

Inhalt

Vorwort	XIII
----------------------	-------------

1 IT-Sicherheit konsequent und effizient umsetzen	1
--	----------

Norbert Pohlmann

1.1	Einleitung	1
1.1.1	Chancen durch die Digitalisierung	1
1.1.2	Risiken durch die Digitalisierung	2
1.1.3	IT-Sicherheitsbedürfnisse als Grundwerte der IT-Sicherheit	3
1.2	Beispiele von aktuellen Angriffsvektoren	4
1.3	IT-Sicherheitsstrategien	7
1.3.1	Vermeiden von Angriffen	8
1.3.2	Entgegenwirken von Angriffen	9
1.3.3	Erkennen von Angriffen	10
1.3.4	Reaktion auf Angriffe	11
1.4	Umsetzung eines angemessenen IT-Sicherheitslevels	12
1.5	IT-Sicherheitsmechanismen, die gegen Angriffe wirken	13
1.6	Die wichtigsten Punkte in Kürze	21
1.7	Literatur	22

2 Grundprinzipien zur Gewährleistung der IT-Sicherheit	23
---	-----------

Hagen Lauer, Nicolai Kuntze

2.1	Einleitung	23
2.1.1	Trends	23
2.1.2	Herausforderungen	24
2.1.3	IT-Sicherheit vs. Sicherheit	25
2.1.4	Schutzziele	26
2.2	Grundprinzipien der IT-Sicherheit	31
2.2.1	Kenne die Bedrohungen	32
2.2.2	Sicherheit und Wirtschaftlichkeit	33
2.2.3	Keine „Security through Obscurity“	34
2.2.4	Security by Design	34
2.2.5	Prinzip der geringsten Berechtigung	35
2.2.6	Trennung der Verantwortlichkeiten	36
2.2.7	Zugriffskontrolle	36

2.2.8	Defense in Depth	37
2.2.9	Der Mensch als Faktor	38
2.2.10	Design for Resilience.	39
2.3	Literatur	41

3 Organisation des IT-Sicherheitsmanagements im Unternehmen . . 43

Markus Nauroth

3.1	Einführende Bemerkungen.	44
3.2	Imperative des IT-Sicherheitsmanagements.	45
3.2.1	Sicherheit ist aktiv und proaktiv	45
3.2.2	Routine	45
3.2.3	Sicherheit liegt in der Verantwortung eines jeden	45
3.2.4	Worst-Case-Szenario	46
3.2.5	Es bedarf vieler Unterstützer.	46
3.2.6	Denken wie ein Angreifer.	46
3.2.7	Mehrschichtige Verteidigung verwenden.	46
3.3	Grundlegende Pfeiler einer IT-Sicherheitsorganisation.	47
3.3.1	Gängige Organisationsstrukturen nach organisatorischem Reifegrad	48
3.3.2	Das Information Technology Risk Council (ITRC)	52
3.4	Die Rolle des CISO: Wie man eine Führungsrolle im Sicherheitsbereich gestaltet	54
3.4.1	Die richtige CISO-Rolle für Ihr Unternehmen entwerfen	54
3.5	Finale Anmerkungen.	59

4 Rechtliche Rahmenbedingungen der IT-Sicherheit 61

Thomas Jansen

4.1	Einleitung.	61
4.2	Vertrags- und haftungsrechtliche Risiken.	62
4.2.1	Allgemeine Sorgfaltspflichten	62
4.2.2	Pflichten zur Gewährleistung der IT-Sicherheit.	63
4.2.3	Haftung für Verstöße gegen IT-sicherheitsrechtliche Anforderungen	64
4.2.4	Anforderungen der DSGVO an technische und organisatorische Schutzmaßnahmen zum Schutz der IT-Sicherheit.	65
4.2.5	Anforderungen des TKG und des TTDSG an technische und organisatorische Schutzmaßnahmen zum Schutz der IT-Sicherheit	66
4.2.6	Empfehlungen des BSI in Bezug auf technisch-organisatorische Maßnahmen.	67
4.3	Straf- und ordnungswidrigkeitsrechtliche Folgen bei der Verletzung der IT-Sicherheit.	68
4.3.1	Strafrechtliche Normen zum Schutz vor Cyberkriminalität	68
4.3.2	Strafrechtliche Verantwortlichkeit der einzelnen Akteure	70
4.4	Das IT-Sicherheitsgesetz (ITSiG 2.0)	71
4.5	Die wichtigsten Punkte in Kürze	73
4.6	Literatur	74

