

# Inhaltsverzeichnis

Vorwort .....	V
---------------	---

Abkürzungsverzeichnis .....	XXV
-----------------------------	-----

## Teil 1 Die bisherige Entwicklung

### A. Das IT-Sicherheitsgesetz 1.0

I. Stärkung der IT-Sicherheit Kritischer Infrastrukturen .....	2
1. Was sind Kritische Infrastrukturen? .....	3
2. Staatliche Maßnahmen zum Schutz Kritischer Infrastrukturen .....	5
3. Verpflichtungen für Betreiber Kritischer Infrastrukturen .....	5
a) Absicherungs- und Nachweispflichten des § 8a BSIG .....	6
b) Meldepflichten des § 8b BSIG .....	7
c) Bußgeldbefugnis – § 14 BSIG .....	9
d) Absicherungspflichten des § 109 TKG .....	9
e) Meldepflichten des § 109 TKG .....	11
f) Absicherungspflichten des § 11 EnWG .....	11
g) Meldepflichten des § 11 EnWG .....	13
h) Meldepflichten nach § 44b AtG .....	14
II. Stärkung der IT-Sicherheit der Bundesverwaltung .....	14
III. Stärkung der IT-Sicherheit für die Allgemeinheit .....	16
1. Verpflichtung der Telemediendiensteanbieter zur Absicherung der IT – § 13 Abs. 7 TMG .....	16
2. Angriffsdetektion in TK-Netzen – § 100 TKG .....	18
3. Verpflichtung der TK-Anbieter zur Warnung der Nutzer – § 109a TKG .....	19
4. Klarstellung zu Umfang und Rahmen der Warnbefugnis – § 7 BSIG .....	20
5. Befugnis des BSI für Reverse-Engineering – § 7a BSIG .....	21

### B. Das NIS-RL-Umsetzungsgesetz

I. Neue Aufgaben für das BSI .....	23
1. Unterstützung des MAD .....	23
2. Unterstützung bestimmter Stellen der Länder .....	24
3. Neue Berichts- und Konsultationsaufgaben .....	24
II. Neue Befugnisse des BSI .....	25
1. Mobile Incident Response Teams – § 5a BSIG .....	26
2. Anordnung ggü. Herstellern bei MIRT-Einsätzen .....	28
3. Erweiterte Weitergabemöglichkeiten für § 5-Daten .....	29

III.	Änderungen für KRITIS . . . . .	30
1.	Absicherungs- und Nachweispflichten in § 8a BSIG . . . . .	30
2.	Meldepflichten in § 8b BSIG . . . . .	31
3.	Meldepflichten in AtG, TKG und EnWG . . . . .	32
4.	Neue Pflichten und Befugnisse im Bereich der Telematikinfrastruktur nach § 291b Abs. 8 SGB . . . . .	33
IV.	Anbieter digitaler Dienste – § 8c BSIG . . . . .	34
V.	Weitere Regelungen zur Erhöhung der IT-Sicherheit . . . . .	36
1.	Erweiterung der Analysemöglichkeiten für TK-Anbieter – § 100 Abs. 1 TKG . . . . .	37
2.	Neue Befugnisse für Walled Gardens – § 109a Abs. 4 TKG . . . . .	38
3.	Neue Befugnisse zur Beschränkung der Nutzung – § 109a Abs. 5 TKG . . . . .	39
4.	Neue Befugnis zur Einschränkung des Datenverkehrs – § 109a Abs. 6 TKG . . . . .	40

## Teil 2

### Kommentierung der durch das IT-Sicherheitsgesetz 2.0 betroffenen Gesetzestexte

#### Art. 1 Änderungen im BSI-Gesetz (BSIG)

<b>§ 1</b>	<b>Bundesamt für Sicherheit in der Informationstechnik . . . . .</b>	41
I.	Gesetzesbegründung (BT-Drs. 19/28844, 39) . . . . .	41
II.	Kommentierung . . . . .	41
1.	Kurzzusammenfassung . . . . .	41
2.	Einzelerläuterungen . . . . .	42
<b>§ 2</b>	<b>Begriffsbestimmungen . . . . .</b>	43
I.	Gesetzesbegründung . . . . .	48
1.	Regierungsentwurf (BT-Drs. 19/26106, 56 ff.) . . . . .	48
2.	Beschlusssempfehlungen des Innenausschusses (BT-Drs. 19/28844, 39) . . . . .	53
II.	Kommentierung . . . . .	54
1.	Hintergrund der Norm . . . . .	54
2.	Einzelerläuterungen . . . . .	54
a)	Absatz 2 – Sicherheit der Informationstechnik . . . . .	54
b)	Absatz 3 – Kommunikationstechnik des Bundes . . . . .	54
c)	Absatz 8a – Protokollierungsdaten . . . . .	55
d)	Absatz 9a – IT-Produkte . . . . .	55
e)	Absatz 9b – Systeme zur Angriffserkennung . . . . .	55
aa)	Zielrichtung . . . . .	56
bb)	Prozesshaftigkeit . . . . .	56

