

# Cybersecurity

Herausgegeben von

**Dennis-Kenji Kipker**

Bearbeitet von dem Herausgeber und von

*Dr. Malek Barudi, M.Jur.*, Hamburg; *Klaus Beucher*, Düsseldorf; *Jun.-Prof. Dr. Dominik Brodowski, LL.M. (UPenn)*, Saarbrücken; *Arnd Boken*, Berlin; *Dr. Axel Freiherr von dem Bussche, LL.M.*, Hamburg; *Prof. Dr. Wolfgang Däubler*, Bremen; *Dr. Theresa Ehlen*, Düsseldorf; *Eike Ekrot*, Berlin; *Matthias Fischer*, Berlin; *Maike Fromageau*, Düsseldorf; *Prof. Dr. Thomas Kemmerich*, Bremen; *Dr. Thomas Lapp*, Frankfurt a.M.; *Dipl.-Ing. Sven Müller*, Frankfurt a.M.; *Prof. Dr. Michael Schmidt*, München; *Dr. Karsten Sohr*, Bremen; *Florian Tannen*, München; *Dr. Friederike Voskamp, LL.M. (Berkeley)*, Hamburg; *Dr. Gunter Warg*, Brühl; *Dr. Nicolai Wiegand, LL.M. (NYU)*, München

1. Auflage 2020

**C.H.BECK**

# Inhaltsverzeichnis

Bearbeiterverzeichnis	XXV
Abkürzungsverzeichnis	XXVII

## Kapitel 1. Grundlagen und Strukturen

A. Grundlegende Begrifflichkeiten und Zusammenhänge	2
B. Technische und rechtspolitische Entwicklungen in der Cyber-Sicherheit – deutsche und europäische Cyber-Sicherheitsstrategien	5
I. Deutsche Cyber-Sicherheitsstrategien	5
II. Europäische Cyber-Sicherheitsstrategien	8
C. Rechtliche Grundlagen der Cyber-Sicherheit in Deutschland und in der EU	9
I. Rahmenvorschriften und Auslegungsmethoden	10
II. Bereichsspezifische gesetzliche Regelungen und Normenhierarchie	12
1. Rechtsnatur	13
2. Gesetzgebungskompetenzen	14
3. Normenhierarchie	15
4. Kollisionsregeln	15
D. Zentrale Themen im Cyber-Sicherheitsrecht	16
E. Schnellübersicht	21

## Kapitel 2. Technische Grundlagen der Informationssicherheit

A. Grundlagen der Informationssicherheit	25
I. Information und Kommunikation	25
II. Schutzziele	26
1. Vertraulichkeit	26
2. Integrität	26
3. Verfügbarkeit	26
4. Datenschutz	27
5. Authentizität	27
6. Zurechenbarkeit/Nicht-Abstreitbarkeit	27
III. Authentisierung, Autorisierung, Audit	27
IV. Berechtigungen und Rollen	28
B. Kryptographie	29
I. Grundlagen der Kryptographie	29
1. Grundlegende Begrifflichkeiten	30
2. Kryptoanalyse	30
II. Symmetrische Verschlüsselung	31
1. Strom- und Blockchiffren	31
2. Betriebsmodi von Blockchiffren	32
3. Gängige Verfahren, Schlüssellängen	32
III. Asymmetrische Verschlüsselung	34
1. Gängige Verfahren, Schlüssellängen	35
2. Eigenschaften asymmetrischer Kryptographie	37
IV. Kryptographische Hashfunktionen	38
1. Typische kryptographische Hashfunktionen	39
2. Message Authentication Codes	40

# Inhaltsverzeichnis

V. Digitale Signaturen	40
VI. Zertifikate und Public Key-Infrastruktur	42
VII. Beispiele für Kryptosysteme aus der Praxis	43
1. Transportverschlüsselung im WWW	43
2. E-Mail-Sicherheit	47
VIII. Zusammenfassung	49
C. Kommunikationsnetze	50
I. Grundlagen der Kommunikationsnetze	50
1. Paketorientierte Kommunikation	50
2. Internet Protocol (IP)	52
3. Die Transport Protokolle TCP und UDP	54
4. Kommunikation in Netzen (OSI Referenz-Modell)	55
5. Kommunikation in lokalen und in globalen Netzen	56
6. Netzdienste (ARP, DNS, DHCP, ICMP, NAT)	57
a) Domain Name System (DNS)	57
b) Address Resolution Protocol (ARP)	58
c) Dynamic Host Configuration Protocol (DHCP)	58
d) Internet Control Message Protocol (ICMP)	58
e) Network Address Translation (NAT)	59
II. Netzkonzepte	59
1. Kabelgebundene Netze	60
2. Drahtlose Netze	60
a) Wireless Local Area Networks (WLAN)	60
b) Mobilfunknetze (GSM, GPRS, 3G, 4G, 5G)	61
III. Zusammenfassung	61
D. Angriffe, Bedrohungen und Gegenmaßnahmen	61
I. Sicherheitslücken als wichtige Ursache für Schadsoftware	62
II. Malware: Viren, Würmer, Trojaner, Spyware und Ransomware	65
III. Social Engineering	67
IV. (Distributed) Denial-of-Service-Angriffe	68
V. Bedrohungen gegen (mobile) Endgeräte und Apps	69
VI. Bedrohungen für komplexe IT-gestützte Anwendungen	71
VII. Sicherheitsmaßnahmen	71
VIII. Zusammenfassung	72
E. Informationssicherheit managen	73
I. Informationssicherheitsmanagementsystem (ISMS)	73
II. Standards in der Informationssicherheit	74
1. ISO 27000-Familie	75
2. BSI IT-Grundschutz	76
a) BSI IT-Grundschutz-Bausteine	76
b) Schutzbedarf	77
c) BSI IT-Grundschutz Vorgehensweise, Standard-Absicherung	78
3. Informationssicherheitsmanagementsystem in zwölf Schritten (ISIS12) ..	79
4. Das Lebenszyklusmodell	81
III. Zusammenfassung	81
F. Schnellübersicht	81

