Inhaltsverzeichnis

1 Einleitung 1
1.1 Weshalb sollten gerade Sie als Arzt, Apotheker, Laborleiter oder IT-Verantwortlicher dieses Buch lesen? 1
1.2 Bei welchen Entscheidungen hilft Ihnen dieses Buch? 3
1.3 Hinweise für den Leser 4
1.4 Deshalb sollten Sie sich als Arzt mit IT-Sicherheit und Datenschutz auskennen 5
1.5 Konkrete Beispiele von Hackerangriffen im Gesundheitswesen 6
1.6 IT-Sicherheit, Compliance und Datenschutz 7
1.7 Haftungsausschluss/Disclaimer 8
1.8 Aktualität des Buches 8
Literatur 9

2 IT-Sicherheit – Was ist zu tun? 11
2.1 Die zehn wichtigsten IT-Sicherheitsmaßnahmen 11
2.1.1 Physische Absicherung der Informatikserver und -räume 12
2.1.2 Regelmäßige Datensicherung erstellen 12
2.1.3 Passwörter: sichere Wahl und Umgang 14
2.1.4 Computersysteme auf aktuellem Stand halten 16
2.1.5 Verantwortlichkeiten präzise definieren 17
2.1.6 IT-Konzepte und grundlegende IT-Prozesse definieren/Notfallkonzepte 18
2.1.7 Nutzerkreise und Netzwerkbereiche präzise definieren 18
2.1.8 Schulungen und Awareness-Programme durchführen 19
2.1.9 Schwachstellen von Experten prüfen lassen 20
2.1.10 IT-Sicherheitswerkzeuge richtig einsetzen 21
2.2 Die zehn typischen Fehler in einer medizinischen IT – vom Schwesternzimmer bis zum Sekretariat 22
2.2.1 Unprofessioneller Umgang mit Passwörtern 22
2.2.2 Datenwiederherstellung wird nicht geprüft oder getestet bzw. geübt 23

Bibliografische Informationen
http://d-nb.info/118700541X

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

2.2.3 Unachtsames Klicken auf an E-Mail anhängende Links 26
2.2.4 Vorhandene Sicherheitsvorkehrungen werden nicht genutzt oder ignoriert 27
2.2.5 Der Chef oder die Leitung der Verwaltung interessiert sich nicht für IT-Sicherheit 28
2.2.6 Kein Anlagenmanagement 29
2.2.7 Fehlende Schulung und kein Awareness-Programm 30
2.2.8 Veraltete Betriebssysteme und Programme werden verwendet 31
2.2.9 Benutzer kann fremde bzw. eigene Software installieren 32
2.2.10 Man fühlt sich zu sicher 33
Literatur 33

3 IT-Sicherheitstechniken und Schutzziele für die medizinische IT 35
3.1 Allgemeine Informationen und Definitionen 35
3.2 Möglichkeiten zur Erhöhung der IT-Sicherheit 39
3.3 IT-Sicherheit für den Computerarbeitsplatz basierend auf Standardtechnik ... 41
3.3.1 Benutzerauthentisierung 43
3.3.2 Rollentrennung 43
3.3.3 Aktivieren von Autoupdate-Mechanismen 43
3.3.4 Regelmäßige Datensicherung 44
3.3.5 Bildschirmsperre 44
3.3.6 Einsatz von Virenschutzprogrammen 44
3.3.7 Protokollierung 45
3.3.8 Nutzung von TLS 45
3.3.9 Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und -Kameras 46
3.3.10 Abmelden nach Aufgabenerfüllung 46
3.4 CIA-Triade 46
3.4.1 Confidentiality: Vertraulichkeit (Datenschutz) 46
3.4.2 Integrity: Integrität (Datensicherheit) 49
3.4.3 Availability: Verfügbarkeit (Datenzugriff) 50
3.4.4 Zusätzliche Schutzziele und Herausforderungen 51
3.5 Mit einfachen Schritten zu härteren Systemen („Hardening") 53
3.5.1 Schutzmaßnahmen für Windows-PCs 53
3.5.2 Schutzmaßnahmen für Apple OS X 57
3.5.3 Schutzmaßnahmen für Mobile Devices 59
Literatur 61

