Inhaltsverzeichnis

Vorwort V
Abkürzungsverzeichnis XXI
Literaturverzeichnis XXVII

Teil 1:
Rechtliche Anforderungen des NISG 2026

1. Einleitung 1

2. Ausgangssituation: Was ist NIS? 1
2.1. Allgemeines 1
2.2. Schutzziele von Informationssicherheit 2
2.3. Verfügbarkeit 3
2.4. Authentizität 4
2.5. Integrität 4
2.6. Vertraulichkeit 5

3. Gesetzgebung 6
3.1. NIS-Richtlinie und NISG 2018 oder wie alles begann 6
3.1.1. NIS-Richtlinie (EU) 2016/1148 6
3.1.2. NIS-Gesetz 2018 6
3.1.2.1. Anwendungsbereich NISG 2018 7
3.1.2.2. Inhalt NISG 2018 7
3.1.2.3. NIS-Verordnung 2019 8
3.1.2.4. Geltungsdauer NISG 2018 und zugehörige Verordnungen 8
3.1.3. Unterschiede NISG 2018 und NISG 2026 8
3.1.3.1. Einrichtungsbezogene Einstufung statt dienstbezogener Betrachtung im NISG 2026 9
3.2. NIS-2-Richtlinie 10
3.2.1. Allgemeines 10
3.2.2. Gründe für die Entstehung der NIS-2-Richtlinie 10
3.2.3. Ziele NIS-2 11
3.2.3.1. Erhöhung der Cyberabwehrfähigkeit und Resilienz 12
3.2.3.2. Harmonisierung und Funktionsfähigkeit des Binnenmarkts 12
3.2.3.3. Ausweitung des Anwendungsbereichs auf weitere Sektoren 12
3.2.3.4. Stärkung von Aufsicht, Durchsetzung und Zusammenarbeit 13

3.2.4. Geplante Änderungen der NIS-2-Richtlinie durch das Cybersicherheitspaket ... 13
3.3. DVO (EU) 2024/2690 ... 14
3.3.1. Verhältnis NIS-2-Richtlinie und Durchführungsrechtsakte ... 14
3.3.2. Was ist die DVO (EU) 2024/2690 – und was nicht? ... 15
3.3.3. Für wen gilt die DVO (EU) 2024/2690? ... 16
3.3.4. Bindungswirkung der DVO (EU) 2024/2690 ... 16
3.3.4.1. Bindung der nationalen Behörden ... 17
3.3.4.2. Bindung der betroffenen Einrichtungen ... 17
3.3.4.3. Bedeutung für die Auslegung des nationalen Rechts ... 17
3.3.5. ENISA-Guidance zur DVO (EU) 2024/2690 ... 18
3.3.5.1. Zweck und Bezug zur DVO (EU) 2024/2690 ... 18
3.3.5.2. Zielgruppe ... 18
3.3.5.3. Keine eigenständige Rechtsverbindlichkeit ... 19
3.3.5.4. Verhältnis von DVO (EU) 2024/2690 und ENISA-Guidance in der Praxis ... 19
3.3.5.4.1. Bedeutung für Aufsicht und Prüfungen ... 19
3.3.5.4.2. Risiko der Übererfüllung bei unkritischer Anwendung ... 20
3.3.6. Kernaussagen ... 20
3.4. Vom differenzierten EU-Recht zum NISG 2026 ... 20
3.5. NISG 2026 ... 21
3.5.1. Entstehungsgeschichte ... 21
3.5.2. Inkrafttreten ... 22
3.5.3. Inhalt ... 23
3.6. Netz- und Informationssystemsicherheits-Verordnung (NISV 2026) ... 23
3.6.1. Rechtsgrundlage und Einordnung ... 23
3.6.2. Risikomanagementmaßnahmen ... 24
3.6.3. Erhebliche Cybersicherheitsvorfälle ... 24
3.6.4. Kernaussagen ... 25
3.7. Exkurs: Änderungen des Telekommunikationsgesetzes durch das NISG ... 25
3.7.1. Was bedeutet die TKG-Novelle in der Praxis? ... 25
3.7.1.1. Cybersicherheit wird im NISG geregelt ... 25
3.7.1.2. Inländische Zustelladresse für Drittstaatenanbieter ... 26
3.7.1.3. Neue Aufgaben der RTR ... 26
3.8. Exkurs: NIS-2-Umsetzung in den anderen EU-Mitgliedstaaten ... 27
3.8.1. Umsetzung der NIS-2-Richtlinie in Deutschland ... 28

