

Inhaltsverzeichnis

Kapitel 1: Einleitung – IT-Sicherheitsmanagement als betriebliches Risikomanagement	19
A. Einleitung und Gang der Untersuchung	19
B. Wirtschaftliche Bedeutung der IT-Sicherheit in deutschen Betrieben	24
I. Betroffenheit von Unternehmen und Auswirkungen auf den Geschäftsbetrieb	25
II. Die Betriebsorganisation als Angriffsvektor	27
III. Die technische Infrastruktur als Angriffsvektor	30
1. Funktionsweise von Ransomware	30
2. Funktionsweise von DDoS-Angriffen	31
3. Aktuelle praktische Entwicklungen	32
C. Technische Standards für IT-Sicherheitsmanagementsysteme	34
I. Einheitliche Implementierungsstandards	34
II. Betriebsspezifischer Anpassungsbedarf	35
III. Maßgebliche Grundsatzentscheidung unter tatsächlicher Unsicherheit	37
D. Fazit	39
Kapitel 2: NIS-Richtlinie: erstes <i>lex generalis</i> zur IT-Sicherheit der Union	41
A. Grundlegende Erwägungen des Europäischen Gesetzgebers	41
I. IT-Systeme und -netze als volkswirtschaftliches Clusterrisiko	42
1. Abweichen des betrieblichen Risikos von volkswirtschaftlichem Risiko	42
2. Das digitale „race to the bottom“	44
3. Der wirtschaftliche Kern der Regulierung	45
4. Grundlegende Mechanismen des Europäischen Regelungskonzepts	46
II. Auslegungsmaßstab und Subsidiarität	47

B. Allgemeine Regelungen der NIS-Richtlinie	48
I. Allgemeine Maßgaben	48
II. Persönlicher Anwendungsbereich	49
1. Wesentliche Dienste	49
2. Dienste mit gemischtem Dienstleistungsprofil	50
3. Digitale Dienste	50
4. Grundlage der materiell-rechtlichen Differenzierung	51
III. Art der Aufsicht – Differenzierung nach Adressaten	52
1. Präventives und reaktives Aufsichtsregime	52
2. Ermittlung wesentlicher Dienste durch Mitgliedstaaten	52
3. Grundlegende qualitative Wertung des Europäischen Gesetzgebers	54
C. Sicherheitsanforderungen aufgrund der NIS-Richtlinie	55
I. Hoher Abstraktionsgrad durch technologieoffenen Regulierungsansatz	55
1. Grundsätzliche Regelungsmöglichkeiten	55
2. Funktionsweise von Software und Auswirkung einer Normung	58
3. Fehlende Infrastruktur für produktbezogenen Regulierungsansatz	60
II. Auslegung des Normbefehls	60
1. Wortlaut: umfassende Risikoprävention	61
2. Telos: Schutz der Produktion	63
3. Eigenes Fazit: teleologische Restriktion	64
III. Materielle Unterscheidung zwischen Adressaten	66
1. Formelle Dopplung sprachlich einheitlicher Standards	66
2. Einordnung des Maßnahmenkatalogs	67
3. Subjektive Auslegung des Tatbestands als Leiterwägung für Betreiber digitaler Dienste	70
IV. Vereinbarkeit der Differenzierung mit Art. 20 GRCh	71
1. Hintergründe der Reformbestrebung	72
2. Wertung im Rahmen des Art. 20 GRCh	72
a. Zulässigkeit der Differenzierung aufgrund des wirtschaftlichen Risikoprofils	73
b. Hilfsweise: Rechtfertigung durch Sicherheitsbelange?	75
3. Rechtsfolge des Verstoßes	77

