

Inhaltsverzeichnis

Vorwort	5
Vorwort zur 1. Auflage	7
Bearbeiterverzeichnis	15
Abkürzungsverzeichnis	19

Teil 1

Grundlagen der IT-Sicherheit

§ 1 Einführung	29
A. IT-Sicherheit als Herausforderung für die Gesellschaft	29
B. Begriffliche Grundlagen	32
C. Spezifika rechtlicher Regelungen zur IT-Sicherheit	36
D. IT-Sicherheitsrecht als Rechtsgebiet im Entstehen	38
§ 2 IT-Sicherheit aus technischer Sicht	42
A. Grundlagen: Computer, Netzwerke und Sicherheit	44
B. Bedrohungen, Sicherheitsanforderungen und ihre Handhabung	49
C. Besondere Angriffstechniken	58
D. Grundlegende Schutzmaßnahmen	62
E. Entwicklungsperspektiven und aktuelle Forschung zur IT-Sicherheit	72
§ 3 IT-Sicherheit aus ökonomischer Perspektive	78
A. Grundlagen der Digitalisierung der Wirtschaft	80
B. Ökonomische Charakteristika der IT-Sicherheit	82
C. Kosten und Wirtschaftlichkeit von IT-Sicherheitsmaßnahmen	83
D. Wirtschaftliches Risiko mangelhafter IT-Sicherheit	86
E. IT-Sicherheit als Wettbewerbsfaktor	90
§ 4 IT-Sicherheit aus Nutzerinnen- und Nutzersicht	93
A. Einführung	93
B. Begrifflichkeiten Usability, Security, Privacy und Trust	94
C. „Usable Privacy and Security“ (UPS)	98
D. Zusammenfassung	109
§ 5 IT-Sicherheit aus gesamtgesellschaftlicher Sicht	110
A. Begriffe IT-Sicherheit und Cybersicherheit	111
B. Wahrnehmung der IT-Sicherheit	113
C. Politikfeld IT-Sicherheit	120

Teil 2

Grundlagen und Querschnittsfragen des IT-Sicherheitsrechts

§ 6	Die völkerrechtliche Dimension der IT-Sicherheit	133
	A. Einleitung	135
	B. UN-Rechtsfindungsprozesse	135
	C. Unilaterale und nichtstaatliche Initiativen	138
	D. Anwendbarkeit friedensvölkerrechtlicher Regelungen	139
	E. IT-Sicherheit durch Internet-Governance und internationales Exportkontrollrecht	155
	F. Fazit und Ausblick	159
§ 7	Verfassungsrechtliche Dimensionen der IT-Sicherheit	160
	A. Einleitung	161
	B. Was ist IT-Sicherheit?	163
	C. Besonderheiten und Herausforderungen der IT-Sicherheit	165
	D. Verfassungsrechtliche Fragestellungen	168
	E. Fazit und Ausblick	184
§ 8	Messung, Prüfung und Nachweis von IT-Sicherheit	185
	A. Einleitung	187
	B. Grundlagen der Prüfung und Bewertung von IT-Sicherheit	188
	C. IT-Sicherheit in Organisationen	191
	D. IT-Sicherheit von Software und Hardware	203
§ 9	IT-Sicherheit im Vertragsrecht und in der Vertragsgestaltung	218
	A. Einleitung	221
	B. IT-Sicherheit: ein Fall der Unmöglichkeit nach § 275 Abs. 1 BGB?	224
	C. Cyberrisiko als höhere Gewalt?	225
	D. IT-Sicherheit und Bestimmbarkeitsgrundsatz des Vertragsrechts	229
	E. Bedürfnis einer vertraglichen Gestaltung der IT-Sicherheit	234
	F. Vertragsrechtliche Implementierung von IT-Sicherheit als notwendiger Bestandteil des Cyberrisiko-Managements der Geschäftsleitung eines Unternehmens	239
	G. Vertragsrechtliche Einordnung der IT-Sicherheitspflicht	242
	H. Gewährleistung und schuldvertragliche Haftung für fehlende IT- Sicherheit	246
	I. Inhaltliche Ausgestaltung von Vertragsklauseln zur IT-Sicherheit	267
	J. Zusammenfassung und Ausblick	279
§ 10	Grundlagen deliktsrechtlicher Sicherheitspflichten	281
	A. Pflichtenbestimmungen	289
	B. Öffentlich-rechtliche Anforderungen und zivilrechtliche Haftung	296
	C. Mitverschulden und Eigenschutz des Betroffenen	310

