Inhaltsverzeichnis

§ 1 Einleitung 1

A. Internetsicherheit als Wissensproblem 1
B. Aufbau der Untersuchung 6

§ 2 Internetsicherheit und Informationsverwaltungsrecht 9

A. Schutzzielbezogene Eingrenzung der Internetsicherheit auf Netz- und Informationssicherheit 9
B. Infrastrukturbedingte Sicherheitsprobleme und Regulierbarkeit des Internets 13
I. Infrastruktur des Internets 13
1. Physikalische Infrastruktur 14
2. Logische Infrastruktur 15
II. Regulierbarkeit des Internets 16
C. Sicherheitsgewährleistung durch Informationsverwaltungsrecht 21
I. Epistemische Funktion des Informationsverwaltungsrechts 22
II. Generierung, Transfer und Distribution von Wissen und sicherheitsrelevanten Informationen 24
III. Daten, Information, Wissen und Kommunikation 26

§ 3 Generierung von Informationen über die Netz- und Informationssicherheit 31

A. Funktion der Informationsgenerierung für die Sicherheitsgewährleistung 31
I. Schutzpflicht zur Informationsgewinnung 32
II. Gewährleistungsverantwortung 34
1. Europäische Dimension 35
2. Grundgesetz 37
a) Internetinfrastruktur als grundrechtliches Schutzgut 37
b) Gewährleistungsverantwortung aus Art. 87f GG . . . 39
B. Informations- und Wissensakteure 42

I. Europäische Institutionen 44
3. Europäische Agentur für Netz- und Informationssicherheit 44
4. EU-Intelligence and Situation Centre 45
II. Nationale Behörden 45
1. Nationale Behörden für Netz- und Informationssicherheit 45
a) Bundesamt für Sicherheit in der Informationstechnik 45
b) Bundesnetzagentur 47
c) Datenschutzbehörden 48
2. Nachrichtendienstliche Einrichtungen 48
a) Bundesnachrichtendienst 48
b) Bundesamt für Verfassungsschutz 49
3. Nationales Cyber-Abwehrzentrum 51
III. Computer Security Incident Response Teams 52
C. Rahmen der Informationsgenerierung 53
I. Internetsicherheit im europäischen Primärrecht 54
1. Raum der Freiheit, der Sicherheit und des Rechts 54
2. Schutz personenbezogener Daten 56
3. Europäisches Infrastrukturrecht 56
4. Europäisches Katastrophenschutzrecht 57
5. Europäisches Statistikrecht 58
6. Gewährleistung der Netz- und Informationssicherheit als Angelegenheit des Binnenmarktes 58
II. Sekundär- und einfachrechtlich erfasste Internetinfrastrukturen, Dienste, Anbieter und Verantwortliche sowie sonstige Quellen 60
1. Telekommunikationsnetzbetreiber und -diensteanbieter sowie Over-the-Top-Kommunikationsdienste 60
a) Europäisches Sekundärrecht und Einordnung im deutschen nationalen Recht 60
b) Einordnung neuer Internetdienste wie Over-the-Top-Dienste 61
2. Betreiber wesentlicher Dienste und kritischer Infrastrukturen 65
3. Anbieter digitaler Dienste und Telemedien 69
4. Verantwortliche im Sinne des Datenschutzrechts 70
D. Rechtsgrundlagen zur Generierung von Informationen über die Sicherheit von Netzen und Informationssystemen 70
I. Pflichten zur Beibringung von Informationen 74
1. Sicherheitsnachweise 74