cc) Technische Werkzeuge und organisatorische Einbindung .....	57
f) Absatz 10 – Kritische Infrastrukturen .....	57
g) Absatz 13 – Kritische Komponenten .....	59
aa) Bedeutung von Abs. 13 Nr. 1 und 2 .....	60
bb) Kontext der „lex Huawei“ .....	61
cc) Das „Potenzial“ der Auswirkung einer Störung genügt .....	61
dd) Vorläufig nur kritische Komponenten im Telekommunikationssektor .....	62
ee) Rechtsklarheit durch Satz 2 und Zitiergebot .....	62
h) Absatz 14 – Unternehmen im besonderen öffentlichen Interesse .....	62
aa) Allgemeines .....	62
bb) Rüstungsindustrie und Verschlussachen (§ 2 Abs. 14 S. 1 Nr. 1) .....	64
cc) Unternehmen von erheblicher volkswirtschaftlicher Bedeutung (§ 2 Abs. 14 S. 1 Nr. 2) .....	65
dd) Betreiber eines Betriebsbereichs der oberen Klasse der Störfall-Verordnung (§ 2 Abs. 14 S. 1 Nr. 3) .....	67
<b>§ 3 Aufgaben des Bundesamtes</b> .....	68
I. Gesetzesbegründung .....	71
1. RegE (BT-Drs. 19/26106, 58 ff.) .....	71
2. Begründung der Beschlussempfehlungen des Innenausschusses (BT-Drs. 19/28844, 39 f.) .....	76
II. Kommentierung .....	77
1. Kurzzusammenfassung .....	77
2. Zweck und Hintergrund der Norm .....	77
3. Systematik .....	78
4. Einzelerläuterungen .....	78
<b>§ 4a Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte</b> .....	83
I. Gesetzesbegründung .....	85
1. RegE (BT-Drs. 19/26106, 60 f.) .....	85
2. Beschlussempfehlungen des Innenausschusses (BT-Drs. 19/28844, 40) .....	86
II. Kommentierung .....	87
1. Zusammenfassung .....	87
2. Hintergrund der Norm .....	87
3. Systematik .....	88
4. Einzelerläuterungen .....	88
a) Absatz 1 – Kontrollbefugnisse .....	88

b)	Absatz 2 – Vor-Ort-Kontrollen . . . . .	89
c)	Absatz 3 – Schnittstellenkontrolle . . . . .	90
d)	Absatz 4 – Untersuchungsergebnisse . . . . .	91
e)	Absatz 5 und 6 – Ausnahmen. . . . .	91
5.	Praxisempfehlungen und Rechtsschutz . . . . .	91
<b>§ 4b</b>	<b>Allgemeine Meldestelle für die Sicherheit in der Informationstechnik . . . . .</b>	93
I.	Gesetzesbegründung . . . . .	94
1.	RegE (BT-Drs. 19/26106, 62 f.) . . . . .	94
2.	Begründung der Beschlussempfehlung des Innenausschusses (BT-Drs. 19/28844, 40). . . . .	96
II.	Kommentierung. . . . .	96
1.	Kurzzusammenfassung . . . . .	96
2.	Zweck und Hintergrund der Norm . . . . .	97
3.	Einzelerläuterungen. . . . .	98
a)	Das BSI als allgemeine Meldestelle (Abs. 1) . . . . .	98
b)	Sicherheitsrisiken der Informationstechnik; Das BSI wird keine allgemeine Beschwerdestelle . . . . .	98
c)	Geeignete und anonyme Meldemöglichkeiten. . . . .	99
d)	Datenschutz für Meldende (Abs. 2) . . . . .	100
e)	Verwendung und Weitergabe der gemeldeten Informationen (Abs. 3) . . . . .	101
f)	Ermessen oder Verpflichtung? . . . . .	102
g)	Mitteilung an die Öffentlichkeit nur nach Abstimmung mit der zuständigen Aufsichtsbehörde . . . . .	103
h)	Datenschutzrechtlicher Erlaubnistatbestand . . . . .	104
i)	Ausnahmen zur Informationsweitergabe nach Absatz 3 (Abs. 4) . . . . .	104
j)	Klarstellung, dass andere Vorschriften unberührt bleiben (Abs. 5) . . . . .	105
<b>§ 5</b>	<b>Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes . . . . .</b>	106
I.	Gesetzesbegründung . . . . .	111
1.	Regierungsentwurf (BT-Drs. 19/26106, 62 ff.) . . . . .	111
2.	Beschlussempfehlungen des Innenausschusses (BT-Drs. 19/28844, 40 f.) . . . . .	112
II.	Kommentierung. . . . .	113
1.	Zusammenfassung . . . . .	113
2.	Hintergrund der Norm . . . . .	113
3.	Systematik . . . . .	114
4.	Einzelerläuterungen. . . . .	114
<b>§ 5a</b>	<b>Verarbeitung behördeneinterner Protokollierungsdaten . . . . .</b>	117
I.	Gesetzesbegründung (BT-Drs. 19/26106, 64 ff.) . . . . .	117