4. Cybersicherheit als zentrales Unternehmensrisiko 29
4.1. Cyberrisiken als weltweit größtes Geschäftsrisiko 29
4.2. Zusammenhang zwischen Cyberrisiken und Künstlicher Intelligenz 30
4.3. Cybersicherheit in Österreich 30

5. Das NISG-Umsetzungsprojekt in der Praxis 32
5.1. Vom Gesetzestext zur Umsetzung 32
5.2. Das Umsetzungsprojekt aufsetzen 32
5.3. Verantwortung der Leitungsorgane 33
5.4. Projektorganisation und Governance 34
5.5. Rollen und Verantwortlichkeiten 35
5.6. Der Projektstart in der Praxis 36
5.7. Erste Bestandsaufnahme 37
5.8. Interviews und Informationsgewinnung 38
5.9. Typische Feststellungen aus der Praxis 39
5.10. Von der Bestandsaufnahme zur GAP-Analyse 39
5.11. Die GAP-Analyse als Grundlage der Umsetzung 40
5.11.1. Ziel und Zweck der GAP-Analyse 40
5.11.2. Der Soll-Zustand: Welche Anforderungen sind zu prüfen? 40
5.11.3. Vorbereitung der Analyse 41
5.11.4. Informationsquellen für die GAP-Analyse 41
5.11.5. Bewertung vorhandener Maßnahmen 42
5.11.6. Häufige Feststellungen in der Praxis 42
5.11.7. Von der Analyse zum Maßnahmenplan 43
5.11.8. Grenzen der GAP-Analyse 43
5.11.9. Dokumentation und Nachvollziehbarkeit der Ergebnisse 43
5.11.10. Die GAP-Analyse als Ausgangspunkt der weiteren Umsetzung 44
5.12. Kosten der Umsetzung 45
5.12.1. Kosten im Kontext von Risiko und Verhältnismäßigkeit 46
5.12.2. Kostenoptimierung in der Umsetzung von Cybersicherheitsmaßnahmen 48

6. Anwendungsbereich – Wer ist betroffen 49
6.1. Allgemeines 49
6.2. Örtlicher Anwendungsbereich 49
6.3. Sachlicher Anwendungsbereich: wesentliche und wichtige Einrichtungen 50
6.3.1. Grundregel sachlicher Anwendungsbereich 51
6.3.1.1. Jede Haupt- und Nebentätigkeit zählt 51

6.4. Begriff der Einrichtung 51
6.4.1. Kein Opting-out oder Opting-in 51
6.4.2. Wesentliche Einrichtungen 52
6.5. Wichtige Einrichtungen 53
6.5.1. Auswirkungen der Einstufung als wesentliche oder wichtige Einrichtung 54
6.6. Territorialität 55
6.7. Sektoren mit hoher Kritikalität – Anwendungsbereich Anlage 1 56
6.7.1. Energie 56
6.7.2. Verkehr 57
6.7.3. Bankwesen und Finanzmarktinfrastrukturen 57
6.7.4. Gesundheitswesen 57
6.7.5. Trinkwasser 58
6.7.6. Abwasser 59
6.7.7. Digitale Infrastruktur 59
6.7.8. Verwaltung von IKT-Diensten (Business-to-Business) 61
6.8. Sektor öffentliche Verwaltung 62
6.8.1. Sonderfall Gemeinden 64
6.8.1.1. Gemeinden – bewusst nicht im Sektor „Öffentliche Verwaltung“ erfasst 64
6.8.2. Weltraum 65
6.9. Sonstige kritische Sektoren – Anwendungsbereich Anlage 2 65
6.9.1. Post- und Kurierdienste 65
6.9.2. Abfallbewirtschaftung 66
6.9.3. Produktion, Herstellung und Handel mit chemischen Stoffen 67
6.9.4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln 67
6.9.5. Verarbeitendes Gewerbe/Herstellung von Waren 68
6.9.6. Anbieter digitaler Dienste 69
6.9.7. Forschung 69
6.10. Ermittlung der Unternehmensgröße 70
6.10.1. Rechtsgrundlagen der Größenberechnung 70
6.10.2. Bedeutung und Funktion der Unternehmensgröße 71
6.10.3. Regelfall: Größenberechnung bei eigenständigen Einrichtungen 71
6.10.4. Mitarbeiterzahl 71
6.10.5. Jahresumsatz und Jahresbilanzsumme 72
6.10.6. Zusammenfassung Größenschwellen 74

