

Inhaltsübersicht

Vorwort zur 2. Auflage	V
Inhaltsverzeichnis	XIII
Bearbeiterverzeichnis	XLIII
Abkürzungsverzeichnis	XLVII

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
C. Rechtliche Grundlagen der Cyber-Sicherheit in Deutschland und in der EU	13
D. Zentrale Themen im Cyber-Sicherheitsrecht	20
E. Schnellübersicht	26

Kapitel 2. Verfassungsrechtliche Grundlagen

A. Allgemeine verfassungsrechtliche Grundlagen	30
B. Die Kompetenzverteilung nach dem Grundgesetz	32
C. Grundrechte und Verfassungsprinzipien	37
D. Ausblick: Verfassungsrechtlicher Anpassungsbedarf?	45
E. Schnellübersicht	47

Kapitel 3. Technische Grundlagen der Informationssicherheit

A. Grundlagen der Informationssicherheit	52
B. Kryptographie	55
C. Kommunikationsnetze	78
D. Angriffe, Bedrohungen und Gegenmaßnahmen	90
E. Anomalie- und Angriffserkennung (IDS/IPS, SIEM, Honeypots)	101
F. Informationssicherheit und Künstliche Intelligenz (KI)	105
G. Internet of Things (IoT)	110
H. Schnellübersicht	114

Kapitel 4. Stand der Technik

A. Stand der Technik als unbestimmter Rechtsbegriff	118
B. „Stand der Technik“ im Bereich des Cyber-Sicherheitsrechts	122
C. Schnellübersicht	129

Kapitel 5. Normen, technische Standards und Zertifizierung

A. Geschichte der Normen	135
B. Grundsätze der Normungsarbeit	138
C. Zertifizierung, Konformitätsbewertung, Akkreditierung	146
D. Unterschiede zwischen den Sicherheitsanforderungen bei IT und OT	157
E. ISO/IEC 27000 et al.	159
F. ISO 27001 auf der Basis von IT-Grundschutz	165
G. Branchenspezifische Sicherheitsstandards (B3S)	171
H. Energiesektor	182
I. IEC 62443 – IT-Sicherheit für industrielle Automatisierungssysteme	188
J. Bahnsektor	203
K. Medizinbereich	207

Inhaltsübersicht

L. Automobilbereich 211

M. Consumer-Bereich – ETSI EN 303 645: Cyber Security for Consumer Internet
of Things 215

N. Common Criteria (ISO/IEC 15408) 217

O. Cybersecurity in der Cloud 219

P. eIDAS 221

Q. Datenschutz-Zertifizierung 223

R. Schnellübersicht 224

Kapitel 6. Branchenübergreifende Vorgaben

A. Einführung 227

B. Typische betriebliche Schadensrisiken und deren Ursachen 228

C. Branchenübergreifende Rechtsgrundlagen der IT-Sicherheit 234

D. Branchenübergreifende Sonderkonstellationen im IT-Sicherheitsrecht 250

E. Schnellübersicht 267

Kapitel 7. Datenschutz

A. Datenschutz und Informationssicherheit im Wechselwirkungsverhältnis 270

B. Datenschutzrechtliche Anforderungen an die Datensicherheit 271

C. Datenschutzrechtliche Beschränkungen für Maßnahmen der
Informationssicherheit 291

D. Schnellübersicht 303

Kapitel 8. Corporate Governance und Compliance

A. Begrifflichkeit: Governance/Compliance und IT-Governance/IT-Compliance 307

B. Grundlagen der IT-Governance 308

C. Grundlagen der IT-Compliance 311

D. IT-Compliance und IT-Sicherheit als Aufgaben der Unternehmensleitung 318

E. Das Risikomanagement im Unternehmen 323

F. Ausgewählte Richtlinien zur IT-Sicherheit im Unternehmen 326

G. Das Compliance-Risiko der Übererfüllung sicherheitsbezogener Pflichten 329

H. Schnellübersicht 332

Kapitel 9. IT-Vertragsrecht

A. Vertragstypologisierung von IT-Verträgen 336

B. Typische IT-Vertragstypen 338

C. Schnellübersicht 361

Kapitel 10. Ziviles Haftungsrecht

A. Rechtsgrundlagen zivilrechtlicher Haftung 366

B. Begrenzung der Haftung 385

C. Fallgestaltungen 391

D. Schnellübersicht 405

Kapitel 11. Urheber- und Lauterkeitsrecht, Know-How-Schutz

A. Urheberrecht und verwandte Schutzrechte 408

B. Lauterkeitsrecht 430

C. Know-How Schutz 434

D. Schnellübersicht 438

Kapitel 12. Arbeitsrecht und IT-Sicherheit

A. Das traditionelle Arbeitsrecht als Ausgangspunkt	443
B. Überlagerung durch Sicherheitsinteressen?	445
C. Arbeitsvertragliche Pflichten zur Wahrung der IT-Sicherheit	452
D. Sicherheitsüberprüfung	461
E. Grundsätze der IT-Sicherheit, insbesondere in Parallele zur Datensicherung	464
F. Der Informationssicherheitsbeauftragte (ISB)	469
G. Schnellübersicht	476

Kapitel 13. Prozessuale Durchsetzung

A. Hauptsacheverfahren vor staatlichen Gerichten	480
B. Einstweiliges Verfügungsverfahren	490
C. Selbständiges Beweisverfahren	490
D. Außergerichtliche Streitbeilegung	491
E. Schnellübersicht	498

Kapitel 14. Kritische Infrastrukturen

A. Einleitung	502
B. Übersicht über die Regelungen für Kritische Infrastrukturen	507
C. Kritische Infrastrukturen iSd BSIG	509
D. Verpflichtungen für Betreiber Kritischer Infrastrukturen	524
E. Besondere Anforderungen an Anbieter digitaler Dienste	559
F. Verpflichtungen für Unternehmen im besonderen öffentlichen Interesse	567
G. Überschneidungen mit sektorübergreifenden IT-Sicherheits- und Meldepflichten nach anderen Gesetzen	572
H. Folgen bei Pflichtverletzungen	572
I. Schnellübersicht	578

Kapitel 15. Verwaltung

Kapitel 15.1. Cybersicherheitsarchitektur des Bundes

A. Strategische Ebene	580
B. Operative Ebene	585

Kapitel 15.2. Kompetenzen und Arbeit des BSI

A. Schutz der Bundesverwaltung	602
B. Das BSI als Aufsichtsbehörde	609
C. Vorfallsbewältigung	609
D. Schutz der Anwender und Verbraucher	614

Kapitel 15.3. IT-Sicherheitsrecht der (Bundes)Länder

A. Kompetenzgefüge der IT-Sicherheit in Bund und Ländern	621
B. Spezifische landesgesetzliche Regelungen	627

Kapitel 15.4. Sichere elektronische Identitäten und sichere Identifizierung im E-Government

A. Sichere elektronische Identitäten	633
B. Rechtsrahmen sicherer elektronischer Identitäten im Verwaltungskontext	636
C. Sichere Identifizierung im E-Government	648
D. Schnellübersicht	656

Kapitel 16. Gesundheit und Soziales	
A. Einführung	663
B. Rechtliche Grundlagen	666
C. Telematikinfrastruktur und deren Anwendungen	678
D. Weitere sektorenspezifische Anforderungen und die Digitalisierung im Gesundheitswesen	734
E. Schnellübersicht	760
Kapitel 17. Gefahrenabwehr und Sanktionierung	
A. Die Gewährleistung von Cyber-Sicherheit als Teil der öffentlichen Sicherheit ...	765
B. Die polizeiliche Abwehr konkreter Gefahren für die Cyber-Sicherheit	767
C. Cyber-Sicherheit durch Strafrecht	773
D. Schnellübersicht	795
Kapitel 18. Nachrichtendienstrecht	
A. Der Auftrag der Nachrichtendienste	800
B. Die Befugnisse der Nachrichtendienste	834
C. Schnellübersicht	848
Kapitel 19. IT-Sicherheitsforschung	
A. Datenschutzrechtliche Anforderungen	851
B. Zivilrechtliche Haftung für Schäden	859
C. Strafrechtliche Grenzen der IT-Sicherheitsforschung	865
D. Schnellübersicht	872
Kapitel 20. Neue Technologien und Verbraucherschutz	
Kapitel 20.1 Vertrauensdienste im privaten Sektor	
A. Vertrauensdienste für sichere Transaktionen im Binnenmarkt	874
Kapitel 20.2 Blockchain, Smart Contracts und Künstliche Intelligenz	
A. Grundlagen der Regulierung neuer Technologien	889
B. Künstliche Intelligenz – KI-Systeme	892
C. Blockchain und Smart Contracts	901
Kapitel 20.3 Digitaler Verbraucherschutz durch Security Updates und IT-Kennzeichen	
A. Security Updates nach der Digitale-Inhalte-Richtlinie (DI-RL) und der Warenkauf-Richtlinie (WK-RL)	915
B. Verbraucherkennzeichen für IT-Sicherheit	932
Kapitel 20.4 Schutz der Meinungs- und Willensbildung vor technologiegestützten Interventionen	
A. Der Schutz demokratischer Öffentlichkeit als IT-Sicherheitsproblem	941
B. Beeinträchtigung der demokratischen Willens- und Meinungsbildung – Akteure und Erscheinungsformen	942
C. Rechtliche Vorgaben, Regulierungsebenen und -instrumente	947

Kapitel 21. Internationaler Rahmen

Kapitel 21.1 Rechtsrahmen in der Europäischen Union

A. EU NIS-Richtlinie	2
B. EU Datenschutz-Grundverordnung	4
C. EU Cybersecurity Act (Rechtsakt zur Cybersicherheit)	5
D. Verordnung zur Errichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung	9

Kapitel 21.2 US-amerikanische Regulierung der IT-Sicherheit

A. Bundesebene	966
B. US-Bundesstaaten	977

Kapitel 21.3 Japanisches Cyber-Sicherheitsrecht

A. Cybersicherheitsgrundgesetz	978
B. Gesetz zum Schutz personenbezogener Daten in Japan	981
C. Weitere wirtschafts- und strafrechtliche Vorschriften	984

Kapitel 21.4 Cybersecurity-Regulierung in Israel

Kapitel 21.5 Korea's Cybersecurity Regulations and Enforcement related to Security Incidents

A. Overview of Korea's Cybersecurity Regulatory Regime	992
B. Protection of ICN: Cybersecurity Provisions under the Network Act	993
C. Protection of personal information: Cybersecurity Provisions under the PIPA ...	995
D. Cybersecurity obligations under other laws	998

Kapitel 21.6 Cybersecurity Regulation in China

A. Introduction	1001
B. Security standards	1002
C. Cross-border data transfer	1003
D. Security reviews for purchases of equipment and services by CIIOs	1004
E. Data Security Law	1005
F. Important data	1006
G. Mandatory breach notifications	1007

