung der Dokumentation eines IT-Sicherheitskonzeptes werden diverse Tools angeboten, zum Beispiel das GSTOOL³ des BSI, das die IT-Grundschutz-Methodik unterstützt.

Inhalt und Anwendungsbereich

In den Dokumenten wird beschrieben, mit welchen Methoden Informationssicherheit in einem Unternehmen generell initiiert und gesteuert werden kann. Dieses Rahmenwerk kann auf die individuellen Belange eines Unternehmens angepasst werden, so dass ein effektives Informationssicherheits-Managementsystem aufgebaut werden kann. Dies schließt Kataloge mit bewährten Vorgehensweisen (best practices) und präzisen Umsetzungshilfen mit ein.

Der zentrale Anwendungsbereich des IT-Grundschutzes ist ein IT-Verbund. Hierunter ist das Zusammenspiel von organisatorischen, personellen, infrastrukturellen und technischen Komponenten zu verstehen, die zur Umsetzung von Geschäftsprozessen erforderlich sind. Die Definition eines IT-Verbunds wird demnach durch einen konkreten Bezug zu den Anforderungen eines Unternehmens abgegrenzt und erfolgt auf Basis einer Untersuchung und Bewertung der Risiken durch die verantwortliche Leitungsebene.

3. GSTOOL - Das BSI Tool zum IT-Grundschutz: www.bsi.bund.de/gstool/index.htm

Methodik

Die Erstellung der IT-Sicherheitskonzeption ist eine der zentralen Aufgaben des IT-Sicherheitsmanagements. Es müssen die erforderlichen IT-Sicherheitsmaßnahmen identifiziert und in einem Konzept dokumentiert werden. Um den unterschiedlichen Anwendungsszenarien in den Unternehmen gerecht zu werden, erfolgt eine strukturierte Vorgehensweise nach dem Baukastenprinzip. Zu übergeordneten Themen, wie unter anderem dem Sicherheitsmanagement, Notfallvorsorge sowie typischen Bereichen des technischen IT-Einsatzes sind Bausteine verfügbar, die Gefährdungen und Maßnahmenempfehlungen zusammenfassen. Im Rahmen der Erstellung eines IT-Sicherheitskonzeptes wird die Umsetzung der folgenden Schritte empfohlen:

- IT-Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung des IT-Verbunds (Auswahl der Maßnahmen, Soll-Ist-Vergleich)
- Ergänzende Sicherheitsanalyse
- Konsolidierung und Umsetzung der Maßnahmen
- Audit / Aufrechterhaltung u. Verbesserung
- Zertifizierung

Seit Anfang des Jahres 2006 können ISO/IEC 27001-Zertifikate auf der Basis von IT-Grundschutz beim BSI beantragt werden. Diese Zertifizierung umfasst eine Prüfung des IT-Sicherheitsmanagements sowie eine darüber hinausgehende Bewertung konkreter IT-Sicherheitsmaßnahmen anhand von IT-Grundschutz und bietet durch diese Kombination einen nachvollziehbareren Überblick über die eingesetzten Maßnahmen als eine reine ISO-Zertifizierung.

Um Unternehmen einen Migrationspfad anzubieten und wichtige Meilensteine bei der schrittweisen Umsetzung der Standard-Sicherheitsmaßnahmen transparent machen zu können, werden weiterhin zwei Vorstufen des eigentlichen IT-Grundschutz-Zertifikats definiert:

- das Auditor-Testat "IT-Grundschutz Einstiegsstufe" und
- das Auditor-Testat "IT-Grundschutz Aufbaustufe".

Damit bleibt das Qualifizierungsverfahren über "Einstiegsstufe" und "Aufbaustufe" weiterhin bestehen, allerdings dürfen die Testate nur von beim BSI lizenzierten Auditoren vergeben werden. Voraussetzung für die Vergabe eines ISO 27001 Zertifikats ist eine Überprüfung durch einen vom BSI lizenzierten ISO 27001-Grundschrift-Auditor. Die Aufgaben eines ISO 27001-Grundschrift-Auditors umfassen eine Sichtung der von der Organisation erstellten Referenzdokumente, die Durchführung einer Vor-Ort-Prüfung und die Erstellung eines Audit-Reports. Für die Vergabe eines ISO 27001-Zertifikats muss dieser Audit-Report zur Überprüfung dem BSI vorgelegt werden. Auf Grundlage des Audit-Reports und des Zertifizierungsschemas [BSI-ZERT] wird entschieden, ob ein Zertifikat ausgestellt werden kann oder nicht.

Weitere Anmerkungen

Das frühere IT-Grundschutz-Zertifizierungsverfahren ist inzwischen durch das Zertifizierungsverfahren für ISO-27001-Zertifikate auf der Basis von IT-Grundschutz abgelöst worden.

6.4 Sektorspezifische ISMS

ISO/IEC 27011

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 Informationssicherheitsmanagement-Leitlinien für Telekommunikationsunternehmen basierend auf ISO/IEC 27002

Inhalt und Anwendungsbereich

Der textgleich als ITU-T Recommendation X.1051 veröffentlichte internationale Standard ISO/IEC 27011 spezifiziert ISMS-Leitlinien für

Telekommunikationsunternehmen. Die Norm basiert auf ISO/IEC 27002, erweitert diesen Standard jedoch um spezifische Aspekte aus dem Bereich der Telekommunikation, die in zwei zusätzlichen Annexes dargestellt werden.

Methodik

Der Standard legt Richtlinien und allgemeine Prinzipien für das Initiieren, Umsetzen, Aufrechterhalten und Verbessern des Informationssicherheitsmanagements in einem Telekommunikationsunternehmen fest. Die Methodik entspricht der von ISO/IEC 27002.

Bisherige Ausgaben

- ISO/IEC 27011:2008 (textgleich zu ITU-T Rec. X.1051:2008)

Richtlinie VDI/VDE 2182 „Informationssicherheit in der industriellen Automatisierung“

Titel:	Informationstechnik
Arbeitsgebiet:	Automatisierungstechnische Anwendungen in der Fabrikautomation und in der Prozessindustrie
Name des Standards:	Informationssicherheit in der industriellen Automatisierung

Inhalt und Anwendungsbereich:

Die Richtlinie VDI/VDE 2182 wurde vom Fachausschuss 5.22 „Security“ der VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) erarbeitet, in dem Vertreter der herstellenden und der anwendenden Industrie sowie von Hochschulen und beratenden Unternehmen mitgewirkt haben.

Die Richtlinie beschreibt, wie die Informationssicherheit von Automatisierungsgeräten sowie automatisierten Maschinen und Anlagen durch die Umsetzung von konkreten Maßnahmen erreicht werden kann.

Methodik:

Die Richtlinie zeigt die Abhängigkeiten zwischen den Herstellern von Automatisierungsgeräten, den Maschinenbauern und System-Integratoren sowie den Betreibern von Fertigungsanlagen auf.

Die Methodik kann auf bereits existierende und auf in Entstehung befindliche Betrachtungsgegenstände angewendet werden.

Das in der Richtlinie beschriebene Vorgehensmodell basiert auf einem prozessorientierten und zyklischen Ansatz. Das Modell besteht dabei aus mehreren Prozessschritten.

Der Prozess selbst muss zu bestimmten Zeiten (zeitlich und/oder ereignisgesteuert) durchlaufen werden, um die Informationssicherheit des Betrachtungsgegenstandes über dessen gesamten Lebenszyklus sicherzustellen.

Der Betrachtungsgegenstand und dessen spezifische beziehungsweise typische Einsatzumgebung muss zunächst im Rahmen einer Strukturanalyse definiert werden. Die Strukturanalyse bildet demnach die Grundlage für eine Abarbeitung der einzelnen Prozessschritte. Weitere Grundlage bildet die Definition der Anlässe, bei welchem Ereignis respektive nach welchen Zeitabschnitten der Prozess zu starten ist. Hiermit wird klar, dass der Prozess auf einem zyklischen, iterativen Modell beruht. Eine weitere essentielle Grundlage bildet die Definition der Rollen, also derjenigen Personen, die in den jeweiligen Prozessschritten aktiv beteiligt sind und dabei eine bestimmte Aufgabe (unter anderem Verantwortlichkeit) übernehmen müssen.

Das Modell selbst sieht die folgenden acht Prozessschritte vor:

1. Assets identifizieren
2. Bedrohungen analysieren
3. Relevante Schutzziele ermitteln
4. Risiken analysieren und bewerten
5. Schutzmaßnahmen aufzeigen und Wirksamkeit bewerten

6. Schutzmaßnahmen auswählen
7. Schutzmaßnahmen umsetzen
8. Prozessaudit durchführen

Die Ergebnisse als auch der Entscheidungsweg eines jeden Prozessschrittes müssen dokumentiert werden. Am Ende steht eine Prozessdokumentation zur Verfügung, die Nachvollziehbarkeit gewährleistet und letztlich Grundlage für eine Auditierung bildet.

Die Anwendung des Vorgehensmodells (Blatt 1 der VDI-Richtlinie 2182) wird aus Sicht des Herstellers, Integrators beziehungsweise Maschinenbauers und Betreibers in den Blättern 2, 3 und 4 anhand konkreter Beispiele beschrieben. Diese werden zurzeit erarbeitet und voraussichtlich Anfang 2010 veröffentlicht (Entwurfssfassung).

Der beschriebene Prozess unterstützt den Anwender der Methodik bei der Bestimmung und Validierung einer angemessenen und wirtschaftlichen Sicherheitslösung für einen konkreten Betrachtungsgegenstand.

Bisherige Ausgaben:

- VDI/VDE 2182 Blatt 1: August 2007

Payment Card Industry Data Security Standard

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Payment Card Industry Data Security Standard v 1.2

Inhalt und Anwendungsbereich

Der Payment Card Industry Data Security Standard (PCI DSS) stellt ein Sicherheitsrahmenwerk dar und enthält eine umfassende Anforderungsliste an die Kontrollen der Bereiche physikalische und logische Sicherheit. Das Ziel des Standards ist die Verbesserung der Sicherheit von Kreditkartendaten und des Online-Zahlungsverkehrs, sofern dieser über Kreditkartenzahlungen abgewickelt wird.

Der PCI DSS wurde von den führenden Kreditkartenunternehmen entwickelt und erstmals 2005 veröffentlicht. Er richtet sich an alle Unternehmen, die Kreditkartendaten verarbeiten, speichern oder übermitteln.

Methodik

Der Standard liefert keine konkrete Methodik. Vielmehr definiert er sechs abstrakte Kontrollziele, aufgeteilt in zwölf Anforderungsbereiche mit über 230 Detailanforderungen. Die Kontrollziele sind für die gesamte Umgebung umzusetzen, welche Kreditkartendaten bearbeitet, speichert oder überträgt beziehungsweise daran angeschlossen ist.

Die Anforderungsbereiche sind:

- Installation und Wartung einer Firewall-Konfiguration
- Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden
- Schutz gespeicherter Karteninhaberdaten
- Verschlüsselung von Karteninhaberdaten bei der Übertragung über öffentliche Netze
- Verwendung und regelmäßige Aktualisierung von Antivirensoftware
- Entwicklung und Wartung sicherer Systeme und Anwendungen
- Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarfs
- Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff
- Beschränkung des physischen Zugriffs auf Karteninhaberdaten
- Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
- regelmäßiges Testen der Sicherheitssysteme und -prozesse
- Befolgen einer Richtlinie zur Informationssicherheit für Mitarbeiter und Subunternehmer

Die konkrete Ausprägung der Maßnahmen muss unternehmensspezifisch erfolgen.

Der Standard fordert darüber hinaus den Einsatz von Sicherheitstechnologien, wie beispielsweise Virens Scanner, Firewalls, Application-Layer-Firewalls oder Vulnerability-Scanner.

Können aus technischen oder geschäftlichen Gründen einzelne Kontrollen nicht erfüllt werden, können sogenannte Kompensationskontrollen eingeführt werden, die aber mindestens genauso stark sein müssen als die zu ersetzende Kontrollen.

Zertifizierung

Einzelhändler oder Dienstleister, die mehr als 1.000.000 Transaktionen pro Jahr ausführen müssen ihre Netzwerksicherheit von einem Approved Scanning Vendor (ASV) prüfen lassen. Die Experten eines ASV führen einen Schwachstellenscan des Netzwerks durch.

Die Einhaltung der weiteren Anforderungen des Standards wird durch externe Parteien (sogenannte Qualified Security Assessor (QSA)) geprüft und bescheinigt.

Zur Aufrechterhaltung des Zertifikats muss der Schwachstellenscan quartalsweise wiederholt und die Erfüllung der weiteren gestellten Anforderungen jährlich durch einen Assessor bescheinigt werden.

Unternehmen mit weniger als 1.000.000 Transaktionen müssen die Anforderungen durch ein jährliches Selbsttestat und einen vierteljährlichen Schwachstellenscan durch einen ASV bestätigen.

Weitere Anmerkungen:

Betroffene Unternehmen, die sich nicht an die Vorgaben dieses Standards halten, können mit Strafzahlungen und Sanktionen – bis hin zum Ausschluss der Teilnahme am Kreditkartenzahlungsverkehr belegt werden.

Der Standard ist auf der Webseite des PCI Security Standard Council www.pcisecuritystandards.org kostenfrei erhältlich.

Bisherige Ausgaben:

- PCI DSS 1.0: 2006
- PCI DSS 1.1: 2007
- PCI DSS 1.2: 2008

6.3 Sicherheitsmaßnahmen und Monitoring

In den folgenden Kapiteln werden ausgewiesene Standards zur Erhöhung der IT-Netzwerksicherheit einer Organisation aufgeführt. Die IT-Netzwerksicherheit beschränkt sich nicht auf das unternehmensinterne Netz sondern berührt auch die Absicherung der Netzzugänge von außen.

IT-Sicherheit kann nur gewährleistet werden, wenn eine regelmäßige Überwachung der durchgeführten Sicherheitsmaßnahmen im IT-Betrieb stattfindet. Hierzu gehört auch das systematische Erkennen von IT-Sicherheitsvorfällen und deren Bewertung sowie Behandlung.

ISO/IEC 18028 (zukünftig 27033)

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	IT Network security IT-Netzwerksicherheit

Inhalt und Anwendungsbereich

Ziel dieses Standards ist es, IT-Netzwerksicherheit mittels verschiedener Richtlinien detailliert für unterschiedliche Zielgruppen in einer Organisation zu adressieren. Dabei werden Sicherheitsaspekte bei Umgang, Wartung und Betrieb von IT-Netzwerken und deren Beziehung, auch Außenverbindungen, betrachtet. Unter Außenverbindung ist sowohl der Fernzugriff von Nutzern, als auch die logischen Verbindungen zu verstehen. Für diejenigen die innerhalb einer Organisation für die IT-Sicherheit im Allgemeinen, und im speziellen für IT-Netzwerksicherheit, verantwortlich sind, können die Informationen dieses

Standards in eigene spezifische Anforderungen adaptiert werden.

Dieser Standard besteht aus fünf Teilen:

- Part 1: Network security management
(zukünftig: Guidelines for network security)
- Part 2: Network security architecture
(zukünftig: Guidelines for the design and implementation of network security)
- Part 3: Securing communications between networks using Security Gateways
- Part 4: Remote access
- Part 5: Securing communications between networks using Virtual Private Networks (VPN)

Methodik

Das Dokument vermittelt zunächst in dem übergeordneten Teil (Teil 1) nach Klassifizierung der Netzwerkverbindungstypen die generelle Vorgehensweise, um ein geeignetes Sicherheitsniveau mittels Risikobewertung in Bezug zu den Organisationsprozessen zu erreichen. Damit findet eine enge Anlehnung an andere Standards statt. Im Teil 2 wird dann die Architektur zur IT-Netzwerksicherheit definiert. In den verbleibenden Teilen (Teil 3, 4, 5) sind spezielle Netzwerktypen und deren Einbettung in die IT-Netzwerksicherheitsarchitektur adressiert.

Weitere Anmerkungen

Das Dokument folgt in seiner generellen Vorgehensweise der ISO/IEC 27002 zur Etablierung eines IT-Sicherheitsniveaus und einer IT-Sicherheitsleitlinie.

Bisherige Ausgaben

- ISO/IEC 18028-1:2006
- ISO/IEC 18028-2:2006
- ISO/IEC 18028-3:2005
- ISO/IEC 18028-4:2005
- ISO/IEC 18028-5:2006

ISO/IEC TR 18044 (zukünftig ISO/IEC 27035)

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Information security incident management Management von Vorfällen in der Informationssicherheit

Inhalt und Anwendungsbereich

Bei ISO/IEC TR 18044 handelt es sich um einen technischen Bericht, der Hinweise und Anleitungen zur systematischen Erkennung, Evaluierung, Behandlung, Dokumentation, Reporting und Bewertung von IT-Sicherheitsvorfällen im Unternehmen gibt. Zielgruppe des Standards ist hierbei das IT-Sicherheitsmanagement-Team. Der Standard gibt des Weiteren Richtlinien für die Identifizierung und Implementierung notwendiger technischer, organisatorischer Maßnahmen und Verfahren zur Behebung oder zum Ausschluss von IT-Störungen vor.

Als Sicherheitsvorfälle werden beispielsweise genannt:

- Denial-of-Service Vorfälle,
- Ausspähung durch Dritte oder
- Unberechtigte Zugriffe auf Informationen

Methodik

Es wird vorgeschlagen, die Aktivitäten zum Management von Sicherheitsvorfällen in vier Phasen zu betrachten, und zwar

Planung und Vorbereitung

In dieser Phase werden Aktivitäten durchgeführt, um auf künftige Sicherheitsvorfälle vorbereitet zu sein.

Erkennung und Behandlung

Diese Phase umfasst die Kernaktivitäten, die durchgeführt werden, wenn ein Sicherheitsvorfall geschehen ist.

Analyse der eigenen Vorgehensweisen

Nachdem ein Sicherheitsvorfall behandelt wurde, wird abschließend analysiert, ob die eigenen Vorkehrungen und Verfahren vor und während der Erkennung und Behandlung des Sicherheitsvorfalls angemessen und wirksam genug waren.

Verbesserung

Schließlich werden Verbesserungen, die durch die vorangegangene Analysephase erkannt wurden, umgesetzt und die eigenen Vorkehrungen und Prozesse optimiert.

Bisherige Ausgaben

- ISO/IEC TR 18044:2004

ISO/IEC 18043

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Selection, deployment and operation of Intrusion Detection Systems (IDS) Auswahl, Einsatz und Betrieb von Systemen zur Erkennung des Eindringens in Netze und Systeme (IDS)

Inhalt und Anwendungsbereich

Ziel des Standards ist es, die Auswahl, Entwicklung und den Betrieb eines IDS im Unternehmen zu beschreiben. Im ausführlichen Anhang werden grundlegende Konzepte der Erkennung von Angriffen respektive des Eindringens in Netze und Systeme dargestellt.

Methodik

Die Einführung eines IDS gliedert sich in drei Phasen, in die auch der Standard eingeteilt ist:

Phase 1: Auswahl

Der Auswahl eines Systems zur Erkennung des

Eindringens in Netze und Systeme (IDS) sollte eine Risikoanalyse vorangehen, mit der festgestellt wird, ob ein IDS erforderlich ist und für welche Systeme und Netze. Für die Auswahl eines Produktes müssen verschiedene Kriterien berücksichtigt werden wie netzwerk- oder systembasiertes IDS, Performanz, Sicherheit oder Kosten für Anschaffung und Betrieb.

Es werden insbesondere weiter technische und organisatorische Aspekte wie Alarmierungsstrategien, Zusatzwerkzeuge oder Korrelation mit anderen Informationsquellen diskutiert, die für den effizienten und wirksamen Einsatz eines IDS überlegt werden müssen.

Phase 2: Einsatz

Der Einsatz eines IDS umfasst Aktivitäten, die der Inbetriebnahme des Systems dienen. Insbesondere werden die Unterschiede in der Inbetriebnahme bei netzwerk- und systembasierten IDS aufgezeigt. Auch die verschiedenen Platzierungsmöglichkeiten für ein netzwerkbasiertes IDS sowie die Sicherheitsaspekte des IDS selbst werden erläutert.

Phase 3: Betrieb

Der Standard nennt als wesentliche Aspekte beim Betrieb eines IDS die Etablierung der Betriebsprozesse, die Feineinstellung (Tuning) des IDS, die Behandlung von Schwachstellen und den Umgang mit Alarmen sowie deren Behandlung. Letztere können durch ein hauseigenes Expertenteam (CSIRT) oder aber auch durch externe Dienstleister ausgewertet werden. Schließlich wird auf die Bedeutung des Rechtsrahmens bei der Erkennung und vor allem bei der Behandlung von IT-Eingriffen hingewiesen.

Weitere Anmerkungen

Der Standard weist darauf hin, dass bestimmte Inhalte Patentansprüchen unterliegen könnten. Bei der Anwendung des Standards sollte dies vom Anwender geprüft werden.

Weiterhin wird mehrfach darauf hingewiesen, dass Planung, Auswahl und Einsatz von Systemen zur Erkennung von Angriffen in Netzen und Systemen durch

entsprechend geschultes und erfahrenes Personal erfolgen sollte.

Bisherige Ausgaben

- ISO/IEC 18043:2006

ISO/IEC 15816

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Security information objects for access control Sicherheitsobjekte für Zugriffskontrolle

Inhalt und Anwendungsbereich

Das Dokument legt eine Leitlinie und weitere Methoden zur Kurzschreibweise von Sicherheitsinformationsobjekten (Security Information Objects (SIOs)) für die Zugriffskontrolle fest. Dazu werden die allgemeinen und speziellen Anforderungen aufgestellt und eine Semantik für die verschiedenen SIO-Bausteine definiert. Dadurch wird eine einheitliche Bezeichnung von Sicherheitsinformationsobjekten unter der Anwendung der so genannten ASN.1-Notation (Abstract Syntax Notation 1) gewährleistet. Der Fokus dabei liegt auf gleich bleibenden Komponenten der SIO und nicht auf den veränderlichen. So wird eine einheitliche Begrifflichkeit für verschiedene Sicherheitsstandards geschaffen.

Weitere Anmerkungen

ITU-T publiziert ISO/IEC 18516 textgleich als Recommendation ITU-T X.841.

Bisherige Ausgaben

- ISO/IEC 15816:2002

ISO/IEC 24762

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Guidelines for information and communications technology disaster recovery services Leitfaden für Wiederherstellungsdienste für Informations- und Kommunikationstechnologien

Inhalt und Anwendungsbereich

Die ISO/IEC 24762 definiert Anforderungen und gute Praktiken an Dienste zur Wiederherstellung (Disaster recovery services) von Informations- und Kommunikationstechnologien wie bspw. Notfall-Arbeitsplätze oder Ausweich-Rechenzentren. Die Nutzung solcher Wiederherstellungsdienste ist ein möglicher Baustein in einem umfassenden Notfallplanungskonzept und kann so zur Umsetzung der Anforderungen der ISO 27001 oder 27002 im Rahmen des Risikomanagements beitragen.

