Inhaltsverzeichnis

1 Einleitung 17
1.1 Daten – Informationen – Informationssicherheit 17
1.2 Wegweiser durch das Handbuch 20
1.3 Vorgehen bei der Umsetzung der Informationssicherheit 23
2 Informationssicherheits-Managementsystem (ISMS) 33
2.1 Informationssicherheit in KMUs und der Verwaltung 33
2.2 Was ist Informationssicherheit? 35
2.3 Komponenten eines ISMS 35
2.4 Der Informationssicherheitsprozess 37
2.5 Management-Prinzipien 39
2.6 Umsetzung des ISMS 45
2.7 Erstellung und Umsetzung des Sicherheitskonzepts 47
2.8 Erfolgskontrolle und Verbesserung 49
2.9 Risiko-Analyse / IT-Grundschutz 50
3 Rechtliche Aspekte 61
3.1 Einführung 61
3.2 E-Commerce 62
3.3 Datenschutz 66
3.4 Überwachung von Online-Diensten am Arbeitsplatz 74
3.5 Verträge 78
3.6 Urheberrecht 86
3.7 Lizenzen 91
3.8 Outsourcing / Zusammenarbeit mit Drittfirmen 94
3.9 Vertraulichkeitsvereinbarung mit externen Mitarbeitenden 99
3.10 Aufzeichnungs- und Archivierungspflichten 102
3.11 Internes Kontrollsystem (IKS) 108
3.12 Haftung 109
3.13 Versicherungen 113
3.14 Strafrecht und Computer Forensics 115
4 Organisatorische Aspekte 121
4.1 Zielpublikumsorientierte Sensibilisierung (Awareness) 121
4.2 Sichere Passwörter 130
4.3 Umgang mit Internet 134
4.4 Umgang mit E-Mail 139
4.5 Clear Desk 143
4.6 Umgang mit PC – Benutzer-Richtlinien 145
4.7 Sicherer Zahlungsverkehr (Online-Banking) 147
4.8 Hilfspersonal – Externe Mitarbeitende 151
4.9 Schlüssel- und Badgeverwaltung 153
4.10 Verhalten im Notfall – Krisenmanagement 156

4.11 Cloud-Nutzung ... 162
4.12 Zugriffskontrolle auf Daten ... 168
4.13 Handhabung von Datenträgern ... 173
4.14 Löschung oder Vernichtung von Datenträgern ... 176
4.15 Beschaffung von Informatikmitteln ... 180
4.16 Richtlinien Dokumentation ... 182
4.17 Verbesserungs- und Meldewesen ... 185
4.18 Unterhalt, Wartung und Reparatur ... 188
4.19 Sicherheit im IT-Projektmanagement ... 192
4.20 Change Management ... 194
4.21 Sicherheit am Arbeitsplatz ... 198
5 Technische Aspekte ... 203
5.1 Verschlüsselung, digitale Signatur und PKI ... 203
5.2 Backup ... 206
5.3 Schutz vor Malware ... 210
5.4 Microsoft Windows Server 2008/2012 Sicherheit ... 215
5.5 Einsatz von Arbeitsplatz-PCs (Clients) ... 224
5.6 Netzwerksicherheit ... 228
5.7 Sicherheit bei drahtlosen Netzwerken (WLAN) ... 232
5.8 Virtual Private Network (VPN) ... 236
5.9 Internet-Verbindung ... 239
5.10 Prüfung der Sicherheit von Internetverbindungen ... 243
5.11 Fernwartung (Remote Access/Control) ... 247
5.12 Telekommunikationsgeräte und Internet-Telefonie (VOIP) ... 250
5.13 Firewall ... 253
5.14 Einsatz mobiler Geräte (Notebooks, Smartphones, Tablets etc.) ... 257
5.15 BYOD (Bring your own device) ... 261
5.16 Telearbeit Heimarbeitsplatz ... 268
5.17 Sicherheit von Webapplikationen ... 271
5.18 Datenbank-Sicherheit ... 276
5.19 Sicherheit in der Applikationsentwicklung und -einführung ... 280
5.20 Unterbrechungsfreie Stromversorgung (USV) ... 285
5.21 Physische Sicherheit ... 287
6 Abkürzungsverzeichnis und Glossar ... 297
7 Index ... 317
8 Literaturverzeichnis ... 325
9 Lizenzbedingungen und Beilagen ... 327