

Prof. Dr. Norbert Pohlmann
Hartmut F. Blumberg

Der IT-Sicherheitsleitfaden



Inhaltsverzeichnis

Gruß	wort.....	17
Vorwort		19
Übersicht		21
Über die Autoren		25
Einleitung		27
i Gefahren sehen und bemessen		43
1.1 Gefahren erkannt, Gefahr gebannt		43
1.2 Allgemeine Risiken und Bedrohungen		44
1.3 Bedrohungen eines IT-Systems		46
1.3.1 Passive Angriffe		47
1.3.2 Aktive Angriffe		50
1.3.3 Unbeabsichtigte Verfälschung		54
1.3.4 Spezifische Bedrohungen der Endsysteme		57
1.4 Die Angreifer		62
1.5 Juristische Rahmenbedingungen		64
1.5.1 Das Grundgesetz		65
1.5.2 Das Volkszählungsurteil		65
1.5.3 Landesverfassungen		66
1.5.4 Bundesdatenschutzgesetz (BDSG)		67
1.5.5 Signaturgesetz und Signaturverordnung		67
1.5.6 Weitere Gesetze und Verordnungen		68
1.6 Gefahren am Beispiel einer Verwaltungsbehörde		68
1.6.1 Sicherheitsmanagement		68
1.6.2 Kontinuitätsplanung		69
1.6.3 Datensicherungskonzept		69
1.6.4 Computervirenschutz-Konzept		70
1.6.5 Gebäudesicherheit		71
1.6.6 Räume für Server und technische Infrastruktur		72
1.6.7 Datenträgerarchiv		72
1.6.8 PC-Systeme		73
1.6.9 Laptops, Notebooks und PDAs		74

1.6.10 Server	75
116.II Heterogenes Netzwerk	76
1.6.12 E-Mail-Kommunikation	76
1.6.13 Internetzugriff	77
1.6.14 IT-Dienste und Anwendungen	78
1.7 Zusammenfassung	78
2 Ziele festlegen und gewichten	81
2.1 IT-Sicherheit als Teil der wesentlichen Unternehmensziele	81
2.2 Das Spannungsfeld der IT-Sicherheitslösungen	83
2.2.1 Ergonomie	84
2.2.2 Effektivität	84
2.2.3 Ökonomie	85
2.2.4 Klassifizierung der IT-Sicherheitsziele	85
2.3 Klare Ziele: erreichbar und messbar	87
2.4 Die IT-Sicherheitsleitlinie	88
2.4.1 Die Inhalte einer IT-Sicherheitsleitlinie	90
2.4.2 Erstellen einer IT-Sicherheitsleitlinie	90
2.4.3 Die Organisation des IT-Risikomanagements	92
2.4.4 Strategien zur Risikoanalyse und Risikobewertung	95
2.4.5 Klassifizierung von Daten und Diensten	97
2.4.6 Organisationsweite Richtlinien zu Sicherheitsmaßnahmen	98
2.4.7 Kontinuitätsplanung	103
2.4.8 Gewährleistung der Sicherheitsniveaus	105
2.4.9 Der Lebenszyklus der IT-Sicherheitsleitlinie	106
2.5 Beispiel einer IT-Sicherheitsleitlinie	107
2.5.1 Einleitung	107
• Aufbau des Dokuments	108
• Gültigkeitsdauer	108
2.5.2 Struktur der IT-Sicherheitsleitlinien des Unternehmens	109
• Allgemeine Sicherheitsleitlinie	109
• Orgaspezifische Sicherheitsleitlinien	110
• Richtlinien	110
2.5.3 Ziele	110
• Ziel der IT-Sicherheit des Unternehmens	110
• Ziel der Allgemeinen IT-Sicherheitsleitlinie	110
• Ziel dieses Dokuments	111
2.5.4 Gegenstand und Geltungsbereich der Leitlinie	111