II.	Kommentierung . . . . .	119
1.	Zusammenfassung . . . . .	119
2.	Hintergrund der Norm . . . . .	119
3.	Systematik . . . . .	119
4.	Einzelerläuterungen . . . . .	119
a)	Schutzgüter- und Gefahrenbegriff . . . . .	119
b)	Daten, die verarbeitet werden dürfen . . . . .	120
c)	Zweckbindung . . . . .	121
d)	Ausnahme Geheimschutzinteressen . . . . .	121
e)	Unterstützungspflicht der Bundesbehörden (Satz 2) . . . . .	122
f)	Befugnis zur Übermittlung von Protokollierungsdaten (Satz 3) . . . . .	122
g)	Entsprechend anzuwendende Vorschriften (Satz 4) . . . . .	122
<b>§ 5b</b>	<b>Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen . . . . .</b>	124
I.	Gesetzesbegründung . . . . .	126
1.	RegE (BT-Drs. 19/26106, 64) . . . . .	126
2.	Begründung der Beschlussempfehlung des Innenausschusses (BT-Drs. 19/28844, 41) . . . . .	126
II.	Kommentierung . . . . .	126
1.	Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme (Abs. 1) . . . . .	126
2.	Definition des herausgehobenen Falls (Abs. 2) . . . . .	127
3.	Verarbeitung personenbezogener oder dem Fernmeldegeheimnis unterliegender Daten (Abs. 3) . . . . .	127
4.	Weitergabe von Informationen (Abs. 4) . . . . .	129
5.	Hilfe durch qualifizierte Dritte (Abs. 5) . . . . .	129
6.	Mitwirkungspflichten (Abs. 6) . . . . .	130
7.	Tätigkeitsersuchen anderer Einrichtungen, insbesondere Stellen des Landes (Abs. 7) . . . . .	131
8.	Anlagen und Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen (Abs. 8) . . . . .	131
<b>§ 5c</b>	<b>Bestandsdatenauskunft . . . . .</b>	132
I.	Gesetzesbegründungen . . . . .	134
1.	RegE (BT-Drs. 19/26106, 64 ff.) . . . . .	134
2.	Änderungsempfehlungen des Ausschusses für Inneres und Heimat (BT-Drs. 19/28844, 41) . . . . .	138
II.	Kommentierung . . . . .	138
1.	Zusammenfassung . . . . .	138
2.	Einzelerläuterungen . . . . .	139
a)	Bestandsdatenauskunft (Abs. 1) . . . . .	139
b)	Auskunft auf Grundlage von IP-Adressen (Abs. 2) . . . . .	141
c)	Auskunftserteilung (Abs. 3) . . . . .	141

d) Inkennisssetzung von betroffenen Stellen (Abs. 4) .....	142
e) Datenschutzrechtliche Übermittlungsermächtigung (Abs. 5) .....	142
f) Benachrichtigung betroffener Personen (Abs. 6).....	142
g) Berichtspflicht gegenüber dem BfDI (Abs. 7) .....	143
h) Entschädigung für Auskünfte (Abs. 8).....	143
<b>§ 7 Warnungen .....</b>	<b>144</b>
I. Gesetzesbegründungen .....	145
1. RegE (BT-Drs. 19/26106, 67) .....	145
2. Änderungsempfehlungen des Ausschusses für Inneres und Heimat (BT-Drs. 19/28844, 41) .....	146
II. Kommentierung.....	146
1. Zusammenfassung .....	146
2. Hintergrund .....	147
3. Systematik .....	147
4. Einzelerläuterungen .....	148
a) Allgemeine Warnungen und Informationen (Abs. 1).....	148
b) Informationspflichten und Ausnahmen (Abs. 1a) .....	150
c) Warnung unter Nennung der Bezeichnung und des Herstellers betroffener Produkte und Dienste (Abs. 2) .....	152
5. Praktische Hinweise .....	153
<b>§ 7a Untersuchung der Sicherheit in der Informationstechnik .....</b>	<b>156</b>
I. Gesetzesbegründung .....	157
1. RegE (BT-Drs. 19/26106, 67 f.) .....	157
2. Begründung der Beschlussempfehlung des Innenausschusses (BT-Drs. 19/28844, 41). ....	159
II. Kommentierung.....	159
1. Kurzzusammenfassung .....	159
2. Untersuchungsbefugnis und Privilegierung des BSI (Abs. 1).....	160
3. Auskunftsverlangen (Abs. 2) .....	161
4. Weitergabe der Informationen (Abs. 3) .....	162
5. Zweckbindung (Abs. 4) .....	162
6. Information der Öffentlichkeit (Abs. 5).....	162
7. Sicherheitslücken als „Mangel“ und Kooperation des BSI mit Verbänden als Ansatzpunkt für eine Stärkung der IT-Sicherheit.....	163
<b>§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden .....</b>	<b>165</b>
I. Gesetzesbegründung .....	166
1. RegE (BT-Drs. 19/26106, 60 ff.) .....	166