Methodik

Der Standard definiert Anforderungen, die bei der Auswahl eines Dienstleisters von Wiederherstellungsdiensten durch eine Organisation oder bei der Gestaltung von Wiederherstellungsdiensten durch den Dienstleister selbst berücksichtigt werden sollen. Die Anforderungen adressieren interne wie externe Dienstleister.

Die Anforderungen beziehungsweise guten Praktiken werden in fünf verschiedenen Kapiteln dargestellt, die jeweils einen wichtigen Teilaspekt von Wiederherstellungsdiensten behandeln:

- Organisation der Wiederherstellungsdienste

Die Organisation der Wiederherstellungsdienste umfasst die Berücksichtigung von Aktivitäten im Umfeld eines Standortes, da diese Aspekte wie Stromversorgung, Telekommunikation oder Personenverkehr beeinträchtigen können. Weiterhin werden hier Themen wie Asset

Management, Entfernung Ausweich- zu Primärstandorten, Beschaffungsmanagement, Informationssicherheit, Aktivierung und Desaktivierung von Wiederherstellungsplänen oder Schulung ausgeführt.

■ Physische und umgebungsbezogene Faktoren

Neben Anforderungen an die physische Auslegung eines Standortes sind auch die technischen Infrastrukturen zum Schutz vor Feuer, Wasser, Klima oder Stromausfall für eine längere Nutzung eines Standortes auszulegen. Es werden zudem Aspekte wie Standortrisiken durch Naturphänomene oder benachbarte Industrieanlagen, gute Erreichbarkeit, physische Zutrittskontrollen, physische Sicherheit oder Beschaffenheit einer Überwachungszentrale behandelt.

■ Überlegungen zu outgesourceten Wiederherstellungsdiensten

Bei der Nutzung von outgesourceten Wiederherstellungsdiensten sind zusätzliche Überlegungen erforderlich wie bspw. Verfügbarkeit von Wiederherstellungsplänen auf Kundenseite, vorhandene Kompetenzen für Planung und Umsetzung, Auslegung von logischen Zugangskontrollen und Berechtigungskonzepten, Erhaltung der Betriebsfähigkeit der Systeme oder simultane Wiederherstellung für mehrere Kunden.

■ Auswahl von Ausweichstandorten

Bei der Auswahl eines Standortes, um Wiederherstellungsdienste zu implementieren, sollten verschiedene Faktoren berücksichtigt werden wie beispielsweise Ausbau der lokalen Infrastrukturen für Stromversorgung, Telekommunikation, Verkehrsanbindungen. Zudem wird die lokale Verfügbarkeit ausgebildeter Experten für Wiederherstellungsdienste und von HW/SW-Anbietern genannt.

■ Kontinuierliche Verbesserung

Anbieter von Wiederherstellungsdiensten sollten aktiv relevante Trends verfolgen, die Performanz ihrer Dienstleistungen regelmäßig messen, die Skalierbarkeit ihrer

Dienstleistung sicherstellen und ein aktives Risikomanagement betreiben.

Weitere Anmerkungen

Im Anhang ist eine Gegenüberstellung des Standards mit den Maßnahmen aus ISO 27002, überwiegend Abschnitt 14, enthalten.

Bisherige Ausgaben

■ ISO/IEC 24762:2008

BS 25777:2008

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	BS 25777:2008 Information and communications technology continuity management. Code of practice

Inhalt und Anwendungsbereich

Ziel des Standards ist die Etablierung und Aufrechterhaltung eines IT Continuity Managements.

Er beschreibt die einzelnen Aktivitäten, die durchzuführen sind. Der BS 25777:2008 richtet sich an IT- Service Continuity Manager und IT-Sicherheitsbeauftragte.

Methodik

Die Vorgehensweise beschreibt die vier Phasen eines IT Continuity Management Prozesses. In Phase eins wird mit dem Ermitteln der Anforderungen an die Wiederherstellung und dem Abgleich mit den bereits umgesetzten Maßnahmen zur Notfallvorsorge begonnen. Darauf folgen in Phase zwei die Definition und Auswahl der IT Continuity Strategien. Für die Definition von Strategien listet der Standard für die Kategorien Fähigkeiten und Kenntnisse, Gebäude, Technologie, Daten und Dienstleister unterstützende Informationen auf. Nach der Auswahl werden in Phase drei konkrete Maßnahmen zur

Umsetzung der Strategien definiert und implementiert. Hierunter fallen auch die Umsetzung von organisatorischen und technischen Notfallvorsorgemaßnahmen sowie das Erstellen von entsprechenden Notfallplänen. Die Mindestplaninhalte sind mit aufgeführt.

In Phase vier folgen das Testen von Maßnahmen und Plänen sowie die Schritte Überprüfung, Pflege und Verbesserung der für das IT Continuity Management implementierten Maßnahmen.

Alle Phasen werden durch eine zentrale Funktion, dem IT Continuity Programm Management gesteuert. Das Programm Management legt auch die Grundlagen und Anforderungen an das IT Continuity in Form einer Policy fest.

Weitere Anmerkungen

Der BS 25777:2008 ist eine Weiterentwicklung der PAS 77. Er kann ergänzend zum BS 25999, der als erster Standard Maßnahmen für ein zertifizierbares Business Continuity Management System definiert, angewendet werden.

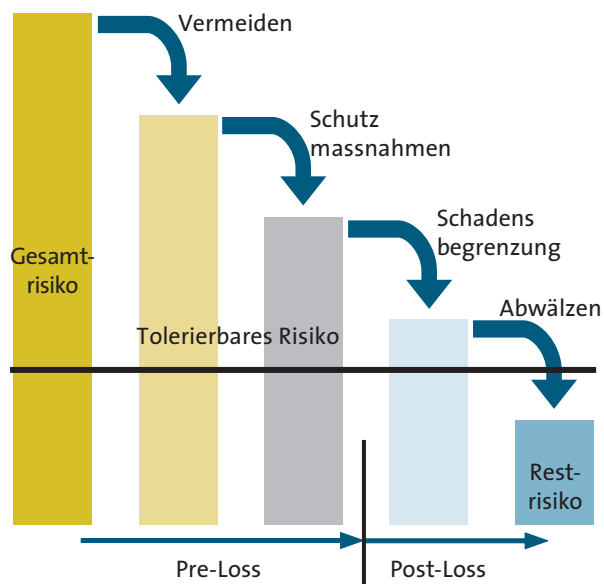


Abbildung 4

Darüber hinaus kann er auch als Unterstützung bei der Implementierung eines durch die ISO 20000 oder ISO/IEC 27002 geforderten IT Continuity Management herangezogen werden.

Bisherige Ausgaben

- PAS 77:2006
- BS 25777:2008

6.4 Risikomanagement

Definition: Risikomanagement ist der Führungsprozess zur Bewältigung der in einer Unternehmung entstehenden Risiken.

Das Ziel des IT-Sicherheitsmanagements ist die Risikoreduktion im Gesamtrisikos bis zum akzeptierbaren respektive tragbaren Restrisiko:

Risikovermeidung: Dabei werden Risiken, denen ausgewichen werden kann, vermieden. Dies kann beispielsweise die Wahl eines geeigneten Raums oder der Aufstellungsart eines Servers sein.

Risikoverminderung durch Schutzmassnahmen: Entgegen der Vermeidung, werden hier Risiken teilweise akzeptiert. Durch geeignete Schutzmassnahmen werden diese Risiken vermindert. Dies kann beispielsweise das Patchen von Systemen sein.

Risikobegrenzung: Durch geeignete Massnahmen wird bei Eintreten eines Risikos der Schaden begrenzt. Dies können beispielsweise Feuerlöschsysteme in einem Raum sein.

Risikoüberwälzung: Bei der Risikoüberwälzung wird das Risiko durch faktische oder vertragliche, teilweise oder vollständig an Dritte übertragen. Dies kann beispielsweise durch Versicherungen der Fall sein oder die Abwälzung auf Vertragspartner.

Risikoakzeptanz: Die Vermeidung, Verminderung und Überwälzung von Risiken kann die Risiken nicht vollständig ausschliessen. Das verbleibende Restrisiko muss das Unternehmen akzeptieren und selbst tragen.

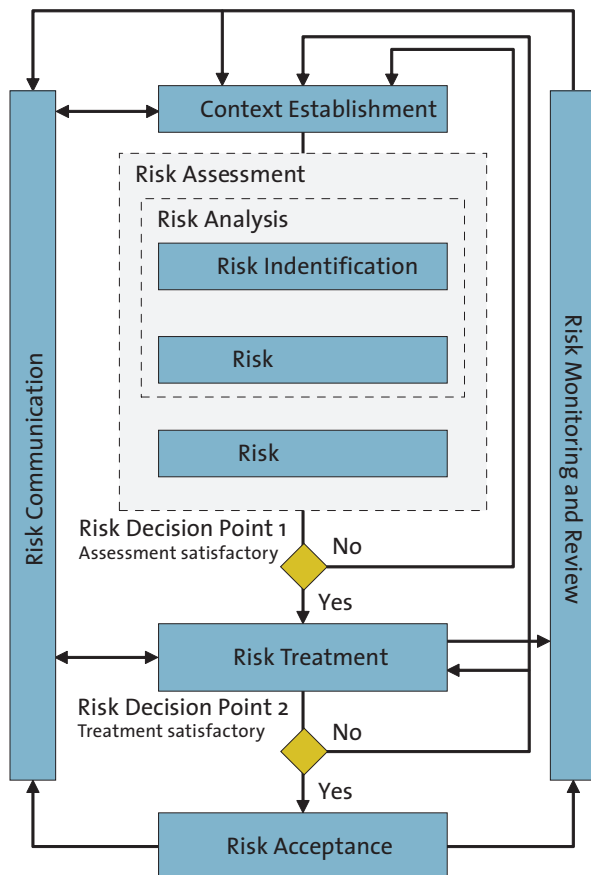


Abbildung 5: Ablauf nach ISO 27005

Das Risikomanagement ist ein ständiger Prozess. Es ist wichtig, regelmäßig die Risiken zu überarbeiten. Sind neue Risiken entstanden? Haben sich Risiken verändert? Es gilt diese Risiken zu erkennen und in einem weiteren Schritt diese zu bewerten. Folgende Schritte sind daher ständig durchzuführen:

- Risiken sind zu erkennen
- Risiken sind in Bezug auf die Geschäftseinflüsse und die Eintrittswahrscheinlichkeiten zu bewerten
- Die Eintrittswahrscheinlichkeiten und Konsequenzen dieser Risiken sind abzuschätzen

- Es müssen Prioritäten zur Abschwächung der Risiken definiert werden
- Alle involvierten Parteien und Personen müssen informiert und, falls notwendig, geschult werden
- Die getroffenen Massnahmen müssen auf ihre Effektivität überwacht werden
- Es müssen geeignete Möglichkeiten zur Abwälzung der Risiken gesucht und umgesetzt werden
- Die Restrisiken müssen bewusst getragen werden

MaRisk / MaRisk VA

Die Mindestanforderungen an das Risikomanagement (MaRisk) für Banken wurden erstmals Ende 2005 von der Bundesanstalt für Finanzdienstleistungsaufsicht herausgegeben. Basierend auf § 25a Abs. 1 des Kreditwesengesetzes (KWG) wird ein Rahmen für die Ausgestaltung des Risikomanagements für Institute dargestellt. Damit wurden die Mindestanforderungen an das Kreditgeschäft (MaK), die Mindestanforderungen an das Betreiben von Handelsgeschäften (MaH) und die Mindestanforderungen an die Ausgestaltung der internen Revision (MaIR) zusammengefasst.

Anfang 2009 wurden eine weitere Version, die für Versicherungen, Leasing- und Factoring-gesellschaften Anwendung findet veröffentlicht (MaRisk VA).

Ziel der MaRisk ist die Etablierung eines angemessenen Risikomanagements in Finanzdienstleistungs-unternehmen. Zum Risikomanagement gehören hier die Festlegung einer angemessenen Risikostrategie, entsprechende aufbau- und ablauforganisatorische Regelungen, die Einrichtung eines angemessenen internen Kontrollsystems, die Etablierung einer internen Revision sowie die Einrichtung von internen Kontrollen.

Im Abschnitt „Organisatorische Rahmenbedingungen“ (MaRisk VA) respektive „Technisch-organisatorische Ausstattung“ (MaRisk) werden auch Anforderungen an die IT-Sicherheit und Notfallplanung gestellt.

Die Vertraulichkeit, Verfügbarkeit, Authentizität und Integrität der Daten muss durch die IT-Systeme (Systeme und Anwendungen) und IT-Prozesse sichergestellt werden. Zur Gewährleistung dieser Anforderungen soll bei der Umsetzung dieser Anforderungen auf „gängige Standards“ angewendet werden. Hier werden in der MaRisk VA explizit die Standards IT-Grundschutz und die ISO 27002 genannt. Weiterhin wird gefordert, dass die Systeme vor erstmaligen Einsatz und nach wesentlichen Änderungen auf Funktionsfähigkeit getestet werden. Für zeitkritische Aktivitäten sind entsprechende Notfallkonzepte zu erstellen. Dies gilt auch für die IT-Systeme, welche die kritischen Aktivitäten unterstützen. Die Funktion der Notfallkonzepte ist auch regelmäßig durch Tests nachzuweisen.

Sollten zeitkritische Aktivitäten ausgelagert (Outsourcing) sein, so besteht die besondere Anforderung, dass internen und externen Notfallkonzepte aufeinander abgestimmt werden müssen.

Bezug zu anderen Standards

BS 25777	ISO 9000:2005 für Begriffsdefinitionen BS 25999 für Referenzen auf das Business Continuity Management ISO/IEC 20000-1, ISO/IEC 20000-2 Definition von ICT Services ISO/IEC 27001, ISO/IEC 27002 für Sicherheitsrelevante Aspekte, wie bspw. Schutz der Vertraulichkeit, Verfügbarkeit und Integrität von kritischen Daten und Erkennung von Sicherheitsvorfällen
PCI DSS	---

ISO/IEC 27005

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Information Security Risk Management Management von Informationssicherheitsrisiken

Inhalt und Anwendungsbereich

Die ISO/IEC 27005 ist aus dem Teil 2 des bisherigen ISO/IEC 13335-2 hervorgegangen. Der Standard enthält Leitlinien für ein systematisches und prozessorientiertes Risikomanagement, das gegebenenfalls auch die Einhaltung der Anforderungen an das Risikomanagements nach ISO/IEC 27001 unterstützt.

Methodik

Ein Informationssicherheitsrisiko wird definiert als Potential, dass eine Bedrohung eine Schwachstelle eines Unternehmenswertes ausnutzt und dadurch zu einem Schaden für eine Organisation führt. Zur systematischen Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken wird ein Prozess beschrieben, der als Ergebnis eine priorisierte Liste von Risiken hat, die anschließend kontinuierlich zu verfolgen sind.

Im Einzelnen definiert der Standard die folgenden wesentlichen Schritte beim Management von Informationssicherheitsrisiken:

■ Definition der Rahmenbedingungen (Context establishment)

Zur Definition der Rahmenbedingungen gehören dann die Festlegung von Kriterien zur Bewertung und Akzeptanz von Risiken, die Abgrenzung des Betrachtungsbereiches sowie die Etablierung einer Organisation für das Risikomanagement.

■ Identifizierung von Risiken (Risk identification)

Risiken werden identifiziert, indem alle Unternehmenswerte erfasst werden, die im Betrachtungsbereich liegen. Dabei ist darauf zu achten, dass Unternehmenswerte nicht nur Hardware und Software umfasst, sondern auch Geschäftsprozesse und Informationen.

Auch müssen alle relevanten Bedrohungen (Beispiel: Brand) sowie vorhandene Schwachstellen (Beispiel: fehlender Brandschutz) ermittelt werden.

Weiterhin werden alle bestehenden oder bereits geplanten Sicherheitsmaßnahmen identifiziert, da diese die Risiken beeinflussen, indem sie Eintrittswahrscheinlichkeiten oder Schadensausmaß reduzieren können.

Schließlich sind die Konsequenzen zu ermitteln, die entstehen können, wenn eine Bedrohung auf eine Schwachstelle trifft. Als Konsequenzen werden unter anderem Verlust von Geschäftsvolumen oder Reputation genannt.

■ Abschätzung von Risiken (Risk estimation)

Die Bewertung des Risikos kann auf der Grundlage verschiedener Einflussgrößen erfolgen wie Kritikalität der Unternehmenswerte, Ausmaß von Schwachstellen oder Auswirkungen bekannter Sicherheitsvorfälle.

Grundsätzlich kann die Bewertung mit qualitativen (Beispiel: „niedrig“, „hoch“, „selten“, „oft“), quantitativen (Beispiel: „10.000 €“, „85 Prozent“) oder hybriden Methoden erfolgen. In der Praxis wird für einen Anwendungszweck eine Methode gewählt, für die hinreichendes Zahlenmaterial verfügbar ist und deren Aussagekraft dem Ziel der Risikobewertung angemessen ist.

Für die Abschätzung von Risiken müssen zum einen die Konsequenzen bewertet werden, genauer gesagt das Schadensausmaß bei Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit. Zum anderen muss die Eintrittswahrscheinlichkeit eines solchen Sicherheitsvorfalls bestimmt werden.

Schließlich wird durch Kombination des Schadensausmaßes und der Eintrittswahrscheinlichkeit ein Risikoniveau bestimmt.

■ Auswertung von Risiken (Risk evaluation)

Dieser Schritt ist im Standard zur Priorisierung der Risiken vorgesehen. Die Priorisierung kann beispielsweise dadurch erfolgen, dass Risiken für Unternehmenswerte, die weniger wichtige Geschäftsprozesse unterstützen, gering priorisiert werden.

■ Behandlung von Risiken (Risk treatment)

Es ist zu entscheiden, ob ein Risiko reduziert, akzeptiert, vermieden oder übertragen wird. Während zur Reduzierung geeignete Sicherheitsmaßnahmen definiert werden müssen, können Risiken, die die Akzeptanzkriterien für Restrisiken erfüllen, unbehandelt bleiben. Ein Risiko kann vermieden werden, indem bspw. ein kritisches System in einer geschützten Umgebung aufgestellt wird, wo es besser gegen Naturkatastrophen geschützt ist. Die Übertragung von Risiken an Dritte kann über Versicherungen oder durch geeignete Vertragsformulierungen erfolgen.

■ Akzeptanz von Risiken (Risk acceptance)

Das Ergebnis der Risikobehandlung ist ein Plan, der für jedes Risiko die entsprechenden Handlungsempfehlungen aufzeigt. Die Leitungsebene einer Organisation kann entscheiden, Risiken zu akzeptieren, auch wenn diese nicht die Akzeptanzkriterien erfüllen. Für diese Fälle wird eine formelle Risikoübernahme gefordert.

■ Kommunikation von Risiken (Information security risk communication)

Informationen über Risiken sollten mit Entscheidungsträger und weiteren relevanten Mitarbeiter ausgetauscht werden.

Während die oben genannten Schritte der erstmaligen Identifizierung, Bewertung und Behandlung von Risiken dienen, definiert der Standard weitere Aktivitäten, um die Aktualität der Ergebnisse und angewandten Methoden sicherzustellen.

■ Überwachung von Risiken und Risikomanagement

Risiken sind von geschäftlichen Anforderungen und technologischen Rahmenbedingungen abhängig und damit einem Änderungsprozess unterworfen. Daher müssen die Risiken, das heißt auch Bedrohungen, Schwachstellen und weitere Einflussgrößen wiederkehrend auf Änderungen untersucht werden.

Ebenso ist der in der Organisation angewandte Ansatz für das Risikomanagement regelmäßig auf Angemessenheit zu überprüfen.

Weitere Anmerkungen

Die Anhänge des Standards enthalten unter anderem Einzelheiten und Beispiele zu Bedrohungen, Schwachstellen und Bewertungsansätzen.

Bisherige Ausgaben

- ISO/IEC 13335-2:1997
- ISO/IEC 27005:2008

7 Standards mit IT-Sicherheitsaspekten

In den folgenden Kapiteln sind generell akzeptierte, vielfach angewendete Standards/Vorschriften aufgeführt, die im Sinne einer „best-practice“ von Verbänden, Interessenvereinigungen für ihre Mitglieder erstellt worden sind. Schwerpunkte dieser Standards sind die Erreichung von Unternehmenszielen, beispielsweise durch die Verbesserung des Kontrollsystems (Cobit), oder durch die Einführung von Prozessen (ITIL) in Unternehmen. Darüber hinaus tragen sie auch zur Erhöhung der IT-Sicherheit bei, weshalb sie hier aufgeführt sind.

■ 7.1 Cobit

Inhalt und Anwendungsbereich

Das Management eines Unternehmens ist unter anderem für die Erreichung der Geschäftsziele, die Kontrolle der dabei verwendeten Ressourcen hinsichtlich Effektivität und Effizienz, die Einhaltung rechtlicher Rahmenbedingungen sowie die Handhabung der mit der Geschäftstätigkeit und dem Ressourceneinsatz verbundenen Risiken (Beispiel: Sicherheitsrisiken) verantwortlich. Dies gilt insbesondere für den Einsatz der IT als Ressource zur Realisierung von Geschäftsprozessen.

Zur Unterstützung des Managements und der damit befassten Fachabteilungen wie beispielsweise Interne Revision bei der Wahrnehmung dieser Verantwortung wurde mit Cobit (Control Objectives for Information and Related Technology) von der ISACA (Information Systems Audit and Control Association – Verband Internationaler Auditoren der Informatik) ein umfassendes Kontrollsystem, respektive Rahmenwerk geschaffen, das alle Aspekte des IT-Einsatzes von der Planung bis zum Betrieb und der Entsorgung berücksichtigt und somit eine ganzheitliche Sicht auf die IT einnimmt.

Die Cobit umfasst eine Sammlung international akzeptierter und allgemein einsetzbarer Kontrollziele. Diese repräsentieren drei Sichten auf die IT und stellen die Interessen der jeweiligen Gruppe und deren Ziele dar. Sie umfassen folgende Aspekte:

- **Managementsicht:** Unterstützung bei der Risikobehandlung in der sich ständig ändernden Umgebung und bei der Entscheidung über Investitionen, die zur Gestaltung der Kontrolle nötig sind
- **Anwendersicht:** Kontrolle und Sicherheit der Informatikdienstleistungen
- **Revisionssicht:** Einheitliche Grundlage für die Wertung der inneren Kontrollen
- Damit unterstützt Cobit die Ziele der IT-Governance⁴ im Unternehmen (als Teil der „Corporate beziehungsweise Enterprise Governance“):
- Ausrichtung der IT auf die Geschäftstätigkeit: Nutzenmaximierung
- Wirtschaftlicher Einsatz von IT-Ressourcen
- Angemessenes Risikomanagement IT-bezogener Risiken

Methodik

Cobit stellt sich als Sammlung von Informationen, Werkzeugen und Richtlinien dar, die die Sichtweisen der einzelnen durch IT-Governance angesprochenen Gruppen umfassend und spezifisch abbilden. Die Elemente von Cobit (und die jeweilige Zielgruppe im Unternehmen) sind:

- Executive Summary (Senior Executives wie CEO, CIO)
- Framework (Senior Operational Management)
- Implementation Toolset (Mittleres Management, Direktoren)
- Management Richtlinien (Mittleres Management, Direktoren)
- Kontrollziele (Mittleres Management)
- Audit-Richtlinien (Linien-Management und Revisoren)

4. Der Begriff IT-Governance bezeichnet die Organisation, Steuerung und Kontrolle der IT eines Unternehmens durch die Unternehmensführung zur konsequenten Ausrichtung der IT-Prozesse an der Unternehmensstrategie. Diese Steuerung (engl. „Governance“) durch die Unternehmensführung ist notwendig, da die Informationsfunktion in vielen Unternehmen eine zunehmend wichtige Rolle spielen und somit deren reibungsloser Ablauf und konsequente Verbesserung der IT-Prozesse ein wesentlicher Erfolgsfaktor für die Unternehmen darstellt.