D. Meldepflichten für Betreiber	78
I. Die Meldepflicht	78
1. Inhalt der Meldepflicht	79
2. Meldepflichtige Vorfälle	79
3. Informationsobliegenheit der Adressaten	80
II. Zulässigkeit der Differenzierung	81
III. Haftungsprivileg der Betreiber im Bereich der Meldepflichten	83
E. Zusammenfassung zur NIS-Richtlinie	86
 Kapitel 3: IT-Sicherheit als Regelungsgegenstand des nationalen Rechts	 89
A. Das IT-SiG und seine Novelle	89
I. Hintergrund zum IT-SiG	89
II. Kontinuierliche Erweiterung des persönlichen Anwendungsbereichs	91
1. Der Begriff des Betreibers Kritischer Infrastruktur	92
a. Bestimmbarkeit der Branchenzugehörigkeit	93
b. Bestimmbarkeit der hohen Bedeutung für das Funktionieren des Gemeinwesens	94
2. Nähere Bestimmung durch Rechtsverordnung	97
a. Die normative Qualität der Rechtsverordnung	98
b. Verhältnis der Wertungen nach § 2 Abs. 10 BSIG und § 10 Abs. 1 BSIG	99
c. Hinreichende Bestimmtheit der Ermächtigung zum Erlass einer Rechtsverordnung	102
d. Der Wesentlichkeitsvorbehalt	104
e. Das Bestimmtheitsgebot	105
3. Unternehmen im besonderen öffentlichen Interesse	107
a. Bisherige Kritik	108
b. Vereinbarkeit mit dem Wesentlichkeitsvorbehalt	108
4. Registrierungspflicht nach dem IT-SiG 2.0	111
a. Registrierung und Informationsrecht des BSI	111
b. De lege ferenda: das BSI als Informationstreuhand?	112
B. inhaltliche Vorgaben des BSIG für die betriebliche IT-Sicherheit	114
I. Der Normtext	114

II. Offene Fragen	116
1. Zwingender Charakter der Regelung	116
2. Angemessenheit der Maßnahmen	118
3. Schutzziel der Maßnahmen	119
4. Das „angemessene“ Schutzniveau	121
a. Systematisch: Die Grenze des Übermaßverbots	122
b. Berücksichtigung des unionsrechtlichen Telos	123
III. Konkretisierung durch Branchenstandards?	124
1. Begrenzte Feststellungswirkung	124
2. Vereinbarkeit fester Standards mit dem Stand der Technik	126
IV. Neuerungen durch das IT-SiG 2.0	128
1. Verpflichtende Einführung von Angriffserkennungssystemen	129
a. Technologieoffenes Regelungskonzept	129
b. Behördlicher Wissenstransfer als Grundlage der Angriffserkennung	130
2. Regulierung des Einsatzes kritischer Komponenten	131
a. Zielsetzung der Regelung	132
b. Befugnisse bei Einsatz kritischer Komponenten	133
3. Zertifizierungsbemühungen	134
a. Zielsetzung und Wirkungskreis der Maßnahme	134
b. Vereinbarkeit mit unionsrechtlichem Regelungsrahmen	135
4. Bußgelder	135
a. Anpassung des Bußrahmens	136
b. Folge: Risiko einer überschießenden Umsetzung des unbestimmten Normbefehls	136
V. Fazit: Unsicherheit der regulierten Entscheidung bewirkt Unbestimmtheit des Rechts	141
1. Sinnvolle Einzelmaßnahmen	141
a. Angriffserkennung als bundesweiter Sicherheitsbeitrag	142
b. Europäische Kultur des Risikomanagements	143
2. <i>Ex ante</i> : Fehlende Möglichkeit zur Erkenntnis der rechtmäßigen Handlung	144
a. Das zentrale Erkenntnisproblem	145

b. Grenzen der Regulierung von Entscheidungen unter Unsicherheit	148
VI. Meldepflichten nach § 8b BSIG	150
1. Meldepflichtige Vorkommnisse	151
2. Inhalt der Meldung	152
3. Zielsetzung: behördliche Informationsplattform	152
4. Einordnung und Bewertung	153
a. Erhöhung der Sicherheit durch Information der Betroffenen	153
b. Strukturelle Unbestimmtheit der Norm als hemmender Faktor	154
C. Umsetzung von NIS-2 – risikobasierte Regulierung <i>de lege ferenda</i> ?	155
I. Hintergründe der Reformbestrebung	156
1. Unionsrechtlicher Kontext und Ziele der Reform	157
2. Umwelt- und Verbraucherschutz als Nebenziel	158
3. Wunsch der Adressaten nach Wettbewerbsneutralität und Gleichbehandlung	158
4. Vereinfachung der Aufsicht	160
II. IT-Sicherheit als Form „richtiger“ Governance von Unternehmen	161
1. Grundsatz: Verantwortung der Geschäftsführung für IT-Sicherheit	161
2. Keine Haftung natürlicher Personen kraft Unionsrecht	163
3. Generalklausel und Konkretisierungsbemühungen	164
4. Erstreckung des Anwendungsbereichs: Regulierung der Lieferkette	167
5. IT-Sicherheit als subjektives Recht qua Unionsrecht?	169
III. Risikobeherrschung statt Risikomanagement?	172
1. Der Normtext	172
2. Der Regelungsplan des Europäischen Gesetzgebers zu den erforderlichen Maßnahmen	174
3. Der Regelungsplan des Europäischen Gesetzgebers zum sachlichen Anwendungsbereich	177
IV. Reform des Meldesystems zum Zwecke der Informationsgewinnung	179
1. Mehrstufiges Meldesystem	180
2. Analytische Folgemeldung	181