Kapitel 21.7 Cybersecurity in Russia

A. General understanding	1008
B. General overview of legal requirements	1010
C. Liability	1014
D. Trends	1015

Kapitel 21.8 Cybersecurity Law and Policy in India

A. Introduction	1016
B. The Information Technology Act, 2000	1016
C. Sectoral Requirements	1021
D. Conclusion	1024

Kapitel 22. Völkerrechtliche Aspekte, Cyberwarfare

A. Völkerrechtlich relevante IT-Sicherheitsvorfälle	1027
B. Die Bundeswehr im Cyber- und Informationsraum	1045
C. Schnellübersicht	1048

Kapitel 23. Anwendungsszenarien

A. Einleitung 1052

B. Typische Angriffe auf IT-Systeme 1052

C. Vorbereitung auf IT-Notfälle 1071

D. Systematische Ansätze zur Steigerung der IT-Sicherheit 1074

E. Schnellübersicht 1083

Glossar 1085

Anhang – Technische Anlage KBV u. BÄK 1113

Sachverzeichnis 1125

Inhaltsverzeichnis

Vorwort zur 2. Auflage	V
Bearbeiterverzeichnis	XLIII
Abkürzungsverzeichnis	XLVII

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	6
II. Europäische Cyber-Sicherheitsstrategien	11
C. Rechtliche Grundlagen der Cyber-Sicherheit in Deutschland und in der EU ...	13
I. Rahmenvorschriften und Auslegungsmethoden	13
II. Bereichsspezifische gesetzliche Regelungen und Normenhierarchie	16
1. Rechtsnatur	17
2. Gesetzgebungskompetenzen	18
3. Normenhierarchie	19
4. Kollisionsregeln	19
D. Zentrale Themen im Cyber-Sicherheitsrecht	20
E. Schnellübersicht	26

Kapitel 2. Verfassungsrechtliche Grundlagen

A. Allgemeine verfassungsrechtliche Grundlagen	30
B. Die Kompetenzverteilung nach dem Grundgesetz	32
I. Gesetzgebungskompetenz	32
II. Verwaltungskompetenz	34
C. Grundrechte und Verfassungsprinzipien	37
I. Relevante Verfassungsprinzipien: Rechtsstaatsprinzip und Demokratieprinzip	37
II. Relevante Grundrechte	39
1. Recht auf informationelle Selbstbestimmung	41
2. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	42
3. Weitere Grundrechte	43
D. Ausblick: Verfassungsrechtlicher Anpassungsbedarf?	45
E. Schnellübersicht	47

Kapitel 3. Technische Grundlagen der Informationssicherheit

A. Grundlagen der Informationssicherheit	52
I. Information und Kommunikation	52
II. Schutzziele	52
1. Vertraulichkeit	53
2. Integrität	53
3. Verfügbarkeit	53

4. Datenschutz	53
5. Authentizität	54
6. Zurechenbarkeit/Nicht-Abstreitbarkeit	54
III. Authentisierung, Autorisierung, Audit	54
IV. Berechtigungen und Rollen	54
B. Kryptographie	55
I. Grundlagen der Kryptographie	56
1. Grundlegende Begrifflichkeiten	57
2. Kryptoanalyse	57
II. Symmetrische Verschlüsselung	57
1. Strom- und Blockchiffren	58
2. Betriebsmodi von Blockchiffren	59
3. Gängige Verfahren, Schlüssellängen	59
III. Asymmetrische Verschlüsselung	60
1. Gängige Verfahren, Schlüssellängen	62
2. Eigenschaften asymmetrischer Kryptographie	64
IV. Kryptographische Hashfunktionen	65
1. Typische kryptographische Hashfunktionen	67
2. Message Authentication Codes	67
V. Digitale Signaturen	68
VI. Zertifikate und Public Key-Infrastruktur	69
VII. Beispiele für Kryptosysteme aus der Praxis	71
1. Transportverschlüsselung im WWW	71
2. E-Mail-Sicherheit	74
VIII. Zusammenfassung	77
C. Kommunikationsnetze	78
I. Grundlagen der Kommunikationsnetze	78
1. Paketorientierte Kommunikation	78
2. Internet Protocol (IP)	80
3. Die Transport-Protokolle TCP und UDP	82
4. Kommunikation in Netzen (OSI Referenz-Modell)	83
5. Kommunikation in lokalen und in globalen Netzen	84
6. Netzdienste (ARP, DNS, DHCP, ICMP, NAT)	85
a) Domain Name System (DNS)	85
b) Address Resolution Protocol (ARP)	86
c) Dynamic Host Configuration Protocol (DHCP)	86
d) Internet Control Message Protocol (ICMP)	86
e) Network Address Translation (NAT)	87
II. Netzkonzepte	87
1. Kabelgebundene Netze	88
2. Drahtlose Netze	88
a) Wireless Local Area Networks (WLAN)	88
b) Mobilfunknetze (GSM, GPRS, 3G, 4G, 5G)	89
III. Zusammenfassung	89
D. Angriffe, Bedrohungen und Gegenmaßnahmen	90
I. Sicherheitslücken als wichtige Ursache für Schadsoftware	90
II. Malware: Viren, Würmer, Trojaner, Spyware und Ransomware	94
III. Social Engineering	96
IV. (Distributed) Denial-of-Service-Angriffe	97
V. Bedrohungen gegen (mobile) Endgeräte und Apps	98
VI. Bedrohungen für komplexe IT-gestützte Anwendungen	99

VII. Sicherheitsmaßnahmen	100
VIII. Zusammenfassung	101
E. Anomalie- und Angriffserkennung (IDS/IPS, SIEM, Honeypots)	101
I. Grundbegriffe Anomalie- und Angriffserkennung und -Verteidigung (IDS/IPS)	101
II. Detektionsmechanismen von IDS und IPS	102
III. Arbeitsweise der Intrusion Detection Systeme und Intrusion Prevention Systeme	103
IV. Honeypots	104
V. Security Information and Event Management (SIEM)	104
VI. Zusammenfassung	105
F. Informationssicherheit und Künstliche Intelligenz (KI)	105
I. Grundbegriffe der Künstlichen Intelligenz	106
II. Einsatz von KI und ML im Bereich der Informationssicherheit	106
1. Anomalieerkennung	106
2. Intelligentes SIEM	107
3. Maschinelles Lernen für das Static Application Security Testing	108
III. Angreifbarkeit von ML-Systemen	109
G. Internet of Things (IoT)	110
I. Grundbegriff des Internet of Things	110
II. Beispielarchitektur für ein IoT-System	110
III. Informationssicherheit von IoT-Systemen	112
H. Schnellübersicht	114

Kapitel 4. Stand der Technik

A. Stand der Technik als unbestimmter Rechtsbegriff	118
I. Abgrenzung unterschiedlicher Technologieniveaus	118
1. Allgemein anerkannte Regeln der Technik	119
2. Stand der Technik	120
3. Stand von Wissenschaft und Technik	120
II. Verwendung des „Standes der Technik“	121
B. „Stand der Technik“ im Bereich des Cyber-Sicherheitsrechts	122
I. Gesetzliche Vorgaben	123
II. Branchenspezifische Sicherheitsstandards (B3S)	127
C. Schnellübersicht	129

Kapitel 5. Normen, technische Standards und Zertifizierung

A. Geschichte der Normen	135
B. Grundsätze der Normungsarbeit	138
I. Internationale Normung	139
1. International Standard (IS)	140
2. Technische Spezifikation (TS)	141
3. Technischer Report (TR)	141
4. Publicly Available Specification (PAS)	142
II. Europäische Normung	142
III. Nationale Normung	143
1. VDE-Anwendungsregel	144
2. DIN SPEC	144

3. Gruppierung von DIN-Normen mit VDE-Klassifikation	144
C. Zertifizierung, Konformitätsbewertung, Akkreditierung	146
I. Akkreditierungsstelle	148
II. Zertifizierungsstellen	150
1. Gegenseitige Anerkennung	150
a) Senior Officials Group Information Systems Security (SOG-IS)	151
b) EU Cybersecurity Certification Framework	152
2. Zertifizierungsstelle für Managementsysteme	152
3. Zertifizierungsstelle für Produkte, Prozesse oder Dienstleistungen	154
III. Prüflabor	155
IV. Inspektionsstelle	156
D. Unterschiede zwischen den Sicherheitsanforderungen bei IT und OT	157
E. ISO/IEC 27000 et al.	159
I. Festlegung des Geltungsbereiches	161
II. Risikoanalyse	162
III. Maßnahmenauswahl mittels ISO/IEC 27002	163
IV. Management der Informationssicherheit	164
V. Regelmäßige Kontrollen	165
VI. Kontinuierliche Verbesserung	165
F. ISO 27001 auf der Basis von IT-Grundschutz	165
I. IT-Strukturanalyse	167
II. Schutzbedarfsfeststellung	168
III. Modellierung	168
IV. IT-Grundschutz-Check	169
V. Risikoanalyse	169
VI. Bausteine	170
G. Branchenspezifische Sicherheitsstandards (B3S)	171
I. Anforderungen an KRITIS-Betreiber	174
II. Erstellung Branchenspezifischer Sicherheitsstandards (B3S)	176
III. Prüfung zum Nachweis der Einhaltung der Anforderungen	178
1. Durchführung der Prüfung	179
2. Beispiele von aktuellen B3S gem. § 8a Abs. 2 BSIG	182
H. Energiesektor	182
I. ISO/IEC 27019 Informationssicherheitsmaßnahmen für die Energieversorgung	183
II. Branchenspezifischer Sicherheitsstandard für Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung (B3S Aggregatoren)	183
III. IEC 62351 Sicherheit in Energiemanagementsystemen und zugehörigem Datenaustausch	184
IV. BDEW Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“	186
V. BDEW „Sichere Fernwartung in der Energie- und Wasserwirtschaft“	187
VI. IT-Sicherheitskatalog der Bundesnetzagentur	187
I. IEC 62443 – IT-Sicherheit für industrielle Automatisierungssysteme	188
I. IEC 62443-1-1: Konzepte und Modelle	191
1. Risikobasierter Ansatz	191
2. Defense-in-Depth	193
3. Zonen-Conduit-Modell	193
4. Secure-by-Design	195