Das Cobit-Framework enthält Anforderungen an die Geschäftsprozesse in den Kategorien Qualität, Sicherheit und Ordnungsmäßigkeit und den sieben Zielkriterien Vertraulichkeit, Verfügbarkeit, Integrität, Effektivität, Effizienz, Zuverlässigkeit und Einhaltung rechtlicher Erfordernisse.

Diese werden mit den verwendeten IT-Ressourcen in den Kategorien Daten, Anwendungen, Technologien, Anlagen und Personal in Zusammenhang gestellt und in die Gesamtsicht des zyklischen Prozesses „Planung & Organisation, Beschaffung & Implementierung, Betrieb & Unterstützung und Überwachung“ eingefügt, der den gesamten Lebenszyklus aller Ressourcen umfasst. Dabei steht das Ziel im Vordergrund, dass IT-Ressourcen kontrolliert geplant, entwickelt, implementiert sowie betrieben und überwacht werden. Diese vier übergeordneten Prozesse sind in insgesamt 34 kritische IT-Prozesse unterteilt, die für ein angemessenes Management der IT ausschlaggebend sind.

Durch Berücksichtigung entsprechender Prozesse und Festlegung von Kontrollziele werden die Ziele der Informationssicherheit im Unternehmen systematisch berücksichtigt. Durch Audit-Richtlinien wird der Stand der Implementierung überprüfbar und im Rahmen des zugehörigen Cobit-Reifegradmodelles mit sechs Reife-Stufen, beispielsweise nicht-existent, definierter Prozess, optimiert, differenziert bewertbar und der Fortschritt in der Implementierung messbar.

Bisherige Ausgaben

- Cobit 4.1: November 2007
- Cobit 4.0: November 2005

■ 7.2 ITIL

Inhalt und Anwendungsbereich

ITIL ist ein Best Practice Referenzmodell für das IT-Service-Management (ITSM). Das Akronym „ITIL“ leitete sich ursprünglich aus der „IT Infrastructure Library“ ab, geht

aber in der aktuellen Version 3 darüber hinaus. Dabei sieht ITIL Sicherheitsaspekte als unverzichtbare Bestandteile eines ordnungsgemäßen IT-Betriebs an. Durch Empfehlungen für die Gestaltung von Unternehmensprozessen werden die Planung, Erbringung und Optimierung von IT-Serviceleistungen mit Blick auf den Nutzen für die unternehmerischen Ziele unterstützt.

ITIL hat sich seit ihrer Einführung 1989 als weltweit akzeptierter Defacto-Standard für ITSM etabliert. Es ist eine Verfahrensbibliothek, die hierfür Best Practices liefert – also Erfahrungen aus der Praxis zusammenträgt und vermittelt. Unternehmen haben an der Erstellung und Verbesserung mitgewirkt. Im Sicherheitsumfeld besteht eine enge Verbindung zum BS 7799-Standard beziehungsweise ISO/IEC 27001.

Das Ziel von ITIL besteht im Wesentlichen darin, die bislang technologiezentrierte IT-Organisation prozess-, service- und kundenorientiert auszurichten. Damit sind die ITIL-Empfehlungen eine entscheidende Grundlage für zuverlässige, sichere und wirtschaftliche IT-Services aus Sicht eines Unternehmens.

Nachdem ITILv2 zu einer gesteigerten Akzeptanz bei Unternehmen geführt hat, wurde 2007 die ITIL Version 3 (ITILv3) herausgegeben. Mit dieser Version wurde der strategische Planungsprozess zur Verzahnung des IT-Service-Management mit der Unternehmensstrategie verbessert und dadurch die Kompatibilität zum IT-Service-Management-Standard ISO 20000 gesichert.

Methodik

Kern des Prozessmanagements sind die Services, die den Kunden angeboten werden. Ziel des Managements ist eine effiziente und effektive Gestaltung der Services. Entsprechend gliedert sich ITIL in eine Einführung und fünf spezialisierte Bücher:

- The Official Introduction to ITIL Service Management (Offizielle ITIL-Service-Management-Einführung)
- Service Strategy (Servicestrategie)
- Service Design (Serviceentwurf)
- Service Transition (Serviceüberführung)

- Service Operation (Servicebetrieb)
- Continual Service Improvement (Kontinuierliche Serviceverbesserung)

Durch die Prozesse im Bereich Service Strategy des Lifecycle-Managements werden die einzuführenden Services auf der Basis der Kunden- und Unternehmensanforderungen definiert und mit der Unternehmensstrategie verknüpft.

Im Service Design werden die Services geplant, genauer gesagt die Änderungen/Anpassungen an den bestehenden Services vorbereitet. Dazu gehören auch die Berücksichtigung der Sicherheitsanforderungen im Rahmen des Security Managements und beispielsweise die Planung von Service Level Agreements und Kapazitätsanforderungen.

Service Transition enthält die Prozesse zur Umsetzung und Einführung der Services. Dabei sollen die Risiken durch die Änderung möglichst minimiert und Beeinträchtigungen der Unternehmenstätigkeit vermieden werden.

In der Phase Service Operation werden die vollständig eingeführten Services betrieben. Schwerpunkte sind die Schnittstellen zu den Kunden und die Behebung von Störungen.

Zuletzt werden durch die Prozesse im Continual Service Improvement die Verbesserungsmöglichkeiten der Services identifiziert und die Qualität der Services kontinuierlich verbessert und optimiert. Speziell dieser fortlaufende Regelkreis zur stetigen Verbesserung der Services und Prozesse wird auch in der ISO 20000 genannt.

Im Zusammenhang der genannten Prozesse würde zum Beispiel einem neuen Service eine Servicestrategie zugrunde liegen, auf der basierend der neue Service konzipiert (Service Design) und realisiert (Service Transition) wird. Der operative Betrieb (Service Operation) wird dann kontinuierlich verbessert (Continual Service Improvement).

Zertifizierung

Personen können ihr ITIL-Wissen zertifizieren lassen. Das Zertifizierungsschema wurde mit ITILv3 vollständig überarbeitet und gliedert sich nun in drei Teile.

1. Foundation (Grundlagen Level)

Diese Stufe bildet die Basis für die ITIL-Ausbildung und vermittelt grundlegendes Wissen über die Prozesse

2. Intermediate (Weiterführendes Level)

Die weiterführende Ausbildung gliedert sich in zwei Bereiche. Der Lifecycle Stream entspricht dem bisherigen Service Manager (ITILv2) und orientiert sich an den fünf Büchern. Die zweite Möglichkeit ist der Capability Stream. Dieser entspricht dem bisherigen Practitioner (ITILv2) und bietet Zertifizierungen zu den Themen:

- Operational Support and Analysis
- Service Offerings and Agreements
- Release, Control and Validation
- Planning, Protection and Optimization

Die übergreifenden Aspekte werden in der Prüfung „Managing across the Lifecycle“ geprüft. Für jede Prüfung erhält man Learning Points und durch Erreichen einer ausreichenden Punktzahl qualifiziert man sich für die Zertifizierung zum ITIL-Expert (vormals ITIL-Diplom).

3. Advanced (Fortgeschrittenes Level)

Das Advanced Level ist bisher noch nicht umgesetzt worden. Es soll der Spezialisierung auf einzelne Themenbereiche und Prozesse dienen und die persönlichen Fähigkeiten zur praktischen Umsetzung verbessern. Eine erfolgreiche Ausbildung soll dann zum Titel ITIL Master führen.

Zusätzlich besteht die Möglichkeit, über Upgrade-Schulungen bestehende ITILv2-Zertifizierungen auf Version 3 zu aktualisieren.

Damit auch Unternehmen ihr Prozess-Management zertifizieren können, wurde der britische Standard BS

15000 geschaffen. Mittlerweile wurde die BS 15000 in den internationalen Standard ISO/IEC 20000 überführt und ist als ISO/IEC 20000:2005 veröffentlicht.

■ 7.3 IDW PS 330

Inhalt und Anwendungsbereich

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) gibt den „IDW Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330)“ heraus. Dieser Standard dient als Leitfaden für Wirtschaftsprüfer zur IT-Prüfung rechnungslegungsrelevanter IT-Systeme, wie zum Jahresabschluss.

Methodik

Der Prüfer bewertet das interne Kontrollsystem auf seine Angemessenheit und Wirksamkeit in Bezug auf inhärente Risiken der rechnungslegungsrelevanten IT-Systeme. Dazu werden folgende Schritte durchgeführt:

- Aufnahme des IT-Systems zur Einschätzung des IT-Kontrollsystems
- Aufbauprüfung des IT-Kontrollsystems
- Funktionsprüfung des IT-Kontrollsystems

Hierzu bewertet der Prüfer das eingesetzte IT-Risikomanagement und dessen Prozesse zur Identifizierung und Analyse von IT-Risiken. Bei dieser werden folgende IT-Risikoindikatoren herangezogen:

- Abhängigkeit von der IT
(Automatisierungsgrad, Systemkomplexität und Sensitivität der Daten)
- Änderungsprozesse
(Projektmanagement, Customizing, Prozess-Reengineering durch von neue IT)
- Know-How und Ressourcen
(erforderliches Spezialistenwissen, Bewusstsein der Nutzer)
- Geschäftliche Ausrichtung des Unternehmens und seiner IT

Für die Bewertung der Risikoindikatoren bietet der Standard eigene Tests an. Insbesondere wird dem Risiko des IT-Outsourcing ein eigenes Kapitel gewidmet. Abschließend ist die Sicherheit des IT-Kontrollsystems selbst und die zur Prüfung unterstützende IT zu bewerten.

Zertifizierung

Nach einer Prüfung darf ein Unternehmen angeben, dass seine Systeme gegen den Standard geprüft wurden. Da das Ergebnis und die Qualität jedoch individuell von der Erfahrung und der Einschätzung des Prüfers abhängig sind, ist das Niveau der IT-Sicherheit in zwei geprüften Unternehmen nicht unbedingt vergleichbar. Hinzu kommt, dass der Standard die Bewertung der Angemessenheit der Maßnahmen betont und der Aspekt des IT-Grundschutzes in den Hintergrund rückt.

Bisherige Ausgaben

Die endgültige Version des IDW PS 330 ist im September 2002 erschienen und direkt über das IDW gegen eine Schutzgebühr zu beziehen. Diese umfasst ca. 30 Seiten.

Eine Vorabversion vom 3.7.2001 steht unter dem Titel „Entwurf IDW Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie (IDW EPS 330)“ von der Webseite des IDW kostenlos zum Download bereit. Die Struktur stimmt mit der endgültigen Fassung überein, inhaltlich wurden nur Feinheiten bis zur endgültigen Verabschiedung geändert.

8 Vorschriften

In den folgenden Kapiteln sind bekannte Vorschriften und Gesetze, beispielsweise das Bundesdatenschutzgesetz, erläutert, die oft im Zusammenhang mit IT-Sicherheit im Unternehmen genannt werden.

Zur Erfüllung der Anforderungen von KonTraG, Basel II sowie SOX ist ein IT-Risiko- und Chancenmanagementsystem⁵ (IT-RCM) sinnvoll, welches das allgemeine Risikomanagement (RCM) des Unternehmens unterstützt.

Die Abbildung 4 verdeutlicht die Abhängigkeiten zwischen Unternehmensstrategie, IT-Strategie, IT-Risikomanagement sowie IT Sicherheitsmanagement. Die Unternehmensstrategie ist die Leitlinie für alle lang- und mittelfristigen Planungen der einzelnen agierenden Einheiten des Unternehmens, also auch der IT. Die IT-Strategie leitet sich somit aus der Unternehmensstrategie ab. Sie legt die zukünftigen Ziele der IT sowie die lang- und mittelfristigen Maßnahmen fest.

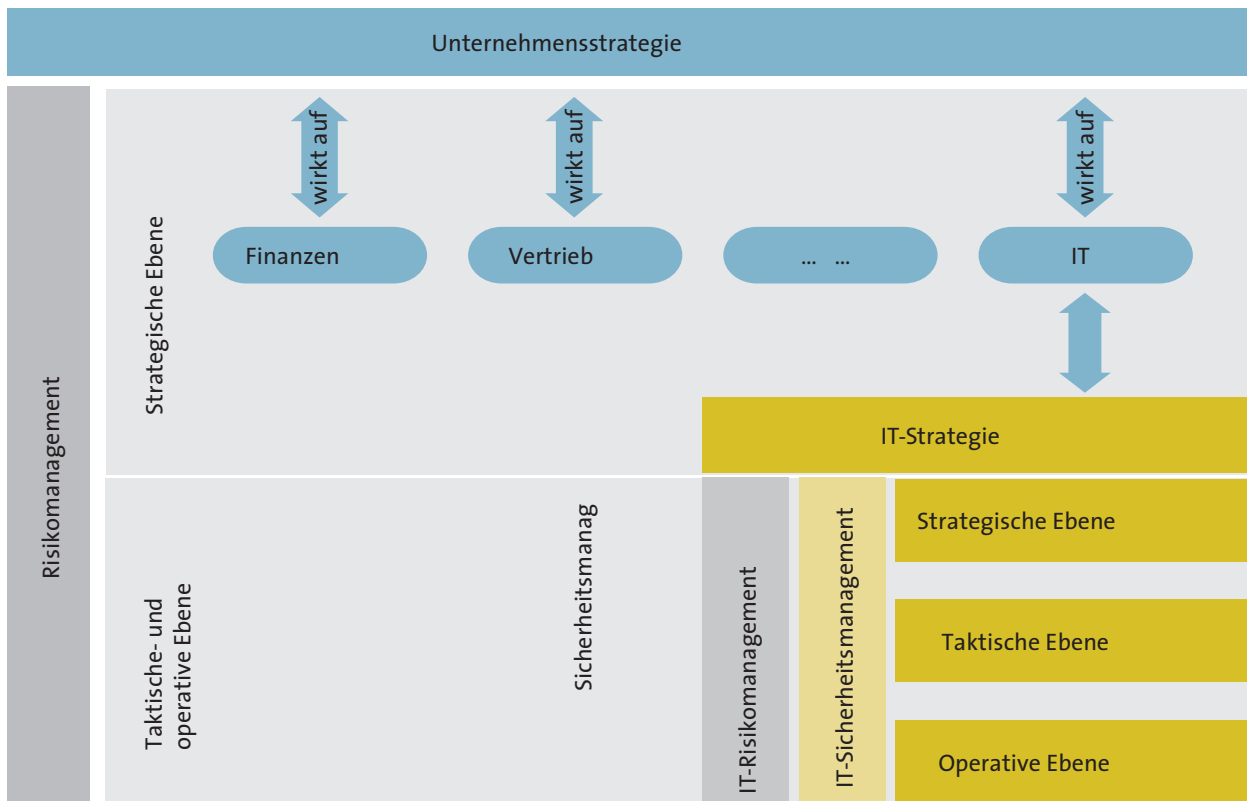


Abbildung 6: Schematische Darstellung der Beziehungen zwischen Unternehmensstrategie, IT-Strategie, IT-Risikomanagement und IT-Sicherheitsmanagement (Quelle: Hanau (selbsterstellt))

5. Siehe dazu auch BITKOM-Leitfaden „Leitfaden IT-Risiko- und Chancenmanagement für kleine und mittlere Unternehmen“, www.bitkom.org/de/publikationen/38337_39864.aspx

Das IT-Risiko- und Chancenmanagement setzt sich mit den IT-Risiken, der IT-Sicherheit und der Gewährleistung eines kontinuierlichen IT-Betriebes auseinander.

■ 8.1 KonTraG

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ist zum 1. Mai 1998 in Kraft getreten. Ausschlaggebend waren zahlreiche Unternehmenskrisen, die zunehmende Internationalisierung der Kapitalmärkte sowie eine steigende Globalisierung der Aktionärsstrukturen.

KonTraG ist kein eigenständiges Gesetz, sondern ein sogenanntes Artikelgesetz, das Ergänzungen und Änderungen in anderen Wirtschaftsgesetzen wie zum Beispiel Aktiengesetz, Handelsgesetzbuch oder dem Gesetz betreffend der Gesellschaften mit beschränkter Haftung bewirkt. Das vorhandene Aktiengesetz sowie das GmbH-Gesetz wurden entsprechend ergänzt (§ 91 II AktG, § 116 AktG) beziehungsweise werden entsprechend angewendet (§ 43 GmbHG). Nach § 91 II AktG hat der Vorstand einer AG geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit eine Entwicklung, die den Fortbestand der Gesellschaft gefährdet, früh erkannt werden kann. Diese Verpflichtung gilt nach § 43 GmbHG auch für Geschäftsführer einer GmbH und unter bestimmten Umständen auch für Personalgesellschaften wie OHG und KG.

Zielrichtung des KonTraG ist es, eine wirtschaftliche Kontrolle und Transparenz der AG und GmbH zu erreichen. Dies erfolgt durch die Einrichtung eines Überwachungssystems zur Früherkennung Existenz gefährdender Entwicklungen sowie die Verpflichtung der Geschäftsführung, ein unternehmensweites Risikomanagement zu implementieren. Es sieht eine persönliche Haftung des Vorstandes, des Aufsichtsrats und der Geschäftsführer bei Verstößen vor. Das unternehmensweite Risikomanagement umfasst auch das IT-Risikomanagement. Bei der Einführung des IT-Risikomanagements sind die entsprechenden Standards (siehe Kapitel 6.1) zu nutzen.

■ 8.2 Basel II

Die neue Baseler Eigenkapitalvereinbarung (Basel II) hat als Ausgangsbasis die im Juli 1988 veröffentlichten Basel I - Regelungen. Der Baseler Ausschuss verfolgte mit Basel I zwei Ziele: Zum einen sollte die Stabilität der internationalen Finanzmärkte gestärkt werden, zum anderen sollten bestehende Unterschiede zwischen den verschiedenen nationalen Bankaufsichtssystemen beseitigt werden, die den Wettbewerb beeinflussen. Während die Regelungen von Basel I extern vorgegeben, sehr pauschal und im Bereich des Kreditrisikos im Zeitablauf praktisch unverändert blieben, arbeiteten die Banken kontinuierlich an der Weiterentwicklung ihrer internen Risikomanagement-Verfahren. Diese ermöglichten eine individuellere Einschätzung des Kreditrisikos oder auch des operationellen Risikos. Die aufsichtsrechtlichen Kapitalanforderungen und die bankinternen Einschätzungen des Risikos liefen somit zunehmend auseinander. Gleichzeitig konnten neue Bankprodukte mit dem bestehenden aufsichtsrechtlichen Instrumentarium nur unzureichend abgebildet werden. Darüber hinaus begannen mehr und mehr Banken über komplexe Transaktionen aufsichtsrechtliche Kapitalanforderungen zu umgehen. Dies alles in Verbindung mit den Turbulenzen innerhalb des weltweiten Finanzsystems in der zweiten Hälfte der 90er Jahre machte eine grundlegende Neuordnung notwendig.

Am 26. Juni 2004 hat der Baseler Ausschuss für Bankenaufsicht das endgültige Rahmenwerk der neuen Baseler Eigenkapitalvereinbarung (Basel II) veröffentlicht. Dabei wird der frühest mögliche Starttermin für den fortgeschrittenen internen Rating Ansatz auf Ende 2007 festgesetzt.

Basel II basiert auf drei Säulen:

- Die erste Säule repräsentiert den minimalen notwendigen Eigenkapitaleinsatz. Dabei soll speziell das tatsächliche Risiko für die Banken berücksichtigt werden.
- Die zweite Säule behandelt die bankenaufsichtlichen Überprüfungsprozesse.
- Die dritte Säule befasst sich mit der Transparenz der Bilanzen für die Öffentlichkeit.

Basel II bezieht sich zunächst auf interne Bankvorschriften. Es wird jedoch allgemein erwartet, dass gleiche Maßstäbe, die an das Kreditrisiko für Banken geknüpft werden, auch an deren Kunden weitergegeben werden. Das bedeutet, dass es auch für die Privat-Wirtschaft eine direkte Abhängigkeit zwischen den Konditionen für die Geldbeschaffung und den Kreditrisiken geben wird.

Die Einrichtung von internen Kontrollen und (IT-) Sicherheitsmaßnahmen, die maßgeblich Risiken für das Unternehmen mindern, werden sich nach den bisherigen Erwartungen aufgrund von Basel II positiv auf mögliche Kreditkonditionen auswirken. Es kann davon ausgegangen werden, dass dies insbesondere für Unternehmen zutrifft, deren Geschäftsfeld stark von der IT abhängig ist.

■ 8.3 SOX

Der Sarbanes-Oxley Act (SOA oder SOX) ist ein US-amerikanisches Gesetz, welches am 23. Januar 2002 erlassen und am 20. Juli vom Präsidenten der Vereinigten Staaten unterzeichnet wurde. Maßgeblich gestaltet wurde es durch die beiden Senatoren Sarbanes und Oxley. Das Gesetz ist eine Reaktion auf diverse Finanzskandale in den USA (Beispiel: Enron und Worldcom). Ziel ist es, Investoren zu schützen und verlorengegangenes Vertrauen wiederzugewinnen, indem die Genauigkeit und Verlässlichkeit der Rechnungslegung unter anderem in Übereinstimmung mit Sicherheits-Gesetzen verbessert wird.

Dabei werden die Verantwortlichkeiten der Unternehmensführung und der Wirtschaftsprüfer grundlegend neu geregelt und Regeln für die Zusammenarbeit zwischen Wirtschaftsprüfern und Unternehmensleitung definiert. Die Unternehmen müssen nachweisen, dass sie ein funktionsfähiges internes Kontrollsystem haben, dies umfasst beispielsweise die Verfahren der Rechnungsprüfung und -zeichnung durch die Vorstände. Vorstände haften mit Gültigkeit dieses Gesetzes persönlich für die Richtigkeit der Jahresabschlüsse.

Die Regelungen des Gesetzes betreffen alle Unternehmen weltweit, die an einer amerikanischen Wertpapierbörse

notiert sind sowie unter bestimmten Voraussetzungen auch deren Tochterfirmen.