6.11. Abweichungen vom Regelfall: Partnerunternehmen und verbundene Unternehmen ... 74
6.11.1. Verbundene Unternehmen ... 75
6.11.1.1. Auswirkungen auf die Größenberechnung ... 75
6.11.2. Partnerunternehmen ... 76
6.11.2.1. Ausnahme bei organisatorischer, technischer und operativer Unabhängigkeit ... 76
6.11.3. Zusammenfassung Zurechnung im Konzern ... 77
6.12. Herausforderungen der Umsetzung im Konzern ... 78
6.12.1. Regulatorische Komplexität im grenzüberschreitenden Konzern ... 78
6.12.1.1. Unterschiedliche nationale Umsetzungen ... 78
6.12.2. Organisatorische Herausforderungen im Konzern ... 78
6.12.2.1. Governance und Verantwortlichkeiten ... 78
6.12.2.2. Konzernsteuerung und rechtliche Selbständigkeit der Einrichtungen ... 78
6.12.3. Technische und operative Umsetzung ... 79
6.12.3.1. Heterogene IT-Landschaften ... 79
6.12.3.2. Meldepflichten und Incident-Management ... 79
6.12.4. Wirtschaftliche und personelle Belastungen ... 80

7. Governance und Leitungsorgane ... 80
7.1. Leitungsorgane sind verantwortlich ... 80
7.2. Wer ist „Leitungsorgan“ ... 80
7.2.1. Verantwortung des Aufsichtsrats ... 81
7.3. Aufgaben der Leitungsorgane ... 83
7.4. Schulungen der Leitungsorgane ... 84
7.4.1. Schulungspflicht für Leitungsorgane ... 84
7.5. Ziele und Inhalte der Schulung ... 84
7.5.1. Ziel der Schulung ... 85
7.5.2. Empfohlene Schulungsinhalte ... 85
7.5.3. Lernziele ... 87
7.5.4. Vorbildfunktion der Leitungsorgane ... 87
7.5.5. Dauer und Intervall der Schulungen ... 87
7.5.6. Nachweis der Schulungen ... 88
7.6. Haftung der Leitungsorgane ... 89

8. Risikomanagementmaßnahmen ... 90
8.1. Allgemeines ... 90
8.1.1. Einordnung, Zielsetzung und Rechtsgrundlagen ... 90
8.1.2. Geltung der Risikomanagementmaßnahmen ... 91
8.1.2.1. Geltung der Risikomanagementmaßnahmen für die gesamte Einrichtung ... 91
8.1.2.2. Geltung der Risikomanagementmaßnahmen seit Inkrafttreten des NISG ... 92

8.1.3. Angemessenheit, Verhältnismäßigkeit, Stand der Technik und Kosten ... 92
8.1.4. Kompensierende Maßnahmen ... 93
8.1.5. Gefahrenübergreifender Ansatz („All-Hazards-Approach") ... 94
8.1.6. Risikokategorien ... 94