3. Förderung des privaten Informationsaustauschs zu IT-Sicherheit	182
V. Verschärfung der Sanktionsdrohung	184
D. Drittschutz der Pflichten nach § 8a und § 8b BSIG	185
I. Leitbildfunktion des § 8a Abs. 1 BSIG	186
1. Stand der Diskussion	186
2. Stellungnahme	187
II. Verkehrssicherungspflichten betreffs regulierter Netze	188
1. Wechselwirkung mit hinreichender Bestimmtheit des Rechts	188
2. Innere Begrenzung der Verkehrssicherungspflichten	188
III. Die nationale Diskussion um das BSIG als Schutzgesetz	191
1. Stand der Diskussion	191
2. Drittschutz des § 8a Abs. 1 BSIG nach nationalem Recht	192
3. Drittschutz des § 8b Abs. 4 BSIG	193
4. NIS-2: Drittschutz kraft unionsrechtskonformer Auslegung	194
a. Der Regelungsplan des Europäischen Gesetzgebers	194
b. Folgerungen für das nationale Recht	195
Kapitel 4: Der Umgang mit Unsicherheit im Recht	197
A. Die Ausprägungen von Unsicherheit im Recht	197
B. Grenzen für Unbestimmtheit durch Gesetzgebung	198
I. Das <i>loi précise</i> nach der Rechtsprechung des EGMR	199
1. Etablierung des Bestimmtheitsgebots durch die Rechtsprechung des EGMR	199
2. Aufgreifen dieser Rechtsprechung durch den EuGH	201
3. Fazit	202
II. Das nationale Bestimmtheitsgebot	202
1. Der allgemeine Bestimmtheitsgrundsatz	203
a. Die Prüfung des BVerfG	203
b. Die Rezeption des Bestimmtheitsgebots in der Literatur	205
c. Auftrag der Rechtsprechung zur Rechtsfortbildung?	206
2. Nullum crimen sine lege certa	208
a. Das Telos des Art. 103 Abs. 2 GG	208

b. Anforderungen an die hinreichende Bestimmtheit	209
(1) Die Optimierungsthese	209
(2) Die Abwägungslösung des BVerfG	210
(3) Der Präzisierungsauftrag der Strafjustiz	211
III. Einordnung und Zwischenfazit	213
C. Der Umgang mit unbestimmtem Recht durch den Rechtsanwender	214
I. Methodische Kritik am „bestimmten Recht“	214
1. Die deklaratorische Theorie der Rechtsanwendung	214
2. Die methodische Kritik Sagans an der deklaratorischen Theorie der Rechtsanwendung	215
3. Folgen dieser Kritik für die Rechtsanwendung	216
II. Widerstreitende Schlussfolgerungen	217
1. Sagan: Rechtsfindung erst durch den Richter	217
2. Scheuch: Relativ richtiges Recht	218
3. Die Analyse Dauner-Liebs und das richtige Recht als regulative Idee	218
III. Wahrheit als regulative Idee und methodische Schlussfolgerungen aus diesem Prinzip	220
1. Der innere Widerspruch der deklaratorischen Theorie	220
2. Beliebigkeit als Grenze der Rechtsanwendung	221
3. Selbstüberprüfung als regulatives Prinzip	222
D. These und Anwendung auf das BSIG	223
I. Zulässigkeit der Unbestimmtheit nach diesen Maßstäben	224
1. Unbestimmtheit als Charakteristikum des Rechts	224
2. Bemessung der Unbestimmtheit als unmöglicher Prüfauftrag	226
3. Der Schutzzweck als Auslegungsmaßstab	227
II. Auslegung des BSIG	231
Kapitel 5: Die rechtmäßige Betriebsorganisation	233
A. Analyse der rechtlichen Anforderungen an die Betriebsorganisation	235
I. Pflicht zur Beobachtung der wirtschaftlichen Lage des Unternehmens	235