2.5.5	Begriffsbestimmung	111
2.5.6	Verpflichtungserklärung der Unternehmensführung	113
2.5.7	Outsourcing der IT	113
	• Schnittstelle FIRMA / OUTSOURCING-FIRMA	114
	• Sicherheitsanforderungen	116
2.5.8	Das IT-Sicherheitsmanagement	117
	• Organisation	117
	• Aufgaben	119
2.5.9	Verantwortlichkeiten	120
	• Eigentümer und Treuhänder von IT-Gütern	120
	• Die OUTSOURCING-FIRMA als Treuhänder	121
2.5.10	Allgemeine Anforderungen und Regeln	122
	• Erlaubnisprinzip	122
	• Unternehmensweite Strategie und Methodik für IT-Sicherheit	122
	• IT-Sicherheit als integraler Bestandteil der IT	122
	• Förderung des Sicherheitsbewusstseins (»Awareness«)	123
	• Einhaltung von Gesetzen und Verordnungen	123
	• Klassifikation von IT-Gütern	123
	• Schutz von IT-Gütern	124
	• Wirtschaftlichkeitsprinzip	124
	• Interessenkonflikte	124
	• Ständige Kontrolle und Fortschreibung der Sicherheitsmaßnahmen	124
	• Orientierung an internationalen Richtlinien und Standards	124
	• Verstöße gegen Sicherheitsleitlinien	124
2.5.11	Sicherheitsrelevante Objekte	124
	• Sicherheitsrelevantes Objekt »Organisation«	126
	• Sicherheitsrelevantes Objekt »Personal«	126
	• Sicherheitsrelevantes Objekt »Kontinuitätsplanung«	127
	• Sicherheitsrelevantes Objekt »Wartung«	128
	• Sicherheitsrelevantes Objekt »Beschaffung«	128
	• Sicherheitsrelevantes Objekt »Infrastruktur«	131
	• Sicherheitsrelevantes Objekt »Netzwerke«	131
	• Sicherheitsrelevantes Objekt »IT-Systeme«	133
	• Sicherheitsrelevantes Objekt »DFÜ / Externe Zugänge«	134
	• Sicherheitsrelevantes Objekt »Telekommunikation«	134

• Sicherheitsrelevantes Objekt »Daten«	135
• Sicherheitsrelevantes Objekt »Applikationen«	138
• Sicherheitsrelevantes Objekt »Virenschutz«	139
• Sicherheitsrelevantes Objekt »Zugangsschutz / Authentisierung«	139
• Sicherheitsrelevantes Objekt »Kryptographie«	140
2.5.12 Orgaspezifische Sicherheitsleitlinien	141
2.5.13 Fortschreibung dieses Dokuments	142
Risiken erkennen und bewerten	143
3.1 Wirksames Risikomanagement braucht einen Startpunkt	143
3.2 Die generelle Schutzbedarfsermittlung	145
3.2.1 Erfassung aller vorhandenen und projektierten IT-Systeme	146
3.2.2 Aufnahme der IT-Dienste	146
3.2.3 Zuordnung der IT-Dienste zu den einzelnen IT-Systemen	146
3.2.4 Klassifizierung des Schutzbedarfs für jedes IT-System	146
3.3 Die Grundschutz-Analysemethodik	149
3.3.1 Abbildung des IT-Systems durch vorhandene Bausteine	150
3.3.2 Erfassen des jeweiligen Bausteins	151
3.3.3 Analyse der Maßnahmenbeschreibungen	152
3.3.4 Soll-Ist-Vergleich zwischen vorhandenen und empfohlenen Maßnahmen	152
3.4 Die detaillierte Risikoanalyse	153
3.4.1 Systemgrenzen definieren	154
3.4.2 »Teile und Herrsche«: Modularisierung	154
3.4.3 Analyse der Module	155
3.4.4 Bewertung der Bedrohungssituation	157
3.4.5 Schwachstellenanalyse	159
3.4.6 Identifikation bestehender Schutzmaßnahmen	159
3.4.7 Risikobewertung	160
3.4.8 Auswertung und Aufbereitung der Ergebnisse	161
3.5 Die Wirksamkeit der Schutzmaßnahmen	161
3.6 Audit bisheriger Schutzmaßnahmen	164
3.6.1 Der Idealfall	164
3.6.2 Der pragmatische Ansatz	165
3.7 Beispiele für Bewertungsmethodiken	166
3.7.1 Schutzbedarfsfeststellung	166
3.7.2 Detaillierte Risikoanalyse	172