9. Technische und methodische Anforderungen laut DVO (EU) 2024/2690 ... 95
9.1. Konzept für die Sicherheit von Netz- und Informationssystemen ... 96
9.1.1. Funktion und Stellenwert des Sicherheitskonzepts ... 96
9.1.2. Mindestinhalte des Sicherheitskonzepts ... 97
9.1.3. Rollen, Verantwortlichkeiten und Weisungsbefugnisse ... 97
9.2. Konzept für das Risikomanagement ... 98
9.2.1. Risikomanagementrahmen ... 98
9.2.2. Überwachung der Einhaltung ... 99
9.2.3. Unabhängige Überprüfung der Netz- und Informationssicherheit und Information der Leitungsorgane ... 99
9.3. Bewältigung von Sicherheitsvorfällen ... 99
9.3.1. Konzept für die Bewältigung von Sicherheitsvorfällen ... 100
9.3.2. Überwachung und Protokollierung ... 100
9.3.3. Meldung von Ereignissen ... 101
9.3.4. Bewertung und Klassifizierung von Ereignissen ... 101
9.3.5. Reaktion auf Sicherheitsvorfälle ... 102
9.3.6. Überprüfungen nach Sicherheitsvorfällen ... 102
9.4. Betriebskontinuitäts- und Krisenmanagement ... 103
9.4.1. Notfallplan für die Aufrechterhaltung und Wiederherstellung des Betriebs ... 103
9.4.2. Backup-Sicherungs- und Redundanzmanagement ... 103
9.4.3. Krisenmanagement ... 104
9.5. Sicherheit der Lieferkette ... 104
9.5.1. Konzept für die Sicherheit der Lieferkette ... 104
9.5.1.1. Umfang der Sicherheit der Lieferkette ... 106
9.5.2. Verzeichnis der Anbieter und Diensteanbieter ... 106
9.5.2.1. Welche Lieferanten sind erfasst? ... 106
9.5.2.2. Vertragliche Regelungen mit Lieferanten ... 107
9.5.3. Exkurs: Was sollten Lieferanten beachten? ... 107
9.6. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen ... 108
9.6.1. Sicherheitsmaßnahmen beim Erwerb von IKT-Diensten oder IKT-Produkten ... 108

9.6.2. Sicherer Entwicklungszyklus ... 108
9.6.3. Konfigurationsmanagement ... 109
9.6.4. Änderungsmanagement, Reparatur und Wartung ... 110
9.6.5. Sicherheitsprüfung ... 110
9.6.6. Sicherheitspatch-Management ... 111
9.6.7. Netzsicherheit ... 111
9.6.8. Netzsegmentierung ... 112
9.6.9. Schutz gegen Schadsoftware und nicht genehmigte Software ... 113
9.6.10. Behandlung und Offenlegung von Schwachstellen ... 113
9.7. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen ... 114
9.8. Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen ... 115
9.8.1. Sensibilisierungsmaßnahmen und grundlegende Verfahren im Bereich der Cyberhygiene ... 115
9.8.2. Sicherheitsschulungen ... 115
9.9. Kryptografie ... 116
9.10. Sicherheit des Personals ... 117
9.10.1. Sicherheit des Personals ... 117
9.10.2. Zuverlässigkeitsüberprüfung ... 117
9.10.3. Verfahren zur Beendigung oder Änderung des Beschäftigungsverhältnisses ... 118
9.10.4. Disziplinarverfahren ... 118
9.11. Zugriffskontrolle ... 119
9.11.1. Konzept für die Zugriffskontrolle ... 119
9.11.2. Management von Zugangs- und Zugriffsrechten ... 119
9.11.3. Privilegierte Konten und Systemverwaltungskonten ... 120
9.11.4. Systemverwaltungssysteme ... 120
9.11.5. Identifizierung ... 121
9.11.6. Authentifizierung ... 121
9.12. Multifaktor-Authentifizierung ... 122
9.13. Anlagen- und Wertemanagement ... 122
9.13.1. Anlagen- und Werteklassifizierung ... 122
9.13.2. Behandlung von Anlagen und Werten ... 123
9.13.3. Konzept für Wechseldatenträger ... 123
9.13.4. Anlagen- und Werteinventar ... 124
9.13.5. Abgabe, Rückgabe oder Löschung von Anlagen und Werten bei Beendigung des Beschäftigungsverhältnisses ... 124
9.14. Sicherheit des Umfelds und physische Sicherheit ... 125
9.14.1. Unterstützende Versorgungsleistungen ... 125
9.14.2. Schutz vor physischen Bedrohungen und Bedrohungen des Umfelds ... 125
9.14.3. Perimeter und physische Zutrittskontrolle ... 126

