

Inhaltsverzeichnis

Inhaltsübersicht.....	IX
Inhaltsverzeichnis.....	XI
1 Aufgaben und Ziele der Informationssicherheit	1
1.1 Aufgaben und Anforderungen eines ISMS	2
1.1.1 Risikomanagement	2
1.1.2 Gefährdungen erkennen und bewerten	3
1.1.3 Angreifermodelle betrachten	4
1.1.4 Hauptursachen für Sicherheitsprobleme identifizieren	5
1.1.5 Sicherheitskonzept erstellen	5
1.1.6 Sicherheitsmaßnahmen überprüfen.....	7
1.2 Generische Sicherheitsziele	8
1.2.1 Vertraulichkeit.....	8
1.2.2 Integrität	9
1.2.3 Verfügbarkeit.....	9
1.2.4 Authentizität.....	10
1.2.5 Sicherheitsziele und Sicherheitskonzept	11
2 Betriebswirtschaftliche Aspekte der Informationssicherheit.....	15
2.1 Quantitative Modelle	16
2.1.1 Kosten von Risiken	17
2.1.2 Kosten von Sicherheitsvorfällen.....	18
2.1.3 Kosten von Sicherheitsmaßnahmen	19
2.1.4 Das ROSI-Modell	20
2.1.5 Grenzen des ROSI-Ansatzes.....	21
2.1.6 Alternative quantitative Modelle	22
2.2 Qualitative Betrachtungen.....	24
2.2.1 Grenzen betriebswirtschaftlicher Betrachtungen	24
2.2.2 Wirtschaftlichkeit von Investitionsentscheidungen.....	24
2.2.3 Pareto-Prinzip.....	25
2.2.4 Erfahrungswerte – Best Practice	25
3 Hackermethoden	29
3.1 Begriffsdefinition „Hacker“.....	29
3.2 Ursachen von Sicherheitsproblemen	29
3.2.1 SQL-Injection.....	30
3.2.2 Buffer Overflows.....	31
3.2.3 Motivation eines Angreifers.....	33
3.3 Vorgehensweise bei Penetrationstests	33
3.3.1 Informationsbeschaffung	34
3.3.2 Portscans	35
3.3.3 Automatische Überprüfungen	36
3.3.4 Manuelle Untersuchungen	36
3.3.5 Anwendung von Exploits.....	37
3.3.6 Social Engineering	37

3.4	Angriffswerkzeuge.....	38
3.4.1	Rootkits	39
3.4.2	Virus Construction Kits.....	39
3.4.3	Trojaner	40
4	ISO 27001 und ISO 27002	43
4.1	Entstehungsgeschichte	43
4.2	Die Familie der ISO 27000-Standards	45
4.3	ISO 27002	46
4.4	ISO 27001	50
4.4.1	Information Security Management System – Plan-Do-Check-Act	51
4.4.2	Inhaltliche Elemente der ISO 27001	53
4.4.3	Einbindung in das Qualitätsmanagement	55
4.4.4	Prüfungs- und Zertifizierungsprozess	56
5	IT-Grundschutz.....	61
5.1	Historie	61
5.2	IT-Grundschutz Ansatz	62
5.3	IT-Grundschutz Dokumente	63
5.3.1	BSI-Standard 100-1: Managementsysteme für Informationssicherheit	64
5.3.2	BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise	67
5.3.3	BSI-Standard 100-3: Risikoanalyse auf der Basis von IT- Grundschutz.....	72
5.3.4	BSI-Standard 100-4: Notfallmanagement.....	73
5.3.5	IT-Grundschutz-Kataloge	73
5.4	Tool-Unterstützung.....	75
5.5	ISO 27001-Zertifizierung auf Basis von IT-Grundschutz	75
6	Sicherheitskonzept	79
6.1	Ziele des Sicherheitskonzepts	79
6.2	Zentrale Aufgaben im Sicherheitskonzept	80
6.2.1	Berechtigte und Unberechtigte	81
6.2.2	Schwachstellen vermeiden	81
6.2.3	Identifikation von Unregelmäßigkeiten	82
6.2.4	Reaktionen auf Störfälle	82
7	Physische Sicherheit	85
7.1	Bedrohungen.....	85
7.2	Erhöhung der Gebäudesicherheit	86
7.2.1	Bewusste Standortwahl.....	86
7.2.2	Sichere bauliche Gestaltung	87
7.2.3	Schutzzonen.....	87
7.2.4	Rettungs- und Fluchtwege	90
7.3	Angemessene Überwachung.....	90
7.4	Monitoring und automatisierte Maßnahmensteuerung	91
7.5	Wirksamer Brandschutz	91
7.6	Stromversorgung.....	92
7.7	Physische Schutzmaßnahmen in externen Bereichen	93
7.7.1	Mobile Endgeräte	93
7.7.2	Häuslicher Arbeitsplatz	93