**Kapitel 3. Stand der Technik**

A. Stand der Technik als unbestimmter Rechtsbegriff	84
I. Abgrenzung unterschiedlicher Technologieniveaus	84
1. Allgemein anerkannte Regeln der Technik	85
2. Stand der Technik	86
3. Stand von Wissenschaft und Technik	86
II. Verwendung des „Stand der Technik“	87
1. Technische Norm	88
2. Standard	89
3. Technische Richtlinien	90
B. „Stand der Technik“ im Bereich des Cyber-Sicherheitsrechts	91
I. Gesetzliche Vorgaben	92
II. Branchenspezifische Sicherheitsstandards (B3S)	95
C. Einführung eines Informationssicherheitsmanagements zur technisch-organisatorischen Abbildung des „Stand der Technik“	97
I. IT-Grundschatz vom BSI	98
1. BSI-Standard 200-1 „Managementsysteme für Informationssicherheit“	98
2. BSI-Standard 200-2 „IT-Grundschatz-Methodik“	99
3. BSI-Standard 200-3 „Risikoanalyse auf der Basis von IT-Grundschatz“	99
4. BSI-Standard 100-4 „Notfallmanagement“	99
II. Informationssicherheitsmanagementsystem (ISMS) auf Basis der ISO/IEC 27001	100
1. Sektor- bzw. Branchenspezifika:	100
2. Themenspezifische Standards:	101
D. Schnellübersicht	102

**Kapitel 4. Branchenübergreifende Vorgaben**

A. Einführung	107
B. Typische betriebliche Schadensrisiken und deren Ursachen	108
I. Risiken von außen	108
II. Risiken von innen	111
1. Die Unternehmensleitung	112
2. Die IT-Systeme	113
3. Die Mitarbeiter	114
C. Branchenübergreifende Rechtsgrundlagen der IT-Sicherheit	115
I. Abgrenzung von branchenübergreifenden und branchenspezifischen rechtlichen Pflichten zur IT-Sicherheit	115
1. Systematik	115
2. Einführung in die bereichsübergreifenden Rechtspflichten	115
3. Kurze Darstellung branchenspezifischer Rechtspflichten	116
a) KRITIS-Betreiber	116
b) Telemedien und Telekommunikationsdienste	117
c) Weitere Sonderregelungen für Einzelbereiche	117
4. Gegenüberstellung	118
II. Gewährleistung der IT-Sicherheit als unternehmerische Sorgfaltspflicht	119
1. Pflicht zur Früherkennung bestandsgefährdender Risiken	119
2. Allgemeine Leitungs- und Sorgfaltspflicht der Unternehmensleitung ....	120
a) Leitungs- und Sorgfaltspflicht des Vorstands der Aktiengesellschaft ...	120
b) Leitungs- und Sorgfaltspflicht des GmbH-Geschäftsführers	124

# Inhaltsverzeichnis

3. Praktische Erwägungen	125
III. Buchführungspflichten als IT-Sicherheitspflichten	126
1. Pflicht zur ordnungsgemäßen Buchführung	126
2. Pflichten bei der Erstellung des Lageberichts	128
3. Die Rolle des Abschlussprüfers	128
4. Checkliste der grundlegenden IT-sicherheitsrechtlichen Pflichten aufgrund branchenübergreifender Rechtsgrundlagen	129
D. Branchenübergreifende Sonderkonstellationen im IT-Sicherheitsrecht	130
I. Cloud Computing	130
1. Technische Rahmenbedingungen	130
2. IT-sicherheitsrechtliche Aspekte	132
3. Datenschutz in der Cloud	133
4. Zertifizierungen als Lösungsansatz	134
II. Industrie 4.0	134
1. Maßnahmen zur Angriffssicherheit	135
2. Schutz von Unternehmensdaten, Knowhow und Geschäftsgeheimnissen	135
3. Schutz personenbezogener Daten	136
4. Haftung in der Smart Factory	136
II. Big Data	136
III. IT-Outsourcing	138
IV. Das Internet der Dinge (IoT)	139
V. Bring Your Own Device	140
1. IT-Sicherheit	141
2. Datensicherheit und Datenschutz	142
VIII. IT-Forensik (rechtssichere Ermittlungen nach IT-Sicherheitsvorfällen)	144
1. Grundlagen der IT-Forensik	144
2. Durchführung einer IT-forensischen Analyse	144
VIII. Versicherungsschutz und Cyberpolicen	146
1. Versicherungsschutz für Eigenschäden	146
2. Versicherungsschutz für Haftpflichtansprüche	146
3. Versicherungsschutz für Datenschutzverfahren	147
4. Versicherungsschutz für Krisenmanagement: Das Incident Response Team	147
E. Schnellübersicht	147