II. Pflicht zur Erkennung bestandsgefährdender Risiken nach	
§ 91 Abs. 2 AktG	236
1. Die maßgebliche Zielvorgabe	237
2. Die hiernach erforderlichen Maßnahmen	238
a. Der Regelungsplan des Gesetzgebers	238
b. Die Rezeption der Pflicht durch Wissenschaft und Rechtsprechung	240
(1) LG Berlin: die Geeignetheit der Maßnahmen als Beweisfrage	240
(2) OLG Celle: kein Risikomanagement erforderlich	241
(3) OLG Frankfurt: Ermessensspielraum, jedoch Beachtlichkeit gesetzlicher Vorgaben	242
(4) LG Stuttgart – „Porsche“: konzernweite Geltung und „gewisses“ Ermessen	244
c. Einordnung	245
3. Folgerung für die Fragestellung	246
III. Kraft Rechtsfortbildung: Legalitätskontrollpflicht	247
1. Der unbestimmbare Gehalt der Legalitätskontrollpflicht	248
2. Einordnung	249
B. Konkretisierung der Fragestellung	250
C. Die Legalitätsbindung bei rechtlicher Unsicherheit	251
I. Einschränkung der Legalitätsbindung bei unklarer Rechtslage	251
1. Die strenge Legalitätsbindung als Ausgangspunkt	251
2. Einschränkung bei rechtlicher Unsicherheit	252
II. Herleitung der Legalitätsbindung von Organen	254
1. Ermessen und Beurteilungsspielraum als immanentes Element von Leitungsmacht	254
a. Bindung nur im Bereich der Rechtsermittlung	255
b. Rechtsbindung nur bei äußerst bedeutsamen Allgemeininteressen	255
c. Strenge Legalitätsbindung als Relikt?	256
d. Pflicht zum rechtlichen Risiko?	257
2. Relativierung der Rechtsbindung aufgrund des Gesellschaftsinteresses	257
a. Vorsätzliche Rechtsverstöße als Grenze	257

b. Gesamtabwägung des Rechtsverstoßes	258
3. Differenzierung zwischen strikter und nicht strikter Gesetzesbindung	259
4. Legalitätsbindung als Grenze der Privatautonomie	260
a. Legalitätsbindung des Vorstands als Grenze der Privatautonomie	260
b. Beschränkung der Legalitätsbindung aufgrund fehlender Regelung	262
5. Legalität als Ausdruck von Verantwortung	264
III. Anforderungen an Umgang mit unklarer Rechtslage	264
1. Strikte Legalitätsbindung	266
2. Negative Abgrenzung der Legalitätsbindung	267
a. Die negative Definition der Legalitätspflicht	267
b. Der Pflichtenkatalog bei unklarer Rechtslage	269
3. Prüfung der Erkenntnis, keine Prüfung der Entscheidung	270
a. Keine freie Rechtswahl durch Geschäftsleiter	270
b. Kein Stillstand des Rechts durch Verrechtlichung des Entscheidungsinhalts	271
4. Soziales Recht zum Risiko	273
a. Das Recht zum wirtschaftlichen Eigennutz	274
b. Geschäftsleiter als Risikoträger der rechtlichen Unsicherheit?	276
c. Kein Fehlanreiz bei unklarer Rechtslage	277
5. Beurteilungsspielraum als Folge unsicherer Rechtslage	278
a. Alleinige Haftung der Gesellschaft bei Bagatellverstößen	278
b. Handlungsspielraum bei Zweckmäßigkeitserwägungen	280
6. Entscheidungszuständigkeit der Organe der Gesellschaft?	282
a. Unergiebige Definitionsversuche	282
b. Unterscheidung nach Art und Überprüfbarkeit der statuierten Handlungspflicht	283
c. Anwendung auf Organisationsentscheidungen und regulatorische Normen	284
IV. Stellungnahme	286
1. Das „Feststehen“ des Rechts im Entscheidungszeitpunkt	286

2. Die allgemeine Abwägung der Rechtsbindung mit dem Unternehmensinteresse	290
3. Anwendung auf das BSIG	292
Kapitel 6: Zusammenfassung in Thesen	297
Literaturverzeichnis	313