Inhaltsverzeichnis

1. Einleitung 23
1.1. Daten – Informationen – Informationssicherheit 23
1.2. Wegweiser durch das Handbuch 26
1.3. Vorgehen bei der Umsetzung der Informationssicherheit 29
2. Informationssicherheits-Managementsystem (ISMS) 39
2.1. Informationssicherheit in KMU und in Verwaltungen 39
2.2. Oft verwendete Standards 42
2.3. Komponenten eines ISMS gemäss ISO/IEC 27001 43
2.4. Der Prozess der Informationssicherheit 45
2.5. Management-Prinzipien 47
2.6. Umsetzung des ISMS in einem KMU/KMV 52
2.7. IT-Risiko-Analyse 56
2.8. IT-Grundschutz 61
2.9. Umgang mit Risiken 67
2.10. Digital Operational Resilience Act DORA 68
2.11. NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2) 69
2.12. Informationssicherheitsmanagement für Kleinstunternehmen 69
3. Rechtliche Aspekte 71
3.1. Datenschutz 71
3.2. Vertragliche Grundlagen / Allgemeine Geschäftsbedingungen (AGB) 81
3.3. E-Commerce 87
3.4. Verträge mit Outsourcing- resp. Cloud-Anbietern 91
3.5. Lizenzen 95
3.6. Urheberrecht 97
3.7. Vertraulichkeitsvereinbarung mit externen Partnern 101
3.8. Aufzeichnungs- und Archivierungspflichten 103
3.9. Computer-Delikte und Computer-Forensik 107
3.10. Schutz im Cyberspace (inkl. Social Media) 110
3.11. Überwachung am Arbeitsplatz 113
3.12. Haftung 117
3.13. Versicherungen 121
3.14. Künstliche Intelligenz (KI) 124
3.15. Revidiertes Informationssicherheitsgesetz (revISG) 127
4. Organisatorische Aspekte 133
4.1. Benutzerrichtlinien 133
4.2. Passwörter und 2FA 137
4.3. BYOD (Bring Your Own Device) 142
4.4. Zielpublikumsorientierte Awareness 145
4.5. Sicherer Zahlungsverkehr (Online-Banking) 155
4.6. Handhabung von Datenträgern und Dokumenten 159

4.7. Umgang mit Geschäftsunterlagen ... 162
4.8. Verhalten im Notfall – Krisenmanagement ... 167
4.9. Outsourcing und Cloud-Nutzung ... 176
4.10. Berechtigungsvergabe ... 181
4.11. Management von technischen Schwachstellen und Software-Updates ... 186
4.12. Incident Management – Reaktion auf Cyber-Attacken ... 189
4.13. Unterhalt, Wartung und Reparatur ... 196
4.14. Sicherheit im Projektmanagement ... 201
4.15. Change-Management ... 204
4.16. Physische Sicherheit ... 209
4.17. Homeoffice ... 219
4.18. Sicherheit im Umgang mit Blockchain ... 222
4.19. Audits ... 227
5. Technische Aspekte ... 231
5.1. Verschlüsselung, digitale Signatur und PKI ... 231
5.2. Back-up / Restore ... 235
5.3. Sicherheit des Microsoft Windows Ecosystems ... 240
5.4. Linux Server-Sicherheit ... 255
5.5. Einsatz von Arbeitsplatz-Clients ... 262
5.6. Collaboration-Tools (SaaS) ... 265
5.7. Sichere E-Mails ... 268
5.8. Netzwerksicherheit ... 272
5.9. Sicherheit in drahtlosen Netzwerken (WLAN) ... 281
5.10. VPN ... 287
5.11. Internet-Anbindung ... 292
5.12. Fernwartung ... 298
5.13. Telekommunikationsgeräte und VOIP ... 302
5.14. Einsatz mobiler Geräte (Notebooks, Smartphones, Tablets usw.) ... 308
5.15. Serverraum-Sicherheit ... 311
5.16. Sicherheit von Webanwendungen ... 317
5.17. Datenbank-Sicherheit ... 323
5.18. Sicherheit in der Applikationsentwicklung und Einführung ... 331
5.19. Internet der Dinge (IoT) ... 337
6. Abkürzungsverzeichnis und Glossar ... 343
7. Index ... 363
8. Lizenzbedingungen und Beilagen ... 369