7.7.3	Datenträger	93
8	Firewalls	97
8.1	Grundlagen von Firewalls	97
8.2	Netzwerkgrundlagen	99
8.2.1	OSI-Modell	99
8.2.2	Protokolle, Adressen und Ports	101
8.2.3	Netzwerksegmentierung	102
8.3	Firewall-Typen	104
8.3.1	Paketfilter	104
8.3.2	Application Level Gateway	105
8.3.3	Stealth Gateway	106
8.4	Firewall-Architekturen	106
8.4.1	Einstufige Paketfilter-Architektur	106
8.4.2	Multi-Homed-Architektur	107
8.4.3	Demilitarisierte Zone	108
8.4.4	PAP-Firewall-Architekturen	110
8.5	Firewall-Konzepte	111
8.5.1	Anforderungsanalyse für den Firewall-Einsatz	112
8.5.2	Betriebliche Anforderungen für die Firewall-Konzeption	112
8.6	Grenzen von Firewalls	113
9	Kryptografie	115
9.1	Vorgehensweise	116
9.2	Begriffsklärung	117
9.3	Angriffs- und Sicherheitsziele	118
9.3.1	Lesen von Daten – Vertraulichkeit	118
9.3.2	Ändern von Daten – Integrität	119
9.3.3	Wiedereinspielen von Daten – Frische von Daten	119
9.3.4	Vortauschen einer Identität – Urheber-Authentizität	120
9.3.5	Abstreiten der Verantwortung – Nicht-Abstreitbarkeit	120
9.3.6	Weitere Angriffs- und Sicherheitsziele	121
9.4	Grundsätzliche Angriffsszenarien	122
9.5	Sichere Kanäle	123
9.5.1	Verschlüsselung	123
9.5.2	Chiffrierverfahren	124
9.5.3	Betriebsmodi	129
9.5.4	Integrität	133
9.5.5	Authentisierte Verschlüsselung	137
9.5.6	Weitere Anwendungen	138
9.6	Herausforderungen der Schlüsselverteilung	139
9.6.1	Der direkte Weg	139
9.6.2	Der indirekte Weg über vertrauenswürdige Dritte	141
9.7	Asymmetrische Verfahren zur Schlüsselverteilung	142
9.7.1	Grundprinzipien asymmetrischer Verfahren	142
9.7.2	Schlüsseltransport	143
9.7.3	Schlüsselaustausch	145
9.8	Digitale Signaturen	147
9.8.1	Grundprinzipien digitaler Signaturen	147
9.8.2	Digitale Signaturen für die Nicht-Abstreitbarkeit	149
9.8.3	Digitale Signaturen für Zertifikate	150

9.9	Praktischer Einsatz	151
9.9.1	Schlüssellängen	151
9.9.2	Proprietäre Verfahren.....	152
9.9.3	Proprietäre Implementierungen	153
9.9.4	Erzeugung von Zufallszahlen.....	154
10	Vertrauensmodelle und PKI-Komponenten.....	157
10.1	Vertrauensmodelle	158
10.1.1	Web of Trust.....	158
10.1.2	Zentrales Modell der Public Key Infrastruktur	160
10.2	Public Key Infrastruktur	160
10.2.1	Zertifikate und CRLs	160
10.2.2	Zertifizierungshierarchien.....	163
10.2.3	Verifikation einer digitalen Signatur	163
10.2.4	Komponenten und Prozesse einer PKI.....	165
10.2.5	Policies für Public Key Infrastrukturen	171
10.3	Standards im Bereich PKI	172
10.3.1	X.509 Standard	172
10.3.2	PKIX-Standards.....	172
10.3.3	PKCS-Standards.....	173
10.3.4	Common PKI Spezifikationen	174
10.4	Verknüpfung von Public Key Infrastrukturen.....	175
10.5	Langzeitarchivierung.....	177
11	Virtual Private Networks.....	181
11.1	VPN-Szenarien.....	182
11.1.1	Site-to-Site-VPN	182
11.1.2	End-to-Site-VPN.....	183
11.1.3	End-to-End-VPN.....	183
11.1.4	Protokollebenen von VPNs und VPN-Tunnel	184
11.2	Technische Realisierung von VPN	185
11.2.1	PPP, L2F und PPTP.....	185
11.2.2	Layer 2 Tunneling Protocol – L2TP	186
11.2.3	IP Security – IPsec.....	190
11.2.4	OpenVPN	198
11.3	Spezielle Risiken von VPN.....	200
12	Sicherheit in mobilen Netzen	203
12.1	Bedrohungen in mobilen Netzen.....	203
12.2	Wireless LAN.....	205
12.2.1	Entwicklung und Standardisierung.....	205
12.2.2	Netzarchitektur und Netzkomponenten.....	206
12.2.3	Sicherheitsverfahren	207
12.2.4	Empfohlene Sicherheitsmaßnahmen.....	210
12.3	Bluetooth	212
12.3.1	Entwicklung und Standardisierung.....	212
12.3.2	Netzarchitektur und -komponenten.....	213
12.3.3	Sicherheitsverfahren in Bluetooth	213
12.3.4	Bluetooth-Sicherheitsmechanismen im Detail	219
12.3.5	Bewertung der Sicherheitsmaßnahmen.....	222
12.4	Mobilfunk	223
12.4.1	GSM	223