5. Maturity Model – Reifegradmodell von organisatorischen Prozessen und Maßnahmen	195
6. Security-Level-Modell – Einstufung von Schutzmaßnahmen eines IACS	196
II. IEC 62443-2-1: Anforderungen an das Sicherheitsprogramm von Betreibern	197
III. IEC TR 62443-2-3: Patchverwaltung im industriellen Umfeld	197
IV. IEC 62443-2-4: Anforderungen an das Sicherheitsprogramm von Dienstleistern	198
V. IEC TR 62443-3-1: Sicherheitstechnologien für IACS	198
VI. IEC 62443-3-2: Risikobeurteilung und Systementwurf	198
VII. IEC 62443-3-3: Systemanforderungen zur IT-Sicherheit und Security-Level	199
VIII. IEC 62443-4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung	200
IX. IEC 62443-4-2: Anforderungen an IACS-Komponenten	201
X. Konformitätsbewertung und Zertifizierung	202
J. Bahnsektor	203
I. CLC/TS 50701: Cybersecurity Case für Anwendungen im Bahnsektor ...	203
II. VDE V 0831-104: Leitfaden für IT-Sicherheit im Signalfeld	206
K. Medizinbereich	207
I. ISO 27799: Informationssicherheit im Gesundheitswesen	208
II. Branchenspezifischer Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus	209
III. Medizinprodukte	210
L. Automobilbereich	211
I. Trusted Information Security Assessment Exchange (TISAX)	212
II. ISO/SAE 21434: Road vehicles – Cybersecurity engineering	213
III. UNECE WP.29 – UN-Regelung Nr. 155	215
M. Consumer-Bereich – ETSI EN 303 645: Cyber Security for Consumer Internet of Things	215
N. Common Criteria (ISO/IEC 15408)	217
O. Cybersecurity in der Cloud	219
I. ISO/IEC 27017 Anwendungsleitfaden für Cloud-Dienste	220
II. ISO/IEC 27018 Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung	221
P. eIDAS	221
Q. Datenschutz-Zertifizierung	223
R. Schnellübersicht	224

Kapitel 6. Branchenübergreifende Vorgaben

A. Einführung	227
B. Typische betriebliche Schadensrisiken und deren Ursachen	228
I. Risiken von außen	228
II. Risiken von innen	231
1. Die Unternehmensleitung	232
2. Die IT-Systeme	233

3. Die Mitarbeiter	234
C. Branchenübergreifende Rechtsgrundlagen der IT-Sicherheit	234
I. Abgrenzung von branchenübergreifenden und branchenspezifischen rechtlichen Pflichten zur IT-Sicherheit	235
1. Systematik	235
2. Einführung in die bereichsübergreifenden Rechtspflichten	235
3. Kurze Darstellung branchenspezifischer Rechtspflichten	236
a) KRITIS-Betreiber	236
b) Telemedien und Telekommunikationsdienste	236
c) Weitere Sonderregelungen für Einzelbereiche	237
4. Gegenüberstellung	238
II. Gewährleistung der IT-Sicherheit als unternehmerische Sorgfaltspflicht	238
1. Pflicht zur Früherkennung bestandsgefährdender Risiken	239
2. Allgemeine Leitungs- und Sorgfaltspflicht der Unternehmensleitung	240
a) Leitungs- und Sorgfaltspflicht des Vorstands der Aktiengesellschaft	240
b) Leitungs- und Sorgfaltspflicht des GmbH-Geschäftsführers	244
3. Praktische Erwägungen	245
III. Buchführungspflichten als IT-Sicherheitspflichten	245
1. Pflicht zur ordnungsgemäßen Buchführung	246
2. Pflichten bei der Erstellung des Lageberichts	248
3. Die Rolle des Abschlussprüfers	248
4. Checkliste der grundlegenden IT-sicherheitsrechtlichen Pflichten aufgrund branchenübergreifender Rechtsgrundlagen	249
D. Branchenübergreifende Sonderkonstellationen im IT-Sicherheitsrecht	250
I. Cloud Computing	250
1. Technische Rahmenbedingungen	250
2. IT-sicherheitsrechtliche Aspekte	252
3. Datenschutz in der Cloud	252
4. Zertifizierungen als Lösungsansatz	253
II. Industrie 4.0	254
1. Maßnahmen zur Angriffssicherheit	255
2. Schutz von Unternehmensdaten, Knowhow und Geschäftsgeheimnissen	255
3. Schutz personenbezogener Daten	255
4. Haftung in der Smart Factory	256
III. Big Data	256
IV. IT-Outsourcing	258
V. Das Internet der Dinge (IoT)	258
VI. Bring Your Own Device	260
1. IT-Sicherheit	260
2. Datensicherheit und Datenschutz	262
VII. IT-Forensik (rechtssichere Ermittlungen nach IT-Sicherheitsvorfällen)	263
1. Grundlagen der IT-Forensik	263
2. Durchführung einer IT-forensischen Analyse	264
VIII. Versicherungsschutz und Cyberpolizen	265
1. Versicherungsschutz für Eigenschäden	265
2. Versicherungsschutz für Haftpflichtansprüche	266
3. Versicherungsschutz für Datenschutzverfahren	266
4. Versicherungsschutz für Krisenmanagement: Das Incident Response Team	266

E. Schnellübersicht	267
---------------------------	-----

Kapitel 7. Datenschutz

A. Datenschutz und Informationssicherheit im Wechselwirkungsverhältnis	270
B. Datenschutzrechtliche Anforderungen an die Datensicherheit	271
I. Regelungssystematik	272
II. Datensicherheit durch geeignete technische und organisatorische Maßnahmen	276
III. Zur Wahl und Umsetzung der erforderlichen Maßnahmen	277
IV. Heranziehung der Datenschutz-Folgenabschätzung im Rahmen der Risikoabschätzung	283
V. Anforderungen an die Datensicherheit bei Drittlandsübermittlungen	286
VI. Genehmigte Verhaltensregeln oder genehmigtes Zertifizierungsverfahren	288
VII. Datenschutzrechtliche Aufsicht	289
C. Datenschutzrechtliche Beschränkungen für Maßnahmen der Informationssicherheit	291
I. IT-Sicherheitsmaßnahmen als Eingriff in die Privatsphäre	291
II. Bestimmung des Personenbezugs	292
III. Anforderungen an die Datenverarbeitung	294
1. Allgemeine datenschutzrechtliche Vorgaben	294
2. Datenschutzrechtliche Vorgaben im Bereich der Telekommunikation	297
3. Mitteilungen an das BSI	299
4. Datenverarbeitung durch das BSI zu Sicherheitszwecken	300
D. Schnellübersicht	303

Kapitel 8. Corporate Governance und Compliance

A. Begrifflichkeit: Governance/Compliance und IT-Governance/IT-Compliance	307
B. Grundlagen der IT-Governance	308
I. IT-Governance nach dem ITGI	308
II. Übersicht der aktuellen Standards und Frameworks im Bereich der IT-Governance	309
III. Die Einbindung der IT-Compliance in die Mechanismen der Governance	310
C. Grundlagen der IT-Compliance	311
I. Relevante Compliance-Themen für die IT-Sicherheit	311
II. Regelungen und Maßstäbe zur Umsetzung der IT-Compliance und IT-Sicherheit im Unternehmen	311
III. Die Implementierung der IT-Sicherheit als Element des Schutzes personenbezogener Daten	315
D. IT-Compliance und IT-Sicherheit als Aufgaben der Unternehmensleitung	318
I. Die Geschäftsführer- bzw. Vorstandshaftung	318
II. Die Informations- und Mitbestimmungsrechte des Betriebsrats bei der Einführung oder Änderung von IT-Systemen	320
III. Der IT-Sicherheitsbeauftragte	321

E. Das Risikomanagement im Unternehmen 323

 I. Typische interne und externe Betriebssicherheitsrisiken 323

 II. Die Einrichtung eines Risikomanagementsystems in der IT 324

 III. Erwägungen zum Abschluss einer Versicherung gegen Cyberrisiken 325

F. Ausgewählte Richtlinien zur IT-Sicherheit im Unternehmen 326

 I. Die IT-Richtlinie als Handlungsstandard 326

 II. Auswahl zentraler Elemente einer IT-Richtlinie 327

 III. Regelmäßige Kontrollen und Sanktionen 328

G. Das Compliance-Risiko der Übererfüllung sicherheitsbezogener Pflichten 329

 I. Rechte Dritter als Beschränkung der IT-Sicherheit 329

 II. Problembereich: Die Überwachung von E-Mail- und Internetnutzung zu Compliance-Zwecken 329

 III. Die betriebsverfassungsrechtliche Zulässigkeit von Maßnahmen der IT-Sicherheit 331

H. Schnellübersicht 332

Kapitel 9. IT-Vertragsrecht

A. Vertragstypologisierung von IT-Verträgen 336

B. Typische IT-Vertragstypen 338

 I. Softwarebeschaffung 339

 1. Entwicklung und dauerhafte Überlassung von Individualsoftware 341

 a) Sonderproblem des § 650 BGB 341

 b) Softwareentwicklung mit Hilfe agiler Projektmethoden 344

 c) Abnahme 345

 2. Dauerhafte Überlassung von Standardsoftware 346

 3. Implementierung und Anpassung von Standardsoftware 347

 4. Befristete Überlassung von Individualsoftware 349

 5. Befristete Überlassung von Standardsoftware 350

 a) Application Service Providing (ASP), Software as a Service (SaaS), Cloud Computing 350

 b) Leasing 351

 c) Leihe 352

 II. Hardwarebeschaffung 352

 III. Pflege und Wartung 352

 IV. Beratung 358

 V. Schulung 358

 VI. Penetrationtest-Vertrag 359

 VII. Sonstige Vertragstypen 361

C. Schnellübersicht 361

Kapitel 10. Ziviles Haftungsrecht

A. Rechtsgrundlagen zivilrechtlicher Haftung 366

 I. Vertragliche Haftung 366

 II. Vertrag 367

 III. Vertragsähnliche Beziehung 368

 IV. Gesetzliche Schuldverhältnisse 368

 1. Geschäftsführung ohne Auftrag 368

 2. Eigentümer-Besitzer-Verhältnis 369

 3. Ungerechtfertigte Bereicherung 370

4. Deliktsrecht	370
5. Typen gesetzlicher Schuldverhältnisse	373
6. Persönliche Haftung von Organen	373
7. Haftung auf Schadensersatz wegen Pflichtverletzung	374
8. Verzugsseintritt	374
9. Verzugschaden	376
10. Rücktrittsrecht im Fall des Verzuges	376
11. Gewährleistungsansprüche	376
V. Haftung für Dritte	378
1. Erfüllungsgehilfen	378
2. Haftung für Mittäter und Beteiligte	378
3. Marktanteilshaftung	378
4. Verrichtungsgehilfen	378
5. Gesamtschuld	379
VI. Weitere Haftungsgrundlagen	379
1. Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)	379
2. Grundsätze ordnungsgemäßer Buchführung	381
3. Datenschutzrecht	382
4. Kritische Infrastrukturen	383
5. Produkthaftung	383
6. Fehlerbegriff	384
7. Störerhaftung des BGH	385
8. eIDAS-Verordnung	385
B. Begrenzung der Haftung	385
I. Haftungsbegrenzung	385
II. Vertragliche Haftungsbegrenzung	385
III. Haftungsbegrenzung durch Rechtsform	387
IV. Haftungsbegrenzung durch Versicherung	387
1. Haftpflichtversicherung	387
2. D&O-Versicherung	389
3. Cyberversicherung	390
C. Fallgestaltungen	391
I. Lieferung von fehlerhafter Software/Updates	392
1. Bedeutung von Programmfehlern	392
2. Arten von Fehlern in Software und Updates	392
3. Beteiligte	392
4. Anbieter	393
a) Hersteller	393
b) Händler	393
c) OEM, VAR, etc	393
d) Systemhäuser	394
e) Dienstleister	394
5. Haftung	395
a) Gewährleistung	395
b) Vertragliche Haftung	397
c) Deliktische Haftung	399
6. Software-Nutzer	400
a) Mitarbeiter	400
b) Datenschutzbeauftragte	400
c) Compliance Officer	401
7. Sonstige	401