5	Standards und Zertifizierungen	77
	<i>Thomas Lohre</i>	
5.1	Einleitung	77
5.2	Standards	79
	5.2.1 Synergien zwischen Standards auflösen und nutzen	87
	5.2.2 Zertifizierung/Testierung	89
5.3	Kompetenznachweise für Beteiligte der Informationssicherheit	92
5.4	Die wichtigsten Punkte in Kürze	96
5.5	Literatur	96
6	Datenschutz und Informationssicherheit: ungleiche Zwillinge ...	99
	<i>Stefan Karg</i>	
6.1	Einleitung	99
6.2	Rechtlicher Rahmen	101
6.3	Strategische/präventive Aspekte	103
	6.3.1 Risikomanagement	103
	6.3.2 Regelmäßige Überprüfung der Maßnahmen	104
	6.3.3 Entwicklungsprozess	105
6.4	Operative Aspekte: technische und organisatorische Maßnahmen	107
	6.4.1 Schutz der Vertraulichkeit	107
	6.4.2 Schutz der Integrität	110
	6.4.3 Schutz der Verfügbarkeit und Belastbarkeit	111
	6.4.4 Vorfallsbehandlung (Incident Management)	111
6.5	Organisationsaspekte	113
6.6	Fazit	114
6.7	Literatur	114
7	Sicherheit durch Bedrohungs- und Risikoanalysen stärken.....	115
	<i>Daniel Angermeier</i>	
7.1	Einleitung	115
7.2	Nutzen und Mehrwert von Bedrohungs- und Risikoanalysen	116
7.3	Ablauf von Bedrohungs- und Risikoanalysen	118
7.4	Einbindung in Unternehmensprozesse	120
	7.4.1 Anforderungsanalyse und Konzeptphase	120
	7.4.2 Tests planen und priorisieren, Testergebnisse bewerten	124
	7.4.3 Schwachstellen bewerten und behandeln	125
	7.4.4 Laufende Systeme bewerten	126
7.5	Auswahlkriterien für geeignete Methoden	126
7.6	Die wichtigsten Punkte in Kürze	127
7.7	Literatur	127

8 Mittels Reifegradanalysen den IT-Security-Level nachhaltig und belastbar steigern 129

Martin Braun

8.1	Einleitung	129
8.2	Aufgabe und Wirkung einer Reifegradanalyse.....	130
8.2.1	Aufgabe der Reifegradanalyse	130
8.2.2	Die Reifegradanalyse hat unterschiedliche Aufgaben	130
8.2.3	Reifegradanalyse auch als Messinstrument der Belastbarkeit der Kernprozesse	131
8.2.4	Wirkung der Reifegradanalyse	132
8.3	Den Reifegrad des IT-Security-Prozesses ermitteln	134
8.3.1	Definition des IT-Security-Reifegrad-Levels 0: Initial	135
8.3.2	Definition des IT-Security-Reifegrad Level 1: wiederholbar	136
8.3.3	Definition des IT-Security-Reifegrad-Levels 2: definiert	137
8.3.4	Definition des IT-Security-Reifegrad-Levels 3: gemanagt	138
8.3.5	Definition des IT-Security-Reifegrad-Levels 4: optimiert	139
8.4	Durch eine kontinuierliche Reifegradmessung das IT-Risiko minimieren	140
8.4.1	Gesamtheitliche Betrachtung der Perspektiven	141
8.4.2	Perspektive Business	142
8.4.3	Perspektive Organisation und IT	144
8.5	Fazit	146

9 Der Chief Information Security Officer in der Praxis 147

Andreas Reisch

9.1	Einleitung	147
9.2	Business und IT, woher – wohin – mit wem?	148
9.3	Wozu gibt es nun den CISO?	149
9.4	Die persönliche Verantwortung des CISO	150
9.5	Verantwortung des Unternehmens	152
9.6	Das ISMS	153
9.7	Culture, Communication & Awareness	154
9.8	Assessments	156
9.9	Approvals und Information Security Consulting	157
9.10	Information Security Consulting	159
9.11	Lohnt sich das SOC?	160
9.12	IS-Operations	161
9.13	Fazit	162

10	Irgendwas ist immer – Informationssicherheit aus Sicht des CISO der Allianz Technology	163
	<i>Fabian Topp</i>	
10.1	Einleitung	163
10.2	Vernetzung – hilf mir, es selbst zu tun	165
10.3	Personal – die schlechten sind die teuersten Mitarbeiter	167
10.4	No Risk (no Privacy, no Audit, ...), no Fun.	171
	10.4.1 Organisation ist ein Mittel, die Kräfte des Einzelnen zu vervielfältigen. .	172
	10.4.2 Mehr als die Summe seiner Teile.	174
10.5	Ende gut, alles gut?	175
11	Entwicklung sicherer Software	177
	<i>Nicolai Kuntze, Hagen Lauer</i>	
11.1	Einleitung	177
11.2	Vorgehensmodelle der Softwareentwicklung	179
11.3	Secure Development Lifecycles	181
11.4	Requirements Engineering.	182
11.5	Architektur und Entwurf.	183
11.6	Implementierung.	184
11.7	Coding-Standards.	184
11.8	Wahl der Programmiersprache.	186
11.9	Tests	188
11.10	Code Reviews	188
11.11	Static Code Analysis	189
11.12	Formale Analyse	189
11.13	Validierung.	190
11.14	Maintenance.	190
11.15	Die wichtigsten Punkte in Kürze	192
11.16	Literatur	192
12	Cybersicherheit in Produktion, Automotive und intelligenten Gebäuden	193
	<i>Marko Schuba, Hans Höfken</i>	
12.1	Einleitung	193
	12.1.1 Automatisierungstechnik	194
	12.1.2 Spezifische Anforderungen der Automatisierungstechnik.	196
	12.1.3 Spezifische Eigenschaften der Automatisierungstechnik.	197
12.2	Schöne neue Welt – das Internet der Dinge	199
	12.2.1 Internet der Dinge (IoT)	200
	12.2.2 IoT-Chancen für die Automatisierungstechnik.	200
	12.2.3 IoT-Risiken für die Automatisierungstechnik.	201