## Kapitel 5. Datenschutz

A. Datenschutz und Informationssicherheit im Wechselwirkungsverhältnis	152
B. Datenschutzrechtliche Anforderungen an die Datensicherheit	153
I. Regelungssystematik	154
II. Datensicherheit durch geeignete technische und organisatorische Maßnahmen	157
III. Zur Wahl und Umsetzung der erforderlichen Maßnahmen	158
IV. Heranziehung der Datenschutz-Folgenabschätzung im Rahmen der Risikoabschätzung	161
V. Genehmigte Verhaltensregeln oder genehmigtes Zertifizierungsverfahren ...	162
VI. Datenschutzrechtliche Aufsicht	163
C. Datenschutzrechtliche Beschränkungen für Maßnahmen der Informationssicherheit	163
I. IT-Sicherheitsmaßnahmen als Eingriff in die Privatsphäre	164

II. Bestimmung des Personenbezugs	164
III. Anforderungen an die Datenverarbeitung	167
1. Allgemeine datenschutzrechtliche Vorgaben	167
2. Datenschutzrechtliche Vorgaben im Bereich der Telekommunikation ...	169
3. Mitteilungen an das BSI	170
4. Datenverarbeitung durch das BSI zu Sicherheitszwecken	171
D. Schnellübersicht	173

## Kapitel 6. Corporate Governance und Compliance

A. Begrifflichkeit: Governance/Compliance und IT-Governance/IT-Compliance ..	177
B. Grundlagen der IT-Governance	178
I. IT-Governance nach dem ITGI	178
II. Übersicht der aktuellen Standards und Frameworks im Bereich der IT-Governance	179
III. Die Einbindung der IT-Compliance in die Mechanismen der Governance	181
C. Grundlagen der IT-Compliance	181
I. Relevante Compliance-Themen für die IT-Sicherheit	181
II. Regelungen und Maßstäbe zur Umsetzung der IT-Compliance und IT-Sicherheit im Unternehmen	182
III. Die Implementierung der IT-Sicherheit als Element des Schutzes personenbezogener Daten	185
D. IT-Compliance und IT-Sicherheit als Aufgaben der Unternehmensleitung	188
I. Die Geschäftsführer- bzw. Vorstandshaftung	188
II. Die Informations- und Mitbestimmungsrechte des Betriebsrats bei der Einführung oder Änderung von IT-Systemen	190
III. Der IT-Sicherheitsbeauftragte	190
E. Das Risikomanagement im Unternehmen	193
I. Typische interne und externe Betriebssicherheitsrisiken	193
II. Die Einrichtung eines Risikomanagementsystems in der IT	194
III. Erwägungen zum Abschluss einer Versicherung gegen Cyberrisiken	195
F. Ausgewählte Richtlinien zur IT-Sicherheit im Unternehmen	196
I. Die IT-Richtlinie als Handlungsstandard	196
II. Auswahl zentraler Elemente einer IT-Richtlinie	197
III. Regelmäßige Kontrollen und Sanktionen	198
G. Das Compliance-Risiko der Übererfüllung sicherheitsbezogener Pflichten	199
I. Rechte Dritter als Beschränkung der IT-Sicherheit	199
II. Problembereich: Die Überwachung von E-Mail- und Internetnutzung zu Compliance-Zwecken	200
III. Die betriebsverfassungsrechtliche Zulässigkeit von Maßnahmen der IT-Sicherheit	202
H. Schnellübersicht	202

## Kapitel 7. IT-Vertragsrecht

A. Vertragstypologisierung von IT-Verträgen	206
---	-----

# Inhaltsverzeichnis

B. Typische IT-Vertragstypen	208
I. Softwarebeschaffung	209
1. Entwicklung und dauerhafte Überlassung von Individualsoftware	211
a) Sonderproblem des § 650 BGB	212
b) Softwareentwicklung mit Hilfe agiler Projektmethoden	214
c) Abnahme	216
2. Dauerhafte Überlassung von Standardsoftware	216
3. Implementierung und Anpassung von Standardsoftware	218
4. Befristete Überlassung von Individualsoftware	219
5. Befristete Überlassung von Standardsoftware	220
a) Application Service Providing (ASP), Software as a Service (SaaS), Cloud Computing	221
b) Leasing	221
c) Leihe	222
II. Hardwarebeschaffung	222
III. Pflege und Wartung	222
IV. Beratung	228
V. Schulung	229
VI. Sonstige Vertragstypen	229
C. Schnellübersicht	230

## Kapitel 8. Ziviles Haftungsrecht

A. Rechtsgrundlagen zivilrechtlicher Haftung	234
I. Vertragliche Haftung	234
II. Vertrag	234
III. Vertragsähnliche Beziehung	236
IV. Gesetzliche Schuldverhältnisse	236
1. Geschäftsführung ohne Auftrag	236
2. Eigentümer-Besitzer-Verhältnis	237
3. Ungerechtfertigte Bereicherung	237
4. Deliktsrecht	237
5. Typen gesetzlicher Schuldverhältnisse	240
6. Persönliche Haftung von Organen	241
7. Haftung auf Schadensersatz wegen Pflichtverletzung	241
8. Verzugseintritt	241
9. Verzugsschaden	243
10. Rücktrittsrecht im Fall des Verzuges	243
11. Gewährleistungsansprüche	243
V. Haftung für Dritte	245
1. Erfüllungsgehilfen	245
2. Haftung für Mittäter und Beteiligte	245
3. Marktanteilshaftung	245
4. Verrichtungsgehilfen	245
5. Gesamtschuld	246
VI. Weitere Haftungsgrundlagen	246
1. Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)	246
2. Grundsätze ordnungsgemäßer Buchführung	248
3. Datenschutzrecht	249
4. Kritische Infrastrukturen	250
5. ProdukthaftungsG	250
6. Fehlerbegriff	251