II. Cyberangriffe	401
III. Infizierte Webseiten	402
IV. Verlust von Daten, Datenträgern oder mobilen Geräten	403
V. Infizierte E-Mails und Chats	405
D. Schnellübersicht	405
 Kapitel 11. Urheber- und Lauterkeitsrecht, Know-How-Schutz	
A. Urheberrecht und verwandte Schutzrechte	408
I. Vorbemerkung	409
II. Allgemeines Urheberrecht	409
1. Schutzgegenstand	409
2. Verwertungsrechte	411
a) Vervielfältigungsrecht	411
b) Recht der öffentlichen Wiedergabe	411
3. Urheberpersönlichkeitsrecht	417
4. Schranken	417
III. Softwareurheberrecht	418
1. Allgemeines	418
2. Schutzgegenstand	419
3. Verwertungsrechte und Schranken	419
IV. Datenbankrecht	421
1. Allgemeines	421
2. Schutzgegenstand	422
3. Rechte des Datenbankherstellers	423
V. Rechtsverletzungen	423
1. Ansprüche	423
2. Aktivlegitimation	424
3. Passivlegitimation	424
a) Täterschaft und Teilnahme	424
b) Störerhaftung	425
4. Haftungsprivilegierungen	426
VI. Technische Schutzmaßnahmen	429
B. Lauterkeitsrecht	430
I. Anwendungsbereich	430
II. Beispiele unlauteren Verhaltens	431
1. Screen Scraping	431
2. Bots	431
3. Domain-Grabbing	432
4. „Metatagging“ und „Index-Spamming“	432
5. Sniper-Software	433
6. Denial-of-Service („DoS Attacken“)	433
7. Haftung für Hyperlinks	433
C. Know-How Schutz	434
I. Frühere Rechtslage	434
II. Änderungen durch Know-How-Richtlinie und GeschGehG	435
1. Anwendungsbereich	435
2. Angemessene Geheimhaltungsmaßnahmen	435
3. Rechtmäßiger und rechtswidriger Erwerb	437
4. Ansprüche	438
D. Schnellübersicht	438

Kapitel 12. Arbeitsrecht und IT-Sicherheit

A. Das traditionelle Arbeitsrecht als Ausgangspunkt	443
I. Historische Entwicklung	443
II. Die zwei Bestandteile des Arbeitsrechts	443
III. Errungenschaften und Lästigkeiten	444
IV. Prekär Beschäftigte	445
B. Überlagerung durch Sicherheitsinteressen?	445
I. Das Beispiel der kerntechnischen Anlagen	446
1. Konkrete Veränderungen im Arbeitsrecht	446
2. Die Auseinandersetzungen um die Mitbestimmungsrechte des Betriebsrats	447
3. Mögliche Alternativen?	448
II. Andere gefährliche Technologien	449
1. Luftverkehr	449
2. Chemische Industrie	450
3. Gefährliche Dienstleistungen, insbesondere im Bankensektor	450
III. Was wird einer Sonderregelung unterworfen?	451
C. Arbeitsvertragliche Pflichten zur Wahrung der IT-Sicherheit	452
I. Allgemein anerkannte Nebenpflichten aus dem Arbeitsverhältnis	452
1. Verhinderung von Angriffen	452
2. Störungen, die von Arbeitskollegen ausgehen	454
3. Mitwirkung an der Schadensbeseitigung	455
II. Erweiterung und Konkretisierung von Pflichten, insbesondere im Zusammenhang mit Compliance?	455
III. Qualifizierung wegen neuer Anforderungen	456
1. Anspruch des Arbeitnehmers auf Weiterqualifizierung?	456
a) § 81 BetrVG?	456
b) Nebenpflicht des Arbeitgebers zur Schaffung der Voraussetzungen für die Arbeit	457
c) Tragweite der Arbeitgeberpflicht	458
d) Einbeziehung der Arbeitszeit	458
2. Pflicht des Arbeitnehmers zur Weiterqualifizierung	458
3. Mitbestimmungsrechte des Betriebsrats bei Weiterbildungsmaßnahmen	459
D. Sicherheitsüberprüfung	461
I. Anwendungsbereich	461
II. Durchführung der Sicherheitsüberprüfung	462
E. Grundsätze der IT-Sicherheit, insbesondere in Parallele zur Datensicherung	464
I. Arbeitsrechtliche Probleme der Datensicherung	464
II. Übertragung auf die IT-Sicherheit?	465
III. Beispiele für Regelungen zur IT-Sicherheit nach ISO 27002	466
1. Schutz der Privatsphäre	466
2. Kein abschließender Katalog	466
3. Sicherheitsüberprüfung bei Einstellungen?	466
4. Verantwortlichkeit des einzelnen Arbeitnehmers	467
5. Maßregelungsprozess	467
6. Regelung des Zugangs zu Informationen	468
7. Ereignisprotokollierung	468
8. Erfassung von Auffälligkeiten	468

IV. Regelungen zur IT-Sicherheit nach BSI-Grundsatz und nach den
Richtlinien der Versicherungswirtschaft für die Informationssicherheit
(VdS 3473) 469

F. Der Informationssicherheitsbeauftragte (ISB) 469

 I. Die Beschreibung der Aufgaben des ISB 470

 II. Voraussetzungen für die Bestellung 471

 III. Sachliche und personelle Ressourcen des ISB 474

 IV. Stellung in der Organisation 475

 V. Beteiligung des Betriebsrats? 476

G. Schnellübersicht 476

Kapitel 13. Prozessuale Durchsetzung

A. Hauptsacheverfahren vor staatlichen Gerichten 480

 I. Formelle Fragen 480

 1. Zuständigkeit 480

 2. Klagearten 481

 II. Sachvortrag 482

 III. Beweis 483

 1. Beweislast 483

 2. Beweisbeschluss 484

 3. Beweis durch Sachverständige 484

 4. Strafanzeige 485

 IV. Streitverkündung 486

 V. Internationale Bezüge 487

 1. Gerichtsstand 487

 2. Discovery 488

 VI. Auswirkungen der DS-GVO 488

B. Einstweiliges Verfügungsverfahren 490

C. Selbständiges Beweisverfahren 490

D. Außergerichtliche Streitbeilegung 491

 I. Verhandlung 492

 II. Schlichtung 493

 III. Schiedsgerichtsbarkeit/Arbitration 493

 IV. Mediation 494

E. Schnellübersicht 498

Kapitel 14. Kritische Infrastrukturen

A. Einleitung 502

 I. Begrifflichkeit 502

 II. Regelungsgegenstände 505

B. Übersicht über die Regelungen für Kritische Infrastrukturen 507

C. Kritische Infrastrukturen iSd BSIG 509

 I. Überblick 509

 II. Kritische Dienstleistungen 510

 1. Sektor Energie (§ 2 BSI-KritisV) 510

 a) Stromversorgung (§ 2 Abs. 1 Nr. 1 BSI-KritisV) 510

 b) Gasversorgung (§ 2 Abs. 1 Nr. 2 BSI-KritisV) 511

 c) Kraftstoff- und Heizölversorgung (§ 2 Abs. 1 Nr. 3 BSI-KritisV) 511

d) Fernwärmeversorgung (§ 2 Abs. 1 Nr. 4 BSI-KritisV)	511
2. Sektor Wasser (§ 3 BSI-KritisV)	511
a) Trinkwasserversorgung (§ 3 Abs. 2 BSI-KritisV)	511
b) Abwasserbeseitigung (§ 3 Abs. 3 BSI-KritisV)	511
3. Sektor Ernährung (§ 4 BSI-KritisV)	511
4. Sektor Informationstechnik und Telekommunikation (§ 5 BSI-KritisV)	512
a) Sprach- und Datenübertragung (§ 5 Abs. 2 BSI-KritisV)	512
b) Datenspeicherung und -verarbeitung (§ 5 Abs. 3 BSI-KritisV)	512
5. Sektor Gesundheit (§ 6 BSI-KritisV)	512
a) Stationäre medizinische Versorgung (§ 6 Abs. 1 Nr. 1 BSI-KritisV)	512
b) Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind (§ 6 Abs. 1 Nr. 2 BSI-KritisV)	513
c) Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper (§ 6 Abs. 1 Nr. 3 BSI-KritisV)	513
d) Laboratoriumsdiagnostik (§ 6 Abs. 1 Nr. 4 BSI-KritisV)	513
6. Sektor Finanz- und Versicherungswesen (§ 7 BSI-KritisV)	514
a) Bargeldversorgung (§ 7 Abs. 1 Nr. 1 BSI-KritisV)	514
b) Kartengestützter Zahlungsverkehr (§ 7 Abs. 1 Nr. 2 BSI-KritisV)	514
c) Konventioneller Zahlungsverkehr (§ 7 Abs. 1 Nr. 3 BSI-KritisV)	514
d) Handel, Verrechnung und Abwicklung von Wertpapier- und Derivatgeschäften (§ 7 Abs. 1 Nr. 4 BSI-KritisV)	514
e) Versicherungsdienstleistungen (§ 7 Abs. 1 Nr. 5 BSI-KritisV)	515
7. Sektor Transport und Verkehr (§ 8 BSI-KritisV)	515
8. Siedlungsabfallentsorgung	515
III. Betreiben einer Anlage	515
1. Anlagenbegriff	516
2. Betreiberbegriff (außer für den Finanzsektor)	517
a) Allgemeiner Betreiberbegriff	517
b) Abweichender Betreiberbegriff für Finanzdienstleistungen	518
c) Betreiberidentität	519
IV. Schwellenwerte	520
1. Grundsätze der Schwellenwertberechnung	520
2. Zeitpunkt der Schwellenwertberechnung	521
3. Berechnung der Schwellenwerte bei „gemeinsamen Anlagen“	521
a) Anlagen derselben Art	522
b) Enger betrieblicher (und räumlicher) Zusammenhang	522
4. Berechnung von Schwellenwerten bei Auslandsbezügen	524
V. Zweite Verordnung zur Änderung der BSI-KritisV	524
D. Verpflichtungen für Betreiber Kritischer Infrastrukturen	524
I. Verpflichtungen nach dem BSIG	525
1. Sicherheit in der Informationstechnik Kritischer Infrastrukturen (§ 8a BSIG)	525
a) Angemessene Sicherheitsvorkehrungen nach dem Stand der Technik (§ 8a Abs. 1 BSIG)	525
b) Systeme zur Angriffserkennung (§ 8a Abs. 1a BSIG)	527
c) Branchenspezifische Sicherheitsstandards (B3S) (§ 8a Abs. 2 BSIG) und weitere Konkretisierungen des Stands der Technik	527
d) Regelmäßige Nachweispflichten (§ 8a Abs. 3 BSIG)	529
e) Kontrollrechte des BSI	531

