edv-buchversand.de

IT-Sicherheit

Technologien und Best Practices für die Umsetzung im Unternehmen

» Hier geht's direkt zum Buch

DAS INHALTS-VERZEICHNIS

Dieses Inhaltsverzeichnis wird Ihnen von www.edv-buchversand.de zur Verfügung gestellt.

Inhalt

Vorwort ..... **XV**

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 3
1.1.3 IT-Sicherheitsbedürfnisse als Grundwerte der IT-Sicherheit 3
1.2 Beispiele von aktuellen Angriffsvektoren 4
1.3 IT-Sicherheitsstrategien 8
1.3.1 Vermeiden von Angriffen 9
1.3.2 Entgegenwirken von Angriffen 11
1.3.3 Erkennen von Angriffen 13
1.3.4 Reaktion auf Angriffe 13
1.4 Umsetzung eines angemessenen IT-Sicherheitslevels 14
1.5 IT-Sicherheitsmechanismen, die gegen Angriffe wirken 16
1.6 Die wichtigsten Punkte in Kürze 25

2 Grundprinzipien zur Gewährleistung der IT-Sicherheit **27**
Hagen Lauer, Nicolai Kuntze

2.1 Einleitung 27
2.1.1 Trends 27
2.1.2 Herausforderungen 28
2.1.3 IT-Sicherheit vs. Sicherheit 30
2.1.4 Schutzziele 31

2.2 Grundprinzipien der IT-Sicherheit 37
2.2.1 Kenne die Bedrohungen 37
2.2.2 Sicherheit und Wirtschaftlichkeit 39
2.2.3 Keine „Security through Obscurity“ 40
2.2.4 Security by Design 40
2.2.5 Prinzip der geringsten Berechtigung 42
2.2.6 Trennung der Verantwortlichkeiten 42
2.2.7 Zugriffskontrolle 43
2.2.8 Defense in Depth 44
2.2.9 Der Mensch als Faktor 45
2.2.10 Design for Resilience 46

3 Organisation des IT-Sicherheitsmanagements im Unternehmen 49
Markus Nauroth

3.1 Einführende Bemerkungen 50
3.2 Imperative des IT-Sicherheitsmanagements 51
3.2.1 Sicherheit ist aktiv und proaktiv 51
3.2.2 Routine 51
3.2.3 Sicherheit liegt in der Verantwortung eines jeden 51
3.2.4 Worst-Case-Szenario 52
3.2.5 Es bedarf vieler Unterstützer 52
3.2.6 Denken wie ein Angreifer 52
3.2.7 Mehrschichtige Verteidigung verwenden 52
3.3 Grundlegende Pfeiler einer IT-Sicherheitsorganisation 53
3.3.1 Gängige Organisationsstrukturen nach organisatorischem Reifegrad 54
3.3.1.1 Neugründung 54
3.3.1.2 Kleine und mittlere Unternehmen (KMU) 55
3.3.1.3 Großunternehmen 57
3.3.2 Das Information Technology Risk Council (ITRC) 58
3.3.2.1 ITRC-Vertreter 59
3.3.2.2 ITRC-Rollen und Zuständigkeiten 59
3.4 Die Rolle des CISO: Wie man eine Führungsrolle im Sicherheitsbereich gestaltet 61
3.4.1 Die richtige CISO-Rolle für Ihr Unternehmen entwerfen 61
3.4.1.1 Identifizieren der dringlichsten sicherheitsrelevanten Herausforderungen 62

3.4.1.2 Priorisierung der CISO-Rolle und -Verantwortlichkeiten ... 62
3.4.1.3 CISO-RACI-Diagramm ... 64
3.4.1.4 Häufig vertretene CISO-Profile ... 64
3.5 Finale Anmerkungen ... 67

4 Rechtliche Rahmenbedingungen der IT-Sicherheit ... 69
Thomas Jansen
4.1 Einleitung ... 69
4.2 Vertrags- und haftungsrechtliche Risiken ... 70
4.2.1 Allgemeine Sorgfaltspflichten ... 70
4.2.2 Pflichten zur Gewährleistung der IT-Sicherheit ... 72
4.2.3 Haftung für Verstöße gegen IT-sicherheitsrechtliche Anforderungen 72
4.2.4 Anforderungen der DSGVO an technische und organisatorische Schutzmaßnahmen zum Schutz der IT-Sicherheit ... 74
4.2.5 Anforderungen des TKG und des TTDSG an technische und organisatorische Schutzmaßnahmen zum Schutz der IT-Sicherheit 75
4.2.6 Empfehlungen des BSI in Bezug auf technisch-organisatorische Maßnahmen ... 76
4.3 Straf- und ordnungswidrigkeitsrechtliche Folgen bei der Verletzung der IT-Sicherheit ... 77
4.3.1 Strafrechtliche Normen zum Schutz vor Cyberkriminalität ... 77
4.3.2 Strafrechtliche Verantwortlichkeit der einzelnen Akteure ... 79
4.4 Das IT-Sicherheitsgesetz (ITSiG 2.0) ... 80
4.5 Das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) 83
4.6 Der Cyber Resilience Act ... 85
4.7 Der AI-Act ... 86
4.8 Die wichtigsten Punkte in Kürze ... 87

