

Inhaltsverzeichnis

Einführung	27
A. Bestrebungen der normativen Gewährleistung der IT-Sicherheit	27
B. Gegenstand der Untersuchung	31
C. Gang der Untersuchung	33
<i>Teil 1</i>	
IT-Sicherheit Kritischer Infrastrukturen als Herausforderung	36
§ 1 Sicherheitsherausforderungen durch den Einsatz von IT	36
A. Rolle der IT in Wirtschaft, Verwaltung und Kritischen Infrastrukturen	38
B. Bedrohungen für die IT und Reaktionen	39
I. IT und IT-System	40
II. Veränderungen der Bedrohungslage	41
1. Besondere Bedrohungslage für die IT	43
a) Hardware	43
b) Software	44
c) Methoden	45
d) Zwischenergebnis	45
2. Erkennbarkeit einer Bedrohung	46
3. Rückverfolgbarkeit eines Angriffs	47
4. Zwischenergebnis	48
III. Bedrohung der IT-Sicherheit Kritischer Infrastrukturen	48
IV. Reaktionen auf die digitale Bedrohungslage	49
1. Staatliche Reaktionen	51
a) Nationale Ebene	51
b) Ebene der Europäischen Union	55
c) Überblick über die Regelungen des IT-Sicherheitsgesetzes und des Gesetzes zur Umsetzung der RL (EU) 2016/1148 für Kritische Infrastrukturen	56
2. Reaktionen in der Wirtschaft	57
V. Teilergebnis	58
§ 2 Klärung der zentralen Begriffe	59
A. IT-Sicherheit	59
I. Das Verständnis des BSIG	60
1. Die Schutzziele im Einzelnen und ihr Zusammenwirken	61

a) Verfügbarkeit	62
b) Unversehrtheit/Integrität	62
c) Unversehrtheit/Authentizität	63
d) Vertraulichkeit	63
e) Interdependenzen der Schutzziele	64
2. Schutzobjekt Information	65
3. Dynamisches Sicherheitsniveau für Informationen	68
4. IT-Sicherheit als Systemschutz	69
II. Abgrenzung zu anderen Sicherheitsbegriffen	69
1. Öffentliche Sicherheit	69
a) Der Schutz der öffentlichen Sicherheit mit Blick auf die IT-Sicherheit	71
aa) Schutz über anerkannte Rechtsgüter	71
bb) Schutz über die Rechtsordnung	73
b) Schutz der IT-Sicherheit als eigenständiges Rechtsgut?	75
c) Zwischenergebnis	77
2. Äußere Sicherheit	78
3. Datensicherheit	79
4. Versorgungssicherheit	82
5. Cybersicherheit	84
III. IT-Sicherheit als neue Teilmenge bekannter Sicherheitsbegriffe	85
IV. IT-Sicherheit im unionsrechtlichen Verständnis	86
B. Kritische Infrastrukturen	88
I. Infrastrukturbegriffe	88
1. Was ist Infrastruktur?	89
a) Definitionsversuche	89
b) Merkmale einer Infrastruktur	91
c) Rechtsbegriff Infrastruktur?	93
aa) In der Gesetzgebung	93
bb) In der Rechtsprechung	95
cc) In der Literatur	95
2. Infrastrukturkategorien	96
II. Kritikalität einer Infrastruktur nach nationalem Verständnis	97
1. Die Bedeutung der Beschreibung als „kritisch“	97
2. Kritische Infrastrukturen nach dem BSIG	98
a) Sektorenspezifische Eingrenzung nach § 2 Abs. 10 S. 1 Nr. 1 BSIG	100
b) Maßstäbe für die hohe Bedeutung einer Infrastruktur	100
aa) Bezugspunkt der Kritikalität	101
bb) Die Kriterien zur Bestimmung der Kritikalität i. e. S. ...	102
(1) Qualität	103
(2) Quantität	106

	Inhaltsverzeichnis	13
	c) Zwischenergebnis	106
	III. Wesentliche Dienste nach unionsrechtlichem Verständnis	107
	1. Die Bestimmung wesentlicher Dienste	109
	2. Vergleich mit nationalem Recht	113
	IV. Teilergebnis	114
§ 3	Rechtssystematische Einordnung	114
	A. Gefahrenabwehr- oder Risikosteuerungsrecht	115
	I. Abgrenzung der beiden Konzepte der Sicherheitsgewährleistung anhand der Trennlinie von Gefahr und Risiko	116
	II. Regelungsstruktur der Betreiberpflichten	120
	B. Abgrenzung von und Schnittmengen mit anderen Regelungsmaterien	123
	I. Datenschutzrecht	123
	II. Recht des Bevölkerungsschutzes	125
	III. Das IT-Sicherheitsgesetz als Vermengung verschiedener Rechts- materien	126