7. Störerhaftung des BGH	251
8. EU-Richtlinie für digitale Inhalte	251
B. Begrenzung der Haftung	252
I. Haftungsbegrenzung	252
II. Vertragliche Haftungsbegrenzung	252
III. Haftungsbegrenzung durch Rechtsform	253
IV. Haftungsbegrenzung durch Versicherung	254
1. Haftpflichtversicherung	254
2. D&O-Versicherung	256
3. Cyberversicherung	256
C. Fallgestaltungen	258
I. Lieferung von fehlerhafter Software/Updates	258
1. Bedeutung von Programmfehlern	258
2. Arten von Fehlern in Software und Updates	258
3. Beteiligte	259
4. Anbieter	259
a) Hersteller	259
b) Händler	260
c) OEM, VAR, etc	260
d) Systemhäuser	260
e) Dienstleister	260
5. Haftung	261
a) Gewährleistung	261
b) Vertragliche Haftung	264
c) Deliktische Haftung	266
6. Software-Nutzer	266
a) Mitarbeiter	266
b) Datenschutzbeauftragte	267
c) Compliance Officer	267
7. Sonstige	268
II. Cyberangriffe	268
III. Infizierte Webseiten	269
IV. Verlust von Daten, Datenträgern oder mobilen Geräten	270
V. Infizierte E-Mails und Chats	271
D. Schnellübersicht	272

## Kapitel 9. Urheber- und Lauterkeitsrecht, Know-How-Schutz

A. Urheberrecht und verwandte Schutzrechte	274
I. Vorbemerkung	275
II. Allgemeines Urheberrecht	275
1. Schutzgegenstand	275
2. Verwertungsrechte	276
a) Vervielfältigungsrecht	277
b) Recht der öffentlichen Wiedergabe ..7	277
3. Urheberpersönlichkeitsrecht	283
4. Schranken	283
III. Softwareurheberrecht	284
1. Allgemeines	284
2. Schutzgegenstand	284
3. Verwertungsrechte und Schranken	285

# Inhaltsverzeichnis

IV. Datenbankrecht	287
1. Allgemeines	287
2. Schutzgegenstand	288
3. Rechte des Datenbankherstellers	288
V. Rechtsverletzungen	289
1. Ansprüche	289
2. Aktivlegitimation	289
3. Passivlegitimation	290
a) Täterschaft und Teilnahme	290
b) Störerhaftung	290
4. Haftungsprivilegierungen	292
VI. Technische Schutzmaßnahmen	294
B. Lauterkeitsrecht	294
I. Anwendungsbereich	295
II. Ausgewählte Einzelfälle	295
1. Screen Scraping	295
2. Bots	296
3. Domain-Grabbing	296
4. „Metatagging“ und „Index-Spamming“	297
5. Sniper-Software	297
6. Denial-of-Service („DoS Attacken“)	298
7. Haftung für Hyperlinks	298
C. Know-How Schutz	299
I. Frühere Rechtslage	299
II. Änderungen durch Know-How-Richtlinie und GeschGehG	300
D. Schnellübersicht	302
<b>Kapitel 10. Arbeitsrecht und IT-Sicherheit</b>	
A. Das traditionelle Arbeitsrecht als Ausgangspunkt	305
I. Historische Entwicklung	305
II. Die zwei Bestandteile des Arbeitsrechts	305
III. Errungenschaften und Lästigkeiten	306
IV. Prekär Beschäftigte	307
B. Überlagerung durch Sicherheitsinteressen?	307
I. Das Beispiel der kerntechnischen Anlagen	308
1. Konkrete Veränderungen im Arbeitsrecht	308
2. Die Auseinandersetzungen um die Mitbestimmungsrechte des Betriebsrats	309
3. Mögliche Alternativen?	310
II. Andere gefährliche Technologien	311
1. Luftverkehr	312
2. Chemische Industrie	312
3. Gefährliche Dienstleistungen, insbesondere im Bankensektor	313
III. Was wird einer Sonderregelung unterworfen?	314
C. Arbeitsvertragliche Pflichten zur Wahrung der IT-Sicherheit	315
I. Allgemein anerkannte Nebenpflichten aus dem Arbeitsverhältnis	315
1. Verhinderung von Angriffen	315
2. Störungen, die von Arbeitskollegen ausgehen	316
3. Mitwirkung an der Schadensbeseitigung	317

