

Inhaltsverzeichnis

	Vorwort von Dr. Markus Morawietz	II
	Vorwort	15
I	Einführung in die IT-Sicherheit	25
I.1	IT-Sicherheit und wie man sie erreicht	25
I.2	Wichtige Begriffe	28
I.2.1	Normenreihe ISO 2700x und Dokumente des BSI	29
I.2.2	Information-Security-Management-System	30
I.2.3	IT-Sicherheitsorganisation	31
I.2.4	Unternehmenswerte	32
I.2.5	Dateneigentümer und Risikoeigentümer	33
I.2.6	Asset-Management	34
I.2.7	Schutzbedarf, Schutzziele, Schutzstufen und die Klassifizierung	35
I.2.8	Risiko, Risikoberechnung, Risikobehandlung und Maßnahmen	37
I.2.9	Angriffspfad, Schwachstellen und Bedrohungen	39
I.2.10	Richtlinien	39
I.2.11	IT-Sicherheitskonzept	40
I.3	Das Hamsterrad	41
I.4	Die allzu menschlichen Fallstricke	42
I.5	Motivation, die IT-Sicherheit zu erhöhen	45
I.5.1	Externe Vorgaben	45
I.5.2	Verpflichtung zur Datensicherheit	47
I.5.3	Haftung auf verschiedenen Ebenen	49
I.6	Reduzierung des Risikos	50
I.6.1	Angriffe durch eigene Mitarbeiter	50
I.6.2	Angriffe von außen	51

2	Das IT-Sicherheitsprojekt	53
2.1	Kurz zusammengefasst	53
2.2	Rahmenbedingungen und Erfahrungen	56
2.2.1	Das Wesen eines Projekts	56
2.2.2	IT-Sicherheit als Top-down-Ansatz	57
2.2.3	Die kontinuierliche Verbesserung	59
2.3	Die Ziele des IT-Sicherheitsprojekts	61
2.3.1	Aufgabe: Der Geltungsbereich	62
2.3.2	Aufgabe: Sicherheitsniveau als Projektziel	64
2.4	Der Projektablauf	68
2.4.1	Das Vorgehen im Überblick	68
2.4.2	Aufgaben, Input und Output	69
2.4.3	Transparenz schaffen	71
2.4.4	Regeln einführen	75
2.4.5	Durchführung von Audits	78
3	Transparenz schaffen	81
3.1	Übersicht über die Vorgehensweise	81
3.2	Die Basisdokumente der IT-Sicherheit	83
3.2.1	Aufgabe: Information Security Policy	84
3.2.2	Aufgabe: Klassifizierungsrichtlinie	87
3.3	Der Workshop und die Erfassung des aktuellen Status	90
3.3.1	Zielsetzung und Ablauf	90
3.3.2	Eine kleine Business-Impact-Analyse (BIA)	94
3.4	Themengebiete der IT-Sicherheit	102
3.4.1	Zugrunde liegende Standards	102
3.4.2	Aufgabe: Themengebiete der IT-Sicherheit auswählen	103
4	Regeln einführen	109
4.1	Richtlinien als formalisierte Regeln	110
4.1.1	Struktur und Inhalt von Richtlinien	110

