

IT-Sicherheit kritischer Infrastrukturen

Von der Staatsaufgabe zur rechtlichen Ausgestaltung

von
Matthias Sonntag

1. Auflage

IT-Sicherheit kritischer Infrastrukturen – Sonntag

schnell und portofrei erhältlich bei beck-shop.de DIE FACHBUCHHANDLUNG

Thematische Gliederung:

Informationsrecht, Neue Medien



Verlag C.H. Beck München 2005

Verlag C.H. Beck im Internet:

www.beck.de

ISBN 978 3 406 51377 0

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
Abbildungsverzeichnis	XXIII
Abkürzungsverzeichnis	XXV
Literaturverzeichnis	XXXV
Einleitung	1
I. Untersuchungsgegenstand	1
II. Gang der Darstellung	6
1. Teil. Schutz kritischer Infrastrukturen	9
A. Überblick	9
B. Diskussion um den Schutz kritischer Infrastrukturen	10
I. Neue Abhängigkeit	10
II. Internet-Sicherheit	13
III. Schutz kritischer Infrastrukturen	14
IV. Rechtliche Facetten der Problematik	16
1.) Kompetenzen zum Schutz der inneren und äußeren Sicherheit	16
2.) Gewährleistung der Versorgungssicherheit	17
3.) Schutz vor Gefahren des Einsatzes der Informa- tionstechnik	18
V. Fazit	18
C. Begriffliche Vorabklärung	19
I. IT-Sicherheit als Rechtsbegriff	20
1.) Gesetzliche Definitionen	20
a) Legaldefinition gemäß § 2 Abs. 2 BSI-Errich- tungsgesetz	20
b) Verhältnis zu anderen Sicherheitsbegriffen	21
(1) Innere und äußere Sicherheit	21
(2) Öffentliche Sicherheit	22
(3) Technische Sicherheit	23
2.) Sicherheitsbegriff der technischen Informatik	24
3.) Fazit	26
II. Kritische Infrastrukturen	26

1.) Zum Begriff der Infrastruktur	27
a) Allgemeiner Sprachgebrauch	27
b) Ökonomischer Infrastrukturbegriff	27
c) Entstehender Rechtsbegriff „Infrastruktur“	29
(1) Rechtswissenschaftliche Literatur	30
(2) Begriff in der Rechtsprechung	32
(3) Begriff im kodifizierten Recht	32
(4) Fazit	34
2.) Warum Kritisch?	34
3.) Fazit und Eingrenzung des Untersuchungsgegenstandes	37
D. Historische Entwicklung und heutige Erscheinungsformen der Infrastruktursektoren	38
I. Informations- und Telekommunikationsinfrastruktur	39
1.) Privatisierung der Telekommunikationsmärkte	39
2.) Heutige Erscheinungsform	41
II. Energieversorgungsinfrastruktur	42
1.) Liberalisierung der Energiemärkte	42
2.) Heutige Erscheinungsform	45
III. Bank- und Finanzinfrastruktur	45
1.) Historische Entwicklung der Finanzaufsicht	45
2.) Heutige Erscheinungsform	47
IV. Fazit	48
E. Informationstechnisches Risikopotenzial kritischer Infrastrukturen	49
I. Entwicklung der Informations- und Kommunikationstechnik	49
1.) Meilensteine der Rechnertechnik	49
2.) Meilensteine der Vermittlungstechnik	51
3.) Heutige Bedeutung der Kommunikations- und Informationstechnik	52
II. IT-Sicherheitsziele	53
III. Allgemeine Bedrohungsszenarien	55
1.) Vernetzung	56
2.) Outsourcing	57
3.) Internetnutzung	58
4.) Sicherheitsvorfälle	58
IV. Infrastrukturspezifische Risikopotenziale	59
1.) Informations- und Kommunikationsinfrastruktur	61
2.) Energieversorgungsinfrastruktur	63
3.) Banken- und Finanzinfrastruktur	65
V. Fazit	68