12.3	Was läuft schief?	201
12.3.1	Zu viel Vertrauen in andere	201
12.3.2	Zu wenig Management-Fokus	202
12.3.3	Sicherheits-Features zu teuer oder nicht genutzt	202
12.3.4	Es ist noch nie etwas passiert – und das bleibt auch so	203
12.3.5	Never change a running system.	203
12.3.6	Sensibilisierung und Weiterbildung zu teuer/aufwendig	204
12.4	Was ist zu tun?	205
12.4.1	Cybersicherheit allgemein	205
12.4.2	Cybersicherheit in der Automatisierung	205
12.5	Praxisbeispiel: Einführung von Cybersicherheit in der Produktion (Orientierung an ISA/IEC 62443)	209
12.5.1	Audit	209
12.5.2	Festlegen eines Sicherheitslevels	210
12.5.3	Risikobeurteilung	210
12.5.4	Defense in Depth	211
12.5.5	Zonierung	212
12.5.6	Patchmanagement	213
12.5.7	Dienstleister	215
12.6	Zusammenfassung und Fazit	216
12.7	Literatur	216
13	Edge Computing: Chancen und Sicherheitsrisiken	219
	<i>Marcel Winandy</i>	
13.1	Einleitung	219
13.2	Was ist Edge Computing?	221
13.2.1	Das Internet der Dinge	221
13.2.2	Von der Cloud zur Edge	222
13.2.3	Impulsgeber für IoT Edge Computing	224
13.3	Chancen und Sicherheitsrisiken	225
13.3.1	Eröffnung neuer Möglichkeiten durch IoT Edge Computing	225
13.3.2	IoT Edge Computing bringt auch neue Sicherheitsrisiken	227
13.4	Entwicklung sicherer Edge-Computing-Plattformen	230
13.4.1	Security-by-Design-Prinzipien	230
13.4.2	Privacy-by-Design-Prinzipien	232
13.4.3	Spezielle Entwicklungsprinzipien für Edge Computing	233
13.5	Technologien für sichere Edge-Computing-Plattformen	234
13.5.1	Sicherheitskerne	235
13.5.2	Trusted Execution Environments	237
13.5.3	Kryptoagilität	237
13.6	Die wichtigsten Punkte in Kürze	238
13.7	Literatur	239

14 IT-Sicherheit in Vergabeverfahren 241

Jutta Pertenais

14.1	Einleitung	241
14.2	Vergabeverfahren in Deutschland	242
14.2.1	Grundsätze und Aspekte	243
14.2.2	Verfahrensarten	246
14.2.3	Elektronische Vergabeplattformen	249
14.3	IT-Sicherheit im Vergabeverfahren	249
14.3.1	TOM im Vergabeverfahren	249
14.3.2	Die Gestaltung der Vergabeunterlagen	251
14.3.3	Die Planung des Vergabeverfahrens	252
14.3.4	Die Verfahrensdurchführung	254
14.3.5	Die elektronische Kommunikation	254
14.3.6	Der Umgang mit Verschlusssachen	255
14.4	Kennzeichnen von Geschäftsgeheimnissen	256
14.5	Rechtsschutzmöglichkeiten	258
14.6	Strafbarkeit im Vergabeverfahren	259
14.7	Bietertipps zum Umgang mit Vergabestellen und zur Erstellung von Angeboten	260
14.8	Die wichtigsten Punkte in Kürze	260
14.9	Literatur	261

15 Sicherheit in der Cloud 263

Christoph Skornia

15.1	Einleitung	263
15.2	Nutzungsmodelle	264
15.2.1	Servicemodelle	264
15.2.2	Bereitstellungsmodelle	265
15.3	Risiken des Cloud Computing	266
15.3.1	Überblick	266
15.3.2	Beispiele	268
15.4	Sicherheitsmaßnahmen	269
15.4.1	Sicherheitsrahmen	269
15.4.2	Zugangskontrolle	271
15.4.3	Datensicherheit	272
15.4.4	Monitoring und Überwachung	274
15.5	Zusammenfassung	276
15.6	Die wichtigsten Punkte in Kürze	277
15.7	Literatur	277

Herausgeber, Autorin und Autoren 279

Stichwortverzeichnis 285