4.1.2	Richtlinien im Kontext	114
4.1.3	Aufgabe: Prozessbeschreibung Erstellung und Pflege von Richtlinien	115
4.1.4	Der Richtlinienbaukasten	117
4.1.5	Regeln und die Klassifizierung	119
4.2	Richtlinien umsetzen	121
4.2.1	Umsetzung von Regeln	121
4.2.2	Von der Richtlinie zur Guideline	123
4.2.3	Anspruch und Wirklichkeit	125
4.2.4	Eine fiktive IT-Umgebung	127
4.2.5	Hilfestellungen durch genormte Vorgehensweisen	131
4.3	Die Richtlinien/Aufgaben des Projekts	142
4.3.1	Aufgabe: Checklisten IT-Sicherheitsrichtlinien und IT-Sicherheitsprozesse	142
4.3.2	Aufgabe: Kommunikation von IT-Sicherheitsthemen	144
4.4	Die sechs Grundsatzthemen	145
4.4.1	Aufgabe: Standardisierung von IT-Systemen und Software	146
4.4.2	Aufgabe: Schutz vor Schadsoftware (Antivirus)	148
4.4.3	Aufgabe: Patchmanagement	151
4.4.4	Zugang zum Unternehmensnetzwerk	153
4.4.5	Aufgabe: Dateiberechtigungen auf Servern analysieren	156
4.4.6	Aufgabe: Grundregeln Benutzerverzeichnisse	160
4.5	Themengebiet IT-Sicherheitsprozesse	162
4.5.1	Aufgabe: IT-Sicherheitsorganisation	163
4.5.2	Aufgabe: Verwaltung der Unternehmenswerte (assets)	168
4.5.3	Aufgabe: Prozess IT-Sicherheitsvorfälle melden	169
4.5.4	Aufgabe: Prozess Schwachstellenanalyse	173
4.5.5	Aufgabe: Prozess Notfallmanagement	175
4.5.6	Aufgabe: Prozess Überwachung von (Sicherheits-) Protokollen (logfiles)	177
4.5.7	Aufgabe: Microsoft-Windows-Ereignisse überwachen	180
4.5.8	Aufgabe: Dateizugriffe auf Servern überwachen	182

4.5.9	Aufgabe: Prozess Änderungsmanagement (change management)	184
4.5.10	Aufgabe: Prozess Backup und Wiederherstellung	185
4.6	Themengebiet Benutzer	186
4.6.1	Aufgabe: Benutzerverwaltung	186
4.6.2	Aufgabe: Generelle Richtlinien für Benutzer	188
4.6.3	Aufgabe: Richtlinien für Administratoren	191
4.6.4	Aufgabe: Umgang mit Gerätschaften	192
4.6.5	Aufgabe: Awareness-Maßnahmen	193
4.7	Themengebiet Zugriff auf Daten	194
4.7.1	Aufgabe: Rollenkonzept erstellen	194
4.7.2	Aufgabe: Temporärer administrativer Zugriff	197
4.7.3	Aufgabe: Regeln zur Vergabe von Berechtigungen	198
4.8	Themengebiet Sichere Systeme	200
4.8.1	Aufgabe: PCs und Laptops sicher konfigurieren	200
4.8.2	Aufgabe: Sicherer Administrations-PC	203
4.8.3	Aufgabe: Sichere Serversysteme	205
4.9	Themengebiet Physische Sicherheit	206
4.9.1	Aufgabe: Zutritt zum Unternehmen	207
4.9.2	Aufgabe: Kritische Bereiche absichern	208
4.10	Themengebiet Netzwerk	212
4.10.1	Aufgabe: Datenübertragung und Verschlüsselung	213
4.10.2	Aufgabe: Verbindungen zu anderen Unternehmen	215
4.10.3	Aufgabe: Trennung von Netzwerken	216
4.10.4	Aufgabe: Regeln zum Zugang zum internen Netzwerk	217
4.11	Aufgabe: Skript- und Softwareentwicklung	219
5	Audits durchführen	223
5.1	Das Audit und seine Komponenten	223
5.1.1	Die Grundzüge	223
5.1.2	Der Auditor	226
5.1.3	Der Interview-Partner	227

5.1.4	Art des Audits	228
5.1.5	Audit-Planung, Geltungsbereich, Abstimmung mit den Fachbereichen	229
5.1.6	Fragenkatalog, Sammeln von Nachweisen	230
5.1.7	Der Audit-Bericht	230
5.1.8	Das Aufsichtsgremium	231
5.1.9	Lessons learned – Verbesserung des Audit-Prozesses	233
5.2	Der Fragenkatalog und das Sammeln von Nachweisen	233
5.2.1	Aufbau eines Fragenkatalogs	233
5.2.2	Auswahl der Fragen und deren Bewertung	237
5.2.3	Erbringung von Nachweisen	239
5.2.4	Auswertung der Antworten	240
5.2.5	Übergabe der Abweichungen zur Abarbeitung	241
5.3	Quellen für die Überprüfung von Regeln	242
5.3.1	Dokumentation und das Asset-Management	243
5.3.2	Auswertung von Protokolldateien	243
5.3.3	Aktive Penetrationstests	244
5.3.4	Ergebnisse aus dem CERT	245
	Index	247