2. Pflicht zur Registrierung und Benennung einer Kontaktstelle (§ 8b Abs. 3 BSIG)	531
3. Meldepflichten bei Störungen (§ 8b Abs. 4 BSIG)	531
a) Voraussetzungen der Meldepflicht nach § 8b Abs. 4 BSIG	532
b) Inhalt der Meldung	535
c) Zeitpunkt der Meldung	535
4. Zusammenarbeit mit dem BSI bei erheblichen Störungen	536
5. Regelung über den Umgang mit im Rahmen der §§ 8a, 8b BSIG erhobenen personenbezogenen Daten	536
II. Einsatz kritischer Komponenten	537
1. Kritische Komponenten iSd BSIG	537
2. Pflichten beim Einsatz Kritischer Komponenten	538
a) Anzeigepflicht	538
b) Einholung einer Garantieerklärung	539
3. Regulierung des Einsatzes kritischer Komponenten	539
a) Untersagungsvorbehalt – ex ante	540
b) Untersagung und Erlass von Anordnungen nach § 9b Abs. 4, 6 und 7 BSIG	541
III. Territoriale Anwendung	542
IV. Spezialgesetzliche IT-Sicherheits- und Meldepflichten für Betreiber bestimmter Kritischer Infrastrukturen	542
1. Grundsatz	542
2. Betreiber öffentlicher Telekommunikationsnetze oder Anbieter öffentlich zugänglicher Telekommunikationsdienste	544
3. Betreiber von Energieanlagen und Energieversorgungsnetzen iSd EnWG	547
4. Die Gesellschaft für Telematik und Betreiber von Diensten der Telematikinfrastruktur	548
5. Genehmigungsinhaber nach § 7 Abs. 1 AtG	549
6. Finanzsektor	549
a) KWG, MaRisk und BAIT	549
b) ZAG	553
c) OTC-Derivate-Verordnung	554
d) WpHG	555
e) Ausblick – Digital Operational Resilience Act (DORA)	555
7. Versicherungssektor	556
V. Übersicht über die IT-Sicherheits-, Melde- und Nachweispflichten sowie Pflichten beim Einsatz Kritischer Komponenten nach den verschiedenen Gesetzen	556
E. Besondere Anforderungen an Anbieter digitaler Dienste	559
I. Digitale Dienste	560
1. Online-Marktplätze (§ 2 Abs. 11 Nr. 1 BSIG)	560
2. Online-Suchmaschinen (§ 2 Abs. 11 Nr. 2 BSIG)	560
3. Cloud-Computing-Dienste (§ 2 Abs. 11 Nr. 3 BSIG)	561
II. Anbieter digitaler Dienste	561
III. Verpflichtungen von Anbietern digitaler Dienste	564
1. Maßnahmen zur Bewältigung von Risiken für die Sicherheit der Netz- und Informationssysteme (§ 8c Abs. 1 und 2 BSIG)	564
2. Meldepflicht bei Störungen (§ 8c Abs. 3 BSIG)	565
3. Schnittmengen mit anderen IT-Sicherheitspflichten	566
a) Zusätzliche Verpflichtung als Telemediendiensteanbieter	566
b) Zusätzliche Verpflichtung als Betreiber Kritische Infrastruktur	566

c) Kritik	567
F. Verpflichtungen für Unternehmen im besonderen öffentlichen Interesse	567
I. Unternehmen im besonderen öffentlichen Interesse	567
1. Unternehmen mit Tätigkeit in den Bereichen der Rüstungsindustrie und Hersteller von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen	568
2. Unternehmen mit besonderer volkswirtschaftlicher Bedeutung	568
3. Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung	568
II. IT-Sicherheitspflichten und Meldepflichten	569
1. Selbsterklärung zur IT-Sicherheit	569
2. Registrierung und Benennung einer Kontaktstelle	570
3. Pflichten bei IT-Sicherheitsstörungen	570
a) Meldepflichten für Unternehmen nach § 2 Abs. 14 S. 1 Nr. 1 u. 2 BSIG	571
b) Meldepflichten für Unternehmen nach § 2 Abs. 14 S. 1 Nr. 3 BSIG	571
G. Überschneidungen mit sektorübergreifenden IT-Sicherheits- und Meldepflichten nach anderen Gesetzen	572
I. DS-GVO	572
II. Kapitalmarktrechtliche Publizitätspflichten	572
H. Folgen bei Pflichtverletzungen	572
I. Bußgelder	573
1. Bußgelder nach § 14 BSIG	573
a) Ordnungswidrigkeiten durch Betreiber Kritischer Infrastrukturen ...	573
b) Ordnungswidrigkeiten durch Anbieter digitaler Dienste	574
c) Ordnungswidrigkeiten durch Unternehmen im besonderen öffentlichen Interesse	574
2. Spezialgesetzliche Bußgeldvorschriften	575
3. Zivilrechtliche Haftung	576
II. Wettbewerbsrechtliche Folgen von IT-Sicherheitsverstößen	576
III. Verlangen der Beseitigung von Sicherheitsmängeln	577
1. Beseitigung von Sicherheitsmängeln nach dem BSIG	577
2. Beseitigung von Sicherheitsmängeln nach Spezialgesetzen	577
I. Schnellübersicht	578

Kapitel 15. Verwaltung

Kapitel 15.1. Cybersicherheitsarchitektur des Bundes

A. Strategische Ebene	580
I. Bundeskanzleramt und Bundesministerien	581
II. Der Nationale Cyber-Sicherheitsrat (NCSR)	582
1. Gründung des NCSR	582
2. Fortentwicklung des NCSR	582
3. Bedarf zur Weiterentwicklung	583
III. Bund-Länder-Zusammenarbeit auf strategischer Ebene	584
B. Operative Ebene	585
I. Gefahrenvorsorge	585
1. Gefahrenvorsorgende Aufgaben des BSI	585
2. Gefahrenvorsorgende Aufgaben des BfV	586

3. Gefahrenvorsorgende Aufgaben des BKA	587
II. Gefährerforschung	587
1. Nachrichtendienstliche Gefährerforschung	587
2. Gefährerforschung durch das BSI	588
III. Gefahrenabwehr	588
1. Die Gefahrenabwehrkompetenz des BKA	589
2. Die Gefahrenabwehrkompetenz der BPol	589
3. Die Gefahrenabwehrkompetenz des BSI	590
4. Angestrebte Kompetenzerweiterungen des Bundes	591
IV. Strafverfolgung	591
1. Strafverfolgungszuständigkeit des BKA	592
2. Strafverfolgungszuständigkeit der BPol	592
3. Unterstützung der Strafverfolgungsbehörden durch das BSI	593
V. Cyberverteidigung	593
VI. Unterstützung und Beratung der Sicherheitsbehörden	594
VII. Behördenübergreifende Kooperation und Koordination	595
VIII. Bund-Länder-Zusammenarbeit auf operativer Ebene	597
1. Das BfV als Zentralstelle	598
2. Das BKA als Zentralstelle	598
3. Das BSI als Zentralstelle	599
IX. Schnellübersicht	599

Kapitel 15.2. Kompetenzen und Arbeit des BSI

A. Schutz der Bundesverwaltung	602
I. Meldestelle der Bundesverwaltung gem. § 4 BSIG	602
II. Mindeststandards für die Bundesverwaltung nach § 8 BSIG und IT-Sicherheitsberatung	603
III. Kontrolle der IT-Sicherheit der Bundesverwaltung nach § 4a BSIG	604
IV. Schadsoftwareerkennung durch das SES gem. § 5 BSIG und Protokollierungsdatenanalyse nach § 5a BSIG	606
V. VS-Zulassungen und Freigaben	607
VI. Umsetzungsplan Bund (UP Bund)	608
B. Das BSI als Aufsichtsbehörde	609
C. Vorfallsbewältigung	609
I. Nationales IT-Lagezentrum und nationales IT-Krisenreaktionszentrum	609
II. CERT-Bund und die Zusammenarbeit der CERTs	610
III. MIRTs	611
D. Schutz der Anwender und Verbraucher	614
I. Warnung und Information (Warnmeldungen)	614
II. Allianz für Cybersicherheit	616
III. Verbraucherschutz (zB Unterstützung der Klagen der Verbraucherzentralen)	616
IV. IT-Sicherheitskennzeichen und Zertifizierung	617
V. Mitarbeit bei der Standardisierung und Normung	618
VI. Mitwirkung bei Digitalisierungsvorhaben	619

Kapitel 15.3. IT-Sicherheitsrecht der (Bundes)Länder

A. Kompetenzgefüge der IT-Sicherheit in Bund und Ländern	621
I. Öffentliche Sicherheit	621

II. IT-Sicherheit als staatsverwaltende und gefahrenabwehrrechtliche Forderung	622
III. Sicherung staatlicher Strukturen	624
IV. Sicherung der Zivilgesellschaft (Daseinsvorsorge)	624
B. Spezifische landesgesetzliche Regelungen	627
I. Grundlegende Strukturen und Probleme	627
II. Grundelemente der IT-Sicherheit der Länder	629
 Kapitel 15.4. Sichere elektronische Identitäten und sichere Identifizierung im E-Government	
A. Sichere elektronische Identitäten	633
I. Identifizierung und Identität in der Rechtsordnung	634
II. Notwendigkeit sicherer elektronischer Identitäten	635
B. Rechtsrahmen sicherer elektronischer Identitäten im Verwaltungskontext	636
I. Verfassungsrechtliche Vorgaben	636
II. Einfachgesetzlicher Rechtsrahmen	636
1. Rechtsrahmen auf EU-Ebene: eIDAS-Verordnung	637
a) Definitionen	638
b) Verpflichtung zur gegenseitigen Anerkennung	638
c) Notifizierung bei der Kommission	638
d) Vertrauensniveaus	639
e) Notifizierung der eID-Funktion des Personalausweises	640
f) Ausblick: EUid	640
2. Rechtsrahmen auf nationaler Ebene	641
a) eID-Funktion des Personalausweises	641
b) Mit der eID-Funktion des Personalausweises verwandte Identifizierungsmittel	646
c) Weitere im Verwaltungskontext relevante elektronische Identitäten	648
C. Sichere Identifizierung im E-Government	648
I. E-Government und wesentliche Rechtsgrundlagen auf Bundesebene	649
II. Anforderungen an die IT-Sicherheit im E-Government	651
III. Sichere elektronische Identifizierung im E-Government	652
1. Allgemeine Anforderungen	652
2. OZG-Nutzerkonten	653
D. Schnellübersicht	656