12.4.2	GPRS	231
12.4.3	UMTS	233
12.5	Mobile Anwendungen und Endgeräte	236
12.5.1	USB-Sticks	236
12.5.2	Anwendungsdaten und Zugriffsschutz	237
12.5.3	PDAs	237
13	Authentifizierung und Berechtigungsmanagement	241
13.1	Identität	241
13.2	Identifizierung	242
13.3	Authentifizierung	242
13.3.1	Authentifizierung durch Wissen	243
13.3.2	Authentifizierung durch Besitz	249
13.3.3	Authentifizierung durch Biometrie	251
13.3.4	Authentifizierung in verteilten Systemen	252
13.4	Autorisierung und Zugriffskontrolle	256
13.4.1	Zugriffsrechtematrix	257
13.4.2	Zugriffskontrolllisten	258
13.4.3	Capabilities	258
13.4.4	Rollenbasierte Zugriffskontrolle	259
13.4.5	Nachteile von Zugriffskontrollstrategien	260
13.5	Identitäts- und Berechtigungsmanagement	260
13.6	Single Sign-On	262
13.6.1	Unternehmensweites Single Sign-On	262
13.6.2	SSO für Web-Services	264
14	Windows Betriebssystemssicherheit	269
14.1	Schutz der Windows-Ressourcen	269
14.1.1	Benutzer- und Gruppenkonten	269
14.1.2	Subjects	271
14.1.3	Objekte	272
14.1.4	Andere Ressourcen in Windows	274
14.2	Security Policies	275
14.2.1	Identifizierung und Authentifizierung	276
14.2.2	Discretionary Access Control	277
14.2.3	Privilegien	279
14.2.4	Wiederverwendung von Objekten	280
14.2.5	Audit-Mechanismen	284
15	Unix: Maßnahmen zur Systemsicherheit	291
15.1	Sicherheitsmechanismen in Unix-Systemen	291
15.1.1	Benutzer, Gruppen und Berechtigungen	292
15.1.2	Zugriffsrechte	296
15.1.3	Dateisystem und Zugriffskontrolle	303
15.1.4	Pfade, Umgebungsvariablen und Pfadlisten	305
15.1.5	Authentifizierung und Passwörter	307
15.2	Sicherheit im Netzwerk	309
15.2.1	Netzwerkdienste	309
15.2.2	Authentifizierung im Netzwerk	310
15.2.3	Unix/Linux als Firewall	313
15.3	Sicherheit im Betrieb	313
15.3.1	Einschränkung des Bootvorgangs	313

15.3.2	Monitoring und Überwachung	314
15.3.3	Eindämmung von Informationslecks	317
15.3.4	Unix-Härtung	318
16	Löschen und Entsorgen	323
16.1	Anforderungen zum Löschen und Entsorgen	323
16.2	Lösch- und Entsorgungskonzept	325
16.2.1	Speicherorte	326
16.2.2	Angemessene Löschrstrategien	329
16.2.3	Verantwortlichkeiten und Integration in den Arbeitsalltag	330
16.3	Technische Löschrmaßnahmen	330
16.3.1	Einfaches Löschrn	331
16.3.2	Sicheres Löschrn	331
16.3.3	Vollverschlüsselung und Löschrn	332
16.3.4	Löschrn auf USB-Sticks und anderen Flash-Medien	332
16.3.5	Vernichten und Entsorgen	333
17	Sicherheit im World Wide Web und E-Commerce	339
17.1	Bedrohungen und Sicherheitsmaßnahmen im Web	339
17.1.1	Einführung in Web-Anwendungen	339
17.1.2	Ausgewählte Angriffe	345
17.1.3	Sicherung von Web-Anwendungen	347
17.1.4	Phishing	348
17.2	E-Commerce und E-Payment	349
17.2.1	Online-Banking	349
17.2.2	Elektronische Bezahlverfahren	352
18	Awareness	357
18.1	„Risikofaktor“ Mensch	357
18.1.1	Zur Wahrnehmung von IT-Sicherheit	358
18.1.2	Randbedingungen und Konsequenzen	359
18.2	Durchführung von Awareness-Kampagnen	360
18.2.1	Kampagnen-Problematiken	360
18.2.2	Zielsetzung einer Awareness-Kampagne	362
18.3	Awareness in der Praxis	364
18.3.1	Erfolgsfaktoren	364
18.3.2	Beteiligte	365
18.3.3	Das Vier-Phasen-Konzept einer Awareness-Kampagne	366
18.3.4	Erfolgsmessung	369
19	Computer-Viren und Content Security	373
19.1	Verbreitungswege von Malware	373
19.2	Unerwünschte Inhalte	374
19.2.1	Klassen von „Malicious Code“	374
19.2.2	Spam	376
19.2.3	Aktive Inhalte	377
19.2.4	Bedrohungen durch Malware	378
19.3	Ansätze zur Abwehr von Malware	380
19.4	Abschottung von Systemen	381
19.5	Content-Analyse	381
19.5.1	Erfassung des Netzwerkverkehrs	383
19.5.2	Dekomposition der Inhalte und Header-Analyse	384