10. Registrierung 127
10.1. Register wesentlicher und wichtiger Einrichtungen 127
10.2. Registrierung 127
10.2.1. Angaben bei der Registrierung 127
10.2.2. Ablauf der Registrierung 128
10.3. Frist für die Registrierung 129
10.4. Strafen 130

11. Nachweis der Wirksamkeit 130
11.1. Allgemeines 130
11.2. Selbstdeklaration 131
11.2.1. Frist für die Übermittlung der Selbstdeklaration 132
11.3. Prüfung durch unabhängige Stelle 132
11.3.1. Allgemeines 132
11.3.2. Nachweis operative und organisatorische Umsetzung 133
11.3.3. Nachweis technische Umsetzung 134
11.3.4. Fristen 134

12. Unabhängige Stellen und unabhängige Prüfer 136
12.1. Von qualifizierten Stellen im NISG 2018 zu unabhängigen Prüfern des NISG 2026 136
12.2. Wozu unabhängige Stellen und Prüfer? 136
12.3. Begriff unabhängige Stellen 137
12.4. Begriff unabhängiger Prüfer 137
12.4.1. Zulassungsvoraussetzungen für unabhängige Prüfer 138
12.4.2. Entziehung der Zulassung und Wiederzulassung 139
12.4.3. Verschwiegenheitspflichten unabhängiger Prüfer 140
12.4.4. Übergangsbestimmungen zu unabhängigen Stellen und Prüfern 140
12.4.4.1. Praxishinweise zur Übergangsphase 141

13. Berichtspflichten bei erheblichem Cybersicherheitsvorfall 141
13.1. Allgemeines 141
13.2. Meldepflicht 142
13.3. Erheblicher Cybersicherheitsvorfall 142
13.3.1. Erheblicher Sicherheitsvorfall nach DVO (EU) 2024/2690 143
13.3.2. Erheblicher Cybersicherheitsvorfall nach der NISV 2026 144
13.4. Ablauf der Meldung 146
13.5. Zusammentreffen mehrerer Meldepflichten 148
13.5.1. Meldepflichten nach verschiedenen Rechtsakten 148

13.5.2. Meldepflichten in mehreren Mitgliedstaaten 149
13.5.3. Information Betroffener 150
13.6. Freiwillige Meldung relevanter Informationen 150

14. Behörden 151
14.1. Bundesamt für Cybersicherheit als zentrale Cybersicherheitsbehörde 151
14.1.1. Agenden der Netz- und Informationssicherheit beim Bundesminister für Inneres 151
14.1.2. Aufgaben des Bundesamts für Cybersicherheit 151
14.1.2.1. Betrieb von IKT-Lösungen durch die Cybersicherheitsbehörde 153
14.1.2.1.1. Betrieb von IKT-Lösungen 153
14.1.2.1.2. Meldeanalysesystem 154
14.1.2.1.3. IKDOK-Plattform 154
14.1.3. Bundesamt für Cybersicherheit als nationales Koordinierungszentrum für Cybersicherheit 154
14.2. Bezirksverwaltungsbehörde verhängt Verwaltungsstrafen 155

15. Computer-Notfallteams 155
15.1. CSIRTs als zentrale Akteure zur Unterstützung der Cybersicherheit 155
15.2. Nationale und sektorspezifische CSIRTs 156
15.2.1. Nationales CSIRT und sektorspezifische CSIRTs 156
15.2.2. GovCERT als sektorspezifisches CSIRT für die öffentliche Verwaltung 156
15.3. Aufgaben der CSIRTs 157
15.4. Koordinierte Offenlegung von Schwachstellen 158

16. Nationale Koordinierung 159
16.1. Cyber Sicherheit Steuerungsgruppe (CSS) 159
16.2. Operative Koordinierungsstrukturen 159
16.2.1. Innerer Kreis der Operativen Koordinierungsstruktur (IKDOK) 159
16.2.2. Operative Koordinierungsstruktur (OpKoord) 160
16.3. Nationale Cybersicherheitsstrategie 161
16.4. Management von Cybersicherheitsvorfällen großen Ausmaßes 161
16.5. Zusammenarbeit auf nationaler, Unions- und internationaler Ebene 162
16.6. Zusammenarbeit auf nationaler Ebene 162
16.7. Zusammenarbeit mit der Datenschutzbehörde 164
16.8. Internationale Zusammenarbeit 165
16.9. Peer Reviews 165