Kapitel 16. Gesundheit und Soziales

A. Einführung	663
I. Relevanz von Cybersicherheit im Gesundheitswesen	663
II. Bedeutung der Schutzziele der Informationssicherheit im Gesundheitsbereich	665
B. Rechtliche Grundlagen	666
I. Rechtsrahmen im Gesundheits- und Sozialbereich	667
II. Gesundheitssektoren	670
1. Stationärer Sektor	670
2. Ambulanter Sektor	672
a) Richtlinie zur IT-Sicherheit für Leistungserbringer nach SGB V	672
b) Informationssicherheit außerhalb des SGB V	673

III. Weitere Bereiche	673
1. Telemedizin	673
2. Medizinprodukte und Digitale Gesundheitsanwendungen	673
3. Cybersicherheit für Sozialdaten	676
4. Weitere Einrichtungen	677
IV. Ausblick zur Rechtsentwicklung	678
C. Telematikinfrastruktur und deren Anwendungen	678
I. Regulierungsrahmen	678
II. Gesellschaft für Telematik (gematik)	679
1. Organisation und Rechtsform	679
2. Gesetzliche Aufgaben und Aufträge	680
a) Zulassung von Betriebsleistungen, Komponenten und Diensten sowie von Anbietern und Herstellern	682
b) Bestätigung von weiteren Anwendungen	684
c) Folgen von Zulassungen und Bestätigungen	685
III. Telematikinfrastruktur als sichere Plattform	685
1. Definition und Systemüberblick	685
2. Systemaufbau und Architekturmerkmale	687
a) Struktur der Gesamtarchitektur	687
b) Bausteine und Zonen der TI	687
c) Sicherheitsrelevante Architekturmerkmale	691
3. Nachweis von Produktsicherheit	692
a) Produktzulassungen	693
b) Anbieter- und Herstellerzulassungen	695
c) Bestätigung der Sicherheit der Kartenherausgabeprozesse	696
4. Sicherheitsleistungen und Sicherheitsarchitektur der TI-Plattform	698
a) Elektronische Signaturen	698
b) Ver- und Entschlüsselung	699
c) PKI	700
d) Digitale Identitäten des Gesundheitswesens	701
e) Sichere Anbindung an das geschlossene Netz der TI	706
f) Sicherer Internetzugang	708
g) Zugang zu weiteren Anwendungen des Gesundheitswesens	709
5. Sicherheit im Betrieb	709
a) Zulassung von Diensten zum operativen Betrieb	710
b) Überwachung der Funktionsfähigkeit und Sicherheit	710
c) Ausblick	714
6. Zugriffskonzept	714
IV. Anwendungen der Telematikinfrastruktur	716
1. Versichertenstammdatenmanagement (VSDM)	717
2. Notfalldaten-Management (NFDm)	718
a) Elektronische Notfalldaten	719
b) Hinweise auf Patientenerklärungen	719
3. Elektronischer Medikationsplan (eMP)	720
4. Sichere Übermittlungsverfahren (SÜV)	721
a) Kommunikation im Medizinwesen (KIM)	721
b) eAU, eArztbrief und eAbrechnung über KIM	722
c) TI-Messenger	723
d) SÜV als zentraler Kommunikationsdienst	723
5. Elektronische Patientenakte (ePA)	724
a) Inhalte der ePA	724
b) Architektur	725

c) Dokumentenverwaltung	726
d) Verschlüsselungskonzept	727
e) Berechtigungsmanagement	728
6. Elektronisches Rezept (E-Rezept)	729
7. Elektronische Patientenkurzakte	733
D. Weitere sektorenspezifische Anforderungen und die Digitalisierung im Gesundheitswesen	734
I. Vertragsärztlicher Sektor	734
1. Rechtliche Vorgaben	734
a) Angemessene Cybersicherheit im ambulanten Bereich	735
b) Richtlinie zur IT-Sicherheit in der vertrags(zahn-)ärztlichen Versorgung	736
c) Vorgaben zur Zertifizierung geeigneter IT-Sicherheitsdienstleister	737
2. Anforderungen nach der IT-Sicherheitsrichtlinie der KBV	738
a) Differenzierung der Anforderungen nach Größe der Praxis	738
b) Maßnahmen für alle Praxen	739
c) Zusätzliche Maßnahmen für mittlere und große Praxen	742
d) Zusätzliche Maßnahmen für große Praxen	744
e) Maßnahmen für Praxen mit medizinischen Großgeräten	746
f) Maßnahmen für Praxen mit Komponenten der Telematik-Infrastruktur	748
g) Kritische Würdigung der IT-Sicherheitsrichtlinie	750
3. Sichere Integration der Telematik-Infrastruktur in die Arztpraxis	752
a) Einsatzumgebung für die TI-Komponenten	752
b) Integration in das Praxisverwaltungssystem (PVS)	752
c) Kartenterminals	752
d) Elektronischer Heilberufsausweis und elektronische Signaturen	753
II. Spezifische Herausforderungen der Digitalisierung im Gesundheitswesen	754
1. Videosprechstunde	754
2. Cloud-Nutzung	755
3. Ersetzendes Scannen	755
4. Umgang mit elektronisch signierten Dokumenten	756
a) Langfristiger Nachweis des Signaturzeitpunkts	757
b) Langfristige Beweiswerterhaltung der QES	757
5. Terminorganisation über Webanwendung	758
6. Cybersicherheit bei der Nutzung von E-Health-Anwendungen	758
E. Schnellübersicht	760

Kapitel 17. Gefahrenabwehr und Sanktionierung

A. Die Gewährleistung von Cyber-Sicherheit als Teil der öffentlichen Sicherheit	765
B. Die polizeiliche Abwehr konkreter Gefahren für die Cyber-Sicherheit	767
I. Polizeiliche Maßnahmen zur Abwehr konkreter Gefahren für die Cyber-Sicherheit	768
1. Standardmaßnahmen zur Abwehr konkreter Gefahren für die Cyber-Sicherheit	769
a) Unterbrechung der Telekommunikation	769
b) Beschlagnahme bzw. Sicherstellung	769
c) Weitere Standardmaßnahmen	770

2. Polizeiliche Generalklausel und die Abwehr konkreter Gefahren für die Cyber-Sicherheit	770
II. Polizeiliche Informationseingriffe	771
C. Cyber-Sicherheit durch Strafrecht	773
I. Strafrechtliche Verfolgung von Verletzungen der Cyber-Sicherheit	774
1. Strafbewehrung von Verletzungen der Cyber-Sicherheit	774
a) Einführung	774
b) Verletzungen der Integrität und Verfügbarkeit informationstechnischer Systeme und der darin gespeicherten Daten	776
c) Verletzungen der Vertraulichkeit informationstechnischer Systeme und der darin gespeicherten Daten	780
d) Überblick	782
2. Strafverfahren zur Verfolgung von Verletzungen der Cyber-Sicherheit	783
a) Besondere strafprozessuale Ermittlungsmaßnahmen zur Ausforschung von Verletzungen der Cyber-Sicherheit im Überblick	785
b) Mitwirkungspflichten in Strafverfahren	788
c) Zum Verhalten als Geschädigter	789
II. Straf- und bußgeldrechtliche Inpflichtnahme zur Gewährleistung von Cyber-Sicherheit	790
1. (Spezial-)Gesetzliche Verpflichtungen zur Gewährleistung von Cyber-Sicherheit	790
2. Erfolgszurechnung bei Verletzungen der Cyber-Sicherheit durch Dritte	792
D. Schnellübersicht	795

Kapitel 18. Nachrichtendienstrecht

A. Der Auftrag der Nachrichtendienste	800
I. Allgemeines	800
1. Abgrenzung der Nachrichtendienste zu Geheimdiensten	801
2. Trennungsgebot	801
3. Sammeln und Auswerten von Informationen	804
4. Keine Beschränkung auf Beratungs- bzw. Frühwarnfunktion	806
II. Der Auftrag der zivilen Verfassungsschutzbehörden (BfV, LfV)	808
1. §§ 3, 4 BVerfSchG als gemeinsamer Auftrag von BfV und LfV	808
2. Tatsächliche Anhaltspunkte als Anlass für ein Tätig werden	808
a) Bedeutung und Abgrenzung zu verwandten Begriffen	808
b) Tatsächliche Anhaltspunkte als Synonym für „Verdacht“	809
c) Begriffsdefinition	809
d) Verdachtsfall und Prüffall	810
3. Unterschied zwischen Extremismusbeobachtung („Bestrebungen“ erforderlich) und Spionageabwehr („Tätigkeit“ genügt)	811
4. Begriff der extremistischen Bestrebung	812
a) Personenzusammenschluss als Beobachtungsobjekt	812
b) Politische Zielsetzung erforderlich	813
c) Ziel- und zweckgerichtete Verhaltensweisen	814
d) Bezug zu Gewalt- bzw. Straftaten	815
e) Bezug zu konkreten Gefahren	815