Teil 2

	IT-Sicherheit Kritischer Infrastrukturen zwischen staatlicher Verantwortung und privater Pflichtigkeit	128
§ 4	Objektiv-rechtliche Grundlagen der Betreiberpflichten zur IT-Sicherheit Kritischer Infrastrukturen im Verfassungs- und Unionsprimärrecht	129
	A. Objektive Schutzgehalte der Grundrechte des Grundgesetzes zugunsten der IT-Sicherheit	129
	I. Schutzpflichten gegenüber Betreibern Kritischer Infrastrukturen ..	130
	1. Art. 14 Abs. 1 GG	132
	a) Infrastruktureinrichtungen	133
	b) IT-Einrichtungen	134
	c) Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Infor- mationen	134
	aa) Eigentumsfähigkeit von Informationen	134
	bb) Das Recht am eingerichteten und ausgeübten Gewerbe- betrieb	137
	(1) Informationen als Schutzobjekt des Rechts am eingerichteten und ausgeübten Gewerbebetrieb ...	137
	(2) Verfassungsrechtliche Anerkennung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb ...	139
	d) Zwischenergebnis	142
	2. Art. 12 Abs. 1 GG	142
	3. Art. 5 Abs. 1 S. 1 Alt. 2 GG	143
	4. Art. 10 Abs. 1 Var. 3 GG	144
	5. Art. 2 Abs. 1 (i. V. m. Art. 1 Abs. 1) GG Recht auf informatio- nelle Selbstbestimmung	146

6. Art. 2 Abs. 1 (i. V.m. Art. 1 Abs. 1) GG Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	149
a) Begründung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	149
aa) Bedeutung der Nutzung	150
bb) Neuartige Gefährdung	151
cc) Grundrechtliche Schutzlücke	151
b) Das Bedürfnis nach einem „neuen Grundrecht“?	152
c) Schutzgegenstand	154
aa) Vertraulichkeit und Integrität	155
bb) Informationstechnisches System	155
d) Schutzgehalt zugunsten der IT-Sicherheit Kritischer Infrastrukturen	157
aa) Objektiver Gewährleistungsgehalt der IT-Sicherheit? ..	158
bb) Objektiver Gewährleistungsgehalt zugunsten der Betreiber Kritischer Infrastrukturen	160
e) Zwischenergebnis	162
II. Schutzpflichten gegenüber Nutzern Kritischer Infrastrukturen	163
1. Art. 2 Abs. 1 i. V.m. Art. 1 Abs. 1 GG Recht auf informationelle Selbstbestimmung	163
2. Art. 2 Abs. 1 i. V.m. Art. 1 Abs. 1 GG Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	164
3. Art. 12 Abs. 1 GG	165
4. Art. 2 Abs. 2 S. 1 GG	166
a) Schutzgegenstand Leben und körperliche Unversehrtheit ..	166
b) Bezug der Schutzpflicht zur IT-Sicherheit Kritischer Infrastrukturen	167
5. Art. 10 Abs. 1 Var. 3 GG	169
III. Verankerung der Betreiberpflichten in den grundrechtlichen Gewährleistungsgehalten	169
B. Infrastrukturgewährleistungsverantwortung	171
I. Verfassungsrechtlich normierte Infrastrukturverantwortung	171
1. Art. 87e Abs. 4 GG	172
2. Art. 87f Abs. 1 GG	174
II. Allgemeine Infrastrukturverantwortung für Kritische Infrastrukturen	175
1. Schutzpflichten	175
2. Sozialstaatsprinzip, Art. 20 Abs. 1 GG	177
3. Art. 87e Abs. 4 GG und Art. 87f Abs. 1 GG	179
III. Teilergebnis	180
C. Verankerung im Unionsprimärrecht	181