17. Aufsicht und Durchsetzung 165
17.1. Stellung von Aufsicht und Durchsetzung 165
17.2. Aufsicht 166
17.2.1. Aufsichtszweck und Reichweite der Befugnisse 166
17.2.2. Aufsichtsmaßnahmen – Befugnisse der Cybersicherheitsbehörde 166
17.2.3. Abgestufter Umfang der Aufsicht bei wesentlichen und wichtigen Einrichtungen 168
17.3. Durchsetzung 168
17.3.1. Allgemeines 168
17.3.2. Aufforderung und Anordnung von Durchsetzungsmaßnahmen 169
17.3.3. Besondere Durchsetzungsmaßnahmen 170
17.3.4. Eskalierende Durchsetzungsmaßnahmen gegenüber wesentlichen Einrichtungen 170
17.3.5. Kriterien der behördlichen Ermessensausübung 171
17.3.6. Kernpunkte – Was Unternehmen zu Aufsicht und Durchsetzung wissen müssen 172

18. Strafbestimmungen 172
18.1. Relevanz der Strafbestimmungen für Einrichtungen 172
18.2. Zuständigkeit der Bezirksverwaltungsbehörden 173
18.3. Wer haftet: Unternehmen, Leitung, Einzelpersonen? 174
18.4. Strafhöhe und Strafbemessung 175
18.5. Besonders sanktionsrelevante Pflichtverletzungen 176
18.5.1. Weitere strafbare Pflichtverletzungen 176
18.6. Strafrahmen 178
18.7. Verhältnis zur DSGVO – Verbot der Doppelbestrafung 178
18.8. Pflichtverletzungen durch Stellen der öffentlichen Verwaltung 179
18.9. Kernaussagen zu den Strafbestimmungen 180

19. Inkrafttreten und Übergangsbestimmungen 180
19.1. Außerkrafttreten des bisherigen Rechts 181
19.2. Übergangsregelungen für Institutionen und Prüfsysteme 181

20. NISG und verwandte Rechtsakte 182
20.1. Allgemeines 182
20.2. Datenschutzgrundverordnung (DSGVO) 182
20.2.1. Kurzüberblick 182
20.2.2. Verhältnis zum NISG 182
20.2.3. Praktische Bedeutung 183
20.3. Resilienz kritischer Einrichtungen-Gesetz (RKEG) 183
20.3.1. Allgemeines 183
20.3.2. Verhältnis zum NISG 183

20.4. Digital Operational Resilience Act (DORA) 184
20.4.1. Allgemeines 184
20.4.2. Anwendungsbereich 184
20.4.3. Verhältnis zum NISG 184
20.4.3.1. Ausgangspunkt 185
20.4.3.2. DORA als sektorspezifischer Rechtsakt (lex specialis) zum NISG 185
20.4.3.3. Kein vollständiger Ausschluss des NISG 185
20.4.3.4. Welche Bestimmungen des NISG werden durch DORA verdrängt? 186
20.4.3.5. Welche Bestimmungen des NISG bleiben dennoch anwendbar? 186
20.4.3.6. DORA-Unternehmen, die in weiteren NISG-Sektoren tätig sind 187
20.4.3.7. IKT-Drittdienstleister 187
20.4.3.8. Sonderfall Erbringung von IKT-Dienstleistungen als IKT-Drittdienstleister im Sinne DORA 187
20.5. Cyber Resilience Act (CRA) 187
20.5.1. Allgemeines 187
20.5.2. Anwendungsbereich 188
20.5.3. Verhältnis zum NISG 188
20.6. Artificial Intelligence Act (AI Act) 188
20.6.1. Allgemeines 188
20.6.2. Anwendungsbereich 189
20.6.3. Verhältnis zum NISG 189