2. Begründung der Beschlussempfehlung des Innenausschusses (BT-Drs. 19/28844, 41) . . . . .	171
<b>II. Kommentierung . . . . .</b>	<b>172</b>
1. Einleitung . . . . .	172
a) Zusammenfassung . . . . .	172
b) Warum die umstrittene Regelung in der Praxis kaum eine Rolle spielen wird. . . . .	173
2. Befugnis zur Durchführung von Portscans (Abs. 1) . . . . .	174
a) Abgrenzung zu § 7a BSIG . . . . .	174
b) An welchen „Schnittstellen“ dürfen Maßnahmen durchgeführt werden. . . . .	175
c) Welche „Maßnahmen“ darf der Portscan umfassen. . . . .	175
d) Das Konzept der Whitelist . . . . .	176
e) Behandlung ungewollt übermittelter Daten . . . . .	177
3. Vorliegen eines ungeschützten Systems und einer Gefahr (Abs. 1 S. 1 und Abs. 2) . . . . .	178
4. Information des Verantwortlichen (Abs. 3) . . . . .	179
5. Befugnis zum Einsatz „aktiver Honeypots“ (Abs. 4) . . . . .	180
6. Privilegierungswirkung . . . . .	181
<b>§ 7c Anordnungen des Bundesamtes gegenüber Diensteanbietern . . . . .</b>	<b>182</b>
<b>I. Gesetzesbegründung RegE (BT-Drs. 19/26106, 71 ff.) . . . . .</b>	<b>183</b>
<b>II. Kommentierung . . . . .</b>	<b>191</b>
1. Kurzzusammenfassung und Bedeutung . . . . .	191
2. Anordnungssubjekt: Telekommunikationsdienstleister (Abgrenzung zu § 7d) . . . . .	192
a) Definition im TKG . . . . .	192
b) Streitfälle zur Definition . . . . .	192
d) Hinweis auf TKG-Reform (Wirkung zum 1.12.2021) . . . . .	193
e) Streitfall: Sind Arbeitgeber TK-Anbieter? . . . . .	194
f) Schwellenwert von 100.000 Teilnehmern für KRITIS-Anbieter im TK-Sektor . . . . .	195
3. Neuartigkeit der Eingriffsbefugnis und Gesetzgebungs-kompetenz . . . . .	195
4. Anordnung an Telekommunikationsanbieter (Abs. 1) . . . . .	195
a) Anordnungen nach § 109a Abs. 5 und 6 TKG (Nr. 1) . . . . .	196
b) Technische Befehle zur Bereinigung (Nr. 2) . . . . .	197
c) Kritik . . . . .	199
5. Bußgeld . . . . .	199
6. Schutzziele (Abs. 2) . . . . .	199
7. Umleitung des Datenverkehrs (Abs. 3) . . . . .	200
8. Verarbeitung umgeleiteter Daten (Abs. 4) . . . . .	200

<b>§ 7d Anordnungen des Bundesamtes gegenüber Anbietern von Telemmediendiensten</b>	201
I. Gesetzesbegründung (RegE BT-Drs. 19/26106, 76 f.)	201
II. Kommentierung	205
1. Kurzzusammenfassung	205
2. Hintergrund der Norm	205
3. Systematik	205
4. Einzelerläuterungen	206
a) Telemedium (§ 1 Abs. 1 S. 1 TMG)	206
b) Diensteanbieter (§ 2 S. 1 Nr. 1 TMG)	206
c) Diensteanbieter als Normadressat des § 13 Abs. 7 TMG	207
d) Unzureichende Umsetzung der in § 13 Abs. 7 TMG normierten Vorkehrungen	208
e) Geschaffene konkrete Gefahr für informations- technische Systeme	208
f) Vielzahl von Nutzern	209
g) Die Anordnung des Bundesamts für Sicherheit in der Informationstechnik	210
h) Aufsichtsbehörden der Länder	210
<b>§ 8 Vorgaben des Bundesamtes</b>	211
I. Gesetzesbegründung	213
1. Regierungsentwurf (BT-Drs. 19/26106, 78)	213
2. Beschlussempfehlungen des Innenausschusses (BT-Drs. 19/28844, 41)	214
II. Kommentierung	215
1. Zusammenfassung	215
2. Einzelerläuterungen	215
a) § 8 Abs. 1	215
b) § 8 Abs. 1a	216
c) § 8 Abs. 3	217
d) § 8 Abs. 4	217
<b>§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen</b>	218
I. Gesetzesbegründung	219
1. RegE (BT-Drs. 19/26106, 79 f.)	219
2. Änderungsempfehlungen des Ausschusses für Inneres und Heimat (BT-Drs. 19/28844, 41 f.)	221
II. Kommentierung	222
1. Zusammenfassung	222
2. Hintergrund	223
3. Systematik	223
4. Einzelerläuterungen	223