F. Möglichkeiten rechtlicher Steuerung	70
G. Zusammenfassung	72
2. Teil. Staatstheoretische und verfassungsrechtliche Vorgaben für die IT-Sicherheit kritischer Infrastrukturen	75
A. Staatstheoretische Vorüberlegungen	75
I. Identifizierung der sachlichen Aufgabenstellung	76
II. Lehre von den Staatsaufgaben	77
1.) Problematik und Stellenwert der Bestimmung von Staatsaufgaben	77
2.) Kategorisierungsansätze	81
3.) Unergiebigkeit der Staatsaufgabendiskussion	82
4.) „Kernbestand“ an Staatsaufgaben	82
III. Ergänzung der Staatsaufgabendiskussion durch den Begriff der „staatlichen Verantwortung“	83
1.) Bedürfnis nach einer begrifflichen Neuorientierung	84
2.) Verantwortung und Verantwortungsteilung	85
3.) Verantwortungskategorien	86
IV. Zwischenergebnis	88
B. Verfassungsrechtliche Direktiven für die staatliche Verantwortung im Bereich des IT-Schutzes der kritischen Infrastrukturen	90
I. Ausgangspunkt der verfassungsrechtlichen Analyse	90
II. Innere Sicherheit und Gefahrenabwehr	91
1.) Rechtsstaatliches Gewaltmonopol	91
a) Verfassungsrechtliche Grundlagen des staatlichen Gewaltmonopols	92
b) Reichweite des staatlichen Gewaltmonopols	93
c) Fazit	95
2.) Spezielle verfassungsrechtliche Vorgaben	96
3.) Staatsaufgabe Sicherheit im Kompetenzgefüge von Bund und Ländern	98
4.) Grundrechtliche Schutzpflichten	98
a) Grundrecht auf Leben und körperliche Unversehrtheit	101
(1) Schutzbereich	101
(2) Staatliche Schutzpflicht in der Rechtsprechung des Bundesverfassungsgerichts	102
(3) IT als Gegenstand der staatlichen Schutzpflicht	103
(4) Maßstab des Art. 2 Abs. 2 Satz 1 GG	104
b) Fernmeldegeheimnis	106

(1) Schutzbereich	106
(2) Objektiv-rechtlicher Gehalt des Art. 10 Abs. 1 GG	107
(3) Maßstab des Art. 10 Abs. 1 GG	108
c) Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG	109
(1) Schutzbereich	109
(2) Objektiv-rechtliche Gehalte	109
d) Kommunikations- und Medienfreiheiten aus Art. 5 Abs. 1 GG	110
(1) Schutzbereich	111
(a) Meinungsäußerungsfreiheit	111
(b) Informationsfreiheit	111
(2) Objektiv-rechtlicher Gehalt von Art. 5 Abs. 1 Satz 1 GG	112
e) Fazit	113
(1) Spezifität des Grundrechtsschutzes	113
(2) Untermaßverbot	114
(3) Ausgestaltungsfreiheit des Gesetzgebers	115
(4) Wissensgenerierung	115
5.) Zwischenergebnis	116
III. Infrastrukturelle Versorgungssicherheit	116
1.) Horizontale Verfassungsdirektiven für die staat- liche Verantwortung	117
a) Sozialstaatsprinzip	117
(1) Infrastrukturverantwortung als Teilbereich der Daseinsvorsorge	118
(2) Infrastrukturverantwortung als eigenständiger Teilbereich des Sozialstaatsprinzips	118
(3) Infrastrukturen als tatsächliche Voraus- setzung der grundrechtlichen Freiheiten	119
(4) Fazit	120
b) Grundrechte und Infrastruktursicherung	120
(1) Subjektiv-rechtliche Dimension der Grund- rechte	120
(a) Originäre Leistungsansprüche	121
(b) Derivative Leistungsansprüche	121
(2) Objektiv-rechtliche Dimension der Grund- rechte	122
(a) Versorgungssicherheit als Gegenstand grundrechtlicher Schutzpflichten	122