Aus Sicht IT-Sicherheit wird die größte Relevanz aus Sektion 404 des Sarbanes-Oxley Act abgeleitet. Der Sarbanes-Oxley Act will sichergestellt haben, dass die Ordnungsmäßigkeit der Verarbeitung und die Integrität der verarbeiteten relevanten Finanzdaten jederzeit gewährleistet ist. Weiterhin sollte der Zugriff auf die Finanzdaten jederzeit, und speziell zu Zeiten der Jahresabschlüsse oder Quartalsberichte sichergestellt sein. Zusätzlich soll eine Missbrauchserkennung ermöglicht werden. Schwachpunkte im IKS sollten deshalb rechtzeitig entdeckt und ausgebessert werden. Sektion 404 schreibt daher folgende Prozess im Unternehmen vor:

- Auswahl und Beurteilung eines Regelwerks für ein internes Kontrollsystem
- Dokumentation des internen Kontrollsystem (IKS)
- Überwachung des IKS.

Über die Funktionsfähigkeit dieses IKS muss in dem periodischen Unternehmensreports berichtet werden. Hierbei wird auf die Managementverantwortung zur Einrichtung und zum Betrieb vom IKS und zu den Prozessen zum Finanz-Reporting hingewiesen. Die Einsetzung eines IT-Risikomanagement spielt hierbei eine wichtige Rolle.

Der SOX ist zurzeit nur für eine Minderheit der deutschen Unternehmen bindend. Eine frühzeitige Betrachtung lohnt sich jedoch, da eine vergleichbare Regelung im deutschen resp. europäischen Rahmen nur eine Frage der Zeit zu sein scheint. Bezogen auf die IT-Sicherheit ergeben sich hier sicherlich keine vollkommen neuen Anforderungen, der Ruf nach ihr wird jedoch verstärkt.

■ 8.4 EURO-SOX

Im Juli 2006 ist die auch als EURO-SOX bezeichnete 8. EU-Richtlinie in Kraft getreten. Ziel ist die Schaffung einer international anerkannten Regelung für EU-Unternehmensabschlüsse. Hierbei gibt es deutliche Übereinstimmungen mit dem Vorbild SOX (siehe oben). So wird beispielsweise die Einrichtung eines internen

Kontrollsysteme (IKS) gefordert, das die Wirksamkeit von internen Kontrollen, Innenrevision und Risikomanagement überwachen soll.

EURO-SOX war bis spätestens 29. Juni 2008 in nationales Gesetz umzusetzen. Im Gegensatz zu SOX sind von EURO-SOX alle Kapitalgesellschaften betroffen, nicht nur börsennotierte Firmen. Damit werden auch kleinere und mittelständische Unternehmen gezwungen, sich mit den Themen Risikomanagement, IT-Security und Sicherheitsaudits intensiver auseinanderzusetzen.

Die Bundesregierung hat diese EU-Vorlage im Rahmen des Bilanzmodernisierungsgesetz (BilMoG) in geltendes nationales Recht umgesetzt. Dieses Gesetz wurde im April 2009 vom Bundesrat verabschiedet und ist am 29. Mai 2009 in Kraft getreten. Die neuen Bilanzierungsregelungen sind verpflichtend für Geschäftsjahre ab dem 1. Januar 2010 anzuwenden.

■ 8.5 BDSG

Die Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich unterliegt vor allem der Reglementierung des Bundesdatenschutzgesetzes (BDSG). Zweck des Gesetzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG). Zu diesem Zweck regelt das BDSG den Umgang mit personenbezogenen Daten unter vier grundlegenden Gesichtspunkten:

1. Zulässigkeit des Umgangs mit personenbezogenen Daten
2. Rechte der Betroffenen
3. Kontrollrechte
4. Sanktionen

Die Zulässigkeit des Umgangs mit personenbezogenen Daten stellt die Verarbeitung und Nutzung unter das sogenannte Prinzip des Verbots mit Erlaubnisvorbehalt. Das heißt, der Umgang mit personenbezogenen Daten ist grundsätzlich verboten und nur dann erlaubt, wenn sich eine Befugnis hierzu aus speziellen Regelungen zum

Datenschutz außerhalb des BDSG, aus dem als Auffanggesetz konzipierten BDSG selbst oder der Einwilligung der Betroffenen ergibt.

Zur Prüfung der Einhaltung der ordnungsgemäßen Verarbeitung personenbezogener Daten im Sinne des BDSG ist eine dreistufige Kontrolle im nicht-öffentlichen Bereich, also etwa bei Wirtschaftsunternehmen, vorgesehen. Diese soll zunächst durch den Betroffenen mittels der Ausübung seiner Rechte durchgeführt werden. Im nicht-öffentlichen Bereich liegt der Kontrolle das Prinzip der „innerbetrieblichen Selbstkontrolle“ zugrunde. Hiernach ist das Wirtschaftsunternehmen selbst für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich.

Es hat zur Sicherstellung der Durchführung der Vorschriften des BDSG in der Regel einen betrieblichen Datenschutzbeauftragten zu bestellen. Die Tätigkeit des Datenschutzbeauftragten wird wiederum nach den jeweils einschlägigen Bestimmungen des BDSG durch externe staatliche Aufsichtsbehörden überwacht.

Zur Durchsetzung der datenschutzrechtlichen Bestimmungen sieht das BDSG abschließend Sanktionen vor. Verstöße können eine zivilrechtliche Haftung nach sich ziehen, mit Geldbußen bis zu 300.000 € in einem Ordnungswidrigkeitenverfahren und in Ausnahmefällen auch mit Geld- oder Freiheitsstrafen im Rahmen eines Strafverfahrens geahndet werden. Ferner kann den Verursacher von Verstößen eine Informationspflicht gegenüber der Aufsichtsbehörde und den Betroffenen treffen.

Soweit die Verarbeitung der personenbezogenen Daten des Betroffenen auf eine rechtlich eigenständige Stelle ausgelagert wird, verändert sich die datenschutzrechtliche Ausgangssituation. Zu unterscheiden ist hierbei zwischen der so genannten Funktionsübertragung einerseits und der Auftragsdatenverarbeitung andererseits.

Bei der Auftragsdatenverarbeitung werden Datenerhebung, -verarbeitung oder -nutzung für die Erfüllung der Aufgaben und Geschäftszwecke der verantwortlichen Stelle ausgelagert. Der Auftragnehmer hat dementsprechend eine Hilfsfunktion, er leistet dem Auftraggeber

in einer oder mehreren Phasen der Datenerhebung, -verarbeitung oder -nutzung weisungsgebundene Unterstützung. Er wird gleichsam als „verlängerter Arm“ des Auftraggebers tätig, weil keine Aufgabe in ihrer Vollständigkeit, sondern lediglich ihre technische Ausführung übertragen wird.

Werden hingegen die den Verarbeitungsvorgängen zugrunde liegenden Aufgaben oder Geschäftszwecke ganz oder teilweise (mit) abgegeben oder erfüllt der Datenverarbeiter überwiegend eigene Geschäftszwecke, dann liegt eine Funktionsübertragung vor und der „ausgelagerte“ Datenverarbeiter wird selbst zur verantwortlichen Stelle. Im Detail sei hierzu auf die BITKOM-Publikation „Mustervertragsanlage zur Auftragsdatenverarbeitung“ verwiesen.

9 Evaluierung von IT-Sicherheit

IT-Sicherheitskriterien beschreiben Schemata zur Bewertung von Sicherheitsvorkehrungen in IT-Systemen und ermöglichen mit den zugehörigen Evaluationshandbüchern deren transparente Prüfung. Die europäischen Information Technology Security Evaluation Criteria (ITSEC) war jahrelang die Grundlage für den Bewertungsstandard für IT-Sicherheit in Europa. Ab Ende 1997 konnte in Deutschland alternativ die Erteilung von Sicherheitszertifikaten auf der Grundlage der Common Criteria (CC) beantragt werden, seit 2005 erfolgt ausschließlich die Prüfung nach CC.

■ 9.1 Common Criteria

Die Common Criteria (CC) sind aus den europäischen ITSEC, den amerikanischen Federal Criteria (FC) und den kanadischen CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) entstanden und werden von ISO/IEC JTC 1/SC 27 international standardisiert. Neben einem Katalog vordefinierter Funktionalitäten legen die CC Anforderungen an die Vertrauenswürdigkeit gemäß einer Vertrauenswürdigkeitsstufe fest. Die CC bieten die Möglichkeit, Sicherheitsanforderungen in vorevaluierten Schutzprofilen zusammenzufassen.

ISO/IEC 15408 (CC)

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Evaluationskriterien für IT-Sicherheit Evaluation criteria for IT security

Inhalt und Anwendungsbereich

Die Norm definiert ein Kriterienwerk für die Sicherheits-evaluierung von IT-Produkten und IT-Systemen. Der Standard besteht aus folgenden drei zusammengehörigen Teilen:

- Teil 1: Einführung und allgemeines Modell
(Introduction and general model)
- Teil 2: Funktionale Sicherheitsanforderungen
(Security functional requirements)
- Teil 3: Anforderungen an die Vertrauenswürdigkeit
(Security assurance requirements)

Teil 1 stellt das allgemeine Konzept der Evaluationskriterien vor. Grundlegende Begriffe wie Sicherheitsanforderungen, Sicherheitsziele, Schutzprofile und Evaluationsgegenstand (Target of Evaluation, TOE) werden eingeführt.

Teil 2 enthält einen Katalog vordefinierter Funktionalitäten. Die Sicherheitsanforderungen an die Funktionalität sind nach Klassen strukturiert und innerhalb einer Klasse weiter in Familien aufgeteilt. Jede Familie besitzt zumindest eine Komponente, in der die Sicherheitsanforderungen an die konkrete Funktionalität beschrieben werden. Darüber hinaus können eigene Sicherheitsvorgaben als Grundlage für die Evaluierung/Zertifizierung definiert werden.

Teil 3 spezifiziert Kriterien für die Evaluierung von Schutzprofilen und Sicherheitsvorgaben. Die Sicherheitsvorgaben werden vor Beginn der eigentlichen Evaluierung eines TOE separat evaluiert. Auch Schutzprofile können vorevaluiert werden. Die Sicherheitsanforderungen an die Vertrauenswürdigkeit sind wie in Teil 2 des Standards mittels Klassen, Familien und Komponenten strukturiert. Sie werden für jede Komponente in einem festgelegten Aufbau formuliert, der sich aus Anforderungen an den Entwickler, Anforderungen an Inhalt und Form der Prüfnachweise, sowie Anforderungen an den Evaluator zusammensetzt.

Zertifizierung

IT-Produkte und IT-Systeme können nach dem Standard, auch unter dem Namen „Common Criteria (CC)“ bekannt, zertifiziert werden. Im Rahmen der Zertifizierung wird die Sicherheit durch eine unabhängige Instanz (Prüfstellen,

Zertifizierungsstellen und die nationalen Behörden) überprüft. Die Nutzer des Standards sind in den folgenden Gruppen zu finden:

Käufer von IT-Sicherheitsprodukten (Institutionen und Verbraucher) können das Vorliegen eines Zertifikats nach ISO 15408 zu einem Maßstab ihrer Kaufentscheidung machen. Dazu müssen sie zwar den Standard nicht selbst inhaltlich benutzen, sollten aber um seine Bedeutung wissen.

Große Institutionen oder Verbände von Verbrauchern können zudem das Mittel des Schutzprofils (Protection Profile) nutzen, um selbst Anforderungen an die Sicherheit von Produkten zu definieren.

Hersteller von IT-Sicherheitsprodukten und –systemen können die Erreichung eines Zertifikats nach ISO 15408 als Marketinginstrument nutzen, um die Vertrauenswürdigkeit ihrer Produkte zu demonstrieren. Um eine Evaluation als Hersteller zu durchlaufen, ist eine intensive Arbeit mit dem Standard erforderlich.

Hersteller und Herstellerverbände können das Mittel des Schutzprofils nutzen, um Mindestanforderungen an einen Produkttyp im Markt zu etablieren.

IT-Sicherheitsberater und IT-Sicherheitsverantwortliche in Institutionen sollten die Norm ebenfalls kennen, auch wenn sie nicht selbst in Evaluationen involviert sind. Zum einen sind sie immer potentielle Nutzer evaluierter Produkte, zum anderen ist die Vorgehensweise der Common Criteria auch für andere Bereiche der IT-Sicherheit interessant.

Weitere Anmerkungen

Die Nutzung der Common Criteria erfolgt im Wesentlichen durch namhafte Hersteller etwa von Chipkarten und Chipkartenhardware oder von hochsicheren Spezialprodukten. Kleinere Hersteller von preiswerten Sicherheitslösungen scheuen oft die Kosten einer Evaluation nach den Kriterien. Staatliche Stellen gehen zunehmend dazu über, die CC zur Grundlage für die Akzeptanz sicherer Systeme

zu machen, in Deutschland wird die CC vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen und benutzt, dass auch an deren Entwicklung maßgeblich beteiligt war. Eines der Ziele des BSI ist, die Anwendung der CC auch für kleine Hersteller attraktiv zu machen.

Für Fachkreise (Hersteller von IT-Sicherheitsprodukten und professionelle Anwender solcher Produkte) gibt es in Form der jährlich stattfindenden ICC3 (International Common Criteria Conference) ein internationales Forum.

Bisherige Ausgaben

- ISO/IEC 15408:1999 (Teile 1 - 3)
- DIN ISO/IEC 15408:2001 (Teile 1 - 3)
- ISO/IEC 15408:2005 (Teile 1 - 3) (2. Ausgabe)
- DIN ISO/IEC 15408:2006 (Teile 1 - 3) (2. Ausgabe)
- ISO/IEC 15408:2008 (Teile 2 - 3) (3. Ausgabe, die dritte Ausgabe von Teil 1 erscheint voraussichtlich 2009)

ISO/IEC TR 15443

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	A framework for IT security assurance Rahmenrichtlinien zur Sicherung von IT-Sicherheit

Inhalt und Anwendungsbereich

Der technische Bericht 15443 soll eine Hilfestellung bei der Entscheidung geben, nach welchen Kriterien und mit welchen Methoden man die Vertrauenswürdigkeit in die Sicherheit von IT-Produkten, -Systemen oder –Dienstleistungen bewertet.

Er besteht aus drei Teilen:

- Teil 1: Überblick und Rahmenrichtlinie (Overview and framework)
- Teil 2: Sicherungsmethoden (Assurance methods)
- Teil 3: Analyse der Sicherungsmethoden (Analysis of assurance methods)

Insofern liegt der unmittelbare Nutzen auf der Anwenderseite. Dies betrifft natürlich weniger den Endverbraucher als die Entscheidungsvorbereitung in Firmen und anderen Organisationen. Beispiele für interessierte Leser könnten daher sein: IT-Sicherheitsverantwortliche in Organisationen, insbesondere Einkaufsverantwortliche, Verfasser von Sicherheitskonzepten, IT-Sicherheits-Berater.

Neben diesen Verantwortlichen für die Nutzung von Produkten, Systemen und Dienstleistungen sind die Kriterien natürlich auch für die Anbieter solcher Leistungen von Interesse, da sie anhand des Berichtes entscheiden können, welche Arten von Verfahren sie anwenden, um Vertrauen bei ihren Kunden zu schaffen. Für sie ist also beispielsweise interessant, welche Kombination von Qualitätsnormen, ISMS-Standards und Produktevaluierungen die Vertrauenswürdigkeit ihrer Firma und deren Produkte am besten demonstriert.

Für Leser des vorliegenden Leitfadens könnte der technische Bericht 15443 besonders von Interesse sein, da er – bezogen auf das Gebiet Vertrauenswürdigkeit – ein ähnliches Ziel wie dieser Leitfaden verfolgt. Sein Ziel ist es ja, die Bedeutung und Nutzbarkeit verschiedener Standards und Methoden in diesem Gebiet einzuordnen und damit eine Grundlage für die Entscheidung zur Nutzung eines oder mehrerer dieser Standards und Methoden zu schaffen.

Bisherige Ausgaben

- ISO/IEC TR 15443-1:2005
- ISO/IEC TR 15443-2:2005
- ISO/IEC TR 15443-3:2007

ISO/IEC 18045

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Methodology for IT security evaluation Methodik zur Evaluation von IT-Sicherheit

Inhalt und Anwendungsbereich

Der Standard ISO/IEC 18045 richtet sich primär an Evaluatoren von IT-Sicherheitsprodukten oder –systemen nach ISO/IEC 15408 (auch Common Criteria). Er ist im Wesentlichen identisch mit der in der Common-Criteria-Gemeinschaft bereits bekannten Common Evaluation Methodology (CEM). Es hat sich gezeigt, dass die Arbeit mit dem Dokument auch für die Hersteller von Produkten und Systemen oder deren Berater sehr empfehlenswert ist, um Herstellerdokumente zu schreiben, die die Anforderungen der ISO/IEC 15408 erfüllen und damit geeignet sind, eine erfolgreiche Evaluierung zu ermöglichen.

Weitere Anmerkungen

Eine freie Version dieses Dokumentes ist bereits seit längerem verfügbar und bildet den de facto Standard für die Durchführung von Evaluierungen nach ISO/IEC 15408 respektive Common Criteria. Insofern ist die Verbreitung in der angesprochenen Nutzergemeinschaft nahezu vollständig. Dies wird auch für künftige Versionen gelten, die jeweils dem Stand der 15408 angepasst sein werden.

Bisherige Ausgaben

- ISO/IEC 18045:2008 (Diese Ausgabe wurde deutlich überarbeitet in Anpassung an die gleichzeitige Version von ISO/IEC 15408.
- ISO/IEC 18045:2005

ISO/IEC TR 19791

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Security assessment of operational systems Bewertung der Sicherheit von Systemen im Betrieb

Inhalt und Anwendungsbereich

Der technische Bericht 19791 dient dazu, die Methoden des Standards 15408 auch auf die Evaluierung von in Betrieb befindlichen IT-Systemen inklusive der organisatorischen Sicherheitsmassnahmen anwendbar zu machen. Daher richtet er sich außer an Evaluatoren vorrangig an die Betreiber solcher großer IT-Systeme, wie große Firmen und Organisationen.

Bisherige Ausgaben

- ISO/IEC 19791:2006

ISO/IEC 19790 (FIPS 140-2)

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Requirements for Cryptographic Modules Anforderungen an kryptographische Module

Inhalt und Anwendungsbereich

Der Standard ISO/IEC 19790 geht als Überarbeitung aus der nationalen US-Norm "Federal Information Processing Standard Publication (FIPS PUB) 140-2, Security requirements for cryptographic modules" hervor. Er soll in Zukunft eine breitere Grundlage anbieten.

Das Dokument dient der Evaluierung von Kryptomodulen und ist daher für Hersteller und Evaluatoren solcher Module interessant, wenn sie sich an FIPS 140-2 anlehnen wollen. FIPS 140-2 beschreibt Sicherheitsanforderungen für Kryptomodule, die in Hardware oder Software realisiert sein können. Eine Anpassung an FIPS 140-3 ist abzusehen.

Die in der Norm detailliert spezifizierten Sicherheitsanforderungen adressieren insgesamt elf Teilbereiche des Designs und der Implementierung derartiger Produkte. Abhängig von der Schärfe dieser Anforderungen unter-

scheidet der Standard vier Sicherheitsniveaus, vom niedrigsten Level 1 bis zum höchsten Level 4.

FIPS 140 bildet eine wichtige Grundlage für die Zertifizierung von Produkten mit kryptographischen Funktionen und ergänzt in diesem Segment Kriterienwerke wie etwa den Common Criteria. Zu den Produkten zählen unter anderem VPN-Lösungen, Chipkarten oder Sicherheitsmodule. Als Ergebnis einer erfolgreichen Zertifizierung nach FIPS 140-2 wird nicht nur ein Gesamtsicherheitsniveau (Level 1 bis 4) bescheinigt, sondern auch individuelle Prüfergebnisse in verschiedenen Teilbereichen. Letztere sind für konkrete Anwendungsfälle vielfach aussagekräftiger als das Gesamtergebnis.

Zertifizierung

Derzeit ist nur eine Zertifizierung nach FIPS 140-2 möglich. Aktuell sind neun Prüfstellen akkreditiert, davon fünf in den USA, sowie je zwei in Kanada und in UK. Bis Ende 2004 wurden etwa 500 Zertifikate erteilt. Eine Liste der zertifizierten Produkte ist verfügbar.

Weitere Anmerkungen

Mittelfristig plant die ISO, die Anforderungen der ISO/IEC 19790 in die Systematik der ISO/IEC 15408 zu integrieren, wobei weiterhin nicht nur eine Norm für die Evaluierung aller Sicherheitsprodukte existieren wird.

Bisherige Ausgaben

- ISO/IEC 19790:2006
- ISO/IEC 19790:2006/Cor.1:2008

ISO/IEC 24759

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Test requirements for cryptographic modules Testanforderung für kryptographische Module

Inhalt und Anwendungsbereich

Der Standard 24759 dient dazu, den Anforderungen des Standards 19790 an kryptographische Module spezifische Testanforderungen zuzuordnen, anhand derer die Erfüllung dieser Anforderungen geprüft werden kann. Er richtet sich damit einerseits an Evaluatoren, vorrangig aber an die Hersteller solcher Module.

Bisherige Ausgaben

- ISO/IEC 24759:2008

ISO/IEC 19792

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Security evaluation of biometrics Evaluierung der IT-Sicherheit biometrischer Technologie

Inhalt und Anwendungsbereich

Der in Erarbeitung befindliche Standard ISO/IEC 19792 dient dazu, grundlegende Aussagen zur Evaluierung biometrischer Produkte und Systeme zu machen. Daher richtet er sich im Wesentlichen an Evaluatoren, Hersteller und potentielle Nutzer solcher Produkte und Systeme.

Weitere Anmerkungen

Da die Norm noch nicht erschienen ist, lässt sich zu ihrer Akzeptanz noch nichts sagen. Der Bedarf für das Thema ist aber zweifellos vorhanden.

Bisherige Ausgaben

- ISO/IEC FDIS⁶ 19792:2009
- ISO/IEC 19792 (voraussichtliche Veröffentlichung 2009)

ISO/IEC 21827 (SSE-CMM)

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Capability Maturity Model (SSE-CMM®) Model der Ablaufstauglichkeit

Inhalt und Anwendungsbereich

Ziel des Dokumentes ist es, Informationssicherheit mittels eines Prozess-Referenz-Modells darzustellen. Der Standard wurde Mitte der Neunziger Jahre in den USA von staatlichen Behörden und einigen Großunternehmen aus dem allgemeinen Reifegradmodell dem sog. Capability maturity model (CMM), das besonders in der Softwareentwicklung verbreitet ist, weiterentwickelt und an die speziellen Anforderungen des Sicherheitsmanagements angepasst.