a) Technische und organisatorische Sicherungsvorkehrungen (Abs. 1) . . . . .	223
b) Systeme zur Angriffserkennung (Abs. 1a) . . . . .	227
c) Branchenspezifische Standards (Abs. 2) . . . . .	230
d) Nachweispflichten (Abs. 3) . . . . .	230
e) Überprüfungsrecht (Abs. 4) . . . . .	231
5. Praktische Hinweise . . . . .	231
<b>§8b Zentrale Stelle für die Sicherheit in der Informationstechnik</b>	
<b>Kritischer Infrastrukturen</b> . . . . .	233
I. Gesetzesbegründungen (BT-Drs. 19/26106, 80 f.) . . . . .	235
II. Kommentierung . . . . .	237
1. Zusammenfassung . . . . .	237
2. Hintergrund . . . . .	238
3. Einzelerläuterungen . . . . .	238
a) Zentrale Meldestelle für die Informationssicherheit (Abs. 1) . . . . .	238
b) Aufgabenzuweisungen (Abs. 2) . . . . .	238
c) Kontaktstelle und Registrierungspflicht (Abs. 3, Abs. 3a und Abs. 5) . . . . .	239
aa) Kontaktstelle . . . . .	239
bb) Registrierung . . . . .	239
d) Meldepflichten (Abs. 4) . . . . .	242
e) Informationspflichten im Zusammenhang mit erheblichen Sicherheitsvorfällen (Abs. 4a) . . . . .	243
f) Mitwirkungspflichten von Herstellern (Abs. 6) . . . . .	244
4. Praktische Hinweise . . . . .	245
a) Rechtsschutz gegen Registrierung . . . . .	245
b) Ordnungswidrigkeiten . . . . .	245
<b>§8c Besondere Anforderungen an Anbieter digitaler Dienste</b> . . . . .	246
I. Gesetzesbegründungen RegE (BT-Drs. 19/26106, 81) . . . . .	248
II. Kommentierung . . . . .	248
<b>§8d Anwendungsbereich</b> . . . . .	249
I. Gesetzesbegründungen . . . . .	251
1. RegE (BT-Drs. 19/26106, 81) . . . . .	251
2. Beschlussempfehlungen des Innenausschusses (BT-Drs. 19/28844, 42) . . . . .	251
II. Kommentierung . . . . .	251
1. Zusammenfassung . . . . .	251
2. Hintergrund . . . . .	251
3. Systematik . . . . .	252
4. Einzelerläuterungen . . . . .	252

a) Unternehmen im besonderen öffentlichen Interesse als Kleinstunternehmen und kleine Unternehmen (Abs. 1a) . . . . .	252
b) Ausnahme von Meldeverpflichtungen (Abs. 3) . . . . .	253
5. Praktische Empfehlungen . . . . .	255
<b>§ 8e Auskunftsverlangen . . . . .</b>	<b>256</b>
I. Gesetzesbegründung . . . . .	256
1. RegE (BT-Drs. 19/26106, 81) . . . . .	256
2. Änderungsempfehlungen des Ausschusses für Inneres und Heimat (BT-Drs. 19/28844, 42) . . . . .	257
II. Kommentierung . . . . .	257
1. Zusammenfassung . . . . .	257
2. Systematik . . . . .	257
3. Einzelerläuterungen . . . . .	258
a) Auskunft gegenüber Dritten (Abs. 1) . . . . .	258
b) Akteneinsichtsrecht von Beteiligten (Abs. 2) . . . . .	260
c) Informationsansprüche nach dem Umweltinformationsgesetz (Abs. 4) . . . . .	261
<b>§ 8f Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse . . . . .</b>	<b>262</b>
I. Gesetzesbegründungen (BT-Drs. 19/26106, 81 ff.) . . . . .	264
II. Kommentierung . . . . .	267
1. Zusammenfassung . . . . .	267
2. Hintergrund . . . . .	268
3. Einzelerläuterungen . . . . .	269
a) Selbsterklärungspflicht (Abs. 1, Abs. 2 und Abs. 3) . . . . .	269
b) Registrierungspflichten und Pflicht zur Benennung einer Kontaktstelle (Abs. 5, Abs. 6 und Abs. 9) . . . . .	270
c) Umsetzungsfrist (Abs. 4 und Abs. 5) . . . . .	272
d) Störungsmeldung (Abs. 7 und Abs. 8) . . . . .	273
e) Informationspflichten im Zusammenhang mit erheblichen Sicherheitsvorfällen (§ 8b Abs. 4a) . . . . .	276
4. Praktische Empfehlungen . . . . .	277
<b>§ 9 Zertifizierung . . . . .</b>	<b>278</b>
I. Gesetzesbegründung RegE (BT-Drs. 19/26106, 83) . . . . .	279
II. Kommentierung . . . . .	279
1. Zusammenfassung . . . . .	279
2. Einzelerläuterungen . . . . .	279
a) Voraussetzungen der Erteilung des Sicherheitszertifikats . . . . .	279
b) Keine Untersagung der Zertifikatserteilung durch das Bundesministerium des Innern, für Bau und Heimat . . . . .	279

3. Praktische Hinweise .....	280
<b>§ 9a Nationale Behörde für die Cybersicherheitszertifizierung</b> .....	<b>281</b>
I. Gesetzesbegründung .....	283
1. RegE (BT-Drs. 19/26106, 83) .....	283
2. Begründung der Beschlussempfehlungen des Ausschusses für Inneres und Heimat (BT-Drs. 19/28844, 42) .....	284
II. Kommentierung .....	284
1. Zusammenfassung .....	284
2. Hintergrund der Norm .....	284
3. Einzelerläuterungen .....	285
a) Das BSI als nationale Behörde für die Cyber- sicherheitszertifizierung (Abs. 1) .....	285
b) Befugniserteilung für Konformitätsbewertungs- stellen (Abs. 2) .....	285
aa) Konformitätsbewertungsstellen .....	286
bb) Aufgaben der Konformitätsbewertungsstellen .....	286
cc) Voraussetzungen für die Befugniserteilung nach der Verordnung (EU) 2019/881 .....	287
dd) Befugniserteilung durch das BSI .....	291
ee) Notifikation nach Art. 61 VO (EU) 2019/881 .....	291
c) Anspruch auf Auskunft und sonstige Unter- stützungsleistungen (Abs. 3) .....	291
d) Auditierungen zur Gewährleistung des Zertifi- zierungsrahmens für Cybersicherheit (Abs. 4) .....	292
e) Betretungs- und Kontrollbefugnisse des BSI (Abs. 5) .....	292
f) Widerruf eines Cybersicherheitszertifikats (Abs. 6) .....	293
g) Widerruf von Befugnissen für Konformitätsbewertungs- stellen (Abs. 7) .....	293
<b>§ 9b Untersagung des Einsatzes kritischer Komponenten</b> .....	<b>295</b>
I. Gesetzesbegründung .....	299
1. RegE (BT-Drs. 19/26106, 83 ff.) .....	299
2. Begründung der Beschlussempfehlung des Innenausschusses (BT-Drs. 19/28844, 42 ff.) .....	304
II. Kommentierung .....	309
1. Kurzzusammenfassung .....	309
a) Ziel der „lex Huawei“ .....	309
b) Zweifel an der Praxisrelevanz .....	309
2. Verpflichtung des Betreibers zur Anzeige kritischer Komponenten (Abs. 1) .....	310
a) Es ist nicht jedes einzelne „Exemplar“ anzeigepflichtig .....	311