I.	Grundrechte der EUGRCH.....	181
1.	Schutzpflichten zugunsten der Betreiber wesentlicher Dienste	183
2.	Schutzpflichten zugunsten der Nutzer wesentlicher Dienste ...	186
3.	Verankerung der IT-Sicherheit wesentlicher Dienste in den Unionsgrundrechten.....	187
II.	Unionsrechtliche Infrastrukturverantwortung.....	188
§ 5	Betreiberpflichten als Ausfluss privater Pflichtigkeit.....	190
A.	Raum für eine verfassungsrechtliche Pflichtigkeit der Betreiber zur Sicherung der IT.....	192
B.	Bestehen einer privaten Pflichtigkeit der Betreiber.....	193
I.	Pflichtigkeit aufgrund einer Verursachungsverantwortlichkeit ...	194
1.	Verfassungsrechtliche Verankerung der Verursachungsverant- wortlichkeit.....	195
2.	Verursachungsverantwortlichkeit im Risikosteuerungsrecht?...	196
3.	Bestehen einer Verursachungsverantwortlichkeit.....	197
4.	Zwischenergebnis.....	200
II.	Grundrechtliche Pflichtigkeit zur IT-Sicherheit.....	200
1.	Abgrenzung der Eigensicherungspflichtigkeit vom Verursacher- prinzip.....	201
2.	Anknüpfungspunkte der Eigensicherungspflichtigkeit.....	201
a)	Eigenständige Pflichtigkeit grundrechtlicher Gehalte.....	202
aa)	Schutzpflichten zugunsten der Betreiber Kritischer Infrastrukturen.....	202
bb)	Subsidiaritätsprinzip.....	204
b)	Altruistischer Begründungsansatz.....	205
aa)	Art. 14 Abs. 2 GG.....	206
bb)	Pflichtigkeit aufgrund der sozialstaatlichen Gebunden- heit grundrechtlicher Freiheit.....	207
cc)	Pflichtigkeit aus Art. 87e, f GG.....	210
dd)	Rückbindung der grundrechtlich gewährten Freiheit an das Gemeinwesen.....	212
III.	Teilergebnis.....	213
C.	Pflichtigkeit im Unionsrecht.....	214

Teil 3

Die normative Gewährleistung der IT-Sicherheit

§ 6	Personelle Begrenzungen der Pflichten zur Gewährleistung der IT-Sicher- heit.....	217
A.	Betreiber Kritischer Infrastrukturen.....	217
I.	Betreiberbegriff.....	217
II.	Bestimmung der Kritischen Infrastrukturen durch Rechtsverord- nung.....	221

1. Konkretisierende oder konstitutive Bestimmung Kritischer Infrastrukturen	222
a) Parlamentsvorbehalt	223
b) Bestimmtheitsgebot	226
c) Konstitutive Festlegung durch die BSI-KritisV	228
2. Ausreichende Ermächtigungsgrundlage für eine Rechtsverordnung	229
a) Anforderungen an die Regelungsdichte	231
b) Hinreichende Regelungsdichte bezüglich des Inhalts	233
c) Hinreichende Regelungsdichte bezüglich des Zwecks	234
d) Hinreichende Regelungsdichte bezüglich des Ausmaßes ...	235
e) Auseinandersetzung mit der Kritik an der Regelungsstruktur der Bestimmung Kritischer Infrastrukturen	236
3. Zulässiger Delegatar	237
4. Rechtspolitische kritische Würdigung der Festlegung durch Rechtsverordnung	238
III. Die Struktur der BSI-KritisV	240
1. Kritische Dienstleistungen	241
2. Anlagen zur Erbringung kritischer Dienstleistungen	242
3. Der Schwellenwert	245
IV. Das Verhältnis zu speziell regulierten Infrastrukturen	248
B. Unionsrechtliche Determinierung der Kritischen Infrastrukturen	252
I. Vergleich der Struktur der BSI-KritisV und der Artt. 5 f. RL (EU) 2016/1148	252
II. Vergleich der Kritischen Infrastrukturen mit den wesentlichen Diensten	255
III. Teilergebnis	256
§ 7 Die Pflichten zur Gewährleistung der IT-Sicherheit	257
A. Pflichten nach dem BSIG	258
I. Die Sicherungspflicht	259
1. Unionsrechtliche Determinierung	260
2. Die Sicherungsmaßnahmen nach § 8a Abs. 1 BSIG	260
a) Organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der IT-Sicherheit	260
aa) Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit	261
bb) Zielrichtung der Maßnahmen	262
cc) Zu gewährleistendes IT-Sicherheitsniveau	264
dd) Sicherungsmaßnahmen im Einzelnen	265
ee) Zwischenergebnis	267
b) Festlegung des angemessenen IT-Sicherheitsniveaus	267
c) Stand der Technik	269
d) Die notwendige IT	271

