

# Inhaltsverzeichnis

Vorwort .....	V
<b>1. Warum dieses Buch?</b> .....	1
<b>2. Rechtliche Anforderungen und wirtschaftliche Relevanz</b> .....	5
2.1. Risikoanalyse als Pflicht und Überlebensstrategie .....	5
2.2. Rechtliche Anforderungen .....	5
2.2.1. DSGVO (GDPR) .....	6
2.2.2. NIS-2-Richtlinie (NIS 2 Directive) – NISG 2026 .....	7
2.2.2.1. Direkt unterworfenen Unternehmen .....	8
2.2.2.2. Indirekt betroffene Unternehmen .....	9
2.2.3. AI-Act (Verordnung über Künstliche Intelligenz) .....	10
<b>3. Grundlagen der Datensicherheit</b> .....	12
3.1. Informationssicherheit – Datensicherheit – Datenschutz .....	12
3.2. Gefährliche Fehleinschätzungen .....	13
<b>4. Das ist (nicht) mein Problem – Risikomanagement</b> .....	19
4.1. Was kann zu meinem Problem werden? – Risiko- identifikation .....	21
4.1.1. Die Grundlage: Wo und wie entsteht konkret ein Risiko? .....	21
4.1.2. Relevante Bestandteile in meinem Unternehmen (Asset) .....	22
4.1.2.1. Informationen und Daten .....	22
4.1.2.2. Prozesse und Vorgehensweisen .....	23
4.1.2.3. Technologie (Anwendungen und Infrastruktur) .....	24
4.1.2.4. Menschen .....	24
4.1.3. Schutzbedarf meiner Assets .....	25
4.1.3.1. Vertraulichkeit .....	27
4.1.3.1.1. Effiziente Handhabung von Vertraulichkeit .....	29
4.1.3.1.2. Integrität (Korrektheit) .....	30
4.1.3.1.3. Verfügbarkeit .....	32
4.1.3.1.4. Häufige Fehler .....	34
4.1.3.1.5. Ergebnis der Schutzbedarfsfeststellung .....	36
4.1.3.1.6. Schutzbedarfsfeststellung und Risikoanalyse – zwei Seiten derselben Medaille .....	36
4.1.4. Mögliche Bedrohungen meiner Assets .....	37
4.1.4.1. Physische und natürliche Bedrohungen .....	37
4.1.4.2. Infrastrukturausfälle .....	41
4.1.4.3. Menschliche Bedrohungen .....	43
4.1.4.4. Social Engineering .....	48

4.1.4.5.	Technische Bedrohungen .....	54
4.1.4.6.	Prozess- und Organisationsfehler .....	58
4.1.4.7.	Besser jetzt als perfekt .....	61
4.1.5.	Schwachstellen meiner Assets .....	62
4.1.5.1.	Organisatorische Schwachstellen .....	62
4.1.5.2.	Technische Schwachstellen .....	68
4.1.5.3.	Physische Schwachstellen .....	71
4.1.5.4.	Abwarten ist kein Schutz .....	72
4.1.6.	Typische Risiken für Kleine und Mittlere Unternehmen .....	73
4.2.	Risikoanalyse .....	75
4.2.1.	Festlegung der Rahmenbedingungen .....	76
4.2.1.1.	Risiko(akzeptanz)kriterien .....	77
4.2.1.2.	Kriterien der Eintrittswahrscheinlichkeit .....	79
4.2.1.3.	Kriterien für Auswirkungen .....	81
4.2.2.	Risikobewertung .....	86
4.2.2.1.	Eintrittswahrscheinlichkeit .....	86
4.2.2.2.	Auswirkung .....	88
4.2.2.3.	Risikomatrix .....	89
4.3.	Risikobewältigung .....	92
4.3.1.	Die vier Strategien der Risikobewältigung .....	93
4.4.	Plan-Do-Check-Act (PDCA) .....	96
<b>5.</b>	<b>Technische Maßnahmen zur Datensicherheit</b> .....	<b>97</b>
5.1.	Stand der Technik .....	98
5.1.1.	Informationsquellen .....	99
5.2.	Grundlegende und prinzipielle Schutzmechanismen .....	100
5.2.1.	Netzwerksicherheit .....	101
5.2.1.1.	Segmentierung von Netzwerken .....	102
5.2.1.2.	Perimeter-Schutz (WAN-LAN-Grenze) .....	105
5.2.1.3.	Absicherung der Kommunikationswege .....	107
5.2.2.	Endgeräteschutz .....	109
5.2.2.1.	Härtung und Grundschutz .....	109
5.2.2.2.	Physische und logische Sicherheit .....	111
5.2.2.3.	Festplattenverschlüsselung .....	112
5.2.2.4.	Mobile Geräte (Smartphones, Tablets) .....	113
5.2.2.4.1.	Geräteschutz und Einstellungen am Beispiel iPhone .....	114
5.2.3.	Identitäts- und Zugriffsmanagement .....	120
5.2.3.1.	Sicheres Passwort- und Anmeldeverhalten .....	121
5.2.3.2.	Berechtigungsmanagement .....	123
5.2.3.3.	Kontenverwaltung .....	125