Es dient dem Managen von Sicherheit in einer Organisation, indem es die einzelnen Aktivitäten – also das “Wie” – beschreibt. Der organisatorische Reifegrad in Bezug auf das Sicherheitsmanagement wird betrachtet. Das Dokument richtet sich an den IT-Sicherheitsbeauftragten einer Organisation.

Methodik

Der Standard unterteilt die sichere Systementwicklung in drei voneinander abhängige Hauptprozesse: Risiko, Vertrauenswürdigkeit und System-Lebenszyklus. Es beschreibt generische und Basis-Aktivitäten. Diese Aktivitäten befähigen eine Organisation zur Entwicklung und Einführung eines systematischen, wohl definierten Prozesses, der es ihr ermöglicht, einen bestimmbareren Reifegrad zu erreichen.

Das Prozess-Referenz-Modell hat zwei Dimensionen (domain und capability), die nach Aktivitäten strukturiert sind. Die Basis-Aktivitäten teilen sich in solche, die zur

6. Final Draft International Standard

sicheren Entwicklung erforderlich sind und andere, die zur Projektorganisation beitragen. Die 61 auf die sichere Entwicklung bezogenen Basis-Aktivitäten werden in elf Prozess-Bereiche zusammengefasst. Bezogen auf die Projektorganisation werden weitere 68 Basis-Aktivitäten (zusammengefasst in wiederum elf Prozess-Bereiche) dargestellt. Die generischen Aktivitäten, die auf alle Prozesse anwendbar sind, lassen sich fünf Fähigkeitsstufen geordnet nach aufsteigendem Reifegrad zuordnen. Folgende Reifegrade sind in SSE-CMM vorgeschlagen:

Informationssicherheit beiträgt. Die einzelnen Aktivitäten des Managementprozesses werden detailliert beschrieben und begründet. Elemente des Managementsystems werden nicht dargelegt. Der Fokus liegt also eindeutig auf dem "Prozess".

Bisherige Ausgaben

- ISO/IEC 21827:2008
- ISO/IEC 21827:2002

Reifegrad	Bezeichnung	Erläuterung
0	Nicht umgesetzt	
1	Formlos umgesetzt	Es existieren zwar einzelne Maßnahmen. Ein wirklicher Prozess ist aber kaum organisiert und noch sehr instabil
2	Geplant und weiterverfolgt	Ein stabiler Prozess existiert und wird in Projekten mit einem Projektmanagement gelebt.
3	Gut definiert	Ein Prozess ist definiert und es existiert ein Prozessmodell, das eine konsistente Implementierung des Prozesses sicherstellt.
4	Quantitativ kontrolliert	Es existieren Prozessmessungen und Prozessdatenanalysen, die für die Weiterentwicklung des Prozesses genutzt werden.
5	Kontinuierlich verbessernd	Das Management ist regelmäßig in die Prozessbewertung und die weitergehende Prozessoptimierung einbezogen.

Über vordefinierte Prüflisten lässt sich ohne großen Aufwand der eigene Status für die einzelnen Sicherheitsprozesse innerhalb einer sechsstufigen Skala ablesen und somit auch ein Benchmarking und eine Zielbeschreibung durchführen. Somit ist dies ein guter Folgeschritt nach der Etablierung eines ISMS, zum Beispiel nach ISO/IEC 27001 oder IT-Grundschutz.

Aber auch in der Entwicklungs- und Etablierungsphase lohnt sich ein Blick in diesen Standard, da hier Teilprozesse teilweise stärker konkretisiert sind, als dies etwa in BS 7799 der Fall ist.

Weitere Anmerkungen

Das Dokument ist generisch gehalten, um auf alle Organisationen unbeachtet Typ, Größe und Geschäftsfeld anwendbar zu sein. Das Dokument beinhaltet Anforderungen an den Managementprozess, der mittelbar zur

9.2 Schutzprofile

Die Sicherheit von IT-Produkten oder IT-Systemen kann nach Common Criteria zertifiziert werden. Für den Nutzer von solch einem zertifiziertem Produkt/System stellt sich die Frage, ob das Produkt/System die Sicherheitsfunktionalität hat, die der Nutzer zurzeit benötigt. Durch die Definition von Schutzprofilen (auch Protection Profile genannt) kann der Nutzer die benötigten Sicherheitseigenschaften (Funktionalität, Vertrauenswürdigkeit) festlegen. Das heißt der Nutzer erstellt ein Sicherheitskonzept für das Produkt/System, das auch Erläuterungen beinhaltet. Die Korrektheit von Schutzprofilen (vollständig, konsistent und technisch stimmig) wird in einem eigenen Evaluierungsprozess nachgewiesen und zertifiziert.

ISO/IEC TR 15446

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Guide on the production of protection profiles and security targets Leitfaden zum Erstellen von Schutzprofilen und Sicherheitsvorgaben

Inhalt und Anwendungsbereich

Der technische Bericht 15446 stellt einen Leitfaden dar, um Sicherheitsvorgaben (Security Targets, STs) und Schutzprofile (Protection Profiles, PPs) gemäß den ISO 15408 (auch Common Criteria) zu verfassen. Insofern ist er für alle potentiellen Verfasser solcher Dokumente zu empfehlen, zu denen Hersteller von IT-Sicherheitsprodukten und –systemen sowie im Fall der Schutzprofile auch Nutzer oder Nutzergruppen solcher Produkte oder Systeme gehören. Berater im Umfeld der Common Criteria sowie Evaluatoren gehören ebenfalls zur Zielgruppe.

Weitere Anmerkungen

Eine frei verfügbare Version dieses Leitfadens ist bereits seit längerem verfügbar und wird nachgefragt. Obwohl diese Version nicht den allerneuesten Stand des Wissens und der Erfahrung im Schreiben von Schutzprofilen und Sicherheitsvorgaben darstellt, ist es das einzige weit verbreitete Dokument, dass auf eine auch für Nicht-CC-Experten gut verständliche Art eine Anleitung zum

Schreiben solcher Dokumente gibt. Zum Zeitpunkt der Erstellung dieses Leitfadens wird gerade eine Revision geplant, die den Leitfaden an neuer CC-Versionen und den Stand der Technik anpassen soll.

Bisherige Ausgaben

- ISO/IEC TR 15446:2004
- ISO/IEC TR 15446:2009 (2. Ausgabe)
Diese Ausgabe wurde deutlich überarbeitet in Anpassung an die Version von ISO/IEC 15408 von 2008.

10 Spezielle Sicherheitsfunktionen 1: Normen zu kryptographischen und IT-Sicherheitsverfahren

Sichere Kommunikation zwischen Sender und Empfänger beruht auf folgenden Eigenschaften der Verarbeitung und Kommunikation: Die Information

- ist nicht unbefugt verändert worden (Integrität)
- von keinem unbefugten Dritten gelesen worden (Vertraulichkeit)
- und wirklich vom Sender an den Empfänger verschickt worden (Authentizität).

Die geforderten sicheren Eigenschaften können technisch durch verschiedene Sicherheits-mechanismen und -dienste realisiert werden, die teilweise miteinander kombiniert werden, mitunter kann der Hashwert eines Dokumentes mit einer digitalen Signatur zur Sicherstellung der Integrität des Dokumentes unterschrieben werden. In den folgenden Kapiteln werden die entsprechenden Standards der Informationstechnik erläutert.

■ 10.1 Verschlüsselung

Die Standardisierung offen gelegter Verschlüsselungsverfahren war lange umstritten. Einerseits soll sie von einer öffentlich geführten Diskussion über die Qualität der spezifizierten Mechanismen begleitet werden und nicht zuletzt aus diesem Grund zu großer Akzeptanz führen. Andererseits stellen veröffentlichte Algorithmen, die auf breiter Basis zum Einsatz kommen, für potentielle Angreifer natürlich ein besonders lohnendes Ziel dar.

Aufgrund dieser Situation gibt es sowohl offen gelegte (Beispiel: DES und AES) als auch nicht offen gelegte Verschlüsselungsstandards; zu letzteren zählt etwa die Mehrzahl der von ETSI/SAGE spezifizierten Verfahren für Telekommunikationsanwendungen.

ISO/IEC 706

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Check character systems Prüfsummensysteme

Inhalt und Anwendungsbereich

Das Dokument zielt auf die Verhinderung von Fehlern beim Eingeben oder Kopieren von Daten durch den Einsatz von festgelegten reinen oder hybriden Prüfsummensysteme, die vor allem einfache und doppelte Ersetzungs-, Umstellungs- und Verschiebungsfehler erfassen. Dies dient dem sicheren Austausch von Informationen zwischen Organisationen und wird als geeignetes Verfahren für interne Informationssysteme vorgeschlagen.

Weitere Anmerkungen

Das Dokument stellt, basierend auf den angegebenen Gruppen, Anforderungen zur erzielenden Übereinstimmung für Produkte auf, die als Prüfsumme oder Prüfsummenketten beschrieben werden. Andere Verfahren, die automatische Korrekturen vornehmen, vorsätzliche Fälschungen erkennen oder intermaschinelle Zeichenketten prüfen, behandelt das Dokument nicht.

Bisherige Ausgaben

- ISO/IEC 7064:2008
- ISO/IEC 7064:2002
- ISO 7064:1983

ISO/IEC 18033

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Encryption algorithms Verschlüsselungsalgorithmen

Inhalt und Anwendungsbereich

Das Hauptziel von Verschlüsselung ist der Schutz der Vertraulichkeit von gespeicherten oder übertragenen Daten. Ein Verschlüsselungsalgorithmus wird auf Daten (die häufig als Klartext bezeichnet werden) angewendet, so dass verschlüsselte Daten (Schlüssel- oder Chiffretext) entstehen; dieses Verfahren wird als Verschlüsselung oder Kryptierung beziehungsweise Chiffrierung bezeichnet. Der Standard ISO/IEC 18033 beschreibt die Anwendung von Verschlüsselungsalgorithmen.

Der Standard besteht aus den Teilen:

- Teil 1: Allgemeines Modell (General)
- Teil 2: Asymmetrische Schlüssel (Asymmetric ciphers)
- Teil 3: Blockschlüssel (Block ciphers)
- Teil 4: Stromschlüssel (Stream ciphers)

Teil 1 hat allgemeinen Charakter und stellt Definitionen auf, die für die weiteren Teile dieser Normenreihe gelten. Die notwendigen Eigenschaften der Verschlüsselung und bestimmte allgemeine Aspekte ihrer Anwendung werden beschrieben. Die Kriterien zur Auswahl eines in den weiteren Teilen festgelegten Algorithmusses werden definiert und der Bezug dieses Dokuments zum Verzeichnis der Algorithmen dargestellt.

Teil 2 legt eine allgemeine Methode zur Erstellung hybrider Verschlüsselungsschemata fest. Die beiden Hauptkomponenten sind ein Schlüssel verkapselnder Mechanismus (key encapsulating mechanism, KEM), der asymmetrische kryptographische Techniken zur Erzeugung und Verschlüsselung eines zufälligen symmetrischen Schlüssels benutzt, und ein Daten verkapselnder Mechanismus (data encapsulating mechanism, DEM), um tatsächlich unter Einsatz dieses symmetrischen Schlüs-

sels eine Nachricht zu verschlüsseln. Es werden jeweils mehrere KEM und DEM definiert.

Teil 3 legt Algorithmen und Eigenschaften von Blockchiffren fest, deren Blocklängen 64 Bit oder 128 Bit betragen. Die Algorithmen erfüllen die im ersten Teil dieser Normenreihe aufgestellten Anforderungen.

Teil 4 legt Algorithmen für Stromchiffren fest. Dazu gehören die Verfahren zur Erstellung von Schlüssel-Datenketten für eine Stromchiffre. Des Weiteren werden bestimmte pseudozufällige Erzeuger für die Erstellung von Schlüssel-Datenketten beschrieben.

Weitere Anmerkungen

Ein Verschlüsselungsalgorithmus sollte so beschaffen sein, dass der Chiffretext keine Informationen über den Klartext verrät, außer vielleicht dessen Länge. Jeder Verschlüsselungsalgorithmus muss außerdem für einen Entschlüsselungsprozess vorgesehen sein, der den Chiffretext in den originalen Klartext zurückwandeln muss.

Bisherige Ausgaben

- ISO/IEC 18033-1:2005
- ISO/IEC 18033-2:2006
- ISO/IEC 18033-3:2005
- ISO/IEC 18033-4:2005

ISO/IEC 10116

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Modes of operation for an n-bit block cipher Betriebsarten für einen n-bit-Blockschlüssel-Algorithmus

Inhalt und Anwendungsbereich

Das Dokument legt vier Funktionsweisen eines n-Bit Blockschlüssel-Algorithmusses fest. Dabei handelt es

sich um Electronic Codebook (ECB), Cipher Block Chaining (CBC), Output Feedback (OFB) und Cipher Feedback (CFB). Diese unterscheiden sich auch im Hinblick auf die Fortpflanzung von Übertragungsfehlern und die Resistenz gegen bestimmte Angriffe. Um die Auswahl der passenden Funktionsweise zu unterstützen, werden die Eigenschaften der vier Funktionsweisen beschrieben und verglichen.

Weitere Anmerkungen

Blockschlüssel-Algorithmen arbeiten mit Datenblöcken festgelegter Größe, die zu verschlüsselnden Nachrichten können jedoch von beliebiger Länge sein. Hauptsächlich werden vier Funktionsweisen von Blockschlüssel-Algorithmen eingesetzt, die die meisten praktischen Anforderungen an den Einsatz der Verschlüsselung bei Computern und Netzwerken abdecken.

Bei einigen Funktionsweisen kann ein Auffüllen erforderlich werden, um die benötigte Eingabelänge für den Algorithmus zu gewährleisten. Diese Auffülltechniken gehören nicht zum Anwendungsbereich dieses Dokuments.

Bisherige Ausgaben

- ISO/IEC 10116: 1991, 1997, 2006

ISO/IEC 19772

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Authenticated encryption authentisierte Verschlüsselung

Inhalt und Anwendungsbereich

Dieses Dokument legt sechs Methoden der authentisierten Verschlüsselung fest, das heißt vorgegebene Wege zur Verarbeitung eines Datenstroms mit den Sicherheitszielen Datenvertraulichkeit, Datenintegrität, Datenursprungsauthentisierung. Für die drei Methoden müssen

der Urheber und der Empfänger der geschützten Daten einen geheimen Schlüssel teilen. Das Schlüsselmanagement selbst liegt nicht im Anwendungsbereich dieses Dokuments.

Weitere Anmerkungen

Falls sowohl ein Schutz der Vertraulichkeit als auch der Integrität erforderlich ist, besteht die Möglichkeit, eine Verschlüsselung und einen Message Authentication Code (MAC) beziehungsweise eine Signatur zusammen zu benutzen. Obwohl diese Verfahren in vielen Kombinationen eingesetzt werden können, bieten nicht alle davon den gleichen Sicherheitsgrad. Daher wird beschrieben, wie die Vertraulichkeits- und Integritätsmechanismen miteinander zu kombinieren sind, um einen möglichst optimalen Sicherheitsgrad zu erreichen. Darüber hinaus können in einigen Fällen signifikante Effektivitätssteigerungen erreicht werden, indem eine einzelne Methode zur Verarbeitung der Daten festgelegt wird, die sowohl die Vertraulichkeit als auch die Integrität schützt.

Bisherige Ausgaben

- ISO/IEC 19772:2008

10.2 Digitale Signaturen

Durch das Verfahren der Digitalen Signaturen soll sichergestellt werden, dass elektronische Dokumente nicht unbemerkt verfälscht und ihre Aussteller nachweisbar identifiziert werden können. Bei Digitalen Signaturen unterscheidet man Schemata, bei denen die unterschriebene Nachricht aus der Unterschrift wieder gewonnen werden kann (Signatures giving message recovery) und solche, bei denen dies nicht der Fall ist, da ein Hashwert gebildet und dieser als eigener Nachrichtenanhang signiert wird (Signatures with appendix). Zu einer besonders attraktiven Alternative zum RSA-Verfahren oder dem Digital Signature Algorithm (DSA) haben sich in den letzten Jahren Signaturmechanismen auf der Basis elliptischer Kurven entwickelt.

ISO/IEC 9796

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Digital signature schemes giving message recovery Digitaler Unterschriftsmechanismus mit Rückgewinnung der Nachricht

Inhalt und Anwendungsbereich

Das Ziel der Normenreihe ist die Festlegung von Digitalen Unterschriftsmechanismen, die eine teilweise oder vollständige Wiederherstellung von Nachrichten bei verringertem Speicher- und Übertragungsaufwand ermöglichen.

Dieser Standard besteht aus folgenden Teilen:

- Teil 2: Mechanismen auf der Basis der Faktorisierung ganzer Zahlen (Integer factorization based mechanisms)
- Teil 3: Mechanismen auf Basis des diskreten Logarithmus (Discrete logarithm based mechanisms)

Teil 1 wurde zurückgezogen.

Teil 2 legt drei Digitale Unterschriftenschemata zur Wiederherstellung von Nachrichten fest, deren Sicherheit auf dem Faktorisierungsproblem (großer) ganzer Zahlen beruht. Die Schemata ermöglichen entweder eine teilweise oder die vollständige Wiederherstellung der Nachricht.

Teil 3 legt zwei Digitale Unterschriftenschemata fest, die eine Datenwiederherstellung ermöglichen und auf dem Problem der diskreten Logarithmen beruhen. Beide Schemata beruhen auf der Schwierigkeit des Problems der diskreten Logarithmen. Das erste Schema wird über ein Hauptfeld definiert, das zweite über eine elliptische Kurve in einem endlichen Feld. Des Weiteren definiert das Dokument ein Redundanzschema, das eine Hash-Funktion zur Zerlegung einer kompletten Nachricht benutzt,

und legt fest, wie die Grundsignaturschemen mit den Redundanzschemen verbunden werden.

Weitere Anmerkungen

Die Normenreihe beschreibt, auf welchen mathematischen Grundlagen die Digitale Unterschriftenschemata aufbauen, für welche Anwendungsfälle sie jeweils geeignet sind, und stellt Beispiele dar.

Bisherige Ausgaben

- ISO/IEC 9796:1991 (inzwischen zurückgezogen)
- ISO/IEC 9796-2: 1997, 2002
- ISO/IEC 9796-3:2000, 2006

ISO/IEC 14888

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Digital signatures with appendix Digitale Signaturen mit Anhang

Inhalt und Anwendungsbereich

Eine Digitale Signatur beim elektronischen Austausch von Informationen bietet die selben Möglichkeiten, die von einer handschriftlichen Signatur bei Postsendungen erwartet werden. Daher kann sie zur Authentisierung, Sicherheit und Nicht-Abstreitbarkeit von Daten eingesetzt werden. Das Ziel der Normenreihe ist die Festlegung von Mechanismen für Digitale Signaturen mit Anhang für Nachrichten beliebiger Länge.

Diese Internationale Norm besteht aus den Teilen:

- Teil 1: Allgemeines Modell (General)
- Teil 2: Identitätsbasierte Mechanismen (Identity-based mechanisms)
- Teil 3: Zertifikatsbasierte Mechanismen (Certificate-based mechanisms)

Teil 1 des Standards deckt die Grundprinzipien und Hauptanforderungen an Digitale Signaturen mit Anhang ab und enthält eine allgemeine Beschreibung der Signatur- und Prüfprozesse. Die verschiedenen Anwendungen wie die Authentisierung von Instanzen, Schlüsselmanagement und Nicht-Abstreitbarkeit werden in diesem Dokument nicht behandelt.

Teil 2 legt die Grundstruktur, die mathematischen Funktionen und möglichen Daten fest, die die Signatur- und Prüfprozesse einer Identitäts-basierten Digitalen Signatur mit Anhang für beliebig lange Nachrichten ausmachen. Dieser Signaturmechanismus erfordert den Dienst einer vertrauenswürdigen Stelle, die den Signaturschlüssel eines Abzeichnenden aus dessen Identität ableitet.

Teil 3 legt Mechanismen der Digitalen Signatur mit Anhang fest, deren Sicherheit auf einer Aufgabe zum diskreten Logarithmus aufbauen. Dieses Dokument enthält eine allgemeine Beschreibung eines Mechanismus für eine Digitale Signatur mit Anhang und eine Anzahl von Mechanismen, die Digitalen Signaturen mit Anhang liefern und legt für jeden dieser Mechanismen die Schlüssel- und Signaturerstellung sowie die Signaturbestätigung fest.

Weitere Anmerkungen

Digitale Signaturen mit Anhang nutzen kollisionsresistente Hash-Funktionen, die sowohl im Signatur- als auch im Prüfprozess eingesetzt werden. Im Prüfprozess ist die Hauptfunktion die Prüffunktion, die durch den Prüfschlüssel festgelegt wird. Andere Hauptfunktionen im Signaturprozess sind das Vor-Abzeichnen und das Abzeichnen. Dabei ist die Vor-Abzeichnen-funktion von der Nachricht unabhängig und die Abzeichnenfunktion wird durch den Signaturschlüssel selbst bestimmt.

Bisherige Ausgaben

- ISO/IEC 14888-1:1998, 2008
- ISO/IEC 14888-2:1999, 2008
- ISO/IEC 14888-3:1998, 2006

ISO/IEC 15946

Titel:	Informationstechnik - Sicherheitstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Cryptographic techniques based on elliptic curves Auf elliptischen Kurven aufbauende kryptographische Verfahren

Inhalt und Anwendungsbereich

ISO/IEC 15946 legt auf elliptischen Kurven aufbauende kryptographische Verfahren für öffentliche Schlüssel fest. Diese schließen die Erstellung von Schlüsseln für Systeme geheimer Schlüssel und Mechanismen für Digitale Signaturen mit ein.

Diese Internationale Normenreihe umfasst die drei Verfahren EC-DSA, EC-GDSA und EC-KCDSA.

Sie besteht aus den Teilen:

- Teil 1: Allgemeines Modell (General)
- Teil 2: Digitale Signaturen (Digital signatures) (zurückgezogen)
- Teil 3: Schlüsselbereitstellung (Key establishment) (zurückgezogen)
- Teil 4: Digitale Signaturen zur Wiederherstellung von Nachrichten (Digital signatures giving message recovery) (zurückgezogen)
- Teil 5: Erzeugung geeigneter elliptischer Kurven (Elliptic curve generation)

Teil 1 beschreibt die für den Einsatz der in den anderen Teilen beschriebenen Mechanismen notwendigen mathematischen Grundlagen und allgemeinen Techniken und bezieht sich vor allem auf die Kryptographie mit elliptischen Kurven.

Im Zuge einer Harmonisierung der verschiedenen Normungsreihen wurden die Teile 2 bis 4 dieser Normenreihe anteilig in andere Normen überführt und danach zurückgezogen.

Teil 5 wird derzeit erstellt und behandelt die Erzeugung geeigneter elliptischer Kurven zur Anwendung mit den in den anderen Teilen beschriebenen Verfahren. Das Auffinden geeigneter elliptischer Kurven hat, wie übrigens auch die Parametrisierung anderer Schlüsselverfahren, wesentliche Bedeutung für die Sicherheit einer Anwendung.