5. Entschließungsermessen und Auswahlermessen bei der Beobachtung	816
6. Nötiger Inlandsbezug, aber Zulässigkeit der Tätigkeit auch im Ausland	816
7. Die zentralen Beobachtungsfelder des Verfassungsschutzes	817
a) Bestrebungen gegen die freiheitlich-demokratische Grundordnung (§ 3 Abs. 1 Nr. 1 BVerfSchG)	817
b) Bestrebungen gegen die Sicherheit des Bundes oder eines Landes (§ 3 Abs. 1 Nr. 1 BVerfSchG)	818
c) Spionageabwehr (§ 3 Abs. 1 Nr. 2 BVerfSchG)	819
d) Bestrebungen, durch die mittels Anwendung oder Vorbereitung von Gewalt auswärtige Belange gefährdet werden (§ 3 Abs. 1 Nr. 3 BVerfSchG)	830
e) Bestrebungen gegen den Gedanken der Völkerverständigung (§ 3 Abs. 1 Nr. 4 BVerfSchG)	831
III. Der Auftrag des Militärischen Abschirmdienstes	831
IV. Der Auftrag des Bundesnachrichtendienstes	832
1. Informationen von außen- und sicherheitspolitischer Bedeutung	832
2. Wichtige Aufklärungsfelder des BND	833
3. Keine eingrenzenden Voraussetzungen für Datenerhebung	833
B. Die Befugnisse der Nachrichtendienste	834
I. Allgemeines zu den Datenerhebungsregeln im BVerfSchG	835
II. Die wichtigsten Regelungen zu Erhebung von personenbezogenen Daten im BVerfSchG	835
III. Besondere Anforderungen für die Datenerhebung aus IT-Systemen	838
IV. Eingriffe in das Telekommunikationsgeheimnis nach Art. 10 GG	840
1. Schutzbereich des Telekommunikationsgeheimnisses	840
2. Überwachungsmaßnahmen nach dem G10	841
V. Übermittlung nachrichtendienstlicher Erkenntnisse an Polizei- und Strafverfolgungsbehörden	842
1. Übermittlungspflicht bei Staatsschutzdelikten (§ 20 Abs. 1 BVerfSchG)	842
2. Fakultative Übermittlungsmöglichkeit bei Allgemeinkriminalität und für sonstige erhebliche Zwecke der öffentlichen Sicherheit (§ 19 Abs. 1 BVerfSchG)	844
3. Übermittlungsverbote (§ 23 BVerfSchG)	845
4. Änderungsbedarf bei den Übermittlungsvorschriften	846
VI. Übermittlung relevanter Informationen an die Nachrichtendienste	847
C. Schnellübersicht	848

Kapitel 19. IT-Sicherheitsforschung

A. Datenschutzrechtliche Anforderungen	851
I. Datenverarbeitung für wissenschaftliche Forschungszwecke	851
II. Personenbezogene Daten	851
1. Verarbeitung von technischen Daten durch IT-Sicherheitsforscher	851
2. Beispiel: Personenbezug von IP-Adressen	852
3. Bedeutung für die Praxis	852
III. Zulässigkeit der Datenerhebung	853
1. Datenerhebung auf Grund berechtigter Interessen (Art. 6 Abs. 1 S. 1 lit. f DS-GVO)	853

- 2. Datenerhebung auf Grund einer Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DS-GVO) 854
 - 3. Zweitverwertung von Daten für Forschungszwecke (Art. 5 Abs. 1 lit. b DS-GVO) 854
 - 4. Datenerhebung auf Grund gesetzlicher Spezialvorschriften 855
- IV. Geeignete Garantien nach Art. 89 DS-GVO 856
 - 1. Die dreistufige Prüfung nach Art. 89 Abs. 1 DS-GVO 856
 - 2. Maßnahmen zur Datenminimierung in der Praxis 857
- V. Privilegierung der Datenverarbeitung für Forschungszwecke 858
- VI. Fazit 859
- B. Zivilrechtliche Haftung für Schäden 859
 - I. Risiken der Forschung 859
 - II. Fachliche Prüfung der Risiken vor Beginn des Forschungsvorhabens 860
 - 1. Konflikt zwischen Eigentums- und Wissenschaftsfreiheit 860
 - 2. Prüfung von Sicherheitsvorschriften und anerkannten Standards 860
 - 3. Fachliche Risikobewertung 860
 - 4. Haftungsrisiken und Risikovorsorge 861
 - a) Eintritt unerwarteter Schäden 861
 - b) Risikovorsorge 861
 - III. Veröffentlichung von Schwachstellen 862
 - 1. Recht zur Veröffentlichung wissenschaftlicher Ergebnisse 862
 - 2. Datenschutzrechtliche Grenzen 862
 - 3. Sicherheitsvorschriften und anerkannte Standards 863
 - 4. Fachliche Risikobewertung 863
 - IV. Fazit 865
- C. Strafrechtliche Grenzen der IT-Sicherheitsforschung 865
 - I. Im IT-Forschungszusammenhang relevante Strafvorschriften 865
 - 1. § 202a StGB (Ausspähen von Daten) 865
 - 2. § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten) 866
 - 3. § 303a StGB (Datenveränderung) 866
 - 4. § 303b StGB (Computersabotage) 866
 - II. Methoden der IT-Sicherheitsforschung 867
 - 1. „Scanning“ 867
 - 2. „IP-Spoofing“ 868
 - 3. „Hacking“ 868
 - 4. Reverse Engineering 868
 - 5. Honeypots 869
 - III. Vertrieb oder Weitergabe von IT-Sicherheitssoftware an Dritte 870
 - IV. Informationen über IT-Sicherheitslücken 871
 - V. Fazit 871
- D. Schnellübersicht 872

Kapitel 20. Neue Technologien und Verbraucherschutz

Kapitel 20.1 Vertrauensdienste im privaten Sektor

- A. Vertrauensdienste für sichere Transaktionen im Binnenmarkt 874
 - I. Sichere elektronische Interaktion zwischen Bürgern, Unternehmen und öffentlichen Verwaltungen 874
 - 1. Sicherheit der Herkunftsangabe (Authentizität, Nichtabstreitbarkeit) 874

2. Sicherheit vor unbemerkter Veränderung (Integrität)	875
3. Sicherheit vor unbefugtem Zugriff (Vertraulichkeit)	875
4. Einhaltung von gesetzlichen oder vertraglichen Formvorschriften (Formwirksamkeit)	875
5. Einhaltung steuerrechtlicher, handelsrechtlicher und sonstiger Vorschriften (Compliance)	877
6. Beweiswirkung und Beweisbarkeit vor Gericht (Durchsetzbarkeit)	877
7. Anerkennung im grenzüberschreitenden Rechtsverkehr (Internationalität, Kompatibilität, Interoperabilität)	877
II. Elektronische Signaturen	878
1. Elektronische Signaturen	878
2. Fortgeschrittene elektronische Signaturen	878
3. Qualifizierte elektronische Signaturen	878
4. Fernsignaturen	879
5. Rechtswirkung und Beweiswert qualifizierter elektronischer Signaturen	879
6. Praktische Anwendung	880
III. Elektronische Siegel	881
1. Elektronisches Siegel	881
2. Fortgeschrittene elektronische Siegel	882
3. Qualifizierte elektronische Siegel	882
4. Rechtswirkung und Beweiswert qualifizierter elektronischer Siegel	882
5. Anwendungsbereiche qualifizierter elektronischer Siegel	882
IV. Zeitstempel	883
1. Elektronische Zeitstempel	883
2. Qualifizierte elektronische Zeitstempel	883
3. Nutzen qualifizierter elektronischer Zeitstempel	883
V. Elektronische Einschreiben	884
1. Elektronische Einschreiben	884
2. Qualifizierte Dienste für die Zustellung elektronischer Einschreiben ...	884
3. Rechtswirkung elektronischer Einschreiben	885
VI. Validierung und Bewahrung von qualifizierten elektronischen Signaturen bzw. Siegeln	885
1. Validierung	885
2. Bewahrung	886
VII. Website-Authentifizierung	887
VIII. Zusammenfassung	887

Kapitel 20.2 Blockchain, Smart Contracts und Künstliche Intelligenz

A. Grundlagen der Regulierung neuer Technologien	889
I. Verfassungsrechtlicher Ausgangspunkt	889
II. Die Rolle europäischen und internationalen Rechts	891
III. Bedeutung von Normen und Standards	891
B. Künstliche Intelligenz – KI-Systeme	892
I. Begriff	892
II. Stand der Regulierung und Normung	894
1. Anwendung der bestehenden Regelungen	894
2. EU-Gesetzesinitiative zu KI-Systemen	895
3. Stand der Normung	897
III. KI-Systeme als Bedrohung und Schwachstelle der Cybersicherheit	897
1. Neuartige Angriffe auf KI-Systeme	897
2. Risikobewertung bei KI-Systemen	898

3. Schutzmaßnahmen 899

IV. KI-Systeme als technische Maßnahme gegen Cyberbedrohungen 900

C. Blockchain und Smart Contracts 901

 I. Grundlagen der Blockchain-Technologie 901

 II. Stand der Regulierung und Normung 902

 1. Anwendung allgemeiner Regelungen – Normadressat 902

 2. Regulierungsbedarf und Initiativen 903

 3. Normen und Standards 904

 III. IT-sicherheitsrechtliche Bewertung 905

 1. Sicherheitseigenschaften der Blockchain-Technologie 905

 2. Konsensmechanismen 906

 3. Bezug zu externen Daten und Vorgängen 907

 4. Angriffspunkte und Schwachstellen 908

 IV Smart Contracts 909

 1. Begriff und rechtliche Bedeutung 909

 2. Angriffspunkte und Gegenmaßnahmen 910

 V. Blockchain-Anwendungen im Finanzsektor 911

 1. Zahlung und Handel mit Kryptotoken 911

 2. Initial Coin Offerings 912

Kapitel 20.3 Digitaler Verbraucherschutz durch Security Updates und IT-Kennzeichen

A. Security Updates nach der Digitale-Inhalte-Richtlinie (DI-RL) und der Warenkauf-Richtlinie (WK-RL) 915

 I. Anwendungsbereiche der DI-RL und der WK-RL und Umsetzung im BGB 916

 1. Sachlicher Anwendungsbereich 916

 2. Persönlicher Anwendungsbereich 918

 3. Daten als Entgelt? 921

 II. Subjektive und objektive Anforderungen an die Vertragsmäßigkeit 921

 III. Anspruch auf (Sicherheits-)Aktualisierungen 923

 IV. Form der Bereitstellung von Updates und Informationspflicht 925

 V. Dauer der Updatepflicht 926

 1. Fortlaufende bzw. dauerhafte Bereitstellung 927

 2. Einmalige Bereitstellung 927

 VI. Abweichende Vereinbarungen 928

 VII. Änderungen an digitalen Produkten 929

 VIII. Rechtsbehelfe und Beweislast 930

 IX. Verjährung 930

 X. Zusammenfassung 931

B. Verbraucherkennzeichen für IT-Sicherheit 932

 I. Freiwilliges IT-Sicherheitskennzeichen (§ 9c BSIG) 932

 1. Sachlicher und persönlicher Anwendungsbereich 933

 2. Inhaltliche Anforderungen 933

 a) Herstellererklärung 934

 b) Sicherheitsinformation des BSI 935

 3. Verfahren 935

 4. Anbringung und Gestaltung des IT-Sicherheitskennzeichens 935

 II. IT-Sicherheitszertifizierung (§ 9 BSIG) 936

 III. Europäische Kennzeichen und Zertifizierungen 938

 1. Freiwillige Selbstbewertung (Art. 53 CSA) 938

2. Cybersicherheitszertifizierung (Art. 56 CSA)	938
IV. Zusammenfassung	939

Kapitel 20.4 Schutz der Meinungs- und Willensbildung vor technologiegestützten Interventionen