a) Vorlage des Sicherheitskonzeptes von Telekommunikationsunternehmen 74
b) Nachweis der Sicherheit von Betreibern wesentlicher Dienste bzw. kritischer Infrastrukturen 76
c) Nachweis der Sicherheit von Anbietern digitaler Dienste 78
2. Meldepflichten bei Sicherheitsverletzungen 80
a) Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten 80
aa) Anlass der Meldung 80
bb) Inhalt der Meldung 84
b) Betreiber wesentlicher Dienste und Kritischer Infrastrukturen 87
aa) Anlass der Meldung 87
bb) Inhalt der Meldung 90
c) Anbieter digitaler Dienste 93
aa) Anlass der Meldung 94
bb) Konkretisierung durch Durchführungsakte der Kommission 95
cc) Inhalt der Meldung 96
d) Meldung auf freiwilliger Basis 97
3. Meldepflicht bei Datenschutzverletzungen 99
a) Meldepflicht im allgemeinen Datenschutzrecht 99
aa) Anlass der Meldung 100
bb) Inhalt der Meldung 101
b) Meldepflicht im Telekommunikationsrecht 104
aa) Anlass der Meldung 104
bb) Inhalt der Meldung 106
II. Befugnisse zur Generierung von Informationen 108
1. Untersuchung von IT-Produkten und -Systemen 108
a) Informationspflichten für Hersteller von Soft- und Hardware im öffentlichen Sicherheitsrecht 108
b) Befugnis zur Untersuchung von IT-Sicherheitsprodukten 110
2. Informationsbefugnisse im sicherheitsbezogenen Telekommunikationsrecht 111
a) Sicherheitsbezogene Informationsbefugnis 111
aa) Sicherstellung materiell-rechtlicher Sicherheitspflichten 112

bb) Kriterium der Erforderlichkeit aus der Wissensperspektive 114
b) Informationelle Generalbefugnis 120
3. Nachrichtendienstliche Instrumente zur Informationsgewinnung 121
a) Überwachung des Internetdatenverkehrs zur Erkennung von Cybergefahren 121
aa) Strategische Fernmeldeaufklärung 122
bb) Überwachung der Ausland-Ausland-Telekommunikation 126
b) Besondere nachrichtendienstliche Mittel zum Schutz kritischer Infrastrukturen 130
c) Nachrichtendienstliche Auskunftsverlangen 131
aa) Auskunft über Bestands- und Nutzungsdaten bei Anbietern von Telemediendiensten 131
bb) Auskunft über Strukturen der Telekommunikationsdienste und -netze 133
III. Übernahme verwaltungsexternen Wissens 134
1. Kooperation mit Privaten 135
a) Vorschlag von technischen Sicherheitsstandards durch Branchenverbände 135
b) Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen 136
c) Einbindung bei der Erstellung von Sicherheitskatalogen 136
d) Einkauf von Expertise und Informationen über Sicherheitslücken 136
e) Einsatz wissenschaftlicher Kommissionen 137
2. Dysfunktion und Zulässigkeit der Informationsgenerierung über Private 137
a) Wissensübernahme von Privaten im Bereich Sicherheit 138
b) Zur Zulässigkeit der Inanspruchnahme Privater bei der Informations- und Wissensgenerierung 140
E. Besondere Grenzen der Informationsgenerierung 142
I. Meldepflichten und Selbstbelastungsschutz 142
1. Verbot der Pflicht zur Selbstbelastung 142
2. Kein absoluter Schutz vor Selbstbelastung 144
3. Ausgleich der betroffenen Interessen 146
II. Besondere datenschutzrechtliche Grenzen der Informationsgenerierung 149

1. Datenschutzrechtliche Relevanz der Netz- und Informationssicherheit 150
a) Datensicherheit im Verhältnis zum Datenschutz . . . 151
b) Personenbeziehbarkeit von Maschinendaten 152
aa) Beispiel der IP-Adresse 153
bb) Personenbeziehbarkeit von IP-Adressen 154
2. Zur Rechtfertigung der Datenverarbeitung zum Zwecke der Netz- und Informationssicherheit 160
a) Datenverarbeitung durch Diensteanbieter und Infrastrukturbetreiber 160
aa) Verarbeitung datenschutzrechtlich geschützter Daten zur Gefahrenabwehr im Telekommunikationsrecht 161
bb) Verarbeitung datenschutzrechtlich geschützter Daten zur Gefahrenabwehr im Telemedienrecht und allgemeinen Datenschutzrecht 163
b) Datenverarbeitung durch NIS-Verwaltung 167
aa) Zur Rechtfertigung der Datenverarbeitung 167
bb) Grundsatz der Datenminimierung 170
cc) Zweckbindung und Regelungstiefe 173
III. Besondere Grenzen der Informationsgenerierung zum Schutz von Unternehmensgeheimnissen 179
1. Schutzbedarf von Unternehmensinformationen 180
2. Der öffentlich-rechtliche Schutz von Unternehmensinformationen bei Bestehen von Informationspflichten in der NIS-Verwaltung 180
a) Keine Anwendbarkeit des Datenschutzrechts auf juristische Personen 181
b) Schutz von Betriebs- und Geschäftsgeheimnissen . . 183
aa) Herleitung des Schutzes 183
bb) Beispiel der Sicherheitslücke 185
(1) Begriff der Sicherheitslücke 185
(2) Schutzvoraussetzungen 186
c) Besonderer Schutz für Betreiber kritischer Infrastrukturen im Rahmen von Meldepflichten . . . 188
3. Schutz vor unbefugter Offenlegung durch das Verwaltungsgeheimnis 191
a) Beachtung der Verhältnismäßigkeit 191
b) Schutz durch das Verwaltungsgeheimnis 193
F. Zwischenergebnis 196