Weitere Anmerkungen

Öffentliche Schlüssel- (sog. Public-Key)-Verfahren auf Basis elliptischer Kurven sind dem RSA-Algorithmus und anderen Public-Key Verfahren der ersten Generation in Bezug auf Sicherheit und Performance deutlich überlegen; so kann mit elliptischen Kurven der Schlüssellänge 160 Bit bereits ein höheres Sicherheitsniveau erreicht werden als mit 1024-Bit RSA. Die Anwendung dieser Normenreihe beschränkt sich auf kryptographische Techniken, die auf elliptischen Kurven aufbauen, die über endliche Felder mit Potenzen erster Ordnung (inklusive der Sonderfälle der ersten Ordnung und Kennzahl Zwei). Die Darstellung des zugrunde liegenden endlichen Feldes (das heißt dessen Basis genutzt wird) liegt außerhalb des Anwendungsbereichs dieses Dokuments.

Bisherige Ausgaben

- ISO/IEC 15946-1:2002, 2008
- ISO/IEC 15946-2:2002 (inzwischen zurückgezogen)
- ISO/IEC 15946-3:2002 (inzwischen zurückgezogen)
- ISO/IEC 15946-4:2004 (inzwischen zurückgezogen)

■ 10.3 Hash-Funktionen und andere Hilfsfunktionen

Eine kryptographische Streuwertfunktion beziehungsweise Hash-Funktion komprimiert (beliebig lange) Nachrichten zu einem nicht manipulierbaren Prüfwert fester Länge (meist 128 oder 160 Bit). Hash-Funktionen sind daraufhin optimiert, so genannten Kollisionen zu vermeiden.

ISO/IEC 10118

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	hash functions Hash-Funktionen

Inhalt und Anwendungsbereich

Der Standard ISO/IEC 10118 beschreibt Aufbau und Anwendung von Hash-Funktionen. Er besteht aus den Teilen:

- Teil 1: Allgemeines Modell (General)
- Teil 2: Hash-Funktionen auf Basis eines n-bit-Blockschlüssel- Algorithmus
(Hash-functions using an n-bit block cipher)
- Teil 3: Fest zugeordnete Hash-Funktionen (Dedicated hash-functions)
- Teil 4: Hash-Funktionen auf Basis modularer Arithmetik (Hash-functions using modular arithmetic)

Teil 1 beschreibt grundlegende Konzepte von Hash-Funktionen und enthält Definitionen, Abkürzungen und Anforderungen, die gleichermaßen für alle anderen Teile dieser Normenreihe gelten.

Teil 2 legt zwei Hash-Funktionen fest, die einen n-Bit Blockschlüssel-Algorithmus nutzen. Daher sind sie für eine Umgebung geeignet, in der ein solcher Algorithmus schon vorhanden ist. Sie bauen auf einem bestimmten Verkettungsmodus auf, der teilweise als MDC (Manipulation/Modification – Detection Code) bezeichnet wird.

Teil 3 legt fest zugeordnete Hash-Funktionen fest, das heißt für einen speziellen Zweck entwickelte Streuwertfunktionen. Die in diesem Teil benutzten Hash-Funktionen bauen auf der iterierten Anwendung von Kompressionsfunktionen auf. Dieser Teil legt sieben verschiedenen Kompressionsfunktionen fest.

Teil 4 legt zwei kollisionsresistente Hash-Funktionen fest, die eine modulare Arithmetik nutzen, um eine Kompressionsfunktion und eine Verringerungsfunktion anzuwenden. Diese Hash-Funktionen kürzen Nachrichten von beliebiger aber begrenzter Länge zu einem Hash-Code, dessen Länge durch die Länge der für die Verringerungsfunktion genutzten Primzahl bestimmt wird.

Weitere Anmerkungen

Hash-Funktionen bilden beliebige Bitfolgen in einem vorgegebenen Bereich ab. Sie können zur Reduktion einer Nachricht zu einem kurzen Abdruck genutzt werden, der als Eingabe in einen Digitale Signaturmechanismus dient, oder damit sich der Benutzer auf eine vorgegebene Bitfolge festlegt, ohne dass diese Zeichenfolge verraten wird. Die in eine Hash-Funktion einzugebende Zeichenkette wird Datenfolge, die ausgegebene Zeichenfolge Hash-Code genannt.

Bisherige Ausgaben

- ISO/IEC 10118-1:1994, 2000
- ISO IEC 10118-2:1994, 2000
- ISO IEC 10118-2 COR2:2007
- ISO/IEC 10118-3:2003, 2004
- ISO/IEC 10118-4:1998

ISO/IEC 18031

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Random bit generation Erzeugung von Zufallszahlen

Inhalt und Anwendungsbereich

Dieses Dokument legt ein konzeptionelles Modell eines Zufallszahlengenerators für kryptographische Zwecke mit seinen Elementen fest. Dazu beschreibt es die für einen nicht-deterministischen Zufallszahlengenerator beziehungsweise einen deterministischen Pseudozufallszahlengenerator notwendigen Hauptelemente sowie deren Eigenschaften und Sicherheitsanforderungen.

Das Dokument bietet umfassende Informationen von der Festlegung eines Begriffsmodells, der Terminologie und der Bausteine eines Zufallsbit-Erzeugers bis hin zu einem Leitfaden für die Entwicklung eines (Pseudo- oder) Zufallszahlengenerators.

Weitere Anmerkungen

Die Erzeugung von zufälligen Bitfolgen für den kryptographischen Einsatz ist anspruchsvoll und für die Wirksamkeit bestimmter kryptographischer Verfahren äußerst wichtig. Falls beispielsweise der Schlüssel eines symmetrischen Algorithmus über seine Vorhersagbarkeit bestimmt werden kann, kann die Sicherheit des Algorithmus gefährdet sein.

Das Dokument bietet neben der Erzeugung binärer Zufallsfolgen ebenso einen Leitfaden für die Umwandlung von Bitfolgen in Zufallszahlen an. Darüber hinaus notwendige Techniken zur statistischen Prüfung von Zufallszahlengeneratoren und ihr detaillierter Aufbau, werden in diesem Dokument nicht behandelt.

Bisherige Ausgaben

- ISO/IEC 18031:2005

ISO/IEC 18032

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Prime number generation Primzahlerzeugung

Inhalt und Anwendungsbereich

Dieses Dokument behandelt die Erzeugung von Primzahlen, wie sie für kryptographische Protokolle und Algorithmen gebraucht werden. Es legt Methoden fest, mit denen Zahlen darauf getestet werden können, ob sie Primzahlen

sind, und zeigt die Anwendung dieser Methoden zur Primzahlenerzeugung und -prüfung. Weiterhin definiert es Varianten der Methoden zur Erzeugung von Primzahlen für die Erfüllung bestimmter kryptographischer Anforderungen.

Weitere Anmerkungen

Die in diesem Dokument festgelegten Methoden zur Erzeugung, Prüfung und Bestätigung von Primzahlen können bei kryptographischen Systemen angewendet werden, die auf den Eigenschaften von Primzahlen aufbauen (zum Beispiel einige asymmetrische Verfahren). Die Festlegungen zu den beschriebenen Tests beschreiben in einfachster Weise, welche Eigenschaften getestet werden müssen.

Bisherige Ausgaben

- ISO/IEC 18032: 2005

■ 10.4 Authentifizierung

Informationstechnische Mechanismen zur Authentifizierung von Kommunikationspartnern bestehen aus einer Abfolge von Berechnungs- und Kommunikationsschritten und beinhalten zumindest zwei verschiedene Instanzen das heißt technische Ausprägungen für juristische oder natürliche Personen. Abhängig vom Typ der Berechnungsschritte unterscheidet man Mechanismen auf der Basis symmetrischer Blockschlüssel, digitaler Signaturen, kryptographischer Prüfsummen und von Zero-Knowledge-Protokollen. Letztere ermöglichen die Begrenzung der Informationsmenge, die in einem kryptographischen Protokoll von der beweisenden zur verifizierenden Instanz fließt.

Mechanismen zur Authentifizierung von Daten basieren auf der Berechnung respektive Verifizierung kryptographischer Prüfsummen und werden häufig als Authentifizierungs-Codes oder MACs (Message Authentication Codes) bezeichnet.

ISO/IEC 9798

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Entity authentication Authentisierung von Instanzen

Inhalt und Anwendungsbereich

Die Normenreihe legt informationstechnische Mechanismen zur Authentisierung von Instanzen fest. Diese werden zur Bestätigung eingesetzt, dass eine Instanz tatsächlich die ist, die sie vorgibt zu sein. Eine zu authentisierende Instanz beweist ihre Identität, indem sie zeigt, dass sie einen geheimen Authentisierungsschlüssel kennt. Die Mechanismen sind für den technischen Austausch von Informationen zwischen Instanzen und, wo notwendig, mit einem vertrauenswürdigen Dritten (Trusted Third Party, TTP) gedacht.

Der Standard besteht aus den Teilen:

- Teil 1: Allgemeines Modell (General)
- Teil 2: Mechanismen auf Basis von symmetrischen Verschlüsselungsalgorithmen (Mechanisms using symmetric encipherment algorithms)
- Teil 3: Authentifikation von Instanzen unter Benutzung eines Algorithmus mit öffentlichem Schlüssel (Mechanisms using digital signature techniques)
- Teil 4: Mechanismen auf Basis einer kryptographischen Prüffunktion (Mechanisms using a cryptographic check function)
- Teil 5: Mechanismen auf Basis von Zero-Knowledge-Techniken (Mechanisms using zero-knowledge techniques)
- Teil 6: Mechanismen auf Basis von manuellem Datentransfer (Mechanisms using manual data transfer)

Teil 1 führt in die grundlegenden Konzepte ein und beschreibt ein allgemeines Modell für die Authentifizierung von Instanzen.

Teil 2 legt vier Mechanismen zur Authentisierung von Kommunikationspartnern fest, die symmetrische Verschlüsselungsalgorithmen nutzen. Diese Mechanismen zeichnen sich dadurch aus, dass die zu authentisierenden Kommunikationspartner ihre Identitäten dadurch beweisen, dass sie einen geheimen Authentisierungsschlüssel kennen.

Teil 3 legt fünf Mechanismen zur Authentisierung von Kommunikationspartnern fest, die einen Algorithmus für öffentliche Schlüssel und eine Digitale Signatur zur Bestimmung der Identität einer Instanz nutzen. Die Anwendung dieses Teils ist nicht auf einen bestimmten Algorithmus begrenzt; jeder Algorithmus für öffentliche Schlüssel, der die Anforderungen der Authentisierungsalgorithmen erfüllt, kann eingesetzt werden.

Teil 4 legt vier Mechanismen zur Authentisierung von Kommunikationspartnern fest, die eine kryptographische Prüffunktion nutzen, und beschreibt den geforderten Inhalt von Nachrichten, der zur Aufstellung der Rahmenbedingungen notwendig ist.

Teil 5 legt drei Mechanismen zur Authentisierung von Instanzen fest, die Zero-Knowledge Techniken nutzen. Mit Zero-Knowledge bezeichnet man dabei die Eigenschaft, nur die Gültigkeit einer Authentisierung aber kein darüberhinausgehendes Wissen ableiten zu können. Alle in diesem Teil der Normenreihe festgelegten Mechanismen bieten die einseitige Authentisierung. Diese Mechanismen sind zwar nach den Prinzipien des Zero-Knowledge aufgebaut, können gemäß der genauen (mathematischen) Definition aber keine völlige Zero-Knowledge-Eigenschaft darstellen.

Teil 6 legt vier Mechanismen zur Authentisierung von Instanzen fest, die auf einem manuellen Datentransfer zwischen den authentisierenden Geräten aufbauen. Diese vier Mechanismen sind für unterschiedliche Gerätetypen geeignet.

Bisherige Ausgaben

- ISO/IEC 9798-1:1991; 1997
- ISO/IEC 9798-2:1994; 1999
- ISO/IEC 9798-2 COR1:2004
- ISO/IEC 9798-3:1993; 1998
- ISO/IEC 9798-4:1995; 1999
- ISO/IEC 9798-5:1999; 2004
- ISO/IEC 9798-6:2005

ISO/IEC 9797

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Message Authentication Codes (MACs) Nachrichten-Authentisierungs-codes (MACs)

Inhalt und Anwendungsbereich

Die Normenreihe legt Algorithmen für Nachrichten-Authentisierungs-codes (Message Authentication Code, MAC) das heißt Datenvollständigkeitsmechanismen fest, die eine kurze Zeichenkette (den MAC) als eine komplexe Funktion aus jedem Datenbit und einem geheimen Schlüssel erzeugen. MAC-Algorithmen werden eingesetzt, um die Integrität von Daten zu gewährleisten. Ihr Zweck ist die Entdeckung jeder unautorisierten Veränderung der Daten wie Löschen, Einfügen oder Transportieren von Objekten innerhalb der Daten.

Der Standard besteht aus den Teilen:

- Teil 1: Mechanismen auf Basis eines Blockschlüssel-Algorithmus (Mechanisms using a block cipher)
- Teil 2: Mechanismen auf Basis einer dedizierten Hash-Funktion (Mechanisms using a dedicated hash-function)

Teil 1 legt sechs MAC-Algorithmen fest, die auf dem CBC-Modus einer Blockchiffre beruhen. Zusätzlich werden drei Auffüllmethoden beschrieben. Das Auffüllen wird notwendig, wenn die Länge des Datensatzes nicht ein Vielfaches der Blocklänge n ist.

Teil 2 legt drei MAC-Algorithmen fest, die einen geheimen Schlüssel und eine Hash-Funktion mit einem n -Bit Ergebnis nutzen, um einen m -Bit MAC zu berechnen. Insbesondere werden die Konstruktionsschemata HMAC und MDx-MAC spezifiziert.

Weitere Anmerkungen

MAC-Algorithmen ermöglichen außerdem die Authentifizierung des Datenursprungs. Damit kann sichergestellt werden, dass eine Nachricht tatsächlich von einer Instanz kommt, die in Besitz eines bestimmten geheimen Schlüssels ist.

Bisherige Ausgaben

- ISO/IEC 9797-1:1999
- ISO/IEC 9797-2: 2002
- ISO/IEC 9797:1994 (zurückgezogen)

■ 10.5 PKI-Dienste

Unter dem Begriff Public-Key Infrastruktur (PKI) werden die Instanzen zusammengefasst, die für den Einsatz asymmetrischer Kryptographie (insbesondere digitaler Signaturen) in offenen Systemen erforderlich sind. Zu den wichtigsten Aufgaben einer PKI zählen die Registrierung der Nutzer sowie das Ausstellen, Verwalten und ggf. Prüfen von Zertifikaten, welche die Grundlage für die informationstechnische Fälschungssicherung darstellen.

Die Beweiskraft elektronischer Dokumente hängt entscheidend davon ab, ob Urheber und Inhalt, aber auch der Erstellungszeitpunkt zweifelsfrei und fälschungssicher feststellbar sind. Aus diesem Grund spielen neben digitalen Signaturen auch Zeitstempeldienste eine

wichtige Rolle für die vertrauenswürdige elektronische Kommunikation.

ISO/IEC 15945

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Specification of TTP services to support the application of digital signatures Spezifikation der Dienste eines vertrauenswürdigen Dritten zur Anwendung auf Digitale Signaturen

Inhalt und Anwendungsbereich

Dieser Standard definiert technische Dienste für einen vertrauenswürdigen Dritten (Trusted Third Parties – TTP, in der Regel Trust Center), die im Zusammenhang mit digitalen Signaturen notwendig sind. Beispiele solcher Dienste sind Registrierung, Zertifizierung, Schlüsselerzeugung und Gegen-Zertifizierung. Erst die damit verbundene Interoperabilität macht auch das kommerzielle Anbieten solcher Dienste lohnend. Die Schwerpunkte des Dokumentes liegen auf der technischen Implementierung, Interoperabilität und technischen Anforderungen dieser Dienste.

Das Dokument richtet sich primär an die Betreiber von Trust-Centern (etwa Zertifizierungsdiensteanbieter), aber auch an die Hersteller von technischen Systemen für die Erbringung oder Nutzung solcher Dienste.

Weitere Anmerkungen

ITU-T publiziert ISO/IEC 15945 textgleich als Recommendation ITU-T X.843.

Bisherige Ausgaben

- ISO/IEC 15945:2002

ISO/IEC TR 14516

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Guidelines for the use and management of Trusted Third Party services Richtlinien für die Nutzung und das Management eines vertrauenswürdigen Dritten

Inhalt und Anwendungsbereich

Dieser Leitfaden behandelt Fragen des Managements und der Nutzung eines vertrauenswürdigen Dritten (in der Regel Trust Center) im Rahmen einer Public-Key Infrastruktur (PKI). Insbesondere spezifiziert er grundlegende Aufgaben und Dienste sowie die Rollen und Verantwortungsbereiche von Trusted Third Parties (TTPs) und deren Nutzern.

Das Dokument legt verschiedene Kategorien wie Zeitstempeldienste, Unleugbarkeit, Schlüsselverwaltung, Zertifikatsverwaltung und elektronische Beurkundung fest, in die Trusted Third Parties (TTP) Dienste eingeteilt werden können. Innerhalb der einzelnen Kategorien sind logisch zu einander gehörenden Dienste zusammen gefasst.

Es werden Leitlinien für TTP Manager, Entwickler und Bediener sowie zur Unterstützung von Einsatz und Verwaltung von TTPs aufgestellt. Des Weiteren werden die Funktionseinheiten von TTP Diensten sowie die jeweiligen Aufgaben und Verantwortlichkeiten von TTPs und Anwendern festgelegt.

Weitere Anmerkungen

ITU-T publiziert ISO/IEC 14516 textgleich als Recommendation X.842.

Bisherige Ausgaben

- ISO/IEC TR 14516: 2002

10.6 Schlüsselmanagement

Aufgabe des Schlüsselmanagements ist die Bereitstellung und Kontrolle von Schlüsselmaterial für kryptographische Mechanismen. Dies umfasst insbesondere die Schlüssel-erzeugung, -verteilung, -speicherung und -zerstörung. Eine Hauptaufgabe ergibt sich in den meisten Anwendungen daraus, dass sich die kommunizierenden Instanzen vor einer kryptographisch gesicherten Datenübertragung erst über die dabei zu verwendenden Schlüssel verständigen müssen. Schlüssel für symmetrische Kryptosysteme müssen auf sicherem Wege zwischen den Teilnehmern ausgetauscht und generell geheim gehalten werden. Bei asymmetrischen Systemen dagegen kann (oder muss sogar) je nach Anwendungsfall der öffentliche Schlüssel offen übertragen oder in einem öffentlich zugänglichen Verzeichnis gespeichert werden.

ISO/IEC 11770

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Key management Schlüsselmanagement

Inhalt und Anwendungsbereich

Der Zweck des Schlüsselmanagements ist die Bereitstellung von Verfahren zum Umgang mit kryptographischem Verschlüsselungsmaterial, das nach den gültigen Sicherheitsbestimmungen in symmetrischen oder asymmetrischen kryptographischen Algorithmen eingesetzt wird.

Dieser Standard besteht aus den Teilen:

- Teil 1: Rahmenrichtlinien (Framework)
- Teil 2: Mechanismen unter Benutzung von symmetrischen Techniken (Mechanisms using symmetric techniques)
- Teil 3: Mechanismen auf Basis von asymmetrischen Techniken (Mechanisms using asymmetric techniques)

Teil 4: Mechanismen auf Basis von schwachen Geheimnissen (Mechanisms using weak secrets)

Teil 1 legt die Ziele des Schlüsselmanagements fest, beschreibt die allgemeinen Modelle auf denen die Mechanismen des Schlüsselmanagements aufbauen, definiert die für alle Teile dieser Reihe gültigen Grundkonzepte der Schlüsselmanagement, bestimmt die Schlüsselmanagementdienste, stellt die Eigenschaften der Schlüsselmanagementmechanismen auf, legt die Anforderungen zur Verwaltung des Verschlüsselungsmaterials über den gesamten Lebenszyklus fest und beschreibt die Rahmenbedingungen für die Verwaltung des Verschlüsselungsmaterials über den gesamten Lebenszyklus.

Teil 2 definiert Mechanismen zur Schlüsselfestlegung unter Verwendung symmetrischer krypto-graphischer Techniken, genauer: entweder symmetrische Verschlüsselungsalgorithmen oder kryptographische Prüffunktionen. Diese Mechanismen können beispielsweise von den Mechanismen zur Authentisierung von Instanzen nach ISO/IEC 9798-2 abgeleitet werden, indem die Verwendung der Textfelder innerhalb dieser Mechanismen festgelegt wird. Das Dokument beschreibt den geforderten Inhalt von Nachrichten, die kryptographische Schlüssel nutzen oder notwendig sind, um die Bedingungen festzusetzen, bei denen ein geheimer Schlüssel erstellt werden kann.

Teil 3 definiert Mechanismen des Schlüsselmanagements für symmetrische Verfahren, die auf asymmetrischen kryptographischen Techniken basieren. Das Dokument befasst sich dabei vor allem mit der Bereitstellung eines gemeinsamen Geheimnisses für die Schlüsselauswahl und den Schlüsselaustausch zwischen zwei Partnern eines symmetrischen Verfahrens sowie die authentische Verteilung von dazu nötigen öffentlichen Schlüsseln der asymmetrischen Technik. Nicht betrachtet werden die weiteren Aspekte des Schlüsselmanagements wie Lebenszyklusverwaltung und Mechanismen zum Lagern, Archivieren, Löschen, Zerstören usw. von Schlüsseln.

Teil 4 definiert Mechanismen des Schlüsselmanagements, die auf schwachen Geheimnissen basieren. Er legt kryptographische Techniken fest, die für die Erstellung von einem oder mehreren geheimen Schlüsseln entwickelt wurden und auf einem von einem gespeicherten Passwort abgeleiteten schwachen Geheimnis beruhen. Das Dokument befasst sich jedoch nicht mit Aspekten wie Lebenszyklusverwaltung oder Mechanismen zum Lagern, Archivieren, Löschen, Zerstören usw. von schwachen Geheimnissen, starken Geheimnissen und erstellten geheimen Schlüsseln.

Weitere Anmerkungen

Teil 1 behandelt sowohl die automatisierten als auch die manuellen Aspekte des Schlüsselmanagements. Teil 2 beschäftigt sich nicht explizit mit dem Gebiet des Interdomain-Schlüsselmanagements. Teil 3 deckt außerdem nicht die Anwendungen der Veränderungen ab, die von den Mechanismen des Schlüsselmanagements genutzt werden. Teil 4 beschreibt Mechanismen die entwickelt wurden, um ausgeglichene Vereinbarungen über passwortauthentisierte Schlüssel, erweiterte Vereinbarungen über passwortauthentisierte Schlüssel und das Abrufen passwort-authentisierter Schlüssel zu erreichen.