5.2.4.	Schutz der Daten durch Verschlüsselung .....	126
5.2.4.1.	Verschlüsselung im Ruhezustand (Data at Rest) .....	127
5.2.4.2.	Verschlüsselung bei der Übertragung (Data in Transit) .....	128
5.2.4.3.	Anwendungsbezogene Verschlüsselung .....	130
5.2.5.	Kommunikationssicherheit .....	131
5.2.5.1.	E-Mail-Sicherheit .....	132
5.2.5.2.	Messenger-Dienste .....	134
5.2.5.3.	Sicherer Umgang mit internen und externen Datenflüssen .....	135
5.2.6.	Datensicherung und Wiederherstellbarkeit .....	136
5.2.6.1.	Backup-Strategie .....	136
5.2.6.2.	Backup-Schutzmechanismen .....	137
5.2.6.3.	Wiederherstellung .....	138
5.2.6.4.	Notfallfähigkeit .....	139
5.3.	Die verwundbarsten Teile im Unternehmen .....	141
<b>6.</b>	<b>Organisatorische Maßnahmen zur Datensicherheit .....</b>	<b>143</b>
6.1.	Rechte, Zuständigkeiten und Vertretungen als organisatorisches Sicherheitsfundament .....	144
6.1.1.	Rollen- und Rechtekonzept: Zugriff folgt Aufgabe .....	144
6.1.2.	Zuständigkeiten und Verantwortungen: Orientierung schafft Sicherheit .....	145
6.1.3.	Vertretungsregelungen: Sicherheit auch im Ausnahmefall .....	145
6.1.4.	Zusammenspiel der Elemente: Denken in Systemen statt in Einzelmaßnahmen .....	146
6.1.5.	Schulung und Bewusstsein: Regeln verständlich machen .....	146
6.2.	Backupkonzept, Wiederherstellungsstrategie und Archivierung .....	146
6.3.	Informationssicherheitsrichtlinie .....	148
6.3.1.	Themenbereiche der allgemeinen Sicherheits- richtlinie .....	149
6.3.1.1.	Grundsätze der Informationsverarbeitung und Verantwortlichkeiten .....	149
6.3.1.2.	Berechtigungskonzept und Zugriffsmanagement .....	149
6.3.1.3.	Onboarding und Offboarding – Pflichten der Mitarbeitenden .....	150
6.3.1.4.	Zugangs- und Gerätesicherheit für IT-Endgeräte .....	150
6.3.1.5.	Physische Sicherheit und sichere Arbeits- umgebung .....	150

6.3.1.6.	Arbeiten außerhalb des Unternehmens und in geteilten Umgebungen .....	151
6.3.1.7.	Betriebliche und private Geräte .....	151
6.3.1.8.	Netzwerkzugang, Internetnutzung und sichere Einwahl .....	151
6.3.1.9.	Nutzung von Anwendungen, Systemen und Plattformen .....	152
6.3.1.10.	Externe Speichermedien und Datentransport .....	152
6.3.1.11.	Kommunikationssicherheit und Informationsübermittlung .....	152
6.3.1.12.	Social Media, Außenwirkung und Veröffentlichung von Arbeitsinhalten .....	153
6.3.1.13.	Meldung von Sicherheitsvorfällen, Verdachtsfällen und Verlusten .....	153
6.3.2.	Was im Alltag erlaubt ist – und was nicht: Mustervorlage .....	153
6.4.	Schulungen als tragende Säule der organisatorischen Sicherheit .....	166
6.4.1.	Datenschutzschulungen: Pflicht und Praxis zugleich .....	166
6.4.2.	Social Engineering: Manipulation erkennen lernen ...	167
6.4.3.	IT-Sicherheitsschulungen: Regeln verstehen statt nur lesen .....	168
6.4.4.	Schulungen zu Künstlicher Intelligenz: Sicherheit im Umgang mit neuen Werkzeugen .....	169
6.4.5.	Meldewege, Ansprechpartner und Zusammenarbeit .....	169
6.5.	Onboarding und Offboarding als Sicherheitsfaktor .....	170
6.5.1.	Vorbereitungsphase (Preboarding): Sicherheit beginnt vor dem ersten Arbeitstag .....	170
6.5.2.	Orientierungsphase: Regeln, Kultur und Erwartungen klar vermitteln .....	171
6.5.3.	Integrationsphase: Verantwortung bewusst erweitern .....	171
6.5.4.	Offboarding: Der oft vergessene Teil der Sicherheitskette .....	171
6.6.	Kontrolle und Nachvollziehbarkeit als dauerhafte Sicherheitsaufgabe .....	172
6.6.1.	Aktualität und Wirksamkeit von Regelungen .....	172
6.6.2.	Nachvollziehbarkeit in der Anwendung durch Mitarbeitende .....	173
6.6.3.	Offene Kommunikation als Sicherheitsfaktor .....	173
6.6.4.	Kontrolle als kontinuierlicher Prozess .....	174