5 Standards und Zertifizierungen ... 91
Thomas Lohre
5.1 Einleitung ... 91
5.2 Standards ... 94
5.2.1 Synergien zwischen Standards auflösen und nutzen ... 103
5.2.2 Zertifizierung/Testierung ... 105
5.3 Kompetenznachweise für Beteiligte der Informationssicherheit ... 109
5.4 Die wichtigsten Punkte in Kürze ... 113

6 Datenschutz und Informationssicherheit: ungleiche Zwillinge 115
Stefan Karg
6.1 Einleitung . . . 115
6.2 Rahmenbedingungen . . . 117
6.2.1 Datenschutz . . . 118
6.2.2 Managementsysteme . . . 120
6.2.3 Das Standard-Datenschutzmodell (SDM) . . . 120
6.3 Strategische/präventive Aspekte . . . 122
6.3.1 Risikomanagement . . . 122
6.3.2 Regelmäßige Überprüfung der Maßnahmen . . . 123
6.3.3 Entwicklungsprozess . . . 124
6.4 Operative Aspekte: technische und organisatorische Maßnahmen . . . 126
6.4.1 Schutz der Vertraulichkeit . . . 128
6.4.2 Schutz der Integrität . . . 130
6.4.3 Schutz der Verfügbarkeit und Belastbarkeit . . . 131
6.4.4 Vorfallsbehandlung (Incident Management) . . . 131
6.5 Organisationsaspekte . . . 133
6.6 Fazit . . . 134

7 IT-Sicherheit durch Bedrohungs- und Risikoanalysen stärken 137
Daniel Angermeier
7.1 Einleitung . . . 137
7.2 Nutzen und Mehrwert von Bedrohungs- und Risikoanalysen . . . 138
7.3 Ablauf von Bedrohungs- und Risikoanalysen . . . 140
7.4 Einbindung in Unternehmensprozesse . . . 142
7.4.1 Anforderungsanalyse und Konzeptphase . . . 142
7.4.2 Tests planen und priorisieren, Testergebnisse bewerten . . . 148
7.4.3 Schwachstellen bewerten und behandeln . . . 148
7.4.4 Laufende Systeme bewerten . . . 149
7.5 Auswahlkriterien für geeignete Methoden . . . 150
7.6 Die wichtigsten Punkte in Kürze . . . 151

8 Sicherheitstesten . . . 153
Jürgen Großmann
8.1 Sicherheitstesten – ein Grundverständnis . . . 154
8.1.1 Testen als Analysemethode . . . 154

8.1.2 Spezifische Herausforderungen beim Sicherheitstesten 156
8.1.3 Testobjekte beim Sicherheitstesten 157
8.1.4 Grundlagen und Ziele des Sicherheitstestens 159
8.1.5 Definition von Sicherheitstestzielen 160
8.2 Testmethoden und Testtechniken 161
8.2.1 Audits und Reviews 161
8.2.2 Statische Analyse 162
8.2.3 Der funktionale Sicherheitstest 163
8.2.4 Fuzz-Testing 164
8.2.5 Last- und Performanztesten 166
8.2.6 Schwachstellen-Scanning 166
8.2.7 Monitoring und passives Testen 167
8.2.8 Risikobasiertes Sicherheitstesten 168
8.2.9 Penetrationstesten 169
8.3 Prozessuale Einbettung des Sicherheitstestens 170
8.3.1 Der Sicherheitstestprozess 171
8.3.2 Sicherheitstesten im SDLC 172
8.3.3 Sicherheitstesten in agiler Entwicklung und DevOps 174
8.4 Chancen und Herausforderungen durch KI 176
8.4.1 KI-gestützte Automatisierung beim Sicherheitstest 176
8.4.2 Sicherheitstesten von KI 178
8.5 Zusammenfassung 179

9 Der Faktor Mensch 183
Kristin Weber

9.1 Der Mensch als Lösung 184
9.2 Der Mensch als Bedrohung 186
9.2.1 Sicheres und unsicheres Verhalten 187
9.2.2 Gründe für unsicheres Verhalten 189
9.3 Der Mensch als Opfer 192
9.3.1 Social Engineering 192
9.3.2 Instrumente im Social Engineering 193
9.3.3 Psychologische Tricks 196
9.4 Menschen sensibilisieren 200
9.4.1 Information Security Awareness 200