3.8	Verantwortung für die IT-Sicherheit179
3.9	Wer unterstützt Sie bei der Sicherheitsanalyse am besten?179
3.10	Angemessener Aufwand für die Erstellung einer IT-Sicherheitsstudie.181
3.11	Resultate einer IT-SicherheitsStudie.182
3.12	Feststellung des Schutzbedarfs.183
	Schutzmaßnahmen priorisieren und umsetzen189
4.1	Rahmenbedingungen.191
4.2	Organisatorische Schutzmaßnahmen.192
4.2.1	Entwicklung einer IT-Sicherheitsleitlinie.193
	• Zweck der IT-Sicherheitsleitlinie193
	• Erstellung und Fortschreibung194
	• Festlegung der Verantwortungsbereiche195
4.2.2	Realisierungsplanung.196
	• Auswahl der Schutzmaßnahmen196
	• Restrisikobetrachtung200
	• IT-Systemsicherheits-Leitlinien201
4.2.3	Migrationspläne.202
4.2.4	Fortschreibung des IT-Sicherheitskonzepts.203
4.3	Administrative Schutzmaßnahmen.204
4.3.1	Implementierung von Schutzmaßnahmen.204
4.3.2	Dokumentation.205
4.3.3	Sensibilisierung.206
4.3.4	Schulung.207
4.3.5	Audit von Sicherheitssystemen.208
4.3.6	Infrastruktur.209
	• Zugangsgesicherter Raum209
	• Unterbrechungsfreie Stromversorgung (USV).209
	• Geschützte Leitungsführung210
	• Dokumentation210
	• Zentrales Netzwerkmanagement-System210
	• Sicherheitsmanagement210
	• Nutzer.214
	• Allgemeine Schutzmaßnahmen.214
4.3.7	Personal.215
	• Sicherheitsmanagement215
	• Nutzer.217

4.3.8	Notfallbehandlung	218
	• Festlegung von Verfügbarkeitsanforderungen	218
	• Redundanzen	218
4.3.9	Zusammenfassung	218
4.4	Technische Schutzmaßnahmen	219
4.4.1	Technologische Grundlagen für Schutzmaßnahmen und Sicherheitsmechanismen	220
	• Private-Key-Verfahren	220
	• Public-Key-Verfahren	221
	• One-Way-Hashfunktion	223
	• Hybride Verschlüsselungstechnik	223
	• Chipkarte (SmartCard)	224
	• Ein Wettlauf um die Sicherheit	226
4.4.2	Public-Key-Infrastrukturen	227
	• Idee und Definition von Public-Key-Infrastrukturen	227
	• Analogie: Standesamt und Einwohnermeldeamt	230
	• Modelle von Public-Key-Infrastrukturen	230
	• Probleme in der Praxis	232
	• Erstellung und Verifizierung von Zertifikaten	234
	• Umsetzungskonzepte von Public-Key-Infrastrukturen	235
	• Migration und Interoperabilität	237
	• Zusammenfassung	241
4.4.3	E-Mail-Security	241
	• Idee und Definition von E-Mail-Security	242
	• Funktionen von E-Mail-Security	242
	• Sicherheitsdienste des E-Mail-Sicherheitssystems	246
	• E-Mail-Security aus Sicht des Nutzers?	247
	• Zusammenfassung	247
4.4.4	Anti-SPAM-Technologie	247
	• Idee und Definition von SPAM-Mails	247
	• Analogie: Verstopfter Briefkasten	250
	• Anti-SPAM-Technologien	250
	• Zusammenfassung	254
4.4.5	Die virtuelle Poststelle: Sicheres E-Mail-Gateway	255
	• Idee und Definition einer virtuellen Poststelle	256
	• Analogie: Die Poststelle	257
	• Systemübersicht und Funktionsweise	257
	• Zentrale Sicherheitsfunktionen	260

• Vorteile der virtuellen Poststelle	260
• Zusammenfassung	262
4.4.6 Verschlüsselungssysteme gespeicherter Informationen	262
• Idee und Definition der Verschlüsselung von Daten	262
• Analogie: Der Safe	263
• Verschlüsselung der Festplatte für Notebooks oder PCs	264
• Unabhängige Dateiverschlüsselung	265
• Verzeichnisverschlüsselung	265
• Dateiverschlüsselung	265
• Zusammenfassung	265
4.4.7 Virtual Private Networks	266
• Idee und Definition von Virtual Private Networks	266
• Analogien: Sicherheitstransporter, Pipeline, Rohrpost	268
• Konzepte von Virtual Private Networks	271
• Vorteile von Black-Box-Lösungen	273
• Anwendungsformen und Einsatzmöglichkeiten von VPNs	276
• Zusammenfassung	279
4.4.8 Secure Socket Layer (SSL), Transport Layer Security (TLS)	279
• Idee und Definition von Transport Layer Security	280
• Analogien: Sicherheitstransporter, Pipeline, Rohrpost	281
• Umsetzungskonzept	281
• Zusammenfassung	282
4.4.9 Authentisierungsverfahren	283
• Idee und Definition von Authentisierungsverfahren	283
• Analogie: Ausweiskontrolle	284
• Generelle Authentisierungsverfahren	284
• Beispiele von Authentisierungsverfahren	286
• Zusammenfassung	296
4.4.10 Firewall-Systeme	296
• Idee und Definition von Firewall-Systemen	297
• Analogie: die Brandschutzmauer und der Pförtner	298
• Aufgaben von Firewall-Systemen	300
• Weitere Ziele eines Firewall-Systems	301
• Aktive Firewallelemente	302
• Das richtige Firewallkonzept für jeden Einsatzfall	305
• Einsatz von Internet Firewall-Systemen	309
• Konzeptionelle Grenzen eines Firewall-Systems	310
• Zusammenfassung	313