4 Einfallspforten für IT-Angreifer in der Medizin 63
4.1 Einführung in die „IT-Risiko-Anamnese" 63
4.2 „Feindbild" und Bedrohungen 63
4.3 Hacker-Angriffe 64

4.4 Die Räumlichkeiten und ihre Risikoprofile ... 66
4.4.1 Wartezimmer ... 66
4.4.2 Behandlungszimmer ... 66
4.4.3 Patientenzimmer (im Krankenhaus) ... 66
4.4.4 Empfang, Sekretariat und Verwaltung ... 67
4.4.5 Häuslicher Arbeitsplatz/Home Office/Mobiler Arbeitsplatz ... 67
4.4.6 Gefährdung durch Reinigungs- oder Fremdpersonal ... 70
4.4.7 Parkplätze, Lagerräume etc. ... 70
4.4.8 Räume der IT ... 70
4.5 Standard-IT-Geräte im medizinischen Umfeld ... 70
4.5.1 Standard-PC ... 70
4.5.2 Tablet und Smartphone ... 71
4.5.3 USB-Stick ... 72
4.5.4 USB-Geräte ... 73
4.5.5 Verkabelter Angriff („Sniffer") ... 75
4.5.6 Radio- oder Funkwellen-Angriff ... 75
4.5.7 Manipulierter WLAN-Router ... 76
4.5.8 Intelligente Virtuelle Assistenzsysteme ... 77
4.6 IT-Zugänge ... 78
4.6.1 Kabelgebundene Zugänge ... 78
4.6.2 Drahtlose Zugänge ... 79
4.6.3 Kommunikationsserver ... 80
4.6.4 Remote-Zugang für Service-Zwecke ... 80
4.7 Medizingeräte ... 81
4.8 Systematisches Vorgehen beim Schützen einer IT im Gesundheitswesen ... 82
4.8.1 IT-Grundschutz des BSI ... 82
4.8.2 Besondere Absicherungsmaßnahmen im Gesundheitswesen ... 85
4.8.3 Anforderungen an Hard- und Software ... 85
4.8.4 Wichtige IT-Sicherheitsmaßnahmen ... 87
4.8.5 Bring Your Own Device (BYOD) ... 98
4.8.6 Security Monitoring in größeren IT-Installationen (SIEM, SOC) ... 102
Literatur ... 106

5 Medizintechnik und medizinische Geräte als potenzielle Schwachstelle ... 109
5.1 Klassifizierung medizinischer Geräte (mit Software oder IT) ... 109
5.1.1 Einteilung in Risikoklassen ... 109
5.1.2 Klassische Medizinprodukte – Bildgebende Systeme ... 111
5.1.3 Lebenserhaltende medizinische Systeme und aktive Systeme ... 112
5.2 Einsatzort ... 113
5.2.1 Stationäre medizinische Geräte ... 113
5.2.2 Mobile medizinische Geräte ... 113

5.3 Vernetzung medizinischer Geräte ... 114
5.3.1 Stand-alone-Betrieb ... 115
5.3.2 Lokal vernetzter Betrieb ... 115
5.3.3 Vernetzter Betrieb mit Zugang zum Internet ... 115
5.4 Verwundbarkeit medizinischer Geräte und daraus resultierende Risiken ... 116
5.4.1 Praxisnahe Beispiel-Szenarien der IT-Sicherheit in Medizingeräten ... 116
5.4.2 Hacken von Krankenhaus-Ausrüstungen ... 118
5.4.3 Geeignete risikokompensierende Gegenmaßnahmen ... 121
5.5 Medizingeräte – Worauf Sie achten sollten ... 122
5.5.1 Lebenszyklus medizinischer Geräte ... 122
5.5.2 Evaluierung ... 122
5.5.3 Einkauf ... 123
5.5.4 Inbetriebnahme und Abnahme ... 123
5.5.5 Wartung und Updates ... 124
5.5.6 Periodische Überprüfung durch den TÜV ... 125
5.5.7 Lebensende und sichere Entsorgung ... 125
5.5.8 Awareness bei den Nutzern und eine Checkliste für jeden Tag ... 125
5.6 Awareness „Medizingeräte" ... 126
5.6.1 Awareness-Programm für interne Mitarbeiter ... 126
5.6.2 Awareness-Programm für externe Mitarbeiter, Firmen und Lieferanten ... 127
Literatur ... 127

