
Inhaltsverzeichnis

1	Einleitung	1
1.1	Für wen dieses Buch interessant ist	2
1.2	Warum dieses Buch entstand	2
1.3	Was dieses Buch leistet	3
1.4	Was dieses Buch nicht bietet	5
1.5	Wie dieses Buch gelesen werden sollte	5
1.6	Konventionen im Buch	6
1.7	Randgedanken	6

Teil I Einführung in das Thema „IT-Sicherheit“

2	Was ist „IT-Sicherheit“?	11
2.1	Versuch einer Herleitung	12
2.2	Sicherheitsgrundbedürfnisse	19
2.3	Begriffsdefinition	22
3	IT-Sicherheit im Kontext	25
3.1	Der allgemeine Kontext	25
3.2	Schutzbedarf	26
3.3	Schutzziele	28
3.4	Schutzmaßnahmen	32
4	Ideen für eine Laborumgebung	43
4.1	Logische Struktur	44
5	Bedrohungen	49
5.1	Motivation der Angreifer	49
5.2	Das Ebenenmodell der Bedrohungsarten	55
5.3	Technische Bedrohungskategorien	60

5.4	Social Engineering	81
5.5	Zusammenfassung	82

Teil II Methodische Grundlagen zur Modellierung und Umsetzung von IT-Sicherheit

6	Anforderungsableitung und -definition	89
6.1	Einleitung	89
6.2	Exkurs: Bundesdatenschutzgesetz (BDSG)	89
6.3	Ausgangssituation	91
6.4	Analyse von Organisation- und IT-Struktur	93
6.5	Anregungen	95
7	Sicherheitsanalyse	97
7.1	Einleitung	97
7.2	Zielsetzung	97
7.3	Vorgehensweise	98
7.4	Ist-Erhebung	98
7.5	Schutzbedarfserhebung	99
7.6	Ableitung Soll-Modell	100
7.7	Ergebnisumfang	104
8	Anwendung der Sicherheitsanalyse	107
8.1	Einführung	107
8.2	Vorgehen	107
8.3	Bedrohungs- und Gefahrenpotentialanalyse	107
8.4	Sicherheitscheck	109
8.5	Ableitung Handlungsbedarf	109
9	Überprüfung und Bewertung von IT-Sicherheit	111
9.1	Vorbemerkungen	111
9.2	Prüfung ist notwendig, Evaluierung nutzbringender!	111
9.3	Assessments	113
9.4	Audits	114
9.5	Möglichkeiten einer Tool-Unterstützung	115
10	IT-Sicherheitskonzept	117
10.1	Überblick	117
10.2	Exkurs: Erstrealisierung von IT-Sicherheit	128
11	Standards zur IT-Sicherheit und Regulatory Compliance ..	129
11.1	Was hat IT-Sicherheit mit Regulatory Compliance zu tun? ...	129
11.2	Regulatory Compliance	130

11.3 Standards zur IT-Sicherheit	139
11.4 Weitere Technologie- und Methodenstandards mit Bezug zur IT-Sicherheit	144

Teil III Etablierung einer Grundabsicherung

12 Methodische Vorgehensweise zur Umsetzung technischer Maßnahmen	153
12.1 Konzeption und PoC	155
12.2 Implementierung und Ausbringung	160
12.3 Betrieb	160
13 Grundlagen zur Härtung von Systemen	163
13.1 Zielsetzung	165
13.2 Betriebskonzeption	165
13.3 Konzeptionelle Härtung des Betriebssystems	167
13.4 Konzeptionelle Härtung systemnaher Dienste	195
13.5 Virtualisierung	198
14 Grundlagen zur Absicherung von Netzen	203
14.1 Netzwerkgrundlagen	206
14.2 Ethernet	210
14.3 TCP/IP	216
14.4 Übergreifende Absicherung von Netzen und Datenverkehr ...	217
15 Querschnittsbetrachtungen zur Absicherung des Betriebs ..	229
15.1 Best Practices	229
15.2 Systems Management	234
15.3 Dokumentation	239
15.4 Information Flow Control	245
15.5 „Externe“	247
15.6 Worst Practices	251

Teil IV Absicherung von Peripheriediensten

16 Überblick und Szenarien	257
16.1 Überblick	257
16.2 Szenarien	258
17 Datensicherung	259
17.1 Allgemeine Anforderungen und Lösungen	259
17.2 Anforderungen an Datensicherungsimplementierungen	262

18	Verzeichnisdienste	267
18.1	Historie und Einsatzfelder	267
18.2	Architekturempfehlungen hinsichtlich Betriebsführung	273
19	RDBMS	275
19.1	Betriebssysteme und Datenbanken	276
19.2	Kommunikation mit Datenbanken über Schnittstellen	277
19.3	Datenhaltung und Zugriff	277
19.4	Kryptologie im RDBMS-Umfeld	278
20	Interpretersprachen zur Web-Ausgabe	279
20.1	Mögliche Schwachstellen	280
20.2	Übergreifende Lösungsansätze	285
21	Web Application Server	295
21.1	Einleitung	295
21.2	Plattform	295
21.3	Technische Aspekte zur Absicherung	297
21.4	Betriebliche Aspekte zur Absicherung	298
22	Exkurs: Technische Sicherheit von Web-Inhalten	301
22.1	Aktive Inhalte	302
22.2	Dynamische Inhalte	307

Teil V Spezielle Sicherheitsdienste

23	Betrachtung spezieller Sicherheitsdienster	311
24	Proxy-Dienste	313
24.1	Grundfunktionalität	313
25	Content-Filter	315
25.1	Funktionsweise	315
26	Eindringlingserkennung	317
26.1	Arten von IDS	317
26.2	Funktionsweisen	319

Teil VI Abschluss

27 Reflexion und Ausblick	323
--	------------

Teil VII Anhänge

Literaturverzeichnis	327
Sachverzeichnis	329

Security@Work

Pragmatische Konzeption und Implementierung von
IT-Sicherheit mit Lösungsbeispielen auf
Open-Source-Basis

Eschweiler, J.; Atencio Psille, D.E.

2006, XIV, 334 S., Hardcover

ISBN: 978-3-540-22028-2