e) Umsetzungsfrist	271
f) Unionsrechtskonforme Umsetzung	272
g) Dogmatische Charakteristika	274
3. Sanktionsmöglichkeiten	275
4. Verhältnis der Sicherungspflicht zu § 9 BDSG	277
5. Verhältnis der Sicherungspflicht zu § 25a Abs. 1 S. 3 Nr. 4, 5 KWG	278
6. Branchenspezifische Sicherheitsstandards	279
a) Anforderungen an den Vorschlag eines branchenspezifischen Sicherheitsstandards	280
aa) Materielle Anforderungen	280
bb) Formelle Anforderungen	282
b) Verfahren der Feststellung	284
c) Rechtswirkungen und Rechtsnatur der Feststellungsentscheidung und des branchenspezifischen Sicherheitsstandards	285
aa) Rechtswirkungen der Feststellungsentscheidung	285
(1) Inhaltliche Reichweite der Selbstbindung	286
(2) Zeitliche Reichweite der Selbstbindung	286
(3) Personelle Reichweite der Selbstbindung	288
bb) In der Feststellungsentscheidung enthaltene Rechtsakte	289
(1) Die Feststellung der Eignung	290
(2) Die konkludent erlassene Verwaltungsvorschrift ...	291
(3) Basis der Rechtswirkung zugunsten der Betreiber	292
cc) Rechtsnatur des branchenspezifischen Sicherheitsstandards i.e.S.	293
(1) Staatliches oder privates Recht	294
(2) Einordnung in die Kategorien öffentlich-rechtlicher Handlungsformen?	295
d) Folge der begrenzten zeitlichen Rechtswirkung: Die Aktualisierung des branchenspezifischen Sicherheitsstandards ...	296
e) Rechtsschutz	297
f) Kritische Würdigung der branchenspezifischen Sicherheitsstandards	298
aa) Eignung zur Gewährleistung des IT-Sicherheitsniveaus nach § 8a Abs. 1 BSIG	298
bb) Instrument innovativer IT-Sicherheitsgewährleistung ..	300
II. Durchsetzungsmechanismen der Sicherungspflicht	302
1. Der Nachweis nach § 8a Abs. 3 BSIG	303
a) Sicherheitsaudits, Prüfungen oder Zertifizierungen	303
b) Prüfer	304
c) Prüfungsverfahren	305

d) Nachweis gegenüber dem BSI	307
2. An den Nachweis andockende Befugnisse	307
3. Die Überprüfungsbefugnis nach § 8a Abs. 4 BSIG	308
4. Unionsrechtskonforme Umsetzung der Kontrollmechanismen	309
5. Verhältnis zu § 25a Abs. 1 KWG	310
6. Funktion der Durchsetzungsmechanismen	311
III. Die Meldepflicht	312
1. Meldepflicht des § 8b Abs. 3, 4 BSIG	313
a) Voraussetzungen	313
aa) Störung der IT-Sicherheit	313
(1) Der Störungsbegriff der Meldepflicht	313
(2) Erheblichkeitsschwelle für die pseudonyme Mel- dung	315
bb) Auswirkungen auf die betriebene Infrastruktur	318
cc) Zwischenergebnis	323
b) Rechtsfolge	323
aa) Unverzügliche Meldung	323
bb) Allgemeine inhaltliche Anforderungen	324
cc) Pseudonyme oder namentliche Meldung	324
(1) Abgrenzung der Pflicht einer namentlichen von der Möglichkeit einer pseudonymen Meldung	325
(2) Die pseudonyme Meldung	326
(3) Die namentliche Meldung	327
c) Dogmatische Bausteine	328
2. Die Kontaktstelle nach § 8b Abs. 3, 5 BSIG	328
3. Umsetzungsfrist und Sanktionen	329
4. Das Verhältnis zu § 42a BDSG	331
5. Kritische Betrachtung der Meldepflicht	332
IV. Ausnahmen	334
1. Kleinstunternehmen, § 8d Abs. 1 BSIG	334
2. Speziell regulierte Infrastrukturen	335
B. Pflichten in gesondert regulierten Bereichen	336
I. Energiesektor	336
1. Die Sicherungspflicht nach § 11 Abs. 1a, 1b EnWG	337
a) Angemessene Sicherungsvorkehrungen	337
b) Der Katalog der Sicherheitsanforderungen	338
aa) Inhalt	339
bb) Rechtswirkungen	342
cc) Rechtsnatur und Zulässigkeit der Fiktionswirkung	342
c) Besonderheiten für Betreiber von Energieanlagen	344
d) Dogmatische Charakteristika	346
2. Die Meldepflicht nach § 11 Abs. 1c EnWG	347