6 Arztpraxen – kleiner, aber umso gefährdeter ... 129
6.1 IT-Sicherheit in der eigenen Praxis ... 129
6.1.1 Was darf niemals, da (grob) fahrlässig, passieren? ... 130
6.2 E-Health-Gesetz ... 131
6.3 Cyber-Versicherung für Arztpraxen ... 134
6.4 Schützenswerte Bereiche einer Arztpraxis ... 134
6.4.1 Empfang ... 134
6.4.2 Wartezimmer ... 135
6.4.3 Labor ... 136
6.4.4 Behandlungszimmer mit PC ... 136
6.4.5 Server-Raum ... 136
6.4.6 Lagerräume für fachgerechte Deponierung, Archivierung und Entsorgung ... 137
6.5 Schützenswerte Daten einer Arztpraxis ... 137
6.5.1 Personenbezogene Datenobjekte ... 137
6.5.2 Unberechtigtem Datenzugriff durch Dritte ... 138
6.6 Maßnahmen zur Gewährleistung der IT-Sicherheit in der Arztpraxis ... 139
6.6.1 Zutrittskontrolle (P, O) ... 139

6.6.2 Zugangskontrolle (T, O) ... 140
6.6.3 Zugriffskontrolle (T, O) ... 140
6.6.4 Weitergabekontrolle (T) ... 140
6.6.5 Eingabekontrolle (T) ... 141
6.6.6 Auftragskontrolle (O) ... 141
6.6.7 Verfügbarkeitskontrolle (T, O) ... 141
6.6.8 Trennungskontrolle (T, O) ... 141
6.7 Checkliste „Arztpraxis“ ... 142
6.7.1 Datenschutz in der Arztpraxis ... 142
6.7.2 Neueinrichtung einer Praxis ... 143
6.7.3 Praxisübernahme ... 145
6.7.4 Verträge mit IT-Lieferanten ... 146
6.7.5 Praxisverkauf oder Praxisaufgabe ... 147
6.8 Awareness „Arztpraxis“ ... 147
6.8.1 Awareness im Allgemeinen ... 147
6.8.2 Awareness-Programm für Mitarbeiter ... 148
6.8.3 Awareness-Programm für externe Mitarbeiter, Firmen und Lieferanten ... 149
6.8.4 Informationssicherheitsrichtlinie ... 150
Literatur ... 151

7 Wichtige Gesetze und Standards der IT-Sicherheit im Gesundheitswesen ... 153
7.1 Gesetze ... 153
7.1.1 Straftatbestände ... 153
7.1.2 Gesetzeslage ... 156
7.1.3 Europäische Vorgaben in der Datenschutz-Grundverordnung (EU-DSGVO/GDPR) ... 157
7.1.4 HIPAA-Gesetz (USA) ... 164
7.2 Die verschiedenen Standards ... 166
7.2.1 Standard ISO/IEC 27000:2016 ... 166
7.2.2 Standard ISO/IEC 27001:2013 ... 166
7.2.3 Standard ISO/IEC 27002:2013 ... 167
7.2.4 Standard ISO/IEC 27005:2018 ... 167
7.2.5 Standard ISO/IEC 27789:2013 ... 167
7.2.6 Standard ISO/IEC 27799:2016 ... 168
7.2.7 Standard ISO 22600:2015-02 ... 168
7.2.8 Standard ISO 22857:2013 ... 169
7.2.9 Standard IEC EN 80001-1:2010 ... 169
7.2.10 IT-Grundschutz ... 170
7.2.11 NIST-Standards und Leitfaden ... 171
Literatur ... 171