<b>7. Wenn was passiert – Geschäftskontinuität und Notfallplan</b> .....	175
7.1. Geschäftskontinuität kompakt für kleine Unternehmen .....	177
7.1.1. Das Krisenteam BAO (Besondere Aufbauorganisation) .....	177
7.1.2. Die Business-Impact-Analyse als Fundament des BCM .....	178
7.1.3. Kennzahlen .....	181
7.1.4. RTA und RPA – Realität schlägt Planung .....	182
7.1.5. Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs .....	183
7.1.6. Das Notfallhandbuch – kompakt, klar, einsatzbereit ...	185
7.1.7. Üben und Testen – vom Konzept zur Handlungsfähigkeit .....	187
7.2. Praxisbeispiel: Therapiezentrum .....	187
7.2.1. Ermittlung der kritischen Prozesse, Daten und Ressourcen .....	188
7.2.2. Erfassung der relevanten Kennzahlen .....	189
7.2.3. Maßnahmen zur Aufrechterhaltung des Betriebs – Kosten-Nutzen-orientiert .....	190
7.2.4. Umgang mit Single Points of Failure und Single Points of Contact .....	191
7.2.5. Fazit aus der Praxis .....	192
<b>8. Umsetzung in der Praxis</b> .....	193
8.1. Umsetzung in 3 Schritten .....	194
8.1.1. Die Risiko-Identifikation auf Basis bestehender Assets .....	194
8.1.1.1. Fragenkatalog für die Strukturierung (Sammlung der Assets) .....	195
8.1.1.1.1. Kategorie: Informationen und Daten .....	195
8.1.1.1.2. Kategorie: Prozesse und Vorgehensweisen .....	197
8.1.1.1.3. Kategorie: Technologie .....	199
8.1.1.1.4. Kategorie: Menschen .....	201
8.1.1.2. Erstellung des Asset-Registers und Erhebung des Schutzbedarfs .....	204
8.1.1.3. Bedrohungen .....	206
8.1.1.4. Schwachstellen .....	207
8.1.1.4.1. Technische Verwundbarkeiten .....	208
8.1.1.4.2. Prozessuale und organisatorische Schwächen .....	208
8.1.1.4.3. Menschliche Faktoren .....	208
8.1.1.4.4. Physische Schwachstellen .....	209
8.1.1.4.5. Rechtliche und administrative Defizite .....	209
8.1.1.4.6. Daten- und Informationsmanagement .....	209

8.1.1.5.	Risiken – Bewertung und Risikomatrix .....	209
8.1.2.	Risikobewältigung .....	209
8.1.2.1.	Quick-Wins in der Risikobewältigung .....	210
8.2.	Praxisbeispiel: Strömi GmbH .....	210
8.2.1.	Assets des Unternehmens .....	211
8.2.2.	Assetregister und Schutzbedarf .....	212
8.2.3.	Bedrohungsanalyse .....	213
8.2.4.	Schwachstellen und Risikobewertung .....	214
8.2.5.	Risikobewältigung/Risikobehandlung .....	215
8.2.6.	Zyklus-Ende und Planung des nächsten Zyklus .....	217
<b>9.</b>	<b>Weitere Ressourcen</b> .....	<b>218</b>
9.1.	Digitale Vorlagen für Ihre Informationssicherheit .....	218
9.2.	Umfrage für KI-Nutzung im Unternehmen .....	218
9.3.	E-Mail-Sicherheit mit SPF, DKIM und DMARC .....	219
9.3.1.	SPF (Sender Policy Framework) .....	219
9.3.2.	DKIM (DomainKeys Identified Mail) .....	221
9.3.3.	DMARC (Domain-based Message Authentication, Reporting and Conformance) .....	223
9.3.4.	Warum SPF, DKIM und DMARC so wichtig sind .....	224
9.3.5.	Prüfen Sie Ihre Domain .....	225
<b>10.</b>	<b>Zum Abschluss</b> .....	<b>226</b>
	Stichwortverzeichnis .....	229