21. Freiwillige Nachweise, Zertifizierungen und Standards 189
21.1. Allgemeines 189
21.1.1. ISO/IEC 27001 als Grundlage für die Umsetzung des NISG 189
21.1.2. Verhältnis zwischen ISO/IEC 27001 und NISG 190
21.1.3. Aussagekraft einer ISO/IEC-27001-Zertifizierung ... 190
21.1.4. Ist eine ISO/IEC-27001-Zertifizierung sinnvoll? 191
21.2. BSI Grundschutz 191
21.3. Europäische Entwicklungen und das Cyber-Risk-Rating-Schema 192
21.3.1. Das KSV1870 CyberRisk Rating und das Cyber Trust Austria Label 193
21.3.2. Einsatz in der Praxis 194
21.3.3. Nutzen für wesentliche und wichtige Einrichtungen 194
21.3.4. Nutzen für indirekt vom NISG betroffene Unternehmen 195
21.3.5. Grenzen und Risiken 195

21.4. Cyber Trust Platinum Label 195
21.5. Die Rolle externer Experten 196
21.5.1. Nutzen externer Experten 196
21.5.2. Grenzen externer Experten 196
21.5.3. Personenzertifizierung Certified NIS Expert 197

Teil 2:
Cybersicherheit wirksam verankern – vom NISG zur operativen Realität

22. Warum Cybersicherheit im Tagesgeschäft entscheidet 199
22.1. Warum Cybersicherheit im Alltag oft nicht funktioniert 199
22.2. Ziel: Cybersicherheit im Unternehmen wirksam verankern 199
22.3. Zusammenspiel von Organisation, Prozessen und Menschen ... 200
22.4. Methodik im operativen Teil: WHAT – WHY – HOW 201
22.5. Was Leserinnen und Leser im operativen Teil erwarten können ... 202

23. Warum Cybersicherheit ohne KVP im operativen Alltag scheitert ... 202
23.1. Cybersicherheit als dynamischer Anpassungsprozess 203
23.2. Grenzen dokumentengetriebener Ansätze 205
23.3. Papiertiger zwischen Audit und Realität 207
23.4. Kontinuierliche Verbesserung als Anforderung des NISG 208

24. Lean-Prinzipien als Grundlage wirksamer Cybersicherheit 209
24.1. Wert definieren: Kundenwert als Maßstab für Sicherheit 210
24.2. Wertstrom verstehen: Informationsflüsse als Grundlage jeder Kundenzufriedenheit 211
24.3. Flussprinzip: Sicherheit an den Übergaben zwischen Prozessschritten 211
24.4. Pull-Prinzip: Nur was tatsächlich benötigt wird 212
24.5. Kontinuierliche Verbesserung: Der Kreislauf, der alles zusammenhält 212
24.6. Vokabular und Werkzeuge in der Praxis 213

25. Zielbild: Informationssicherheit entlang des gesamten Wertstroms 218
25.1. Integration in Geschäftsprozesse und Entscheidungen 218
25.2. Sicherheit als Teil der täglichen Arbeit 219
25.3. Auflösung von Silodenken und isolierten Strukturen 220

26. Kontinuierliche Verbesserung als Steuerungs- und Integrationssystem 222
26.1. KVP als verbindendes System im Unternehmen 222
26.2. Standards als Grundlage der kontinuierlichen Verbesserung 223
26.3. Reparatur versus Verbesserung: Der PDCA-Zyklus im Detail ... 225
26.4. Sichtbarkeit durch Visualisierung und Kennzahlen 227
26.5. KVP und regulatorische Anforderungen 228

27. Verantwortung im Unternehmen: Sicherheit beginnt im Prozess ... 229
27.1. Experte für den eigenen Prozess: Probleme erkennen und lösen ... 229
27.2. Verantwortung für Entscheidungen ... 231
27.3. Verantwortung, Kompetenz und Handlungsspielraum ... 232

28. Einbindung in das operative Tagesgeschäft ... 233
28.1. Zusammenarbeit über Abteilungsgrenzen als internes Kunden-Lieferanten-Verhältnis ... 234
28.2. Empathischer Pragmatismus: Bedürfnisse verstehen ... 235
28.3. Entwicklung praktikabler Lösungen und Rollout ... 236