A. Der Schutz demokratischer Öffentlichkeit als IT-Sicherheitsproblem	941
B. Beeinträchtigung der demokratischen Willens- und Meinungsbildung – Akteure und Erscheinungsformen	942
I. Veränderung der öffentlichen Meinungsbildung	943
II. „Hassrede“, Desinformation und verwandte Phänomene	944
III. Automatisierte Propaganda und „nichtauthentisches“ Verhalten	946
IV. „Dark Social“ – Kommunikation in geschlossenen Foren	947
C. Rechtliche Vorgaben, Regulierungsebenen und -instrumente	947
I. Staatliche Gewährleistungsverantwortung für die Integrität der Kommunikation	947
II. Der Schutz von Wahlen und Abstimmungen	948
III. Der Schutz der gesellschaftlichen Meinungsbildung	950
1. Schutz von Infrastrukturen und digitalen Diensten	950
2. Standards für die Kommunikation in den sozialen Netzwerken	951
IV. Grenzen des IT-Sicherheitsrechts	955

Kapitel 21. Internationaler Rahmen

Kapitel 21.1 Rechtsrahmen in der Europäischen Union

A. EU NIS-Richtlinie	958
B. EU Datenschutz-Grundverordnung	960
C. EU Cybersecurity Act (Rechtsakt zur Cybersicherheit)	961
D. Verordnung zur Errichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung	965

Kapitel 21.2 US-amerikanische Regulierung der IT-Sicherheit

A. Bundesebene	966
I. Sektorspezifische Cybersecurity-Gesetze	967
1. Health Insurance Portability and Accountability Act (HIPAA)	967
2. Gramm-Leach-Bliley Act	968
3. Federal Information Security Management Act (FISMA)	969
4. Sarbanes-Oxley-Act (SOX)	970
II. Strafrechtliche Regelungen	971
III. Die Rolle der Federal Trade Commission (FTC)	972
IV. Sonstige staatliche Maßnahmen und Förderung der Selbstregulierung	972
V. Gesetzesinitiativen	976
B. US-Bundesstaaten	977

Kapitel 21.3 Japanisches Cyber-Sicherheitsrecht

A. Cybersicherheitsgrundgesetz	978
I. Zweck und Entstehungsgeschichte	979
II. Charakteristika	980
III. Relevante Institutionen	980
1. Strategische Zentrale für Cybersicherheit	980

2. NISC: Nationales Institut für Cybersicherheit	981
3. Cybersicherheitsrat (überarbeitet in 2018)	981
B. Gesetz zum Schutz personenbezogener Daten in Japan	981
I. Grundlegende Merkmale des japanischen Gesetzes zum Schutz personenbezogener Daten	981
II. Gesetzesreform von 2015	982
III. Gesetzesreform von 2020	982
1. Meldepflicht für Datenlecks	983
2. Verschärfung der Sanktionen	983
3. Extraterritoriale Anwendung von Gesetzen und grenzüberschreitende Datentransfers	983
4. Keine Datenlokalisierung	983
C. Weitere wirtschafts- und strafrechtliche Vorschriften	984
I. Strafrecht	984
II. Geschäftsgeheimnisschutz	984
1. Zweck und Entstehungsgeschichte	984
2. Schutzvoraussetzungen	985
3. Verletzungstatbestände und Rechtsfolgen	986
III. Wettbewerbsrechtlicher Schutz von Big Data	987

Kapitel 21.4 Cybersecurity-Regulierung in Israel

**Kapitel 21.5 Korea’s Cybersecurity Regulations and Enforcement
related to Security Incidents**

A. Overview of Korea’s Cybersecurity Regulatory Regime	992
B. Protection of ICN: Cybersecurity Provisions under the Network Act	993
I. Overview	993
II. Security obligations imposed on ICSPs	994
III. Penalty provisions for cybercrime perpetrators	995
C. Protection of personal information: Cybersecurity Provisions under the PIPA	995
I. Overview	995
II. Obligations which arise from personal information leakage	997
III. Investigation and issuance of administrative sanctions by regulators with respect to personal information leakages	997
D. Cybersecurity obligations under other laws	998
I. Overview	998
II. EFTA’s cybersecurity provisions	998
1. Security obligations for financial companies and electronic financial business operators	998
2. Penalty provisions for cybercrime perpetrators	999
III. Other laws’ cybersecurity provisions	999
1. Matters of compliance regarding cloud computer services	999
2. Penalty provisions for cybercrime perpetrators in other laws	999

Kapitel 21.6 Cybersecurity Regulation in China

A. Introduction	1001
B. Security standards	1002

C. Cross-border data transfer	1003
I. Critical information infrastructure operators	1003
II. Other organisations	1004
D. Security reviews for purchases of equipment and services by CIIOs	1004
E. Data Security Law	1005
F. Important data	1006
G. Mandatory breach notifications	1007

Kapitel 21.7 Cybersecurity in Russia

A. General understanding	1008
B. General overview of legal requirements	1010
I. Information security	1010
II. Sovereign Internet	1011
III. Security of critical information infrastructure	1012
IV. The Yarovaya Law and the Telegram case	1012
V. Personal data	1013
VI. Restrictions on the use of anonymisers	1014
C. Liability	1014
D. Trends	1015

Kapitel 21.8 Cybersecurity Law and Policy in India

A. Introduction	1016
B. The Information Technology Act, 2000	1016
I. National Cybersecurity Agency	1017
II. Reasonable Security Practices and Procedures and Cybersecurity Obligations	1018
III. Critical Infrastructure	1019
IV. Management of Security Incidents	1020
C. Sectoral Requirements	1021
I. Financial Services	1021
II. Insurance Sector	1022
III. Securities Market	1023
IV. Telecom Sector	1023
D. Conclusion	1024

Kapitel 22. Völkerrechtliche Aspekte, Cyberwarfare

A. Völkerrechtlich relevante IT-Sicherheitsvorfälle	1027
I. DDoS-Attacken, Defacement, Stuxnet	1027
II. Völkerrechtliche Relevanz	1028
III. Begriff der Cyber-Operation	1029
IV. Cyber-Operationen mit hoher Intensität	1030
1. Art. 39 UN-Charta: Aggression	1031
2. Art. 2 Nr. 4 UN-Charta: Gewaltverbot	1032
a) Waffenbegriff der UN-Charta	1032
b) Effekt-Äquivalenz und Kriterienkatalog nach Tallinn Manual	1033
3. Art. 51 UN-Charta: Selbstverteidigungsrecht	1033
a) Erheblichkeitsschwelle	1034

b) Identifikation des Angreifers	1034
c) Verhältnismäßigkeit	1035
d) Präventivmaßnahmen	1035
e) DDoS-Attacken und gezielter Einsatz von Schadprogrammen als bewaffneter Angriff	1035
V. Niederschwellige Cyber-Operationen	1036
1. Interventionsverbot	1036
2. Propaganda und Spionage	1036
VI. Cyber-Operationen als Gegenmaßnahme	1038
1. Countermeasures	1038
2. Self-contained Regime	1038
VII. Zurechnungsfragen	1039
1. Attribution	1039
2. Cybersecurity Due Diligence	1039
VIII. Cyber-Operationen gegen Nichtverantwortliche (Notstand)	1040
IX. Entwicklung der Staaten-, Resolutions- und sonstigen Praxis	1040
X. Neuere Entwicklung in der völkerrechtlichen Debatte um „Hackbacks“	1043
XI. EU Cyber-Sanktionsmechanismus	1044
B. Die Bundeswehr im Cyber- und Informationsraum	1045
I. Struktur- und Kompetenzentwicklung	1045
1. Das Kommando Cyber- und Informationsraum (KdoCIR)	1045
2. Agentur für Innovation in der Cybersicherheit (Cyberagentur)	1045
II. Verfassungsrechtliche Determinanten	1046
1. Art. 26 GG	1046
a) Eignung und Absicht der Friedensstörung	1046
b) Art. 26 und offensives Wirken im Cyberraum	1047
2. Art. 87a GG	1047
a) „Verteidigung“ und „Einsatz“ iSd Art. 87a GG	1047
b) Bewertung einzelner Szenarien	1048
C. Schnellübersicht	1048

Kapitel 23. Anwendungsszenarien

A. Einleitung	1052
B. Typische Angriffe auf IT-Systeme	1052
I. Externes Perimeter	1053
1. Firewall	1053
a) Typische Schwachstellen	1053
b) Gegenmaßnahmen	1054
2. Webpräsenz	1054
a) Typische Schwachstellen	1054
b) Gegenmaßnahmen	1055
II. Benutzersicht	1056
1. PC-Arbeitsplätze	1056
a) Typische Schwachstellen	1056
b) Gegenmaßnahmen	1057
2. Mobiles Arbeiten	1058
a) Typische Schwachstellen	1058
b) Gegenmaßnahmen	1059
3. Bring your own Device (BYOD)	1059
a) Typische Schwachstellen	1059

b) Gegenmaßnahmen	1060
III. Administrationssicht	1060
1. Netzwerksicherheit	1060
a) Typische Schwachstellen	1061
b) Gegenmaßnahmen	1062
2. Patchen von Systemen	1063
a) Typische Schwachstellen	1063
b) Gegenmaßnahmen	1064
3. Härtung	1065
a) Typische Schwachstellen	1065
b) Gegenmaßnahmen	1066
IV. Operational IT (OT)	1066
1. Typische Schwachstellen	1067
2. Gegenmaßnahmen	1067
V. Nicht technische Angriffe	1068
1. Typische Angriffe	1069
2. Gegenmaßnahmen	1071
C. Vorbereitung auf IT-Notfälle	1071
I. Typische Fehler bei einem IT-Notfall	1071
II. Gegenmaßnahmen	1073
D. Systematische Ansätze zur Steigerung der IT-Sicherheit	1074
I. Offensive Security	1074
1. Penetrationstests	1074
2. Redteaming	1075
3. Dokumentation	1076
4. Nachteile offensiver Security-Tests	1077
II. Security-by-Design	1077
1. Einführung	1077
2. Angewandte Vorgehensmodelle und Best Practice-Lösungen	1078
3. Bedrohungsmodellierung nach der STRIDE-Methodik	1079
4. Systematisierte Risikobewertung	1080
5. Erarbeitung von Maßnahmen, Sollvorgaben und Sicherheitszielen	1082
6. Security-by-Design Nutzenpotenziale für mehr IT-Souveränität in Deutschland und der EU	1083
E. Schnellübersicht	1083
Glossar	1085
Anhang – Technische Anlage KBV u. BÄK	1113
Sachverzeichnis	1125