§ 4 Transfer von Informationen im Rahmen der europäischen Zusammenarbeit zur Gewährleistung der Netz- und Informationssicherheit 201

A. Funktion des Informationstransfers für die Sicherheitsgewährleistung 202
I. Kognitive Dimension des Europäischen Verwaltungsverbunds 202
II. Verwaltungskooperation im Bereich Sicherheit von Netz- und Informationssystemen 206
1. Europäisches Sicherheitsverwaltungsrecht als Informationsverwaltungsrecht 206
2. Informationskooperation zur Gewährleistung der Netz- und Informationssicherheit 208
B. Struktur des Informationsaustausches 209
I. Formen des europäischen Informationstransfers 209
1. Vielgestaltigkeit europäischer Informationsaustauschverfahren 210
2. Grundtypen europäischer Informationsaustauschmechanismen 212
II. Ausgestaltung der Informationszusammenarbeit durch die NIS-Richtlinie 213
1. Organisationsrechtliche Ausgestaltung 214
a) Strategischer Informationsaustausch in der Kooperationsgruppe 214
b) Operativer Informationsaustausch im CSIRTs-Netzwerk 215
c) Informationsaustausch außerhalb der NIS-Zusammenarbeit 215
2. Verfahrensrechtliche Ausgestaltung 215
a) Prävention durch Informations- und Wissensaustausch 216
aa) Sach- und Kontrollberichte 216
(1) Sachberichte über gemeldete Sicherheitsverletzungen 216
(2) Kontrollberichte über den Vollzug 218
(3) Telekommunikationsrechtliche Informationsbefugnis zur Erfüllung von Berichtspflichten 219
bb) Austausch von Erfahrung und bewährten Praktiken 220

(1) Austausch spezifischer Formen von Wissen über die Sicherheit 220
(2) Kooperationsgruppe als Wissensspeicher . . . 222
cc) Konsultationspflichten 224
(1) Konsultation mit nationalen Strafverfolgungsbehörden 225
(2) Konsultation mit Datenschutzbehörden 227
(3) Konsultation als Teil des Notfallmanagements 229
b) Detektion von Gefahren durch Frühwarnmechanismus 231
aa) Rascher Austausch über Gefahren durch Frühwarnsysteme 232
bb) Frühwarnungen durch CSIRTs 232
c) Reaktion auf Sicherheitsvorfälle und Abschwächung von Risiken 235
aa) Horizontaler Informationsaustausch über Sicherheitsvorfälle 235
(1) Informationsaustausch in Deutschland 235
(2) Informationsaustausch zwischen den Mitgliedstaaten 237
bb) Horizontaler Informationsaustausch über Sicherheitsvorfälle mit vertikalen Bezügen 239
(1) Informationen zu einzelnen Sicherheitsvorfällen im CSIRTs-Netzwerk 239
(2) Informationen im Zusammenhang mit Sicherheitsvorfällen und über Computerkriminalität 242
cc) Reaktion auf einen Sicherheitsvorfall 244
(1) Austausch impliziten Wissens durch Übungen 244
(2) Koordinierte Reaktion 245
(3) Zusammenarbeit mit Datenschutzbehörden bei der Bearbeitung von Sicherheitsvorfällen bei wesentlichen Diensten 246
III. Förderung des Informationsaustausches 248
1. Grundsatz der loyalen Zusammenarbeit 248
a) Allgemeine Kooperationspflicht 249
b) Inhaltliche Anforderungen an auszutauschende Informationen 250
2. Rechtliche Sicherung des gegenseitigen Vertrauens . . . 251
a) Vertrauen als Gelingensvoraussetzung der NIS-Informationskooperation 251