b)	Keine Verpflichtung zur Anzeige für Hersteller und Importeure . . . . .	312
c)	Keine rückwirkende Verpflichtung für bereits bestehenden Einsatz . . . . .	312
d)	Ausnahme für den Einsatz desselben Typs zur selben Art des Einsatzes (Abs. 1 S.3) . . . . .	313
aa)	Bedeutet „Typ“ „Gattung“ oder „Typenbezeichnung des Herstellers“ . . . . .	313
bb)	Art des Einsatzes . . . . .	314
3.	Anordnungsbefugnis und Untersagungsbefugnis (Abs. 2) . . . . .	315
a)	Zuständige Behörde und Benehmenserfordernis . . . . .	315
b)	Tatbestandliche Voraussetzung für Befugnisse . . . . .	315
aa)	Kontrolle über den Hersteller . . . . .	317
bb)	Bisherige Beteiligung des Herstellers an Sicherheitsrisiken der westlichen Welt . . . . .	317
cc)	Übereinstimmung des Einsatzes der kritischen Komponente mit sicherheitspolitischen Zielen . . . . .	317
c)	Frist . . . . .	318
4.	Garantieerklärung des Herstellers (Abs. 3) . . . . .	318
a)	Zur zeitlichen Geltung der Verpflichtung der Betreiber . . . . .	318
b)	Auswirkung auf die Vertragspraxis . . . . .	319
5.	Ex-post-Regulierung (Abs. 4) . . . . .	319
6.	Gründe für mangelnde Vertrauenswürdigkeit (Abs. 5) . . . . .	319
7.	Weitere Folgen (Abs. 6 und 7) . . . . .	320
<b>§ 9c</b>	<b>Freiwilliges IT-Sicherheitskennzeichen</b> . . . . .	321
I.	Gesetzesbegründung . . . . .	323
1.	RegE (BT-Drs. 19/26106, 86 f.) . . . . .	323
2.	Änderungen durch den Ausschuss für Inneres und Heimat (BT-Drs. 19/28844, 45) . . . . .	327
II.	Kommentierung . . . . .	328
1.	Zusammenfassung . . . . .	328
2.	Systematik . . . . .	328
3.	Einzelerläuterungen . . . . .	329
a)	Einführung des freiwilligen IT-Sicherheitskennzeichens (Abs. 1) . . . . .	329
b)	Komponenten des IT-Sicherheitskennzeichens (Abs. 2) . . . . .	331
aa)	Die Herstellererklärung (Nr. 1) . . . . .	331
bb)	Die dynamische Sicherheitsinformation (Nr. 2) . . . . .	333
c)	Anforderungen in Bezug auf die IT-Sicherheit (Abs. 3) . . . . .	334

d) Verfahrensvorgaben für die Freigabe durch das BSI (Abs. 4) . . . . .	335
e) Voraussetzungen für die Erteilung der Freigabe des IT-Sicherheitskennzeichens (Abs. 5) . . . . .	336
f) Anbringung des IT-Sicherheitskennzeichens (Abs. 6) . . . . .	337
g) Erlöschen der Freigabe (Abs. 7) . . . . .	339
h) Prüf- und Widerrufsrecht des BSI (Abs. 8) . . . . .	340
i) Verfahrensvorgaben für die Maßnahmen nach Abs. 8 (Abs. 9) . . . . .	341
<b>§ 10 Ermächtigung zum Erlass von Rechtsverordnungen</b> . . . . .	342
I. Gesetzesbegründung . . . . .	344
1. Regierungsentwurf (BT-Drs. 19/26106, 88 f.) . . . . .	344
2. Beschlussempfehlungen des Innenausschusses (BT-Drs. 19/28844, 45) . . . . .	345
II. Kommentierung . . . . .	346
1. Zusammenfassung . . . . .	346
2. Einzelerläuterungen . . . . .	346
a) Absatz 3 – IT-Sicherheitskennzeichen . . . . .	346
b) Absatz 5 – Unternehmen im besonderen öffentlichen Interesse und Zulieferer . . . . .	347
aa) Allgemeines . . . . .	347
bb) Unternehmen von erheblicher volkswirtschaftlicher Bedeutung . . . . .	347
cc) Zulieferer . . . . .	349
dd) Probleme . . . . .	350
ee) Voraussetzungen für den Erlass der Verordnung . . . . .	350
<b>§ 11 Einschränkung von Grundrechten</b> . . . . .	352
I. Gesetzesbegründung (RegE BT-Drs. 19/26106, 89) . . . . .	352
II. Kommentierung . . . . .	352
1. Kurzzusammenfassung . . . . .	352
2. Einzelerläuterungen . . . . .	353
<b>§ 13 Berichtspflichten</b> . . . . .	354
I. Gesetzesbegründung – Innenausschuss (BT-Drs. 19/28844, 88 f.) . . . . .	354
II. Kommentierung . . . . .	355
1. Zusammenfassung . . . . .	355
2. Einzelerläuterungen . . . . .	355
a) Absatz 2 – Verweis auf § 7 Abs. 1a BSIG . . . . .	355
b) Absatz 3 – Berichtspflicht des BMI . . . . .	355
<b>§ 14 Bußgeldvorschriften</b> . . . . .	357
I. Gesetzesbegründung Regierungsentwurf (BT-Drs. 19/26106, 89 ff.) . . . . .	359
II. Kommentierung . . . . .	370