II. Erweiterung und Konkretisierung von Pflichten, insbesondere im Zusammenhang mit Compliance?	317
III. Qualifizierung wegen neuer Anforderungen	318
1. Anspruch des Arbeitnehmers auf Weiterqualifizierung?	318
a) § 81 BetrVG?	319
b) Nebenpflicht des Arbeitgebers zur Schaffung der Voraussetzungen für die Arbeit	319
c) Tragweite der Arbeitgeberpflicht	320
d) Einbeziehung der Arbeitszeit	320
2. Pflicht des Arbeitnehmers zur Weiterqualifizierung	321
3. Mitbestimmungsrechte des Betriebsrats bei Weiterbildungsmaßnahmen	321
D. Sicherheitsüberprüfung	323
I. Anwendungsbereich	323
II. Durchführung der Sicherheitsüberprüfung	325
E. Grundsätze der IT-Sicherheit, insbesondere in Parallele zur Datensicherung	326
I. Arbeitsrechtliche Probleme der Datensicherung	326
II. Übertragung auf die IT-Sicherheit?	327
III. Beispiele für Regelungen zur IT-Sicherheit nach ISO 27002	328
1. Schutz der Privatsphäre	328
2. Kein abschließender Katalog	328
3. Sicherheitsüberprüfung bei Einstellungen?	329
4. Verantwortlichkeit des einzelnen Arbeitnehmers	329
5. Maßregelungsprozess	329
6. Regelung des Zugangs zu Informationen	330
7. Ereignisprotokollierung	330
IV. Regelungen zur IT-Sicherheit nach BSI-Grundschutz und nach den Richtlinien der Versicherungswirtschaft für die Informationssicherheit (VdS 3473)	331
F. Der Informationssicherheitsbeauftragte (ISB)	331
I. Die Beschreibung der Aufgaben des ISB	331
II. Voraussetzungen für die Bestellung	333
III. Sachliche und personelle Ressourcen des ISB	335
IV. Stellung in der Organisation	337
V. Beteiligung des Betriebsrats?	337
G. Schnellübersicht	338

## Kapitel 11. Prozessuale Durchsetzung

A. Hauptsacheverfahren vor staatlichen Gerichten	342
I. Formelle Fragen	342
1. Zuständigkeit	342
2. Klagearten	343
II. Sachvortrag	344
III. Beweis	345
1. Beweislast	345
2. Beweisbeschluss	346
3. Beweis durch Sachverständige	346
4. Strafanzeige	347
IV. Streitverkündung	347
V. Internationale Bezüge	349
B. Einstweiliges Verfügungsverfahren	350

# Inhaltsverzeichnis

C. Selbständiges Beweisverfahren	350
D. Außergerichtliche Streitbeilegung	351
I. Verhandlung	352
II. Schlichtung	352
III. Schiedsgerichtsbarkeit/Arbitration	352
IV. Mediation	353
E. Schnellübersicht	354

## Kapitel 12 Kritische Infrastrukturen

A. Übersicht der Regelungen für Kritische Infrastrukturen	361
B. Kritische Infrastrukturen iSd BSI-G	363
I. Überblick	363
II. Kritische Dienstleistungen	363
1. Sektor Energie (§ 2 BSI-KritisV)	364
a) Stromversorgung (§ 2 Abs. 2 BSI-KritisV)	364
b) Gasversorgung (§ 2 Abs. 2 BSI-KritisV)	364
c) Kraftstoff- und Heizölversorgung (§ 2 Abs. 3 BSI-KritisV)	364
d) Fernwärmeversorgung (§ 2 Abs. 4 BSI-KritisV)	364
2. Sektor Wasser (§ 3 BSI-KritisV)	365
a) Trinkwasserversorgung (§ 3 Abs. 2 BSI-KritisV)	365
b) Abwasserbeseitigung (§ 3 Abs. 3 BSI-KritisV)	365
3. Sektor Ernährung (§ 4 BSI-KritisV)	365
4. Sektor Informationstechnik und Telekommunikation (§ 5 BSI-KritisV)	365
a) Sprach- und Datenübertragung (§ 5 Abs. 2 BSI-KritisV)	365
b) Datenspeicherung und -Verarbeitung (§ 5 Abs. 3 BSI-KritisV)	365
5. Sektor Gesundheit (§ 6 BSI-KritisV)	366
a) Stationäre medizinische Versorgung (§ 6 Abs. 2 BSI-KritisV)	366
b) Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind (§ 6 Abs. 3 BSI-KritisV)	366
c) Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper (§ 6 Abs. 4 BSI-KritisV)	367
d) Laboratoriumsdiagnostik (§ 6 Abs. 5 BSI-KritisV)	367
6. Sektor Finanz- und Versicherungswesen (§ 7 BSI-KritisV)	367
a) Bargeldversorgung (§ 7 Abs. 2 BSI-KritisV)	367
b) Kartengestützter Zahlungsverkehr (§ 7 Abs. 3 BSI-KritisV)	368
c) Konventioneller Zahlungsverkehr (§ 7 Abs. 4 BSI-KritisV)	368
d) Verrechnung und Abwicklung von Wertpapier- und Derivatgeschäften (§ 7 Abs. 5 BSI-KritisV)	368
e) Versicherungsdienstleistungen (§ 7 Abs. 6 BSI-KritisV)	368
7. Sektor Transport und Verkehr (§ 8 BSI-KritisV)	368
8. Erweiterter Adressatenkreis durch IT-SiG 2.0	369
III. Betreiben einer Anlage	370
1. Anlagenbegriff	370
2. Betreiberbegriff (außer für den Finanzsektor)	371
a) Allgemeiner Betreiberbegriff	371
b) Abweichender Betreiberbegriff für Finanzdienstleistungen	372
c) Betreiberidentität	373
IV. Schwellenwert	374
1. Berechnung der Schwellenwerte bei „gemeinsame Anlagen“	375
a) Anlagen derselben Art	375