Bisherige Ausgaben

- ISO/IEC 11770-1:1996
- ISO/IEC 11770-2:1996
- ISO/IEC 11770-3:1999
- ISO/IEC 11770-4:2006

■ 10.7 Kommunikationsnachweise

Kommunikationsnachweise dienen dazu, das nachträgliche Ableugnen einer tatsächlich stattgefundenen Kommunikation technisch zu verhindern. Sicherheitsmechanismen für diesen Bereich werden häufig als eine Domäne asymmetrischer Kryptographie betrachtet, können jedoch auch mit symmetrischen Verfahren realisiert werden.

ISO/IEC 13888

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Non-repudiation Nicht-Abstreitbarkeit

Inhalt und Zweck

Der Zweck von Nicht-Abstreitbarkeitsdiensten ist das Erstellen, Sammeln, Erhalten, Verfügbar-machen und Prüfen von technischen Beweisen zu geforderten Ereignissen oder Aktionen um Streitfälle über das Auftreten oder Wegbleiben dieser Ereignisse oder Aktionen lösen zu können.

Dieser Standard besteht aus den Teilen:

- Teil 1: Allgemeines Modell (General model)
- Teil 2: Mechanismen auf Basis von symmetrischen Techniken (Mechanisms using symmetric techniques)
- Teil 3: Mechanismen auf Basis von asymmetrischen Techniken (Mechanisms using asymmetric techniques)

Teil 1 beschreibt ein Modell für Nicht-Abstreitbarkeitsmechanismen, bei dem die Beweiserbringung auf kryptographischen Prüfwerten beruht, die mit symmetrischen oder asymmetrischen kryptographischen Techniken erzeugt werden. Darunter fallen generische Beweiserzeugungs- und Prüfmechanismen, die sichere Hüllen und Digitale Signaturen umfassen und auf symmetrischen beziehungsweise asymmetrischen kryptographischen Techniken beruhen.

Teil 2 legt symmetrische Techniken nutzende Mechanismen für die Erzeugung, den Austausch und die Bestätigung von Nicht-Abstreitbarkeitsmerkmalen fest. Er beschreibt fünf Grundmechanismen zur Erstellung der Nicht-Abstreitbarkeit von Ursprung, Versendung, Empfang und Transport sowie für Zeitstempel. Für jeden

davon müssen die beteiligten Instanzen in der Lage sein, einzeln mit dem vertrauenswürdigen Dritten (TTP) zu kommunizieren. Die Mechanismen erfordern den Einsatz bestimmter Nicht-Abstreitbarkeitsmerkmale.

Teil 3 legt zwei Mechanismen für die Bereitstellung von Nicht-Abstreitbarkeitsdiensten fest, die asymmetrische kryptographische Techniken nutzen und die Erzeugung von Beweisen für die Nicht-Abstreitbarkeit des Ursprungs (non-repudiation of origin, NRO) und die Nicht-Abstreitbarkeit der Zustellung (non-repudiation of delivery, NRD) ohne die direkte Beteiligung einem vertrauenswürdigen Dritten (TTP) ermöglichen. Darüber hinaus definiert dieser Teil Mechanismen für NRO und NRD unter Beteiligung einer TTP sowie für die Nicht-Abstreitbarkeit der Vorlage und die Nicht-Abstreitbarkeit des Transports.

Weitere Anmerkungen

Diese Normenreihe bietet Nicht-Abstreitbarkeitsmechanismen für die folgenden Phasen der Nicht-Abstreitbarkeit: Beweiserzeugung, Beweistransfer, -lagerung und -abfrage sowie Beweisbestätigung. Die Streitschlichtung liegt außerhalb des Anwendungsbereiches dieses Dokuments.

Bisherige Ausgaben

- ISO/IEC 13888-1:1997; 2004
- ISO/IEC 13888-2:1998
- ISO/IEC 13888-3:1997

10.7 Zeitstempeldienste

Die Beweiskraft elektronischer Dokumente hängt entscheidend davon ab, ob Urheber und Inhalt, aber auch der Erstellungszeitpunkt zweifelsfrei und fälschungssicher feststellbar sind. Aus diesem Grund spielen neben digitalen Signaturen auch Zeitstempeldienste eine wichtige Rolle für die vertrauenswürdige Kommunikation.

ISO/IEC 18014

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Time-stamping services Zeitstempeldienste

Inhalt und Anwendungsbereich

In der Normenreihe werden Mechanismen und Protokolle für vertrauenswürdige Zeitstempel spezifiziert.

Der Standard besteht aus den Teilen:

- Teil 1: Rahmenangaben (Framework)
- Teil 2: Zeitstempelmechanismen mit dedizierten Zeitstempeln (Mechanisms producing independent tokens)
- Teil 3: Zeitstempelmechanismen mit verknüpften Zeitstempeln (Mechanisms producing linked tokens)

In Teil 1 wird das Ziel einer Zeitstempelstelle bestimmt, ein allgemeines Modell, auf dem Zeitstempeldienste aufbauen, beschrieben, Zeitstempeldienste und die Grundprotokolle von Zeitstempeln definiert, das allgemeine Protokoll zwischen den beteiligten Instanzen festgelegt und die Vernetzungsprotokolle für eine Zeitstempelstelle bestimmt.

Teil 2 definiert Zeitstempelmechanismen, die unabhängige Merkmale erstellen, damit ein Existenzbeweis nach dem anderen geprüft werden kann. Es werden drei voneinander unabhängige Mechanismen betrachtet:

Zeitstempel, die Digitale Signaturen nutzen, Zeitstempel, die Codes zur Authentisierung von Nachrichten (MCA) nutzen und Zeitstempel, die Archivierung nutzen.

Teil 3 beschreibt Zeitstempeldienste, die verknüpfte Merkmale erzeugen. Ein allgemeines Modell solcher Zeitstempeldienste wird ebenso vorgestellt wie die Hauptkomponenten zu deren Erstellung. Datenstrukturen und -protokolle für den Austausch mit solchen Zeitstempeldiensten werden definiert und typische Beispiele beschrieben. Dieser Teil definiert die zusätzlichen Datenarten, die die Anwendung von Zeitstempelmechanismen unterstützen, um verknüpfte Merkmale zu erzeugen. Außerdem werden die Verknüpfungs-, Gruppierungs- und Veröffentlichungsabläufe sowie die dazugehörigen Protokolle festgelegt.

Weitere Anmerkungen

Der Einsatz von unabhängigen Merkmalen (Teil 2) setzt Vertrauen in die Zeitstempelstelle (Time stamping authority, TSA) voraus.

Bisherige Ausgaben

- ISO/IEC 18014-1:2002
- ISO/IEC 18014-2:2002
- ISO/IEC 18014-3:2004

11 Spezielle Sicherheitsfunktionen 2: Physische Sicherheit

Im Wesentlichen wird in den Standards der physischen Sicherheit die Widerstandsfähigkeit oder die Einhaltung zugesicherter Eigenschaften für einzelne Module oder Produkte wie Wände, Türen oder Baustoffe beschrieben. Die Evaluierung kompletter Systeme wie IT-Sicherheitsräume, Brandschutzracks oder Datensafes ist in der Regel schwieriger und daher umfangreicher und teurer. Europäische Normen wie beispielsweise die EN 1047 sind daher in mehrere Teile gefasst. Je nach IT-System oder Einzelmodul kann solch ein Standard dann für die Prüfung herangezogen werden.

Zertifizierungen sind nur als Herstellererklärungen üblich. Die Bauteile und Baustoffe werden auf Grundlage von Prüfergebnisse unabhängiger Prüfer in beispielsweise Brandschutzklassen eingeteilt. Diese Prüfberichte erlauben es dem Hersteller auf dem Produkt eine Angabe zur Brandschutzklasse mit Verweis auf das Prüfergebnis anzubringen.

■ 11.1 BSI Technische Leitlinie (TL) 03400 (vormalig BSI 7500)

Inhalt und Anwendungsbereich

Die Leitlinie 03400 (Produkte für materielle Sicherheit) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) legt Sicherheitsanforderungen für mechanische Sicherungseinrichtungen, Komponenten von Alarmanlagen, Zutrittskontrollen sowie Geräte der Bürotechnik fest. Hintergrund für diese Festlegung ist die Aufgabe des BSI, Vorgaben für die sichere Verwahrung von (behördlichen) Verschlusssachen zu erstellen. Die entsprechenden physischen Komponenten werden gemäß den Sicherheitsanforderungen der Leitlinie geprüft und zertifiziert. Die Leitlinie umfasst alle vom BSI empfohlenen sicherheitsrelevanten Produkte und die dazugehörigen Hersteller

Methodik

Die Komponenten werden entsprechend der Standards geprüft.

Zertifizierung

- Die Zertifizierung erfolgt über die verschiedenen Verfahren der Zertifizierungsanbieter (abhängig von der Komponente:
- Komponenten von Alarmanlagen, Brandmeldeanlagen, Einbruchmeldeanlagen und mechanische Sicherungseinrichtungen: VdS Schadenverhütung GmbH
- Mechanische Sicherungseinrichtungen (einbruchshemmende Türen und Fenster, Schlösser, Profilylinder, Beschläge): DIN CERTCO Gesellschaft für Konformitätsbewertung
- Einbruchshemmenden Türen und Fenstern: Instituts für Fenstertechnik (IFT)
- Sicherheitsschränke, Wertschutzschränke, Wertschutzräume und Datensicherungsschränke, -räume und -container.: Das European Certification Board • Security Systems (ECB • S)

Bisherige Ausgaben

- Februar 2009
- März 2006

■ 11.2 Brandschutz

DIN 4102

Titel:	Bauwesen
Arbeitsgebiet:	Brandschutz
Name des Standards:	Brandverhalten von Baustoffen und Bauteilen

Inhalt und Anwendungsbereich

Zweck von DIN 4102 ist es, das Brandverhalten von Baustoffen und Bauteilen mittels Brandprüfungen zu beurteilen sowie die Baustoffe und Bauteile anhand der gewonnenen Ergebnisse in Brandschutzklassen wie etwa nicht brennbare Stoffe oder brennbare Stoffe einzuordnen.

Der Standard besteht aus folgenden Teilen:

- Teil 1: Baustoffe, Begriffe, Anforderungen und Prüfungen
- Teil 2: Bauteile, Begriffe, Anforderungen und Prüfungen
- Teil 3: Brandwände und nichttragende Außenwände, Begriffe, Anforderungen und Prüfungen
- Teil 4: Zusammenstellung und Anwendung klassifizierter Baustoffe, Bauteile und Sonderbauteile
- Teil 5: Feuerschutzabschlüsse, Abschlüsse in Fahr-schachtwänden und gegen feuerwiderstandsfähige Verglasungen, Begriffe, Anforderungen und Prüfungen
- Teil 6: Lüftungsleitungen, Begriffe, Anforderungen und Prüfungen
- Teil 7: Bedachungen, Begriffe, Anforderungen und Prüfungen
- Teil 8: Kleinprüfstand
- Teil 9: Kabelabschottungen, Begriffe, Anforderungen und Prüfungen
- Teil 11: Rohrummantelungen, Rohrabschottungen, Installationsschächte und -kanäle sowie Abschlüsse ihrer Revisionsöffnungen, Begriffe, Anforderungen und Prüfungen
- Teil 12: Funktionserhalt von elektrischen Kabelanlagen, Anforderungen und Prüfungen
- Teil 13: Brandschutzverglasungen, Begriffe, Anforderungen und Prüfungen
- Teil 14: Bodenbeläge und Bodenbeschichtungen, Bestimmung der Flammenausbreitung bei Beanspruchung mit einem Wärmestrahler
- Teil 15: Brandschacht
- Teil 16: Durchführung von Brandschachtprüfungen

- Teil 17: Schmelzpunkt von Mineralfaser-Dämmstoffen, Begriffe, Anforderungen, Prüfung
- Teil 18: Feuerschutzabschlüsse, Nachweis der Eigenschaft „selbstschließend“ (Dauerfunktionsprüfung)
- Teil 22: Anwendungsnorm zu DIN 4102-4

Anmerkung: Teil 10, Teil 20 und Teil 21 wurden nicht erstellt. Teil 19 wurde 2006 zurückgezogen.

Weitere Anmerkungen

Im DIN ist der Normenausschuss Bauwesen (NABau) für diese Norm zuständig.

Bisherige Ausgaben

Die heute gültigen Teile von DIN 4102 wurden zwischen den Jahren 1977 und 2004 veröffentlicht. Auf eine vollständige Auflistung aller bisherigen Ausgaben wird hier verzichtet, da die Historie von DIN 4102 bis in das Jahr 1934 zurückreicht und den hier verfügbaren Rahmen sprengen würde. Auskünfte zur fachlichen Entwicklung der Norm über die Jahrzehnte hinweg sind beim DIN-Normenausschuss Bauwesen erfragbar.

DIN 18095

Titel:	Bauwesen
Arbeitsgebiet:	Brandschutz
Name des Standards:	Rauchschutzabschlüsse

Inhalt und Anwendungsbereich

Zweck von DIN 18095 ist es, die notwendigen Anforderungen an Rauchschutztüren und -abschlüsse zu definieren und Prüfverfahren zur Bestimmung unter anderem der Dichtheit festzulegen.

Der Standard besteht aus folgenden Teilen:

- Teil 1: Begriffe und Anforderungen
- Teil 2: Bauartprüfung der Dauerfunktionstüchtigkeit und Dichtheit
- Teil 3: Anwendung von Prüfergebnissen

Der Teil 1 enthält Begriffe und Anforderungen für Rauchschutztüren. Rauchschutztüren werden in den Bauordnungen der Länder gefordert. Die Norm ist daher Konkretisierung der unbestimmten Rechtsbegriffe der Landesbauordnungen.

Der Teil 2 enthält das Prüfverfahren zur Beurteilung von Rauchschutztüren.

Der Teil 3 gilt für Rauchschutzabschlüsse zum Einbau in lichte Wandöffnungen mit einer Breite von 3,0 m bis 7,0 m und mit einer Höhe von 3,0 m bis 4,5 m. Die Norm legt das beim Eignungsnachweis für Rauchschutzabschlüsse anzuwendende Verfahren für die Beurteilung ihrer Dichtheit bei Umgebungstemperatur und bei erhöhter Temperatur sowie ihrer Dauerfunktionstüchtigkeit fest, wenn ihre lichte Öffnung die größte prüfbare Größe überschreitet. Bei Rauchschutzabschlüssen für Wandöffnungen mit einer Breite und Höhe von höchstens 3,0 m gilt DIN 18095-2. Voraussetzung für die Extrapolation nach dieser Norm ist das Vorliegen von Prüfergebnissen nach DIN 18095-2.

Weitere Anmerkungen

Im DIN ist der Normenausschuss Bauwesen (NABau) für diese Norm zuständig.

Bisherige Ausgaben

- DIN 18095-1:1988
- DIN 18095-2:1991
- DIN 18095-2:1988
- DIN 18095-3:1999

DIN EN 1047

Titel:	Maschinenbau
Arbeitsgebiet:	Wertbehältnisse
Name des Standards:	Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand

Inhalt und Anwendungsbereich

Der Standard besteht aus folgenden Teilen:

- Teil 1 Datensicherungsschränke und Disketteneinsätze
- Teil 2 Datensicherungsräume und Datensicherungscontainer

Aufgrund der Prüfbedingungen nach dieser Norm werden Brände zur reproduzierbaren Ermittlung des Feuerwiderstandes von Wertbehältnissen verschiedener Güteklassen simuliert. Die Güteklassen ermöglichen einen Vergleich der Widerstandsfähigkeit verschiedener Konstruktionen gegen Brände.

DIN EN 1047-1 legt Anforderungen an Datensicherungsschränke und Disketteneinsätze zum Schutz gegen Brände fest. Zwei Prüfverfahren dienen der Ermittlung der Widerstandsfähigkeit von Datensicherungsschränken, temperatur- und feuchtigkeitsempfindliches Füllgut vor Brandeinwirkung zu schützen: eine Feuerwiderstandsprüfung und eine Feuerstoß- und Sturzprüfung.

Ferner wird ein Schema zur Klassifizierung von vor Brandeinwirkung schützenden Datensicherungsschränken und Disketteneinsätzen nach ihrem Prüfergebnis gegeben.

Die aktuelle (2.) Ausgabe von DIN EN 1047-1:2006 enthält gegenüber ihrer Vorgängerin zusätzlich prüftechnische Kriterien für Disketteneinsatz, die auf Grundlage der Anforderungen nach dem Einheitsblatt VDMA 24991-1 aufgenommen worden.

Die in DIN EN 1047-2 angegebenen Prüfbedingungen beschreiben die Simulation von Bränden zur reproduzierbaren Ermittlung des Feuerwiderstandes von

Datensicherungsräumen und -containern. Der Standard legt Anforderungen an Datensicherungsräume und -container fest. Die Norm umfasst eine Prüfmethode zur Ermittlung der Widerstandsfähigkeit von Datensicherungsräumen und -containern zum Schutz von temperatur- und feuchtigkeitsempfindlichem Füllgut und verbundenen Hardwaresystemen vor Brandeinwirkung von außerhalb des Datensicherungsraumes und -containers.

Ferner wird eine Prüfmethode zur Messung des Widerstandes gegen mechanische Beanspruchung (Stöße) auf Datensicherungscontainer und bestimmte Datensicherungsräume festgelegt.

Die Ergebnisse der Prüfungen werden zur Klassifizierung der Datensicherungsräume und Datensicherungscontainer herangezogen.

Weitere Anmerkungen

Im DIN ist der Normenausschuss Maschinenbau (NAM) für diese Norm zuständig.

Bisherige Ausgaben

DIN EN 1047-1:1997
DIN EN 1047-1:2006

DIN EN 1047-2:1996
DIN EN 1047-2:2000

■ 11.3 Einbruchshemmung

DIN EN 1143-1

Titel:	Maschinenbau
Arbeitsgebiet:	Wertbehältnisse

Name des Standards:	Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl – Teil: Wertschutzschränke, Wertschutzschränke für Geldautomaten, Wertschutzraumtüren und Wertschutzräume
---------------------	--

Inhalt und Anwendungsbereich

Auf Grundlage dieser Europäischen Norm werden freistehende Wertschutzschränke, Einbauschränke (Boden und Wand), Wertschutzschränke für Geldautomaten (ATM-Safes) und ATM-Sockel, Wertschutzraumtüren sowie Wertschutzräume (mit oder ohne Tür) gemäß ihrem Widerstandswert gegen Einbruchdiebstahl geprüft und klassifiziert. Diese Norm gilt nicht für die Prüfung und Klassifizierung von Deposit-Systemen und Geldautomaten (ATM-Systemen).

DIN EN 1143-1 enthält neben den Prüfverfahren auch die Definitionen der Begriffe des behandelten Fachgebiets, die für das korrekte Verständnis der Norm unentbehrlich sind.

Weitere Anmerkungen

Die Norm enthält Prüfungen, deren Ergebnisse zur Klassifizierung des Widerstandswertes gegen Einbruchdiebstahl herangezogen werden. Die Klassifizierung des Widerstandes kann auch für den Aufbau von Sicherheitssystemen berücksichtigt werden. Bei tatsächlichen Einbruchversuchen ist in Abhängigkeit vom Täter, von den Bedingungen am Tatort und der Verfügbarkeit von Werkzeugen mit erheblich längeren Zeiten zu rechnen als bei der Prüfung.

Bei manuell durchzuführenden Prüfungen hängen die Ergebnisse und die Reproduzierbarkeit von der Befähigung des Prüfungsteams ab. Automatisierte Prüfungen befinden sich noch im Entwicklungsstadium. Mit ihrer Einbeziehung in DIN EN 1143-1 ist eventuell bei einer Überarbeitung der Norm zu rechnen.

Im DIN ist der Normenausschuss Maschinenbau (NAM) für diese Norm zuständig.

Bisherige Ausgaben

- DIN EN 1143-1:2006
- DIN EN 1143-1:2002
- DIN EN 1143-1:1997

DIN V ENV 1627

Titel:	Bauwesen
Arbeitsgebiet:	Einbruchhemmung
Name des Standards:	Fenster, Türen, Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung

Inhalt und Anwendungsbereich

Diese Europäische Vornorm (daher die „Vs“ in der Normnummer), beschreibt die Anforderungen und Klassifizierung der einbruchhemmenden Eigenschaften von Fenstern, Türen, Abschlüssen. Sie ist anwendbar auf die folgenden Öffnungsarten: drehen, kippen, falten, drehkippen, schwingen, schieben (horizontal und vertikal) und rollen, sowie auf fest montierte Konstruktionen. Die Norm ist nicht anwendbar für die Manipulation und Einbruchversuche bezüglich elektronischer oder elektromagnetischer Einrichtungen.

Weitere Anmerkungen

Die Prüfverfahren, um die einbruchhemmenden Eigenschaften von Fenstern, Türen und Abschlüssen zu beurteilen, werden in folgenden Standards festgelegt:

DIN V ENV 1628 „Fenster, Türen, Abschlüsse - Einbruchhemmung - Prüfverfahren für die Ermittlung der Widerstandsfähigkeit unter statischer Belastung“

DIN V ENV 1629 „Fenster, Türen, Abschlüsse - Einbruchhemmung - Prüfverfahren für die Ermittlung der Widerstandsfähigkeit unter dynamischer Belastung“

Die DIN V ENV 1627:1999 wird durch die sich derzeit in Entwicklung befindende DIN EN 1627 ersetzt werden. Im DIN ist der Normenausschuss Bauwesen (NABau) für diese Norm zuständig.

Bisherige Ausgaben

- DIN V ENV 1627:1999

11.4 Gehäuse

DIN EN 60529 (VDE 0470-1)

Titel:	Elektrotechnik
Arbeitsgebiet:	Schutzarten
Name des Standards:	Schutzarten durch Gehäuse (IP-Code)

Inhalt und Anwendungsbereich

Der Zweck dieser Norm ist es, folgendes festzulegen:

- Begriffe für Schutzarten durch Gehäuse von elektrischen Betriebsmitteln, betreffend:
 - Schutz von Personen gegen den Zugang zu gefährlichen Teilen innerhalb des Gehäuses;
 - Schutz des Betriebsmittels innerhalb des Gehäuses gegen Eindringen von festen Fremdkörpern;
 - Schutz des Betriebsmittels innerhalb des Gehäuses gegen schädliche Einwirkungen durch das Eindringen von Wasser.
- Bezeichnungen für diese Schutzarten.
- Anforderungen für jede Bezeichnung.
- Prüfungen, die durchzuführen sind, um zu bestätigen, dass das Gehäuse die Anforderungen dieser Norm erfüllt.

DIN EN 60529 findet auf die Einteilung von Schutzarten durch Gehäuse für elektrische Betriebsmittel mit Bemessungsspannungen nicht über 72,5 kV Anwendung.