1.	Zusammenfassung . . . . .	370
2.	Hintergrund der Norm . . . . .	370
3.	Systematik . . . . .	370
4.	Einzelerläuterungen . . . . .	371
<b>§ 14a</b>	<b>Institutionen der Sozialen Sicherung . . . . .</b>	<b>372</b>
I.	Gesetzesbegründung (RegE BT-Drs. 19/26106, 96) . . . . .	372
II.	Kommentierung . . . . .	373
1.	Zusammenfassung . . . . .	373
2.	Einzelerläuterungen . . . . .	373
<b>Art. 2 Änderungen im Telekommunikationsgesetz (TKG)</b>		
<b>§ 109</b>	<b>Technische und organisatorische Schutzmaßnahmen . . . . .</b>	<b>375</b>
I.	Gesetzesbegründung . . . . .	379
1.	RegE (BT-Drs. 19/26106, 96 f.) . . . . .	379
2.	Begründung der Beschlussempfehlung des Innenausschusses (BT-Drs. 19/28844, 45 f.) . . . . .	382
II.	Kommentierung . . . . .	383
1.	Kurzzusammenfassung . . . . .	383
2.	Änderungen in Absatz 2 („Technische Vorkehrungen und sonstige Schutzmaßnahmen“) . . . . .	383
a)	Berücksichtigung der Auswirkung auf Dienste . . . . .	383
b)	Pflichten für Netzbetreiber mit erhöhtem Gefährdungspotenzial . . . . .	384
c)	Zertifizierungspflicht für kritische Komponenten . . . . .	384
d)	Keine Übergangsfrist in § 109 Abs. 2 S. 4 TKG . . . . .	385
3.	Sicherheitskonzept bezieht sich auch auf neue Detailvorgaben aus der Verordnung (Abs. 4) . . . . .	385
4.	Mitteilungspflichten von beträchtlichen Sicherheitsverletzungen (Abs. 5) . . . . .	386
5.	Katalog an Sicherheitsanforderungen (Abs. 6) . . . . .	386
a)	Hintergrund: Der Gesetzgeber erlässt typischerweise keine Detailvorgaben für die IT-Sicherheit . . . . .	386
b)	Bisheriger Katalog von Sicherheitsanforderungen der BNetzA . . . . .	387
c)	Neue Regelungen für den Katalog . . . . .	387
d)	Definition der kritischen Komponenten durch den Katalog . . . . .	388
e)	Definition der TK-Netzbetreiber mit erhöhtem Gefährdungspotenzial . . . . .	388
6.	Überprüfung durch qualifizierte unabhängige oder eine zuständige nationale Behörde (Abs. 7) . . . . .	388
a)	Verpflichtung bei erhöhtem Gefährdungspotenzial (§ 109 Abs. 7 S. 2 TKG) . . . . .	389