b) Enger betrieblicher (und räumlicher) Zusammenhang	375
2. Berechnung von Schwellenwerten bei Auslandsbezügen	377
C. Verpflichtungen für Betreiber Kritischer Infrastrukturen	378
I. Verpflichtungen nach dem BSIG	378
1. Sicherheit in der Informationstechnik Kritischer Infrastrukturen (§ 8a BSIG)	378
a) Angemessene Sicherheitsvorkehrungen nach dem Stand der Technik (§ 8a Abs. 1 BSIG)	378
b) Branchenspezifische Sicherheitsstandards (B3S) (§ 8a Abs. 2 BSIG) und weitere Konkretisierungen des Stands der Technik	380
c) Regelmäßige Nachweispflichten (§ 8a Abs. 3 BSIG)	381
d) Kontrollrechte des BSI	383
2. Kontaktstelle (§ 8b Abs. 3 BSIG) und übergeordnete Ansprechstelle (§ 8b Abs. 5 BSIG)	383
3. Meldepflichten bei Störungen (§ 8b Abs. 4 BSIG)	383
a) Voraussetzungen der Meldepflicht nach § 8b Abs. 4 BSIG	383
b) Inhalt der Meldung	385
c) Zeitpunkt der Meldung	386
4. Regelung über den Umgang mit iRd § 8b BSIG erhobenen personenbezogenen Daten	386
II. Territoriale Anwendung	387
III. Vorrang von Spezialregelungen für bestimmte Betreiber	387
1. Betreiber öffentlicher Telekommunikationsnetze oder öffentlich zugänglicher Telekommunikationsdienste	388
2. Betreiber von Energieanlagen und Energieversorgungsnetzen iSd EnWG	390
3. Die Gesellschaft für Telematik und Betreiber von Diensten der Telematikinfrastruktur	391
4. Genehmigungsinhaber nach § 7 Abs. 1 AtG	391
5. Besonderheiten für den Finanzsektor	392
IV. Übersicht über die IT-Sicherheits-, Melde- und Nachweispflichten nach den verschiedenen Gesetzen	392
D. Besondere Anforderungen an Anbieter digitaler Dienste	394
I. Digitale Dienste	395
1. Online-Marktplätze (§ 2 Abs. 11 Nr. 1 BSIG)	395
2. Online-Suchmaschinen (§ 2 Abs. 11 Nr. 2 BSIG)	396
3. Cloud-Computing-Dienste (§ 2 Abs. 11 Nr. 3 BSIG)	396
II. Anbieter digitaler Dienste	396
III. Verpflichtungen von Anbietern digitaler Dienste	398
1. Maßnahmen zur Bewältigung von Risiken für die Sicherheit der Netz- und Informationssysteme (§ 8c Abs. 1 und 2 BSIG)	399
2. Meldepflicht bei Störungen (§ 8c Abs. 3 BSIG)	399
3. Anbieter von Telemedien (§13 Abs. 7 TMG) und zusätzliche Verpflichtung als Anbieter einer Kritischen Infrastruktur	400
E. Folgen bei Pflichtverletzungen	401
I. Bußgelder	402
1. Bußgelder nach § 14 BSIG	402
a) Ordnungswidrigkeiten durch Betreiber Kritischer Infrastrukturen ....	403
b) Ordnungswidrigkeiten durch Anbieter digitaler Dienste	403
2. Spezialgesetzliche Bußgeldvorschriften	405
3. Geplante Anpassung der Bußgeldnormen	406

# Inhaltsverzeichnis

III. Zivilrechtliche Haftung	406
IV. Wettbewerbsrechtliche Folgen von IT-Sicherheitsverstößen	407
V. Beseitigung von Sicherheitsmängeln	407
1. Beseitigung von Sicherheitsmängeln nach dem BSIG	407
2. Beseitigung von Sicherheitsmängeln nach Spezialgesetzen	408
F. Schnellübersicht	408

## Kapitel 13. Gefahrenabwehr und Sanktionierung

A. Die Gewährleistung von Cyber-Sicherheit als Teil der öffentlichen Sicherheit ....	413
B. Die polizeiliche Abwehr konkreter Gefahren für die Cyber-Sicherheit	415
I. Polizeiliche Abwehr konkreter Gefahren für die Cyber-Sicherheit	416
1. Standardmaßnahmen zur Abwehr konkreter Gefahren für die Cyber-Sicherheit	417
a) Unterbrechung der Telekommunikation	417
b) Beschlagnahme bzw. Sicherstellung	417
c) Weitere Standardmaßnahmen	418
2. Polizeiliche Generalklausel und die Abwehr konkreter Gefahren für die Cyber-Sicherheit	418
II. Polizeiliche Informationseingriffe	419
C. Cyber-Sicherheit durch Strafrecht	421
I. Strafrechtliche Verfolgung von Verletzungen der Cyber-Sicherheit	422
1. Strafbewehrung von Verletzungen der Cyber-Sicherheit	422
a) Einführung	422
b) Verletzungen der Integrität und Verfügbarkeit informationstechnischer Systeme und der darin gespeicherten Daten	424
c) Verletzungen der Vertraulichkeit informationstechnischer Systeme und der darin gespeicherten Daten	428
d) Überblick	430
2. Strafverfahren zur Verfolgung von Verletzungen der Cyber-Sicherheit ..	431
a) Besondere strafprozessuale Ermittlungsmaßnahmen zur Ausforschung von Verletzungen der Cyber-Sicherheit im Überblick	432
b) Mitwirkungspflichten in Strafverfahren	436
c) Zum Verhalten als Geschädigter	437
II. Straf- und bußgeldrechtliche Inpflichtnahme zur Gewährleistung von Cyber-Sicherheit	437
1. (Spezial-)Gesetzliche Verpflichtungen zur Gewährleistung von Cyber-Sicherheit	438
2. Erfolgszurechnung bei Verletzungen der Cyber-Sicherheit durch Dritte	440
D. Schnellübersicht	442