b) Konkrete Maßnahmen der Erwartungsstabilisierung 252
c) Umgang mit Ungewissheit als Gewissheit 254
3. Primärrechtliche Möglichkeiten der Stärkung des Wissenstransfers 254
a) Parallelität der mitgliedstaatlichen Informationsverarbeitung 254
b) Allgemeine Informationsbefugnis der Kommission . 256
C. Besondere Grenzen des Informationstransfers 258
I. Grenzen des Informationstransfers durch den Datenschutz 258
1. Übermittlung nach Maßgabe des allgemeinen Datenschutzrechts 260
2. Übermittlung im Rahmen der Aufklärung von Cybergefahren zum Schutz kritischer Infrastrukturen . . 260
a) Übermittlung von Daten durch das Bundesamt für Verfassungsschutz 260
b) Übermittlung der im Rahmen der Fernmeldeaufklärung von Cybergefahren gewonnenen Daten 261
c) Übermittlung der im Rahmen der Ausland-Ausland-Fernmeldeaufklärung gewonnenen Daten 263
3. Besondere Zweckbindung für die Meldedaten beim BSI 264
II. Grenzen des Informationstransfers durch den Schutz unternehmensbezogener Daten 266
1. Anforderungen an den Austausch vertraulicher Informationen 268
2. Besondere Begrenzungen 270
a) Begrenzungen der ENISA und allgemeine unionsrechtliche Geheimhaltungspflicht 270
b) Begrenzungen der deutschen NIS-Behörden 271
aa) Weitergabe von Erkenntnissen aus Produkt- und Systemuntersuchungen an europäische NIS-Stellen 271
bb) Geringe Regelungsdichte zur Weitergabe vertraulicher Informationen durch die NIS-Behörden 272
III. Grenzen des Informationstransfers durch Organisationsrecht 275
1. Trennungsgebot und Informationsaustausch im Nationalen Cyber-Abwehrzentrum 275
a) Sicherheitsbehördliches Trennungsgebot 276
b) Reichweite des informationellen Trennungsprinzips 278
2. Unabhängigkeit der NIS-Behörde 280

a) Stärkung der technischen Sicherheit durch Neutralität 280
b) Unionsrechtliche Zulässigkeit weisungsfreier Räume 282
c) Sachliche Rechtfertigung der Unabhängigkeit 284
aa) Stärkung der Wissensfunktion durch Unabhängigkeit 284
bb) Verfassungsrechtliche Einwände gegen organisationsrechtliche Unabhängigkeit 288
cc) Veröffentlichung von Weisungen als Gestaltungsoption 290
IV. Informationsverweigerungsrecht der Mitgliedstaaten zur Wahrung wesentlicher Sicherheitsinteressen 291
D. Zwischenergebnis 294

§ 5 Distribution von Informationen über die Netz- und Informationssicherheit 299

A. Funktion der Informationsdistribution für die Sicherheitsgewährleistung 300
I. Sicherheit durch staatliche Informationstätigkeit 301
II. Sicherheit durch Transparenz 305
1. Begrenzung von Datenmacht am Beispiel des Datenschutzes 307
2. Argumente aus der Kryptokontroverse gegen exklusives staatliches Wissen 308
3. Transparenzgedanke in der Debatte um Freie Software 311
III. Sicherheit durch Informationszugang und -weiterverwendung 313
B. Aktives Informationshandeln 315
I. Öffentlichkeitsbezogene Informationstätigkeit 315
1. Allgemeine Anforderungen an Publikumsinformationen 316
a) Erfordernis der Rechtsgrundlage 316
b) Qualität der Information 317
2. Aufklärung zur Sensibilisierung für Sicherheitsprobleme 318
a) Berichte der NIS-Behörden 319
aa) Bericht des Bundesamts für Sicherheit in der Informationstechnik 319
bb) Bericht der Bundesnetzagentur 321
cc) Bericht der Datenschutzaufsichtsbehörde 322
b) Stellungnahmen der Datenschutzaufsichtsbehörden . 323
c) Information über Sicherheitsvorfälle 324