(b) Allgemeine Handlungsfreiheit, Art. 2 Abs. 1 GG	123
c) Kompetenzvorschriften	125
2.) Vertikale Vorgaben – Verwaltungskompetenzen . .	127
a) Telekommunikationsinfrastruktur	127
(1) Infrastrukturgewährleistungsauftrag des Art. 87f GG	127
(2) Sicherheitsspezifischer Regelungsgehalt	129
(a) Materieller Garantiegehalt	130
(b) Organisationsrechtlicher Ausgestaltungsauftrag	131
(3) Bindungswirkungen hinsichtlich der privat- wirtschaftlichen Leistungserbringer	132
(4) Fazit	132
b) Finanzwesen	133
3.) Fazit	134
C. Autonomie der privaten Betreiber als verfassungsrechtliche Grenze der staatlichen Verantwortung	136
I. Grundrechte des Infrastrukturbetreibers	136
1.) Berufsfreiheit des Infrastrukturbetreibers	137
a) Schutzbereich und Eingriff	137
b) Rechtfertigung und Grenzen von Berufsausübungsregelungen	138
(1) Geeignetheit und Erforderlichkeit	139
(2) Zumutbarkeit	140
(a) Maßgebliche Gemeinwohlbelange	140
(b) Risikovorsorge als Gemeinwohlbelang . .	141
c) Fazit	142
2.) Eigentumsgarantie, Art. 14 GG	143
a) Abwehr von Sicherheitspflichten	143
b) Fazit	144
II. Subsidiaritätsprinzip	145
D. Zwischenergebnis	146
3. Teil. Einfach- und untergesetzliche Ausgestaltung des Schutzes kritischer Infrastrukturen	151
A. Überblick	151
B. Polizeirechtlicher Ausgangspunkt der Verantwortungs- verteilung	152
I. Materielle Polizeipflichtigkeit und Eigensicherungs- pflichten	152
1.) Risikoträger als Zustandsstörer?	152

2.) Eigensicherungspflichten	155
II. Fazit	156
C. Private Verantwortung – Sicherungspflichten im Bereich kritischer Infrastrukturen	158
I. Horizontale Regelungen	160
1.) Sicherheit der elektronischen Kommunikation	161
a) Elektronische Signaturen	162
(1) Gesetz über die Elektronische Signatur	162
(2) Relevanz für die IT-Sicherheit kritischer Infrastrukturen	163
b) Kryptographie	164
c) Fazit	166
2.) Sicherung von Daten	167
a) Schutz personenbezogener Daten	167
(1) Vorgaben des Bundesdatenschutzgesetzes ..	168
(a) Verhältnis von IT-Sicherheit und Datenschutz	168
(b) Sicherungspflichten	168
(c) Offenbarungs- und Mitteilungspflichten	170
(d) Organisatorische Pflichten der Eigenüberwachung	171
(2) Bewertung	172
b) Sonstige organisatorische Pflichten – Risikomanagementsysteme im Unternehmensbereich .	174
(1) Hintergrund: Organhaftung	175
(2) Sorgfaltspflichten	175
(a) Risikomanagementsystem	176
(b) Pflicht zur ordnungsgemäßen Buchführung	178
(c) Haftungsbegrenzung	178
(3) Untergesetzliche Konkretisierungen	179
(a) Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme	179
(b) Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie	179
(c) ISO 17799	180
(4) Fazit	181
c) Repressive Absicherungen	182
(1) Funktion des Strafrechts	182
(2) Straftatbestände mit Bezug zur IT-Sicherheit	182
(3) Fazit	183

3.) Zwischenergebnis	183
a) Berücksichtigung IT-sicherheitsspezifischer Aspekte	184
b) Privater Verantwortungsbereich	184
II. Vertikale Regelungen	185
1.) Telekommunikationsinfrastruktur	185
a) Einfachgesetzlicher Regelungsrahmen	185
(1) Telekommunikationsgesetz	185
(a) Anwendungsbereich	186
(b) Zielsetzung	186
(c) Pflicht zur Wahrung des Fernmeldegeheimnisses und Abhörverbot	186
(d) Vorsorge- und Sicherungspflichten	186
(e) Offenbarungspflichten	189
(i) Allgemeine Auskunftspflichten	189
(ii) Besondere Offenbarungs- und Dokumentationspflichten	190
(f) Organisatorische Pflichten	191
(2) Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen	192
(3) PTSG	193
(a) Anwendungsbereich	193
(b) Zweck	193
(c) Vorsorge- und Sicherungspflichten	194
(d) Offenbarungspflichten	194
(e) Sonstige organisatorische Pflichten	195
(4) Bewertung	195
(a) Kritik an Sprache und Systematik des § 87 TKG	196
(b) Überregulierung durch TKG und PTSG	197
(c) Fehlende Notwendigkeit wegen Eigeninteresses	198
(d) Weitere Schwächen des Regelungsansatzes von § 110 TKG	199
(e) Fazit	199
b) Untergesetzliche Konkretisierungen und Selbstregulierung	200
(1) TKSiv, PTZSV, PTKAusV	201
(2) Selbstverpflichtung der TK-Unternehmen	201
(3) Technische Regeln und Normen	202
(4) Fazit	202
c) Zwischenergebnis	202