## Kapitel 14. Nachrichtendienstrecht

A. Der Auftrag der Nachrichtendienste	446
I. Allgemeines	446
1. Abgrenzung der Nachrichtendienste zu Geheimdiensten	446
2. Trennungsgebot	447
3. Sammeln und Auswerten von Informationen	449
4. Keine Beschränkung auf Beratungs- bzw. Frühwarnfunktion	452
II. Der Auftrag der zivilen Verfassungsschutzbehörden	453
1. §§ 3, 4 BVerfSchG als gemeinsamer Auftrag von BfV und LfV	453

2. Tatsächliche Anhaltspunkte als Anlass für ein Tätig werden	454
a) Bedeutung und Abgrenzung zu verwandten Begriffen	454
b) Tatsächliche Anhaltspunkte als Synonym für „Verdacht“	454
c) Begriffsdefinition	455
d) Verdachtsfall und Prüffall	455
3. Unterschied zwischen Extremismusbeobachtung („Bestrebungen“ erforderlich) und Spionageabwehr („Tätigkeit“ genügt)	456
4. Begriff der Bestrebung	457
a) Personenzusammenschluss als Beobachtungsobjekt	457
b) Politische Zielsetzung erforderlich	459
c) Ziel- und zweckgerichtete Verhaltensweisen	460
d) Bezug zu Gewalt- bzw. Straftaten	460
e) Bezug zu konkreten Gefahren	461
5. Entschließungsermessens und Auswahlennessen bei der Beobachtung ...	461
6. Nötiger Inlandsbezug, aber Zulässigkeit der Tätigkeit auch im Ausland	462
7. Die zentralen Beobachtungsfelder des Verfassungsschutzes	462
a) Bestrebungen gegen die freiheitlich-demokratische Grundordnung (§ 3 Abs. 1 Nr. 1 BVerfSchG)	462
b) Bestrebungen gegen die Sicherheit des Bundes oder eines Landes (§ 3 Abs. 1 Nr. 1 BVerfSchG)	464
c) Spionageabwehr (§ 3 Abs. 1 Nr. 2 BVerfSchG)	465
d) Bestrebungen, durch die mittels Anwendung oder Vorbereitung von Gewalt auswärtige Belange gefährdet werden (§ 3 Abs. 1 Nr. 3 BVerfSchG)	473
e) Bestrebungen gegen den Gedanken der Völkerverständigung (§ 3 Abs. 1 Nr. 4 BVerfSchG)	474
III. Der Auftrag des MAD	474
IV. Der Auftrag des Bundesnachrichtendienstes	475
1. Informationen von außen- und sicherheitspolitischer Bedeutung	475
2. Wichtige Aufklärungsfelder des BND	476
3. Keine weiteren Voraussetzungen für Datenerhebung	477
B. Die Befugnisse der Nachrichtendienste	477
I. Allgemeines zu den Datenerhebungsregeln im BVerfSchG	478
II. Die wichtigsten Regelungen zu Erhebung von personenbezogenen Daten im BVerfSchG	478
III. Besondere Anforderungen für die Datenerhebung aus IT-Systemen	481
IV. Eingriffe in das Telekommunikationsgeheimnis nach Art. 10 GG	483
1. Schutzbereich des Telekommunikationsgeheimnisses	483
2. Überwachungsmaßnahmen nach dem G10	484
V. Übermittlung nachrichtendienstlicher Erkenntnisse an Polizei- und Strafverfolgungsbehörden	485
1. Übermittlungspflicht bei Staatsschutzdelikten (§ 20 Abs. 1 BVerfSchG)	485
2. Fakultative Übermittlungsmöglichkeit bei Allgemeinkriminalität und für sonstige erhebliche Zwecke der öffentlichen Sicherheit (§ 19 Abs. 1 BVerfSchG)	486
3. Übermittlungsverbote (§ 23 BVerfSchG)	488
VI. Übermittlung relevanter Informationen an die Nachrichtendienste	489
C. Schnellübersicht	489