114.ii	Personal Firewall	313
	• Idee und Definition einer Personal Firewall	313
	• Analogie: Vitamin C für den PC oder das Notebook	315
	• Komponenten einer Personal Firewall	315
	• Zusammenfassung	319
4.4.12	PC-Systeme durch benutzer- und anwendungsspezifische Rechte sichern	319
	• Idee und Definition benutzerspezifischer Rechte	319
	• Analogie: Immunisierung von PCs oder Notebooks	320
	• Das Sicherheitskonzept	320
	• Zusammenfassung	321
4.4.13	Intrusion Detection	322
	• Idee und Definition von Intrusion Detection Systemen	323
	• Analogie: Videoüberwachung und Alarmanlage	324
	• Das Sicherheitskonzept	325
	• Aufbau und Funktionsweise von IDS	326
	• Anwendungsformen und Auswertungskonzepte	328
	• Grenzen von IDS	332
	• Zusammenfassung	333
4.4.14	Anti-Malware-Systeme	334
	• Idee und Definition eines Anti-Malware-Systems	334
	• Analogie: Virus	334
	• Probleme bei der Erkennung von Viren	334
	• Zusammenfassung	336
4.4.15	Biometrische Verfahren	336
	• Idee und Definition von biometrischen Verfahren	336
	• Vergleich der verschiedenen biometrischer Verfahren	339
	• Verfahren der Fingerabdruckmessung	339
	• Match on Card	341
	• Zusammenfassung	341
4.5	Fallbeispiele	342
4.5.1	Das Ende des PIN-Codes	342
	• Anforderungen	342
	• Lösung	343
	• Ablauf	343
4.5.2	Sicherheit für die Geschäftsprozesse in einer Bank	343
	• Anforderungen	344
	• Lösung	344
	• Ablauf	344

4.5.3	Firewall - sicherer Internetzugriff bei großen Organisationen .	346
	• Anforderungen	346
	• Lösung	346
	• Ablauf	347
4.5.4	Authentisierungsverfahren mittels Mobiltelefon.	348
	• Anforderung	348
	• Lösung	349
	• Ablauf	350
4.5.5	PKI im Finanzsektor.	350
	• Anforderungen	350
	• Lösung	351
	• Ablauf	351
4.5.6	Verschlüsselung von Notebooks.	351
	• Anforderungen	352
	• Lösung	352
	• Ablauf	352
4.5.7	Datei- und Verzeichnisverschlüsselung.	353
	• Anforderungen	353
	• Lösung	354
	• Ablauf	354
4.5.8	Sichere Ankopplung von Außendienstmitarbeitern	354
	• Anforderungen	355
	• Lösung	355
	• Ablauf	355
4.5.9	Vertrauenswürdige Vernetzung	357
	• Anforderung	357
	• Lösung	357
	• Ablauf	357
4.6	Zusammenfassung	358
5	Sicherheit fortschreiben - die Wirksamkeit gewährleisten.	359
5.1	Nur eine kontinuierliche Sicherheit ist nachhaltig wirksam.	359
5.2	Der Faktor Mensch	360
5.2.1	Vertretungsregelungen.	361
5.2.2	Nachhaltige Gewährleistung eines positiven Betriebsklimas .	362
5.2.3	Prüfung der Einhaltung der organisatorischen Vorgaben	362
5.2.4	Geregelte Verfahrensweise bei vermuteten Sicherheitsverletzungen	363