(1) Berücksichtigung der IT-Sicherheit	202
(2) Privater Verantwortungsbereich	203
2.) Energieversorgung	204
a) Energiewirtschaftsgesetz	204
(1) Anwendungsbereich	205
(2) Ziel der sicheren Energieversorgung	206
(3) Vorsorge- und Sicherungspflichten	206
(4) Offenbarungspflichten	207
b) Untergesetzliche Konkretisierungen und Selbstregulierung – die VDE-Bestimmungen	207
c) Fazit Energieversorgung	209
(1) Allgemeines	209
(2) Berücksichtigung der IT-Sicherheit	209
(3) Privater Verantwortungsbereich	210
(4) Ausblick	210
3.) Finanzinfrastruktur	211
a) Einfachgesetzliche Vorgaben	212
(1) Kreditwesengesetz (KWG).	212
(a) Organisatorische Pflichten	212
(b) Vorsorge- und Sicherungspflichten	213
(c) Mitteilungs- und Dokumentations- pflichten	214
(2) Wertpapierhandelsgesetz (WpHG).	215
(3) Börsengesetze	215
(a) Börsen als Teil der öffentlichen Verwal- tung	216
(b) Besondere technische Situation	217
(c) Fazit	218
b) Untergesetzliche Konkretisierungen und Selbst- regulierung	218
(1) Verlautbarungen und Rundschreiben der BAFin	219
(a) Verlautbarung „Grenzüberschreitende Datenfernverarbeitung im Bankbuchfüh- rungswesen“	219
(b) Rundschreiben I 3 – 272 A – 2 / 98	220
(2) Branchenspezifische Standards	220
(3) Bewertung der untergesetzlichen Regelun- gen	221
c) Zwischenergebnis	221
(1) Berücksichtigung der IT-Sicherheit	221
(2) Privater Verantwortungsbereich	221

4.) Vergleich der drei Sektoren	222
a) Vorsorge-, Überwachungs- und Sicherungspflichten	222
b) Sonstige Organisationspflichten	223
c) Offenbarungs- und Mitwirkungspflichten	223
III. Resümee „private Sicherungspflichten“	223
1.) Berücksichtigung der IT-Sicherheit	223
2.) Verantwortungszuordnung	224
D. Verantwortung des öffentlichen Sektors – der institutionelle Rahmen	225
I. Horizontaler institutioneller Rahmen	226
1.) Elektronische Kommunikation	226
a) Schutz von Integrität und Authentizität	226
b) Schutz der Vertraulichkeit	228
2.) Datenschutz	229
a) Überwachungsbefugnisse	229
b) Untersagungsermächtigung	230
c) Sanktionen	230
d) Fazit	231
3.) Bundesamt für Sicherheit in der Informationstechnik	231
a) Entwicklung des BSI	231
b) Zielsetzung und Handlungsauftrag	232
c) Informationsaustausch	233
d) Bewertung	234
e) Fazit	235
4.) Zwischenergebnis	236
II. Vertikaler institutioneller Rahmen	236
1.) Telekommunikationsaufsicht	237
a) Meldepflichten	238
b) Überwachungsbefugnisse	238
(1) Allgemeine Befugnisse	238
(2) IT-spezifische Befugnisse	238
c) Hilfsbefugnisse	239
d) Untersagungsermächtigung und Sanktionen	239
e) Fazit	239
(1) Staatlicher Verantwortungsbereich	239
(2) Zugang zum Risikowissen	240
2.) Energieaufsicht	240
a) Genehmigungsvorbehalt	240
b) Überwachung	241
c) Sanktionen	242

d) Fazit	242
(1) Staatlicher Verantwortungsbereich	242
(2) Zugang zum Risikowissen	243
(3) Ausblick	243
3.) Finanzaufsicht	244
a) Reform durch das Finanzdienstleistungsaufsicht-Errichtungs-Ge- setz	245
(1) Frühere Struktur	245
(2) Neue Struktur	245
b) Aufsicht der Kredit- und Finanzdienstleistungsinstitute nach KWG	247
(1) Ziele der Aufsicht	247
(2) Genehmigungsvorbehalt	247
(3) Überwachungsbefugnisse	248
(4) Untersagungsermächtigung und Sanktionen	248
c) Sicherheit der Zahlungsverkehrssysteme	249
d) Fazit	251
(1) Staatlicher Verantwortungsbereich	251
(2) Zugang zum Risikowissen	251
4.) Vergleich der vertikalen Aufsichtsstrukturen	252
a) Erlaubnisvorbehalte	252
b) Anzeigepflichten	253
c) Überwachungsbefugnisse	253
d) Untersagungsermächtigungen	253
e) Fazit	254
III. Resümee	255
1.) Staatliche Verantwortungsbereiche	255
2.) Zugang zu Risikowissen	256
E. Bewertung der einfachgesetzlichen Ausgestaltung	257
I. IT-Sicherheit als Regelungsgegenstand	257
1.) Allgemeine Situation	257
2.) Horizontaler Regelungsrahmen	258
3.) Vertikaler Regelungsrahmen	258
4.) Gesetzgeberischer Nachbesserungsbedarf	260
II. Verantwortungsordnung	260
III. Informationsaustausch	262
F. Zwischenergebnis	263
I. Überarbeitung vorhandener Regelungen	263
II. Kein Erlass neuer Regelungen	264
III. Risikoermittlung und -bewertung im Bereich kritischer Infrastrukturen	265