9.4.2 Psychologische Grundlagen von Awareness ... 203
9.4.3 Individualisierung ... 205
9.5 Awareness fördern ... 207
9.5.1 Wissen erhöhen und Fähigkeiten fördern ... 208
9.5.2 Verhaltensabsicht fördern und beeinflussen ... 211
9.5.3 Salienz fördern ... 218
9.5.4 Gewohnheiten fördern ... 220
9.6 Ausblick ... 223
9.7 Die wichtigsten Punkte in Kürze ... 225

10 IT-Sicherheit – Aus dem Blickwinkel eines CISO ... 229
Ümit Kuşdoğan
10.1 Einleitung ... 229
10.1.1 Das Wichtigste beim Start mit IT-Sicherheit ... 230
10.1.2 Strategien, Methoden und Tools ... 232
10.2 Organisatorische Verankerung ... 241
10.2.1 Rollen in der IT-Sicherheit ... 244
10.2.2 Kompetenzen in der IT-Sicherheit ... 245
10.3 Entscheidende Änderungen bei IT-Sicherheit ... 247
10.4 Besondere IT-Sicherheitsherausforderungen ... 248
10.5 Erfolge erzielen – Fehler vermeiden ... 248
10.5.1 Erfolgsfaktoren ... 249
10.5.2 Fehler, die zu vermeiden sind ... 249
10.5.3 Verbesserungspotenziale ... 250
10.5.4 Lessons Learned ... 250
10.5.5 Was könnte man anders machen? ... 251
10.6 Zusammenfassung ... 252
10.6.1 Hot Topics ... 253
10.6.2 Top-3-Ratschläge ... 254

11 Warum IT-Sicherheit zwischen Erfolg und Insolvenz entscheidet ... 257
Florian Jörgens
11.1 Das Wichtigste beim Start mit IT-Sicherheit ... 257
11.2 Organisatorische Verankerung ... 259
11.3 Verbesserungspotenzial ... 260

11.4 Entscheidende Änderungen bei IT-Sicherheit 261
11.5 Besondere IT-Sicherheitsherausforderungen in der eigenen Branche 262
11.6 Rolle des „IT-Sicherheitsverantwortlichen“ 263
11.7 Kompetenzen der IT-Sicherheitsverantwortlichen sowie aller Beschäftigen 264
11.8 Top-3-Ratschläge 265

12 IT-Sicherheit heute und morgen – aus Sicht eines CISO 267
Markus Schmall

12.1 Das Wichtigste beim Start mit IT-Sicherheit. 267
12.2 Aufnahme des IST-Zustands 269
12.2.1 Verständnis der Angriffsvektoren/Angreiferlage 271
12.2.2 Verständnis der Angriffspfade 272
12.3 Typische Fehler 273
12.4 Organisation. 275
12.5 Erfolgsfaktoren 277
12.5.1 Kommunikation 277
12.5.2 Großes technisches Wissen 278
12.5.3 Umfangreiches Wissen über Security bzw. die Angreiferlage 279
12.5.4 Lösungsorientierung 279
12.5.5 Doppelte Absicherung/Avoid Vendor Lock-in 280
12.5.6 Betriebliche Nähe 280
12.6 Verbesserungspotenziale 281
12.7 Entscheidende Änderungen bei IT-Sicherheit 281
12.8 Besondere IT-Sicherheitsherausforderungen in der eigenen Branche 283
12.9 Hot Topics 284
12.10 Rolle des IT-Sicherheitsverantwortlichen 285
12.11 Lessons Learned 286
12.12 Kompetenzen eines erfolgreichen Sicherheitsverantwortlichen 287
12.13 Top-3-Ratschläge 288
12.14 Die wichtigsten Punkte in Kürze 289

13 Entwicklung sicherer Software 291
Nicolai Kuntze, Hagen Lauer

13.1 Einleitung 291
13.2 Vorgehensmodelle der Softwareentwicklung 293
13.3 Secure Development Lifecycles 295

13.4 Requirements Engineering ... 297
13.5 Architektur und Entwurf ... 298
13.6 Implementierung ... 299
13.7 Coding-Standards ... 300
13.8 Wahl der Programmiersprache ... 302
13.9 Tests ... 304
13.10 Code Reviews ... 304
13.11 Static Code Analysis ... 305
13.12 Formale Analyse ... 305
13.13 Validierung ... 306
13.14 Maintenance ... 307
13.15 Die wichtigsten Punkte in Kürze ... 308