29. Human Systems Engineering: Der Mensch als Hebel für Informationssicherheit ... 238
29.1. Human Factor: vom Risikofaktor zur Wirksamkeit ... 238
29.2. Warum ein fundiertes Verständnis des Menschen jede Facette der Informationssicherheit betrifft ... 238
29.3. Der Decision Loop: Wie Entscheidungen im Gehirn entstehen ... 239
29.4. Poka-Yoke: Fehler unmöglich machen ... 241
29.5. Aufmerksamkeit erhalten: Pausen als Informationssicherheitsmaßnahme ... 242
29.6. Ausblick: Verhaltensbiometrie und neuronale Überwachung ... 243

30. Eigenverantwortung und Eigenmotivation ... 244
30.1. Cybersicherheit als Ergebnis individueller Entscheidungen ... 244
30.2. Die Komfortzonen-Leiter: von „Muss“ zu „Bin“ ... 245
30.3. Eigenverantwortung und Identifikation im Arbeitsalltag fördern ... 247
30.4. Rahmenbedingungen für wirksames Handeln ... 248

31. Wie Menschen Sicherheitsentscheidungen treffen ... 249
31.1. Das Gehirn als Informationssicherheitssystem ... 249
31.2. Wie wir lernen: die vier Säulen wirksamer Awareness ... 251
31.3. Weltmodelle als schützenswerte Infrastruktur ... 252
31.4. Der neurobiologische Sicherheitsregelkreis ... 253

32. Risikowahrnehmung und Entscheidungsverhalten unter Druck ... 254
32.1. Warum Risikoeinschätzung unter Stress selten rational ist ... 254
32.2. Risiken erkennen: Wo entstehen Gefährdungen ... 256
32.3. Risikobewusstsein als Aufgabe aller Mitarbeiter ... 257
32.4. Risikomanagement als gelebte Kompetenz ... 258

33. Fehlerkultur, Vertrauensbrüche und Lernen aus Vorfällen ... 260
33.1. Vertrauen nach einem Vorfall gemeinsam wiederherstellen ... 260
33.2. Die Heinrich-Pyramide übertragen auf Cybersicherheit ... 261
33.3. Melde- und Eskalationsstrukturen für Cybersicherheit ... 262
33.4. Lernen aus Fehlern und Sicherheitsvorfällen ... 263

34. Führung, psychologische Sicherheit und Sicherheitskultur 265
34.1. Klare Zielvorgaben und Managementsysteme als Rahmen 265
34.2. Vorbildwirkung und kulturelle Verankerung 266
34.3. Psychologische Sicherheit als Führungsaufgabe 267
34.4. Von der Komfortzone zur Sicherheitskultur: „Ich bin Teil der Sicherheitsarchitektur“ 268

35. Fachkräftemangel in der Informationssicherheit: Anforderungsprofil und Vielfalt als Antwort 270
35.1. Die Anforderungen: Welche Kompetenzen machen in der Informationssicherheit erfolgreich? 270
35.2. Frauen in der Informationssicherheit: Karrierechancen an einer Schlüssel-Schnittstelle 270

36. Gelebte Informationssicherheit in der ganzen Organisation 272
36.1. Klare Ansprechpartner für Cybersicherheit 272
36.2. Sichtbarkeit vergleichbar mit Qualität und Arbeitssicherheit 273
36.3. Verankerung im organisatorischen Alltag 274
36.4. SQDCM: Informationssicherheit im bestehenden Reporting- und Meetingschema verankern 275
36.5. Steuerungskennzahlen: KAI und KPI für Informationssicherheit 277
36.6. Von lernenden Menschen zu einer lernenden Organisation 278

37. Umsetzung in unterschiedlichen Unternehmensrealitäten 279
37.1. Kleinst- und Kleinunternehmen ohne eigene IT-Sicherheitsexpertise: Auslagerung an externe IT-Sicherheitsexperten 280
37.2. Unternehmen ohne strukturierte Prozesse 282
37.3. Integration in bestehende Systeme 282
37.4. Skalierung und Weiterentwicklung 284

38. Leitlinien und Kernaussagen 285
38.1. Wirksamkeit vor Formalität 285
38.2. Integration vor Parallelstruktur 285
38.3. Verantwortung, Sichtbarkeit und Einbindung als Erfolgsfaktoren 286

Anhang 1 NISG 2026 289

Anhang 2 Schummelzettel NISG 347

Stichwortverzeichnis 351