§ 11	Verantwortung der IT-Hersteller (produktbezogene Pflichten)	313
	A. Überblick	313
	B. Verschuldensabhängige Produzentenhaftung	315
	C. Produkthaftung infolge Schutzgesetzverletzung (§ 823 Abs. 2 BGB): öffentlich-rechtliche Produktsicherheitsnormen	339
	D. Verschuldensunabhängige Produkthaftung (ProdHaftG)	341
	E. Haftung bei Open Source Produkten	350
§ 12	Verantwortung der Intermediäre, Betreiber und Nutzer	357
	A. Haftung der Intermediäre	357
	B. Haftung der Betreiber und Nutzer	362
§ 13	IT-Sicherheitsanforderungen an Kritische Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse und digitale Dienste nach dem BSIG	370
	A. Einführung	371
	B. Kritische Infrastrukturen	371
	C. Unternehmen im besonderen öffentlichen Interesse	402
	D. Digitale Dienste nach dem BSIG	403
§ 14	IT-Sicherheitsinfrastrukturen und -dienste	410
	A. Sicherheitsbedarf	413
	B. Sicherheitsinfrastrukturen und -dienste	414
	C. Recht der Sicherheitsinfrastrukturen und -dienste	419
	D. Zusammenfassung und Ausblick	443
§ 15	Recht der IT-Sicherheitsbehörden	445
	A. Einführung	446
	B. Internationaler und europäischer Rahmen	447
	C. Nationales Recht	458
	D. Ausblick	474
§ 16	Rechtliche Regeln für die IT-Sicherheit in Organisationen	478
	A. Gesetzliche Grundlagen	479
	B. Innere Verantwortlichkeitsverteilung in Unternehmen	481
	C. Typische Konfliktlinien	501
	D. Best Practices in Organisationen im Hinblick auf IT	502
	E. Ausblick auf zukünftige Gesetzesvorhaben	506
§ 17	IT-Sicherheit als Mittel und als Bedrohung des Datenschutzes	508
	A. IT-Sicherheit und Datenschutz	509
	B. Rechtliche Grundlagen	511
	C. Ambivalenz und Aggregation von IT-Sicherheit und Datenschutz	527
	D. Fazit	536

§ 18	Schutz der IT-Sicherheit durch Gefahrenabwehr, Strafverfolgung und nachrichtendienstliche Aufklärung	538
	A. Allgemeines	540
	B. Rechtsrahmen	540
	C. Systematik der sicherheitsbehördlichen Maßnahmen zum Schutz der IT-Sicherheit	545
	D. Akteure des behördlichen Schutzes der IT-Sicherheit und ihre Befugnisse	548
	E. Fazit und Ausblick	559
§ 19	Aufgaben und Befugnisse der Bundeswehr	560
	A. Cyberattacken und hybride Bedrohungen	561
	B. Art. 87a GG – Verteidigung	562
	C. Art. 24 Abs. 2 GG – Friedenssicherung	573
	D. Friedensgebot und parlamentarische Kontrolle	574
	E. Art. 35 GG – Amtshilfe und Katastrophennotstand	577
	F. Gesetzliche Grundlagen zur Ausübung von Befugnissen gemäß Art. 87a Abs. 1 S. 1 und 2 GG, Art. 24 Abs. 2 GG sowie Art. 87a Abs. 3 GG	580
§ 20	Schutz der IT-Sicherheit durch das Strafrecht	582
	A. Grundlagen	585
	B. Tatbestände zum Schutz der Vertraulichkeit von Daten	597
	C. Tatbestände zum Schutz der Integrität und Verfügbarkeit	606