b) Gemeinsame Bewertung durch BNetzA und BSI (§ 109 Abs. 7 S.4 TKG) . . . . .	389
<b>§ 113 Manuelles Auskunftsverfahren</b> . . . . .	390
I. Gesetzesbegründung . . . . .	392
1. RegE (BT-Drs. 19/26106, 98) . . . . .	392
2. Begründung der Änderungen durch den Ausschuss für Inneres und Heimat (BT-Drs. 19/28844, 46) . . . . .	392
II. Kommentierung . . . . .	393
1. Zusammenfassung . . . . .	393
2. Hintergrund der Norm . . . . .	393
3. Einzelerläuterungen . . . . .	394
a) Auskunftsziel i. S. d. § 113 Abs. 3 Nr. 8 TKG . . . . .	394
b) Weitere Voraussetzungen nach § 113 Abs. 3 Nr. 8 TKG . . . . .	394
c) Auskunftsberechtigung für dynamische IP-Adressen nach § 113 Abs. 5 Nr. 9 TKG . . . . .	395
<b>Art. 3 Änderungen im Energiewirtschaftsgesetz (EnWG)</b>	
<b>§ 11 Betrieb von Energieversorgungsnetzen</b> . . . . .	397
I. Gesetzesbegründung . . . . .	402
1. RegE (BT-Drs. 19/26106, 98) . . . . .	402
2. Begründung der Beschlussempfehlung des Innenausschusses (BT-Drs. 19/28844, 46) . . . . .	402
II. Kommentierung . . . . .	402
1. Inhaltliche Verpflichtung . . . . .	403
a) Intrusion Detection and Prevention System . . . . .	403
b) Eigenschaften und Angemessenheit des Intrusion Detection and Prevention Systems . . . . .	403
2. Nachweis der Erfüllung der Anforderungen des Abs. 1d und Mängelbeseitigungsverlangen (Abs. 1e) . . . . .	404
3. Datenschutzrechtliche und betriebsverfassungsrecht- liche Implikationen . . . . .	404
4. Kritik an der zögerlichen Gesetzgebung zu konkretisie- renden IT-Sicherheitsvorgaben . . . . .	405
<b>Art. 4 Änderungen in der Außenwirtschaftsverordnung (AWV)</b>	
<b>§ 55(a) Voraussichtliche Beeinträchtigung der öffentlichen     Ordnung oder Sicherheit</b> . . . . .	407
I. Gesetzesbegründung (BT-Drs. 19/26106, 98) . . . . .	407
II. Kommentierung . . . . .	407
1. Zusammenfassung . . . . .	407
2. Hintergrund der Norm . . . . .	408
3. Systematik . . . . .	408

4. Einzelerläuterungen . . . . .	409
5. Praxisempfehlung . . . . .	410

### **Art. 5 Änderungen im Zehnten Sozialgesetzbuch (SGB X)**

<b>§67c Zweckbindung sowie Speicherung, Veränderung und Nutzung von Sozialdaten zu anderen Zwecken</b> . . . . .	411
I. Gesetzesbegründung (RegE BT-Drs. 19/26106, 98) . . . . .	412
II. Kommentierung . . . . .	412
1. Zusammenfassung . . . . .	412
2. Hintergrund der Norm . . . . .	413
3. Einzelerläuterungen . . . . .	413

### **Art. 6 und 7 IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)**

<b>Artikel 6 Evaluierung</b> . . . . .	415
I. Gesetzesbegründung (RegE BT-Drs. 19/26106, 98 f.) . . . . .	415
II. Kommentierung . . . . .	417
1. Kurzzusammenfassung . . . . .	417
2. Einzelerläuterungen . . . . .	417
3. Praktische Empfehlungen . . . . .	419
<b>Artikel 7 Inkrafttreten</b> . . . . .	421
I. Gesetzesbegründung (BT-Drs. 19/26106, 99) . . . . .	421
II. Kommentierung . . . . .	421

### **Teil 3 Synopse**

BSI-Gesetz (Auszug) . . . . .	423
Telekommunikationsgesetz (TKG) . . . . .	486
Energiewirtschaftsgesetz (EnWG) . . . . .	494
Außenwirtschaftsverordnung (AWV) . . . . .	497
Sozialgesetzbuch 10 (SGB X) . . . . .	498

### **Teil 4 Material zum IT-Sicherheitsgesetz 2.0**

I. Referentenentwürfe des IT-Sicherheitsgesetzes 2.0 . . . . .	501
1. Erster mutmaßlich geleakter Referentenentwurf vom 27.3.2019 . . . . .	501
2. Zweiter mutmaßlich geleakter Referentenentwurf vom 7.5.2020 . . . . .	501
3. Erster offizieller Referentenentwurf für die Verbände-anhörung vom 9.12.2020 . . . . .	502
3. Zweiter offizieller Referentenentwurf für die Verbände-anhörung vom 11.12.2020 . . . . .	502
II. Parlamentarisches Verfahren (chronologisch) . . . . .	502

1. Dokumentationsseite des Deutschen Bundestages . . . . .	502
2. Regierungsentwurf des IT-SiG 2.0 (BT-Drs. 19/26106) . . . . .	503
3. Öffentliche Anhörung zum IT-SiG 2.0 im Bundestags-Ausschuss für Inneres und Heimat vom 1.3.2021 – Videoaufzeichnung, Tagesordnung, Protokoll und Sammlung der Stellungnahmen – . . . . .	503
4. Beschlussempfehlungen des Bundestags-Ausschusses für Inneres und Heimat (BT-Drs. 19/28844) . . . . .	503
<b>III. Weiterführendes Material . . . . .</b>	<b>504</b>
1. Relevante Verordnungsentwürfe des BMI. . . . .	504
a) Entwurf des BMI für die Verordnung zum IT-Sicherheitskennzeichen nach § 9c BSIG . . . . .	504
b) Zweite Verordnung zur Änderung der BSI-KritisV – Entwurf und Verbände-Stellungnahmen . . . . .	504
2. Gesetzgebungsmaterial zum IT-SiG 1.0 . . . . .	504
3. Gesetzgebungsmaterial zum NIS-RL-Umsetzungsgesetz . . . . .	505
4. Vorschlag der EU-Kommission für eine NIS-RL 2.0 vom 16.12.2020 . . . . .	505
<b>Literaturverzeichnis . . . . .</b>	<b>507</b>
<b>Stichwortverzeichnis . . . . .</b>	<b>513</b>