4. Teil. Supranationale Vorgaben und Entwicklungsperspektive	267
A. Überblick	267
B. Entwicklung auf europäischer Ebene	268
I. Primäres Gemeinschaftsrecht	268
1.) Telekommunikation und Energieversorgung	268
2.) Finanzsektor	270
II. Sekundäres Gemeinschaftsrecht	270
1.) Horizontal wirkende Richtlinien	271
2.) Richtlinien in den einzelnen Sektoren	272
a) Telekommunikationsinfrastruktur	272
b) Energieversorgung	274
(1) Hintergrund	274
(2) Sicherheit der Energieversorgung	275
c) Finanzinfrastruktur	276
III. Sonstige Einzelmaßnahmen	277
1.) Sicherheit von IT-Systemen	278
2.) Sicherheits-Initiativen	279
3.) Begleitende Forschungsprogramme	281
4.) Informationsaustausch	283
5.) ENISA.	283
IV. Zwischenergebnis	285
C. Internationale Vorgaben	286
I. UNO	286
II. FIRST	287
III. OECD-Empfehlungen	287
IV. Cybercrime-Konvention	288
V. Telekommunikationsinfrastruktur	288
1.) WTO	289
2.) ITU	289
VI. Energieversorgungsinfrastruktur	290
VII. Finanzinfrastruktur	291
VIII. Zwischenergebnis	292
D. Nationale Initiativen zum Schutz kritischer Infrastrukturen	293
I. USA	293
1.) Anfänge	294
a) Analyse der Situation	294
b) Schlussfolgerungen	295
c) Presidential Decision Directive 63.	296
(1) National Infrastructure Assurance Council (NIAC)	296
(2) Critical Infrastructure Assurance Office (CIAO)	296

(3) National Infrastructure Protection Center (NIPC)	297
(4) Information Sharing and Analysis Center (ISAC).	297
(5) Partnership for Critical Infrastructure Security (PCIS)	298
2.) Umgestaltung unter der Bush Administration	298
a) PCIPB und Homeland Security Advisory Council	299
b) Office of Homeland Security und Homeland Security Council	299
c) National Infrastructure Advisory Council	300
d) Department of Homeland Security	300
e) National Strategy to Secure Cyberspace	301
II. Andere Länder	302
1.) Großbritannien	302
2.) Schweiz	304
3.) Kanada	306
III. Bewertung	306
IV. Handlungsansätze in Deutschland	307
1.) Anfänge	307
2.) AG KRITIS	308
3.) Partnerschaft Sichere Internet-Wirtschaft	310
4.) Internet-Portal Sicherheit-im-Internet	310
5.) Task Force Sicheres Internet	311
6.) Arbeitskreis Sicherheit von Infrastruktursystemen (AKSIS).	311
V. Zwischenergebnis	312
E. Entwicklungsperspektive	313
I. Zugang zu Risikowissen	314
1.) Informationspflichten nach dem Vorbild der Störfallverordnung	314
a) Informationsaustausch zwischen den Betreibern	314
b) Meldesystem zwischen Betreiber und Aufsichtsbehörden	314
c) Überwachungssystem der Behörden	316
d) Fazit	316
2.) Freiwilliger Informationsaustausch	317
II. Behebung von Vollzugsdefiziten	318
1.) Erfahrungen mit dem Jahr-2000-Problem	318
2.) Bewertung	320
III. Ansätze für eine institutionelle Neuorientierung	320

1.) Reform des BSI	321
2.) Beratungsgremien	321
IV. Europäische und Internationale Einbettung	323
F. Ergebnis	325
G. Schlusswort	325
Stichwortverzeichnis	327