Teil 3 Sektorales IT-Sicherheitsrecht

§ 21	Telekommunikation und digitale Dienste	617
	A. IT-Anwendung und IT-Infrastrukturen	619
	B. Besondere Risiken und Bedrohungen	631
	C. Sektorale Rechtsvorschriften	639
	D. Typische Problemlagen und Konfliktlinien	667
	E. Ausblick	669
§ 22	Mobilität und Verkehr	671
	A. IT-Anwendungen und IT-Infrastrukturen in den Verkehrsbranchen	674
	B. Besondere Risiken und Bedrohungen	687
	C. Sektorale Rechtsvorschriften im Bereich des Straßenverkehrs	693
	D. Typische Problemlagen und Konfliktlinien	711
	E. Fazit	715
§ 23	Energieversorgungsnetze und Energieanlagen	716
	A. IT-Anwendungen und IT-Infrastrukturen	716
	B. Besondere Risiken und Bedrohungen	718

C.	Sektorspezifische Rechtsvorschriften im EnWG, Seitenblick auf das Atomgesetz (AtG)	719
D.	Typische Problemlagen und Konfliktlinien	746
§ 24	Smart Metering	748
A.	IT-Anwendungen und IT-Infrastrukturen	750
B.	Besondere Risiken und Bedrohungen	752
C.	Sektorale Rechtsvorschriften im MsbG	753
D.	Typische Problemlagen und Konfliktlinien	773
§ 25	Öffentliche Verwaltung	778
A.	Einleitung	780
B.	Supranationales Recht	782
C.	Bundes- und Landesrecht	787
D.	Öffentliche Verwaltung als Kritische Infrastruktur	815
E.	Zusammenarbeit zwischen Bund und Ländern	822
F.	Fazit und Ausblick	828
§ 26	Private Haushalte	830
A.	IT-Anwendungen und IT-Infrastrukturen	832
B.	Besondere Risiken und Bedrohungen	837
C.	Spezielle Rechtsvorschriften	846
D.	Typische Problemlagen und Konfliktlinien	858
§ 27	Justiz	860
A.	Einleitung	861
B.	IT-Sicherheit in der Justizkommunikation	866
C.	IT-Sicherheitsaspekte im Scanvorgang	888
D.	Fazit und Ausblick	893
§ 28	Gesundheitswesen	894
A.	Einleitung	896
B.	IT-Anwendungen und IT-Infrastrukturen	896
C.	Besondere Risiken und Bedrohungen	897
D.	Sektorale Rechtsvorschriften	900
E.	Typische Problemlagen und Konfliktlinien	933
§ 29	IT-Sicherheitsrecht im Finanzsektor	935
A.	Einleitung	936
B.	Anwendung des allgemeinen IT-Sicherheitsrechts im Finanzsektor	937
C.	DORA (Digital Operational Resilience Act)	938
D.	Besonderes IT-Sicherheitsrecht bei Banken	945
E.	Besonderes IT-Sicherheitsrecht bei Versicherungen	957
F.	Besonderes IT-Sicherheitsrecht bei Finanzintermediären	961

G. Vertragsgestaltung zu IT-Sicherheit im Finanzsektor	962
H. Fazit	968
§ 30 Zusammen- und Widerspiel von Künstlicher Intelligenz und IT-Sicherheit(srecht)	969
A. „Künstliche Intelligenz“ – Annäherung an einen schillernden Begriff	970
B. Spezifische Problemstellungen	974
C. IT-Sicherheit von KI-Systemen	975
D. Gefahr für die IT-Sicherheit: KI als Angriffssystem	986
E. Mittel der IT-Sicherheit: KI als Präventions- und Reaktionsinstrument ...	989
F. Gewährleistungsrechte bei IT-Sicherheitsmängeln	990
G. Deliktische Haftung bei der Verletzung von IT-Sicherheitsanforderungen im Zusammenhang mit dem KI-Einsatz	992
Stichwortverzeichnis	997