3. Die Meldepflicht nach § 44b AtG	348
4. Sanktionen	351
5. Charakteristika der Regulierung der IT-Sicherheit im Energie- sektor	352
II. TKG	352
1. Die Sicherungspflicht	353
a) Vorgaben des § 109 Abs. 2 TKG	353
b) Sicherheitsbeauftragter, Sicherheitskonzept und Sicherheits- katalog	355
c) Dogmatische Bausteine	356
2. Das Verhältnis von § 109 Abs. 2 TKG zum PTSG	357
3. Die Meldepflicht nach § 109 Abs. 5 TKG	358
4. Sanktionen	362
5. Abgrenzung zu datenschutzrechtlichen Benachrichtigungs- pflichten des § 109a TKG	363
6. Charakteristika der Regulierung der IT-Sicherheit im Telekom- munikationssektor	364
C. Wesentliche dogmatische Bausteine des Pflichtenkanons	364
D. Einfachgesetzliche Normierung einer privaten Verantwortlichkeit und Inpflichtnahme	366
E. Wirksamkeit und Einheitlichkeit der Pflichten?	368
I. Wirksamkeit	368
1. Sicherungspflichten und ihre Durchsetzungsmechanismen	368
2. Meldepflichten	371
3. Teilergebnis	372
II. Einheitlichkeit	373
1. Sicherungspflichten und ihre Durchsetzungsmechanismen	373
2. Meldepflichten	374
3. Vereinheitlichung des IT-Sicherheitsniveaus	375
§ 8 Die Rolle des BSI	375
A. Behördliche Aufgaben	376
I. IT-Wirtschaftsaufsichtsbehörde	376
II. Zentrale Stelle für die IT-Sicherheit Kritischer Infrastrukturen ...	379
1. Wissensakkumulation und Analyse	379
2. Internationale Vernetzung	380
3. Multiplikator	380
4. IT-Sicherheitsdienstleister	382
III. Behördlicher IT-Sicherheitsexperte	384
B. Verantwortungsteilung zwischen Staat und Privaten	384
I. Kooperation oder bloßes Zusammenwirken	385
II. Das BSI als staatlicher Garant der IT-Sicherheit Kritischer Infra- strukturen	387

§ 9 Verfassungs- und unionsrechtliche Zulässigkeit der Inpflichtnahme Privater	389
A. Kompetenz des Bundes	390
I. Gesetzgebungskompetenz	390
II. Exkurs: Verwaltungskompetenz für das BSI	392
B. Grundrechte	393
I. Grundrechtskanon des Grundgesetzes	396
1. Art. 12 Abs. 1 GG	396
a) Schutzbereich	396
b) Eingriff	396
aa) Sicherungspflicht	397
bb) Nachweispflicht	397
cc) Meldepflicht	398
(1) Die Pflicht zur Meldung von IT-Sicherheitsvorfällen	398
(2) Die Kontaktstelle nach § 8b Abs. 3 BSIG	400
c) Rechtfertigung	400
aa) Legitimes Ziel	400
bb) Geeignetheit und Erforderlichkeit	401
cc) Angemessenheit	401
(1) Sicherungspflicht	403
(2) Nachweispflicht	406
(3) Meldepflicht	406
(a) Die Pflicht zur Meldung von IT-Sicherheitsvorfällen	406
(b) Die Kontaktstelle nach § 8b Abs. 3 BSIG	408
dd) Zwischenergebnis	408
2. Art. 14 Abs. 1 GG	409
a) Schutzbereich	409
b) Inhalts- und Schrankenbestimmung	410
c) Rechtfertigung	410
3. Art. 2 Abs. 1 GG, Recht auf informationelle Selbstbestimmung	412
a) Schutzbereich	412
b) Eingriff	413
c) Rechtfertigung	415
4. Art. 2 Abs. 1 GG, Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	416
II. Unionsrechtliche Grundrechte	418
1. Schutzbereiche	418
2. Beeinträchtigungen	419
a) Sicherungspflicht	419
b) Nachweispflicht	419
c) Meldepflicht	420

Inhaltsverzeichnis	21
3. Rechtfertigung	420
III. Teilergebnis	421
C. Verstoß gegen den nemo tenetur se ipsum accusare-Grundsatz	422
I. Nachweispflicht	423
II. Meldepflichten	423
<i>Teil 4</i>	
Schlussbetrachtung	425
§ 10 Zusammenführung	425
A. Die Pflichten zur Gewährleistung der IT-Sicherheit als modernes infrastrukturbezogenes Sicherheitsrecht	425
B. Entwicklungstendenzen	427
§ 11 Thesen	430
Literaturverzeichnis	449
Sachregister	476