Weitere Anmerkungen

Maßnahmen zum Schutz sowohl des Gehäuses als auch des Betriebsmittels innerhalb des Gehäuses gegen äußere Einflüsse oder Bedingungen wie beispielsweise mechanische Stöße, Korrosion, ätzende Lösungen (Beispiel: Schneid- und Kühlflüssigkeiten), Schimmel, schädliche Insekten, Sonnenstrahlung, Vereisung, Feuchtigkeit (durch Kondensation gebildet), explosionsfähige Atmosphäre und der Schutz gegen das Berühren von gefährlichen sich bewegenden Teilen außerhalb des Gehäuses (wie zum

Beispiel Lüfter) sind Angelegenheiten einer jeweils zu erstellenden Produktnorm.

Hierfür ist die Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (DKE) zuständig.

Bisherige Ausgaben

DIN EN 60529:2000

12 Anhang

■ Bezug zu anderen Standards

Standards beziehen sich auch auf andere Standards. In der folgenden Liste sind diese Abhängigkeiten aufgeführt. Die Liste besitzt nicht den Anspruch auf Vollständigkeit.

Informationssicherheits-Managementsysteme (ISms)

ISO/IEC 27001	ISO/IEC 27001 bezieht sich besonders eng auf ISO/IEC 27002 und hat eine inhaltliche Verbindung zu allen anderen Normen der 2700x-Familie. Im Kontext integrierter Managementsysteme ist auch ISO 9000 als Normenreihe zu nennen.
ISO/IEC 27002	Da hier Sicherheitsmanagement behandelt wird, besteht ein enger Bezug zu ISO/IEC 27001.
ISO/IEC 27006	Hier besteht ein enger Bezug zur ISO/IEC 27001. Weiterhin ist als Auditierungs- und Zertifizierungsstandard die ISO/IEC 17021 von Bedeutung.
IT-Grundschutz	Die Umstellung der IT-Grundschutz-Vorgehensweise erfolgte konform zur Verabschiedung des internationalen Standard ISO/IEC 27001, welcher aus der BS 7799-2 hervorgegangen ist. Ebenso werden die Empfehlungen der Norm ISO/IEC 27002 berücksichtigt, deren Umsetzung die Anforderungen des Standards ISO/IEC 27001 erfüllen. Methoden zur Risikoanalyse werden in der Norm ISO/IEC 27005 beschrieben.

Sektor-spezifische ISMS

ISO/IEC 27011	Dieser Standard kann als eine sektorspezifische Erweiterung von ISO/IEC 27002 gesehen werden.
Richtlinie VDI/VDE2182	Dieser Standard kann als eine sektorspezifische Erweiterung von ISO/IEC 27002 gesehen werden.

Sicherheitsmaßnahmen und Monitoring

ISO/IEC 18028	ISO/IEC 27005, ISO/IEC 27002:2005, ISO/IEC 27001:2005, ISO/IEC 18044:2004, ISO/IEC 18043
---------------	--

ISO/IEC TR 18044	Der Technische Bericht kann als Detaillierung des Kapitels “Behandlung von Sicherheitsvorfällen” von ISO/IEC 27002 gesehen werden. ISO/IEC 18043 liefert Hinweise zur Auswahl, Einsatz und Betrieb entsprechender technischer Eingriffserkennungssysteme. Die Methodik der Risikoanalyse wird in diesem Standard referenziert. Hierzu liefert wiederum ISO/IEC 27005 weitere Inhalte.
ISO/IEC 18043	Der Standard hilft bei der Implementierung einiger Anforderungen aus dem ISO/IEC 27002, nämlich der Erkennung nicht berechtigter Zugriffe auf IT-Systeme und deren sicherheitstechnischen Überwachung. ISO 18043 liefert Hinweise zur Auswahl, Einsatz und Betrieb entsprechender technischer Eingriffserkennungssysteme. Die Methodik der Risikoanalyse wird in diesem Standard referenziert. Hierzu liefert wiederum ISO/IEC 27005 weitere Inhalte.
ISO/IEC 15816	Es ist beabsichtigt, andere Normen auf die Definitionen aus diesem Dokument zu verweisen.
ISO/IEC 24762	Die Themenblöcke Disaster Recovery Management (ISO/IEC 24762) und Business Continuity Management (BS 25777) sind inhaltlich eng verwoben. Daher werden beide Normen häufig parallel betrachtet.
BS 25777	

Risikomanagement

MaRisk	MaRisk kann als Sektorspezifische Ausprägung der ISO/IEC 27005 gesehen werden. Weiterhin sind Bezüge zum IT-Grundschutz gegeben.
ISO/IEC 27005	Das Risikomanagement hat wesentliche inhaltliche Bezüge zur ISO/IEC 27001 und zur ISO 9000.

Standards mit IT-Sicherheitsaspekten

Cobit	Einen konkreten Bezug zu anderen Standards gibt es nicht. Cobit leitet sich mit Fokus auf Informationstechnologie aus dem COSO Framework ab. In Cobit sind Bestandteile aus insgesamt 41 nationalen und internationalen Standards eingearbeitet und gemeinsam ausgerichtet worden.
ITIL	Die IT-Sicherheitsmaßnahmen werden aus BS 7799 genommen, Zertifizierung erfolgt über BS 15000 beziehungsweise ISO/IEC 20000.

IDW PS 330

Der Standard für IT-Systemprüfungen baut auf dem „International Standard on Auditing (ISA 401)“ auf. Der zeitliche Aufwand ist wesentlich geringer als bei einer Prüfung nach IT-Grundschutz oder ISO/IEC 27001. In Erfahrungsberichten ist von wenigen Tagen für Prüfungen im Mittelstand die Rede.

Die Aufteilung der zu prüfenden Bereiche

- IT-Umfeld (Richtlinien, IT-Strategie)
- IT-Organisation
- IT-Infrastruktur
- IT-Anwendungen
- IT-Geschäftsprozesse

erinnert an Aufteilung im BSI-Grundschutz. Der Detaillierungsgrad der abzufragenden Maßnahmen bewegt sich jedoch eher auf der Ebene von der des ISO/IEC 27002.

Evaluierung von IT-Sicherheit

Common Criteria

ISO/IEC 15408 (CC)

Mehrere andere Dokumente stehen in Bezug zu diesem Standard:

ISO/IEC 18045 definiert die Methodologie, mit der Evaluierungen gemäß 15408 durchgeführt werden. Insofern ist hier eine unmittelbare Abhängigkeit vorhanden.

ISO/IEC 15446 gibt Hinweise, wie Schutzprofile (Protection Profiles) und Sicherheitsvorgaben (Security Targets) verfasst werden, die im Kontext der Evaluierung nach 15408 relevant sind.

ISO/IEC 15292 stellt die Arbeitsweise von Registrierungsstellen für Protection Profiles dar.

Der technische Bericht ISO/IEC 19791 stellt eine Möglichkeit dar, die Evaluierung auf IT-Systeme inklusive ihres Betriebs anzuwenden.

ISO/IEC TR 15443

Da es das Ziel dieses Standards ist, einen Weg zur Auswahl von Vertrauenswürdigkeitsmethoden aufzuzeigen, besteht naturgemäß ein Zusammenhang zu allen anderen Standards, die in diesem Abschnitt genannt sind. Fast alle von ihnen gehören zu einer der Vertrauenswürdigkeitsmethoden, die im Standard behandelt werden.

Darüber hinaus werden aber auch viele ISO- und Nicht-ISO-Standards in ISO/IEC TR 15443 behandelt, die im vorliegenden Dokument nicht behandelt wurden.

ISO/IEC 18045

Ein Bezug besteht unmittelbar zur ISO/IEC 15408 (Common Criteria), und dadurch indirekt zu weiteren damit zusammenhängenden Standards.

ISO/IEC TR 19791

Ein Bezug besteht einerseits zu ISO/IEC 15408 (Common Criteria), da deren Methoden für in Betrieb befindliche IT-Systeme nutzbar gemacht werden sollen.

Da hier Aspekte des IT-Sicherheitsmanagements eine große Rolle spielen, sind auch Standards zu diesem Thema relevant. Einige Beispiele sind: die ISO/IEC 2700x-Familie; ISO/IEC TR 15443-1/3; ISO/IEC 27002; ISO/IEC 18028-1/4; ISO/IEC 21827: 2002

ISO/IEC 19790 (FIPS 140-2)	Da viele kryptographische Verfahren, etwa zu Verschlüsselung, Signaturen, Hash-Funktionen, Zufallszahlen, in dem Standard erwähnt werden, sind alle Standards, die solche Algorithmen definieren, für ISO/IEC 19790 relevant. Sie werden hier nicht im Einzelnen aufgezählt, es sei auf die entsprechenden Abschnitte und kryptographischen Standards in dieser Liste verwiesen. Relevant ist zudem "Federal Information Processing Standard Publication (FIPS PUB) 140-2, Security requirements for cryptographic modules", wie im vorigen Abschnitt erwähnt. Relevant ist auch der Bezug zu 15408, also den allgemeinen Evaluations-kriterien. Diese erlauben auch die Evaluierung von Produkten, die als Kryptomodule dienen, und werden dafür (etwa im Fall von Chipkarten) auch genutzt. Die Tatsache, dass eine solche allgemeine Evaluationsnorm (15408) und eine spezielle Norm für Kryptomodule (19790) parallel existieren werden, ist wesentlich historisch bedingt, insbesondere auch durch die Nutzung von FIPS 140-2.
ISO/IEC 24759	27002
ISO/IEC 19792	Ein Bezug besteht natürlich einerseits zur ISO/IEC 15408 (auch Common Criteria), da auch diese ein allgemeines Kriterienwerk zur Evaluierung von Sicherheitsprodukten und -Systemen darstellen. Des Weiteren besteht ein enger Bezug zu Standards der WG5 aus der ISO/IEC JTC 1/SC 37, die sich mit den Testaspekten zu biometrischen Verfahren im Sinne ihrer Leistungs-fähigkeit beschäftigen.
ISO/IEC 21827 (SSE-CMM)	SSE-CMM wurde ebenfalls als Fast Track in der ISO/IEC – als International Standard (IS) 21827 – eingereicht. Zu folgenden Standards besteht ein Bezug: ISO/IEC 12207, , ISO/IEC 15288, ISO/IEC TR 1504-2, ISO/IEC TR 1504-4, ISO/IEC 27002.
Schutzprofile	
ISO/IEC TR 15446	Ein Bezug besteht unmittelbar zur ISO/IEC 15408 (Common Criteria), und dadurch indirekt zu weiteren damit zusammenhängenden Standards.

Spezielle Sicherheitsfunktionen 1: Normen zu kryptographischen und IT-Sicherheitsverfahren

Verschlüsselung

ISO/IEC 18033	ISO/IEC 10116
ISO/IEC 10116	ISO/IEC 8372, ANSI X3.106, FIPS Publication 81
ISO/IEC 19772	ISO/IEC 9796-2/6, ISO/IEC 9797-1/2, ISO/IEC 11770-1/4, ISO/IEC 14888-1/3, ISO/IEC 18033-1/4

Digitale Signaturen

ISO/IEC 9796	ISO/IEC 9797-2, ISO/IEC 10118-1/4, ISO/IEC 9798-1, ISO/IEC 14888-1/3
ISO/IEC 14888	ISO/IEC 8825-1, ISO/IEC 10118 (alle Teile), ISO/IEC 15946-1
ISO/IEC 15946	ISO/IEC 9796-3, ISO/IEC 11770-3

Hash-Funktionen und andere Hilfsfunktionen

ISO/IEC 10118	ISO/IEC 9797
ISO/IEC 18031	ISO/IEC 10116, ISO/IEC 10118-3, ISO/IEC 11770-1, ISO/IEC 18032, ISO/IEC 18033-3, ISO/IEC 19790
ISO/IEC 18032	ISO/IEC 18031

Authentifizierung

ISO/IEC 9798	ISO 7498-2, ISO/IEC 10181-2
ISO/IEC 9797	ISO 7498-2, ISO/IEC 10116, ISO/IEC 10118-1, ISO/IEC 10118-3

PKI-Dienste

ISO/IEC 15945	ISO/IEC 9594-8, ISO/IEC 9798-1, ISO/IEC 10118-1, ISO/IEC 10118-2, ISO/IEC 10118-3, ISO/IEC 10118-4, ISO/IEC 11770-1, ISO/IEC 11770-3, ISO/IEC 14888-2, ISO/IEC 14888-3 ISO/IEC 27002, ISO/IEC 13888-1, ISO/IEC 13888-2, ISO/IEC 13888-3 ISO/IEC TR 14516 ergänzt diesen Standard durch Richtlinien zur Nutzung und Management eines vertrauenswürdigen Dritten (in der Regel Trust Center).
ISO/IEC TR 14516	ISO/IEC 9594-8, ISO/IEC 10181-1, ISO/IEC 10181-4, ISO 7498-2, ISO/IEC IS 15945 ergänzt diesen TR durch die technische Spezifikation von Protokollen für solche Services.

Schlüsselmanagement

ISO/IEC 11770	ISO/IEC 9796-3, ISO/IEC 9798-2, ISO/IEC 9798-3, ISO/IEC 10118-1, ISO/IEC 10118-3, ISO/IEC 15946-1, ISO/IEC 18031, ISO/IEC 18032, ISO/IEC 18033-1
---------------	--

Kommunikationsnachweise

ISO/IEC 13888 ISO/IEC 9796, ISO/IEC 9797, ISO/IEC 10118 (alle Teile), ISO/IEC 14888 (alle Teile)

Zeitstempeldienste

ISO/IEC 18014 ISO/IEC 9798-1, ISO/IEC 10118-1, ISO/IEC 10118-2, ISO/IEC 10118-3, ISO/IEC 10118-4, ISO/IEC 11770-1, ISO/IEC 11770-3, ISO/IEC 14888-2, ISO/IEC 14888-3, ISO/IEC 15946-2

Spezielle Sicherheitsfunktionen 2: Physische Sicherheit

Technische Leitlinie 03400 Die Leitlinie prüft die Komponenten anhand von verschiedensten physischen Standards, die in der Leitlinie aufgeführt sind.

Brandschutz

DIN 4102 Es besteht Bezug zu vielen Normen, als dass sie einzeln hier aufgeführt werden könnten.

DIN 18095 DIN 4102-18:1991

DIN EN 1047 DIN EN 206-1, DIN EN 1363-1, DIN EN 1363-2, DIN EN 1364-1, DIN EN 1365-1, DIN EN 1365-2

Einbruchshemmung

DIN EN 1143-1 DIN EN 1300:2004

DIN V ENV 1627 DIN V ENV 1628, DIN V ENV 1629

Gehäuse

DIN EN 60529 IEC 60050-195:1998, IEC 60050-826:1982, IEC 60068-1:1988, IEC 60068-2-68:1994, IEC 60071-2:1996.

Links

BSI / IT-Grundschutz	Alle Unterlagen zum IT-GSHB findet man auf der Webseite des Bundesamt für Sicherheit in der Informationstechnik (www.bsi.bund.de). Alle Unterlagen zum IT-Grundschutzhandbuch sind beim BSI unter www.bsi.bund.de/gshb/index.htm zu finden, sowohl der Leitfaden (www.bsi.bund.de/gshb/Leitfaden/index.htm) als auch das Grundschutztool (www.bsi.bund.de/gstool/index.htm).
CC	Der internationale Standard ISO/IEC 15408 steht kostenlos zur Verfügung, z. B. unter standards.iso.org/ittf/PubliclyAvailableStandards/index.html
FIPS 140-2	Der internationale Standard steht kostenlos zur Verfügung, z. B. unter csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
ISO	Informationen zur ISO-Organisation findet man auf der Webseite (www.iso.org).
ITTF	Informationen zu ISO/IEC Joint Technical Committee 1 (JTC 1) und dem Arbeitsprogrammen einzelner Unterkomitees des JTC 1 sowie zu prozeduralen Fragen findet man auf der Webseite (isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/ITTF.htm)
ISO/IEC JTC 1	Webseite des ISO/IEC Joint Technical Committee 1 (JTC 1): isotc.iso.org (siehe dann: Home, dann: ISO/IEC 001 JTC 1 „Information technology“)
ISO/IEC JTC 1/SC 27	Informationen über das ISO/IEC-Unterkomitee ISO/IEC JTC 1/SC27 „IT Security techniques“ sind unter www.jtc1sc27.din.de/en verfügbar
SD 6 „Glossary of IT Security Terminology“	Standing Document 6 (SD6) - Glossary of IT Security Terminology ist verfügbar unter www.jtc1sc27.din.de/sce/sd6 (siehe dann: Downloads)
SD 7 „Catalogue of SC27 Projects and Standards“	Standing Document 7 (SD7) – ISO/IEC JTC 1/SC27 Catalogue of Projects and Standards kann heruntergeladen werden unter www.jtc1sc27.din.de/sce/sd7 (siehe dann: Download)
NIST	Das National Institute of Standards and Technology des US Handelsministerium hat eine Webseite unter www.nist.gov.
DIN	Informationen über die Tätigkeiten des Deutschen Institut für Normung findet man auf der Webseite (www.din.de).
DIN NI	Informationen über den DIN-Normenausschuss „Informationstechnik“ (NI) und seine Arbeitsausschüsse sind unter www.nia.din.de verfügbar

DIN VDE	Das VDE-Vorschriftenwerk umfasst Satzungen und sonstige Grundsatzschriftstücke des VDE, DIN VDE-Normen (VDE-Bestimmungen), VDE-Leitlinien und Beiblätter zu den vorgenannten Schriftstücken (www.vde-verlag.de/normen.html)
ISACA	Information Systems Audit and Control Association – Verband Internationaler Auditoren der Informatik. Der Cobit Standard kann kostenlos bei www.isaca.de heruntergeladen werden. (Es existiert nur von der Version 4.0 eine deutschsprachige Fassung)

13 Danksagung

Auch die vierte Ausgabe des Leitfadens „Kompass der IT-Sicherheitsstandards“ entstand durch die enge Zusammenarbeit zwischen BITKOM und DIN, insbesondere dem Normenausschuss Informationstechnik des DIN, IT-Sicherheitsverfahren, NIA-27.

Wir danken allen federführenden Autoren der ersten Versionen des Leitfadens Jan Dittberner (DIN, Deutsches Institut der Normung e.V.), Dr. Walter Fumy (Bundesdruckerei GmbH), Dr. Michael Gehrke (TTS trusted technologies), Karl-Heinz Holtz (Hewlett Packard GmbH), Heiko Jacob (IT Audit GmbH, Wirtschaftsprüfungsgesellschaft), Timo Kob (HiSolutions GmbH), Helko Kögel (IABG mbH), Knut Krabbes (QMK IT-Security + Quality-Management Services Ltd.), Dr. Marie-Luise Moschgath (PriceWaterhouseCoopers AG), Roland Müller (Daimler Financial Service AG), Thomas Nowey (Universität Regensburg), Daniel Rudolph (Consecur GmbH), Jürgen Sander (PreSecure Consulting GmbH), Andreas Teuscher (SICK AG), Jörg Thomas (Avaya GmbH & Co. KG), Dr. Oliver Weissmann (atsec informations security GmbH), Manfred Willems (TÜV Rheinland Group), Cord Wischhöfer (DIN), Ralph Wölpert (Rittal GmbH & Co. KG).

Unser besonderer Dank gilt den Autoren der vierten Version des Leitfadens für das kontinuierliche Interesse am Thema sowie die zahlreichen Textbeiträge, die diesen umfassenden Leitfaden erst ermöglichten:

- Fumy, Dr. Walter (Bundesdruckerei GmbH),
- Kallwies, Robert, (Controll-IT GmbH)
- Kamp, Thorsten, (datenschutz nord GmbH)
- Koch, Klaus, (CAT-Consulting für Automatisierungstechnik)
- Stutz, Oliver, (datenschutz nord GmbH)
- Wisler, Andreas (GO OUT Production GmbH)

sowie allen Sprechern der Arbeitskreise des DIN NIA-27 IT-Sicherheitsverfahren (vormals DIN NI-27) für Ihre Beiträge und Expertise:

- Rohde, Martina (BSI Bundesamt für Sicherheit in der Informationstechnik)
- von Sommerfeld, Hans (Rohde & Schwarz SIT GmbH)
- Krüger, Dr. Bertolt (SRC Security Research & Consulting GmbH)

sowie für das Korrekturlesen, die Koordination und die Bereitstellung der bibliographischen Angaben

- Ambrosio, Leila (BITKOM e.V.)
- Uhlherr, Martin (DIN Normenausschuss Informationstechnik und Anwendungen)

14 Fragebogen

Ihre Meinung ist uns wichtig.

Bitte nehmen sich 3 Minuten für uns Zeit. Wir möchten diesen Leitfaden weiterentwickeln und noch besser Ihren Bedürfnissen anpassen. Bitte beantworten Sie dazu die nachfolgenden Fragen.

- Wurden Ihre Erwartungen an einen derartigen Leitfaden erfüllt?

☐ ganz ☐ teilweise ☐ gar nicht

- Was war das konkrete Problem, vor dem Sie standen?

- Haben Ihnen die Informationen bei der Lösung Ihrer Problemstellung genutzt?

☐ ja, sehr ☐ ja, teilweise ☐ eher weniger ☐ gar nicht

- Welche Informationen haben Sie vermisst?

- Gibt es Ihrer Ansicht nach Bereiche, die nicht so stark in den Vordergrund gerückt werden sollen, die wir kürzen sollten?

- Ist der Leitfaden für Sie

☐ interessant ☐ hilfreich ☐ zu allgemein ☐ eher unklar/unverständlich (im Sinne von zu abgehoben oder zu technisch)

- Was Sie uns sonst noch sagen möchten

Vielen Dank!

Falls Sie Interesse an der nächsten Version haben, teilen Sie uns bitte Ihre E-Mailadresse mit. Ihre personenbezogenen Daten werden nur für diesen Zweck gespeichert.

Vorname, Name

Email-Adresse

Rückantwort an

BITKOM e.V.
Lutz Neugebauer, Fax: 030.27576-409

oder

DIN e.V.
Cord Wischhöfer, Fax: 030.2601-1723



Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.300 Unternehmen, davon 950 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

Das DIN ist ein eingetragener gemeinnütziger Verein mit Sitz in Berlin (DIN Deutsches Institut für Normung e.V., gegründet 1917). Das DIN ist die für die Normungsarbeit zuständige Institution in Deutschland und vertritt die deutschen Interessen in den weltweiten und europäischen Normungsorganisationen. Dieser Status wurde im Vertrag mit der Bundesrepublik Deutschland am 5. Juni 1975 anerkannt.

Das DIN ist der runde Tisch, an dem sich Hersteller, Handel, Verbraucher, Handwerk, Dienstleistungsunternehmen, Wissenschaft, technische Überwachung, Staat, d. h. jedermann, der ein Interesse an der Normung hat, zusammensetzen, um den Stand der Technik zu ermitteln und unter Berücksichtigung neuer Erkenntnisse in Deutschen Normen niederzuschreiben.



Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org



Deutsches Institut der Normung e.V.
Normenausschuss Informationstechnik und Anwendung (NIA)

Burggrafenstraße 6
10787 Berlin
Telefon 030/2601-0
Telefax 030/2601-1231
nia@din.de
www.nia.din.de