5.2.5	Externe Mitarbeiter	363
5.2.6	Schulung und Sensibilisierung zu IT-Schutzmaßnahmen . . .	364
5.2.7	Sicherheitssensibilisierung und Schulung für neue Mitarbeiter und neue IT-Systeme.	366
5.2.8	Betreuung und Beratung der IT-Nutzer.	367
5.2.9	Aktionen beim Auftreten von Sicherheitsproblemen (Incident Handling Pläne).	367
5.2.10	Schulung des Wartungs- und Administrationspersonals	368
5.2.11	Einweisung in die Regelungen der Handhabung von Kommunikationsmedien.	368
5.3	Qualitätssicherung der Sicherheit	369
5.4	Kriterien zur Fortschreibung der Sicherheitsziele	369
5.5	Reaktion auf Sicherheitsvorfälle.	370
5.6	Kontinuierliche Administration und Schwachstellenanalyse.	371
5.6.1	Die Sicherheitsadministration	371
5.6.2	Die kontinuierliche Schwachstellenanalyse.	371
5.6.3	Das Computer Emergency Response Team	373
5.7	Audits und Reviews.	373
5.8	Minimal-Checkliste	376
5.8.1	IT-Sicherheitsmanagement	376
5.8.2	Sicherheit von IT-Systemen.	377
5.8.3	Vernetzung und Internet-Anbindung	377
5.8.4	Beachtung von Sicherheitserfordernissen.	378
5.8.5	Wartung von IT-Systemen: Umgang mit Updates.	378
5.8.6	Passwörter und Verschlüsselung	378
5.8.7	Kontinuitätsplanung	379
5.8.8	Datensicherung	379
5.8.9	Infrastruktur Sicherheit.....	379
5.8.10	Mobile Sicherheit	379
6	Philosophische Aspekte der Informationssicherheit	381
6.1	Einleitung	381
6.2	Die Grenzen der technischen Risikoanalyse.	382
6.3	Der Beitrag philosophischer Disziplinen zur Wertediskussion	384
6.4	Die »postmoderne« Informationsgesellschaft	385
6.5	Das Internet - ein »böses« Medium?	386
6.6	Der Wert der Privatsphäre.	388
6.7	Schlussfolgerung	390

7	Sicherheit und Vertrauenswürdigkeit in der Informationsgesellschaft...	393
7.1	Einleitung	393
7.2	Sicherheit	393
7.2.1	Kryptographie: Ein Wettlauf um die Sicherheit.....	393
7.2.2	Firewall-Systeme	395
7.2.3	Biometrie-Verfahren	396
7.2.4	Betriebssysteme	398
7.2.5	Fazit	398
7.3	Vertrauenswürdigkeit	399
7.3.1	Sichere Betriebssysteme	400
7.3.2	Administrative Schutzmaßnahmen	401
7.3.3	Organisatorische Schutzmaßnahmen	401
7.3.4	Rechtliche Rahmenbedingungen	401
7.3.5	Internationale Kooperationen	402
7.3.6	IT-Sicherheit kostet Geld	402
7.3.7	Total Risk Management	402
7.3.8	Sicherheitsaudits	403
7.3.9	Fazit	403
7.4	Ausblick	403
8	Wirtschaftlichkeitsbetrachtung von IT-Schutzmaßnahmen	405
8.1	Einführung	405
8.2	IT-Sicherheitsrisiken und -investment	408
8.3	Total Cost of Ownership - Kostenaspekte	409
8.3.1	Beschaffungsphase	409
8.3.2	Aufrechterhaltung des Betriebs	411
8.3.3	Zusammenfassung: Total Cost of Ownership	414
8.4	Kosten-Nutzen-Betrachtung im Hinblick auf das zu tragende Risiko	415
8.4.1	Diskussion der Kosten-Nutzen-Betrachtung	416
8.4.2	Wahrscheinlichkeit eines bestimmten Profits	417
8.5	Return on Security Investment (RoSI) - Nutzenaspekt	418
8.5.1	Beispiel: Notebookverluste	420
8.5.2	Return on Security Investment (RoSI) - Berechnung	421
8.6	Kosten-Nutzen-Betrachtung - Internet als Kommunikationsplattform	424
8.7	Kosten-Nutzen-Betrachtung im Hinblick auf eine Nicht-Nutzung des Internets	427
8.8	Gesamtwirtschaftliche Betrachtung von IT-Sicherheit	428
8.9	Zusammenfassung	428

A	Literaturverzeichnis	431
	A.i Fundstellen im Internet	435
	A.2 CERT (Computer Emergency Response Teams).	436
	A.3 Standards und Zertifizierung.	437
	A.4 Datenschutz.	437
B	Glossar, Abkürzungen	439
	Stichwortverzeichnis	469