## Kapitel 15. IT-Sicherheitsforschung

A. Datenschutzrechtliche Anforderungen	493
I. Datenverarbeitung für wissenschaftliche Forschungszwecke	493
II. Personenbezogene Daten	493
1. Verarbeitung von technischen Daten durch IT-Sicherheitsforscher	493
2. Beispiel: Personenbezug von IP-Adressen	493
3. Bedeutung für die Praxis	494
III. Zulässigkeit der Datenerhebung	495
1. Datenerhebung auf Grund berechtigter Interessen (Art. 6 Abs. 1 S. 1 lit. f DS-GVO)	495
2. Datenerhebung auf Grund einer Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DS-GVO)	496
3. Zweitverwertung von Daten für Forschungszwecke (Art. 5 Abs. 1 lit. b DS-GVO)	496
4. Datenerhebung auf Grund gesetzlicher Spezialvorschriften	497
IV. Geeignete Garantien nach Art. 89 DS-GVO	497
1. Die dreistufige Prüfung nach Art. 89 Abs. 1 DS-GVO	498
2. Maßnahmen zur Datenminimierung in der Praxis	498
V. Privilegierung der Datenverarbeitung für Forschungszwecke	499
VI. Fazit	500
B. Zivilrechtliche Haftung für Schäden	500
I. Risiken der Forschung	500
II. Fachliche Prüfung der Risiken vor Beginn des Forschungsvorhabens	501
1. Konflikt zwischen Eigentums- und Wissenschaftsfreiheit	501
2. Prüfung von Sicherheitsvorschriften und anerkannten Standards	501
3. Fachliche Risikobewertung	501
4. Haftungsrisiken und Risikoversorge	502
a) Eintritt unerwarteter Schäden	502
b) Risikoversorge	503
III. Veröffentlichung von Schwachstellen	503
1. Recht zur Veröffentlichung wissenschaftlicher Ergebnisse	503
2. Datenschutzrechtliche Grenzen	504
3. Sicherheitsvorschriften und anerkannte Standards	504
4. Fachliche Risikobewertung	504
IV. Fazit	506
C. Strafrechtliche Grenzen der IT-Sicherheitsforschung	506
I. Im IT-Forschungszusammenhang relevante Strafvorschriften	506
1. § 202a StGB (Ausspähen von Daten)	506
2. § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten)	507
3. § 303a StGB (Datenveränderung)	507
4. § 303b StGB (Computersabotage)	508
II. Methoden der IT-Sicherheitsforschung	508
1. „Scanning“	508
2. „IP-Spoofing“	509
3. „Hacking“	509
4. Honey pots	510
III. Vertrieb oder Weitergabe von IT-Sicherheitssoftware an Dritte	511
IV. Informationen über IT-Sicherheitslücken	511
V. Fazit	512
D. Schnellübersicht	512

**Kapitel 16. Internationaler Rahmen**

A. Europäisches Cyber-Sicherheitsrecht	516
I. EU NIS-Richtlinie	517
II. Datenschutz-Grundverordnung	519
III. EU Cybersecurity-Act (Rechtsakt zur Cybersicherheit)	519
IV. Verordnung zur Errichtung des Europäischen Kompetenzzentrums für Cyber-Sicherheit in Industrie, Technologie und Forschung	523
B. US-amerikanisches Cyber-Sicherheitsrecht	523
I. Föderale Ebene	523
1. Sektorspezifische Cyber-Security-Gesetze	523
2. Rolle der Federal Trade Commission (FTC)	524
3. Sonstige Einrichtungen und Regulierungsbestrebungen	525
4. Gesetzesinitiativen	526
II. US-Bundesstaaten	526
C. Chinesisches Cyber-Sicherheitsrecht	527
D. Russisches Cyber-Sicherheitsrecht	531
I. Cyber-Sicherheitsstrategie der Russischen Föderation	531
II. Neues russisches Cyber-Sicherheitsgesetz	532
E. Schnellübersicht	534

**Kapitel 17. Völkerrechtliche Aspekte, Cyberwarfare**

A. Völkerrechtlich relevante IT-Sicherheitsvorfälle	537
I. DDoS-Attacken, Defacement, Stuxnet	537
II. Völkerrechtliche Relevanz	538
III. Begriff der Cyber-Operation	539
IV. Cyber-Operationen mit hoher Intensität	540
1. Art. 39 UN-Charta, Aggression	540
2. Art. 2 Nr. 4 UN-Charta: Gewaltverbot	542
a) Waffenbegriff der UN-Charta	542
b) Effekt-Äquivalenz und Kriterienkatalog nach Tallinn Manual	543
3. Art. 51 UN-Charta: Selbstverteidigungsrecht	543
a) Erheblichkeitsschwelle	544
b) Identifikation des Angreifers	544
c) Verhältnismäßigkeit	545
d) Präventivmaßnahmen	545
e) DDoS-Attacken und gezielter Einsatz von Schadprogrammen als bewaffneter Angriff	545
V. Niederschwellige Cyber-Operationen	546
1. Interventionsverbot	546
2. Propaganda und Spionage	546
VI. Cyber-Operationen als Gegenmaßnahme	548
1. Countermeasures	548
2. Self-contained Regime	548
VII. Zurechnungsfragen	548
1. Attribution	548
2. Cybersecurity Due Diligence	549
VIII. Cyber-Operationen gegen Nichtverantwortliche (Notstand)	549
IX. Entwicklung der Staaten-, Resolutions- und sonstigen Praxis	550

# Inhaltsverzeichnis

B. Die Bundeswehr im Cyber- und Informationsraum	553
I. Struktur- und Kompetenzentwicklung	553
1. Das Kommando Cyber- und Informationsraum (KdoCIR)	553
2. Agentur für Innovation in der Cybersicherheit (Cyberagentur)	553
II. Verfassungsrechtliche Determinanten	554
1. Art. 26 GG	554
a) Eignung und Absicht der Friedensstörung	554
b) Art. 26 und offensives Wirken im Cyberraum	554
2. Art. 87a GG	555
a) „Verteidigung“ und „Einsatz“ im Sinne des Art. 87a GG	555
b) Bewertung einzelner Szenarien	556
C. Schnellübersicht	556
Glossar	559
Sachverzeichnis	583