8 Krankenhäuser und Kliniken – groß, anonym und damit ideal für Angreifer 175
8.1 Herausforderung für Krankenhäuser 175
8.2 Schutzbedarfsfeststellung gemäß IT-Grundschutz 176
8.3 Schützenswerte Bereiche eines Krankenhauses 180
8.3.1 Vergleich mit Arztpraxen 180
8.3.2 Operationsräume 180
8.3.3 Chirurgie-Roboter 181
8.3.4 Technikräume 184
8.3.5 Patientenzimmer 185
8.4 Schützenswerte Daten eines Krankenhauses 185
8.4.1 Schutzpflichtige Daten 185
8.4.2 Unberechtigter Datenzugriff durch Dritte 186
8.5 Gewährleistung der IT-Sicherheit in einem Krankenhaus 186
8.6 Awareness „Krankenhaus“ 186
8.6.1 Überblick 186
8.6.2 Organisation der Awareness-Maßnahmen 187
8.6.3 Stufengerechte Sensibilisierungsinhalte 189
8.6.4 Awareness-Programm für alle internen Mitarbeiter 191
8.6.5 Awareness-Programm für externe Mitarbeiter, Firmen und Lieferanten 193
Literatur 194

9 Musterverträge für die DSGVO 197
9.1 Allgemeine und Copyright-Hinweise 197
9.2 Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO 198
9.2.1 Gegenstand und Dauer des Auftrags 199
9.2.2 Konkretisierung des Auftragsinhalts 199
9.2.3 Technisch-organisatorische Maßnahmen 201
9.2.4 Berichtigung, Einschränkung und Löschung von Daten 201
9.2.5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers ... 201
9.2.6 Unterauftragsverhältnisse 203
9.2.7 Kontrollrechte des Auftraggebers 204
9.2.8 Mitteilung bei Verstößen des Auftragnehmers 205
9.2.9 Weisungsbefugnis des Auftraggebers 205
9.2.10 Löschung und Rückgabe von personenbezogenen Daten 206
9.2.11 Fernzugriff oder -wartung 206
9.2.12 Gerichtsstand 208
9.3 Mustervertrag Anlage – Technisch-organisatorische Maßnahmen 208
9.3.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO) 208
9.3.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO) 209
9.3.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO) ... 209

9.3.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO) ... 209
9.4 Beispiel für eine Vertraulichkeitserklärung zur Verpflichtung des eingesetzten Personals ... 209
9.4.1 Verpflichtung auf das Datengeheimnis nach Art. 28 Abs. 3 S. 2 lit. b DSGVO ... 210
9.4.2 Verpflichtung auf das Fernmeldegeheimnis ... 210
9.4.3 Verpflichtung auf Wahrung von Geschäftsgeheimnissen ... 210
Literatur ... 211

10 Nützliches für den täglichen Gebrauch ... 213
10.1 Nützliche Internet-Links ... 213
10.2 Bestimmungen, Checklisten, Praxistipps ... 214
10.2.1 Checkliste „IT-Sicherheit in der Praxis" ... 214
10.2.2 Geräteverlust oder Diebstahl – Was ist zu tun? ... 218
10.2.3 IT-Sicherheitsstrategie und -management ... 219
10.2.4 Gesetzliche Aufbewahrungspflichten ... 220
10.2.5 Checkliste „Medizingeräte" ... 220
10.2.6 Spurensuche: Warum sind die IT-Sicherheitsmaßnahmen nicht umgesetzt? ... 221
10.2.7 Methoden und Maßnahmen ... 222
10.2.8 Notfallkonzept ... 223
10.2.9 Anzeichen für Phishing-Attacken ... 224
10.2.10 Anzeichen dafür, dass Ihr PC gehackt worden ist ... 224
10.2.11 Teilnahme an Konferenzen im Ausland ... 225
10.2.12 Ergebniserwartung an einen Sicherheitscheck durch Spezialisten ... 226
10.2.13 Websites ... 227
10.2.14 Checkliste „Härtungsmaßnahmen" ... 228
10.2.15 Arbeitsvertrag – Datenschutz und IT-Sicherheit ... 230
10.2.16 Neubau einer Arztpraxis ... 231
10.3 Risiko-Kategorisierung ... 232
Literatur ... 232

Glossar: IT-Fachausdrücke ganz einfach erklärt ... 237

Glossar ... 239

Literatur ... 261

Stichwortverzeichnis ... 263