aa) Unterrichtung über Sicherheitsverletzungen . . . 324
(1) Sicherheitsverletzungen bei Telekommunikationsunternehmen 324
(2) Fehlende Rechtsgrundlage für das BSI 326
bb) Veröffentlichung einer Verletzung des Schutzes personenbezogener Daten durch Verantwortliche 328
3. Veröffentlichung von Sicherheitsanforderungen und Untersuchungsergebnissen 329
a) Veröffentlichung des Sicherheitskatalogs 330
b) Veröffentlichung der Erkenntnisse aus Produkt- und Systemuntersuchungen 330
4. Warnungen vor Sicherheitslücken und sonstigen Gefahren 332
a) Voraussetzungen und Reichweite des Tatbestands . . 332
b) Responsible Disclosure als ermessensleitende Strategie für die Warnung vor Sicherheitslücken . . . 333
5. Empfehlungen von Sicherheitsmaßnahmen und Sicherheitsprodukten 337
a) Empfehlung bei Gefahrenverdacht 337
b) Problem eigendynamischer Verstärkungseffekte . . . 340
c) Besondere Anforderungen an die Informationsdarstellung 341
II. Individualbezogene Informationstätigkeit 345
1. Betreiber kritischer Infrastrukturen 345
2. Information in informellen Zusammenschlüssen 347
3. Datenschutzrechtlich Verantwortliche und Betroffene einer Verletzung 349
a) Betroffene einer Datenschutzverletzung 349
b) Individuelle Beratung in Fragen der Datensicherheit 350
C. Reaktives Informationshandeln 351
I. Grundrecht auf Informationszugang 351
1. Grundsatz der Offenheit und Recht auf Zugang zu Dokumenten im Unionsrecht 352
2. Verankerung der Informationsfreiheit im Grundgesetz 353
II. Zugang zu Informationen bei den NIS-Stellen 354
1. Zugang bei europäischen NIS-Stellen 355
a) Reichweite der Transparenz-Verordnung und Verhältnis zur NIS-Richtlinie 355
b) Zugang zu Informationen am Beispiel der ENISA . . 357
2. Zugang bei nationalen NIS-Stellen 358
a) Bundesamt für Sicherheit in der Informationstechnik 359

b) Bundesnetzagentur 359
c) Kein Zugang zu Informationen bei Nachrichtendiensten 360
III. Informationsinteresse und Geheimhaltungsbedürfnis . . . 360
1. Reichweite der Ausnahme vom IFG im BSIG 362
2. Auswirkungen der allgemeinen Ausnahmen vom Informationszugangsrecht 364
a) Belange der Sicherheit 365
b) Geheimnisschutz auf Grund öffentlicher Belange . . 366
c) Schutz vertraulich erhobener und übermittelter Informationen 367
d) Datenschutz 368
e) Betriebs- und Geschäftsgeheimnisse 369
f) Geistiges Eigentum 370
3. Pauschalabwägung der Interessen im BSIG 371
IV. Bereitstellung und Verwendung der Informationen 374
1. Anforderungen an die Informationen 375
2. Weiterverwendung zugänglicher Informationen 376
3. Maschinenlesbare Bereitstellung von Daten 378
D. Zwischenergebnis 380

§ 6 Zusammenfassende Bewertung und Fazit 385

A. Beitrag des Informationsverwaltungsrechts zur Netz- und Informationssicherheit 385
I. Erkennung von Gefahren und systemischen Risiken 386
II. Europäisierte Informationskooperation auf Vertrauensbasis 387
III. Zugang zu und freie Weiterverwendung von generierten Informationen und produziertem Wissen als Teil der Sicherheitsgewährleistung 390
B. Intelligente Datenverarbeitung und Operationalisierung von Nichtwissen 391

Literaturverzeichnis 395

Sachregister 437