14 Cybersicherheit in Produktion, Automotive und intelligenten Gebäuden ... 311
Marko Schuba, Hans Höfken

14.1 Einleitung ... 311
14.1.1 Automatisierungstechnik ... 312
14.1.2 Spezifische Anforderungen der Automatisierungstechnik ... 314
14.1.3 Spezifische Eigenschaften der Automatisierungstechnik ... 316
14.2 Schöne neue Welt – das Internet der Dinge ... 318
14.2.1 Internet der Dinge (IoT) ... 318
14.2.2 IoT-Chancen für die Automatisierungstechnik ... 319
14.2.3 IoT-Risiken für die Automatisierungstechnik ... 320
14.3 Was läuft schief? ... 320
14.3.1 Zu viel Vertrauen in andere ... 321
14.3.2 Zu wenig Management-Fokus ... 321
14.3.3 Sicherheits-Features zu teuer oder nicht genutzt ... 321
14.3.4 Es ist noch nie etwas passiert – und das bleibt auch so ... 322
14.3.5 Never change a running system ... 322
14.3.6 Sensibilisierung und Weiterbildung zu teuer/aufwendig ... 323
14.4 Was ist zu tun? ... 324
14.4.1 Cybersicherheit allgemein< ... 324
14.4.2 Cybersicherheit in der Automatisierung ... 325
14.5 Praxisbeispiel: Einführung von Cybersicherheit in der Produktion (Orientierung an ISA/IEC 62 443) ... 328

14.5.1 Audit ... 329
14.5.2 Festlegen eines Sicherheitslevels ... 330
14.5.3 Risikobeurteilung ... 330
14.5.4 Defense in Depth ... 331
14.5.5 Zonierung ... 332
14.5.6 Patchmanagement ... 333
14.5.7 Dienstleister ... 335
14.6 Zusammenfassung und Fazit ... 336

15 Edge Computing: Chancen und Sicherheitsrisiken ... 339
Marcel Winandy

15.1 Einleitung ... 339
15.2 Was ist Edge Computing? ... 341
15.2.1 Das Internet der Dinge ... 341
15.2.2 Von der Cloud zur Edge ... 342
15.2.3 Impulsgeber für IoT Edge Computing ... 344
15.3 Chancen und Sicherheitsrisiken ... 345
15.3.1 Eröffnung neuer Möglichkeiten durch IoT Edge Computing ... 346
15.3.2 IoT Edge Computing bringt auch neue Sicherheitsrisiken ... 348
15.4 Entwicklung sicherer Edge-Computing-Plattformen ... 351
15.4.1 Security-by-Design-Prinzipien ... 351
15.4.2 Privacy-by-Design-Prinzipien ... 353
15.4.3 Spezielle Entwicklungsprinzipien für Edge Computing ... 354
15.5 Technologien für sichere Edge-Computing-Plattformen ... 356
15.5.1 Sicherheitskerne ... 356
15.5.2 Trusted Execution Environments und Confidential Computing ... 359
15.5.3 Kryptoagilität ... 359
15.6 Die wichtigsten Punkte in Kürze ... 361

16 Cybersicherheit für kritische Infrastrukturen (KRITIS) ... 363
Martin Serror

16.1 Einleitung ... 363
16.1.1 Technische Grundlagen ... 365
16.1.2 Regulierungen und Pflichten ... 366
16.1.3 Bedrohungen durch Cyberangriffe ... 369

16.2 Herausforderungen ... 371
16.2.1 IT/OT-Konvergenz ... 371
16.2.2 „Safety first“ ... 372
16.2.3 Mangelnde physische Sicherheit ... 373
16.2.4 Mangelnde Eigeninitiative ... 374
16.3 Cyberangriffe verstehen ... 375
16.3.1 Fähigkeiten des Angreifers ... 375
16.3.2 Vorgehen und Ablauf ... 377
16.4 Gegenmaßnahmen ... 380
16.4.1 Prävention ... 382
16.4.2 Detektion ... 385
16.4.3 Reaktion ... 387
16.5 Fazit ... 389
16.6 Die wichtigsten Punkte in Kürze ... 390

17 Sicherheit in der Cloud ... 393
Christoph Skornia

17.1 Einleitung ... 393
17.2 Nutzungsmodelle ... 394
17.2.1 Servicemodelle ... 394
17.2.2 Bereitstellungsmodelle ... 396
17.3 Risiken des Cloud-Computing ... 397
17.3.1 Überblick ... 397
17.3.2 Beispiele ... 399
17.4 Sicherheitsmaßnahmen ... 400
17.4.1 Sicherheitsrahmen ... 400
17.4.2 Zugangskontrolle ... 403
17.4.3 Datensicherheit ... 404
17.4.4 Monitoring und Überwachung ... 406
17.5 Zusammenfassung ... 409
17.6 Die wichtigsten Punkte in Kürze ... 409

Herausgeber, Autorin und Autoren ... 411

Index ... 419