19.5.3	Klassifikation von Inhalten.....	385
19.5.4	Aktion	386
19.5.5	Besonderheiten bei Anti-Spam-Maßnahmen.....	387
19.5.6	Content-Filter und verschlüsselte Inhalte.....	389
19.6	Verhaltensanalyse.....	390
20	Intrusion Detection	393
20.1	Einordnung und Definitionen.....	393
20.2	Architektur und Komponenten von Intrusion-Detection-Systemen	394
20.3	Grundproblem der Analyse - oder „der Schein trügt“.....	396
20.4	Typen von Intrusion-Detection-Systemen.....	397
20.4.1	Host-based Intrusion-Detection-Systeme	397
20.4.2	Network-based Intrusion-Detection-System	398
20.4.3	Hybride Intrusion-Detection-Systeme	399
20.5	Komponenten von Intrusion-Detection-Systemen	399
20.5.1	Hostsensoren	399
20.5.2	Netzsensoren	400
20.5.3	Datenbankkomponenten	401
20.5.4	Managementstation.....	401
20.5.5	Auswertungsstation.....	401
20.6	Methoden der Angriffserkennung.....	402
20.6.1	Erkennen von Angriffsmustern.....	402
20.6.2	Anomalieerkennung	402
20.6.3	Korrelation von Ereignisdaten.....	403
20.7	Das Intrusion-Detection-Dilemma	403
20.8	Ausblick und Vorgaben für IDS.....	404
20.8.1	Anforderungen an die Sicherheitsadministration.....	405
20.8.2	Auswahl und Test eines IDS.....	406
21	Datensicherung	409
21.1	Zwecke der Datensicherung	409
21.2	Strategien der Datensicherung	411
21.3	Backups von vertraulichen Daten	413
21.4	Backup-Medien	413
21.5	Erfolgsfaktoren für Recovery.....	414
21.5.1	Physische Verfügbarkeit	414
21.5.2	Betriebliche Voraussetzungen für Recovery.....	415
21.5.3	Recovery-Fähigkeit überprüfen.....	415
21.6	Datensicherungskonzept	416
22	Business-Continuity-Management.....	419
22.1	Business Continuity.....	419
22.1.1	Hohe Verfügbarkeit und schwere Störfälle beherrschen	419
22.1.2	Business-Impact-Analyse.....	420
22.1.3	Verantwortung für Business Continuity.....	425
22.2	Business Continuity vorbereiten	425
22.2.1	Notfall-Teams und Krisenstab etablieren.....	426
22.2.2	Störfall-Eskalationswege aufbauen.....	427
22.2.3	Notfallhandbuch bereitstellen.....	428
22.2.4	Notfallvorsorge	431
22.2.5	Krisenkommunikation vorbereiten.....	432

22.2.6	BC-Training, BC-Awareness, und BC-Kultur	433
22.3	BCM etablieren.....	434
22.3.1	Das BCM-Team.....	434
22.3.2	Initialisierung des Business-Continuity-Management	435
22.3.3	BCM-Planungsphase	435
22.3.4	Umsetzungsphase	437
22.3.5	Überwachung	437
22.3.6	Weiterentwicklung	438
22.4	Standards für BCM.....	439
22.4.1	BS 25999.....	439
22.4.2	BCI Good Practice Guidelines	442
22.4.3	BSI-Standard 100-4 Notfallmanagement	443
	Verzeichnisse.....	445
	Verzeichnis der Autoren	445
	Übersicht zu Standards der Informationssicherheit	449
	Verzeichnis der Abbildungen.....	473
	Verzeichnis der Tabellen	477
	Abkürzungen und Glossar	479
	Index	479